Crypto Valley

www.cryptovalley.swiss

CVA RESEARCH JOURNAL 2023

DON'T TRUST, VERIFY.

RISK MANAGEMENT IN WEB3

TABLE OF CONTENTS

1. FOREWORD

The success of the 2022 Crypto Valley Association Research Journal stands as a testament to the collaborative dedication within the Crypto Valley Association's Education Working Group. Building on this accomplishment, the Working Group is resolutely advancing the project into the current year.

This year again, I spearheaded the Call for Papers 2023 on "Don't trust, verify. Risk Management in Web3." This publication primarily reflects the dedication of researchers and professionals who have committed their expertise and insights to drive excellence in our field.

The aim was to curate a select collection of essays aligned with the central theme, penned by both academic scholars and industry experts. The inclusion of these essays emerged from a voluntary and enthusiastic endeavor to support the Working Group within a remarkably demanding timeline.

Looking ahead, the Education Working Group intends to leverage the close collaboration between the Crypto Valley Association and the contributing authors, fostering strong connections for future endeavors. The Working Group and the Association express their satisfaction with the resounding success of this collaborative initiative.

Beyond the esteemed authors, the fruition of this project owes much to the diligent contributions of Aurelio Schmid, Luis Schaubhut, and Nikoletta Csanyi, whose multifaceted support was indispensable to its realization.

In conclusion, I extend heartfelt appreciation to all authors who submitted their papers and actively contributed to shaping a corpus of research crucial for the continuous evolution and prosperity of our industry. This collective effort is pivotal for steering the industry toward a thriving future.

Tilmar Wilhelm Goos, LL.M
Crypto Valley Association
Chairman Working Group Education
Initiator of the CVA Research Journal

2. THE CRYPTO VALLEY ASSOCIATION & ITS EDUCATION WORKING GROUP

The Crypto Valley, located in Zug, Switzerland, has emerged as a pivotal center for blockchain innovation, attracting key players in the industry. Notably, it became the headquarters of the Ethereum Foundation, established in 2014 by Vitalik Buterin, which introduced the groundbreaking smart contract platform revolutionizing decentralized applications (dApps) and the wider blockchain landscape. Additionally, the region has witnessed the rise of other influential blockchain ventures, including Cardano, a platform co-founded by Charles Hoskinson, and SEBA Bank, a financial institution offering digital asset-related services.

The Crypto Valley Association, formed in 2017, has played an integral role in fostering this ecosystem. Within the association, the Education Working Group collaborates with international universities on diverse educational projects to disseminate a comprehensive understanding of blockchain technology and its practical applications. This proactive involvement aims to enrich the industry by sharing cutting-edge research and insights, culminating in the annual release of the Crypto Valley Association Research Journal.

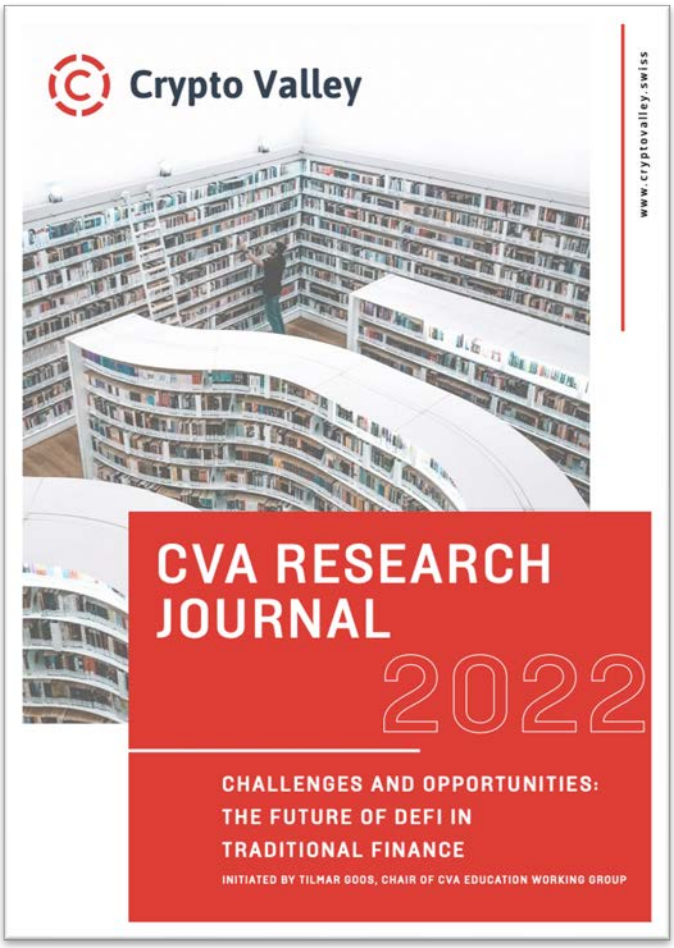
Recognizing the paramount importance of knowledge sharing, the Crypto Valley Association and its Education Working Group emphasizes the significance of disseminating expertise and experiences within the blockchain space. This dissemination of knowledge not only fuels innovation but also plays a fundamental role in advancing the adoption and utilization of blockchain technology, ensuring its continued growth and evolution.

3. 2022 RESEARCH JOURNAL: OPPORTUNITIES AND CHALLENGES. THE FUTURE OF DEFI IN TRADITIONAL FINANCE.

The Crypto Valley Association Education Working Group cordially invited interested author(s) to submit research papers for its 2022 Research Journal. Similar to several industries, the traditional financial industry has been adversely impacted by the COVID-19 pandemic.

The pandemic has highlighted the fragility of regional but also international economies and, more importantly, accelerated the digitalization in every aspect. Especially since the publication of the Bitcoin Whitepaper there is an urgent need to accelerate structural transformation and business resilience across the traditional financial industry. Greater digitalization and the ever-expanding DeFi industry clearly require the need for adaptation by the traditional financial industry are some of the most compelling policy considerations that can improve the trajectory of the recovery and resilience of the traditional financial industry.

Download the
2022 CVA RESEARCH JOURNAL
Challenges and Opportunities.
The Future of DeFi
in Traditional Finance



4. THE REGULATORY TAPESTRY: SWITZERLAND'S INTEGRAL ROLE IN NURTURING ZUG'S CRYPTO VALLEY

Abstract:
This in-depth exploration illuminates the nuanced regulatory framework that has propelled Switzerland, with particular emphasis on Zug, into a global epicenter for blockchain innovation, colloquially known as the "Crypto Valley." Examining historical foundations, legal intricacies, investor protection measures, decentralized governance models, fiscal advantages, and the global reputation that collectively define Switzerland's approach to blockchain, this analysis sheds light on the multifaceted regulatory ecosystem fostering innovation in Zug's Crypto Valley.

Historical Foundations:
Switzerland's journey into blockchain prominence commenced in the early 2010s, leveraging its historical reputation for financial stability and neutrality. As projects like Ethereum emerged, Switzerland strategically positioned itself as a global leader in the burgeoning blockchain industry, setting the stage for the development of Zug's Crypto Valley.

Legal Precision and Assurance:
Central to Switzerland's regulatory prowess is the commitment to legal clarity and certainty. The Swiss Financial Market Supervisory Authority (FINMA) has provided comprehensive guidelines, delineating the legal treatment of diverse token types. This approach mitigates regulatory uncertainties, instilling confidence and fortifying Zug's Crypto Valley as a beacon of legal assurance in the global blockchain landscape (FINMA, n.d.).

Investor Protection as a Pillar:
Switzerland's regulatory framework meticulously balances fostering innovation with safeguarding investor interests. Clear rules for token sales and stringent compliance with anti-money laundering (AML) and know your customer (KYC) regulations create an environment where investors feel protected (FINMA, n.d.).

Decentralized Governance Dynamics:
A distinctive feature of Switzerland's regulatory approach is its decentralized governance structure, rooted in federalism. This structure empowers cantons like Zug to enact policies independently, facilitating agile decision-making tailored to the dynamic needs of the blockchain industry (Swiss Confederation, n.d.).

Taxation Dynamics: Progressive and Strategic:

Switzerland's progressive taxation system, complemented by cantonal and municipal tax incentives, creates a fiscal environment conducive to blockchain enterprises. This strategic advantage attracts companies seeking innovation-friendly surroundings with tangible economic benefits (Swiss Federal Tax Administration, n.d.).

Seamless Integration with Banking Services:

Integral to the operational functionality of blockchain enterprises is seamless access to banking services. Switzerland's well-established banking sector, recognized for its openness to innovation, has been relatively receptive to blockchain businesses, fostering a symbiotic relationship between the traditional financial system and blockchain entities (Swiss Bankers Association, n.d.).

Global Trust Anchored in Reputation:

Switzerland's enduring reputation for financial stability and neutrality becomes a cornerstone for the global trust invested in its blockchain industry (World Economic Forum, 2021). Investors and businesses regard Switzerland as a reliable and secure jurisdiction, reinforcing the credibility of Zug's Crypto Valley on the international stage.

Conclusion:

A Tapestry of Regulatory Excellence and Innovation:

In the intricate tapestry of Switzerland's blockchain regulatory framework, each thread is carefully woven to create a masterpiece that is Zug's Crypto Valley. This comprehensive exploration has traversed the historical roots, legal intricacies, investor-centric focus, governance dynamics, fiscal advantages, and the global reputation that collectively define Switzerland's approach to blockchain.

As the dynamic landscape of blockchain technology continues to evolve, Switzerland's regulatory model stands as a guiding light, illuminating the path for other jurisdictions seeking to navigate the delicate balance between fostering innovation and maintaining regulatory oversight. The benefits derived from Swiss blockchain regulation are not confined to legal statutes; they are embedded in the very fabric of Zug's Crypto Valley, where the past, present, and future converge in a harmonious symphony of regulatory excellence and blockchain innovation.

Sources:

- FINMA. (n.d.). Guidelines for Enquiries Regarding the Regulatory Framework for Initial Coin Offerings (ICOs).
- Swiss Confederation. (n.d.). Federalism in Switzerland.
- Swiss Federal Tax Administration. (n.d.). Swiss tax system.
- Swiss Bankers Association. (n.d.). Blockchain/DLT: Regulatory Framework.
- World Economic Forum. (2021). The Global Competitiveness Report 2021.

Aurelio Schmid

Member of the Academic Committee

CVA Working Group Education

5. LIECHTENSTEIN: EMERGING AS A BLOCKCHAIN HUB IN THE HEART OF THE ALPS

Nestled between Switzerland and Austria, the Principality of Liechtenstein has quietly emerged as a formidable contender in the global blockchain and crypto landscape. Despite its small size, Liechtenstein has demonstrated a forward-thinking approach by fostering an environment conducive to innovation in the realm of blockchain technology. With a unique blend of regulatory clarity, geographic advantages, and strategic partnerships, this Alpine nation is positioning itself as the next blockchain powerhouse alongside its renowned neighbor, Switzerland.

A Regulatory Pioneer

One of Liechtenstein's defining moments came in 2019 when it solidified its commitment to the blockchain industry by enacting the Token and Trusted Technology Service Providers Act (TVTG), also known as the Liechtenstein Blockchain Act. This landmark legislation marked Liechtenstein as one of the first countries globally to establish comprehensive regulation for the crypto and blockchain domain. The TVTG introduced the revolutionary concept of the Token Container Model (TCM), which classified tokens based on their functionalities—utility tokens, security tokens, or payment tokens. This pioneering approach laid the foundation for a dynamic and flexible regulatory framework that adapts to the ever-evolving blockchain landscape. This foresight has proven vital, as innovations such as decentralized finance (DeFi) and non-fungible tokens (NFTs) have rapidly gained prominence.

Innovation Amidst the Alps

Despite the absence of decentralized finance applications and non-fungible tokens on the scale they exist today, Liechtenstein's Blockchain Act anticipated the future scope of blockchain applications. With an emphasis on an open and innovation-friendly approach, the TVTG stands as a testament to the country's commitment to encouraging technological advancement while mitigating risks.

Crucially, Liechtenstein's regulatory framework provides a balance between regulatory certainty and fostering innovation. The Act mandates regulatory requirements for activities that pose user risks, irrespective of their business models. This innovative approach incentivizes businesses to adopt technology-driven solutions to manage these risks while avoiding stifling overregulation.

This small nation, with its progressive regulatory framework and strategic positioning, is not only fostering innovation but also hosting influential conferences that shape the future of the industry. Let's delve into how Liechtenstein is paving the way for blockchain innovation while hosting premier conferences in the DACH region: Fintech.li Conference: Embracing the

Future of Finance: One of the cornerstones of Liechtenstein's blockchain ecosystem is the Fintech.li Conference. This conference serves as a nexus for industry leaders, innovators, and changemakers in the digital assets and web3 space. As the world of blockchain and fintech rapidly evolves, the Fintech.li Conference provides a platform to explore the latest trends, navigate regulatory landscapes, and uncover investment opportunities. And the Token Summit by the CCA: Unraveling the Blockchain Landscape. This flagship blockchain conference not only delves into the legal fundamentals of the blockchain industry within and beyond Liechtenstein's borders but also seeks to demystify the underlying technology. As blockchain technology continues to redefine industries, understanding its intricacies is pivotal for both newcomers and veterans in the field. The Token Summit serves as an educational beacon, bridging the gap between legalities and technological advancements.

MiCA and Liechtenstein's Compatibility

The European Union's forthcoming Markets in Crypto-Assets (MiCA) regulation mirrors Liechtenstein's visionary model. The Token Container Model (TCM), licensing requirements, and information standards present in the Liechtenstein Blockchain Act have served as inspiration for the MiCA draft. The alignment between the two regulatory approaches creates a harmonious environment for the blockchain industry, fostering cross-border innovation and growth. The country's proactive stance ensures compatibility between the TVTG and MiCA, enhancing regulatory clarity and minimizing ambiguity for businesses.

A Progressive Approach to Payments

Liechtenstein's foray into the world of blockchain extends beyond regulation. Finance Minister Daniel Risch has proposed the integration of Bitcoin as a means of payment for public services. This initiative highlights Liechtenstein's continued enthusiasm for blockchain technologies, driven by a recognition of their potential to transform traditional systems. However, the proposal comes with a twist: Bitcoin payments will be instantly converted into the Swiss franc, the nation's currency, to mitigate the cryptocurrency's notorious volatility. This innovative approach demonstrates Liechtenstein's commitment to harnessing the benefits of blockchain technology without exposing its citizens to unnecessary risks.

Strategic Geographical Positioning

Liechtenstein's location provides a strategic advantage that complements its regulatory approach. Its close proximity to Switzerland and membership in the European Economic Area (EEA) place it at the crossroads of European financial markets. This unique positioning enables Liechtenstein to leverage the benefits of both regions, offering a gateway to the vast European market while maintaining a favorable regulatory framework.

Additionally, the country's small size enhances its adaptability. While Switzerland's efforts are commendable, Liechtenstein's agility in tailoring its regulations to the blockchain

landscape's rapid evolution showcases its commitment to remaining at the forefront of innovation.

Liechtenstein's ascent as a prominent blockchain hub underscores the nation's foresight, innovation, and dedication to embracing technological progress. With its pioneering regulatory framework, commitment to adaptation, and strategic alliances, Liechtenstein is proving itself a worthy contender in the blockchain realm alongside its esteemed neighbor, Switzerland. In the picturesque landscape of the Alps, Liechtenstein is quietly spearheading blockchain innovation and solidifying its place as a global leader in the industry. With a pioneering regulatory environment that encourages both innovation and investor protection, Liechtenstein stands as a beacon of progres. By its pioneering regulatory framework, represented by the Token and Trusted Technology Service Providers Act, not only safeguards users but also encourages businesses to embrace technological solutions for risk management. The compatibility between Liechtenstein's framework and the MiCA regulation underscores its global influence in shaping the future of blockchain governance. Moreover, by hosting conferences like the Fintech.li Conference and the Token Summit, the nation is not only shaping discussions but also laying the groundwork for a future where blockchain technology and digital assets play an integral role in reshaping industries and economies across the world.

Furthermore, Liechtenstein's practical approach to blockchain adoption, as exemplified by Finance Minister Daniel Risch's proposal, showcases a nation that seeks to capitalize on blockchain's benefits while safeguarding its citizens against the inherent volatility of cryptocurrencies. In the heart of the Alps, Liechtenstein stands not only as a blockchain hub but as a beacon of innovation that takes a well-rounded and holistic approach to the opportunities and challenges presented by the ever-evolving blockchain landscape.

Luis Schaubhut
Member of the Academic Committee
CVA Working Group Education

6. 2023 CALL - FOR - PAPERS: DON'T TRUST, VERIFY. RISK MANAGEMENT IN WEB3

The Crypto Valley Association Working Group Education cordially invited researchers and professionals from all over the world to submit their original research papers for the Call for Papers 2023 (CFP23) with the theme "Don't Trust, Verify. Managing Risk in Web3."

It is even more important after the various happenings from 2021 to 2023 in the blockchain, DeFi and TradFi world. The theme for this year's call for papers focused on exploring these risks and developing strategies to manage them.

We wee seeking high-quality, original research papers that address the various aspects of risk management in the context of Web3. Papers could include, but were not limited to, topics such as:

- Cybersecurity threats and vulnerabilities in Web3
- Technology Tech to mitigate counterparty risk
- Risk management strategies for decentralized networks
- Legal and regulatory issues in managing risk in Web3 Privacy concerns and data protection in Web3
- Economic and financial risks in decentralized networks
- DeFi Decentralized finance risk management.
- Governance and decision-making in decentralized networks
- Geopolitical and regulatory challenges for web3

Why Participate?

The Call for Papers 2023 provides an excellent opportunity for researchers and professionals to present their latest research findings, share their knowledge and expertise, and contribute to the advancement of the Web3 ecosystem.

Accepted papers are published in a high-quality, peer-reviewed journal, giving authors the opportunity to showcase their work to a global audience.

Sub-Themes

- Decentralized Finance (DeFi) risks and management strategies
- Smart contract risks and auditing techniques
- Governance risks and management practices in decentralized systems
- Privacy risks and protection strategies in decentralized systems
- Interoperability risks and solutions in Web3 ecosystems
- Security risks and best practices for Web3 applications and platforms
- Legal and regulatory risks in Web3 and their management
- User education and adoption of risk management practices in Web3 environments

Scoring Domains

- Originality and significance of the research topic
- Clarity and coherence of the research question/hypothesis
- Relevance and contribution to the field
- Methodological rigor and appropriateness of research methods
- Quality and thoroughness of data analysis and interpretation
- Use of appropriate and relevant literature and sources
- Logical and coherent argumentation
- Writing quality, including grammar, style, and organization
- Implications and potential impact of the research
- Future directions for research or practical applications

Roadmap

- 4. June 2023: Official Announcement at the Crypto Valley Conference 2023. Rotkreuz and Kick Off Call for Papers 2023 WATCH HERE
- 25. August 2023: Abstract Deadline
- September 2023: Announcement selected Authors
- 25. October 2023: Final Paper Deadline
- 27. November 2023: Research Journal 2023 Publication
- January & February 2024: WG Education CFP2023 Conference

2023 RESEARCH PAPERS

7.1. DeFi in the Global South: A beacon of inclusive development or a geopolitical hazard?

AUTHOR:

Dimitris Symeonidis

DeFi in the Global South: A beacon of inclusive development or a geopolitical hazard?

- A how to guide for the majority world to thrive under a DeFi dominated society

Abstract

This century has been touted by many as the “century of Africa”. As demographic growth and industrialization of countries in the Global South increase, economic growth rates are following and creating numerous opportunities for the local population. However, a key impediment in making this growth inclusive within all local communities is access to finance. In Africa, access to financial services is available to less than half of the population, whereas in the Pacific Island states, similarly, more than half of the people cannot find banking services or anything related to fueling their dreams through funding resources. At the same time, even for the small part of the population that manages to access these services, they have to face instability, as several of these countries’ banking systems has currencies that are non-reliable and highly prone to inflation.

Decentralized Finance has a major role to play in these countries. It can function as a unique financial paradigm for the Global South, leveraging distributed ledger technologies to offer services such as lending, investing or exchanging crypto assets in a decentralized manner, without the need for increase of banking infrastructure.

However, development and deployment of cryptocurrencies and decentralized finance comes with inherent challenges in some of these countries, such as cybersecurity, lack of accountability, risk of centralization, interoperability and governmental, regulatory risks. All of the aforementioned get heightened in a period where many of the Global South countries face major geopolitical challenges which can bring further instability within their premises, hence, even though a decentralized finance network with cryptocurrencies would help them grow immensely, there should be a strategy to mitigate these risks.

This paper will analyze the geopolitics-related risks of the introduction of decentralized finance in countries of geopolitical interest. Case studies of countries who already announced their introduction in the market will be used. The two cases will be Central African Republic and the Republic of the Marshall Islands, both of which are of uttermost geopolitical importance for different reasons. The aforementioned risks will be put in their context and painstakingly

analyzed on how they could even bring regional instability. Based on this analysis, a set of policy recommendations will be provided, so that the risks of governance and centralization are avoided and decentralized currencies are deployed responsibly, bringing economic prosperity and sustainability in these countries.

The century of the Global South

The notion of the “century of Africa” when discussing about the 21st century has been perpetuated among politicians, C-suite officers within the business sector and economists. The reason behind this is that these 100 years are considered to be the ones the continent will see peace, economic prosperity and cultural revival (Mbembe 2016). While two out of the three elements can be contested, economic prosperity can be justified by certain indicators African economies are enjoying. Only during the past year, the whole continent experienced a 3.7% GDP growth rate, while, out of the 54 countries, only 4 have faced recession, with the other 50 eyeing development with a GDP growth of up to 5.7% (Sadigov, 2022). The situation is similar in Latin America, the Caribbean and the APAC region. Hovering between the COVID-19 pandemic and the energy crisis following the Russian invasion of Ukraine, these figures are nothing short of impressive. This is only expected to change for the better, with business-to-business spending expected to rise by more than $200 billion by 2030, reaching $700 billion (Matenkeya & Moyo, 2022) .

However, this is not something that is reflected on all local communities as well. The key characteristics, whose absence is clear in the economic growth of Africa are inclusivity and efficiency. Access to electricity still lies at an alarming 43%, whilst access to clean water also is around 40%. Finally, virtually all countries have a low-quality road network, being at the second half of the world rankings. This results in a colossal infrastructure gap that can only be remedied by expenditure of more than $170 billion per year for the next 20 years, something that is impossible for many countries in the Global South, contemplating their excessively high public debt (Mamadou Asngar, 2022).

One effective way to overcome these obstacles is decentralization. Building decentralized production units in the energy and agriculture sectors and financing it can create autonomous communities, which gives them the power to thrive by increasing their revenue and leveraging their own strengths to generate jobs and incomes for their own citizens (Akramov, 2009). This, nonetheless, requires good financing services and a stable economy, so that the right financing scheme for each community can be found. Nevertheless, this too is a problematic situation that countries in the Global South are facing, as almost 70% of all Africans are lacking access to finance, whereas this figure is similar to other regions in the Global South, such as Central Asia, the Pacific and the Caribbean Islands. A way to overcome this and bring inclusive prosperity into all communities of the Global South is decentralized finance (DeFi). DeFi is a new financial paradigm that leverages distributed ledger technologies to offer services such as lending,

investing, or exchanging cryptoassets without relying on a traditional centralized intermediary (Chen & Bellavitis, 2019). Cryptoassets include cryptographically secured digital representations of value or contractual rights that uses a form of distributed ledger technology and can be transferred, stored, or traded electronically. Examples of such entail cryptocurrencies, such as Bitcoin and Ethereum, but also non-fungible tokens (NFT) that can receive or alter their financial value (Baker et al, 2023).

DeFi, as mentioned, can be a means of inclusive development and provide local communities with the opportunity to fulfill and fuel their dreams, whether it's about personal career goals or community development projects. At the same time, decentralizing financial infrastructure comes with inherent challenges (He et al, 2022), which encompass:

- The choice of cryptocurrencies, given the volatile nature of many of them, as well as the purpose of each one, mandated by the white paper and the entities who support it
- The energy intensity of a large number of cryptoassets
- The geopolitical nature of DeFi, as different state actors within the political decision-making arena have widely different approaches over the subject

Research Gap

There are several research gaps that have been indicated. So far, decentralization has been touted by scholars as a means to overcome infrastructure obstacles for development in the Global South. Decentralized electricity production and autonomous communities have been elaborated as a means to scale development and eliminate poverty in the less deprived communities (Alstone et al, 2015). At the same time, DeFi has been researched as a means to resolve issues in the energy and agriculture sector and modernize them (Popescu, 2022). However, there have been virtually no studies looking into how DeFi can resolve development problems and challenges that the Global South is facing. DeFi has been mentioned only as part of a series of alternative finance models, in a very brief manner, only with the ultimate objective of understanding the increase in global interest of these alternative finance methods. Taking these into consideration, as well as the necessity for decentralization in the Global South, it is of uttermost importance to comprehend what the main impediments of safe, inclusive, sustainable and profitable deployment of DeFi in these countries are and to be able to avoid them.

Taking the aforementioned into consideration, the research question can be shaped as follows:

" How can the Global South use DeFi in a manner that maximizes inclusive development, while navigating away from the geopolitical, societal and environmental challenges that lie ahead?"

Methodology

Different methods were chosen during data collection and data analysis for this research. Regarding data collection, both qualitative and quantitative data was taken into account and utilized in the analysis. For the policy, politics, legal and regulatory landscape of countries in the Global South, data will be collected from databases and reports from secondary sources, such as governmental websites, websites of the respective regional blocs and international institutions. These types of information revolve around the state of affairs of the financing system, as well as the institutional frameworks and what the approach of each state/group of states is with regards to decentralization. Regarding other types of qualitative data, similar sources will be used, but complementary to those, data collection from secondary sources that will be the results of a comprehensive literature review of scientific journals will also take place. These will be used to understand the historic trajectory of each case's approach to decentralization and decentralized finance and comprehend what are the drivers or obstacles of deploying such technologies and financing systems into local communities, in order to be able to better understand what are the key risks that we should be expecting and trying to avoid.

The choice of case studies was performed on the basis of specific characteristics of each country. These characteristics included:

- The already existing framework, which has not only allowed the deployment of cryptocurrencies in the country.
- The deployment of CDBC or other decentralized national currencies
- Projects already undertaken in the country, directly related with cryptocurrencies mining of utilization of local stakeholders.
- The existence of geopolitical risks

Based on these criteria, the two case studies that were chosen were the Republic of the Marshall Islands and the Central African Republic. Regarding the former, it was the first country that introduced a national digital currency based on a blockchain system, whilst the region has recently gained geopolitical interest. The reason for that is that China has been exercising its grip over the Pacific Island states and attempting to seal military agreements, with a successful agreement already being in place in the Solomon Islands and Kiribati being already leaning towards accepting the Chinese offer. At the same time, cyber attacks tracing to Chinese sources have already unfolded, with Guam being the first victim of such an attempt.
Regarding the latter, CAR has been the first country in Africa that made ledgers such as Bitcoin and Ethereum fully legal within the country. Despite the fact that this legislation was repealed later in 2023, the nation is considered to be the one who has set the pace for DeFi introduction in Sub-Saharan Africa. At the same time, it has been one of the first countries in Africa which

initiated a partnership with the Russian PMC Wagner Group and has actively participated in the geopolitical chessboard that Russia is pursuing within the continent.

Data analysis will be mostly qualitative, as thematic and narrative analysis will be the key elements, where information/data collected through the first phase will then be used to find emerging patterns and convert them to themes that will be able to explain the future trajectory of the seaweed industry in Southeast Asia. From the collection of qualitative and quantitative data, themes will revolve around:

1) The existing or emerging geopolitical risks related to DeFi systems
2) The expected benefits of DeFi for local communities
3) The energy efficiency issues of cryptocurrency mining and the ways to overcome this
4) The geostrategic location of the aforementioned countries

Adding all this information and data into different themes and converting them in a narrative regarding the main challenges and opportunities related with DeFi infrastructure deployment in the Global South, very important insights will unfold and converted into meaningful policy recommendations.

Having a clear understanding of the methodology that will be followed, the next step will be to comprehend what is the societal and economic value that DeFi can bring in the global south, but also the geopolitical, societal and environmental challenges that lie ahead if it is not properly introduced into the local communities.

Geopolitical Risks

Cybersecurity

In general, DeFi is accompanied with inherent cybersecurity threats and risks, which increase the vulnerability and can create serious threats for the local economy. These are related to:

- Smart Contract Vulnerabilities: These include flawed code implementations within the algorithm of each cryptocurrency. These can easily be exploited by hackers, the most common of which was the DAO hack in 2016, which resulted in $60 million being lost. Another issue that can occur with that regard are unaudited contracts that do not have a third-party audit, which can cause similar issues. This took place in 2022, when the Ronin Network leak resulted in the loss of over $600 million in Ethereum and USDC (He et al, 2020).
- Interoperability vulnerabilities: The element of interoperability can often be a double-edged sword, as it can be leveraged by hackers for exploitative protocol interactions, with the example of Cream Finance protocol resulting in the loss of $120 million being the most prevalent one (Khan et al, 2021).

- Centralized Points of Failure: Even in DeFi, elements such as oracles and admin keys remain managed by centralized entities and, hence, a cyberattack on them can cause the whole decentralized system to paralyze, such as the Oracle manipulation in the QuickSwap exchange and the BadgerDAO hack (Ushida & Angel, 2021).
- Front-running: These include bot attacks that can result in the system going down and give attackers the opportunity to manipulate the existing crypto tokens (Yin et al, 2020).

All of these issues are highly pertinent in both case studies. In the Central African Republic, as well as other countries in the region, Russia's military presence has been heightened over the past 5 years. This does not only translate to troops on the ground, but also to digital presence that creates not only disinformation campaigns, but has also resulted in cyber attacks in the past (Lam, 2018). Both tactics, taking into account the vulnerabilities mentioned, can cause serious harm on the DeFi networks. They can easily cause distortion on oracles and admin keys, create bot attacks with the same mechanisms that they use for disinformation and exploit smart contract and interoperability vulnerabilities. Wagner Group and other Russian PMC's have been accused on performing cyber attacks and hacks on satellite telecommunication networks and digital infrastructures throughout the continent, and hence this is considered to be a substantially high risk for African countries in the Global South and similar cases that fit the aforementioned profile (Buchanan & Sulmeyer, 2016).

There are some differences in the case of the Marshall Islands, albeit the similarities that exist. The Pacific Island complex has not yet experienced cyber attacks, however in the broader region, and more precisely in the island of Guam, there has been a security breach reported which was traced back to Chinese sources (Newsham, 2023). Nevertheless, this was a unique occasion and not the modus operandi of malevolent actors in this segment of the Global South. In most cases across the Pacific, concerns over naval attacks or military presence are much higher than cyber ones and this cyber attack is considered as an outlier (Johnson, 2017). Taking this into consideration, the risk in countries that fit this profile is deemed as rather medium-sized.

Energy Intensity and Access to Electricity

Another major impediment that prevents successful and efficient deployment of DeFi in the Global South is related with energy consumption. Bitcoin, the most common and well-known distributed ledger, is estimated to consume more than 127 TWh a year, putting it above many countries, such as New Zealand and Norway (Kufeoglu & Ozkuran, 2019). In the USA alone, it is consuming more than 50 TWh per year, converting it into an obstacle for the energy transition and even causing distress among local communities who might experience power outages (Niaz et al, 2022) .

For cases like the Central African Republic, where less than 15% of the population has access to electricity, consuming such high amounts solely for crypto mining which might not generate immediate benefits to local communities, this has a high chance of being perceived as

provocative towards the less privileged part of the country. As a result, this might generate social unrest, which, in many countries who fit the profile, such as Mali, Burkina Faso and Sudan, this has resulted in military operations and an overthrowing of the democratically elected government (Dunne & Tian, 2014). Spillover effects are always a possibility in such cases. Taking into account that these regions are already ravaged by instability and have faced border disputes in the past, the likelihood of an escalation of conflicts is not negligible and the effects of it on the local population are immense. As a result, there is an extensively high risk that needs to be taken into account and an attempt to remedy this is paramount.

For cases like the Marshall Islands, the situation is rather the opposite. Countries within the Global South that fit this profile have almost 100% access to electricity. At the same time, island states face waste management issues, which presents itself as readily available biomass that can be converted to energy, which can be used for crypto mining activities (Gundaboina et al, 2022). This shows that an environmental hazard can be converted into a profitable and socially beneficial project. More importantly, however, this depicts that the risk in all similar cases is rather low.

Environmental Conflict Creation

An issue directly correlated with the energy intensive nature of DeFi is the environmental devastation it can cost, and the conflict that this devastation can bring, if not dealt with correctly. Solely in the USA, DeFi activities account for 25-50 million tons of CO_2. The tally is expected to be much higher in countries, where coal, oil and gas account for higher percentage of their energy mix (Stoll et al, 2023).

CAR is a special case with regards to its energy mix and climate profile. The country's little energy production mainly comprises of wood as a heating and energy source, followed by oil and hydro. This creates a highly emitted profile by itself. However, its solar and wind potential is immense and, hence, DeFi activities, without any energy policy reforms, currently can have a devastating effect on CO_2 emissions and a major environmental impact. Its affect on local climate is also expected to be substantial, causing instability in the raining seasons, which can result in food insecurity and further exacerbate social unrest (Soule-Baoro et al, 2018). The risk in this case is far from negligible, and can be considered as moderate.

The case in the Marshall Islands is considered to be even worse. The country currently depends on diesel generators and imports and, hence, increasing need for electricity will result in a surge in CO_2 emissions, but also in an energy imports crisis, if the energy mix is not enriched with renewables. The effects of climate change are also expected to be even more dire than the ones in countries with the profile of CAR. The reason is that the main effect in small island states is sea level rise, which can cause the extinction of these countries (Weir et al, 2017). Hitherto, this is a considerably higher effect and the risk can be deemed as excessively high.

Choice of currency and volatility of the market

Apart from the efficiency component, another issue that should be taken into consideration is the price volatility of cryptocurrencies. It has been studied that, while during bear markets the fluctuations among crypto assets is low, the same thing does not happen in bull markets, where there are considerably large fluctuations. This might have strong implications for the local communities, depending on the currencies that they choose to use for their everyday activities (Hu et al, 2019). Shock-absorbing capacity of these fluctuations is currently considered as low, thus any country that wishes to deploy DeFi solutions for its local communities should have a comprehensive strategy to deal with these volatility trends (Kyriazis, 2021).
In countries such as CAR, the strategy of a national digital ledger is unlikely to rip many benefits and is more likely to pose a risk. The reason is that the CFA is highly vulnerable to high fluctuations, and countries like Zimbabwe, who share that trend, should also steer away from such a strategy (Omojimite & Akpokoje, 2010). In case this is chosen, the risk is expected to be very high and the foregoing state actors would benefit from the choice of globally available cryptocurrencies after an appropriate risk management strategy takes place. In case this does not happen, a market crash is moderately likely, with its likelihood depending on the adoption of this type of crypto asset by the local populus.
Actors such as the Marshall Islands, on the other hand, would enjoy very low risk by the adoption of a national ledger. The USDC is already an existing digital currency and it can also be adopted by the island state, by pegging it to the national cryptocurrency. However, there is also the risk that pegging a currency that does not fully reflect the economy of the island state would actually backfire and restrain investors from supporting this initiative, which might result in a run-risk and do more harm than good to the local communities (White, 2017).

Societal Acceptance

Finally, local communities ought to be taken into consideration. Blockchain and cryptocurrencies have actually been introduced to citizens globally and they have been used to a small extent, but mass adoption is far from being achieved. This is even more the case in the Global South, where there is even more lack of trust and fear of such tools being used by criminal associations in order to exploit them and against national interests. This sentiment is keeping them away both from becoming more knowledgeable over the subject and to learn how to use cryptocurrencies responsibly (Voskobojnikov et al, 2021).

In the case of CAR, the recalling procedure of the legislation on digital currencies shows exactly this lack of social awareness. Ever since, the national government has introduced measures to help raise awareness and make citizens feel more comfortable with the use of digital technologies. However, this by itself shows that countries that fit the profile, most of which lie in Sub-Saharan Africa, have a high risk of the deployment of DeFi not being efficient, and instead being met with distrust, which can again spur internal conflict (Adeola, 2022).

The case of the Marshall Islands is different, as digital literacy is at much higher levels and already citizens have been using the national distributed ledger. The risk in this case is deemed as lower and these countries have a higher chance of being more competitive geopolitically when deploying DeFi and relevant infrastructure within the local communities (Wetere, 2019).

The following analysis is being displayed in brief in Tables 1, 2 and 3 as a form of a risk assessment:

Table 1: Risk assessment for the two case studies concerning the adoption of DeFi

	CAR	**RMI**
Cybersecurity		
Energy Intensity		
Environmental Conflict		
Price Volatility		
Societal Acceptance		

Table 2: Risk analysis for the different types of DeFi risks for countries closer to the CAR case

	Likelihood	**Impact**
Cybersecurity	Low	High
Energy Intensity	High	High
Environmental Conflict	Moderate	High
Price Volatility	Moderate	Moderate
Societal Acceptance	High	High

Table 3: Risk analysis for the different types of DeFi risks for countries closer to the RMI case

	Likelihood	**Impact**
Cybersecurity	High	High
Energy Intensity	High	Low
Environmental Conflict	High	High

Price Volatility	Moderate	Low
Societal Acceptance	Low	High

Policy Recommendations

Based on the aforementioned analysis, DeFi has a grand opportunity of reshaping the local communities across Sub-Saharan Africa, Latin America and Asia-Pacific. However, in order to achieve this, several obstacles need to be overcome and, in order to achieve that, sophisticated policy levers ought to be utilized. These, again, can be divided based on their presence in the financial, societal or technological realm.

Technological reforms

A new regulatory framework should be developed by policymakers and regulators. This should not encourage centralization of cryptocurrencies, however it ought to provide incentives and support for good technological practices. These should include measures in the following sectors:

DeFi security

1. Rigorous Code Audits

Third-party audits: Currencies and ledgers that support third-party audits should be the only ones allowed for citizens to engage.

2. Bug Bounty Programs

Community-driven checks: Involving the crypto community can be invaluable. By offering incentives or rewards, projects can encourage enthusiasts, developers, and white-hat hackers to identify and report vulnerabilities, ensuring a more resilient system.

3. Insurance for DeFi Products

Coverage against failures: An insurance-like coverage program should be developed by state actors to protect citizens against such DeFi failures

4. Layer-2 Scaling Solutions

With congested networks come a plethora of issues:

Reduced congestion: Implementing layer-2 or off-chain solutions can alleviate network congestion, leading to faster transaction times and reduced gas fees.

Enhanced reliability: With transactions processed off-chain, the likelihood of failed transactions due to congestion diminishes, ensuring a smoother user experience.
5. Decentralized Governance
The essence of DeFi lies in decentralization, and governance should be no different:

Community-driven decisions: DeFi platforms can harness decentralized governance models instead of a centralized entity making decisions. This involves the community in decision-making processes, from protocol upgrades to security measures.
Mitigating centralized risks: A decentralized governance model minimizes risks associated with central points of failure. If a single point gets compromised, the collective decision-making process remains unaffected.

Choice of cryptocurrency

Similarly to the previous measures, sophisticated frameworks should focus on the adoption of cryptocurrencies that comprise of the following characteristics

- Energy-efficiency: Currencies that harness low amounts of energy to provide high-value ledgers should be preferable. A task force among policymakers, given the task to pinpoint and verify the currencies that can be mined or exchanged using energy-efficient means.
- Low volatility: Citizens should be discouraged to use ledgers that have high volatility or their projected trajectory in the DeFi space is unknown.
- Verified standards: ISO 20022 should be used as a bridge between centralized and decentralized finance and similar standards should be developed at a national levels for all countries of the Global South.

Society

Social awareness programs, as well as education among the local communities is critical. Education state actors should focus on creating the following infrastructure that can result in a well-informed, educated and ready to use DeFi society:

- Education courses for web 3 technologies on local communities
- Economic education courses
- Policy advocacy for civil society, so that they can effectively advocate for a policy framework that will comprise of justice, equity and prosperity for all.

Conclusion

In summary, while the road to a fully secure DeFi landscape is fraught with challenges, the combination of rigorous audits, community engagement, insurance, scaling solutions, and decentralized governance offers a promising pathway. As the industry evolves, it’s imperative to prioritize these measures to ensure the safety, reliability, and longevity of the DeFi ecosystem. At the same time, countries in the Global South ought to make a comprehensive risk assessment, not only from the aforementioned hazards, but also from ones that might inhibit the full real societal

and economic value of DeFi. Navigating around these hazards will require a comprehensive and sophisticated policy, regulatory and legal framework and a group of policy experts on web 3.0 to deal with that, and the approach will have to be adaptive, considering that the business and societal environment of these communities largely varies depending on culture, geography and other conditions.

References

Adeola, O., 2022. Leveraging trust to enhance the public sector brand in Africa. *New Public Management in Africa: Contemporary Issues*, pp.47-66.

Alstone, P., Gershenson, D. and Kammen, D.M., 2015. Decentralized energy systems for clean electricity access. *Nature climate change*, *5*(4), pp.305-314.

Akramov, K.T., 2009. *Decentralization, agricultural services and determinants of input use in Nigeria* (Vol. 941). Intl Food Policy Res Inst.

Baker, H.K., Benedetti, H., Nikbakht, E. and Smith, S.S., 2023. Cryptoassets: An Overview. *The Emerald Handbook on Cryptoassets: Investment Opportunities and Challenges*, pp.3-11.

Buchanan, B. and Sulmeyer, M., 2016. Russia and cyber operations: Challenges and opportunities for the next US administration. *Carnegie Endowment for International Peace*, *3*.

Chen, Y. and Bellavitis, C., 2019. Decentralized finance: Blockchain technology and the quest for an open financial system. *Stevens Institute of Technology School of Business Research Paper*.

Dunne, J.P. and Tian, N., 2014. Conflict spillovers and growth in Africa. *Peace Economics, Peace Science and Public Policy*, *20*(4), pp.539-549.

Gundaboina, L., Badotra, S., Bhatia, T.K., Sharma, K., Mehmood, G., Fayaz, M. and Khan, I.U., 2022. Mining cryptocurrency-based security using renewable energy as source. *Security and Communication Networks*, *2022*, pp.1-13.

He, D., Deng, Z., Zhang, Y., Chan, S., Cheng, Y. and Guizani, N., 2020. Smart contract vulnerability analysis and security audit. *IEEE Network*, *34*(5), pp.276-282.

He, M.D., Kokenyne, A., Lavayssière, X., Lukonga, M.I., Schwarz, N., Sugimoto, N. and Verrier, J., 2022. *Capital Flow Management Measures in the Digital Age: Challenges of Crypto Assets* (Vol. 2022, No. 5). International Monetary Fund.

Hu, Y., Rachev, S.T. and Fabozzi, F.J., 2019. Modelling crypto asset price dynamics, optimal crypto portfolio, and crypto option valuation. *arXiv preprint arXiv:1908.05419*.

Johnson, J.S., 2017. China's “Guam Express” and “Carrier Killers”: The anti-ship asymmetric challenge to the US in the Western Pacific. *Comparative Strategy*, *36*(4), pp.319-332.

Khan, S., Amin, M.B., Azar, A.T. and Aslam, S., 2021. Towards interoperable blockchains: A survey on the role of smart contracts in blockchain interoperability. *IEEE Access*, *9*, pp.116672-116691.

Küfeoğlu, S. and Özkuran, M., 2019. Bitcoin mining: A global review of energy and power demand. *Energy Research & Social Science*, *58*, p.101273.

Kyriazis, N.A., 2021. A survey on volatility fluctuations in the decentralized cryptocurrency financial assets. *Journal of Risk and Financial Management*, *14*(7), p.293.

Lam, C., 2018. A slap on the wrist: Combatting Russia's cyber attack on the 2016 US presidential election. *BCL Rev.*, *59*, p.2167.

Mamadou Asngar, T., 2022. Does financial development improve access to electricity in sub-Saharan Africa?. *SN Business & Economics*, *2*(9), p.146.

Matekenya, W. and Moyo, C., 2022. Innovation as a driver of SMME performance in South Africa: a quantile regression approach. *African Journal of Economic and Management Studies*, *13*(3), pp.452-467.

Mbembe, A., 2016. Africa in the new century. *The Massachusetts Review*, *57*(1), pp.91-111.

Newsham, G., 2023. *When China Attacks: A Warning to America*. Simon and Schuster.

Niaz, H., Shams, M.H., Liu, J.J. and You, F., 2022. Mining bitcoins with carbon capture and renewable energy for carbon neutrality across states in the USA. *Energy & Environmental Science*, *15*(9), pp.3551-3570.

Omojimite, B.U. and Akpokodje, G., 2010. A comparative analysis of the effect of exchange rate volatility on exports in the CFA and non-CFA countries of Africa. *Journal of Social Sciences*, *24*(1), pp.23-31.

Popescu, A.D., 2022. Understanding FinTech and Decentralized Finance (DeFi) for Financial Inclusion. In *FinTech Development for Financial Inclusiveness* (pp. 1-13). IGI Global.

Sadigov, R., 2022. Rapid growth of the world population and its socioeconomic results. *The Scientific World Journal*, *2022*.

Soulé Baoro, S.K.G., Song, S. and Fagariba, C.J., 2018. Climate Change Adaptation and Agricultural Development in Central Africa Republic-Evidence of North-West. *J Food Process Technol*, *9*(761), p.2.

Stoll, C., Klaaßen, L., Gallersdörfer, U. and Neumüller, A., 2023. *Climate Impacts of Bitcoin Mining in the US*. MIT CEEPR Working Paper Series, https://ceepr. mit. edu/files/papers/2023-011. pdf.

Ushida, R. and Angel, J., 2021. Regulatory considerations on centralized aspects of DeFi managed by DAOs. In *Financial Cryptography and Data Security. FC 2021 International Workshops: CoDecFin, DeFi, VOTING, and WTSC, Virtual Event, March 5, 2021, Revised Selected Papers 25* (pp. 21-36). Springer Berlin Heidelberg.

Voskobojnikov, A., Abramova, S., Beznosov, K. and Böhme, R., 2021. Non-Adoption of Crypto-Assets: Exploring the Role of Trust, Self-Efficacy, and Risk. In *ECIS*.

Weir, T., Dovey, L. and Orcherton, D., 2017. Social and cultural issues raised by climate change in Pacific Island countries: an overview. *Regional Environmental Change*, *17*, pp.1017-1028.

Wetere, A., 2019. *An employer's perspective of the living wage in Fiji, Tonga and Marshall Islands: a thesis presented in partial fulfilment of the requirements for the degree of Master of Business Studies in Management at Massey University, Albany, New Zealand* (Doctoral dissertation, Massey University).

White, L.H., 2017. Dollar‐Denominated Cryptocurrencies: Flops and Tethered Success.

Yin, J., Cui, X., Liu, C., Liu, Q., Cui, T. and Wang, Z., 2020. CoinBot: A covert botnet in the cryptocurrency network. In *Information and Communications Security: 22nd International Conference, ICICS 2020, Copenhagen, Denmark, August 24–26, 2020, Proceedings 22* (pp. 107-125). Springer International Publishing.

7.2. Cryptocurrency Risk, Trust, and Acceptance in Thailand: A Comparative Study with Switzerland.

AUTHORS:

Kanyanut Suriyan

Tim Weingaertner

HSLU Hochschule Luzern

Cryptocurrency Risk, Trust, and Acceptance in Thailand: A Comparative Study with Switzerland.

Kanyanut Suriyan
Siam Technology College, Bangkok Thailand
kunyanuts@siamtechno.ac.th

Tim Weingaertner
Lucerne University of Applied Sciences and Arts, Switzerland.
tim.weingaertner@hslu.ch

Abstract: The adoption of the "Pao Tang" digital wallet in Thailand, promoted under the "Khon la Krueng" (50-50 Co-Payment) Scheme, illustrates Thailand's receptiveness to digital financial instruments, amassing over 40 million users in just three years during the COVID-19 social distancing era. Nevertheless, acceptance of this platform does not confirm a broad understanding of cryptocurrencies and Web 3.0 technologies in the region. Through a mix of documentary research, online surveys and a targeted interview with the Pao Tang app's founder, this study evaluates the factors behind the Pao Tang platform's success and contrasts it with digital practices in Switzerland. Preliminary outcomes reveal a pronounced knowledge gap in Thailand regarding decentralized technologies. With regulatory frameworks for Web 3.0 and digital currencies still nascent, this research underscores the need for further exploration, serving as a blueprint for shaping strategies, policies, and awareness campaigns in both countries.

Keywords: Digital Wallets, Cryptocurrencies, DLT, Pao Tang, Risk, Regulatory Frameworks.

1. Introduction

1.1 Global Trend of Digital Financial Tools Adoption

The digital economy is continuously evolving, and digital wallet platforms have become pivotal tools for both individuals and businesses worldwide. These platforms not only serve as conduits for managing a myriad of digital assets, from loyalty points to cryptocurrencies, but also facilitate secure transactions. As illustrated in Figure 1, the adoption of such digital financial tools has been on the rise since 2020 and is forecasted to continue its growth trajectory till 2024. The global trend showcases a shift towards "cashless societies", propelled further by innovations in digital wallets, QR code transactions, and enhanced digital payment systems. In the context of this paper, we define a digital wallet as a secure mobile app or online service that allows individuals to store and manage various forms of digital assets and information, such as credit card details, bank account information, loyalty cards, or digital identities. While digital wallets can hold cryptocurrencies, they are not limited to them and can encompass a wide range of financial and identification tools and services.

1.2 "Pao Tang" in the Thai Digital Era

Thailand witnessed a significant digital shift during the COVID-19 pandemic, as Thai citizens rapidly adapted to the "Pao Tang" mobile application. With over 40 million users registered over the span of three years, this platform has become indispensable for daily transactions (Banchongduang, S., 2022). Furthermore, the "Pao Tang" app, developed by Krungthai Bank, supports various digital payment services. Initially conceived to back the government's social welfare and economic stimulus schemes during the pandemic, it's now integral to the country's digital financial landscape, bridging the digital divide, enhancing the financial system, and steering Thailand towards a cashless society (Krungthai Bank's Super App, 'Pao Tang', an All-in-one Platform for Thais, 2022).

Figure 1: *Number of Active Online Banking Users Worldwide in 2020 with forecasts from 2021 to 2024, In million*. (Digital adoption available from Team, D. A. (2022))

1.3 Switzerland: A Comparative Study

Switzerland stands as an epitome of economic stability, with strengths in sectors ranging from banking to pharmaceuticals. The nation's esteemed financial sector, coupled with its emerging role as a pro-blockchain hub also called "Crypto Valley" in the canton of Zug is used frequently as a global benchmark and presents a fascinating contrast to Thailand's rapidly growing economy. While Thailand's economic strategies lean more towards protectionism, Switzerland champions

liberal economic ideologies. Nevertheless, the percentage of Thai cryptocurrency account holders increases doubly from 2019 to 2022 compared with Swiss cryptocurrency account holders (see Figure 2). This research seeks to unravel how these contrasting nations navigate the realms of blockchain, providing insights into the regulation, usage, and risk awareness.

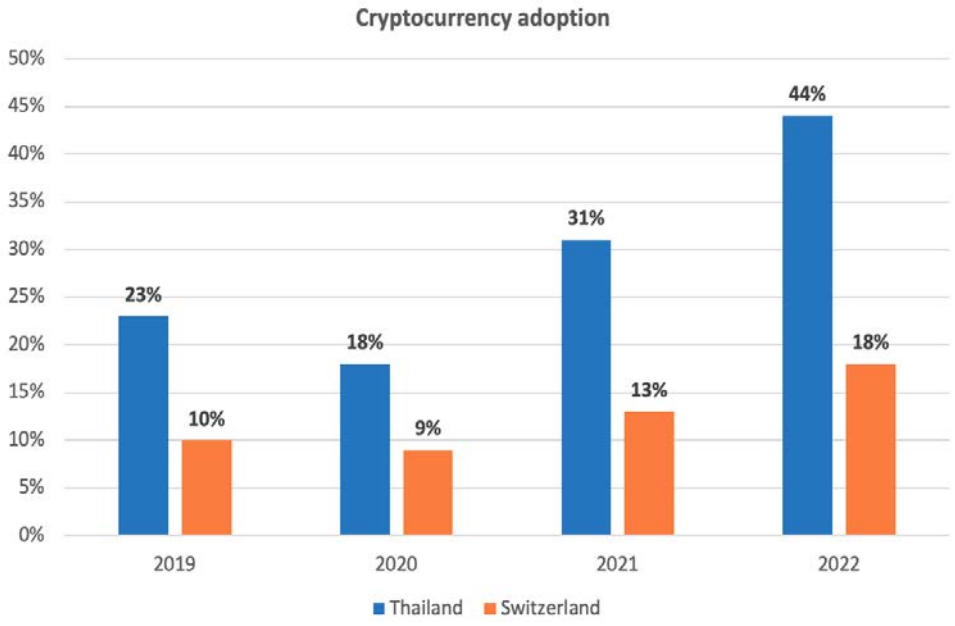


Figure 2 *Cryptocurrency account holders. (Own diagram, data source Crypto ownership by country. (2023))*

To benchmark the trading volumes in cryptocurrencies between Thailand and Switzerland, we performed a comparison of trading volumes analogous to IFZ (2023). Figure 3 and 4 show results of this study.

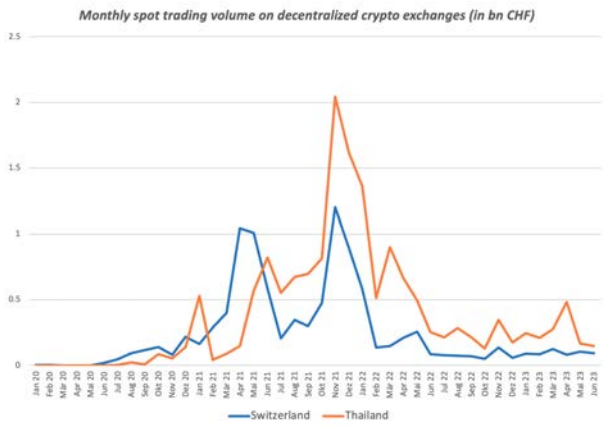


Figure 3 *Monthly spot trading volume on decentralized crypto exchanges (in bn CHF, own diagram)*
Figure 4 *Monthly spot trading volume on decentralized and centralized crypto exchanges including derivatives (in bn CHF, own diagram)*

1.4 Problem Statement

The digital transformation, marked by the surge of digital payments, brings to the fore several challenges and opportunities. While digital wallets, underpinned by decentralized technologies like blockchain and DLT, promise benefits such as increased financial autonomy, they also come with inherent risks. Despite the growing excitement around these wallets, a clear gap exists in users' understanding of the underlying decentralized technologies. This paper delves into this contrasting landscape. Main objectives include:

- Analyzing cryptocurrency acceptance and risk awareness in Thailand compared to Switzerland.
- Unraveling the factors behind the success of the "Pao Tang" app.
- Understanding the potential of integrating Web 3.0 technologies and cryptocurrencies in Thailand.

2. Current Financial Landscape and Recent Work

The financial landscape, driven by technology, reveals intricate details about a nation's economic posture, technological acceptance, and future trajectories. This section delves into understanding these nuances by studying the landscapes of both Thailand and Switzerland. Subsequent discussions offer insights into regulatory structures, comparative economic and cultural analysis, and reflections from prior academic work.

2.1 Digital Financial Landscape in Thailand

Traditional vs. Digital Payments in Thailand: In Thailand, traditional payment methods have been the norm for many years. However, technological advancements have caused a paradigm shift towards digital payment mechanisms, such as the QR-code payments and digital wallets. Such innovations are enhancing financial services and narrowing financial divides for both businesses and households (Financial Landscape for Digital and Sustainable Economy, n.d.).

Challenges in the Digital Era: Technological adoption is not without challenges. If businesses and households fail to adapt, there's potential for widening economic disparities, including issues like rising household debts. Thus, the Thai financial sector's challenge is to harmonize innovation with risk management (Moenjak et al., 2020).

The Role of the Pao Tang App: "Khon la Krueng" (Let's Go Halves/50-50 Co-Payment) scheme was one of the government's economic stimulus measures that help people, small business owners, hawkers, street vendors, and other businesses. Krungthai Bank has developed a registration website for people and shop owners. Eligible participants paid only 50% of the goods price and the government would transfer the other 50% of the price to merchants. Since payment and transfer of money must be made via the Pao Tang application, a product of Krungthai Bank, this app played a pivotal role in the scheme's success. "In the first phase of the Khon La Khrueng scheme, there were more than 15 million people registered and more than 1 million merchants participating, which generated more than 45,000-million-Baht circulating funds" (Krung Thai, 2022).

2.2 Regulatory Framework in Thailand

Thailand's approach to the rapidly emerging digital assets and cryptocurrencies has been proactive and comprehensive. The foundation for this approach is the regulatory directives established to govern the use, issuance, and trading of these assets.

The Royal Decree on Digital Asset Businesses B.E. 2561 (2018) decree forms the bedrock of Thailand's cryptocurrency regulation. It came into effect to provide clarity and to set clear parameters for both individuals and businesses engaged in digital asset transactions. Some key provisions include:

1. *Classification of Digital Assets:* The decree specifically categorizes digital assets into two primary types: Cryptocurrencies, serving as a medium of exchange, and Digital Tokens, which represent rights of a person in an investment or to acquire goods and services. This distinction aids in providing specific regulations for each type (Legal Counsel and Development Department, The Office of the Securities and Exchange Commission, 2018).
2. *Registration Requirements*: Entities wishing to engage in digital asset businesses are required to register with the Securities and Exchange Commission (SEC) within 90 days. This is vital for monitoring and supervisory purposes.
3. *Protection Measures*: To safeguard consumers and maintain market integrity, the Bank of Thailand has prohibited commercial banks from direct participation in cryptocurrency transactions. However, they have given green lights to certain companies as exchanges and dealers after a rigorous vetting process.

4. *Central Bank Digital Currency (CBDC):* The project "Inthanon" was introduced, representing the Bank of Thailand's interest in creating a CBDC to further streamline and secure financial transactions.(Legal Counsel and Development Department The Office of the Securities and Exchange Commission, 2018)
5. *Obligations for Digital Token Issuers:* Entities intending to publicly offer Digital Tokens must be either a limited company or public limited company established under Thai law. Before any public offering, they must obtain approval from the SEC. Furthermore, these entities have ongoing disclosure requirements, including updating the SEC about their financial status, business operations, and other pertinent information (Legal Counsel and Development Department, The Office of the Securities and Exchange Commission, 2018).
6. *Role of the SEC:* The SEC has been empowered not just to oversee but also to grant exemptions. This ability ensures flexibility in adapting to evolving market dynamics without stifling innovation.

	Digital asset exchange	**Digital assets broker**	**Digital assets Dealer**
Status	Center or a network	Person	Person
Purpose	Purchasing, selling, or exchanging of digital assets	Being a broker or an agent for any person in the purchase, sale, or exchange of digital assets to other person	Purchasing, selling, or exchanging digital assets for his/her own account
Process/Operation	Matching or arranging the counterparty or providing the system	In consideration of a commission, fee, or other remuneration	Outside the digital -asset exchange

Table 1. Digital asset business in Thailand (Source: Security Exchange Commission of Thailand (Tamphakdiphanit & Laokulrach 2020)

While Thailand's regulatory stance is clear and well-structured, it reflects an understanding of the complex nature of digital assets. This progressive regulatory environment not only fosters innovation but also ensures that risks are managed, striking a balance that many nations strive to achieve.

2.3 Payment Systems and Regulatory Aspects in Switzerland

Switzerland, with its robust banking infrastructure, continues to embrace both traditional (like cash) and modern payment methods. During the COVID-19 pandemic, the number of cash

payments has been reduced (Digitalisation trends in the Swiss payment landscape. (n.d.)). Mobile payment solutions like Apple Pay, Samsung Pay, and Google Pay have gained popularity in Switzerland. In addition, the Swiss e-payment solution TWINT, a mobile payment solution developed by Swiss banks, has gained massive traction in the last few years. TWINT allows users to make payments, transfer money, and even make online purchases. Due to the ease of using it with QR codes, many small businesses use this payment method. Moreover, Switzerland's proactive approach towards cryptocurrency, highlighted by its "Crypto Valley", underscores its commitment to innovation in the blockchain sector. Bitcoin and other cryptocurrencies can be used for payments in various establishments, and there are also Bitcoin ATMs available.

Switzerland has been adept in evolving its regulations to match the pace of technological advancements. In relation to blockchain, Switzerland has implemented a "technology-neutral" approach, ensuring that regulations are flexible enough to accommodate advancements without stifling innovation. In contrast to other countries, Switzerland refrained from creating its own blockchain law and instead adapted several existing laws (State Secretariat for International Finance SIF. (n.d.)).

The Swiss Financial Market Supervisory Authority (FINMA) has provided guidelines on Initial Coin Offerings (ICOs) (Finma (2018)). They have been used as a blueprint for many other countries and describe a distinction into three token classes: payment token, utility token, and security token. On 2 November 2022, FINMA introduced its revised anti-money laundering ordinance (AMLO-FINMA) with new provisions targeting virtual currency transactions. The Swiss National Bank (SNB) has set criteria for DLT trading facilities to access the Swiss Interbank Clearing (SIC) payment system, but they must first obtain a FINMA license (Schärli et al. 2023).

2.5 Economic and Cultural Landscape: Thailand vs. Switzerland

Comparing the economic and cultural landscapes of Thailand and Switzerland provides a deep insight into the underlying factors that influence their respective approaches to digital currencies.

2.5.1 Economic Overview

Thailand's economy is a fascinating blend of its agrarian roots and modern sectors like tourism, manufacturing, and digital services. The nation's GDP is heavily reliant on exports, including electronics, automotive goods, and agricultural products. On the other hand, Thailand adopts a

more protectionist approach in its economic policies, often emphasizing state control in vital sectors.

Switzerland stands tall as an economic powerhouse, bolstered by its industrial and service sectors. With industries ranging from banking, pharmaceuticals, and premium manufacturing (like watches), the nation's GDP per capita ranks among the highest globally. Switzerland's liberal economic ideologies further promote substantial economic liberty, providing a fertile ground for innovations, including those in the digital currency realm.

While Thailand's average monthly salary remains at about 19'410.77 Baht (482.34 CHF), Swiss residents enjoy an almost 12-fold higher income at approximately 224'386.09 Baht (5,572.84 CHF) (Rankings by Country of Average Monthly Net Salary, n.d.).

2.5.2 Cultural Dynamics

The heartbeat of *Thailand* is its rich Buddhist heritage. Strong communal ties underscore its collectivist ethos. Traditional arts and crafts remain an integral part of daily life, reflecting the nation's profound cultural roots.

Switzerland presents a melting pot of diverse cultures, thanks to its linguistic diversity, including German, French, Italian, and Romansh. The Swiss value individualism, punctuality, and precision, which manifests in their work ethics and societal norms. Structured education and a strong leaning towards classical music and art form the foundation of Switzerland's cultural dynamics.

The economic compasses of Thailand and Switzerland point in distinct directions. While Thailand finds strength in sectors like agriculture and tourism, Switzerland emerges as a beacon in the financial realm. Such differences extend to their respective regulatory postures towards cryptocurrencies, with Switzerland possibly having a more encompassing risk assessment strategy.

2.6 Previous Studies on Digital Payments

The process of adopting and comprehending digital financial tools is steered by multiple factors. A detailed examination of prior studies furnishes a holistic view of these influential elements, especially emphasizing trust, perceived risks, and user acceptance.

Trust emerges as a pivotal determinant in the adoption of digital financial tools. Decaro & Saleh (2003) emphasized the essence of trust over technological advancements in online banking

adoption. Echoing these sentiments, Patil et al. (2018) delved into the role of trust in mobile payments. They underlined its influential role in shaping both the behavioral intentions and the satisfaction levels of users. Furthermore, Bashir & Madhavaiah (2015) augmented the technology acceptance model by integrating trust, revealing that it significantly propels positive behavioral intentions in internet banking.

On the other hand, the perception of risk, especially in the digital sphere, profoundly impacts user acceptance. Liu et al. (2008) embarked on an exploration of internet banking user acceptance in contexts fraught with risk and uncertainty. Their conclusions emphasized the profound influence of perceived risk and uncertainty on acceptance levels. Supporting this notion, Decaro & Saleh (2003) contended that perceived risks and trust are inextricably linked when it comes to the adoption trajectory of online banking.

Delving into user acceptance, insights into the mechanisms and reasons behind the acceptance of new digital financial tools offer a comprehensive understanding of the broader dynamics at play in the digital economy. Pertaining to the context of Thailand, several scholars have imparted valuable insights. Lamsam et al. (2018) spotlighted the coexistence of traditional cash systems and electronic payments in Thailand, suggesting ways to optimize cash management efficiency. Achyar et al. (2022) identified international tourism receipts as a potent catalyst accelerating digital payment utilization in the country. Moreover, Khiaonarong (2000) provided a thorough examination of the evolution of electronic payment systems in Thailand, attributing a pivotal role to the central bank in the management and investment of these systems. Lastly, Gohwong (2017) categorized various digital payment forms in Thailand, singling out e-Money as the most prominent, closely followed by in-house funds transfer and payment cards.

3. Research Questions and Methodology

The main objectives of our research as described in section 1.4 first is to delve deep into the cryptocurrency acceptance and risk consciousness in Thailand compared to Switzerland, and second, to identify the factors that have made the Pao Tang wallet so popular, while also exploring the challenges and prospects of adopting cryptocurrencies and Web 3.0 technologies in Thai digital payments. This leads to the following research questions and their sub-questions:

RQ 1: How is the acceptance and risk awareness of cryptocurrencies in Thailand compared to that of Switzerland?

RQ 1.1: How is the acceptance of cryptocurrencies perceived among individuals and institutions in Thailand?

RQ 1.2: What is the level of risk awareness associated with cryptocurrencies among Thai stakeholders?

RQ 1.3: How is the acceptance and risk awareness of cryptocurrencies perceived in Switzerland?

RQ 2: What are the key success factors behind the Pao Tang App, and what challenges and opportunities arise from integrating cryptocurrency and Web 3.0 technologies in Thailand?

RQ 2.1: What are the key success factors behind the Pao Tang App in Thailand?

RQ 2.2: What opportunities exist for integrating cryptocurrency and Web 3.0 technologies within the Pao Tang App or similar platforms in Thailand?

To ensure comprehensive and sound research, different research methods were used. In the following, these are assigned to the research questions.

RQ 1.1 was addressed by a survey among Thai individuals, inquiring about their knowledge, attitudes, and acceptance of cryptocurrencies. The above survey was also used for RQ 1.2, focusing on questions that assessed the depth of their risk understanding related to cryptocurrency investments and transactions. RQ 1.3 was addressed by a comparative analysis of the same survey conducted in Switzerland. The results led to an answer of the overall RQ 1.

For RQ 2 a qualitative approach has been chosen. For RQ 2.1 and RQ 2.2 an interview with the Pao Tang app's founder Somkid Jiranuntarat, an adviser to the president of Krungthai Bank, which oversees the Pao Tang app and offered insights into the success factors, strategies, and user satisfaction metrics.

4. Results

This section presents a comprehensive analysis, shedding light on factors contributing to the success of the Pao Tang platform and offering a comparative exploration of user knowledge and trust in cryptocurrency and Web 3.0 technologies between Thailand and Switzerland.

4.1 Survey of User Knowledge and Trust in Cryptocurrencies in Thailand

In our endeavor to comprehend the underlying factors influencing the adoption and perception of cryptocurrencies and Web 3.0 technologies, a comprehensive survey was administered to

respondents in Thailand (n=465). This survey aimed to gather quantifiable data on various demographics, unraveling correlations between age, gender, educational background, and their subsequent influence on cryptocurrency understanding, trust, and usage. By decoding these patterns these findings and inferences derived from this survey data:

- *Age:* In summary, older respondents in this dataset tend to find it more challenging to understand and use cryptocurrencies, feel they lack enough financial knowledge to understand them and are less aware that they can exchange cryptocurrencies with traditional currencies (Understand and use cryptocurrencies: 20-30 years: 43.43% don't use, 56.57% use; 31-40 years: 65.93% don't use, 34.07% use; 41-50 years: 62.79% don't use, 37.21% use; more than 50 years: 64.71% don't use, 35.29% use). Also older respondents tend to be less confident about the security aspects of cryptocurrency (20-30 years: 46.80% not confident, 53.20% confident; 31-40 years: 78.02% not confident, 21.98% confident; 41-50 years: 65.12% not confident, 34.88% confident; more than 50 years: 70.59% not confident, 29.41% confident)
- *Gender:* Male respondents are more likely to be aware of the advantages and disadvantages of cryptocurrencies (female: 41.83% aware, 58.17% unaware; male: 56% aware, 44% unaware). They are also more likely to follow news about cryptocurrencies regularly (female: 27.12% follow, 72.88% don't follow; male: 34.67% follow, 65.33% don't follow).
- There is no correlation between the level of education and usage of cryptocurrency.
- There is a statistically significant correlation between age and the influence of others suggesting that younger respondents are more likely to be influenced by others to use cryptocurrencies (20-30 years: 59.26% not influenced, 40.74% influenced; 31-40 years: 81.32% not influenced, 18.68% influenced; 41-50 years: 76.74% not influenced, 23.26% influenced; more than 50 years: 73.53% not influenced, 26.47% influenced).
- Among the people who view cryptocurrencies as high-risk (348), 162 people intend to or currently use cryptocurrencies for payments and 198 people intend to or currently use cryptocurrencies for speculation or financial gain. From this analysis, we can infer that even if they perceive cryptocurrencies as high-risk, a significant number of respondents still use or intend to use them.
- Among the respondents who find it convenient to use cryptocurrency anytime and anywhere (265), only 159 of them intend to or currently use cryptocurrencies for payments.

- There is a positive correlation between the belief that using cryptocurrencies can enhance one's financial goals and living standards, and the use of cryptocurrencies for speculation (0.418). This positive value indicates that respondents who believe that cryptocurrencies can improve their financial situation and standard of living are more likely to use cryptocurrencies for speculation.
- There is a higher correlation between those who are more aware of the advantages and disadvantages of cryptocurrencies and the usage for speculation (68.81%). This implies that awareness plays a more significant role in influencing the use of cryptocurrencies for speculation than for payments.

4.2 Comparative Survey in Switzerland

To draw a comparative insight, an analogous survey was conducted among respondents in Switzerland (n=79). Deploying a parallel set of questions, this survey aimed to uncover the intricacies of cryptocurrency and Web 3.0 technology adoption within a Swiss context. The subsequent table 2 provides a detailed account of the Swiss responses and how they contrast or align with the findings from Thailand.

Question	**Thailand (Yes %)**	**Switzerland (Yes %)**	**Absolute Difference (Yes %)**
Are you aware of the advantages and disadvantages of Bitcoin or cryptocurrency investments	46.88%	92.41%	45.52%
Do you actively follow cryptocurrency news?	29.68%	55.70%	26.02%
Would you consider using cryptocurrencies as not requiring significant mental effort?	72.26%	26.58%	45.68%
Would you consider it convenient to use cryptocurrency anytime and anywhere?	56.99%	67.09%	10.10%
Do you possess the necessary resources and understanding to effectively use cryptocurrencies?	43.44%	65.82%	22.38%
Do you view cryptocurrencies as a high-risk investment?	74.84%	91.14%	16.30%

Question	Thailand (Yes %)	Switzerland (Yes %)	Absolute Difference (Yes %)
Would you say you possess sufficient financial knowledge to understand cryptocurrencies?	40.65%	77.22%	36.57%
Do you know that you can exchange cryptocurrencies with Swiss francs or other currencies like any traditional money?	37.57%	97.47%	60.05%
Are you confident about the security aspects of cryptocurrency?	43.66%	55.70%	12.04%
Do you intend to or currently use cryptocurrencies for payments?	41.29%	30.38%	10.92%

Table 2. Comparison of both surveys in Thailand and Switzerland, listing the most significant differences between both countries (difference > 10%).

4.3 Analysis of the Pao Tang Platform's Success

Derived from the interview with Somkid Jiranuntarat, the Pao Tang app amplified its reach through multiple government-backed projects, notably "Chip-Shop – Chai" and "Khon la Krueng". These initiatives aimed to foster a culture of digital payment adoption among the Thai populace. Several determinants underscored its success:

- *Scalable Architecture:* The app's infrastructural design ensured it could manage a burgeoning user base without compromising efficiency.
- *User Experience:* Emphasizing intuitiveness, the app's interface was designed to cater to users spanning various age brackets, including the elderly.
- *Governmental Backing:* State support, especially through the mentioned campaigns, provided the requisite thrust to the app's adoption and incentivized citizens to use the app.
- *Cost Efficiency:* The platform's operations streamlined services, driving down costs while simultaneously widening its outreach.
- *Versatility:* Beyond mere payments, Pao Tang diversified by integrating a suite of services, like lottery, into its framework.
- *Future Vision:* The app's envisioned trajectory moves from a basic wallet, escalating to a more complex digital ecosystem, envisaging an open platform allowing for holistic third-party integrations.

However, despite its digital-forward stance, the platform currently has no roadmap to incorporate cryptocurrencies or blockchain integrations. Somkid Jiranuntarat recognized the advantages of cryptocurrencies, especially in fostering innovation and tokenization. Yet, the challenges were equally pronounced, encompassing the need for comprehensive public education, potential misuse, speculative tendencies, and the nuances of regulating digital assets versus digital currencies. Drawing inspiration from countries like Switzerland could pave the way forward for Thailand. Initiatives like the Eastern Economic Corridor (EEC) could provide a conducive environment for testing these technologies, leveraging a sandbox approach. A recurrent challenge echoed the scarcity of skilled personnel in emerging technologies within Thailand.

5. Discussion

In this section, we delve into the findings derived from the survey conducted among respondents in Thailand and Switzerland and the interview with Pao Tang's founder Somkid Jiranuntarat. The analysis unveils the levels of acceptance, understanding, and risk awareness associated with cryptocurrencies in both countries.

RQ 1.1: *How is the acceptance of cryptocurrencies perceived among individuals and institutions in Thailand?*

The data from Thailand illuminates a growing acceptance of cryptocurrencies, especially among younger and male demographics. Interestingly, despite the high-risk perception, there is a pronounced inclination towards both speculative engagements and genuine payment uses. The fear surrounding cryptocurrency security, more palpable among older respondents, underscores the necessity for bolstered public education on this frontier.

RQ 1.2: *What is the level of risk awareness associated with cryptocurrencies among Thai stakeholders?*

A significant 74.84% of Thai respondents categorize cryptocurrencies as high-risk. Yet, this apprehension does not deter them from either speculative engagements or direct payments. This suggests a complex interplay between risk perception and the perceived benefits or necessities driving cryptocurrency engagement among Thai stakeholders.

RQ 1.3: *How is the acceptance and risk awareness of cryptocurrencies perceived in Switzerland?*

Swiss data showcases a high level of cryptocurrency acceptance, coupled with comprehensive risk awareness. Notably, while 91.14% recognize the inherent risks, a substantial proportion (59.49%) still ventures into speculative cryptocurrency engagements. This suggests that Swiss stakeholders are not only well-informed but are also willing to engage with cryptocurrencies despite the associated risks.

This leads to the following findings for RQ 1: *How is the acceptance and risk awareness of cryptocurrencies in Thailand compared to that in Switzerland?*

Awareness and Knowledge: A significant majority of respondents from Switzerland (92.41%) are aware of the advantages and disadvantages of Bitcoin or cryptocurrency investments compared to about half (46.88%) from Thailand. Similarly, 77.22% of Swiss respondents claim to have sufficient financial knowledge to understand cryptocurrencies, in contrast to only 40.65% of Thai respondents. This suggests that Swiss respondents, on average, feel more knowledgeable about cryptocurrencies than their Thai counterparts. Such disparities may be rooted in cultural and educational differences, with Switzerland's rich financial heritage potentially fostering a deeper literacy.

Cryptocurrency as a High-Risk Investment: Datasets from both countries reflect a belief that cryptocurrencies are high-risk investments. However, this sentiment is even more pronounced among Swiss respondents (91.14%) compared to Thai respondents (74.84%). This variance may reflect a deeper understanding or exposure to financial matters, possibly driven by Switzerland's robust financial sector. Moreover, Switzerland's longstanding tradition of financial literacy could contribute to more informed perspectives on the inherent volatility and risk associated with cryptocurrencies. Conversely, the lower risk awareness in Thailand may indicate a need for enhanced financial education and outreach to foster a more nuanced understanding of cryptocurrency risks.

Cryptocurrency Usage and Speculation: The intention to use or currently use cryptocurrencies for speculation or financial gain is slightly higher among Swiss respondents (59.49%) compared to Thai respondents (48.82%). The convenience of using cryptocurrency anytime and anywhere is perceived higher among Swiss respondents (67.09%) than Thai respondents (56.99%). On the other hand, there is a slight preference among Thai respondents for using cryptocurrencies as a payment method (41.29%) over speculation or financial gais. This suggests a potential cultural or regulatory divergence in cryptocurrency utilization. Switzerland’s established financial

infrastructure might foster a speculative approach, while in Thailand, a growing acceptance of digital transactions might be encouraging the use of cryptocurrencies for everyday payments. These trends reflect the evolving narratives of cryptocurrencies within different socio-economic contexts.

Cryptocurrency Security and Resources: More Swiss respondents (65.82%) feel they possess the necessary resources and understanding to use cryptocurrencies effectively compared to Thai respondents (43.44%). Confidence in the security aspects of cryptocurrency is slightly higher in the Swiss dataset (55.70%) compared to the Thai dataset (43.66%).

Influence of Peer Group and Community: The influence of the personal environment is slightly higher in Thailand (34.84% vs. 26.58% in Switzerland). In Thailand the age plays a statistically significant role while in Switzerland the age has no significant influence. This divergence might be indicative of deeper societal structures and cultural predilections influencing financial behaviors.

In summary, Swiss respondents, based on the conducted survey, generally seem more informed and more aware of the risks that come with the usage of cryptocurrencies compared to Thai respondents. This could be influenced by numerous factors, including financial infrastructure, education, cultural attitudes towards investments, and exposure to global financial trends.

RQ 2.1: *What are the key success factors behind the Pao Tang App in Thailand?*

The key success factors behind the Pao Tang app in Thailand include its scaling architecture, outstanding usability, and government support through initiatives like "Chip-Shop – Chai" and "Khon la Krueng" that encourage digital payment adoption. The app's ease of use, QR code-based payment system, and its adoption by small businesses and elderly individuals significantly contribute to its success. Moreover, Pao Tang has reduced service costs and enhanced accessibility to a broader population segment, gradually evolving from a wallet app to envisioning an open digital ecosystem, amplifying its usability and scope.

RQ 2.2: *What opportunities and challenges exist for integrating cryptocurrency and Web 3.0 technologies within the Pao Tang App or similar platforms in Thailand?*

Opportunities for integrating cryptocurrency and Web 3.0 technologies within the Pao Tang app or similar platforms in Thailand include driving innovation, fostering an open economy, and enabling tokenization and digitization of physical assets. Challenges encompass the need for public

education on these technologies, risks of misuse and scams, speculative behaviors, and the regulation of digital assets versus digital currencies. Moreover, the demand for skilled individuals in these technologies, who are currently scarce, presents a significant hurdle. The Eastern Economic Corridor (EEC) is suggested as a potential testbed for such technologies, reflecting a sandbox approach to foster learning from other countries' experiences like Switzerland.

6. Conclusion and Recommendations

Based on our research we can state that in both Thailand and Switzerland there is a functioning digital payment ecosystem. The need for cryptocurrencies in payment is limited and a slightly larger group is using cryptocurrencies for speculation. Most people in Thailand are not aware of the risks, which gives the potential for further education.

Nevertheless, cryptocurrencies offer additional chances, like decentralization, cross border payments, financial inclusion, low fees, open ecosystems, peer-to-peer transactions, and a high innovative potential. Especially for Web 3, global accessibility, ownership over tokens and NFT, and smart contract secured transactions are major advantages.

From our research we derive the following recommendations:

- *Combination of centralized and decentralized payment system:* Web 3 offers a new and global possibility for many people and economies. While centralized digital payment systems are proven and functioning in many countries, a combination with decentralized, blockchain based cryptocurrencies and tokens enfold the full potential of Web 3 use cases. In order to benefit from this innovation, further research like Istrefaj, A. (2023) and sandboxes could help to take advantage of this opportunity.
- *Educational Workshops and Seminars:* One of the primary barriers to understanding decentralized technologies is a lack of foundational knowledge. Only 50.74% of Thai respondents are aware of the advantages and disadvantages of Bitcoin or cryptocurrency investments (92.41% in Switzerland). This disparity in perceived understanding suggests that there is room for educational improvement in Thailand. Partner with universities, colleges, and tech institutions in Thailand to host workshops, seminars, and courses dedicated to blockchain and decentralized technologies.
- *Regulatory Collaboration and Public Campaigns:* The regulatory frameworks between Thailand and Switzerland differ. There is still uncertainty with the industry and public. Thai

regulatory bodies should establish clear guidelines and standards for digital wallet operations that can create a safer and more trustworthy environment for users.

- *Grassroots Community Building:* Another possibility is the usage of communities since they play a pivotal role in fostering learning and sharing experiences. Encouraging grassroots communities in Thailand can help disseminate such fundamental information more effectively. By encouraging peer-to-peer learning, early adopters and enthusiasts can share their experiences and knowledge with newcomers. The Eastern Economic Corridor (EEC)[1] offers a chance to build a sandbox and testbed for experimenting with new regulations and approaches to this technology.
- *Clear Licensing and Registration:* Only 45.22% of Thai respondents are confident about the security aspects of cryptocurrency. A clear licensing system can enhance trust and security confidence among users by ensuring that platforms adhere to standardized security practices. This would help ensure that only legitimate and compliant entities operate in the market.
- *Consumer Protection Mechanisms:* With 78.31% of Thai respondents viewing cryptocurrencies as high-risk investments, robust consumer protection mechanisms can address these concerns and build confidence in the technology. Establishing mechanisms to protect consumers from fraud, market manipulation, and platform insolvencies could support the trust in this technology. This could be achieved by including mandatory insurance for exchanges or dedicated funds to compensate users in case of losses.

8. Acknowledgments

We extend our heartfelt gratitude to all the survey participants who generously gave their time and shared their insights, enabling us to gather invaluable data for this research. Special thanks are due to our interview partner, Somkid Jiranuntarat, the innovator of the Pao Tang app and the contributor to our perspectives which enriched our understanding and significantly contributed to the depth of this study. We are also very thankful to the President of Siam Technology College, Asst. Prof. Pornpisud Mongkhonvanit, for his guidance and for providing the opportunity to undertake this research study. Lastly, our appreciation goes to Levin Reichmuth and Thomas Ankenbrand from IFZ for the data delivery of the comparative study in Figure 3 and 4.

[1] https://www.eeco.or.th/en

9. References

Achyar, D. H., Hasyyati, Z., Yumni, H., & Wafda, F. (2022, March). Acceleration of international tourism improves digital payments usage: The case of Thailand. In 2022 International Conference on Decision Aid Sciences and Applications (DASA) (pp. 212-214). IEEE.

Al-Dmour, A., Al-Dmour, H. H., Brghuthi, R., & Al-Dmour, R. H. (2021). Factors influencing consumer intentions to adopt e-payment systems: Empirical study. International Journal of Customer Relationship Marketing and Management (IJCRMM), 12(2), 80-99. http://doi.org/10.4018/IJCRMM.2021040105

Banchongduang, S. (2022, December 15). KTB set to roll out digital loans on Pao Tang in 2023. Bangkok Post. Retrieved from https://www.bangkokpost.com/business/general/2460865/ktb-set-to-roll-out-digital-loans-on-pao-tang-in-2023

Bashir, I., & Madhavaiah, C. (2015). Trust, social influence, self-efficacy, perceived risk and internet banking acceptance: An extension of technology acceptance model in Indian context. Metamorphosis, 14(1), 25-38.

Crypto ownership by country. (2023, August 29). Statista. https://www.statista.com/statistics/1202468/global-cryptocurrency-ownership/

Decaro, F., & Saleh, Z.I. (2003). An examination of the internet security and its impact on trust and adoption of online banking.

Digitalisation trends in the Swiss payment landscape. (n.d.). European Payments Council. Retrieved October 2, 2023, from https://www.europeanpaymentscouncil.eu/news-insights/insight/digitalisation-trends-swiss-payment-landscape

Editorial Team. (2022). Krungthai Bank's super app, 'Pao Tang', an all-in-one platform for Thais. INTLBM. https://intlbm.com/2022/07/25/krungthai-banks-super-app-pao-tang-an-all-in-one-platform-for-thais/

Financial Landscape for Digital and Sustainable Economy. (n.d.). Bank of Thailand. Retrieved September 20, 2023, from https://www.bot.or.th/en/financial-innovation/financial-landscape.html

Finma. (2018). FINMA publishes ICO guidelines. Eidgenössische Finanzmarktaufsicht FINMA. Retrieved October 2, 2023, from https://www.finma.ch/en/news/2018/02/20180216-mm-ico-wegleitung/

Gohwong, S. G. (2017). The state of the art and trend of cashless society in Thailand. Asian Political Science Review, 1(2).

IFZ (2023). Crypto Assets Study 2023: An overview of the Swiss and Liechtenstein crypto assets ecosystem. Institute of Financial Services Zug IFZ 2023.

Istrefaj, A. (2023). How can classic payments be linked to Web3 payment systems without acquiring cryptocurrencies? Bachelor Thesis, Lucerne University of Applied Sciences and Arts, 2023.

Khiaonarong, T. (2000). Electronic payment systems development in Thailand. International Journal of Information Management, 20(1), 59-72.

Krungthai Bank. (2022, July 25). Krungthai Bank's super app, 'Pao Tang', an all-in-one platform for Thais. International Business Magazine. Retrieved September 20, 2023, from https://intlbm.com/2022/07/25/krungthai-banks-super-app-pao-tang-an-all-in-one-platform-for-thais/

Krugthai. (2022). Growing together for sustainability: Sustainability Report 2020. Retrieved September 20, 2023, from https://krungthai.com/Download/CSR/CSRDownload_70SD_report_63_en.pdf

Lamsam, A., Pinthong, J., Rittinon, C., Shimnoi, A., & Trakiatikul, P. (2018). The journey to less-cash society: Thailand's payment system at a crossroads. Pouey Ungphakorn Institute for Economic Research, 1–53.

Legal Counsel and Development Department, The Office of the Securities and Exchange Commission. (2018, May). Summary of the Royal Decree on the Digital Asset Businesses B.E. 2561. Retrieved September 8, 2023, from https://www.sec.or.th/EN/Documents/ActandRoyalEnactment/LawReform/summary-decree-digitalasset2561.pdf

Liu, G., Huang, S. P., & Zhu, X. K. (2008, November). User acceptance of Internet banking in an uncertain and risky environment. In 2008 International Conference on Risk Management & Engineering Management (pp. 381-386). IEEE.

Moenjak, T., Kongprajya, & Monchaitrakul, C. (2020). Fintech, financial literacy, and consumer saving and borrowing: The case of Thailand. ADBI Working Paper Series, 110. Retrieved from https://www.adb.org/sites/default/files/publication/575576/adbi-wp1100.pdf

Okanurak, W., Nakarat, W., & Koohasaneh, S. (n.d.). Emergemcu Decree on Digital Asset Businesses B.E.2561(2018). Retrieved September 5, 2023, from https://www.sec.or.th/EN/Documents/EnforcementIntroduction/digitalasset_decree_2561_EN.pdf

Patil, P., Rana, N., Dwivedi, Y., & Abu-Hamour, H. (2018). The role of trust and risk in mobile payments adoption: a meta-analytic review.

Payong Srivanich. (n.d.). Growing together towards sustainability in Thailand. World Finance. Retrieved from https://www.worldfinance.com/banking/growing-together-towards-sustainability-in-thailand

Rankings by Country of Average Monthly Net Salary (After Tax). (n.d.). Retrieved October 2, 2023, from https://www.numbeo.com/cost-of-living/country_price_rankings?itemId=105&displayCurrency=CHF

Schärli, K., Luthiger, R., & Trost, A. (2023). Switzerland - Trends and Developments. In Fintech 2023. MLL Legal. Retrieved from https://mll-legal.com/wp-content/uploads/2023/05/041_SWITZERLAND-TD.pdf

Tamphakdiphanit, J. & Laokulrach, M. (2020). Regulations and Behavioral Intention for Use Cryptocurrency in Thailand. Journal of Applied Economic Sciences, Volume XV, Fall, 3(69) 523-531.

Team, D. A. (2022). Digital adoption in the banking industry. Digital Adoption. Retrieved from https://www.digital-adoption.com/digital-adoption-banking-research/

Whatfix. (n.d.). Digital Adoption & Banking: a 7-Step framework. LinkedIn. Retrieved from https://www.linkedin.com/pulse/digital-adoption-banking-7-step-framework-whatfix/

7.3. Toxic Liquidation Spirals

AUTHORS:

Jakub Warmuz

Amit Chaudhary

Daniele Pinna

Toxic Liquidation Spirals

Jakub Warmuz [*] Amit Chaudhary [†] Daniele Pinna [‡]

December 14, 2022

Abstract

On November 22nd 2022, the lending platform AAVE v2 (on Ethereum) incurred bad debt resulting from a major liquidation event involving a single user who had borrowed close to $40M of CRV tokens using USDC as collateral. This incident has prompted the Aave community to consider changes to its liquidation threshold, and limitations on the number of illiquid coins that can be borrowed on the platform. In this paper, we argue that the bad debt incurred by AAVE was not due to excess volatility in CRV/USDC price activity on that day, but rather a fundamental flaw in the liquidation logic which triggered a toxic liquidation spiral on the platform. We note that this flaw, which is shared by a number of major DeFi lending markets, can be easily overcome with simple changes to the incentives driving liquidations. We claim that halting all liquidations once a user's loan-to-value (LTV) ratio surpasses a certain threshold value can prevent future toxic liquidation spirals and offer substantial improvement in the bad debt that a lending market can expect to incur. Furthermore, we strongly argue that protocols should enact dynamic liquidation incentives and closing factor policies moving forward for optimal management of protocol risk.

1 Introduction

On November 13th, Avraham Eisenberg[1], the trader linked to last month's $114 million Mango Markets exploit, borrowed 92 million curve (CRV) tokens (worth $38 million at the time), using 90 million USDC as collateral, on the decentralized lending platform Aave. After a series of wild swings in the CRV price, Eisenberg's position was abruptly liquidated on November 22nd. This ultimately left Aave with $1.78 million of bad debt. In response to the attack, the Aave community is considering making changes to its liquidation threshold, implementing limitations on the number of illiquid coins that can be borrowed on the platform, and curtailing rehypothecation. Aave rehypothecates collateral posted by its clients, which increases capital efficiency but also exposes the protocol to the risk of not being able to liquidate collateral in the event of a price drop. In addition, Llama and Gauntlet authored a proposal suggesting that Aave's reserve fund and Gauntlet's insolvency fund could be used together to cover the outstanding debt. Aave's Protocol has about $165 million in its reserve fund, while Gauntlet's has about 4,923 Aave tokens worth about $283,000 in total. The proposal is currently under review for a governance vote.

On DeFi lending markets, users are liquidated whenever their loan-to-value (LTV) ratio surpasses a threshold value. Once that takes place, the protocol's algorithm incentivizes the repayment of the user's loans. It does so by allowing anyone to purchase the user's

[*] jakub@0vix.com
[†] a.chaudhary.1@warwick.ac.uk
[‡] phys2172@ox.ac.uk / daniele@0vix.com
[1] Wallet address: 0x57E04786E231Af3343562C062E0d058F25daCE9E

collateral funds at a discount. In this paper we quantify how this incentive mechanism can behave sub-optimally, and cause bad debt accrual. We further show how insolvency risks can be managed with small tweaks to the liquidation logic. We quantitatively study the statistical consequences of alternatively halting all liquidations past a certain point, adjusting the liquidation incentive dynamically as a function of the user's LTV, and modulating a technical parameter known as the closing factor.

In Section 2 we summarize the salient features of how a liquidation functions with a minimal model. In Section 3 we introduce a limit beyond which the liquidation logic itself will deterministically accrue bad debt to the protocol. As a case study, we review the mechanics of the bad debt incurred by AAVE on November 22nd by employing the ∅VIX protocol simulator Chaudhary and Pinna (2022). Using a mixture of all available on-chain data and minute-level price histories, all theoretical results discussed are confirmed through extensive numerical simulations. To avoid singling out the AAVE protocol, we note that the conditions for enabling such toxic liquidation spirals are actually shared ny a number of major DeFi lending markets, thus deserving significant attention.

This work aims to extend the limited but rapidly growing literature on systematic stability in decentralized finance. Recent quantitative literature has focused on the stability of automatic market makers (AMMs)Lehar and Parlour (2022) and their value towards liquidity providers versus retaining optionality over funds Milionis, Moallemi, Roughgarden, and Zhang (2022). The interplay of AMMs and lending markets is has gathered interest recently due to a number of ways it can exhibit dynamical fragility due to a price-liquidity feedback exacerbated by informational asymmetry Chiu, Ozdenoren, Yuan, and Zhang (2022). Our research adds the role of liquidation logic and risky borrowing to understand the insolvency risk carried by DeFi lending protocols.

2 Liquidation Mechanics

To liquidate a given user, liquidators are required to first repay some amount ΔB of the user's total loan B with their own funds before the protocol allows them to repossess some amount ΔC of the user's collateral C. Generally speaking, the precise amounts paid by/to the liquidator are the result of an optimization problem whose complex details fall outside the scope of this letter. For our purposes, it will suffice the reader to know that the collateral value [2] repossessed is equal to the loan amount repaid plus a premium known as the *liquidation incentive* which we will represent mathematically with the letter i.

For completeness, the reader should know that a liquidator is limited in how much of a user loan they are allowed to repay. This limit is imposed through a protocol-set parameter known as the *closing factor*, which will be represented mathematically with the lower-case letter c.

The relationship between ΔC, ΔB, B, i, and c can be expressed mathematically as:

[2] All values are expressed using the US Dollar-$ as numeraire.

$$\Delta B < c \cdot B \tag{1}$$
$$\Delta C = (1+i) \cdot \Delta B, \tag{2}$$

where i is the liquidation incentive. This is how liquidations function in a nutshell.

Liquidation incentives often vary depending on which collateral asset the liquidator wishes to repossess. More exotic assets are typically assigned larger liquidation incentives to urge liquidators to repossess a user's riskiest assets first, before focusing on safer assets such as major stablecoins (USDC, USDT) and bluechip tokens (ETH, wBTC).

In Avi's case, his portfolio only consisted of USDC collateral and CRV loans. As such, liquidators making liquidation calls to his portfolio only had the option to repay some amount of his CRV loan to repossess USDC from his collateral to capture a protocol-set liquidation incentive of 4.5%.

The aim of liquidations is to make the portfolio of a risky user healthier. The health of a user is defined by comparing his portfolio's LTV to a threshold value LTV_{liq} above which the protocol will allow liquidators to intervene. Each collateral asset on a lending market has its own protocol-set threshold value, from which the user's specific LTV_{liq} is computed by performing a weighted average across the user's available collateral assets.

In the case at hand, as Avi only held USDC as collateral, his portfolio's liquidation threshold was equivalent to AAVE's liquidation LTV threshold for USDC: 89%. Whenever Avi's portfolio's loan-to-value ratio satisfied $LTV > 0.89$ (the thin horizontal black line in Figure 1) liquidations would be allowed to commence (thin vertical black lines in Figure 1). The reader should appreciate that when liquidations are allowed to commence, the liquidated user's portfolio is abundantly overcollateralized (i.e. total value of the collateral is greater than the total value of loans $C > B$). This is a necessary condition for trustless lending markets to operate safely.

3 Toxic Liquidation Spirals

If at any point, the liquidation incentives lead the liquidated user's LTV to worsen as a result of liquidations taking place, we will denote the liquidation as *toxic*. Toxic liquidations are dangerous for the protocol since they mathematically guarantee that the user's portfolio health will worsen through no fault of their own. Let us now see when this may occur.

Denote a user's initial and final loan-to-value as LTV_{init} and LTV_{fin} respectively. From our overview of liquidation mechanics (Equation 2 specifically), we have that:

$$LTV_{fin} = \frac{B - \Delta B}{C - \Delta C} = \frac{B - \Delta B}{C - (1+i)\Delta B} = \frac{B/C - (\Delta B/C)}{1 - (1+i)(\Delta B/C)} = \frac{LTV_{init} - (\Delta B/C)}{1 - (1+i)(\Delta B/C)}, \tag{3}$$

where the values B, C, and ΔB can be considered constant once the liquidation is initiated

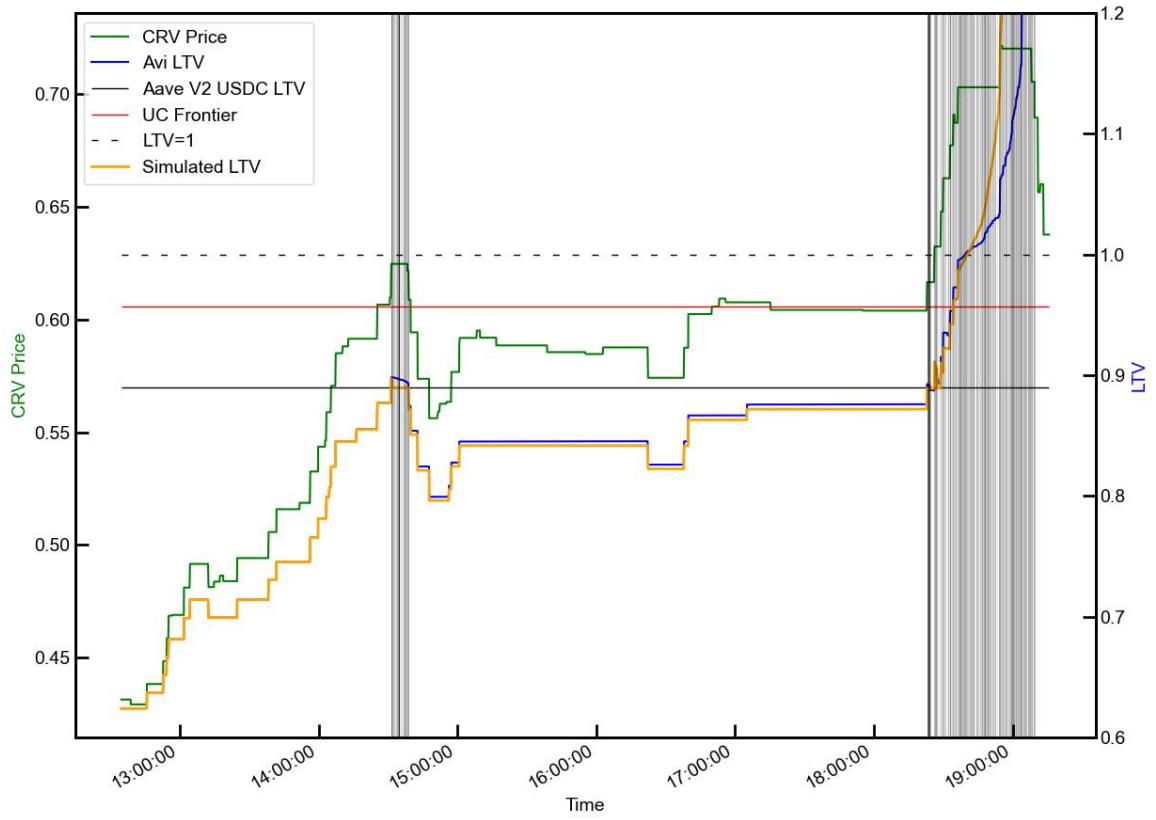


Figure 1: Avi's loan-to-value (LTV) ratio (blue; right axis) and CRV/USDC price (green; left axis) as a function of time on November 22nd, 2022. The plot follows a 6-hour timespan of activity leading to the bad debt creation event. Our simulator's reproduction of Avi's portfolio LTV is shown in gold. A thin black horizontal line marks the 89% LTV threshold above which Avi becomes liquidatable. A red horizontal line marks the threshold beyond which liquidations become toxic (the undercollateralization frontier). A black dashed line shows $LTV = 1$ above which the user's portfolio becomes undercollateralized. Once Avi's LTV crosses the UC frontier, his LTV is worsened by each new liquidation instead of being made healthier. Upon crossing this threshold, his portfolio was guaranteed to become undercollateralized, incurring bad debt for the protocol in the process. Liquidation cascade events are shown as vertical thin lines.

as the entire operation takes place in one single block.

As just defined, the liquidation will be considered *toxic* if the final loan-to-value of the user is larger after the liquidation takes place, $LTV_{fin} > LTV_{init}$. Plugging 3 into this condition [3] results in a fundamental condition between the user's initial LTV and the liquidation incentive offered to liquidators by the protocol for liquidation to be toxic:

$$LTV_{init} > \frac{1}{1+i} \tag{4}$$

If at *A*NY point the user is liquidated while this condition holds, the user's LTV will be made worse by the liquidation. Barring some sudden and very fortuitous price action in the user's favor, this will guarantees that every successive liquidation will have the exact same effect. Liquidations will proceed until all the user's collateral has been used to repay their loans. The leftover loans once all collateral has been repossessed by liquidators will be the final bad debt incurred by the protocol. We will denote this fundamental threshold the undercollateralization (UC) frontier LTV_{UC}.

In Avi's case, his portfolio's constant liquidation incentive of 4.5% implied:

$$LTV_{UC} = \frac{1}{1+0.045} \simeq 0.9569 = 95.69\%. \tag{5}$$

The reader should appreciate that $LTV_{UC} < 1$. This means that when the toxic liquidation spiral commences, the user's portfolio is still overcollateralized. The user has enough collateral to still cover all their loans (i.e. there is no bad debt). However, once $LTV > LTV_{UC}$, even if asset prices were to remain static, the user's portfolio will be guaranteed to become undercollateralized entirely as a result of the liquidation incentives enforced by the protocol, thus incurring bad debt.

In Figure 1 the reader can see how Avi's LTV evolved throughout the day. Whereas the LTV mostly changed proportionally to changes in the CRV/USDC price, once the LTV crossed the LTV_{UC} threshold (horizontal red line) his LTV skyrocketed independently of the CRV/USDC price. In Figure 2 one can see in detail how radically the statistics of Avi's portfolio's LTV adjustments $\Delta LTV = LTV_{fin} - LTV_{init}$ change as his loan-to-value crosses the LTV_{UC} threshold.

[3] Detailed steps can be found in Appendix A

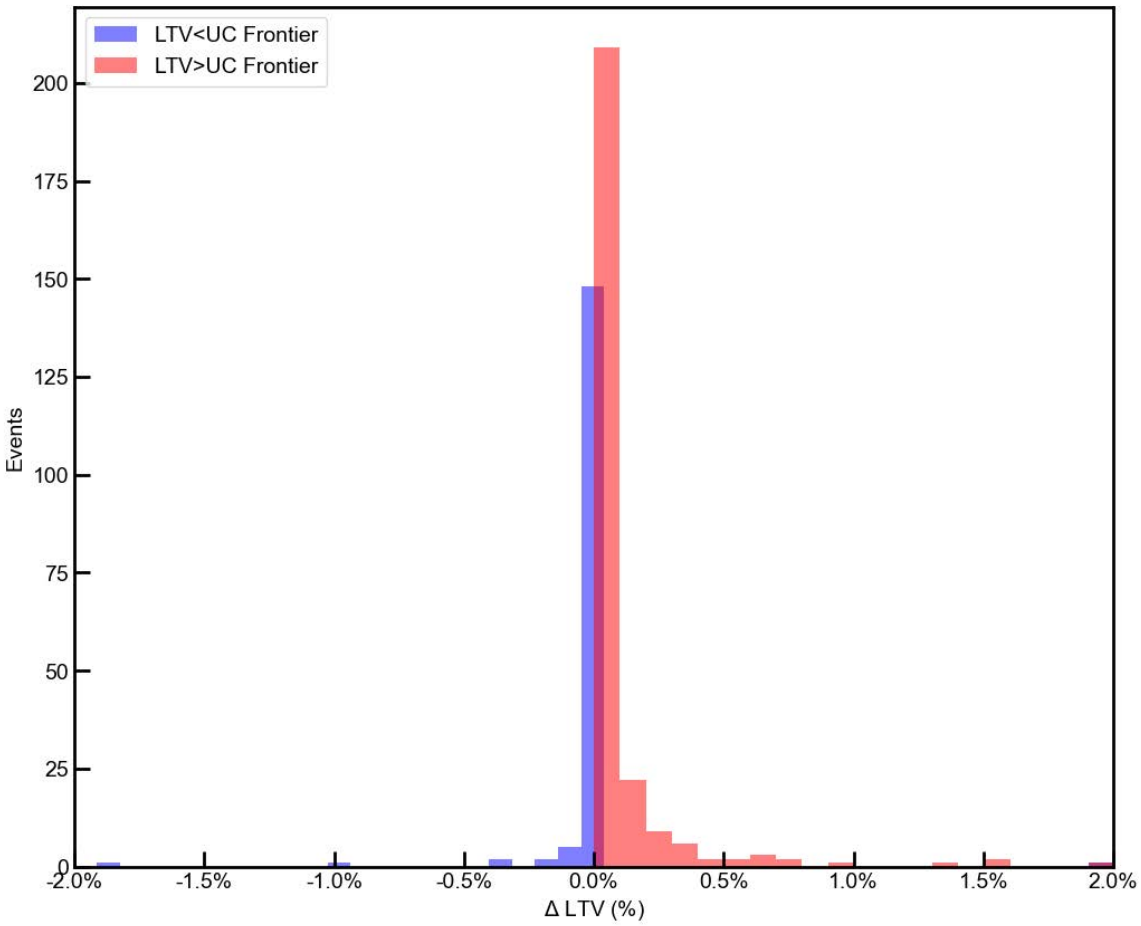


Figure 2: Distribution of changes in user's portfolio $\Delta LTV/LTV_{init} = (LTV_{fin}/LTV_{init}) - 1$ resulting from liquidations when $LTV < LTV_{UC}$ (blue) and when $LTV > LTV_{UC}$ (red).

4 Mitigation Measures

The preceding section should evoke an obvious question in the reader's mind:

Should have AAVE halted liquidations?

In short, the answer is YES. By the time the toxic liquidation spiral commenced CRV/USDC prices were close to topping out after a massive 75% run-up in prices earlier that day. Had AAVE halted all liquidations once Avi's $LTV > LTV_{UC}$, his portfolio would've momentarily become undercollateralized (to the tune of ~$750k) before immediately returning to a healthy state on its own once the CRV/USDC ultimately corrected downwards. This can be seen in the purple line on Figure 3 showing what the bad debt incurred by AAVE would've been on that specific day if liquidations had simply been halted instead of allowing the toxic liquidation spiral to take place.

Alas though, hindsight is 20/20, and nobody at the time could have possibly known how the CRV/USDC price was going to behave from that moment forward. It does however lead to a more meaningful statistical question.

How much bad debt could AAVE have expected to incur moving forward if liquidations had been halted?

At the first $LTV > LTV_{UC}$ moment there are many possible price histories that could develop. The price could in principle keep pumping forever, forcing AAVE to incur massive amounts of bad debt (significantly larger than what was actually realized). The price could also suddenly dump (as it actually happened) leading to no bad debt whatsoever. The price could also stabilize Avi's LTV, or make it oscillate up and down enough for healthy liquidations to take place at intervals. Both of these latter scenarios could lead to some finite amount of bad debt less than what AAVE actually incurred from the toxic liquidation spiral. Anything could've been possible, the question is: *how likely would it have been?*

The market risk assessment methodology described in the Chaudhary and Pinna (2022) allows us to do precisely this. In Figure 1, the solid gold line is our liquidation simulator's reproduction of Avi's price history. The reader can appreciate how faithfully it tracks the real behavior of Avi's LTV (shown in blue). A deviation can be seen in our simulator's liquidation module after Avi's portfolio becomes undercollateralized (i.e. crosses the dashed horizontal black line). This is due to our modelling of slippages incurred by our fictitious liquidators [4] who follow an on-chain state at each block. Overall though, our simulated reproduction of Avi's LTV is satisfactory in the overcollateralized regime, which the main thesis of this paper focuses on. In the undercollateralized regime [5], our liquidation module appears to execute liquidations more efficiently than what happened in real life. As such, statistical results pertaining to toxic liquidation spirals should be deemed as optimistic.

We can use historical CRV/USDC prices to simulate alternative price histories (results are shown for 20k distinct price simulations) [6]. In each, we halt/enable liquidations depending on whether, at any given moment, Avi's LTV is greater/less than LTV_{UC}. Through each individual price trajectory simulation, we track any bad debt incurred and analyze statistics across 20k distinct runs. Readers can see the result of these simulations in the blue curve in Figure 3, where the growing shading around the curve represents 95% confidence bands on the estimated average. At the time Avi's LTV first exceeded LTV_{UC}, AAVE could've expected to incur ~$500k over the following 24 hours. This is roughly significantly less bad debt than what the protocol actually assured itself by allowing liquidations to proceed along their toxic spiral (red curve in Figure 3). Significantly though, the median bad debt of our simulations is ZERO (see Figure 4 discussion). In the majority of simulations, the stress-testing of Avi's portfolio would not have actually incurred any bad debt whatsoever. All for something as simple as halting liquidations.

[4] More details on our slippage modelling can be found in Appendix B.
[5] When undercollateralization ($LTV > 1$) is reached, outstanding loans amount to $ 12.9M.
[6] Refer to Appendix C for more info on data and methods used

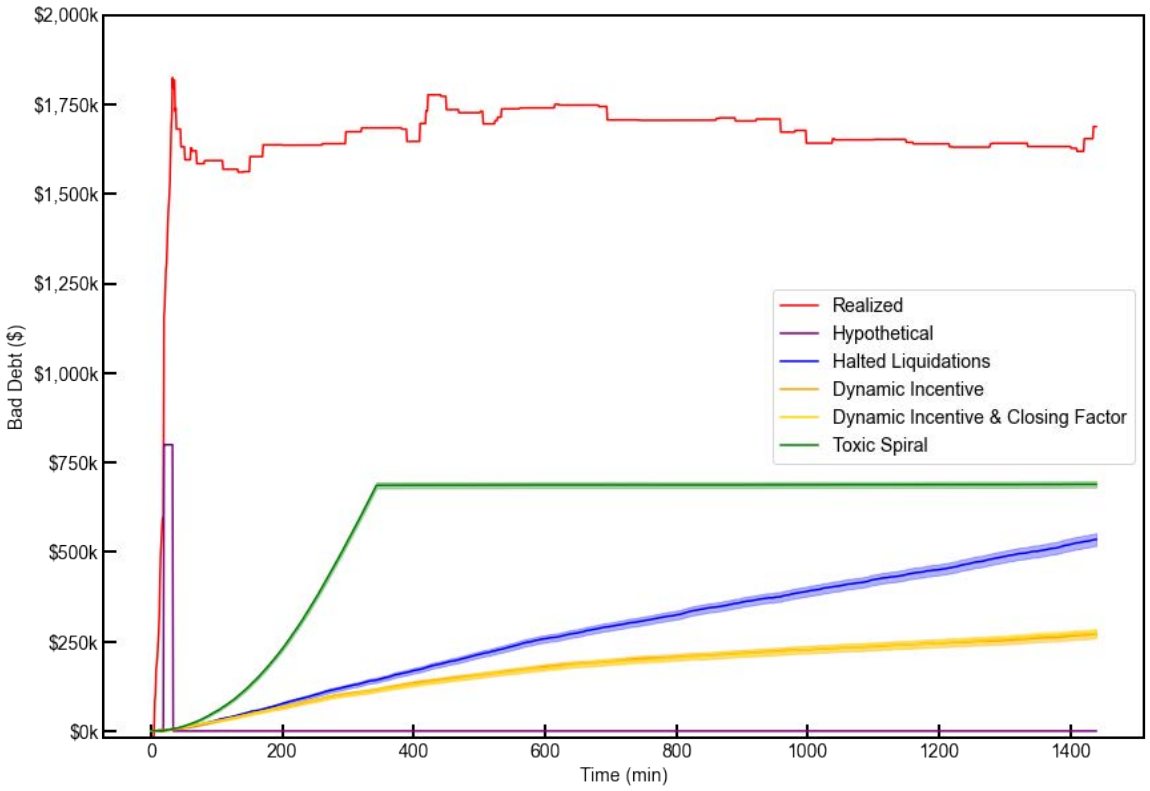


Figure 3: Bad debt incurred by AAVE as a function of time in the 24 hours (1440 minutes) following the moment where Avi's loan-to-value ratio crossed the undercollateralization threshold $LTV > LTV_{UC}$ (Equation 5) implied by AAVE's static liquidation incentives for USDC collateral assets. *Red*: Bad debt AAVE realized due to the liquidation spirals affecting Avi Eisenberg's portfolio health. *Purple*: Bad Debt AAVE would have incurred if liquidations had been simply halted once Avi's $LTV > LTV_{UC}$. *Green*: Average bad debt Aave could have expected from the toxic liquidation spirals as per the current protocol policy. *Blue*: Average bad debt that AAVE could have statistically expected to incur if liquidations had been halted (simulation performed over $20k$ CRV/USDC historical price trajectories). *Gold/Orange*: Average bad debt that AAVE could have statistically expected to incur if liquidations had been handled using dynamic incentives alone (Orange) and with dynamic closing factor policies (Gold) (simulation performed over $20k$ CRV/USDC historical price trajectories).

4.1 Dynamic incentives

The result of halting liquidations is enlightening in its simplicity, but the simulated bad debt can be improved even further with slight tweaks to the liquidation logic. Ultimately, Equation 4 can be flipped on its head to obtain the largest allowable liquidation incentive given the user's LTV at the moment of being liquidated, such that the liquidation is not toxic. The condition reads:

$$i < \frac{1}{LTV} - 1 \tag{6}$$

As long as the liquidation incentive satisfies this condition, user liquidations will always proceed in a healthy manner. It is important to note that when the user's portfolio

becomes borderline undercollateralized ($LTV = 1$) the liquidation incentive vanishes altogether. This is a safer condition than halting liquidations altogether as some liquidators may still find it profitable to liquidate a position by arbitraging the lending market's oracle's price feed. To avoid complications leading to nonsensically negative incentives when $LTV > 1$, and to impose some maximal protocol-set incentive i_0 for a given collateral asset, the full model for healthy liquidation incentives can be written as:

$$i(LTV, i_0) = \max\left[\min\left[i_0, \frac{1}{LTV} - 1 - \epsilon\right], 0\right] \tag{7}$$

where, for extra safety, we have introduced a static modulation parameter ϵ to guarantee that the incentive is strictly less than the right-hand side of condition 6. For practical purposes, ϵ can be any arbitrarily small, non-zero number.

4.2 Dynamic closing factors

The dynamic liquidation incentive 7 can be further paired with a dynamic closing factor which increases as the user's LTV inches towards unity. The idea here is that progressively larger portions of a user's portfolio should be allowed to be closed as the user's portfolio comes progressively closer to becoming undercollateralized. Whenever $LTV \geq 1$, liquidators (or protocol safety modules) should be allowed to liquidate entire asset positions of the user's portfolio in one go. There are many ways this can be expressed mathematically. For concreteness and simplicity we have tested the following linear model:

$$c(LTV, c_0) = \min\left[c_0 \cdot \frac{1 - LTV}{1 - LTV_{liq}} + \frac{LTV - LTV_{liq}}{1 - LTV_{liq}}, 1\right] \tag{8}$$

where we introduce the minimum protocol-set closing factor c_0 similarly to what was done for liquidation incentives earlier, as well as a $\min[\cdot, 1]$ operation to guarantee that closing factors are always a number $c \leq 1$. The reader can verify on their own that whenever $LTV = LTV_{liq}$ the closing factor becomes $c(LTV_{liq}, c_0) = c_0$, while when $LTV \geq 1$ the closing factor becomes $c(1, c_0) = 1$.

The choice of expressions for 7 and 8 is not unique. They can be modified in a number of different ways and optimized for different purposes according to protocol prerogatives. Our choice is meant solely for demonstrative purposes (where the prerogative is simplicity).

Simultaneous use of dynamic incentives and closing factors should allow the protocol to compensate for the decreasing incentives by offering liquidators more absolute liquidity to profit from as a user's LTV becomes more risky to the protocol. In Figure 3, we simulate dynamic incentives both with (orange) and without (yellow) dynamic closing factors. The reader can appreciate how dynamical incentives significantly improve on simple liquidation halting, while the additional inclusion of dynamical closing factors leads to virtually identical results. The orange/gold line (and its shaded confidence interval) shows an expectation of only ~$250k of total bad debt created 24 hours into the future. This is a significant improvement in risk management that any lending market should consider

adopting.

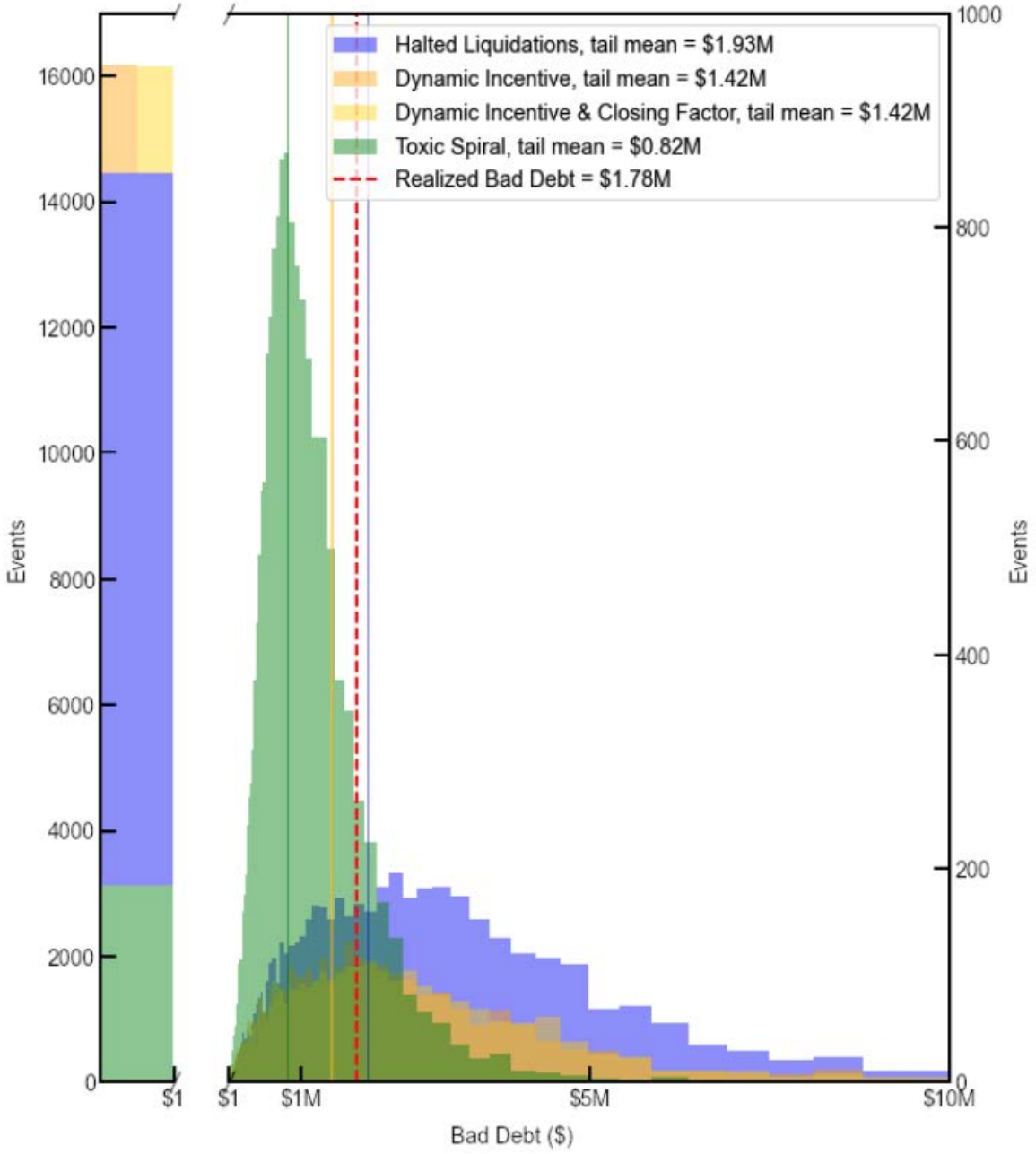


Figure 4: Distribution of bad debt after 24 hours of evolution across the various liquidation policies discussed: toxic spirals (green), halted liquidations (blue), dynamic incentives only (orange), and dynamic incentives + closing factors (gold). The x-axis is broken into two sections to highlight the magnitude of the events involving no bad debt (left vertical axis), while still offering insight into the distribution of tail events (right vertical axis).

The average bad debt shown in 3 does not however tell the entire story of the performance of the different policies shown. For a more nuanced insight, one must look in detail at the distribution of bad debt across the 20k price trajectories used. In Figure 4 we show a detailed histogram of such bad debt distributions taken at the end of the 24hr simulation run. In Figure 4, we plot the histograms of bad debt incurred across all our policy sim-

ulations, at the end of the 24-hour simulation timeframe. Whereas the toxic liquidation spirals trade off higher chances of generating bad debt ($\sim 85\%$) for more certainty on its size (tail mean $= \$820k$), the mitigation policies discussed in the text offer significantly lower chances of generating bad debt ($\sim 19\%$) with slightly larger worst-case outcomes (tail mean$= \$1.4M$). This however assumes that no other open market interventions take place. The mitigation policies discussed in the text offer the protocol optionality on how they wish to handle toxic users on a case-by-case basis, whereas toxic liquidation spirals do not.

5 Discussion and Conclusion

We have demonstrated how the bad debt incurred by AAVE on November 22nd is not the result of speculative price action or irresponsible portfolio positioning. Rather, it is due to a fundamental flaw in the liquidation logic of the protocol which guaranteed that Avi Eisenberg's position would become undercollateralized with almost absolute certainty past some risky, but still overcollateralized portfolio health. We have termed this dynamic, a toxic liquidation spiral. Whereas the phenomenon was qualitatively described in the 2019 Compound audit, to the author's knowledge a detailed study of its effects on insolvency risks was still lacking.

The theoretical insights led us to more deeply analyze alternative tweaks to lending market liquidation logic with the objective of minimizing the expectation of bad debt in the event of a sudden worsening of user's portfolio health [7]. These tweaks were explored by stress-testing Avi Eisenberg's portfolio with thousands of alternative price trajectories using the ∅VIX protocol simulator Chaudhary and Pinna (2022).

Our analysis results in a strong recommendation to all active lending markets to either halt liquidations past a certain user loan-to-value or enact dynamic liquidation incentives and closing factor policies for optimal results. Whereas very little statistical difference can be seen in the performance of dynamic liquidation incentive policy alone versus one that also adds dynamic closing factors, we argue that utilizing dynamic closing factors could offer benefits by allowing non-toxic emergency liquidations of entire user portfolios if necessary. These fall outside the scope of our simulations and would have to be studied on their own. Overall, our suggested policies show a welcome change to the risk profile taken by the protocol. A smaller amount of expected undercollateralized users created is a benefit to all entities involved. A number of major DeFi protocols could benefit from an active consideration of this analysis.

Ultimately, the reason why liquidation LTV thresholds are set to conservative values is not just to allow buffer room for liquidators to aid in keeping lending markets healthy, but also to allow prices to evolve without the need for immediate short-term action. As a general rule of thumb, sudden short-minded responses to complex dynamical behaviors lead to outcomes worse than what the response set out to achieve. They should be avoided

[7] The risk of generating bad debt can never be entirely extinguished.

unless absolutely necessary.

References

Chaudhary, A., & Pinna, D. (2022). Market risk assessment: A multi-asset, agent-based approach applied to the defi lending protocols. *arXiv:2211.08870*.

Chiu, J., Ozdenoren, E., Yuan, K., & Zhang, S. (2022). On the inherent fragility of defi lending.

Lehar, A., & Parlour, C. A. (2022). Systemic fragility in decentralized markets. *Available at SSRN*.

Milionis, J., Moallemi, C. C., Roughgarden, T., & Zhang, A. L. (2022). Automated market making and loss-versus-rebalancing. *arXiv preprint arXiv:2208.06046*.

A Toxicity Spiral Condition

Upon plugging Equation 3 into the toxicity condition $LTV_{init} > LTV_{fin}$ one obtains:

$$LTV_{fin} = \frac{LTV_{init} - (\Delta B/C)}{1 - (1+i)(\Delta B/C)} > LTV_{init},$$

which, upon rearranging, gives:

$$(\Delta B/C) \cdot [(1+i) \cdot LTV_{init} - 1] > 0 \tag{9}$$

The condition 4 is then obtained by noting that the term outside the parentheses in 9 is always greater than zero ($\Delta B/C > 0$) and thus does not contribute to the condition being true or not. If $\Delta B = 0$ it would simply imply that no liquidation is taking place.

We are thus left with the condition:

$$(1+i) \cdot LTV_{init} - 1 > 0, \tag{10}$$

which upon rearranging gives Equation 4 in the main text.

B Slippage Factors

Liquidators are required to first repay a loan with their own funds before repossessing collateral from the liquidated user's portfolio as discussed in Section 2. Since modelling liquidator funds is outside the scope of a first-order liquidation analysis, we assume that liquidators can flash-loan all required funds for no fees.

A liquidator must thus compute the optimal amount $q_{repay} \equiv \Delta B$ they must flash-loan to repay the liquidated user's loan and initiate the liquidation process. All amounts are to be intended as denominated in USD$.

In this Appendix, we walk the reader through the math of the simulator's liquidation module and how we extracted the empirical slippage factors going into our simulations (Figure 5).

B.1 Liquidation Modelling

The first condition on q_{repay} is set by the protocol's closing factor c:

$$q_{repay} < c \cdot B \tag{11}$$

Where B is the total dollar amount of outstanding user loans as described in the main text. Once q_{repay} is repaid, the liquidator is allowed to repossess an amount of collateral $\Delta C = (1+i) \cdot q_{repay}$. Since a liquidator cannot repossess more collateral than the total amount C which the user actually owns. This leads to a second condition on q_{repay}:

$$(1+i) \cdot q_{repay} < C. \tag{12}$$

Once the collateral has been repossessed, the liquidator will swap some amount x to repay the initial flash-loan, incurring some net slippage due to swap routes and trading fees $s(x)$:

$$\begin{aligned} x \cdot (1 - s(x)) &= q_{repay} \\ x &< (1+i) \cdot q_{repay}. \end{aligned} \tag{13}$$

The liquidator's profit Π is whatever is leftover from the operation:

$$\Pi(q_{repay}) = (1+i) \cdot q_{repay} - x(q_{repay}), \tag{14}$$

where $x(q_{repay})$ requires inverting Equation 13 first.

The final condition on q_{repay} is that it be less than the amount $q_{repay} \leq q_{opt}$ which maximizes liquidator profit:

$$\partial_q \Pi(q)|_{q=q_{opt}} = 1 + i - \partial_q x(q)|_{q=q_{opt}} = 0 \tag{15}$$

From which the three constraints defining q_{repay} can be written together as:

$$q_{repay} = \min\{q_{opt}, c \cdot B, \frac{C}{1+i}\} \tag{16}$$

B.2 Linear Slippage Model

In the linear slippage model approximation, one has:

$$s(x) = \gamma + \sigma \frac{x}{L}, \tag{17}$$

where $gamma$ is the trading fee, σ is the *linear slippage factor*, x is the amount being swapped, and L the total available swap liquidity used for normalization.

Inverting equation 13 for x, one gets:

$$x(q) = L \frac{1-\gamma}{2\sigma} \left[1 - \sqrt{1 - \frac{4\sigma q}{L \cdot (1-\gamma)^2}} \right], \tag{18}$$

whose derivative computes to:

$$\partial_q x(q) = \frac{1}{1-\gamma} \left[1 - \frac{4\sigma q}{L \cdot (1-\gamma)^2} \right]^{-1/2} = \frac{1}{1-\gamma} \left[1 - \frac{4\sigma q}{L(1-\gamma)^2} \right]^{-1/2}. \tag{19}$$

The optimal repay amount q_{opt} can then be obtained by plugging 19 into 15 and solving. One gets:

$$q_{opt} = L \cdot \frac{(1+i)^2(1-\gamma)^2 - 1}{4\sigma(1+i)^2} \tag{20}$$

B.3 Empirical Slippage Factors

Slippage factors σ are model parameters that must be extracted from real-world data. Ideally, they require linearly approximating the real-world slippage curve as extracted from aggregators. Due to the unavailability of this historical data, we approach the slippage modelling in reverse.

Upon collecting all liquidation calls made on November 22nd, they can be classified according to whether $q_{repay} = q_{opt}$ or not. For each such liquidation, the slippage factor σ can be obtained empirically from Equation 20 to give:

$$\sigma = \frac{(1+i)^2(1-\gamma)^2 - 1}{4(1+i)^2} \cdot \frac{L}{q_{repay}}, \tag{21}$$

where we set $\gamma = 0.003$ in line with typical on-chain AMM trading fees, and $L = \$190M$ in line with normally available liquidity.

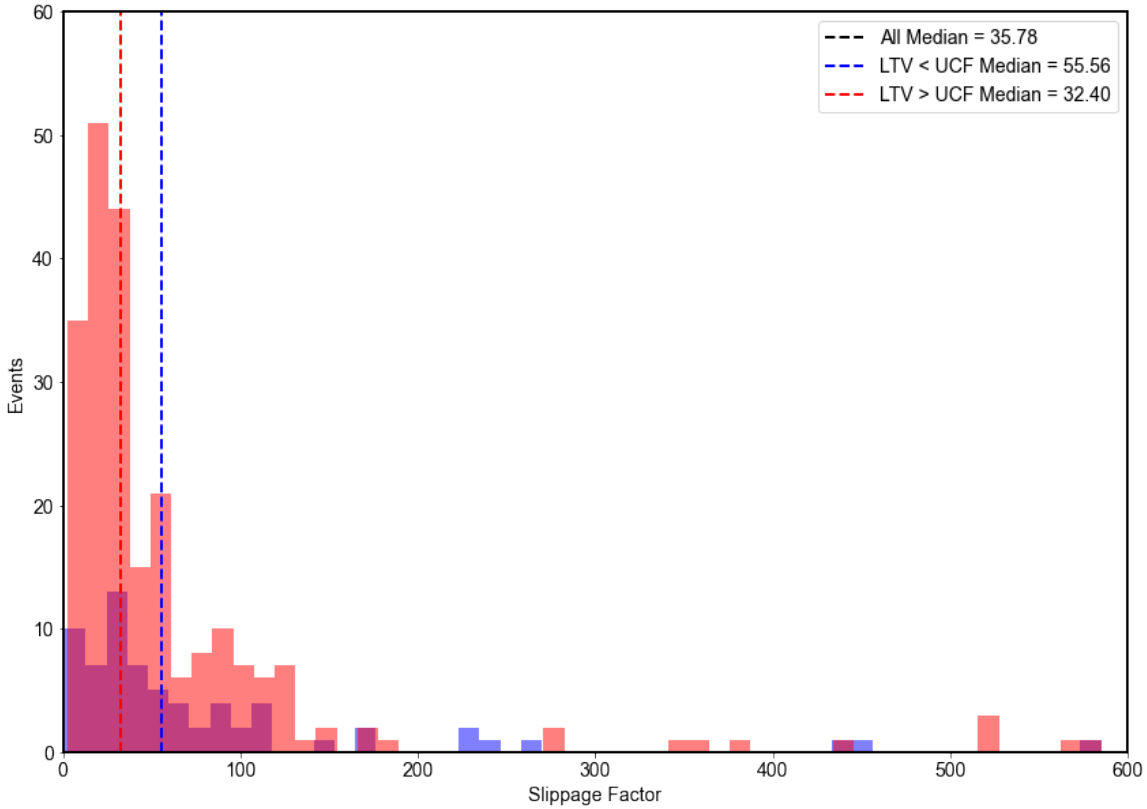


Figure 5: Independent histogram of linear slippage factors as derived from real-life liquidation events occurring before (blue) and after (red) Avi's LTV crossed the UC frontier along with their respective medians (vertical lines). The vertical black line represents the computed median of the entire data set of slippage factors, which was used as the static slippage factor in the simulator's liquidation module.

In Figure 5 we show two histograms charting the empirical distribution of liquidation slippage factors as computed through 21. Following the same color-coding scheme used in Figure 2, we show the slippage factor distribution both before (blue) and after (red) Avi's

portfolio crossed the UC frontier $LTV > LTV_{UC}$. Vertical dashed lines show the median slippage factor of each distribution (dashed red/blue vertical lines), as well as for the entire data as a whole (black dashed vertical line). We use the median of the entire dataset as the slippage factor in the liquidation module of the ∅VIX protocol simulator Chaudhary and Pinna (2022) when running simulations on Avi's portfolio's bad debt.

For readability, Figure 5 cuts the x-axis off at values of $\sigma = 600$ while 22 larger values (out of 318 total events) were observed.

C Data & Methods

To conduct this analysis, we queried all available on-chain data pertaining to Avi's interactions with the AAVEv2 protocol. All historical CRV and USDC price data was collected through Amberdata.

The on-chain data was collected from the protocol's subgraph. We made static calls to Aave's smart contracts at selective timestamps to confirm the reliability of TheGraph's data. Our initial dataset was comprised of 385 liquidation calls on Avi's position, starting on November 22, 2022, 1:31:23 PM GMT, and ending on Tuesday, November 22, 2022, 6:09:23 PM. We have enriched it, also using the same source, by collecting the CRV and USDC prices at each block, beginning 2 hours before the first liquidation call and ending 24 hours after the last one. Given that the prices can fluctuate across oracles, we have decided that relying on the protocol's own will be the most reasonable approach.

As per the asset prices, we had access to the minute-tick OHLCV data from December 11, 2021, to the day of Avi's strategy execution. We transformed this raw data into logarithmic minute-level returns, from which 10k, 24-hour-long samples were drawn for our simulations (1440 price returns per trajectory). To overcome the negative bias trend resulting from the past 12 months of CRV price history, each price trajectory was also reversed and used to collect simulation data. This led to 20k total price trajectories used in this study.

We use an agent-based simulation of crypto money markets with Aave V2 parameters obtained by querying the protocol's smart contracts. For a more detailed discussion, refer to the original paper on the ∅VIX protocol simulator Chaudhary and Pinna (2022).

7.4. How the Travel Rule Protocol (TRP) Addresses the Challenges Presented by the Travel Rule

AUTHORS:

Nicole Giani

21 ANALYTICS

Dominik Spicher

21 ANALYTICS

HOW THE TRAVEL RULE PROTOCOL (TRP) ADDRESSES THE CHALLENGES PRESENTED BY THE TRAVEL RULE

Nicole Giani

Dominik Spicher

ABSTRACT

Nicole Giani & Dominik Spicher: How The Travel Rule Protocol (TRP) Addresses The Challenges Presented By The Travel Rule

With the growing adoption of the Financial Action Task Force's (FATF) Travel Rule and the EU's Transfer of Funds Regulation (TFR), virtual asset service providers (VASPs) have been presented with a handful of challenges.

This paper will illustrate how the Travel Rule Protocol (TRP) addresses the challenges posed by Travel Rule compliance and ensures seamless integration within existing technological solutions.

Firstly, it elucidates how TRP deployment results in seamless compliance with the FATF's Travel Rule and the EU's Transfer of Funds Regulation that respects data protection and risk mitigation requirements common to the financial services industry.

After that, it describes how the TRP framework, supported by a case study, displays the protocol's decentralised and open-source nature and allows for easy implementation for developers due to its free development tools and the fact that it is built using existing and familiar technologies.

Thirdly, the paper will focus on TRP's ability to circumvent sensitive data issues and facilitate peer-to-peer communication, ensuring that privacy and security remain paramount. It introduces the Travel Address, which effectively solves the VASP discovery problem, bolstering the efficiency of the compliance process.

In conclusion, this paper will demonstrate how TRP emerges as a transformative solution aligning with the tenets of the FATF Travel Rule and TFR requirements via its steadfast commitment to decentralisation, open-source principles, permissionless access, and user-centricity.

TRP bridges the gaps between compliance and innovation and propels the financial ecosystem towards a future of integrity, security, and interconnectivity.

Through its multifaceted approach, TRP pioneers a new era of compliance, where data verification, risk management, and global cooperation coalesce to reshape the contours of modern finance.

TABLE OF CONTENTS **PAGE**

1. LIST OF FIGURES

2. LIST OF ABBREVIATIONS

AML	Anti-money Laundering
CASP	Crypto Asset Service Provider
CDD	Customer Due Diligence
CFT	Combating the Financing of Terrorism
EDD	Enhanced Due Diligence
FATF	Financial Action Task Force
IVMS	InterVASP Messaging Standard
KYC	Know Your Customer
KYV	Know Your VASP
SAR	Suspicious Activity Reporting
TA	Travel Address
TFR	Transfer of Funds Regulation
TRP	Travel Rule Protocol
VASP	Virtual Asset Service Provider

3. CHAPTER 1: TRP DOESN'T TRUST; IT VERIFIES TO MEET TRAVEL RULE COMPLIANCE STANDARDS

3.1 Compliance Standards Explained

Anti-money laundering (AML) standards and recommendations like the Financial Action Task Force's (FATF's) Travel Rule are designed to prevent and detect illegal activities, such as money laundering and terrorist financing, within the financial sector. The *don't trust, verify* principle is also highly relevant in AML and Travel Rule compliance.

Below, we elucidate how the *don't trust, verify* principle is emphasised by AML and Travel Rule standards, followed by their ties to the Travel Rule in section 3.2. *Travel Rule Requirements.*

3.1.1. Customer Due Diligence

The Travel Rule requires virtual asset service providers (VASPs) to conduct thorough customer due diligence (CDD), which includes verifying the identity of customers through government-issued identification documents, verifying the source of funds, and assessing the risk associated with each customer.

3.1.2. Enhanced Due Diligence

For high-risk customers, these standards often mandate enhanced due diligence (EDD), which includes more rigorous verification processes and ongoing monitoring—ensuring that VASPs do not blindly trust but verify the legitimacy of high-risk clients.

3.1.3. Transaction Monitoring

VASPs are required to implement systems for real-time or post-transaction monitoring, as per the FATF and Transfer of Funds Regulation's (TFR's) Travel Rule. Suspicious transactions are flagged for further investigation. The focus is verifying the legitimacy of transactions to prevent illicit money flows.

3.1.4. Suspicious Activity Reporting

If VASPs identify suspicious transactions or activities, they are legally obligated to file suspicious activity reports (SARs) with the appropriate regulatory authorities. This reporting requirement manifests the "*verify*" aspect of these standards to alert authorities to potential wrongdoing.

3.1.5. Record-keeping

VASPs are mandated to maintain accurate and comprehensive customer information and transaction records. This practice ensures that there is a trail of verified information to follow in case of an investigation.

3.1.6. Ongoing Monitoring

VASPs are required to continuously monitor their customers and their activities. This ongoing vigilance ensures that institutions don't trust their own initial assessment but continually verify their customers' legitimacy and transactions.

3.1.7. Beneficial Ownership Disclosure

With AML standards and the implementation of the Travel Rule, VASPs are required to identify and verify the beneficial owners of legal entities, such as corporations and trusts, when onboarding them. This promotes transparency and helps prevent the misuse of legal entities for money laundering.

3.1.8. Technology and Automation

Many VASPs use advanced technologies, including artificial intelligence and machine learning, to improve AML compliance. These technologies help verify claims based on vast amounts of data quickly and accurately, reducing reliance on manual processes.

In summary, AML standards and the Travel Rule emphasise the *don't trust, verify* principle by requiring VASPs to implement rigorous CDD, transaction monitoring, and reporting processes. They promote the verification of customer identities, the legitimacy of transactions, and the ongoing vigilance necessary to prevent and detect money laundering and illicit financial activities.

3.2. Travel Rule Requirements

The FATF Travel Rule, as explained by the FATF (2018), serves the primary purpose of assisting law enforcement authorities in monitoring individuals engaged in fund transmissions through authorised payment systems, thereby acting as a deterrent against illicit financial activities and facilitating the identification, investigation, and prosecution of money laundering, violations of sanctions, and other forms of illicit financial conduct.

3.2.1. The FATF's Travel Rule Requirements

Initially only applicable to fiat wire transfers, the Travel Rule underwent an expansion in response to the advancements in digital technology and the growing popularity of cryptocurrencies.

In 2018, the FATF introduced amendments to its Recommendations, explicitly addressing financial activities involving virtual assets and VASPs while providing comprehensive definitions for these terms. It is noteworthy that the FATF Travel Rule, while constituting a recommendation, holds legal force upon implementation by individual jurisdictions, and numerous jurisdictions have indeed adopted and followed the FATF's suggestions regarding the Travel Rule.

The FATF (2019) put forward Recommendation 16, extending the purview of the Travel Rule to encompass virtual assets. This recommendation specifically mandated the enforcement of the Travel Rule in several scenarios, including

- conventional wire transfers,
- transfers involving virtual assets between VASPs and other obligated entities, as well as
- transfers between VASPs and self-hosted wallets.

It is important to note that while the FATF put forth these specifications above, jurisdictions are free to interpret and implement them as seen fit.
For instance, the TFR instructs CASPs to obtain Travel Rule data on the transfer's originator and beneficiary in the event of a self-hosted wallet transfer, whereas the USA's implementation does not; in fact, it does not include self-hosted wallets within its scope.

Furthermore, it is up to the implementing jurisdiction to decide if the Travel Rule data is to be merely collected or collected and exchanged.

VASPs are defined by the FATF (2021:109) as organisations or individuals operating on behalf of others, engaging in various activities related to virtual assets, such as exchanges between virtual assets and fiat currencies, interchanges among multiple virtual assets, the transfer of virtual assets, safekeeping and administration of virtual assets, and participation in financial services linked to the issuance and sale of virtual assets.

Within this context, VASPs must ascertain the control of **the destination address for funds** (where the funds are being sent or received from), ensuring avoidance of sanctioned entities or individuals. The fundamental principle of *don't trust, verify* guides these operations, with requisite **data exchange occurring before transaction execution**.

Verification criteria encompass the originator's:

- name,
- account number,
- physical address, national identity number, customer identification, or date and place of birth, as verified by the Originator VASP.

Similarly, the beneficiary VASP is tasked with verifying the beneficiary's name and account number to ensure compliance with the Travel Rule's stipulations. (FATF:2021, p.57).

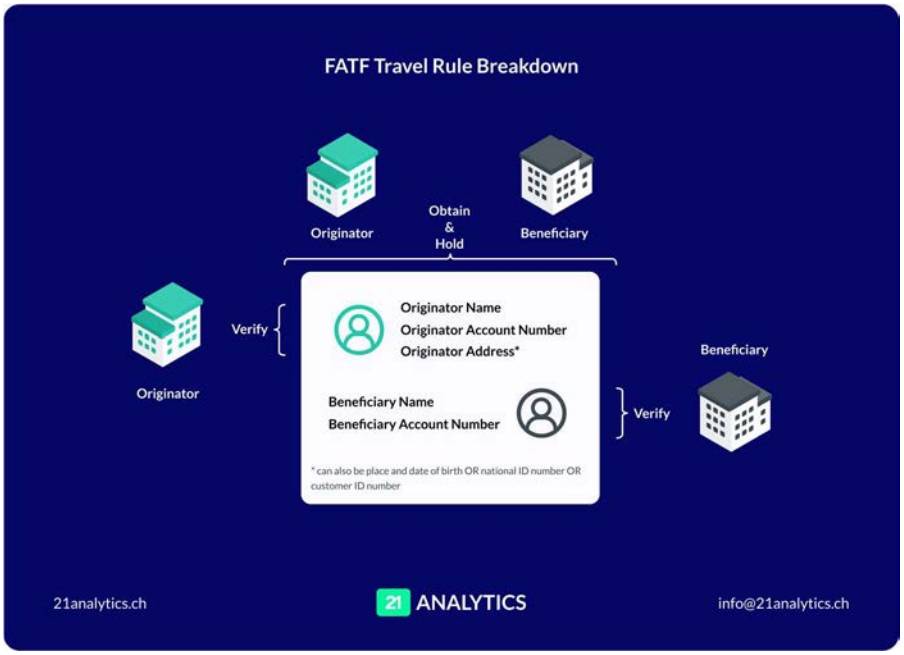


Figure 1: FATF Travel Rule Breakdown. Source 21 Analytics

3.2.2. The TFR's Travel Rule Requirements

In July 2021, the European Commission introduced an AML action plan that established a pan-European AML supervisory body. This initiative sought to standardise AML regulations across the European Union's 27 Member States and expand the scope of anti-financial crime obligations to encompass all CASPs (VASPs).

Subsequently, on 29 June 2022, a provisional agreement was reached between the European Parliament, Council, and Commission concerning the revised TFR. The primary objective of this Regulation is to implement the Recommendations of the FATF, specifically Recommendation 16.

As mentioned above, the Travel Rule applied exclusively to traditional wire transfers; however, with this regulatory development, it is extended to encompass virtual asset transfers involving crypto asset service providers (CASPs) operating within the European Union. Importantly, this Regulation is set to directly apply to all CASPs within EU member countries, eliminating the need for transposition into local legislation. (21 Analytics:2022).

To summarise, a business qualifies as a CASP if it offers any of the following services to European Union citizens:

- providing custody and management services for crypto assets on behalf of a third party,
- offering cryptocurrency exchange services or operating a cryptocurrency exchange,
- providing cryptocurrency advisory services or offering information categorised as advice related to investing in cryptocurrency assets (this definition excludes portfolio management services). (“Is a VASP a CASP?,” 2022).

In essence, the core elements remain consistent within the context of the FATF's Travel Rule framework. Firstly, a prescribed list of data must be exchanged, encompassing various key details. The European Parliament (2023. p.16) lists these details as:

Originator data, which includes

- name,
- distributed ledger address,
- crypto asset account number,
- address, which must include the name of the country, official personal document number and customer identification number, or date and place of birth,
- LEI (where applicable, or an equivalent official identifier).

Beneficiary data, which includes

- name,
- distributed ledger address,
- crypto asset account number,
- LEI (where applicable, or an equivalent official identifier).

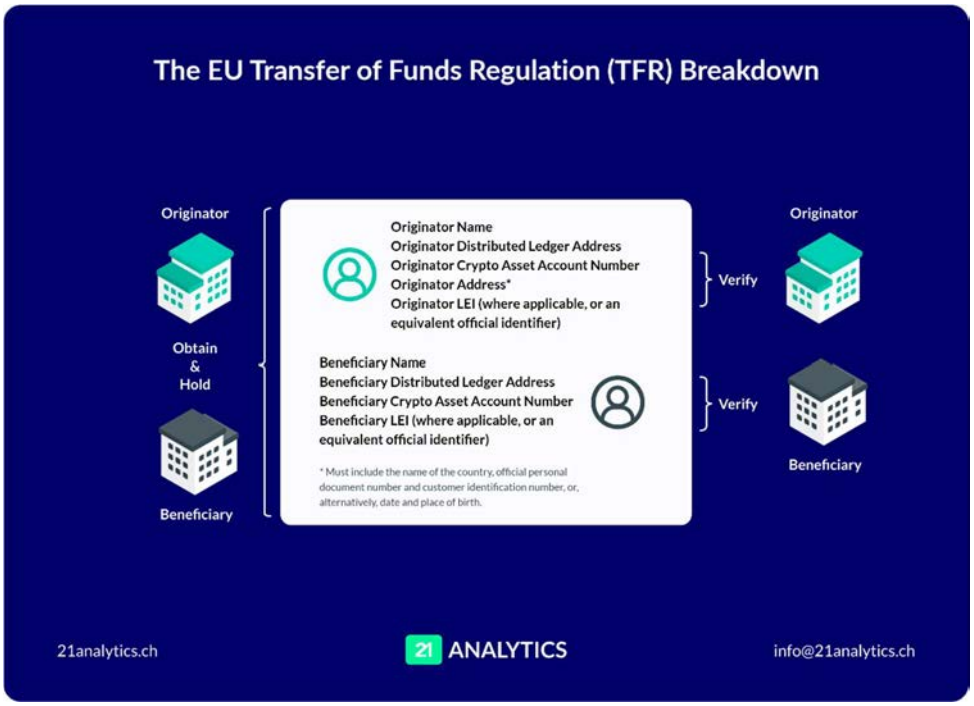


Figure 2: The EU Transfer of Funds (TFR) Breakdown. Source 21 Analytics

Additionally, a robust understanding of the counterparty, often requiring EDD, is imperative to ensure compliance. Equally critical is the **timing of data transmission**, as the **release of funds is contingent upon the receipt and verification of this essential information**. It is noteworthy that the intricacies of the General Data Protection Regulation must be observed during this process. Furthermore, self-hosted wallets are included in the TFR framework.

Like the FATF's Travel Rule requirement, which it is supposed to implement, the TFR stipulates the need for data to be verified and received before the transfer of virtual assets can occur—reiterating the notion of *verification over trust*: a pivotal element in the Travel Rule. (The European Parliament:2023. p.17).

As seen above, the need for VASPs to implement rigorous CDD, transaction monitoring, and reporting processes is paramount to comply with AML policies and the Travel Rule.

At any but the smallest scales, this involves the use of technological solutions. This introduces a new burden on VASPs: They need to ensure that their technological tools are actually compliant with relevant policies. As we will see, this is often not the cases. (These deficiencies will be explained in section 3.3, followed by a discussion of how TRP counters these deficiencies in section 3.4.)
This again highlights the theme of *don't trust, verify* - if technological solutions are not compliant, VASPs cannot engage in compliant business practices.

3.3. Deficiencies in Travel Rule Solutions

Based on the above commentary, many of the available Travel Rule solutions lack the required fundamentals to ensure Travel Rule compliance, resulting in a failed attempt at risk management, often succinctly summarised as *trusting without verification*. Examples of these failures will be elaborated upon below.

3.3.1 Travel Rule Information Not Exchanged as per Regulations

The originating VASP must validate and furnish the subsequent details, as seen in Figure 1, page 9, before initiating a transaction:

- originator's full name,
- originator's account number,
- either the originator's physical address or their national identity number, customer identification, or their date and place of birth.

Furthermore, the beneficiary VASP must obtain and verify the following information prior to conducting any transactions:

- beneficiary's complete name,
- beneficiary's account number.

The verification process is a crucial facet within the integral components of the Travel Rule. In order to execute the Travel Rule efficiently, this information should be communicated to the beneficiary VASP and securely retained. Care needs to be taken to ensure this data is not exposed.
If this data is not exchanged, VASPs cannot release the assets.

3.3.2 Incorrect Timing of Data

A further concern emerging in Travel Rule software pertains to the temporal aspect of Travel Rule information exchange. The Travel Rule's principal aim is to empower VASPs to promptly respond to potentially dubious virtual asset transfers, thus imposing stringent timing requirements for data transmission. Consequently, Travel Rule data should be disseminated prior to or concurrently with the transaction execution in strict adherence to regional data protection regulations to ensure secure handling.

3.3.3 Allowing Transfers to Sanctioned Addresses and Countries

The FATF Travel Rule (2021:p.62) and implementations thereof mandate originators and beneficiaries to know where the funds are being sent to or received to avoid receiving funds from sanctioned addresses and sanctioned counties.

Therefore, Travel Rule solutions need a means for users to verify this information before sensitive Travel Rule data exchanges and the release of assets.

Many solutions do not have this functionality, resulting in virtual asset transfers on behalf of sanctioned entities.

3.3.4. Absent VASP Discovery

As explained above (section 3.3.3), individuals and entities cannot send and receive funds to and from unknown VASPs, reiterating *don't trust, verify*.

In regular instances, as seen in a bitcoin address, no information is provided besides the currency. In other words, no additional information - which is pertinent to make a Travel Rule compliant and low-risk transfer - is provided.

3.3.5. Insufficient Due Diligence

With the exchange of an address alone, VASPs cannot conduct sufficient due diligence.

- They cannot ascertain if the funds are being sent to a self-hosted wallet or VASP, as explained in 3.3.4.
- They cannot check if the beneficiary has been KYVed before sharing further information or if it has been sanctioned.

The recent FATF Virtual Assets Contact Group (VACG) displayed its concern at the increased number of shell VASPs (parasite VASPs) used to conduct illicit activities.

> *"The use of shell VASPs to conduct illicit activities has been discussed as a problem, and it is essential for VASPs to detect whether a shell VASP is using their services. In short, a shell VASP (also known as parasite VASP) uses a regulated VASP's services to offer VASP services to sanctioned parties".* ("FATF Virtual Assets Contact Group (VACG): 21's Takeaways", 2023).

3.3.6. Insufficient Virtual Asset Support

The Travel Rule is all-encompassing, extending its applicability to **every virtual asset**. Consequently, any Travel Rule-compliant solution must encompass all virtual assets and provide the requisite Travel Rule data alongside each transaction. If a virtual asset is not supported by the solution, the software must decline such transactions as it is not Travel Rule compliant. It is essential to underscore that transactions must not proceed without including Travel Rule data.

3.4. TRP Doesn't Trust; It Verifies to Meet Travel Rule Compliance Standards

The FATF Travel Rule is the epitome of *don't trust, verify* with its requirement of data collection, verification and storage to ensure safe transactions, and as such, it requires a protocol that can meet this need.

As seen repeatedly with failed exchanges, one cannot trust the information gleaned from one's counterparty. The information must be verified via trustworthy and reliable means, such as protocols like TRP.

TRP effectively addresses the aforementioned shortcomings within the virtual asset transaction space. When initiating a transaction through TRP, VASPs are prompted to input customer Travel Rule information strictly per the Travel Rule requirements before proceeding.

Furthermore, TRP offers VASPs the capability to authorise or reject inbound transactions (21 Analytics:2022) prior to any on-chain activities, ensuring comprehensive Travel Rule compliance. This is enforced on a protocol level by sharing blockchain destination addresses only once the supplied Travel Rule data has been deemed satisfactory. This feature is especially advantageous for VASPs not engaging in transactions involving specific currencies, as it facilitates swift rejection procedures.

Additionally, all transactions facilitated by TRP include internal account numbers and postal addresses, positioning the protocol as the most Travel Rule-compliant software available in the current landscape.

It is important to emphasise that TRP is one of the sole protocols in full adherence to FATF Recommendations due to its functionalities, further discussed in section 4.3, the TRP Flow. Its attributes encompass a global perspective, allowing VASPs to operate without being tied to any jurisdiction.

In section 4, TRP's framework and design will be discussed to illustrate its seamless integration into existing solutions and technologies, ensuring familiarity and ease of implementation for IT and development teams.

TRP is permissionless, decentralised, and open-source, enabling unrestricted contribution to its development and implementation, free from dependencies on specific entities or gatekeepers.

In tangent, the FATF remarked that the Travel Rule has not been widely adopted by low-resource countries; one of the rationals is the cost of Travel Rule software and protocols. Therefore, the FATF has recognised the significance of enabling low-resource countries to engage in the virtual asset arena and has designated them as a primary focus.

To facilitate their participation, the FATF is encouraging the development and adoption of open-source protocols and solutions, like TRP. (Cited in 21 Analytics:2023).

4. CHAPTER 2: TRP: AN OPEN-SOURCE STANDARD

4.1. TRP Adherers to the *Don't Trust, Verify* Principle

Several key concepts and techniques can be applied to make a protocol or system adhere to the concept of *don't trust, verify*. TRP was designed under these principles.

4.1.1. Open Source and Transparent

The protocol's specification is open for inspection and auditing. Transparency allows anyone to review the code, find vulnerabilities, and ensure no hidden backdoors or malicious components.

4.1.2. Decentralisation and Permissionless Access

Decentralisation was achieved through the distribution of control and verification responsibilities among multiple parties or nodes. Within the protocol, no privileged party exists between the originator and beneficiary VASPs and may act as a gatekeeper. This is in stark contrast to numerous other Travel Rule protocols that have been proposed.

4.1.3. Auditing and Third-Party Verification

Independent security auditors and experts have reviewed and verified the security and integrity of the protocol, adding an additional layer of trustworthiness.

4.1.4. Permissionless and Trustless Systems

The protocol was designed to be permissionless and trustless. In a trustless system, participants can interact without having to trust a central authority.

4.1.5. Community Involvement

TRP calls for active community participation in the development and verification of the protocol.

By implementing these principles and techniques, a protocol can work towards meeting the *don't trust, verify* standard, enhancing security, transparency, and trustworthiness in various domains, including blockchain, cybersecurity, and beyond.

4.2. Tools and Libraries to Accompany TRP

TRP was designed with various open-source tools and libraries readily available for development teams tasked with implementing the Travel Rule Protocol. These resources afford developers comprehensive access to the underlying source code, promoting transparency and ease of integration into TRP-related projects.

Sections 4.2.1 - 4.2.3 are intended to offer a brief overview of these tools, which will be revisited in later chapters. The purpose is to give the reader a basic understanding of these tools.

4.2.1. The IVMS Validator and Open-source Library

Developers can use the IVMS 101 Validator to assess the compatibility of input data with the IVMS 101 data model standard, a framework used within the context of the TRP.

The open-source IVMS library aids faster and broader adoption of TRP through straightforward integration into existing software.

- Example of protocol flow: https://gitlab.com/OpenVASP/travel-rule-protocol/-/blob/master/core/specification.md#detailed-protocol-flow
- IVMS Library source code: gitlab.com/21analytics/ivms101

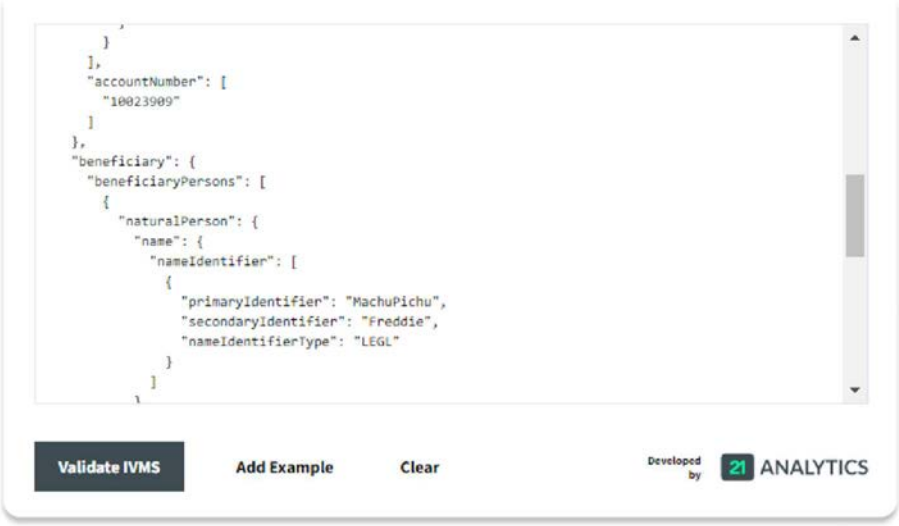


Figure 3: IVMS Validator with Example. Source 21 Analytics

4.2.2. The LEI Generator and Open-source Library

TRP uses the "nationalIdentification" field of IVMS 101 for identifying the originating VASP, and for the "nationalIdentifierType", LEIs are used.

The LEI Generator allows developers to create dummy LEI codes which can be used to test products and software.

The open-source LEI library permits developers to use and modify the code according to their needs. Additionally, LEIs are required to be exchanged per the TFR. Therefore, they form a part of TRP's foundation.

- LEI Library source code: gitlab.com/21analytics/lei
- LEI specification: https://www.gleif.org/en/about-lei/iso-17442-the-lei-code-structure
- LEI search: https://search.gleif.org

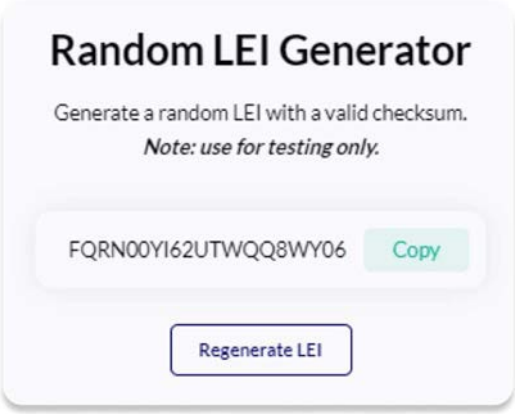


Figure 4: Random LEI Generator. Source 21 Analytics

4.2.3. The TRP Travel Address Encoder/Decoder

This tool lets users see exactly what information a Travel Address comprises.

A Travel Addresses allows VASPs to identify their counterparty VASP as it confirms which VASP controls the receiving address and the VASP's URL to receive Travel Rule data, data not present in a "normal" address.

A Travel Address is a URL encoded in the base58 format, housing a unique URL. Once the originating VASP deciphers the Travel Address, it initiates a request to the associated URL to seek authorisation for transaction execution.

Figure 5: TRP Travel Address Encoder/Decoder with Example. Source 21 Analytics

4.3. The TRP Flow

A VASP using TRP will conduct a Travel Rule-compliant transaction due to the careful verification processes of TRP.

As demonstrated above, TRP uses existing technologies, such as IVMS101 and LEIs, to ascertain customer data and the Travel Address to identify the beneficiary VASP, resulting in additional verification processes, which many other protocols do not factor into the data verification process.

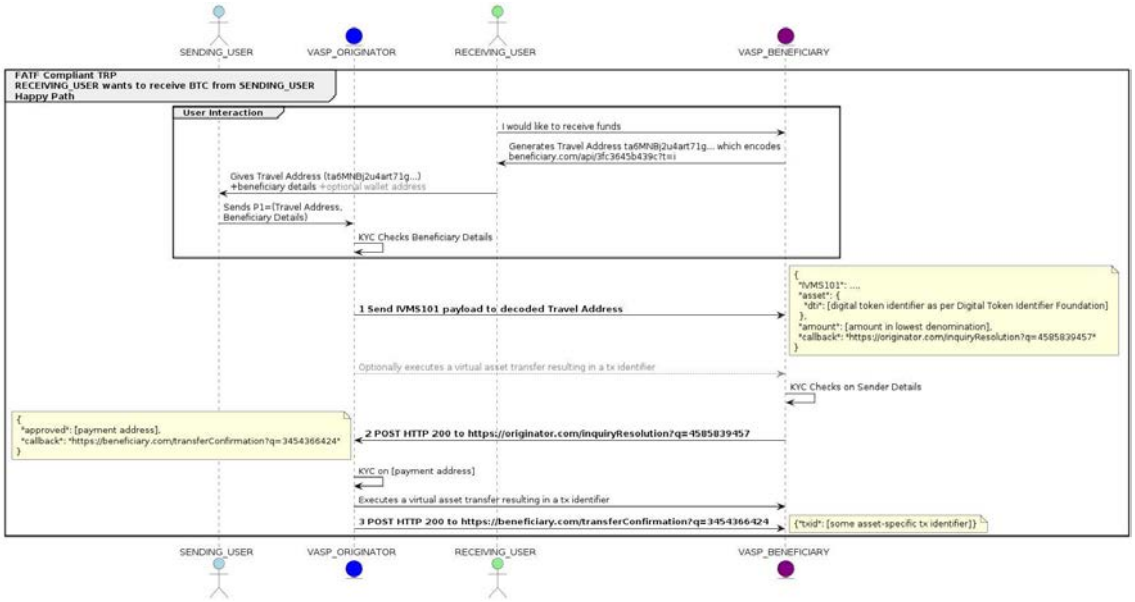


Figure 6: TRP Flow. Source Travel Rule Protocol GitLab Repository

Participants:

Sender: Ori

Receiver: Ben

Originating VASP: VASP O

Beneficiary VASP: VASP B

Objective:

Ben intends to receive bitcoin (BTC) from Ori, and both parties use VASPs to facilitate this transaction.

Actions Taken by Ben and Ori:

- Ben, the beneficiary, communicates his desire to receive BTC from Ori to his VASP.
- The beneficiary's VASP (VASP B) initiates the process by generating a TA and giving it to Ben.
- Ben, as the beneficiary, sends the generated TA to Ori.
- In his role as the originator, Ori conveys this TA to his VASP (VASP O) along with beneficiary details (like Ben's name).

Behind the Scenes Processing:

- Ori's VASP undertakes a sanctions and politically exposed person (PEP) check to verify the details of the beneficiary (Ben).
- If the beneficiary's details are found to be in order, an IVMS payload is sent to the decoded Travel Address. VASPs could use the Travel Address Encoder/Decoder described in section 4.2.3.
- Subsequently, VASP B carries out a sanctions and PEP check on Ori, the sender.
- If Ori's details are deemed satisfactory, VASP B transmits a crypto address to VASP O.
- Ori's VASP (VASP O) optionally runs the provided address through an on-chain analytics tool and executes the transfer.
- The Transaction ID is then sent to VASP B, concluding the transfer.

4.4. A TRP Case Study: The Implementation of TRP and the Challenges Faced

TRP is less complex to implement than most Travel Rule protocols as it uses existing technology building blocks that IT and development teams are familiar with. Below, a case study is presented, which explores the experience of Blockchain Intelligence Group's* (BIG) implementation of the TRP and the challenges encountered during the process. The TRP is a critical protocol for the cryptocurrency industry, designed to address regulatory requirements for transferring customer information between VASPs during cryptocurrency transactions.

Implementation of TRP

BIG embarked on the implementation of TRP to comply with emerging regulatory requirements in the cryptocurrency sector. The institution was keen on evaluating whether TRP effectively addressed the challenges presented by the Travel Rule.

Addressing Travel Rule Challenges

The institution's perspective on TRP was positive. When asked if TRP addressed the Travel Rule's challenges, the response was affirmative. The implementation of TRP was seen as a step in the right direction towards ensuring compliance with Travel Rule requirements.

Implementation Ease and Challenges

The implementation process was generally regarded as straightforward. However, the institution encountered several challenges during the implementation, which were seen as potential roadblocks:

a) Handling KYC Rejections

A challenge was the absence of direct calls for acknowledging the counterparty VASP in the event of Know Your Customer (KYC) rejections. The institution was uncertain if this was the common practice within the banking system. However, the absence of a clear mechanism for handling KYC rejections meant that the counterparty VASP was left waiting for a response, potentially causing delays and uncertainties in the transaction process.

b) Use of Development Tools and Libraries

The institution leveraged development tools and libraries from 21 Analytics, including the IVMS validator and LEI library. However, a notable hurdle was the use of a different

programming framework other than Rust. Nevertheless, the institution expressed an interest in the availability of these tools in various languages, particularly in Java, given its widespread use in fintech applications and banking systems.

Conclusion

In conclusion, BIG's implementation of TRP was generally seen as a positive step towards addressing Travel Rule challenges. The institution recommended the development of TRP tools and libraries in multiple programming languages to facilitate broader industry adoption. Despite the challenges, the institution expressed gratitude for the assistance received during the implementation and emphasised its commitment to compliance with evolving cryptocurrency regulations.

> **"Blockchain Intelligence Group builds technology to power compliance and intelligence for the blockchain-centric future. Leaders use our solutions to transact cryptocurrency or power complex investigations into criminal activity using digital currencies. Banks and crypto companies depend on our technology to monitor risk from crypto transactions. Investigators and law enforcement quickly identify and track illicit activity."* (“Blockchain Intelligence Group: About Us”, 2021)

5. CONCLUSION

In conclusion, TRP exemplifies a compelling model for adequate adherence to AML standards and the Travel Rule, underpinned by a rigorous implementation of the *don't trust, verify* principle. This protocol harmoniously integrates meticulous procedural protocols and state-of-the-art technological advancements to ensure the highest echelon of compliance, emphasising the perpetual verification of transactional legitimacy and customer engagement.

TRP demonstrates an unwavering commitment to the core tenets of CDD, characterised by its insistence upon exacting identity validation procedures, and the persistent scrutiny and validation of customer information and transactional conformity to EDD protocols are judiciously applied in cases of heightened risk, amplifying the verification process when requisite.

In real-time, the salient transaction monitoring and prompt reporting of suspicious activities encapsulate the fundamental "verify" paradigm inherent to AML regulations and the Travel Rule. Transactions flagged as suspicious undergo expedient investigation and, when substantiated, are duly reported to the relevant regulatory authorities, effectively safeguarding against the potential obfuscation of money laundering endeavours.

Moreover, TRP harnesses cutting-edge technology and automated systems, facilitating the expeditious and precision-driven management and processing of substantial data volumes, thereby mitigating the inherent risks of human fallibility and streamlining the verification procedures. This embrace of technology demonstrates TRP's unwavering dedication to staying at the forefront of the ongoing fight against financial crimes.
The incorporation of beneficial ownership disclosure practices within the TRP framework fosters an environment that is notably less conducive to the surreptitious concealment of illicit activities behind corporate facades. This commitment to transparency harmonises with the overarching AML principle of validating the veritable ownership and purposes of legal entities.

In summary, TRP manifests a robust dedication to the pinnacle of AML standards, and the *don't trust, verify* maxim through meticulous CDD practises, the vigilant monitoring of transactions, the prudent integration of advanced technology, and an unwavering commitment to regulatory oversight. In adopting these measures, TRP not only enhances its own integrity but also substantively contributes to the broader mission of curtailing money laundering and illegitimate financial practices.

6. APPENDIX I: DEFINITIONS

Term	Definition
Beneficiary	Where virtual assets are being sent to. It can be a person or entity.
Decentralised	A system, organisation, or network structure where control, authority, or decision-making is not concentrated in a central authority or entity but is instead spread among multiple independent nodes or participants. There is no single entity with ultimate control.
Financial Action Task Force (FATF)	*"The Financial Action Task Force (FATF) leads global action to tackle money laundering, terrorist and proliferation financing. The FATF researches how money is laundered and terrorism is funded, promotes global standards to mitigate the risks, and assesses whether countries are taking effective action"*. (FATF:2023)
InterVASP Messaging Standard (IVMS)	*"IVMS 101.2023 Universal common language for communication of required originator and beneficiary information between virtual asset service providers."* InterVASP Standards Working Group (2023, p1).
Legal Entity Identifier (LEI)	A unique identifier specific to a business entity. Comprised of 20 alphanumeric characters, this code facilitates the global identification of businesses within a database. When using the LEI search tool provided by the Global Legal Entity Identifier Foundation (GLEIF), the following information will be displayed: • The business's name. • Its address. • Whether the business is a subsidiary of another entity. • The location where it has been registered. (GLEIF:2023)
Open Source	Computer software distributed under a licensing arrangement where the copyright holder provides users with the freedom to use, examine, modify, and share both the software itself and its underlying source code with anyone, without restrictions on purpose.

Originator	Where virtual assets are being sent from. It can be a person or entity.
Protocol	A protocol is a collection of guidelines governing the exchange of data between various entities. It essentially functions as a specification, a formal documentation. An engineer possesses the capability to transform this specification into a tangible product.
Travel Address (TA)	The Travel Address is a string of characters used to replace a wallet address in crypto transfers. It contains the following information to allow for VASP discovery: • The VASP who controls the receiving address • The VASP's URL to receive the Travel Rule data.
Transfer of Funds Regulation (TFR)	The TFR is the European Union's implementation of the Travel Rule.
Travel Rule	The Travel Rule is an important measure in anti-money laundering and countering the financing of terrorism (AML/CFT) efforts. Its purpose is to empower VASPs and financial institutions in preventing terrorists, money launderers, and criminals from utilising wire transfers to move their funds, including virtual assets. Additionally, it aids in identifying and addressing such misuse if it occurs. The primary objective of these requirements is to ensure that originator and beneficiary information is readily accessible for the following purposes: • Assisting law enforcement authorities in detecting, investigating, and prosecuting terrorists or other criminals, as well as tracing their assets. • Facilitating financial intelligence units in analysing suspicious or unusual activities.

	• Enabling ordering, intermediary, and beneficiary VASPs and financial institutions to identify and report suspicious transactions, freeze funds, and prevent transactions involving sanctioned individuals or entities. ("What Is the FATF Travel Rule?", 2022)
Travel Rule Protocol (TRP)	*"Short for Travel Rule Protocol, TRP is an open-source standard for exchanging crypto-asset transfer-related data between virtual asset service providers (VASPs) as required by the FATF Travel Rule Recommendation 16.*" (21 Analytics:2021)
Virtual Asset Service Provider (VASP)	As defined by the FATF (2021, p.109): *"A virtual asset service provider means any natural or legal person who is not covered elsewhere under the Recommendations, and as a business conducts one or more of the following activities or operations for or on behalf of another natural or legal person:* • *exchange between virtual assets and fiat currencies;* • *exchange between one or more forms of virtual assets;* • *transfer of virtual assets;* • *safekeeping and/or administration of virtual assets or instruments enabling control over virtual assets; and* • *participation in and provision of financial services related to an issuer's offer and/or sale of a virtual asset".*

7. APPENDIX II: HOW TO IMPLEMENT TRP

To implement TRP, developers must access the tools, libraries and links in section 4.2. Thereafter, follow the below prompts.

Step 1: Initiate a Request

1. Generate a Travel Address on Beneficiary. Note the crypto asset and beneficiary name.
2. Decode the Travel Address using the Travel Address Decoder/Encoder explained in section 4.2.3.
3. Use a sample request payload from: https://gitlab.com/OpenVASP/travel-rule-protocol/-/blob/master/core/specification.md#detailed-protocol-flow
4. Specify the callback https://workshop.21analytics.xyz/<some thing else>
5. Use the correct asset (4H95J0R2X).
6. Use the correct beneficiary name.
7. Use the correct LEI (of the VASP configured to have https://workshop.21analytics.xyz as an API endpoint, GTFZ00N6IHYMHHNT8S51).
8. Ensure that mandatory headers have been added.

Step 2: Capture the Beneficiary's Response

1. Login to https://testing.21analytics.xyz and approve the initiated transaction.
2. Go to https://workshop.21analytics.xyz/log.txt
3. Copy and paste the callback field.

Step 3: Finalise Response

1. Collect a random transaction ID. Then visit a block explorer or https://blockbook.21analytics.xyz/blocks

2. Make an HTTP POST request to the callback URL copied and pasted with the body as defined in the TRP specifications.

Lastly, to create a TRP server, cURL requests are to be used

To initiate:

- curl -v -H 'content-type: application/json' -H 'api-version: 3.2.0' -H 'request-identifier: foo' -d @ivms.json

'https://api.testing.21analytics.xyz/transfers/7b20efe3-e0e1-42d4-b976-1ca9d324cff1?t=i'

To finalise:

- curl -v -H 'content-type: application/json' -H 'api-version: 3.2.0' -H 'request-identifier: foo' -d '{"txid": "4a5e1e4baab89f3a32518a88c31bc87f618f76673e2cc77ab2127b7afdeda33b"}' "https://api.testing.21analytics.xyz/transfers/a18f0447-3be1-450b-a48a-5a068b7850e2/conf Irmation"

8. REFERENCES

European Commission. (2021). *Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on information accompanying transfers of funds and certain crypto-assets (recast)*. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52021PC0422

Financial Action Task Force. (2021). *Updated Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers.* https://www.fatf-gafi.org/content/dam/fatf-gafi/guidance/Updated-Guidance-VA-VASP.pdf.coredownload.inline.pdf

Financial Action Task Force. (2022). *Targeted Update on Implementation of FATF's Standards on VAs and VASPs.* https://www.fatf-gafi.org/en/publications/Fatfrecommendations/Targeted-update-virtual-assets-vasps.html

Global Legal Entity Identifier Foundation. (2023). *Introducing the Legal Entity Identifier (LEI).* https://www.gleif.org/en/about-lei/introducing-the-legal-entity-identifier-lei

interVASP Standards Working Group (17 July 2023). *interVASP Messaging Standards: Working Draft.* https://www.gdf.io/wp-content/uploads/2020/12/IVMS101.2023-Working-Draft-For-Consultation.pdf

Official Journal of the European Union. (2023). *REGULATION (EU) 2023/1113 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 31 May 2023*. https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32023R1113

Travel Rule Protocol Specification. (2023). https://gitlab.com/OpenVASP/travel-rule-protocol/-/blob/master/core/specification.md?ref_type=heads#overview

21 Analytics. (n.d). *What Is TRP?* https://www.21analytics.ch/what-is-trp/

21 Analytics. (07.09.2021). *How the TRP Travel Address Solves the FATF Travel Rule.* https://www.21analytics.ch/blog/how-the-trp-travel-address-solves-the-fatf-travel-rule/

21 Analytics. (07.06.2022). *How TRP Allows for VASPs to Accept or Reject Transfers Before They Take Place?* https://www.21analytics.ch/blog/how-trp-allows-for-vasps-to-accept-or-reject-transfers-before-they-take-place/

21 Analytics. (26.09.2022). *Is a VASP a CASP? https://www.21analytics.ch/blog/is-a-vasp-a-casp-market-in-crypto-assets/*

21 Analytics. (04.10.2022). *What Does The Revised Transfer of Funds Regulation (TFR) Entail?* https://www.21analytics.ch/blog/what-does-the-revised-transfer-of-funds-regulation-entail/

21 Analytics. (26.04.2023). *FATF Virtual Assets Contact Group (VACG): 21's Takeaways.* https://www.21analytics.ch/blog/fatf-virtual-assets-contact-group-vacg-21s-takeaways/

21 Analytics. (01.05.2023). *The Transfer of Funds Regulation (TFR) Summarised.* https://www.21analytics.ch/blog/the-transfer-of-funds-regulation-tfr-summarised/

21 Analytics. (10.05.2023). *Deficiencies in Travel Rule Solutions.* https://www.21analytics.ch/blog/deficiencies-in-travel-rule-solutions/

21 Analytics. (25.05.2023). *TRP Workshop: Implementing the Open Travel Rule Standard.* https://www.21analytics.ch/blog/trp-workshop-implementing-the-open-travel-rule-standard/

21 Analytics. (27.06.2023). *Guidelines for Choosing Travel Rule Technological Solutions.* https://www.21analytics.ch/blog/guidelines-for-choosing-travel-rule-technological-solutions/

21 Analytics. (11.10.2023). *European Union.* https://www.21analytics.ch/travel-rule-regulations/european-union-eu-travel-rule-regulation/

7.5. Risk Management Standards For Crypto Asset Service Providers

AUTHORS:

Francesco Mochi Sismondi

Marco Pagnini

RISK MANAGEMENT STANDARDS FOR CRYPTO ASSET SERVICE PROVIDERS

FOSTERING MARKET INTEGRITY AND CONSUMER PROTECTION PRINCIPLES FOR SUSTAINABLE GROWTH

25 October 2023

Authors: **Francesco Mochi Sismondi & Marco Pagnini**, co-founders of **Not Your Money**

Abstract

Since Bitcoin's birth 15 years ago, the crypto and Web3 industry have shown impressive growth and adoption through cutting edge and financial services on blockchain rails. Yet, mishappenings of various kinds have been prominent ranging from opaque projects, scams and broken promises for infinite returns ending up in smoke.

As the industry takes stock of key learnings from the latest crypto winter and prepares to build more solid foundations for the future, time is ripe to set clear market standards and rigorous practices to keep investors' concerns around toxic and murky "FOMO" projects at bay[1]. If this industry is to thrive, antagonise and to a degree replace or upgrade traditional financial rails and investment opportunities for the future then it also needs to mature and stand up to the test of institutional grade scrutiny and eliminate the toxic habits of the incumbent industry it seeks to outshine.

Vast demand potential sits in the hands of investment powerhouses, such as Investment Firms and Banks, Asset Managers and Pension Funds, all of which will be willing to step more decisively into the market only once they can see the wood from the trees and get passed the fragile "to the moon" promises and grasp the true value of crypto and Web3.

While trustless and truly decentralised infrastructure and governance remain a hopeful evolution of the industry, at present its Crypto Asset Service Providers (CASPs) and exchanges in particular have a critical role to play in the industry, sitting at the intersection between crypto projects and investors. In their role, as outright centralised entities, CASPs are critical in maintaining the highest possible standards to safeguard the crypto markets from low quality projects on one side, and protecting the interests of investors on the other.

At the time of writing, while acknowledging the potential from developments in Decentralised Finance (DeFi), our focus will primarily target centralised players of the market, given their lion share of the industry volumes. However, the recommendations put through in this paper should be considered for future evolutions of the DeFi space as well, by building out regulatory compliance, market integrity and consumer protection standards programmatically as part of its core proposition and building blocks.

This paper addresses the current areas of weakness in CASP practices and proposes areas we believe should be strengthened, specifically regarding the following 3 key areas:

a) the adoption a **clearer classification or taxonomy of tokens** enabling investors to better understand the subtleties and characteristics of each type;

b) the **due diligence process** in the listing of tokens and new projects; and

c) the **dynamic risk assessment** and **disclosure** pertaining to each category of crypto assets. This applies as much at time of sale as when market conditions deteriorate, specifically with regards to any signals that may suggest a listed crypto project may be at risk.

Financial inclusion and technological innovation at scale cannot come at the expense of investor security and protection.

There are no shortcuts around this.

[1] FOMO (Fear of Missing Out)

Introduction

The crypto market is entering its teenage years and as any youngster it is learning some tough lessons as it seeks to disintermediate and innovate the financial system on one hand and miserably come to grips with inexperience in various mishappenings on the other.

From Bitcoins' launch in 2009, the crypto asset ecosystem has seen multiple evolutions of blockchain use cases and crypto projects, including the craze of the 2017 ICO boom[2], the advent of Non Fungible Tokens (NFTs) and the birth of Decentralised Finance (DeFi).

According to Messari[3], as at August 2023 there were 22,400 crypto assets in circulation in a market worth USD 1.11 trillion, down from a peak of USD 3 trillion in 2021 (see Chart 1) [4]. While the crypto asset market is still a drop in the wider ocean of the total worldwide financial assets valued over USD 1,500 trillion in 2020[5], the short history of crypto assets has witnessed an overwhelming amount of investors' assets burned into ashes, raising widespread distrust and concerns among retail and institutional investors.

Advocating for promises of innovative technologies, democratising access to financial assets and fueled by expectations of irresistible growth, CASPs such as brokers and exchanges have often rushed to load up their platforms with any crypto asset on the market to boost transaction volumes and profits. As a result, downstream retail investors, for the large part with inadequate insights and understanding of crypto, and easily influenced and hypnotised by instant money promises of getting rich overnight, have been left drained or bankrupted from irresponsible, reckless and "black box" investing.

Chart 1 - $2 trillion wipeout from 2021 peak to 2022 post FTX

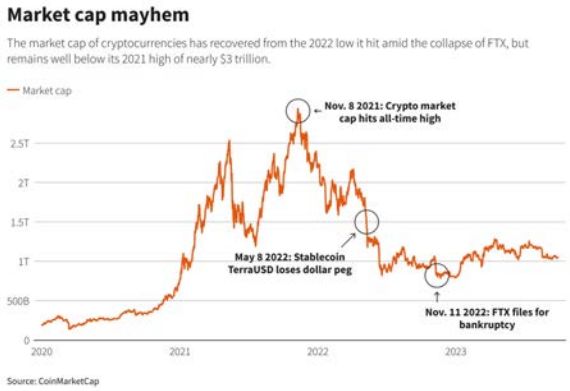


Image source: Reuters

This paper focuses on the importance of the role of CASPs and the minimum safeguards expected to be upheld to ensure a more stable market for investors, particularly as it applies to the Swiss and European landscape. Specifically, we explore existing due diligence practices and proposed enhancements that we expect central market intermediaries to embrace to ensure crypto assets marketed on their platforms are not only geared towards short term business growth, but are also optimised for longer term market integrity and consumer protection.

Crypto and Web3 market participants need to start walking the walk, earning respect and trust through greater self imposed rigour and risk management standards by injecting security and confidence in the system while eradicating the toxic behaviours from the past.

New regulatory requirements such as the Markets in Crypto Assets (MiCA) Regulation across European jurisdictions will raise the bar setting stricter expectations from crypto asset issuers to centralised intermediaries. As the crypto industry

[2] ICO (Initial Coin Offering, a mechanism of crypto and web3 firms to raise funds through crypto tokens)
[3] As per Messari.io as at Oct 10, 2023
[4] As per to Coinmarketcap.com on Aug 13, 2023
[5] McKinsey Global Institute - Nov 15, 2021 Report

regulatory regime converges towards TradFi frameworks, CASPs will need to evolve further to have a right to operate or otherwise see their licences and ability to operate revoked or rejected. We are already seeing this happen as regulators are increasingly on the lookout to identify and sanction inappropriate practices for lack of compliance with existing frameworks.

As regulations are evolving to strengthen the building blocks across the European landscape, we believe CASPs should do more than simply ticking the regulatory compliance box. For instance, CASPs should take steps to enhance investor education, assess the risks of crypto assets and clearly disclose these to investors thus allowing a more fair and transparent exchange of value with their end investors. This includes applying assessments to ensure crypto investments make sense and align to investors' individual appetite, their propensity to take risks as well as their financial capacity, financial knowledge, investment experience and objectives.

CEOs, CTOs and Product Leads should remember that this isn't just about the technology, innovative use cases, business models or fancy user interfaces. While indeed this is a technical revolution, this isn't like building any other app or technical device. Ultimately what flows through blockchain rails are investors' **money** and **savings**. Thus, security and integrity are critical.

Lets not forget that the crypto and Web3 industry would likely not exist without Bitcoin, a blockchain that has made risk, security, censorship resistance and holistically - risk management - its entire value proposition and raison d'être. Unsurprisingly, such hardness still sustains Bitcoin as the building block of the industry, now back on the rise again with over 51% of the total market cap (see Chart 2)[6].

Building a crypto industry for the future should embrace the driving principles and fundamental values of Bitcoin's hardness, building a superior financial system, anchored on mathematics, cutting edge technology and computer science *without compromising risk management on every level*.

Chart 2 - BTC dominance on the rise again

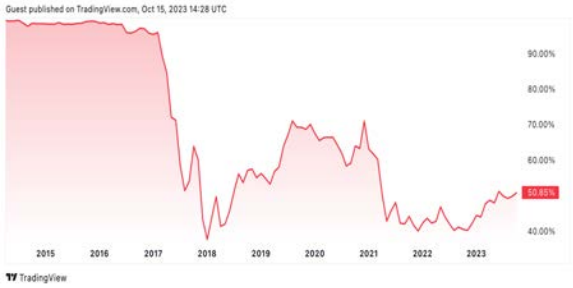


Image source: TradingView

CASPs' focus on the upholding trustworthiness of the market is existentially important and doesn't stop with proof of assets and reserves which is often assumed to be what "risk management" is all about in the crypto space. Far from it. Much more needs to be done, for instance, in scrutinising crypto assets and market participants and flagging or even sidelining those that are most suspicious. Failure to do so will, by association, tarnish their perceived standards and reputation and in turn deteriorate the market as a whole. Collectively CASPs need to work alongside each other, and in open dialogue with regulators and relevant authorities to enhance the robustness and resilience of the market for everyone's benefit.

Just like the airline industry "open sources" the black box learnings from all failures to enhance the air industry's and passenger safety, the crypto and Web3 industry needs to start demonstrating that it truly takes investment security and risk management at heart as a central component of the innovative industry being built. The industry needs a self cleansing mechanism and higher standards to identify legitimate projects from others that appear too good to be true.

As the crypto slogan goes, "**don't trust, verify**".

[6] As per Coinmarketcap.com on October 10th 2023 - https://coinmarketcap.com/

The Changing Regulatory Landscape

(legal input from Nicola Massella[7])

Pre-MiCA

Over the past decade, the crypto asset industry has been largely an unregulated playing field for entrepreneurs and investors alike. As D. Jur. Nicola Massella puts it, this far, "the issuance and listing of crypto-assets that do not qualify as financial instruments is vastly unregulated". Massella further explains that "cryptocurrencies such as BTC or ETH first, and utility tokens later, have flourished within a regulatory loophole which allowed for these instruments that provide access to a digital ecosystem where token holders can enjoy certain utilities and governance powers".

Until the arrival of MiCA regulation in Europe or even the Blockchain and DLT Act in Switzerland, the regulatory landscape was limited to ensuring anti money laundering (AML) requirements were adhered to through standard customer and business identification processes (KYC/KYB) and through the monitoring of transactions to enable the identification, monitoring and reporting of suspicious activity. Hence, all CASPs needed to worry about was to implement minimal onboarding and transaction monitoring systems and processes to "tick the box" and get going.

Massella explains how "both in the Swiss Confederation and the European Union, legislative and regulatory bodies recognised the existence of utility tokens outside of the financial instruments perimeter… As a consequence, crypto-assets not qualifying as financial instruments can be publicly sold without any authorisation requirement or public notice based on contractual agreements with the purchasers on the European continent".

With limited to no requirements on market conduct and consumer protection, the market was able to develop with great laissez-faire, leaving ample room for manipulation, illegitimate and improper practices from projects entering the market.

Post-MiCA

With the arrival of MiCA, due to come into full effect by the end of 2024, the picture changes significantly placing more stringent requirements on token issuers as well as industry venues such as CASPs responsible for marketing and distribution of such tokens to end customers.

On the token issuer side, significant emphasis will be placed on the publication of a white paper which will act similarly to a prospectus in traditional financial markets. Each project will be required to provide a significant amount of information within the white paper and keep the document updated including relevant features such as the token utilities, tokenomics, the project roadmap but also important information on the project's team itself, on their technology and relevant known risks.

Massella underlines that "the white paper serves as the cornerstone of MiCAR's efforts to ensure market transparency and consumer protection" as the regulation will oblige both token issuers and CASPs acting on their behalf to publish white papers and ensure these are fair, clear and non misleading, hence eliminating the use of jargon, unfounded claims and deceptive statements. Similar duties are established with respect to marketing communications.

These are encouraging developments that bring greater robustness and confidence to the whole industry and will ensure better informed decision making from end investors.

[7] D.Jur. Nicola Massella, Legal Partner at STORM Partners - https://storm.partners/

CASPs as market guardians

With 20,000+ crypto projects crowding the industry in less than a decade it is clear that bars to entry have been very low in attracting retail investor's assets in exchange for tokens, particularly during the 2017 ICO boom. As with most technological innovations, regulators have been slow to react and get a grip on the technology leaving ample room for projects to build their empires prioritising growth and revenue over rigorous processes, risk management and controls.

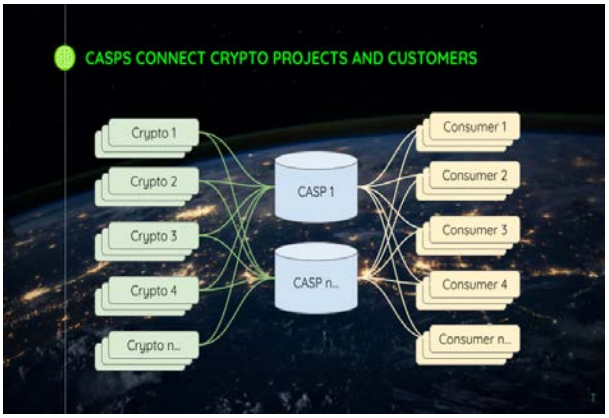
To non crypto natives, the crypto market is not easy to read. Even traditional finance professionals struggle to navigate the market, make sense of new technologies and grasp fundamentals while seeking to evaluate projects and derive their true investment potential through traditional tools.

It is largely crypto geeks and expert industry operators such as CASPs, responsible for bringing crypto projects to the market, that are able to navigate the landscape and constantly scan for new exciting projects and assess their value and listing potential (so far with questionable success). This is done by reviewing white papers, scanning websites and code audit reviews, as well as connecting with like minded industry members keeping their eyes wide open all along for projects with greatest incentives and market momentum.

MICA defines CASPs as any market player fulfilling any of the following activities[8]:

- the custody and administration of crypto assets on behalf of third parties,
- the operation of a trading platform for crypto assets,
- the exchange of crypto assets for fiat currency that is legal tender, or for other crypto assets,
- the execution of orders for crypto assets on behalf of third parties,
- the placing of crypto assets,
- the reception and transmission of orders for crypto assets on behalf of third parties,
- providing advice on crypto assets.

Chart 3 - CASPs at the heart of the market



Operating at the epicentre of the market, connecting projects and investors, it impinges upon CASPs to adopt standards and best practices to strengthen the integrity of the market and act as a filter against bad actors and shady projects. MiCA regulations clearly raise the bar in this regard.

CASPs should go over and beyond regulatory requirements and focus on educational efforts directed at investors, differentiating clearly between different crypto asset types, their risk factors, and drawing the line between legitimate projects and those that get sidelined, alongside the methodologies adopted to make that assessment.

Moreover, CASPs should also seek mechanisms to dynamically provide actionable insights to investors not only based on traditional market factors (price, liquidity, volatility, etc) but also covering qualitative factors that are important for investors to be able to make better informed, risk based, investment decisions. We explore some of these elements in more detail in the following sections alongside key areas where CASPs should lead the way in ensuring a more robust and resilient market

[8] Grant Thornton - https://www.grantthornton.ee/en/

Current Token Listing Practices

In the relatively "short" history of the crypto industry, token listing practices have differed significantly across market players and jurisdictions even more so in light of a regulatory landscape that has been somewhat passive in keeping up with the pace and providing clear standards to follow.

On one end of the spectrum, fully regulated players and exchanges, including licenced banks (such as Sygnum or Seba banks in Switzerland) have typically embraced more rigorous scrutiny of new projects compared to other CASPs that have been less constrained by regulation, policy and internal standards and more eager to focus on revenue growth above other considerations. For many players the opportunity of earning transaction fees on new trading pairs has this far significantly outweighed the desire or time to investigate the opaqueness and doubts over low quality projects. Even for some of the largest industry players servicing European customers, like Binance, Crypto.com, Huobi or Kraken, due diligence practices are unknown and risk assessments and disclosures are practically non-existent. Same goes for FTX, the poster child exchange for lack of transparency and disclosure to investors - among other things - which we describe in **Annex II.**

Below we outline a basic set of common key steps and criteria for the listing of a new token on a centralised trading venue[9]:

- Firstly, the project team submits an application to the CASP providing details about the token, its use case, technology, and compliance with any applicable regulations.
- The CASP reviews the application evaluating factors such as the token's legitimacy, market demand and other security features.
- Once approved, the token's technical integration with the exchange is initiated, involving the creation of wallets, enabling deposits and withdrawal capabilities, and activating all applicable trading pairs.
- Market makers will also be engaged to facilitate initial trading and ensure adequate liquidity.
- Pre- and post-integration testing takes place to ensure seamless functionality and security.
- Upon successful testing, the token is listed, enabling users to deposit, trade, and withdraw.
- Once listed, exchanges typically perform ongoing monitoring of crypto assets to ensure adherence to exchange minimum standards, mainly regarding their liquidity and correct functioning in the marketplace be it for changes in the underpinning blockchains such tokens transact on, managing the effects of blockchain forks, other technology upgrades and so on.

It's important to note that the CASP review and due diligence processes are proprietary processes and unique to each market player in the absence of clear rules or requirements set by regulators. Hence, while it is in the own interests of all CASPs to balance and optimise business growth and platform as well as market integrity, the primary incentives are largely tilted towards maximising the former at the expense of the latter.

The crypto ecosystem

According to insights by Coinopsy (see next table), which has analysed more than 2,400 crypto startups since 2011, 9 out of 10 projects fail within 18 months. We can hence draw a parallel between the world of crypto assets and the dynamics of traditional startups due to their inherently high risk of failure. However, a crucial distinction needs to be made between traditional startups and those we see in the crypto and Web3 industry: the liquidity and accessibility we see in crypto, allow for immediate access to these high-risk projects which is not really possible in more traditional startups.

[9] We focus here on the key steps of exchanges, given their central role and marketplace for the purchase and sale of crypto assets. Similar steps are also expected by other CASPs in the market supporting directly or indirectly the purchase and sale of crypto assets.

Traditional finance demands that companies mature and undergo rigorous scrutiny to be listed for an IPO, creating high barriers to entry. In contrast, the possibility for crypto investments opens the door to participation for all, offering opportunities for everyone to engage in the market. At least this has been the case in an environment where the listing of crypto assets to the market has been largely unregulated.

Table 1. Volume and reasons of Dead Crypto project by Year[10]

Year	Abandoned / No volume	Scams / Other issue	ICO Failed / Short lived	Joke / No purpose
2013	9	0	0	0
2014	277	20	5	2
2015	223	27	1	2
2016	152	22	4	5
2017	169	71	46	6
2018	390	237	112	12
2019	203	73	51	2
2020	77	19	9	0
2021	34	36	2	2
2022	50	23	8	2
Total	**1.584**	**528**	**238**	**33**

While centralization in traditional finance offers a better standard of due diligence, it typically caters primarily to venture capitalists, investment bankers, large funds and wealthy "qualified" individuals. Crypto, on the other hand, provides accessibility and democratises investment options to everyone regardless of their status and wallet size.

Notwithstanding the benefits that the crypto ecosystem provides to end consumers the intrinsic risks of a startup dominated industry denominated must be carefully assessed on top of the merits of the risks associated by each of its constituent projects and crypto assets. This far we haven't seen this happen leaving end investors with easy access to a wide array of investment opportunities that most likely aren't appropriate for the masses without being more carefully explained and understood.

Known Pitfalls & Opportunities for Growth

Democratising access to financial services through crypto assets is undoubtedly a breaking innovation that can open the world to financial investment in a way that wasn't conceivable a short while ago. However, this cannot happen without ensuring appropriate safety warnings and measures are put forward to educate investors and protect them from unexpected risks and inconsiderate potential for loss of capital.

CASPs such as centralised exchanges as well as crypto brokers and asset managers, face distinct challenges in their listing process:

- **Transparency Deficit** - CASPs lack clear, standardised criteria for listing tokens, leading to confusion and inconsistency. This opacity creates an environment ripe for market manipulation and investor misinformation.
- **Regulatory Ambiguity** - prior to the DLT Act and MiCA, the lack of a clear regulatory framework has resulted in uncertainties for both CASPs and token projects in navigating the regulatory maze
- **Inadequate due diligence** in the token listing process can result in listing tokens with vulnerabilities, misbehaviour, lack of transparency and misleading information, leading to misrepresentations, security breaches and financial losses for investors. Ensuring the security of listed tokens is a paramount concern for both CASPs and investors.
- Assessing **token's intrinsic risk factors** - understanding all risk factors relevant to any

[10] Source: https://www.coinopsy.com/dead-coins/

given token remains a challenge. This is not only limited to grasping quantitative risk factors such as liquidity and volatility, but other risk factors such as understanding the team, project, technology, incentives and tokenomics behind each project. A painful reminder of this issue was the crash of UST algorithmic stablecoin and TerraLuna project, as described in **Annex III**.

In terms of opportunities instead a way forward to attract more institutional investors resides in developing better discipline and control processes to gain the trust and confidence such as:

- Developing a **standardised set of criteria** for token listings can enhance transparency and fairness. Clear guidelines will create a level playing field for projects, ensuring that innovative and promising tokens have an opportunity to reach the market.
- **Enhanced Due Diligence** by implementing rigorous analytical processes that can bolster investor trust. Exchanges investing in comprehensive security audits and evaluations of token projects can mitigate risks, safeguarding both the exchange and its users.
- **Regular monitoring** and compliance checks should be maintained to ensure continued adherence to proprietary, industry and regulatory standards.
- Promote **educational initiatives** by empowering users with knowledge about token investments and market risks can enhance overall market resilience. Exchanges can play a pivotal role in educating investors, promoting responsible trading practices, and reducing the impact of market volatility.

Moreover, proactive collaboration with regulatory bodies can provide much-needed clarity. CASPs working closely with regulators can create an environment conducive to innovation while ensuring compliance with existing laws as well as designing new standards for the future, fostering a healthier market ecosystem.

We dive into these items in more detail in the following sections. Before that we will briefly explore what is brewing in the DeFI space.

Building a securer industry through DeFi

In the realm of decentralised exchanges (DEXs), the incorporation of DeFi protocols represents a promising pathway toward fortifying current token listing practices and fostering a more secure industry for crypto assets. DeFi platforms bring an array of transformative advantages, including transparency, security through smart contracts, immutable transaction records, and true decentralisation and disintermediation of traditional financial market structures.

These attributes can address a number of flaws in centralised financial activities, including the limitations we raised in traditional token listing processes, inspiring trust among participants and reducing risks of inappropriate behaviour or outright manipulation. However, plenty of challenges remain to be addressed before DeFi can truly build up and antagonise centralised market players at scale. We'll expand more into both the opportunities and some of the major challenges of the DeFi space later on in the paper.

Token Classification

The crypto landscape encompasses a diverse array of tokens, from payment tokens to DeFi tokens, stablecoins and so on. Unfortunately, these are often oversimplified and grouped together as if all tokens are simply flavours of the same macro asset class. Drawing an analogy with traditional finance, this is akin to considering equities, bonds, real estate and commodities as part of the same family of investments which is clearly far from the truth. This largely misleading perception suggests that crypto assets are merely different types of tokens and simply interchangeable into one another just like traditional currencies, such as USD, CHF or EUR. This is far from the truth and needs correcting.

While indeed crypto assets can easily be "swapped" into one another at a click of a button, each crypto asset possesses unique characteristics that require thorough comprehension starting with the very fact of understanding that for the most part, crypto assets aren't really much like what we typically perceive as *currencies* in their more traditional sense (eg. as a means of payment).

To highlight the complexity, prominent market data platforms categorise crypto assets very differently, with Coinmarketcap.com listing 210 categories, Coingecko using 119, and Messari employing 37. Establishing an industry-wide standard taxonomy is crucial for bringing clarity and structure to the market. This may take years, especially as new use cases emerge, making it imperative for CASPs and other market participants to collaborate in setting appropriate classification standards while adapting within the broader regulatory grouping of crypto assets according to their actual purpose eg. payment, utility and asset tokens.

Clarity in this space will provide the much needed transparency for all stakeholders, including entrepreneurs and end investors, who will be able to grasp a clearer understanding of the array of categories and types available, and how they differ from one another. In turn this will aid more pertinent comparisons between projects and tokens against their category "peers" (eg. stablecoins, utility tokens, payment tokens, DeFi, etc) as opposed to against the entirety of the 20,000+ crypto market.

Concretely, CASPs should consider adopting the following best practices:

CRYPTO CLASSIFICATION GUIDELINES

1. ***The broad "cryptocurrency" label should be avoided*** *and confined to payment tokens only. The term is misleading and should be replaced by crypto (or digital) assets classifications defined by FINMA, MICA and other regulators, eg. payment tokens, utility tokens, asset tokens and hybrids.*

2. ***CASPs should adopt clear crypto taxonomy -*** *in the absence of industry standard and complementing the broad regulatory definitions, all CASPs should take steps to detail crypto asset sub categories and explain how they differ from one another. Over time industry taxonomies will evolve*[11]*.*

[11] A taxonomy example - Global Crypto Classification Standard (GCCS) developed by 21 Shares and CoinGecko

Enhancing the Listing Due Diligence Process

In order to hold on to its disruptive promises and propel us into a more inclusive financial era, the crypto industry cannot afford to inherit the toxic culture often associated with the industry it seeks to outshine. While not advocates of regulation per se, there is a long history of severe market crashes, disruptions and wrongdoings in financial markets that have led to the regulations we have in traditional finance today. As crypto assets start attracting greater attention around concerns and potential impact on the stability of the wider financial system, it is no wonder regulators are making their way in. In that regard, both Swiss and European regulation and legislation are welcome developments, helping set level playing field standards on one hand while promoting industry growth on the other without stifling innovation.

CASPs should continue leading the way for financial innovation keeping market integrity and robustness as key performance indicators (KPIs) and not merely a nice to have. Technological innovation has been existentially interconnected with human evolution and prosperity but as it pertains to financial markets there is very little room for error. Immutable blockchains cannot do miracles without harnessing the way we use them.

All CASPs and market players are accountable to their customers, stakeholders and wider market in playing their role to eradicate its association to crime, scams and projects with weak foundations. Clear guardrails and boundaries must be set to avoid polluting the market with, black box, fragile, and wild west projects at every cost. In this context “less is more”. The number of projects in the industry, per se, cannot be a measure of the industry’s evolution and success. The number of sustainable, high quality projects is.

Institutional level scrutiny

As more experienced institutional investors, such as banks, asset managers and pension powerhouses are increasingly growing appetite to jump on the crypto assets train, their scrutiny of the market will follow significantly higher constraints than most crypto projects are prepared to offer. Institutions have legal and regulatory obligations to adhere to, internal policy requirements and stacks of stakeholders to keep in check, from boards to executives and advisors, shareholders and customers, not to mention the reputations they need to preserve. There will be no appetite to put their legacy at risk by gambling on promises of 100x returns. Institutions will be looking for diversification in their portfolios through reliable, scalable and serious technologies with yield potential, track records and an acceptable risk adjusted rate of return.

Starting with traditional measures, such as market cap, liquidity and track record, institutional interest will ignore anything other than what can be readily transacted at institutional sizes. With that alone we can expect almost 99% of the crypto universe to be out of scope of the investment horizon for institutional powerhouses. The few remaining palatable crypto assets will then be competing on the level of assurances they can provide not only on technological innovation but on regulatory adherence, governance, and risk management. Similar standards will be applied to CASPs and exchanges as well.

Hence we can expect the next wave of Institutional driven volume to concentrate on fewer, more reputable crypt projects able to pass their scrutiny. In turn, institutional demand will send a “flight to quality” signal which will spill over and further legitimise investor confidence and demand onto the wider retail investor universe.

Due Diligence Standards

Evidence of robust risk management, compliance, internal control and assurance systems and processes will be differentiating factors in attracting institutional assets and for CASPs to remain relevant in the next phase of the market cycle.

As such, CASPs need to take active steps to bridge the gap and meet the growing demands by investing and upgrading their internal risk management processes and control standards, injecting relevant skills, competencies and capabilities into their teams, as well as adopting risk management KPIs as part of broader incentive and reward mechanisms across the board.

CASPs' ability to provide timely and adequate services on operational elements such as trade & regulatory reporting, or on corporate governance elements access to financial statements, governance security audits and so on will become the norm. Market players that will fail to keep up with the growing demands, will be left behind.

To meet the growing rigour of the industry we believe all CASPs should impose rigorous due diligence standards covering the following 4 key areas:

DUE DILIGENCE STANDARDS

1. ***Robust Listing Due Diligence Process*** *- a comprehensive process should be in place including a set of criteria to closely examine and dissect the merits as well as the risks of each project considered. Criteria selected should cover a wide range of quantitative and qualitative elements* ***(see next page****) ahead of any projects being listed. Independent functions such as risk, legal, compliance and security experts should be incorporated into the process to balance decision bias.*

2. ***Transparency of Due Diligence Process*** *- the due diligence process including relevant features and characteristics from the review of each crypto project listed should be made available to end investors in order to provide clarity on their internal standards and ultimately help investors make better informed investment decisions.*

3. ***Ongoing Due Diligence Monitoring -*** *due diligence doesn't stop after listing. CASPs should implement monitoring mechanisms to assess how projects evolve over time and raise flags or warnings where any signals or concerns of fragility or deterioration are triggered that could jeopardise investor's interests as well as market integrity. Where deterioration of projects is identified, users should be duly informed and invited to consider taking action.*

4. ***De Listing Mechanisms -*** *CASPs should also consider mechanisms for delisting projects upon certain red flags being triggered, taking all possible steps to keep customer interests and market integrity at the forefront. In such cases investors should be provided with actionable options to sell, divest or take other relevant steps including ways to transact such assets.*

Due Diligence Criteria

As it pertains to the specific criteria to be considered for robust due diligence screening both pre-listing as well as on an ongoing basis, CASPs should ensure a number of key factors have been carefully scrutinised to acceptable levels in line with the risk appetite of each CASP. The following are a list of best practices we believe all market players should consider adopting as part of their due diligence process. A further list of "red flags" and current market practices that should be categorically avoided can be found in **Appendix I**. These criteria should be clearly documented, and reviewed by stakeholders across different business and functional lines and technical competences to balance growth incentives and biases with security and risk.

10 DUE DILIGENCE BEST PRACTICES TO ADOPT

1. ***Founders & Team*** *- who is behind the project? What is their background? Do they have adequate experience and competence on all key competences necessary (eg. tech, business, finance, as well as security, legal, risk and compliance) ? Are they contactable?*

2. ***Project Fundamentals, Funding and Traction*** *- is a documented white paper available? What is the project about? What problem are they solving? Do they have a clear strategy and funding? What traction do they have and how likely is the project to prevail?*

3. ***Technology*** *- what innovation do they bring? What blockchain(s) do they use and why? What dependencies do they have? Is it audited? What change management controls are in place? Who has access to critical systems and data? What vulnerabilities are known?*

4. ***Security*** *- what security measures are in place? Are user assets ring fenced and secured versus company assets? Who controls company and customer wallets? Have controls been independently audited? Do they have an audited Proof of Reserves? What is their uptime and what safeguards and processes are in place in case critical systems go down?*

5. ***Governance, Risk, Compliance & Ethics*** *- Who is calling the shots? Is governance in place and are independent Board members appointed? Are independent teams in place to challenge the business, provide assurance and uphold regulatory, security and compliance standards?*

6. ***Company Audits*** *- are financials audited? How about compliance, technology and security?*

7. ***Licencing and Regulatory Setup*** *- where is the company based? What licence does it hold? Is there a disconnect between the jurisdiction of licence, founders, teams and customers? How mature is the regulatory regime in the chosen legal nexus? And how does the entity setup align with the location of directors, teams and customers?*

8. ***Tokenomics*** *- how does the token work? How do the incentive mechanisms work? Are they credible and realistic? Who controls the token supply? Is the supply of tokens concentrated in a few hands only? Are any tokens locked for investment?*

9. ***Financial Engineering*** *- how liquid is the token? Where is the token listed? Who are the market makers? What significant inflows and outflows exist to / from entity wallets? Are there any significant affiliates to be noted and of concern?*

10. ***Community and Target Market*** *- who is the target community? What do they value? Any flags or toxic warnings we can infer from scanning the web or social media channels?*

Dynamic Risk Assessment & Disclosure

Trust Scores

Combining the above mentioned due diligence criteria together should support the creation and use of an overall **trust score** for each crypto asset that can be measured and monitored over time. Trust scores can go a long way in demonstrating the due diligence performed by the CASP and inform the user of how different tokens compare to one another, highlighting potential areas of weakness they should consider before investing. Trust scores should be disclosed alongside their methodology to investors who in turn will be able to use these factors to make better informed investment decisions not solely based on market price, and momentum. At present a price and a historical chart is typically all you find.

Coingecko.com, a leading market data provider, has adopted trust scores (albeit limited to exchanges as opposed to the underlying crypto assets listed) and published their methodologies to the market. Similarly, Certik has taken steps to independently audit and assess smart contracts and blockchains. These examples are promising but remain marginal and more like the exception than the rule as exchanges and CASPs continue promoting crypto assets for investment with little to no insights whatsoever on token risk factors[12].

Education and Disclosure

Crypto and Web3 are becoming synonymous with innovative interfaces enabling investment at ease with QR-like and instant “click of a button” user experience. Moreover, gamification and AI are constantly being explored to make investing even easier to savvy investors as well as to novices with close to zero financial experience let alone knowledge of blockchains, crypto and Web3.

This has a number of advantages on matters such as efficiency, access, and inclusivity, but also comes with challenges regarding the ease and rapidity with which retail investors can commit significant capital with limited to no financial and investment knowledge, and with no precautions or warning signs whatsoever. If this industry is truly about financial inclusivity, then that journey starts with understanding who the customers are and ensuring they have every right to understand what they are getting into. According to a recent paper on crypto risks published by the BIS, data shows clearly that it is the least savvy retail individuals - unsurprisingly - who have proved to be affected the worst in chasing prise rises during bull markets, and being slower than proficient investors in divesting and cutting losses during market falls[13]. Investors with least capital and knowledge to start with are those who end up with greatest losses. White this may not be unique to crypto, the safeguards and provisions you can expect from banks and brokers in TradFi are on another level.

All CASPs are ultimately centralised financial intermediaries and as such they cannot really hide from basic fiduciary responsibilities to the end consumer, particularly with respect to the average retail investor. Even more so in the early stages of this industry, until crypto assets are better understood, classified and regulated, it is essential that CASPs lead the way in educating retail investors and ensuring they have every opportunity to appreciate the nature of the risks of the products they are getting into.

Current standards are substandard, ranging from optional video or educational academies available on websites and media channels such as youtube, instagram or similar. Others offer one liner generic risk disclosures and warnings in tucked away sections in their apps and websites, and most CASPs hesitate to provide pre-investment warnings

[12] https://www.coingecko.com/en/methodology & https://www.certik.com/

[13] BIS - The crypto ecosystem: key elements and risks

and pop up features to avoid scaring customers from their next trade. Furthermore, practically all market players rely on long legalese and incomprehensible jargon in small font terms and conditions that do everything to escape responsibility of CASPs and practically nothing to help users make well informed investment decisions. None of this helps investors embrace the crypto revolution and really learn what they are getting into.

It is every CASP's fiduciary responsibility to adequately present their customers with a clear set of key facts to enable them to make sounder investment decisions. This should not be limited to market information such as price, volatility, market cap or 24hr trend (up or down) but should also cover pertinent risk factors which may differ depending on the type of crypto asset in question, such as its purpose, its' token mechanics, and other key elements and dynamics which may be affecting the token's current or future price.

The risk characteristics of stablecoin differ enough among one another (say USDT vs UST), let alone against other types of tokens such as a blockchain token (eg. Solana) a DeFi token (eg. LIDO, AAVE) and so on. Risk disclosures should be designed to provide specific insights and disclaimers to help users understand their intrinsic properties. Similarly, a token subject to an imminent fork, a change in utility, a change in tokenomics, or a token subject to low liquidity will also have different risk characteristics needing to be appreciated and considered in order to anticipate the possible ranges of impacts on their future value.

Suitability and Appropriateness

For most CASPs acting as pure market venues (i.e. no advice given) and hence largely executing unsolicited orders, current appropriateness assessments on behalf of customers are nowhere to be seen. This is simply not good enough. This is not how we democratise and open up financial inclusion to the masses. This is how we scare them and see their future propensity to invest hibernate as opposed to encouraging them to learn and have another go.

In this regard, the crypto industry should inherit queues and best practices from the financial industry (eg. MiFid) and ensure reasonable measures are taken to assess the appropriateness of any given investment with respect to investor's relevant experience, and other key factors such as their declared wealth, knowledge and experience, their profession and background, as well as volume and frequency of past investment activity. Besides, CASPs already collect varying amounts of user information from more static profiling data (typically to satisfy KYC requirements) to dynamic investment behaviour inferred through their trading history hence with minimal further "engagement" steps can be easily taken to broaden CASPs understanding of investors' key information.

With relatively simple models and digitally enabled data matching pre- and post-trade mechanisms, CASPs should be looking for opportunities to notify investors when trading activity and exposure levels may appear out of range or risk appetite and warrant a prompt for users to acknowledge and take action on, and that way earning their trust. Crafty gamification and AI can also be put at work to improve legacy traditional finance approaches towards optimising risk taking for retail customers.

For any CASPs venturing into advisory services, whether through proactive marketing and financial promotions, direct solicitation of investment ideas or through outright management of assets, then the fiduciary responsibilities become even higher, requiring further care and consideration in ensuring appropriate controls and mechanisms are put in place to assess the suitability of each trade and investment idea against any given investors' needs.

CASPs operating in this capacity should think carefully as to how to adapt and upgrade their control infrastructure or change their business models altogether to avoid prohibitive regulatory fines and sanctions. Time is up, party time is over.

Challenges and Future Outlook

An industry of tech Start-ups

Granted, due diligence takes time, can be painful and costly and it can slow down growth too. That is clear. Also, if not done comprehensively following clear regulations and standards applicable to all players, certain CASPs may attempt to cut corners and seek competitive first move advantage in listing promising new projects ahead of others. Those are risk and reward trade offs that CASPs need to carefully evaluate.

Let's face it though. Despite the standard gospel and marketing cry for *decentralisation*, 99% of crypto assets are everything but decentralised with most of their value locked into the minds of smart founders and code bases of clever engineers. With Bitcoin (and latest DeFi evolutions) to one side, all crypto projects are centrally run by people and teams, taking strategic decisions on anything from tech stacks to product designs, writing code and building infrastructure on blockchains or fancy interfaces, making tradeoffs along the way on use cases and every possible security feature you can imagine.

The crypto market, including the very largest exchanges as depicted in figure 3, are dominated by de facto tech “startups" and “scale-ups” that for all intents and purposes operate just like any other early stage tech companies searching for innovative breakthroughs, facing similar challenges in attracting funds, scaling up and making their founders and investors wealthier than they started with while having enough cash to fund their near term payroll and runways. Even as we look at the wider global crypto market and the very largest centralised players, we should remember that none of these existed a decade ago and practically all of them face the challenges described above as well as the higher demands and scrutiny of investors, regulators and the wider public. With a universe of startups leading the crypto industry, shortsightedness and lack of maturity on a spectrum of matters such as risk management, legal and compliance had to be somewhat expected. Going forward, hardcoding risk management, leadership behaviours and principles, aided by regulatory compliance, proper licensing in trusted jurisdictions, including robust and independent audits has got to be the way forward to gain wider trust and adoption from the public.

Figure 3 – Monthly Market Share of Analysed Exchanges, 2022

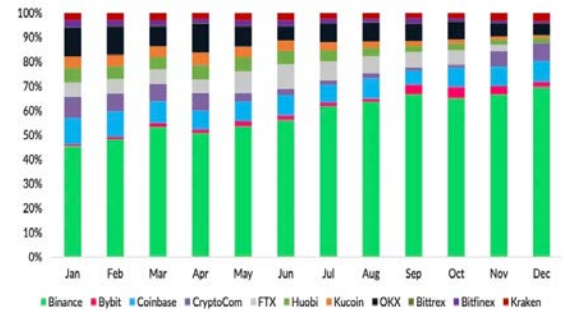


Image Source: Coindesk

On Innovation & DeFi

Despite the impact of the crypto winter and the incoming pressure of growing regulatory requirements and scrutiny, the crypto market keeps building relentlessly by strengthening technologies and opening up to further use cases which we can only expect to bring more disruptive innovation to an extent we have hardly begun to imagine.

Alongside innovation will come new types of crypto assets, and with them, new risk dimensions and characteristics which will need to be debunked, clearly articulated and disclosed along the lines of the same recommendations laid out in this paper.

We can also expect further technological advancements in DeFi, for instance enabled via Zero Knowledge (ZK) Proofs to accelerate crypto

adoption through truly decentralised trade venues capable of fully regulated and compliant protocols with embedded risk management capabilities.

It has to be recognised that even at the peak of the 2022 sell-offs in the crypto markets, all major decentralised exchanges (DEXs) platforms have continued working seamlessly allowing users to access their positions and exit them as they preferred albeit at lower prices[14]. An important DeFi takeaway from the 2002 distressed markets is that while prices might have been falling significantly, users maintained full control of their assets guaranteeing a level of consumer protection that the industry should draw inspiration from at least insofar as removing counterparty risk from the equation.

While DeFi solutions continue to show promising signs in providing for permissionless and trustless financial services, and eliminate the least efficient and manipulation prone centralised finance, they still have a long way to go in solving the possibility of bad actors programmatically gaming the system and draining consumer assets through carefully designed attacks. According to Coingecko, 91% of all the crypto markets' hacks in Q1 2022 were exploited in the DeFi space[15]. The figure below shows how DeFi security hacks have grown relative to the industry during 2021 and 2022.

Figure 4 - Crypto assets hacks by platform type

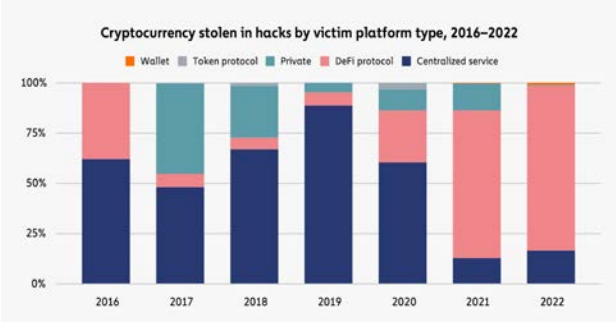


Image Source: Hacken

Moreover, DeFi user experience as well as genuine understanding of its mechanics also need to mature to gain the trust of retail and institutional investor communities. Until we get there, it is CASPs and other centralised players that will hold the keys to the industry's success.

Besides its current challenges around liquidity, cybersecurity and user experience, and in order to hold on to its promise of genuine decentralisation of traditional finance, DeFi needs to solve for the "oracle problem", due to the fact that blockchains have no secure and meaningful means to interact with external sources of data[16]. DeFi needs to find a trustless and immutable way of injecting real world regulatory, risk management and compliance certainty into its underpinning smart contracts.

Once trusted data oracles can be provided into the DeFi space, decentralised platforms will be able to leverage the programmatic nature of tokens and smart contracts to provide automatic rule-based analysis of tokenomics sustainability and financial scrutiny without needing any qualitative filters.

Though these challenges and considerations persist and remain to be solved for, the evolution of DeFi holds immense potential to propel us into a new era of confidence, trust, and robust security in the crypto and Web3 ecosystem. The genie is now out of the bottle and there is no way of ignoring it anymore or putting it back in.

[14] Cassatt (2022)
[15] 2022 Q2 Quarterly Report - Coingecko
[16] Blockpit - The Oracle Problem

Conclusion

The tech mantra of “break things and move fast” has had the upper hand in opening rounds of the crypto industry and while plates have been broken, plenty of ground has been covered. For starters, there is no longer a question as to whether crypto and blockchain technologies are here to stay. There is practically no government on the planet that hasn’t taken note and taken steps to regulate, enable or, in some cases, censor the use of crypto. Many major governments and central banks are seeking to re-engineer their existing monetary frameworks and currencies on blockchain rails.

Web 3.0 technologies, governed through cutting edge computer science, blockchain and smart contracts, have the potential - if properly used - to bring about unparalleled transparency and security to the crypto and wider financial industry. Yet, if crypto and Web3 are to pursue the vision of a more inclusive and efficient financial ecosystem for the world, then they need to innovate, disrupt and do better than the incumbent industry on every level, embedding regulation, risk management and resilience at its very core. While in the medium term we can expect these elements to be built directly onto decentralised DeFi rails, which in turn will likely attract further confidence and investment flows, it is CASPs in the near term that will have to evolve and play a greater leadership and guardianship role in taking this industry forward.

Regulations such as MiCA are already providing the much needed pillars upon which the industry can continue building with confidence. Imminent white paper and marketing disclosure requirements will no doubt provide a solid base to start for all industry players. But this is likely not to be enough.

In this paper we outlined the 3 key areas we believe to be critical for CASPs and other central actors to adopt in order to enhance the security of the market, the protection of its investor base and regain much of the eroded industry trust.
Specifically we proposed that CASPs:

- Adopt clear token classifications,
- Enhanced due diligence processes,
- Implement dynamic risk assessments and disclosures

Being digitally native by design, the crypto industry should leverage its in-built tools and capabilities to self-impose these standards without inhibiting growth. If anything, industry players should seek to redefine risk management approaches, adapting them as necessary to provide water tight security to this financial technology evolution via clever engineering, harnessing AI advances and bringing together experts from technology, traditional finance and the regulatory space as well.

The scars left from the latest crypto winter coupled with inbound institutional demand and heightened regulatory pressure, will see risk management provide for a clear differentiating factor in attracting sustainable investment flows and drive towards an industry made of fewer, higher quality projects. This might not be great news to all crypto entrepreneurs out there but will drive greater competition for the smartest ones to come on top. As ever, risk and reward are just two sides of the same coin. You cannot have one without the other.

The Swiss market remains well positioned to continue playing a leadership role in this industry, with a clear regulatory and tax framework on blockchain and crypto assets, an innovative track record seeing the first native crypto banks, becoming a hub for some of the world’s leading crypto projects, adopting Bitcoin as means of payment (eg. Lugano, Zug), and even enabling Bitcoin ATMs since 2014. Despite the crypto winter, 1000+ companies are busy innovating and building out the foundations and use cases for the future of the crypto industry on Swiss pastures.

This is promising, though market participants and crypto builders cannot afford to stay complacent and rest on their laurels.

References

BIS - The crypto ecosystem: key elements and risks (Jul 2023) - https://www.bis.org/publ/othp72.pdf

BIS - Addressing the risks in crypto: laying out the options (Jan 2023) - https://www.bis.org/publ/bisbull66.pdf

Blockpit - The Oracle Problem - https://blockpit.io/en/blog/how-to-solve-the-oracle-problem/

Cassatt - FTX Showed the Problems of Centralized Finance, and Proved the Need for DeFi (Nov 2022) - https://www.coindesk.com/layer2/2022/11/11/ftx-showed-the-problems-of-centralized-finance-and-proved-the-need-for-defi/

Chanalysis - The 2022 Geography of Cryptocurrency Report (2022) - https://go.chainalysis.com/geography-of-crypto-2022-report.html

Coingeko - 2022 Q2 Quarterly Report https://assets.coingecko.com/reports/2022-Q2-Report/CoinGecko-2022-Q2-Report.pdf?utm_source=web&utm_campaign=Q2%2B2022%2Breport&utm_medium=display&0=

Cointelegraph - An Overview of The Cryptocurrency Regulations in Switzerland - https://cointelegraph.com/learn/an-overview-of-the-cryptocurrency-regulations-in-switzerland

Cybavo - DeFi Q2 Report (2022) https://www.cybavo.com/blog/defi-q2-report/

ESMA - Crypto assets and their risks for financial stability - https://www.esma.europa.eu/sites/default/files/library/esma50-165-2251_crypto_assets_and_financial_stability.pdf

ESMA - ESMA encouraged preparations for a smooth transition to MICA - https://www.esma.europa.eu/press-news/esma-news/esma-encourages-preparations-smooth-transition-mica

ESRB - Crypto assets and decentralized finance (May 2023) - https://www.esrb.europa.eu/pub/pdf/reports/esrb.cryptoassetsanddecentralisedfinance202305~9792140acd.en.pdf?853d899dcdf41541010cd3543aa42d37

FCA - Financial Promotion Rules for Cryptoassets - https://www.fca.org.uk/publication/policy/ps23-6.pdf

FSB - Assessment of Risks to Financial Stability from Crypto Assets - https://www.fsb.org/2022/02/assessment-of-risks-to-financial-stability-from-crypto-assets/

IMF - The Crypto Ecosystem and Financial Stability Challenges (Oct 2021)

The Law Reviews - The Virtual Currency Regulation Review (Sep 2023) - https://thelawreviews.co.uk/title/the-virtual-currency-regulation-review/switzerland

Swiss Federal Council - Blockchain / DLT - https://www.sif.admin.ch/sif/en/home/finanzmarktpolitik/digitalisation-financial-sector/blockchain.html

Swiss Federal Council - Legal framework for distributed ledger technology and blockchain in Switzerland - https://www.newsd.admin.ch/newsd/message/attachments/55153.pdf

Appendix I - 10 Due Diligence “RED FLAGS” to avoid

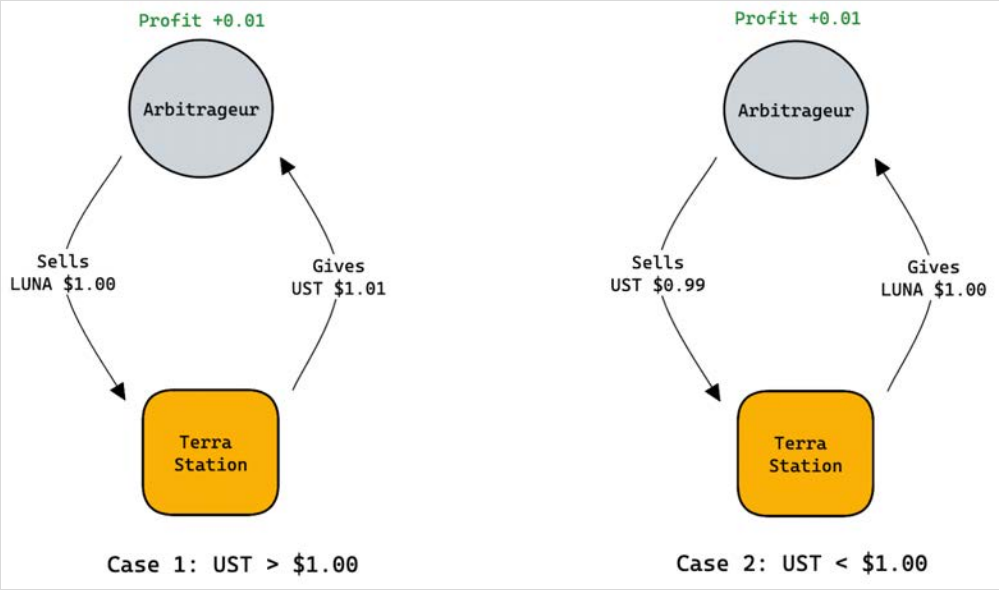
Below is a list of practices and signals to avoid or that should raise concerns to anyone involved in the listing process.

10. Red Flags that should raise concerns
1. ***“The CEO wants to list them, we must list ahead of the market...” -*** *Nothing wrong per se, still need to do the homework and scrutinise the project carefully. Prioritise safety ahead of reputation even if this might compromise early revenues. Nurture a long term culture.*
2. ***“They are the biggest thing in town…” -*** *So what? If they go down everyone else is exposed (eg. FTX). Understand what is attracting demand and question what might be missing. Bring a contrarian in the room and find arguments to consider against the case for listing the project.*
3. ***“Everybody wants XYZ…”*** *If everyone wants opium do you need a piece too? Get over “get rich soon” schemes. Demand is promising, but healthy demand is much better. Dare to be different. In the long run it pays off.*
4. ***“They are offering 20% returns…”*** *Ask yourself why? What are the tokenomics and incentives? Where does the money go to enable that? Think TerraLuna. If you can't understand it or if you can’t explain it to your neighbour, let go. There are no free lunches.*
5. ***“Company X and Y or Super Personality Z are investors…”*** *So what? What do they get in return? What links and ties are there? Are there affiliates in place?*
6. ***“Investment Fund X is behind them…”****. What are the trading flows and links between the project and other exchanges or entities? What blockchain or banking activity is known and public? Are there significant flows that raise questions? Think FTX flows Alameda Research or even FTX and Solana.*
7. ***“We need volumes and fees to come in…” -*** *Everybody does. Do your homework first. Long term customers value standards and security over short term wins. Greed and desperation can lead to reputation and brand value vaporising overnight. Tread carefully*
8. ***“Our CEO / Directors know the guy directly…” -*** *So what? Everybody knew Madoff and SBF. We know how the story went…*
9. ***“Their technology is the best…”*** *Really? For what? How? Has it been audited and battle tested? Do they have a track record? What is their uptime? What dependencies do they have?*
10. ***“Their incentives and airdrops are awesome…”*** *Really? For what? Why are they giving free money? What is behind it? Where is the catch?*

Appendix II - UST and Luna Crash

An overview of the major flaws relating to the depegging of the algorithmic UST stablecoin and collapse of the Luna token

The Terra protocol creates stablecoins designed to consistently track the price of a fiat currency. Because the primary value of stablecoins is derived from the stability of the price peg, theoretically bypassing the volatility typical of cryptocurrencies, the Terra protocol attempts to maintain the price of the Terra stablecoin by ensuring that the supply and demand for it are always balanced by employing arbitrage.
Terra's ecosystem, which included LUNA – the reserve asset backing the UST stablecoin – was unable to maintain the UST-dollar peg. UST relied on arbitrageurs to maintain its peg to the US dollar:

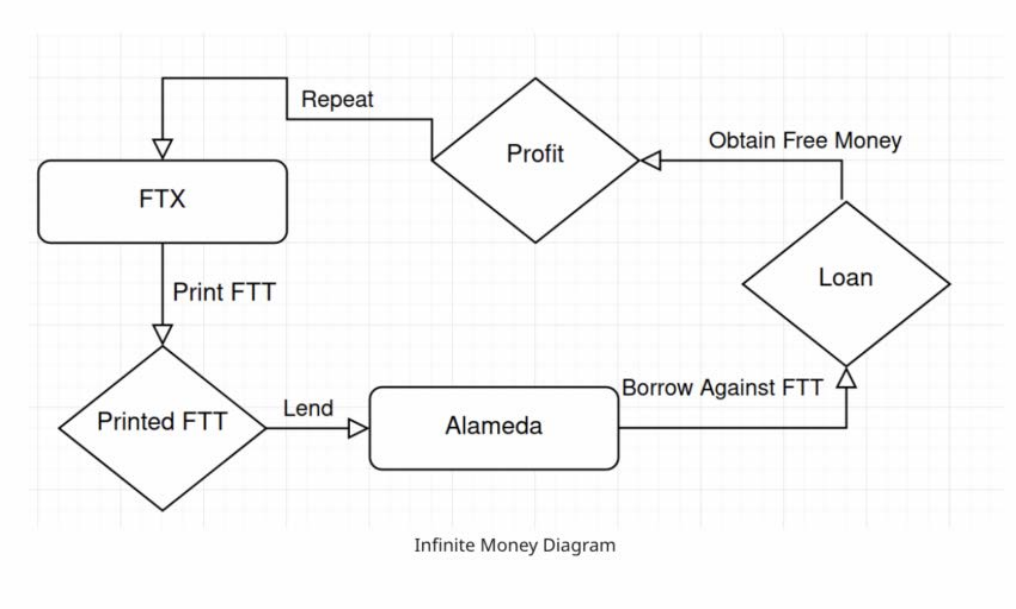


Terra, the issuer of the stablecoin UST, collapsed in May of 2022 due to spiralling losses related to its token design. The value of the UST stablecoin was pegged to the US dollar. It relied on the minting and burning of collateral token LUNA (through the central platform Terra Station) to adjust its value in the case of deviations. There was an overreliance on arbitrageurs to maintain the peg of the stablecoin UST to the US dollar.
The sharp price drop of UST depegging from its $1 peg (which arbitrageurs could not correct) induced widespread panic in the market and caused the project, originally valued at $60 billion, to lose nearly all value in a matter of days. The prices of both LUNA and UST eventually dropped by more than 99%.
Risk analysis and stress testing related to the risk of depegging and the behaviour of stakeholders such as arbitrageurs could have helped to prepare for the risk of the inevitable event.

Appendix III - The FTX Collapse

An overview of the major flaws relating to the collapse of the FTX exchange and related tokens.

FTX, a centralised exchange platform, faced a critical issue when it used customer deposits for purposes undisclosed to its users. Instead of holding secure assets or acquiring desired cryptocurrencies, FTX diverted these funds, lending them to Alameda Research, an FTX subsidiary. Alameda, in turn, used these funds to purchase FTT, FTX's less popular token.
In November 2022, CoinDesk published an article exposing FTX's improper holding of FTT tokens, amounting to approximately $5-6 billion in price (not the actual value). As a result, FTX users discovered that their funds were not being utilised as expected. Many customers withdrew their assets, but FTX could not fulfil these requests as it lacked the necessary funds. Consequently, FTX attempted to sell its FTT holdings, causing a sharp decline in FTT's market value. FTX had no choice but to declare bankruptcy on November 11.



Infinite Money Diagram

This turn of events sent shockwaves through the cryptocurrency market, causing a significant drop in FTT and FTX's prices, as well as affecting the prices of Ether and Bitcoin. The incident revealed a substantial crisis in the crypto economy, raising questions about the security and transparency of centralised exchanges.
FTX and its sister companies did not produce balance sheets showing assets and liabilities, which is standard financial reporting procedures. FTX's balance sheets were never audited because it was a private company. Without these audits, there was no record of cash flow or assets to show the company could cover liabilities or customer assets. FTX balance sheets showed assets were less than their CEO, Sam Bankman-Fried, had stated.

About the Authors

Francesco Mochi Sismondi
co-founder of Not Your Money

Francesco read Economics & Finance at the University of York and obtained a Masters in European Business before embarking on a 20+ year career managing risk, governance and internal controls in major Private & Retail Banks, Central Banks as well as a Swiss Crypto startup.
Francesco specialised in the domain of Operational Risk implementing risk frameworks, governance, internal control and transformational programs, taking on several senior roles covering European and Asian markets at Morgan Stanley and HSBC.
He also advised the Bank for International Settlements (BIS) before building out the Risk function and capabilities at SwissBorg, a Swiss-based CASP.
Francesco is passionate about sustainability, innovation and the disruptive promise of crypto and decentralised finance. He fell into the blockchain and crypto rabbit hole in 2019 and hasn't looked back.

Marco Pagnini
co-founder of Not Your Money

Marco holds a master degree in software engineering and is passionate about breaking down entry barriers to crypto markets and complex financial markets.
He recently served as a Quantitative Investment Manager at SwissBorg and Principal at SwissBorg Ventures, a crypto VC firm. Before that he spent 10+ years in finance, from credit & financial risk analysis to algorithmic Forex trading systems.
Marco has a deep knowledge of the mechanisms that regulate digital financial systems (at their core) which allowed him to build CFD based products, Market Making strategies and new crypto-based structured products.
Marco advises FinTech startups to bring forth their full potential while making the smart technological choices that are a basic component of every modern company.

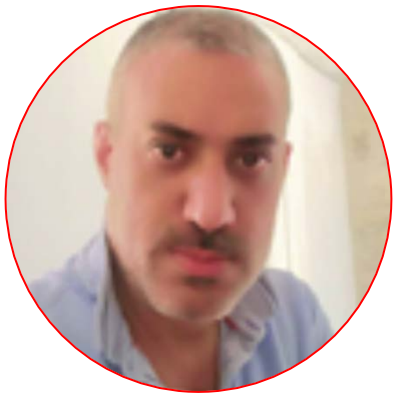
About the "Not Your Money" platform

Not Your Money is an educational and advisory platform aimed at demystifying the complexities around crypto, and making them accessible to everyone and in turn enabling investment with confidence.

www.notyourmoney.org

7.6. Automated Market Making with Synchronized Liquidity Pools

AUTHORS:



Houman Falakshahi

AllianceBlock

Matthieu Mariapragassam

AllianceBlock

Rachid Ajaja

AllianceBlock

Automated Market Making with Synchronized Liquidity Pools

HOUMAN FALAKSHAHI* MATTHIEU MARIAPRAGASSAM* RACHID AJAJA*

15th November 2021

Abstract

We propose a new approach to automated market making (AMM) by synchronizing two constant function market makers (CFMM). Our methodology combines the advantages of each individual CFMM and reduces the downside risk for liquidity providers (LP). The approach can be extended to any combination of AMMs. The application of our technique described in this paper is suitable for assets with high volatility that can deviate from the entry price for LPs. The deviation risk, compared to a buy-and-hold strategy and often referred to as impermanent loss can counterbalance the benefit of liquidity mining, that is the earning of associated trading fees. We show in this paper how our approach provides a way to largely limit the impact of such risk and compare the behavior of the new AMM to the well known exchanges, such as Uniswap and Balancer.

1 Introduction

With the recent surge of Decentralized Finance (DeFi), a variety of blockchain-powered applications aimed at creating decentralized alternatives to traditional financial services have emerged. With very large accessibility, DeFi brings benefits such as greater transparency, decentralization, enhanced security and peer-to-peer global transactions among many other advantages as discussed e.g. in [10]. The underlying mechanics rely on smart-contract technologies and equivalents. More specifically, the emergence of the Ethereum blockchain [9], which allows the encoding of arbitrary smart-contract functionalities and execution on a blockchain has been a catalyst for DeFi applications. DeFi reached impressive amounts of capital, with 100 billion USD in September 2021 up from 20 billion USD within a year, see [1]. The industry proves to be in constant expansion and provides continuous innovation.

DeFi has allowed its users to lend or borrow with services on the blockchain, see for example [24, 3], among others. A crucial DeFi application is the decentralization of asset exchanges. Until recently, exchanging digital and traditional assets was only feasible on classic systems that share an accepted and common design known as a continuous-limit order-book, see e.g. [18] for details. Such an order-book consists of a list of all bids and offers from buyers and sellers in the system, i.e. prospective buyers place a limit buy order, which specifies a maximum price at which they are willing to buy an asset. Other types of orders such as market order or stop loss are usually available depending on the Centralized Exchange (CEX). While offering a range of advantages, CEXs have also experienced problems ranging from high-profile thefts, some of which are reviewed in [8], to offenses such as price manipulation [16].

Decentralized exchanges (DEXs), improve several aspects of CEXs, for example, security vulnerabilities, centralized control of assets, custodian challenges and more as reported in [10]. There have been interesting

*AllianceBlock Foundation - Quantitative Research, Radonweg 2D, 3542 AN Utrecht, The Netherlands, houman@allianceblock.io, matthieu@allianceblock.io, rachid@allianceblock.io

The authors gratefully thank Thomas Chabert, Yassine El Kourt, Lyubomir Kiprov, Sebastien Py and Kaveh Ertefai for their insightful comments and discussions.

designs to decentralize, at least partially, the continuous limit order-book. For example, a counter-party can select an order in the order book and present it to the smart contract with a signed counter-order. The smart contract executes the order and counter-order, clearing the order from the order book. In this model traders themselves perform order matching, an approach that has been used for example by Etherdelta. Similar off-chain trade matching with on-chain settlement enforced by smart contracts has been proposed by dYdX [23] and IDex [22] among others, where the exchange itself performs the matching of orders. dYdX [23] has, for example, seen large volume increases in recent market setups. Fully decentralized exchanges have been recently built upon protocols acting as Automated Market Makers (AMM). AMMs are algorithmic agents that provide liquidity in electronic markets, a topic that has been well studied in algorithmic game theory, see [27], and for which an early work is the logarithmic market scoring rule introduced in [19].

The first fully decentralized exchanges for digital assets have been built around Constant Function Market Maker models (CFMM), see e.g. [20, 4, 26, 13]. The mechanism links two or more reserves of the different participating assets dynamically, relying on a driving constant function with specific properties. The liquidity available on the reserves and the CFMM function then jointly determine the market price of any two assets.

Liquidity providers (LPs) in DEXs can generate revenues by providing their funds as liquidity to the DEX of their choice, which will allow traders to exchange the assets of interest. In other words the liquidity provided will allow trading of the digital assets to be fully handled, in a decentralized manner, on the blockchain. Funds provided by liquidity providers are protected because the custody and exchange logic is processed and guaranteed by the smart contract directly.

Traders will generally pay a trading fee for each exchange, which is then shared among the liquidity providers and represents a direct remuneration for the funds provided. Over time, the trading fees get accumulated and LPs can see substantial return on their capital. However, as a counterpart for that reward, LPs also face a risk associated to the change of spot price value, commonly referred to as impermanent loss (IL). The term "impermanent" is employed in the field since, without withdrawal, the LP has a non-zero probability to recover this loss if the spot reverts back to its initial value. An intuitive view of the phenomenon is when the market moves heavily, a LP can recover through the DEX dynamics, more of the cheaper assets and less of the valuable assets than when he/she entered the AMM. In practice however, trading fees accumulated during that time can counterbalance the impermanent loss if the LP holds his/her position long enough in the DEX and if the market does not deviate too drastically. Because of the last point, this risk therefore remains a main concern for LPs and an area of innovation among various participants in the DEX industry. Uniswap and associated constant product two-assets CFMM [4], represent one of the most widely used DEX by volume as of today. However, it also embeds an impermanent loss profile which can strongly negatively impact the returns of the liquidity provider. In Uniswap V3 [5], the authors provide a way to optimize liquidity and therefore mitigate indirectly the risk of impermanent loss by increasing returns from trading fees in a designated range of spot chosen by the LP. However, the intrinsic properties of the underlying Uniswap CFMM being unchanged, the impermanent loss impact can worsen if the spot exits the fixed range where the liquidity was concentrated.

A detailed analysis of the Uniswap V2 market maker is provided in [8]. In [26], Balancer has generalized the Uniswap formula by introducing the geometric mean market maker CFMM. A precise analysis of geometric mean markets can be found for example in [15, 6, 7]. Geometric mean markets with asymmetric weights can improve the impermanent loss profile and therefore increase the returns of LPs on either the rise or the fall of the spot, but not both. Indeed, the IL on one side of the spot deviation stays uncovered as with Uniswap and slippage properties for traders are significantly worse on one trade direction as well. As in [5], there are also different approaches which do not directly amend the impermanent loss profile of the AMM itself. Bancor V2 [21] provides a system of insurance pools as well as a protection of impermanent loss, paid-out with their own protocol's token. It is an efficient solution in most market regimes, however, as discussed in detail in [25], this methodology presents a systemic risk under a stressed market scenario; more precisely there is an exposure to a downward spiral risk that can highly affect both liquidity providers and the protocol's token holders. Dodo [12] relies fully on external price oracles, such as ChainLink [14], to create a market maker algorithm. One of the main advantages of Dodo, similarly to Bancor V2, is to allow single sided liquidity provisioning by construction.

The impermanent loss is also improved, however, liquidity providers bear inventory risks that have similar disadvantages to impermanent loss, particularly in highly volatile market conditions. Additionally, market making with external oracles may raise issues for non-liquid assets.

Some analyses have discussed the returns and impermanent loss of liquidity providers with some possibilities to statically or dynamically hedge the IL risk. For example [15, 7] analyse LPs' returns under geometric mean markets and CFMM more generally and introduce some hedging possibilities. In this paper we propose to work directly on the intrinsic mechanism of the automated market maker with a new approach in order to reduce the impermanent loss. This new methodology has advantages in that it can be used in combination with other non-AMM specific improvements of the impermanent loss, such as the ones proposed in [21, 5] to only cite a few. Our approach, which we denominate as sync-AMM standing for Synchronized Automated Market Maker, proposes to combine the properties of two, or possibly more, CFMM and therefore obtain improved joint-properties. The synchronization process allows to align the spot prices of the CFMMs at play for each new trade. While we discuss a duo of geometric mean markets in the current work, it is possible to work with a combination of other types of CFMM such as the one proposed in [13]. Numerical results show that even under highly volatile scenarios, the LPs returns are significantly improved compared with other CFMMs. In the market setup tested and over the paths analyzed, the liquidity providers simulated in our test case, were able to obtain positive returns from trading fees compared to a buy-and-hold strategy with spot deviations rising and falling by a factor of 150.

We note that, this work provided the theoretical and computational background for the decentralized exchange at the AllianceBlock Foundation named AllianceDEX.

The remainder of this paper is organized as follows. In Section 2, we define the automated market market models of interest as well as discuss the definition of standard nomenclature of the field. Additionally, we derive and provide a detailed analysis of the impermanent loss and slippage in geometric mean markets. Secondly, in Section 3, we discuss the main contribution of the paper and a new approach to AMM which provides a considerably improved impermanent loss profile. Additionally, Section 4 provides details on the simulation framework used for the testing of the sync-AMM as well as showcase its impermanent loss profile under different market scenarios. Finally, Section 5 concludes with a brief summary of the contributions.

1.1 Disclaimer

The results discussed by the authors in this article do not constitute, in any form, an investment advice in the associated AllianceBlock decentralized exchange or any other mentioned decentralized exchange. The authors and AllianceBlock are not responsible for any loss incurred as a result of the use of the AllianceBlock decentralized exchange or any information discussed and reported in this paper. This article is meant to provide informational research and does not aim to detail the risks involved in trading or liquidity providing associated with the automated market maker models of interest.

2 Definitions

2.1 Framework definition

We consider a set of n-assets denoted $(\alpha_i)_{i\leq n}$ and we additionally define $\beta = \alpha_n$ for writing convenience. The spot $\left(S^i_{t\geq 0}\right)_{i\leq n}$ associated with the asset pair α_i, β denotes the amount of units of β needed to buy one unit of α_i at time t. Naturally, this would imply that $S^n_t \equiv 1$ by construction at any time. In the remainder of the paper, when no additional information is provided, we assume that the numéraire of choice will be the asset β, that is all quantities will be denominated in amounts of β. Moreover, when referring to the pair α, β without specific indices, it signifies that we are working under the two-assets case where $\alpha \equiv \alpha_1$ and $\beta \equiv \alpha_2$.We assume the existence of a filtered probability space $\left(\Omega, \mathcal{F}, \{\mathcal{F}_t\}_{t\geq 0}, \mathbb{P}\right)$ with a real-world measure associated $\mathbb{P}$. The

spot S, as well as all subsequent stochastic processes defined, are assumed adapted to the filtration $\mathcal{F}$.

In the AMM framework, and the now well established constant market maker function, it is common practice to have reserves amounts appear explicitly in the formulation and definition of the CFMM function, which as discussed in extensive details in [6] allows to link a valid trade to the reserves time evolution. While the scope of CFMM covers a large set of possible automated market maker, in this paper we will focus primarily on Uniswap V2 [4] and Balancer V1 [26], that are examples of constant product market makers. Let us denote pool reserve sizes as $\left(R^i_{t\geq 0}\right)_{i\leq n}$, a positive quantity that represents the reserve amounts of asset α_i. Where no super-script is specified, the process $\boldsymbol{R}_t$ is a n-dimensional representation of each reserve with R^i_t as element.

A trade will give rise to a constant proportion of fee denoted $(1-\gamma)$, where $0<\gamma\leq 1$ and with $\gamma=1$ for the case where no trading fees are considered. This means that any amount a trader is willing to sell will be scaled by γ to compute the actual input amount of the trade, which will naturally provide a lower output amount. The reserves are however updated with the total input amounts such that liquidity providers are rewarded for providing liquidity to the DEX.

Following the definition in [6], we let a trade be a tuple of vector values, $(\boldsymbol{\Lambda},\boldsymbol{\Delta})$ where $\boldsymbol{\Lambda}$, a n-dimensional real valued vector is the output amounts resulting from the AMM following a valid trade and $\boldsymbol{\Delta}$, also a n-dimensional real valued vector is the input amounts for a given trade. Each element of the vector, that is $\left(\Lambda^i,\Delta^i\right)$ are the output and input amounts respectively of asset α_i for a specific trade. Let us write the following definition,

Definition 1. An automated market maker is a constant function market maker if and only if there exists a continuous, once differentiable with continuous derivatives function with respect to all variables, $\phi:\left(\mathbb{R}^+\right)^n\times\left(\mathbb{R}^+\right)^n\times\left(\mathbb{R}^+\right)^n\to\mathbb{R}$, such that for any given valid trade $(\boldsymbol{\Lambda},\boldsymbol{\Delta})$ at a positive time t,

$$\phi(\boldsymbol{R}_t,\boldsymbol{\Lambda},\boldsymbol{\Delta})=\phi(\boldsymbol{R}_t,\boldsymbol{0},\boldsymbol{0})\,, \tag{2.1}$$

and where each underlying asset is active, namely that, for all $i\in[\![1,n]\!]$,

$$\partial_{R^i}\psi(\boldsymbol{R}_t)\neq 0\,, \tag{2.2}$$

where $\psi(\boldsymbol{R}_t)=\phi(\boldsymbol{R}_t,\boldsymbol{0},\boldsymbol{0})$ and $\partial_{R^i}\psi$ denotes the partial derivative of ψ with respect to the $i-$th element of $\boldsymbol{R}_t$.

If the trade is executed, the above formula should be understood with reserves immediately prior to the jump associated to the trade, that is $\boldsymbol{R}_{t-}$ since the value of the reserves is updated at trade time.

As described in [6], this function is not necessarily unique for a given AMM, for example a constant scaling of the constant product of Uniswap would still behave in a similar fashion resulting in an equivalent CFMM. While continuity and differentiability is not a necessary assumption, we will assume this to be verified in the remainder of the paper. A classic example is the Balancer [26] n-assets expression which accounts for Uniswap as a limit case with,

$$\phi(\boldsymbol{R}_t,\boldsymbol{\Lambda},\boldsymbol{\Delta})=\prod_{i=1}^{n}\left(R^i_t+\gamma\Delta^i-\Lambda^i\right)^{w_i}, \tag{2.3}$$

where $w_i\in\,]0,1[$ and $\sum_{i=1}^n w_i=1$ and where Uniswap is the duo of assets case with weights of 0.5.

Remark. In the remainder of the article, when not specified, 'Uniswap' will refer to the Uniswap V2 DEX [4], while 'Balancer' will refer to the Balancer V1 DEX [26].

2.2 Dynamical properties

Quantities defined in the previous section such as pool reserves, are jump processes and their value will change at trade or liquidity addition/withdrawal times. Therefore, we define two random time sets; the set of liquidity addition and withdrawal times $\Theta=\{\theta_1,\theta_2,...\}$ with $(\theta_i)_{i\geq 1}\in\mathbb{R}^+\cup\{\infty\}$, and the set of trading times

$\mathcal{T} = \{\tau_1, \tau_2, ...\}$, with $(\tau_i)_{i\geq 1} \in \mathbb{R}^+ \cup \{\infty\}$. This also allows to define the processes $(\boldsymbol{\Lambda}_t)_{t\geq 0}$ and $(\boldsymbol{\Delta}_t)_{t\geq 0}$ that are zero except on trade times $t \in \mathcal{T}$ where they are linked together by (2.1). We note that a market participant performing a trade at time t can choose to either provide the input amounts $\boldsymbol{\Delta}_t$ which are asset quantities to be sold, or output amounts $\boldsymbol{\Lambda}_t$ that are asset quantities to be received. Any combination is theoretically possible for each element, namely Λ_t^i and Δ_t^i. However, a rational trader is unlikely to have both Λ_t^i and Δ_t^i to be jointly non-zero [6].

The evolution of the pool reserves can be summarized by jump processes, namely, for any $t \in \mathcal{T}$,

$$\boldsymbol{R}_t = \boldsymbol{R}_{t-} + \boldsymbol{\Delta}_t - \boldsymbol{\Lambda}_t \,. \tag{2.4}$$

And for any $t \in \Theta$,

$$\boldsymbol{R}_t = \boldsymbol{R}_{t-} + \boldsymbol{L}_t \,,$$

where $\boldsymbol{L}_t$ is the liquidity addition or withdrawal at time $t \in \Theta$ which is precisely zero for any $t \notin \Theta$.

We note that the paths discussed in this paper are all right-continuous with left limit. More details about path properties of jump processes can be found in [11].

Remark 2. In the remainder of the paper we will indistinguishably use Δ_t^i and Λ_t^i as processes, and Δ^i, Λ^i without specific time index as arguments of a function of the trade sizes. Therefore, a quantity y_t which holds a direct relationship to trade sizes can be understood as the value y_t for the trade at time t, or as the function $y_t(\boldsymbol{\Delta}, \boldsymbol{\Lambda})$ which still depends on reserve sizes but can have varying trade sizes. Additionally, we note that $\boldsymbol{\Delta}_t$ and $\boldsymbol{\Lambda}_t$ can effectively be defined as trades sizes on the timeline since all events are assumed to happen sequentially; where two traders cannot trade at the same time.

2.3 Reported, marginal and effective spot price

The spot value bears a primary importance in the definition of a market. In the foreign exchange (FX) market, the spot is defined as the ratio of notional values involved in a FX cash exchange operation; that is an order to trade an amount of N^{ccy1} for an amount of N^{ccy2} specifies the spot value as $N^{\text{ccy2}}/N^{\text{ccy1}}$. The spot value of the Uniswap V2 decentralized exchange [8] follows a similar definition. Indeed, the spot is defined as the ratio of the reserves at any given time. However, for other CFMM the spot is not necessarily intuitive and is linked to the trading function ϕ. Let us provide hereafter a few definitions that will be useful for the remainder of this paper.

The reported spot $\left(S_t^i\right)_{i\in[\![1,n]\!]}$ is defined as the price of the AMM at time $t \geq 0$. Following [6, 7] and with Definition 1 in Section 2.1 $\psi(\boldsymbol{R}_t) = \phi(\boldsymbol{R}_t, \boldsymbol{0}, \boldsymbol{0})$, the reported price S_t^i is defined as,

$$S_t^i = \frac{\partial_{R^i}\psi(\boldsymbol{R}_t)}{\partial_{R^n}\psi(\boldsymbol{R}_t)}, \tag{2.5}$$

since the chosen numéraire is β, that is the asset associated to the reserve R^n.

Additionally, we can also write the reported spot from asset i to asset j as,

$$S_t^{i,j} = \frac{S_t^i}{S_t^j} = \frac{\partial_{R^i}\psi(\boldsymbol{R}_t)}{\partial_{R^j}\psi(\boldsymbol{R}_t)} \,.$$

Because ϕ has been assumed differentiable in all variables, the above spots are unique [6]. As an example, the reported spot for Balancer using

$$\psi_{\text{Bal}}(\boldsymbol{R}_t) = \prod_{i=1}^{n} \left(R_t^i\right)^{w_i} \,, \tag{2.6}$$

leads to the ratio of the weights and pool sizes,

$$S_t^i = \frac{w_i R_t^n}{w_n R_t^i}\,. \tag{2.7}$$

For Uniswap, as $\psi_{\text{Uni}}(\boldsymbol{R}_t) = \sqrt{R_t^1}\sqrt{R_t^2}$, the reported spot is simply the ratio of the pool sizes which is similar to a FX cash trade as expected.

The marginal price $\left(\hat{S}_t^i\right)_{i\in[\![1,n]\!]}$ is defined as the spot price for an infinitesimal trade size where we have $\hat{S}_t^i = \gamma S_t^i$ from [7]. Hence, the reported and marginal prices differ only by the scaling attributed to trading fees.

Finally, the effective spot $\left(\bar{S}_t^i\right)_{i\in[\![1,n]\!]}$ is the price of a trade of arbitrary size, which generally accounts for slippage, see sub-section 2.6 . The latter would depend on the trade size and theoretically should be written as $\bar{S}_t^i(\boldsymbol{\Lambda}, \boldsymbol{\Delta})$ as per Remark 2, which we will omit for ease of notation. For a trade where all input amounts are zero except for asset α_i, we can define for any $i \in [\![1, n]\!]$,

$$\bar{S}_t^i(\boldsymbol{\Lambda}, \boldsymbol{\Delta}) = \frac{\sum_{j=1}^n \Lambda^j S_t^j}{\Delta^i}\,. \tag{2.8}$$

2.4 Liquidity providers

A CFMM, and more generally, an automated market maker relies on liquidity providers to give traders the ability to exchange assets. Each liquidity provider owns a share of the total reserve upon entry in the DEX. This share will fluctuate generally when other liquidity providers join or exit the liquidity pools. Liquidity events follow the below assumption,

Assumption 3. *Adding or withdrawing liquidity does not change the reported spot of the AMM or impact the liquidity holdings of other liquidity providers.*

For a particular LP m we denote his/her share by $\left(\boldsymbol{X}_{t\geq 0}^m\right)_{m\leq U_t}$ where $U_t \in \mathbb{N}^*$ is the total number of liquidity providers in the liquidity pool at time t. We note that U_t is increasing, such that a liquidity provider who exits the AMM, will get a share of zero but still be accounted for in the numbering. Additionally, we can define the holdings of the liquidity provider $\boldsymbol{r}_t^m$ for which the $i-$th element is denoted $r_t^{i,m}$ and represents the amount of asset α_i which belongs to the m-th LP, and where, with $\odot$ the element-wise product,

$$\boldsymbol{r}_t^m = \boldsymbol{X}_t^m \odot \boldsymbol{R}_t^m\,.$$

In the case where the share $\boldsymbol{X}_t^m$ does not depend on a specific asset, we will simply denote it as X_t^m, which is the case for geometric mean markets such as Uniswap or Balancer. Indeed, when entering the DEX at time t_0 with a quantity $r_{t_0}^j$ of asset α_j, a liquidity provider gets a share for the corresponding pool,

$$X_{t_0}^{j,m} = \frac{r_{t_0}^{j,m}}{R_{t_0}^j}\,. \tag{2.9}$$

For Uniswap and Balancer, given Assumption 3, to keep every spot constant around liquidity events, one needs the above share $X^{j,m}$ to be the same for any $j \in [\![1, n]\!]$. However we note that this does not represent a generic property of AMMs.

Additionally, to ease notations and when the reserves of only one liquidity provider are involved, we will drop the superscript such that for a liquidity provider m we will directly write $\boldsymbol{r}_t \equiv \boldsymbol{r}_t^m$ where $\boldsymbol{r}$ is implicitly assumed to be associated to the LP m of interest. We also define $(\boldsymbol{L}_t)_{t\geq 0}$, the process of liquidity addition or removal where each component, L_t^i, represents the liquidity change in the corresponding pool of asset α_i.

2.4.1 Liquidity addition in geometric mean CFMM

In this section the aim is to discuss the fact that, with geometric mean CFMM, one can work with each liquidity provider's holdings rather than the DEX reserves and ignore liquidity events. That simplifies the calculation of the IL in the following sections. For geometric mean CFMM and Balancer, the Assumption 3 implies for any $t \in \Theta$ and $i \in [\![1, n]\!]$,

$$S_t^i = S_{t-}^i \,, \tag{2.10}$$

which combined with (2.7) provides,

$$\frac{\left(R_{t-}^n + L_t^n\right)}{R_{t-}^n} = \frac{\left(R_{t-}^i + L_t^i\right)}{R_{t-}^i}.$$

From the above equation and with an addition/withdraw ratio $\lambda = \frac{L_{t-}^n}{R_{t-}^n}$ chosen on one of the assets, for instance α_n, one can get

$$\boldsymbol{R}_t = \boldsymbol{R}_{t-}(1+\lambda)\,. \tag{2.11}$$

Given liquidity movements are always proportional to reserve sizes for Uniswap and Balancer, the LP share is independent of the assets for any $t \geq 0$. Therefore, with $\boldsymbol{r}_t$ being the holdings of the considered LP m, we can write,

$$\boldsymbol{r}_t = X_t^m \boldsymbol{R}_t\,. \tag{2.12}$$

The share of each liquidity provider remains constant between two consecutive liquidity events. On each new event $\theta \in \Theta$, when another LP j adds or withdraws liquidity in proportion λ, reserves are updated following (2.11). Therefore, the share of the considered LP $m \neq j$ jumps according to,

$$X_\theta^m = \frac{X_{\theta-}^m}{1+\lambda}\,. \tag{2.13}$$

Using the above equations and the geometric mean markets condition $\sum_{i=1}^n w_i = 1$, we get the following useful property, for any time $t > 0$,

$$\psi_{\text{Bal}}(\boldsymbol{r}_t) = X_t^m \psi_{\text{Bal}}(\boldsymbol{R}_t)\,, \tag{2.14}$$

By combining (2.11), (2.12) and (2.13), we find that around liquidity events, the holdings of LPs remain constant which is in line with Assumption 3. Therefore,

$$\psi_{\text{Bal}}(\boldsymbol{r}_\theta) = \psi_{\text{Bal}}(\boldsymbol{r}_{\theta-})\,. \tag{2.15}$$

Additionally, when no transaction fee is involved, for any time t between any two consecutive liquidity events, (θ_k, θ_{k+1}),

$$\psi_{\text{Bal}}(\boldsymbol{R}_t) = \psi_{\text{Bal}}(\boldsymbol{R}_{\theta_k})\,,$$

from which one gets,

$$\psi_{\text{Bal}}(\boldsymbol{r}_t) = \psi_{\text{Bal}}(\boldsymbol{r}_{\theta_k}) = \psi_{\text{Bal}}(\boldsymbol{r}_{t_0})\,, \tag{2.16}$$

where t_0 is the entry-time of the m-th LP. Equation (2.16) shows that each LP's holdings follow the CFMM equation.

2.5 Impermanent loss for geometric mean markets

As discussed, liquidity providers will earn trading fees by providing their assets to the DEX. These will then be used as reserves for trading. This means that LPs make a choice to switch from a static buy-and-hold portfolio, where the amount of assets stays constant over time, to a dynamic portfolio where their assets will fluctuate according to the AMM dynamic and market movements. It is natural to compare the evolution of

LPs holdings when they enter a DEX versus a buy-and-hold portfolio. In the crypto-currency field, this is commonly known as the impermanent loss. In this section, we show that as the name suggests, without any trading fees, providing liquidity to a CFMM DEX such as Uniswap or Balancer will always result in holdings being worth less than under a buy-and-hold strategy. We will look at the details of the expression of the IL for geometric mean markets with and without trading fees. Since Balancer is a generalization of the two-asset constant product CFMM, this will allow to conclude about Uniswap as well. We remind that the reported spot $\left(S^i_{t\geq 0}\right)_{i\leq n}$ associated with the asset pair (α_i, β) denotes the amount of units of β needed to buy one unit of α_i at time t and where the numéraire of choice will be the asset β. Let us suppose that a liquidity provider entered the DEX at time t_0. We drop all liquidity provider's specific superscript in that section for ease of notation. The holdings of the LP at time $t \geq t_0$ are worth under numéraire β,

$$P_t = \sum_{i=1}^{n} r^i_t S^i_t \,. \tag{2.17}$$

The same assets, if not invested in a DEX but kept in a static portfolio would be worth,

$$P^{\mathrm{S}}_t = \sum_{i=1}^{n} r^i_{t_0} S^i_t \,. \tag{2.18}$$

The impermanent loss at time t, $(\mathrm{IL}_t)_{t\geq 0}$ is the relative difference of the portfolio of the liquidity provider with respect to his/her holdings under a buy-and-hold strategy,

$$\mathrm{IL}_t = \frac{P_t - P^{\mathrm{S}}_t}{P^{\mathrm{S}}_t} \,. \tag{2.19}$$

Balancer's constant product function $\psi_{\mathrm{Bal}}(\boldsymbol{R}_t)$ is defined in (2.6). To ignore the jump processes of the reserves or the LP shares X, we use the individual liquidity provider holdings $\boldsymbol{r}_t$, see (2.16). By doing so, the expression of the reported spots depends only on the holdings of individual liquidity providers,

$$S^i_t = \frac{w_i r^n_t}{w_n r^i_t} \,. \tag{2.20}$$

In the next sections we calculate the impermanent loss for each LP without and with trading fees.

2.5.1 Impermanent loss without trading fees

Proposition 4. *The impermanent loss for a liquidity provider entering at time t_0, in a geometric mean CFMM without trading fees, is given by, for any $t \geq t_0$,*

$$IL_t = \frac{\prod_{i=1}^{n} \left(z^i_t\right)^{w_i}}{\sum_{i=1}^{n} w_i z^i_t} - 1 \,, \tag{2.21}$$

with for any $i \in [\![1, n]\!]$,

$$z^i_t = S^i_t / S^i_{t_0} \,, \tag{2.22}$$

and $IL_t \leq 0$.

Proof. Without loss of generality, we set $t_0 = 0$. Our goal is to compute (2.19) with (2.17) and (2.18). We remind here that by definition we have $S^n_t = 1$. Using the expression of the spot S^i_t from (2.20), we can write

$$P_t = \sum_{i=1}^{n-1} r^i_t \frac{w_i r^n_t}{w_n r^i_t} + r^n_t = \frac{r^n_t}{w_n} \,. \tag{2.23}$$

Similarly, P_t^S can be rewritten as,

$$P_t^{\mathrm{S}} = \sum_{i=1}^{n} r_0^i S_t^i = \sum_{i=1}^{n} r_0^i S_0^i \left(\frac{S_t^i}{S_0^i} \right).$$

By using $r_0^i S_0^i = \frac{w_i r_0^n}{w_n}$ from (2.20) and (2.22) we can rewrite P_t^S as,

$$P_t^{\mathrm{S}} = \sum_{i=1}^{n} r_0^i S_0^i z_t^i = \sum_{i=1}^{n} \frac{w_i r_0^n}{w_n} z_t^i = P_0 \sum_{i=1}^{n} w_i z_t^i \,. \tag{2.24}$$

That gives,

$$\mathrm{IL}_t = \frac{r_t^n / r_0^n}{\sum_{i=1}^{n} w_i z_t^i} - 1 \,. \tag{2.25}$$

By using (2.20), we can rewrite (2.6),

$$\psi_{\mathrm{Bal}}(\boldsymbol{r}_t) = \prod_{i=1}^{n} \left(r_t^i\right)^{w_i} = \prod_{i=1}^{n} \left(\frac{w_i r_t^n}{w_n S_t^i} \right)^{w_i} = r_t^n \prod_{i=1}^{n} \left(\frac{w_i}{w_n S_t^i} \right)^{w_i}. \tag{2.26}$$

Without taking into account trading fees, equation (2.16) holds. Hence, combining (2.16) with the above expression we have,

$$\frac{r_t^n}{r_0^n} = \prod_{i=1}^{n} \left(\frac{S_t^i}{S_0^i} \right)^{w_i} = \prod_{i=1}^{n} \left(z_t^i\right)^{w_i}. \tag{2.27}$$

We conclude the proof by replacing (2.27) into (2.25). Furthermore, according to the Jensen's inequality and since the logarithm is a concave function, we have,

$$\ln \prod_{i=1}^{n} \left(z_t^i\right)^{w_i} = \sum_{i=1}^{n} w_i \ln\left(z_t^i\right) \leq \ln\left(\sum_{i=1}^{n} w_i z_t^i \right),$$

which shows that the impermanent loss in (2.21) is always negative. □

For Uniswap, $n = 2$, we can define $z_t \equiv z_t^1$ and by definition, the second asset being β, we have $z_t^2 \equiv 1$. Therefore, the expression of the IL becomes,

$$\mathrm{IL}^{\mathrm{Uni}}(z_t) = \frac{2\sqrt{z_t}}{z_t + 1} - 1 \,, \tag{2.28}$$

It is interesting to notice that,

$$\mathrm{IL}^{\mathrm{Uni}}(z) = \mathrm{IL}^{\mathrm{Uni}}(1/z) \,,$$

which means that under Uniswap by ignoring the trading fee, for a liquidity provider that enters the pool, the risk of loss against a buy-and-hold portfolio will be similar if the spot increases or decreases by a factor η or $1/\eta$, respectively. This symmetry suggests to plot the impermanent loss curves on a logarithmic scale.

For Balancer with two assets, we additionally introduce $w \equiv w_1$ and therefore $w_2 = 1 - w$. In this case the expression of the IL becomes,

$$\mathrm{IL}^{\text{Bal-2}}(z_t) = \frac{z_t^w}{w z_t + 1 - w} - 1 \,. \tag{2.29}$$

Contrary to Uniswap where we have perfect symmetry for high and low spot returns, Balancer shows asymmetry. For $w < 0.5$ one has smaller IL for any return $z < 1$ compared to high spot regimes $z > 1$. Symmetric conclusions hold for $w > 0.5$. Therefore Balancer provides an effective solution for improving the impermanent

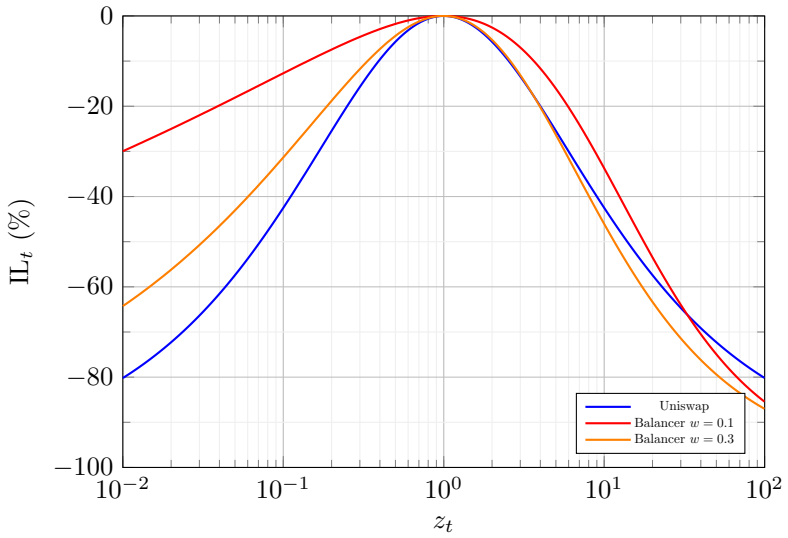


Figure 2.1: Impermanent loss under Uniswap, Balancer $w = 0.1$ and Balancer $w = 0.3$ as a function of z_t on a log-scale. The Balancer IL is improved on the downside spot movements when the weight is decreased.

loss on one direction of spot movement. However, if the spot deviates to the opposite side, Balancer is close to Uniswap in terms of impermanent loss. We will also see in sub-section 2.6 that Balancer with weights diverging from 0.5 does not offer good slippage properties on one trading direction.

In Figure 2.2 and 2.1 one can see the asymmetric improvement of Balancer's impermanent loss depending on the weights. For instance with $w = 0.1$, on Figure 2.2, if the spot drops by 90% compared to the entry level of the LP, Balancer offers an improvement of IL, namely from -42.5% under Uniswap to -12.7%. However, on the flip side when spot increases by a factor of 10, the improvement is smaller; from -42.5% under Uniswap to -33.7% only. For the same weight, one can also notice that the Balancer IL becomes worse than Uniswap when the spot increases by a factor greater than 30.

2.5.2 Impermanent loss with trading fees

As seen in sub-section 2.5, providing liquidity without earning trading fees will lead to a loss due to the unfavorable balance of assets as soon as the spot deviates from the entry level. Trading fees are a very efficient way of cancelling this potential loss and more importantly allowing to earn returns when sufficient trading volumes accumulate over time.

In the following we assume that, if trades on different assets are executed at the same time, we decompose these as sequential trades each involving one asset for another. That is for any trade, if $\Delta_t^i > 0$ and $\Lambda_t^j > 0$, then for any $k \neq i$, $\Delta_t^k = 0$ and for any $m \neq j$, $\Lambda_t^m = 0$. We introduce for every $\tau \in \mathcal{T}$, the input asset index $(k_\tau)_{\tau\in\mathcal{T}} \in [\![1, n]\!]$ which is defined by the trader's decision to exchange asset α_{k_τ} for another asset $(\alpha_i)_{i\leq n, i\neq k_\tau}$.

Proposition 5. *The impermanent loss for a liquidity provider entering at time t_0, in a geometric mean CFMM, with trading fees for any $t \geq t_0$, is given by,*

$$IL_t = \rho_t \frac{\prod_{i=1}^n \left(z_t^i\right)^{w_i}}{\sum_{i=1}^n w_i z_t^i} - 1\,, \tag{2.30}$$

with for any $i \in [\![1, n]\!]$,

$$z_t^i = S_t^i / S_{t_0}^i\,, \tag{2.31}$$

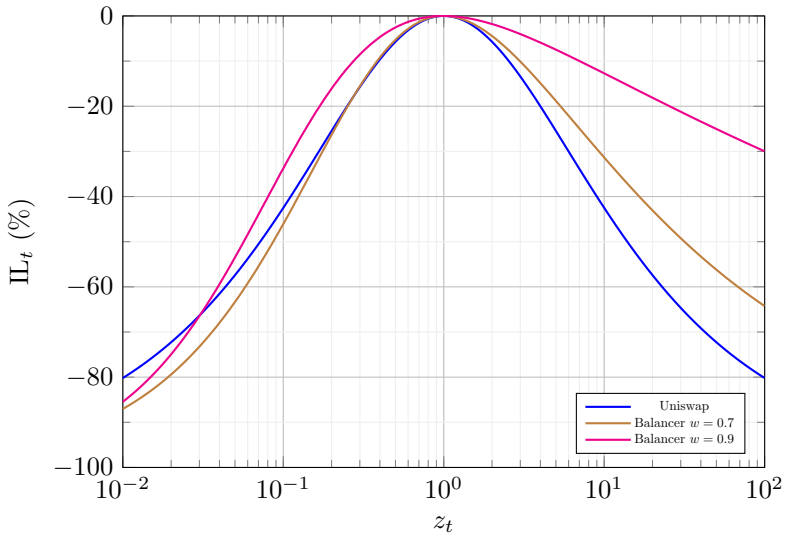


Figure 2.2: Impermanent loss under Uniswap, Balancer $w = 0.7$ and Balancer $w = 0.9$ as a function of z_t on a log-scale. The Balancer IL is improved on the upside spot movements when the weight is increased.

and where,

$$\rho_t = \prod_{\tau \in \mathcal{T}, t_0 \leq \tau \leq t} \left(\frac{1 + V_\tau}{1 + \gamma V_\tau}\right)^{w_{k_\tau}} \geq 1, \qquad \forall \tau \in \mathcal{T},\, V_\tau = \frac{\Delta_\tau^{k_\tau}}{R_{\tau-}^{k_\tau}}\,. \tag{2.32}$$

V_τ is the trading volume in percentage of the pool size at trade time τ. The parameter ρ_t takes into account all the trading volumes between t_0 when the liquidity provider joins the pools, and time t.

Proof. We first recall that the geometric mean CFMMs follows at any time,

$$\psi_{\mathrm{Bal}}(\boldsymbol{R}_t) = \prod_{i=1}^{n} \left(R_t^i\right)^{w_i} = C_t\,,$$

where the newly defined quantity C_t jumps due to liquidity movements, but also with trading fees according to the way the protocols are built. A fact that was ignored in the previous result in Proposition 4. We recall that a rational trader will not buy and sell the same asset for a given trade as per [6]. Therefore, following our assumption where each trade involves only one input and output asset at a time, for any $\tau \in \mathcal{T}$, there exists $j \in [\![1, n]\!]$ such that we can consider trades from asset α_{k_τ} to asset α_j and as per Section 3 write,

$$\left(R_{\tau-}^{k_\tau} + \gamma \Delta_\tau^{k_\tau}\right)^{w_{k_\tau}} \left(R_{\tau-}^{j} - \Lambda_\tau^{j}\right)^{w_j} \prod_{i \neq k_\tau, j}^{n} \left(R_{\tau-}^{i}\right)^{w_i} = \prod_{i=1}^{n} \left(R_{\tau-}^{i}\right)^{w_i} = C_{\tau-}\,.$$

After the trade occurs, the remaining fraction of the input amount $(1-\gamma)\Delta_\tau^{k_\tau}$, accounting for the fees is injected in the reserve associated to the asset α_{k_τ}. This impacts the value C_τ which gets updated according to,

$$C_\tau = \left(R_{\tau-}^{k_\tau} + \Delta_\tau^{k_\tau}\right)^{w_{k_\tau}} \left(R_{\tau-}^{j} - \Lambda_\tau^{j}\right)^{w_j} \prod_{i \neq k_\tau, j}^{n} \left(R_{\tau-}^{i}\right)^{w_i} = C_{\tau-} \left(\frac{1 + V_\tau}{1 + \gamma V_\tau}\right) \geq C_{\tau-}\,. \tag{2.33}$$

The constant value is increased after each trade due to the commission. By using the liquidity provider holdings rather than the reserve sizes we can ignore the jumps of C_t due to liquidity movements. Let us denote,

$$c_t = \psi_{\text{Bal}}(\boldsymbol{r}_t) = \prod_{i=1}^{n} \left(r_t^i\right)^{w_i}.$$

Since $\boldsymbol{r}$ is not impacted by a liquidity event as seen in Assumption 3, the newly defined value c_t only jumps after each trade. Using the fact that the share X^m of each LP is constant between two liquidity events with equations (2.14) and (2.33), one obtains for $\tau \in \mathcal{T}$,

$$c_\tau = c_{\tau-} \left(\frac{1 + V_{\tau-}}{1 + \gamma V_{\tau-}} \right)^{w_{k_\tau}}. \tag{2.34}$$

The above equation implies

$$\frac{\psi_{\text{Bal}}(\boldsymbol{r}_t)}{\psi_{\text{Bal}}(\boldsymbol{r}_0)} = \frac{c_t}{c_{t_0}} = \rho_t, \tag{2.35}$$

with ρ_t as defined in (2.32). Combining (2.26) and the above equation (2.35), one finds

$$\frac{r_t^n}{r_0^n} = \frac{c_t}{c_{t_0}} \prod_{i=1}^{n} \left(\frac{S_t^i}{S_0^i} \right)^{w_i} = \rho_t \prod_{i=1}^{n} \left(z_t^i\right)^{w_i}. \tag{2.36}$$

Finally, replacing (2.36) within (2.25) gives the result of the proposition. □

The parameter ρ_t increases with each new trade starting from 1 at inception when the LP joins the pools. The longer the LP holds his/her position in the DEX, the higher will be the value of ρ_t. It is also worth noting that if trading volume increases, this parameter grows faster, improving the IL even more efficiently. In Figure 2.3 several profiles of IL are represented with different fixed values of ρ_t. The gradual increase of ρ_t shifts the impermanent loss profile higher and reduces the area where the IL is negative. For example, when trading fees bring ρ_t from 1 to 1.7, compared to a buy-and-hold strategy, liquidity providing remains profitable even when the spot changes by a factor of 10 (either increase or decrease). The profile of IL obtained with $\rho_t \equiv 1$ corresponds to the case with no trading commission described in the previous section.

2.6 Slippage

Slippage is the difference between the price at which a trade is expected to get executed and the actual price at which it occurs. With exchanges relying on order books [18], slippage can be positive or negative, depending on whether the difference is favorable or not. For DEXs, such as Uniswap or Balancer, the prices depend on the liquidity pools sizes which have slower dynamic properties than order books. The resulting slippage is often unfavorable for the trader.

We are defining the slippage as the difference of the effective spot of asset i, $\bar{S}_t^i$, which is the price of a trade of arbitrary size and its associated marginal price $\hat{S}_t^i$ as discussed in sub-section 2.3. The rationale behind this definition is that a trader submitting an order with very small size will experience a trade flow in line with $\hat{S}_t^i$. However, if the trade size is larger, the effective spot of the trade will differ from $\hat{S}_t^i$ and the difference is generally seen as a slippage. Other definitions or views are possible as well. Additionally, and to simplify reasoning, we ignore the impact of trading fees such that, following [6], $\hat{S}_t^i = S_t^i$ that is, the marginal price is equal to the reported price and we can write the slippage Υ_t without trading fees as,

$$\Upsilon_t = \frac{\bar{S}_t^i - S_t^i}{S_t^i}.$$

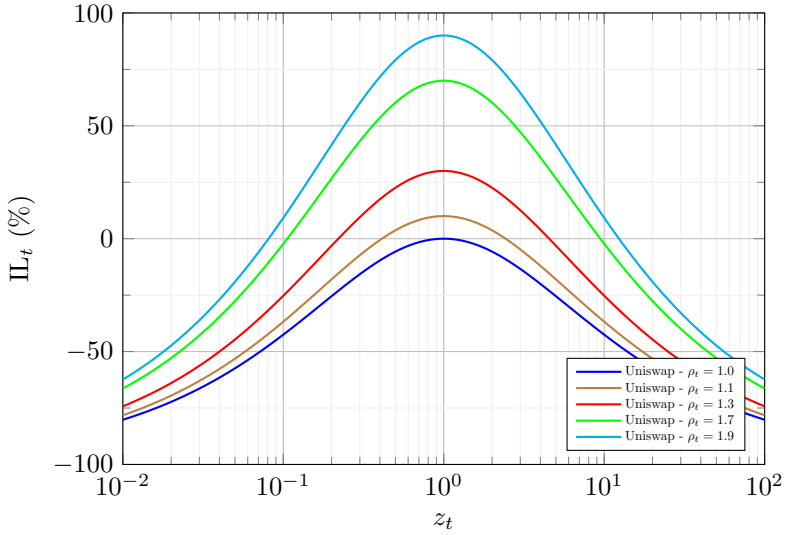


Figure 2.3: Impact of trading fees on the profile of impermanent loss for a LP joining a DEX similar to Uniswap. The accrual of commissions increases ρ_t gradually. Different IL profiles are represented for $\rho_t = \{1, 1.1, 1.3, 1.7, 1.9\}$. $\rho_t = 1$ corresponds to the case without trading fees. The x-axis is z_t on a log-scale.

We focus on the case of two assets for the geometric mean market CFMM. Let us consider a trader who exchanges $\Delta_t^1 \geq 0$ to obtain Λ_t^2 at time t. By writing the two-assets equation of (2.3) with $\gamma = 1$ we have,

$$\left(R_{t-}^1 + \Delta_t^1\right)^w \left(R_{t-}^2 - \Lambda_t^2\right)^{1-w} = \left(R_{t-}^1\right)^w \left(R_{t-}^2\right)^{1-w}.$$

This gives,

$$\Lambda_t^2 = R_{t-}^2 \left(1 - \left(1 + \frac{\Delta_t^1}{R_{t-}^1}\right)^{-\frac{w}{1-w}}\right).$$

Let us remark that expression (2.8) simplifies to $\bar{S}_t^1 = \Lambda_t^2 / \Delta_t^1$ in the case of two assets with $\alpha \equiv \alpha_1$ and $\beta \equiv \alpha_2$.

By using the expression 2.7: one finds,

$$\Upsilon_t{}^{\alpha \to \beta} = \frac{1-w}{w} \frac{R_{t-}^1}{\Delta_t^1} \left(1 - \left(1 + \frac{\Delta_t^1}{R_{t-}^1}\right)^{-\frac{w}{1-w}}\right) - 1\,, \tag{2.37}$$

This slippage, when defined as a function of the trade size Δ^1 converges to zero when $\Delta^1 \to 0$. For Uniswap, with $w = 0.5$, expression (2.37) becomes $\Upsilon_t{}^{\alpha \to \beta} = -\Delta_t^1 / \left(R_{t-}^1 + \Delta_t^1\right)$. The negative slippage here, means when selling a non-zero quantity Δ_t^1 at time t, the obtained spot is less favorable than if the trade size was marginal. Symmetrically for a trader selling an amount $\Delta_t^2 \geq 0$ to obtain Λ_t^1 one finds,

$$\Upsilon_t{}^{\beta \to \alpha} = \frac{w}{1-w} \frac{R_{t-}^2}{\Delta_t^2} \left(1 - \left(1 + \frac{\Delta_t^2}{R_{t-}^2}\right)^{-\frac{1-w}{w}}\right) - 1\,, \tag{2.38}$$

In the case of Uniswap expression (2.38) simplifies to $\Upsilon_t{}^{\beta \to \alpha} = -\Delta_t^2 / \left(R_{t-}^2 + \Delta_t^2\right)$ which can be similarly interpreted as above.

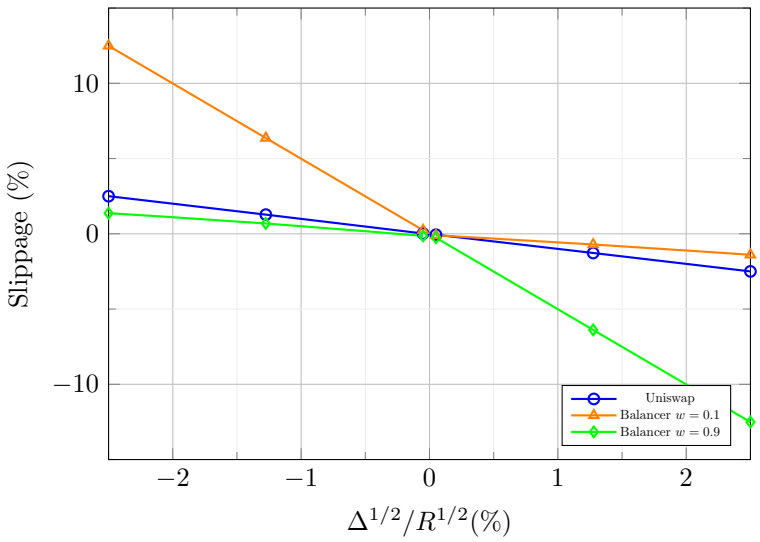


Figure 2.4: Slippage for geometric mean markets, with Uniswap and Balancer $w = \{0.1, 0.9\}$ as a function of Δ^1/R^1 for positive values on the abscissa and $-\Delta^2/R^2$ for negative values on the abscissa. The ordinate is the slippage for a trade to sell α for β on positive abscissa values. Similarly, the ordinate is - slippage for a trade to sell β for α on negative abscissa values. One can see symmetrical slippage for Uniswap for both trade directions but asymmetric slippage for each Balancer. For example, Balancer with weight 0.1 is favorable for traders who sell α for β.

On Figure 2.4, both functions $\Upsilon^{\beta\to\alpha} : \mathbb{R}^+ \to \mathbb{R}^-$ and $\Upsilon^{\alpha\to\beta} : \mathbb{R}^+ \to \mathbb{R}^-$ are represented on the same graphic,

$$\Upsilon^{\alpha\to\beta}(x) = \frac{1-w}{xw}\left(1-(1+x)^{-\frac{w}{1-w}}\right) - 1, \quad \Upsilon^{\beta\to\alpha}(x) = \frac{w}{x(1-w)}\left(1-(1+x)^{-\frac{1-w}{w}}\right) - 1\,,$$

where negative abscissas are mapped to $x \to$ -$\Upsilon^{\beta\to\alpha}(-x)$ and positive abscissas, mapped to $x \to \Upsilon^{\alpha\to\beta}(x)$.

One can see that Balancer with weights different from 0.5, offers very asymmetric behavior in terms of slippage depending on the trade direction. For example low weights offers low slippage when selling α for β. However from β to α, the slippage is much higher than Uniswap. The situation is symmetric for high weights. We remind here that Balancer with asymmetric weights helps improve the IL for one direction of spot movement but not both. In conclusion, using Balancer with low or high weights partially improves the IL either on the increase or decrease of the spot but also offers very asymmetric slippage depending on the trade direction.

3 Synchronized AMM

In this article, we introduce a new type of AMM which combines the properties of several CFMMs together. The goal is two-fold, on the one hand this approach allows to gain flexibility on the features of the resulting AMM, on the other hand, as a direct application of this technique and driving result of the paper, we propose an AMM with strongly reduced downside risk for liquidity providers. The latter comes from the interesting properties of geometric mean markets CFMM with asymmetric weights which improve the impermanent loss either on the rise or on the fall of the spot, depending on the value of the weights of the geometric mean as seen in sub-section 2.5.1.

To avoid complex notations, we focus on the two-CFFM synchronized AMM. This bears similarities with the two-pools Balancer with aligned spot prices discussed in [7]. In sub-section 2.1, we have denoted $(\boldsymbol{R}_t)_{t\geq 0}$

the reserves for a given CFMM, which we will use here to account for the reserves of a first CFMM ($\mathcal{G}_1$). Therefore, we also denote $\left(\bar{\boldsymbol{R}}_t\right)_{t\geq 0}$ the reserve process for a second CFMM ($\mathcal{G}_2$). Both $\mathcal{G}_1$ and $\mathcal{G}_2$ are defined by their associated constant function $\phi_1(\boldsymbol{R}_t,\cdot,\cdot)$ and $\phi_2\left(\bar{\boldsymbol{R}}_t,\cdot,\cdot\right)$ respectively. We propose the following definition,

Definition 6. Let $\boldsymbol{S}_{t-}$ be the reported spot of $\mathcal{G}_1$ and $\boldsymbol{Y}_{t-}$ be the reported spot of $\mathcal{G}_2$ at a positive time $t-$ prior to a trade or a liquidity addition or withdrawal. An automated market maker is a synchronized CFFM if and only if, for any valid trade $(\boldsymbol{\Lambda},\boldsymbol{\Delta})$, there exist a vector $\boldsymbol{q}\in[0,1]^n$ such that,

$$\phi_1(\boldsymbol{R}_{t-},\boldsymbol{\eta},\boldsymbol{q}\odot\boldsymbol{\Delta})=\phi_1(\boldsymbol{R}_{t-},\boldsymbol{0},\boldsymbol{0})\,, \tag{3.1}$$

as well as,

$$\phi_2\left(\bar{\boldsymbol{R}}_{t-},\bar{\boldsymbol{\eta}},(\boldsymbol{1}-\boldsymbol{q})\odot\boldsymbol{\Delta}\right)=\phi_2\left(\bar{\boldsymbol{R}}_{t-},\boldsymbol{0},\boldsymbol{0}\right),$$

with $\boldsymbol{\Lambda}=\bar{\boldsymbol{\eta}}+\boldsymbol{\eta}$, $\odot$ the element-wise (Hadamart) product and $\boldsymbol{1}$ the unit vector of n-entries. Additionally, the reported spots, $\boldsymbol{S}_t$ and $\boldsymbol{Y}_t$ after the trade and at liquidity events must agree, that is the following relationship must hold for any $i\in[\![1,n]\!]$ and at any time $t\geq 0$,

$$\frac{\partial_{R^i}\psi_1(\boldsymbol{R}_t)}{\partial_{R^n}\psi_1(\boldsymbol{R}_t)}=\frac{\partial_{R^i}\psi_2\left(\bar{\boldsymbol{R}}_t\right)}{\partial_{R^n}\psi_2\left(\bar{\boldsymbol{R}}_t\right)}\,, \tag{3.2}$$

with,

$$\psi_{1/2}(\boldsymbol{.})=\phi_{1/2}(\boldsymbol{.},\boldsymbol{0},\boldsymbol{0}),$$

and where, as per (2.4),

$$\begin{aligned}\boldsymbol{R}_t&=\boldsymbol{R}_{t-}+\boldsymbol{q}\odot\boldsymbol{\Delta}-\boldsymbol{\eta}\\ \bar{\boldsymbol{R}}_t&=\bar{\boldsymbol{R}}_{t-}+(\boldsymbol{1}-\boldsymbol{q})\odot\boldsymbol{\Delta}-\bar{\boldsymbol{\eta}}\,.\end{aligned}$$

Less formally, this entails that the synchronization allows to split any valid trade between $\mathcal{G}_1$ and $\mathcal{G}_2$, making it a valid trade for both $\mathcal{G}_1$ and $\mathcal{G}_2$ individually. Additionally, the reported spots before and after the trade should match perfectly. Without loss of generality, since the reported spots of both $\mathcal{G}_1$ and $\mathcal{G}_2$ are matching, we will denote the reported spot of the synchronized AMM by $(\boldsymbol{S}_t)_{t\geq 0}$, following the reported spot notation of $\mathcal{G}_1$.

3.1 Two-assets synchronized geometric mean AMM

In this section, as a concrete example of the above general definition, we consider a two assets AMM built with the synchronization of two geometric mean CFMM. In the remainder of the article we refer to this automated market maker as sync-AMM. There are two reasons behind this choice; the first is that two assets within two synchronized CFMM is a natural configuration for such a system and therefore also the easiest both numerically and theoretically. The second and most important reason is that by combining two geometric CFMM, with well chosen weights, we can take advantage of their best properties and combine them to improve the impermanent loss for LPs. It is important here to pin-point the fact that traders will not be able to interact with the two internals CFMM, as this will be done following the procedure below, and will result in a standard AMM from an end-user perspective. The trade splitting and rerouting into the two internal CFMM as well as the synchronization of the reported spots is handled by the new type of DEX.

This section derives the main result of this article and the two-assets synchronized geometric mean CFMM will be discussed in extensive details in the remainder of the paper. We write,

$$\psi_1(\boldsymbol{R}_t)=\left(R_t^1\right)^w\left(R_t^2\right)^{1-w},\qquad \psi_2\left(\bar{\boldsymbol{R}}_t\right)=\left(\bar{R}_t^1\right)^{\bar{w}}\left(\bar{R}_t^2\right)^{1-\bar{w}}, \tag{3.3}$$

where the driving weights of the geometric mean $\mathcal{G}_1$ and $\mathcal{G}_2$ are w and $\bar{w}$ respectively. The Definition 6 can be written naturally under that setup, more specifically, the spot equality condition (3.2) becomes for any t,

$$\frac{w}{1-w}\frac{R_t^2}{R_t^1}=\frac{\bar{w}}{1-\bar{w}}\frac{\bar{R}_t^2}{\bar{R}_t^1}. \tag{3.4}$$

This combined with (3.1) provides insights on the necessary and sufficient condition for what is required at trade times $t \in \mathcal{T}$. We also assume that reserves of the geometric mean CFMM are strictly positive for any time $t > 0$,

$$R_t^{1/2} > 0, \qquad \bar{R}_t^{1/2} > 0. \tag{3.5}$$

Finally, while most of the derivations and discussions below can be made under the assumptions that w and $\bar{w}$ are not linked together. In our case, we will work with

$$\bar{w} = 1 - w\,. \tag{3.6}$$

3.1.1 Trade events and trade routing

Let us denote a valid trade $(\mathbf{\Lambda}, \mathbf{\Delta})$ at time $t \in \mathcal{T}$ and $q \in [0,1]$ a trade split. We also assume that at $t-$ the reported spot of $\mathcal{G}_1$ and $\mathcal{G}_2$ are synchronized following (3.4), and we therefore write,

$$S_{t-} = Y_{t-}\,.$$

Without loss of generality, we work under the case where the trader wishes to sell a predefined amount $\Delta_1 > 0$ of asset α_1 and is expecting to receive an amount Λ_2 of asset $\alpha_2 \equiv \beta$. The rational trader is not expecting to input any amount of asset β for that operation, such that $\Delta_2 = 0$ and will not receive any amount of asset α_1 such that $\Lambda_1 = \eta_1 = \bar{\eta}_1 = 0$. For $\mathcal{G}_1$ with (3.1) we therefore have,

$$\left(R^1_{t-} + \gamma q \Delta_1\right)^w \left(R^2_{t-} - \eta_2\right)^{1-w} = \left(R^1_{t-}\right)^w \left(R^2_{t-}\right)^{1-w}, \tag{3.7}$$

and similarly for $\mathcal{G}_2$,

$$\left(\bar{R}^1_{t-} + \gamma(1-q)\Delta_1\right)^{\bar{w}} \left(\bar{R}^2_{t-} - \bar{\eta}_2\right)^{1-\bar{w}} = \left(\bar{R}^1_{t-}\right)^{\bar{w}} \left(\bar{R}^2_{t-}\right)^{1-\bar{w}}. \tag{3.8}$$

Since at $t-$ we have (3.4), before the trade we can write the condition on the output amounts η_1 and η_2 which are unique solutions of (3.7) and (3.8), namely,

$$\eta_2 = R^2_{t-}\left(1 - \left(\frac{R^1_{t-}}{R^1_{t-} + \gamma q \Delta_1}\right)^{\frac{w}{1-w}}\right), \qquad \bar{\eta}_2 = \bar{R}^2_{t-}\left(1 - \left(\frac{\bar{R}^1_{t-}}{\bar{R}^1_{t-} + \gamma(1-q)\Delta_1}\right)^{\frac{\bar{w}}{1-\bar{w}}}\right),$$

which provides the unique solution for the output amount of the synchronized AMM

$$\Lambda_2 = \eta_2 + \bar{\eta}_2. \tag{3.9}$$

To find the term q, we use the fact that after the trade, reserves get updated and the spots are required to remain synchronized according to (3.4) with the new reserves. This gives

$$\frac{w}{1-w}\frac{R^2_{t-}\left(\frac{R^1_{t-}}{R^1_{t-}+\gamma q \Delta_1}\right)^{\frac{w}{1-w}}}{R^1_{t-} + q\Delta_1} = \frac{\bar{w}}{1-\bar{w}}\frac{\bar{R}^2_{t-}\left(\frac{\bar{R}^1_{t-}}{\bar{R}^1_{t-}+\gamma(1-q)\Delta_1}\right)^{\frac{\bar{w}}{1-\bar{w}}}}{\bar{R}^1_{t-} + (1-q)\Delta_1}. \tag{3.10}$$

By using $S_{t-} = \frac{w}{1-w}\frac{R^2_{t-}}{R^1_{t-}}$ and $Y_{t-} = \frac{\bar{w}}{1-\bar{w}}\frac{\bar{R}^2_{t-}}{\bar{R}^1_{t-}}$, the above expression is simplified into

$$S_{t-}\frac{\left(1+\gamma\frac{q\Delta_1}{R^1_{t-}}\right)^{\frac{-w}{1-w}}}{1+\frac{q\Delta_1}{R^1_{t-}}} = Y_{t-}\frac{\left(1+\gamma(1-q)\frac{\Delta_1}{\bar{R}^1_{t-}}\right)^{\frac{-\bar{w}}{1-\bar{w}}}}{1+(1-q)\frac{\Delta_1}{\bar{R}^1_{t-}}}\,. \tag{3.11}$$

Here we use the fact that $S_{t-} = Y_{t-}$ and $S_{t-} > 0$, such that we remove the spots from (3.11). This condition translates in defining a continuous function $f : [0,1] \to \mathbb{R}$, such that q is solution of $f(q) = 0$, where

$$f(q) = \left(1 + (1-q)\frac{\Delta_1}{\bar{R}^1_{t-}}\right)\left(1 + \gamma(1-q)\frac{\Delta_1}{\bar{R}^1_{t-}}\right)^{\frac{\bar{w}}{1-\bar{w}}} - \left(1 + \frac{q\Delta_1}{R^1_{t-}}\right)\left(1 + \gamma\frac{q\Delta_1}{R^1_{t-}}\right)^{\frac{w}{1-w}}.$$

Additionally we note that,

$$f(0) = \left(1 + \frac{\Delta_1}{\bar{R}^1_{t-}}\right)\left(1 + \gamma\frac{\Delta_1}{\bar{R}^1_{t-}}\right)^{\frac{\bar{w}}{1-\bar{w}}} - 1 > 0, \qquad f(1) = 1 - \left(1 + \frac{\Delta_1}{R^1_{t-}}\right)\left(1 + \gamma\frac{\Delta_1}{R^1_{t-}}\right)^{\frac{w}{1-w}} < 0,$$

and since f is a continuous and strictly decreasing function we conclude that there exists a unique q_0 such that $f(q_0) = 0$.

Remark. This is of paramount importance as it signifies that any trade can be performed with a unique split and routing into $\mathcal{G}_1$ and $\mathcal{G}_2$ that also allows to keep both $\mathcal{G}_1$ and $\mathcal{G}_2$ with a synchronized reported spot at any time t around a trade event. We see in the next section that synchronization holds also during liquidity addition and withdrawal. Therefore the reported spots for both $\mathcal{G}_1$ and $\mathcal{G}_2$ will remain synchronized at any given time t.

3.1.2 Liquidity addition and withdrawal

Liquidity addition in the synchronized AMM follows two requirements. On the one hand, we require that the spot should not move when liquidity is changed, which is a generally standard desired property as part of Assumption 3. On the other hand, thanks to extra degrees of freedom within the sync-AMM, we can also require that the ratio of the assets added follows the current reported spot, which is a property shared with Uniswap. Namely, assuming the liquidity provider desires to add a liquidity amount $r^1_{t_0}$ of asset $\alpha \equiv \alpha_1$ at joining time t_0, the amount of asset $\beta \equiv \alpha_2$ to put alongside will follow,

$$r^2_{t_0} = S_{t_0} r^1_{t_0}.$$

We also make use of the link between the weights in $\mathcal{G}_1$ and $\mathcal{G}_2$, from equation (3.6). Additionally, we have seen in (3.4) that liquidity addition in geometric mean market makers should be proportional to the current reserve sizes, such that, for any $\theta \in \Theta$ and for a given $\lambda > 0$ the reserve increase is,

$$\boldsymbol{R}_\theta = \boldsymbol{R}_{\theta-}(1+\lambda).$$

This naturally leads to matching spots at t_0- and t_0 for both $\mathcal{G}_1$ and $\mathcal{G}_2$, where we define two addition factors, λ and $\bar{\lambda}$ respectively and where we get,

$$\boldsymbol{R}_{t_0} = \boldsymbol{R}_{t_0-}(1+\lambda), \quad \bar{\boldsymbol{R}}_{t_0} = \bar{\boldsymbol{R}}_{t_0-}\left(1+\bar{\lambda}\right).$$

Spot equality is therefore guaranteed by construction, the only extra condition would translate in finding the tuple $\left(\lambda, \bar{\lambda}\right)$ such that,

$$\lambda R^1_{t_0-} + \bar{\lambda}\bar{R}^1_{t_0-} = r^1_{t_0}, \quad \lambda R^2_{t_0-} + \bar{\lambda}\bar{R}^2_{t_0-} = S_{t_0-} r^1_{t_0}, \tag{3.12}$$

where we used the fact that the reported spots of $\mathcal{G}_1$ and $\mathcal{G}_2$ match precisely at t_0-. Since we have assumed (3.6) as well as (3.4) which ensures equality of reported spots, the unique solution to the linear system (3.12) is,

$$\lambda = w\frac{r^1_{t_0}}{R^1_{t_0-}}, \quad \bar{\lambda} = (1-w)\frac{r^1_{t_0}}{\bar{R}^1_{t_0-}}.$$

This means that the liquidity amount is split between $\mathcal{G}_1$ and $\mathcal{G}_2$ with proportions w and $1-w$ respectively. The liquidity provider shares are then updated naturally for each of the geometric mean market makers $\mathcal{G}_1$ and $\mathcal{G}_2$ independently following (2.13). It is worth noting that $\mathcal{G}_1$ and $\mathcal{G}_2$ having a spot as defined in (2.7), the AMM

dispatches a share w of asset α and a share $(1-w)$ of asset β into the first internal pool $\mathcal{G}_1$. Symmetrically, the AMM dispatches a share $(1-w)$ of α assets and a share w of tokens β into the second internal pool $\mathcal{G}_2$.

Liquidity removal is similar to liquidity withdrawal in the individual geometric mean market makers $\mathcal{G}_1$ and $\mathcal{G}_2$. For both $\mathcal{G}_1$ and $\mathcal{G}_2$, the spots naturally do not move since the share of the liquidity providers in the reserves for asset α and reserve for asset β are under the same proportion following (2.13) and therefore the withdrawal is done by a down-scaling of the reserve sizes.

3.1.3 Impermanent loss of a synchronized AMM without trading fees

We consider here the case where the AMM accounts for two assets $\alpha \equiv \alpha_1$ and $\beta \equiv \alpha_2$ and provide the impermanent loss for the sync-AMM discussed in Section 3.1 in the case where there is no trading fees. We recall that for each individual internal geometric CFMM $\mathcal{G}_1$ and $\mathcal{G}_2$, the total value of the assets of a liquidity provider under numéraire β and at time $t \geq 0$, is $p_t = \frac{r_t^2}{1-w}$ for $\mathcal{G}_1$ and $\bar{p}_t = \frac{\bar{r}_t^2}{1-\bar{w}}$ for $\mathcal{G}_2$ according to (2.23). Here, r_t^2 and $\bar{r}_t^2$ are the holdings of the LP for asset β in the corresponding CFMM.

At any time $t \geq 0$, the total holding P_t of the LP is the sum of his holdings in the two internal pools,

$$P_t = p_t + \bar{p}_t \,.$$

Let us denote $Q_{t_0}^{\beta}$ the total amount of liquidity added at time t_0 by the LP into the sync-AMM denominated in amounts of β. Following the details in sub-section 3.1.2, the sync-AMM will distribute this initial liquidity by dispatching a fraction $\nu Q_{t_0}^{\beta}$ into $\mathcal{G}_1$ and $(1-\nu)Q_{t_0}^{\beta}$ into $\mathcal{G}_2$. By combining the generic equations (2.23), (2.24) and (2.27) we can write the difference between the holdings in the DEX versus a buy-and-hold strategy,

$$P_t - P_t^S = \nu Q_{t_0}^{\beta}(z_t^w - wz_t - (1-w)) + (1-\nu)Q_{t_0}^{\beta}\left(z_t^{\bar{w}} - \bar{w}z_t - (1-\bar{w})\right).$$

That gives the expression of the impermanent loss,

$$\mathrm{IL}(z_t) = \frac{\nu(z_t^w - wz_t - (1-w)) + (1-\nu)(z_t^{\bar{w}} - \bar{w}z_t - (1-\bar{w}))}{\nu[wz_t + (1-w)] + (1-\nu)[\bar{w}z_t + (1-\bar{w})]}.$$

As a sanity check if both internal pools are following Uniswap dynamics $w = \bar{w} = \frac{1}{2}$, one recovers $\mathrm{IL}(z)^{\mathrm{Uni}} = \frac{2\sqrt{z}}{z+1} - 1$. Following (3.6), we set $\bar{w} = 1 - w$ and the choice of ν can be restricted by imposing the buy-and-hold portfolio to behave similarly to Uniswap; that means that at inception the liquidity provider will have to provide assets with equal quantity as discussed in sub-section 3.1.2. For this purpose, the following equation must be satisfied,

$$(\nu w + (1-\nu)(1-w)) = \frac{1}{2},$$

which leads to

$$\nu = \frac{1}{2}\,. \tag{3.13}$$

The above equation means the internal CFMM $\mathcal{G}_1$ and $\mathcal{G}_2$ receive equal quantities of asset α and β. This choice provides a rather elegant form for the impermanent loss of the sync-AMM,

$$\mathrm{IL}(z) = \frac{z^w + z^{1-w}}{z+1} - 1\,. \tag{3.14}$$

It is interesting to notice that (3.14) is always smaller than zero, as expected, but greater than $\mathrm{IL}^{\mathrm{Uni}}(z)$ for any $z \geq 0$. Indeed,

$$\mathrm{IL}(z) - \mathrm{IL}^{\mathrm{Uni}}(z) = \frac{z^w + z^{1-w} - 2\sqrt{z}}{z+1} = \frac{(z^w - \sqrt{z})^2}{z^w(z+1)} \geq 0\,.$$

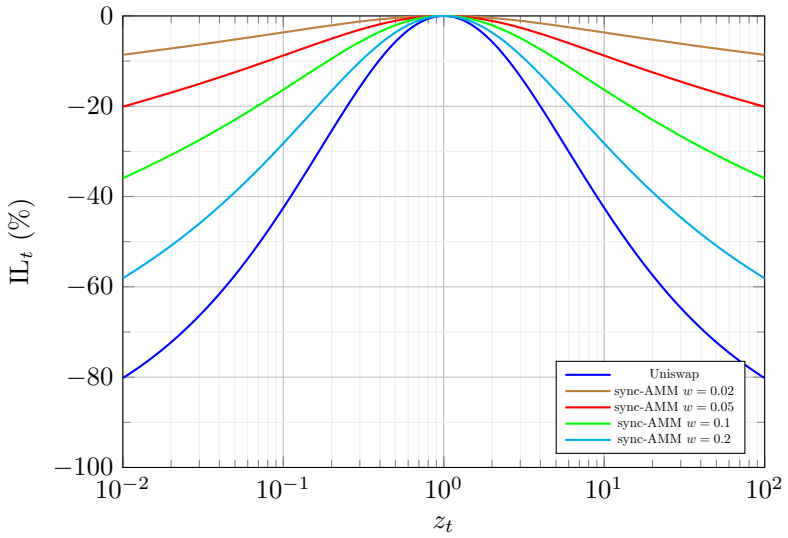


Figure 3.1: Impermanent loss without trading fees for LP under Uniswap and Sync-AMM with different values of w, namely $w = \{0.02, 0.05, 0.1, 0.2\}$. The plot is as a function of z_t on a log-scale.

The sync-AMM therefore improves the impermanent loss compared to Uniswap. Moreover the smaller the weight w, the higher the improvement. However, small w have lower quality for the slippage, which brings a trade-off between the improvement of the IL and the spot slippage to take into consideration.

As seen on Figure 3.1, the new AMM takes advantages of the best features of each CFMM and helps improve the IL on both increase and decrease of the spot performance. For example, the synchronized AMM with $w = 0.1$, leads to an IL of -16.3% against -42.5% for Uniswap if the spot either increases or decreases by a factor of 10 with respect to the LP entry value. The IL for the new AMM is perfectly symmetric as chosen in (3.6).

The gradual accumulation of trading fees combined with this new profile of impermanent loss is the building-block of improved returns for liquidity providers. More details and associated simulations are provided in Section 4.

3.1.4 Expression of slippage

A trade on the sync-AMM is decomposed in two portions which are dispatched to the internal geometric mean CFMMs. A root-finding algorithm solves for trade splitting proportion q_t that keeps the internal CFMM spot synchronized as per sub-section 3.1 for a given trade. We assume that (3.6) holds, and using the result of Section 2.6, we can obtain the effective spot price after a trade. For example, selling a strictly positive amount Δ_t^1 of asset α to obtain Λ_t^2 of asset β,

$$\bar{S}_t^1 = \frac{1}{\Delta_t^1}\left[R_{t-}^2\left[1-\left(1+\frac{q_t\Delta_t^1}{R_{t-}^1}\right)^{-\frac{w}{1-w}}\right]+\bar{R}_{t-}^2\left[1-\left(1+\frac{(1-q_t)\Delta_t^1}{\bar{R}_{t-}^1}\right)^{-\frac{1-w}{w}}\right]\right].$$

And we also have the marginal spot defined as,

$$\lim_{\Delta^1\to 0}\bar{S}_t^1(\Delta^1) = q_t\frac{w}{1-w}\frac{R_{t-}^2}{R_{t-}^1}+(1-q_t)\frac{1-w}{w}\frac{\bar{R}_{t-}^2}{\bar{R}_{t-}^1}.$$

And from the spot equality in (3.4), we can write the expression of the slippage without trading fees as,

$$\Upsilon_t^{\alpha\to\beta}(\Delta^1) = \frac{1-w}{w}\frac{R^1_{t-}}{\Delta^1}\left[1-\left(1+\frac{q_t\Delta^1}{R^1_{t-}}\right)^{-\frac{w}{1-w}}\right] + \frac{w}{1-w}\frac{\bar{R}^1_{t-}}{\Delta^1}\left[1-\left(1+\frac{(1-q_t)\Delta^1}{\bar{R}^1_{t-}}\right)^{-\frac{1-w}{w}}\right].$$

The above expression is the sum of the slippage of each internal CFMM taking respectively the input trades $q_t\Delta^1_t$ and $(1-q_t)\Delta^1_t$. Given that the trade split q_t is a function of the input trade size and the states of the internal reserves just before a trade, it makes the slippage calculation more complex than a more standard CFMM. And because of this, the slippage is not a function of $\Delta^1_t/\left(R^1_{t-}+\bar{R}^1_{t-}\right)$ anymore and cannot be obtained in closed form. If only the total value of $R^{1/2}_t + \bar{R}^{1/2}_t$ were to be reported as reserves publicly, but not the individual reserves of $\mathcal{G}_1$ and $\mathcal{G}_2$, it would be more difficult to perform front-running due to the missing information required to calculate the slippage.

4 Simulations and numerical results

In this section, we discuss the simulation of the synchronized two-assets AMM introduced in sub-section 3.1. First and foremost we will use the following simplified market model; we suppose the market spot$(Z_t)_{t\geq 0}$ representing one unit of α in terms of β, follows a geometric Brownian motion stochastic differential equation under $\mathbb{P}$ with,

$$\begin{cases} dZ_t &= \mu Z_t dt + \sigma Z_t dW_t \\ Z_0 &\geq 0, \end{cases} \tag{4.1}$$

where W is a Brownian motion under $\mathbb{P}$, and where $\mu \in \mathbb{R}$ and $\sigma \in \mathbb{R}^+$. The diffusion parameters μ and σ are not calibrated to the market but arbitrarily chosen values which align with the high growth-rate and volatility sometimes encountered on crypto-currency markets. For example, over the second half of March 2021, Bitcoin realized volatility ranged from 70% to 85%, and similarly Ethereum realized volatility ranged from 60% to 95% (source [2]). More precisely, we present the set of results obtained with the below driving numbers,

$$Z_0 = 137, \quad \mu = 25\%, \quad \sigma = 120\%.$$

The trading fees are assumed fixed at 0.3% per trade and the simulations are run over periods of 3 years with an average amount of 50 000 trades per year, excluding arbitrage trades.

The state variables of the AMMs simulated are calculated following details from sub-section 2.2. Extensive details about Monte Carlo simulations as well as sampling procedure for both (4.1) and random times as described in sub-section 4.1 can be found in [17].

4.1 Trade generation and arbitrage

Our assumption for the different simulations is that trades are simulated such that inter-arrival times follow an exponential distribution of mean $\frac{1}{\lambda}$, which provides an average of λ jumps per unit of time. We chose an average of 50 000 trades per year, randomly happening on the timeline. Let $t \in \mathcal{T}$ be a trade time, the trade size associated to the trade is defined as a Gaussian random variable with mean 0 and standard deviation $N^1_t/400$, where resulting sizes are truncated to stay within the bounds,

$$\left[-N^1_t/100, N^1_t/100\right],$$

where we denoted that for any $t \geq 0$,

$$N^1_t = R^1_t + \bar{R}^1_t, \quad N^2_t = R^2_t + \bar{R}^2_t.$$

A positive trade size is assumed to be a trade to buy or sell asset α for asset β, whereas a negative trade size, is a trade to buy or sell asset β for asset α. The buy or sell order choice is determined randomly with equal probability.

The trade generation discussed above accounts for any spontaneous trades done by traders but does not account for a quoted market spot, e.g. the spot value available on a centralized exchange. Where a market spot is available outside of the sync-AMM, it is possible for arbitrage opportunities to arise, and we assume that in between any two trades, an arbitrageur will try to take advantage of the AMM reported spot divergence with the market spot. More precisely, at time $t = \frac{t_{k+1}+t_k}{2}$ in between non-arbitrage related trades $(t_k, t_{k+1})_{k\in\mathbb{N}} \in \mathcal{T}^2$, an arbitrageur will perform the following operations. If the market spot Z_t is higher than the sync-AMM reported spot S_t, that means one can sell α for β more expensively in the market than on the DEX. Therefore the arbitrageur will optimize a sell order of asset β for asset α in the DEX,

$$A_t = \max_{(\mathbf{\Lambda},\mathbf{\Delta})\in\mathcal{H}_t} \left(Z_t\Lambda^1 - \Delta^2\right),$$

symmetrically if the market spot Z_t is smaller than the sync-AMM reported spot S_t, the arbitrageur will optimize a sell order of asset α for asset β in the DEX,

$$A_t = \max_{(\mathbf{\Lambda},\mathbf{\Delta})\in\mathcal{H}_t} \left(\frac{\Lambda^2}{Z_t} - \Delta^1\right),$$

where $\mathcal{H}_t$ is the set of all valid trade of the sync-AMM at time t. If $A_t > 0$, then the arbitrageur will execute the trade to sell Δ^1 or Δ^2 of asset α or β respectively, recover the output amount Λ^2 or Λ^1 of asset β or α and sell this amount back on the centralized exchange at spot price $(Z_t)^{-1}$ or Z_t respectively, therefore realizing a profit. We note that A_t is not necessarily positive even if the market and reported spot differ, this is due to the impact of trading fees. For example, in [8], the authors show that for Uniswap, it is not efficient to perform an arbitrage trade if the reported spot is smaller that Z_t/γ and higher than γZ_t.

4.2 Liquidity addition and withdrawal

The liquidity addition follows very closely the discussion in sub-section 3.1.2, where each liquidity provider, can either join as a new provider in the AMM or withdraw his/her liquidity. Our assumptions are simplistic but provide a good model for the analysis of the liquidity provider returns, e.g. impermanent loss.

We will work with an initial liquidity amount, brought by a first liquidity provider at time $t = 0$,

$$N_0^1 = 10\,000\,000, \quad N_0^2 = Z_0 N_0^1 = 1\,370\,000\,000.$$

Each subsequent liquidity provider will bring precisely 5% of the initial reserve size N_0^1 when he/she joins the sync-AMM. The liquidity provider will also deposit $Z_0 N_0^1$ into the reserve of β as part of the liquidity addition. Withdrawal can be done in full or partially by the LP in both of the underlying synchronized CFMM. For ease of testing and showcase, we assume that the user exits fully from both synchronized CFMM, at the same time. The associated return is discussed hereafter and displays both the impact of impermanent loss and the rewards thanks to trading fees.

Over a $3Y$ time frame, 20 new liquidity providers will enter the AMM with entry times uniformly distributed over the timeline. While this assumption is simplistic, it allows to validate the dynamics of the DEX.

4.3 Liquidity provider returns

When entering the AMM, the liquidity provider returns, which we will refer to as impermanent loss, can be calculated at every point in time. More specifically, since the liquidity provider can decide to exit the DEX at any given time, it is possible to evaluate the profit-and-loss of the holdings compared to a simple buy-and-hold

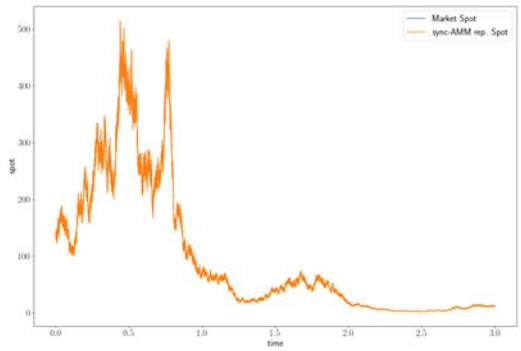


Figure 4.1: Paths 1: Market spot Z_t, sync-AMM reported spot S_t. X axis is the time in years.

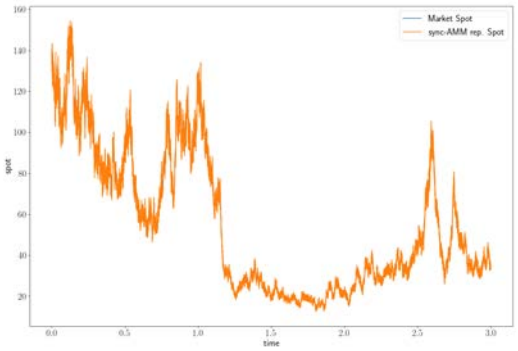


Figure 4.2: Paths 2: Market spot Z_t, sync-AMM reported spot S_t. X axis is the time in years.

strategy started at the LP entry time in the DEX. This without the need for the LP to effectively exit the liquidity pools, which allows to assess the robustness of impermanent loss over different exit points, therefore provides a large scope of possible outcomes.

4.4 Numerical results

The aggregated results for the liquidity provider returns and impermanent loss are computed with 30 paths. While this is low to achieve any reasonable convergence properties on the market spot distribution, this amount of paths combined with the number of possible exit points allows the gathering of a considerable amount of information and scenario outcomes on the liquidity provider PnL and IL. Exit points can happen and profit-and-loss can be calculated at every time step, which will range between 50 000 and 100 000 times per year with the lower bound being the amount of trades independent of arbitrage and the upper bound which accounts for the extra amount of trades a year attributed to arbitrage.

Out of the total number of paths, we hereafter extract 4 of them to display dynamic behaviors. In Figures 4.1 4.2 4.3 4.4 we display the time series of the market spot as well as the sync-AMM reported spot. We can see that the spot moves in a large range of values which provides useful stress test cases.

We also display in Figure 4.5 4.6 4.7 4.8 the impermanent loss of all LPs who entered the given AMM at different time and therefore different spot values. Consequently, they are exposed to different effects of market moves and their profit-and-loss will naturally look different. We note that an important feature of the sync-AMM, which is shared by most CFMM such as Uniswap or Balancer and follows Assumption 3, is that liquidity addition or withdrawal does not impact the PnL of other liquidity providers within the DEX.

Remark. The various colors in Figures 4.5 4.6 4.7 4.8 correspond to the IL of different liquidity providers, entering at different times as well as on possibly different paths, which provides an aggregated view of a large amount of possible outcomes and scenarios.

4.4.1 Time series under stressed markets

In addition to the above, in Table 2, we display the values of the IL with trading fees, i.e. the liquidity providers returns with trading fees compared with a buy-and-hold strategy started time $t = 0$. One can notice that in both cases (when the initial spot increases or decreases by a factor of 100), the IL of the sync-AMM is considerably better than on Uniswap and either a Balancer with low weight or high weight depending on the

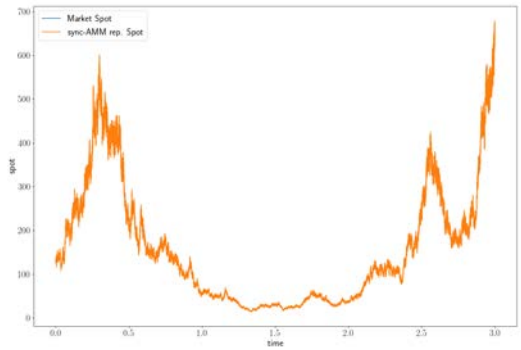


Figure 4.3: Paths 3: Market spot Z_t, sync-AMM reported spot S_t. X axis is the time in years.

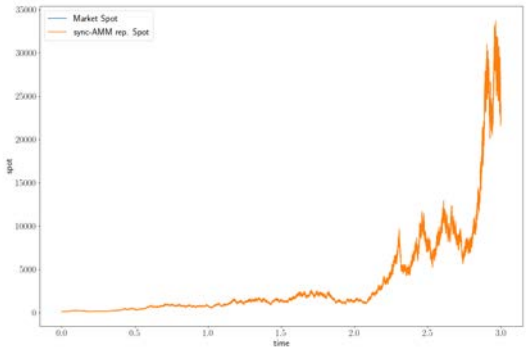


Figure 4.4: Paths 4: Market spot Z_t, sync-AMM reported spot S_t. X axis is the time in years.

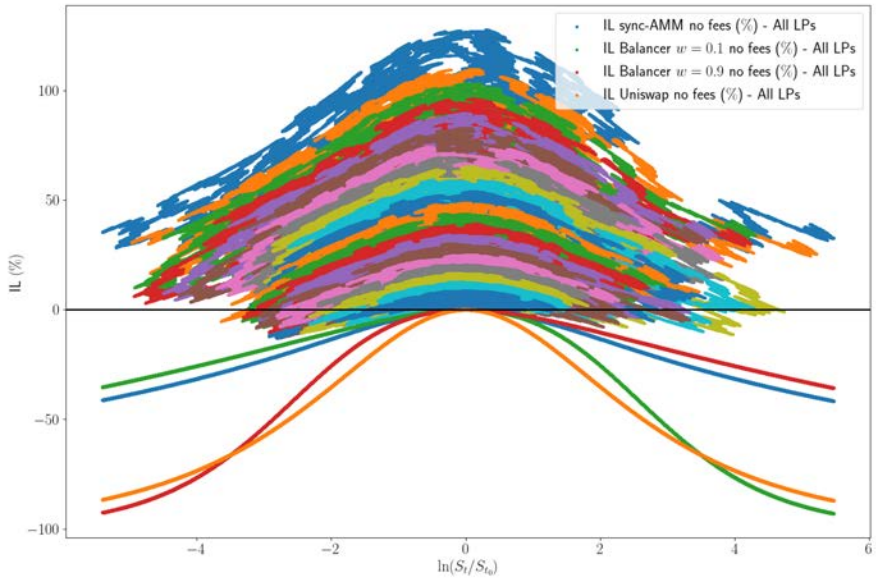


Figure 4.5: Sync-AMM $w = 0.1$: Impermanent loss with trading fees for all liquidity providers who entered the AMM. Each color corresponds to a given liquidity provider and path.

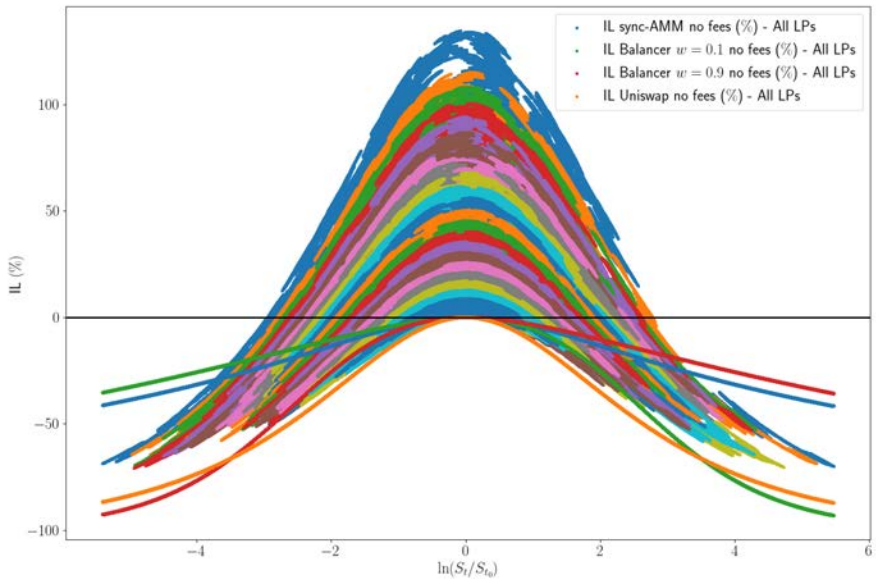


Figure 4.6: Uniswap: Impermanent loss with trading fees for all liquidity providers who entered the AMM. Each color corresponds to a given liquidity provider and path

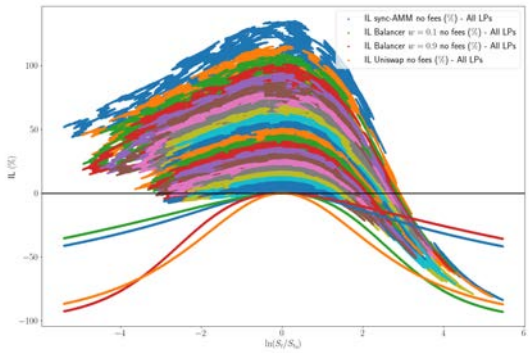


Figure 4.7: Balancer $w = 0.1$: Impermanent loss with trading fees for all liquidity providers who entered the AMM. Each color corresponds to a given liquidity provider and path

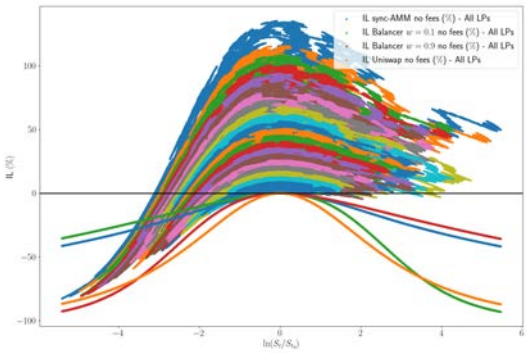


Figure 4.8: Balancer $w = 0.9$: Impermanent loss with trading fees for all liquidity providers who entered the AMM. Each color corresponds to a given liquidity provider and path

	LP returns: IL with trading fees								
	Downward trend					Upward trend			
Time	**3Y**	**2Y**	**1Y**	**6M**	**Start**	**6M**	**1Y**	**2Y**	**3Y**
Spot (ratio)	1.35 (/101.5)	3.79 (/36.1)	31.14 (/4.4)	31.05 (/4.4)	137 (×1)	1 119.59 (×8.2)	1 693.07 (×12.4)	5 210.34 (×38.0)	14 260.38 (×104.1)
IL sync-AMM $w = 0.1$	48.24%	25.04%	20.81%	5.21%	0%	−1.84%	7.41%	23.61%	46.24%
IL Uniswap	−53.56%	−42.78%	3.10%	−10.46%	0%	−28.26%	−29.72%	−44.34%	−54.24%
IL Balancer $w = 0.1$	65.18%	36.91%	24.42%	7.79%	0%	−17.21%	−19.39%	−46.11%	−66.71%
IL Balancer $w = 0.9$	−66.05%	−44.01%	14.60%	−0.34%	0%	2.25%	13.61%	35.61%	63.84%
IL Balancer $w = 0.33$	−24.01%	−20.55%	9.20%	−5.17%	0%	−31.67%	−35.48%	−55.88%	−68.92%
IL Balancer $w = 0.67$	−68.38%	−54.31%	1.71%	−11.53%	0%	−19.07%	−16.75%	−22.13%	−24.89%

Table 1: Liquidity provider returns *with trading fees* compared to a buy-and-hold strategy, i.e. "impermanent loss with trading fees". The initial spot value is $S_0 = 137$; the right-hand side of the table displays a path that increases significantly whereas the left-hand side displays a path that decreases significantly.

	LP returns: IL without trading fees								
	Downward trend					Upward trend			
Time	**3Y**	**2Y**	**1Y**	**6M**	**Start**	**6M**	**1Y**	**2Y**	**3Y**
Spot (ratio)	1.35 (/101.5)	3.79 (/36.1)	31.14 (/4.4)	31.05 (/4.4)	137 (×1)	1 119.59 (×8.2)	1 693.07 (×12.4)	5 210.34 (×38.0)	14 260.38 (×104.1)
IL sync-AMM $w = 0.1$	−36.02%	−28.15%	−8.28%	−8.26%	0%	−14.36%	−18.32%	−28.65%	−36.22%
IL Uniswap	−80.27%	−67.59%	−22.38%	−22.30%	0%	−37.74%	−47.12%	−68.50%	−80.55%
IL Balancer $w = 0.1$	−30.02%	−22.60%	−6.57%	−6.54%	0%	−28.23%	−39.48%	−69.55%	−85.90%
IL Balancer $w = 0.9$	−85.55%	−68.24%	−13.51%	−13.45%	0%	−11.17%	−14.27%	−23.05%	−30.23%
IL Balancer $w = 0.33$	−67.59%	−54.90%	−17.73%	−17.67%	0%	−40.68%	−51.44%	−74.98%	−86.75%
IL Balancer $w = 0.67$	−86.49%	−74.03%	−23.23%	−23.15%	0%	−29.67%	−37.20%	−55.75%	−67.90%

Table 2: Liquidity provider returns *without trading fees* compared to a buy-and-hold strategy, i.e. "impermanent loss without trading fees". The initial spot value is $S_0 = 137$; the right-hand side of the table displays a path that increases significantly whereas the left-hand side displays a path that decreases significantly.

spot deviation direction. Because of the latest remark, the sync-AMM is then consistent both on the rise and fall of the spot which provides a strong improvement of impermanent loss in the two scenarios. As a benchmark, we also provide the impermanent loss without trading fees in Table 1 in which we notice a similar behavior where the sync-AMM provides consistent improvement compared to Uniswap in both up- and down-trend scenarios.

In Figure 4.9, we display the same sample paths as per Table 2 but with the entire time-series of the liquidity providers returns where it is possible to display more precisely the different changes over time of the impermanent loss with the addition of trading fees. The sync-AMM improves the liquidity provider returns, even when large swings of spot prices occur.

4.4.2 Slippage

In Figures 4.10 , 4.11 , 4.12 and 4.13 we display the slippage of the sync-AMM DEX which can be compared to the ones of Uniswap as well as Balancer. The impact of trading fees can be observed as the gap at the origin which shifts all curves above or below the x-axis by the fee amount. The average slippage becomes symmetrical in the sync-AMM compared to Balancer which displays a highly asymmetric behavior when weights are either small or close to 1. This feature favors trading in both directions as opposed to Balancer in such cases. Additionally, an interesting feature of the sync-AMM is a slippage that depends on the current market

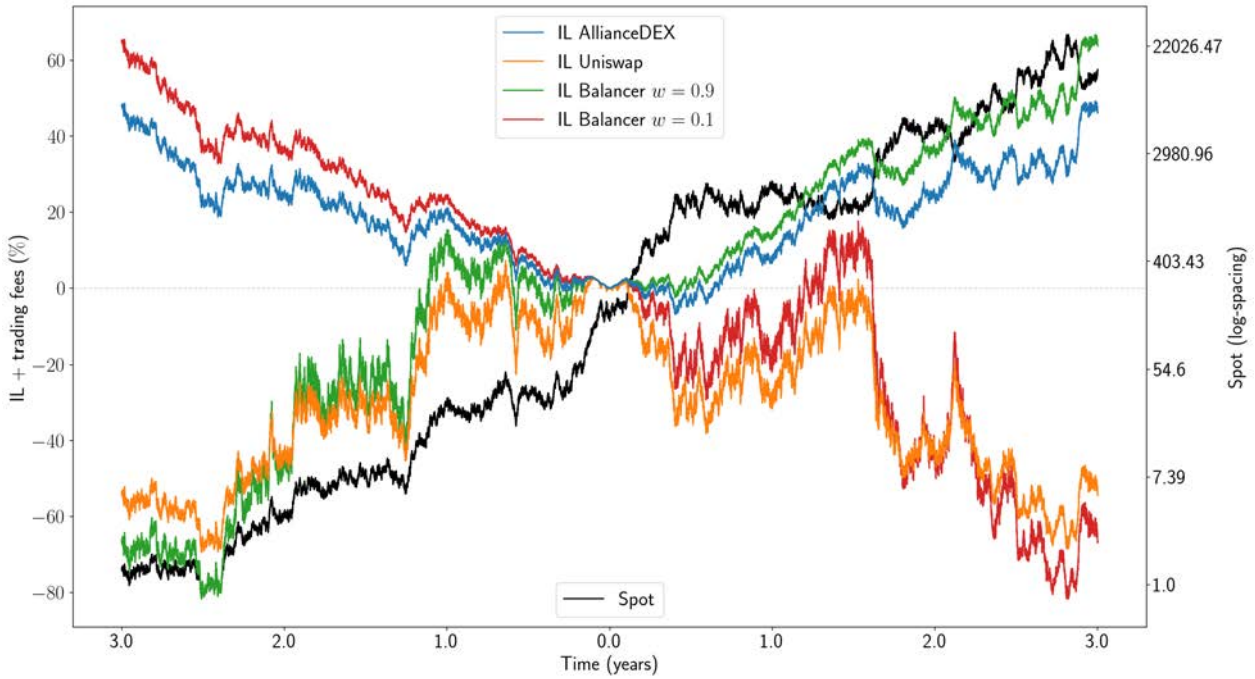


Figure 4.9: Liquidity provider returns *with trading fees* compared to a buy-and-hold strategy, i.e. "impermanent loss with trading fees". The initial spot value is $S_0 = 137$; the right-hand side of the graphic displays a path that increases significantly whereas the left-hand side displays a path that decreases significantly.

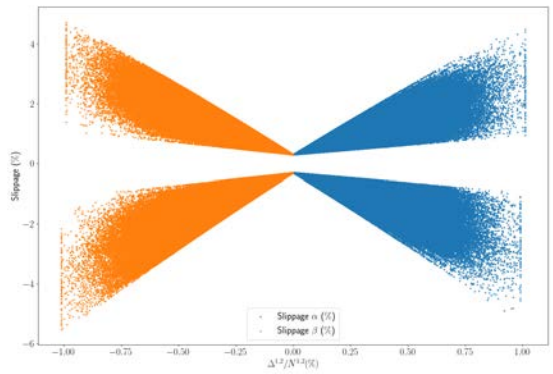


Figure 4.10: Slippage of the sync-AMM with weight $w = 0.1$.

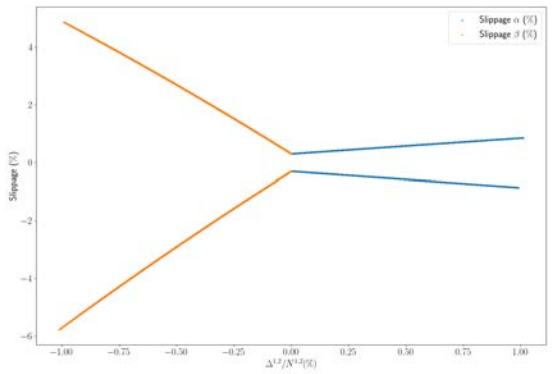


Figure 4.11: Slippage of Balancer with weight $w = 0.1$.

and reserve states and not only on the ratio of the trade size with respect to the associated reserve size like geometric mean markets CFMM. This feature displays the slippage as an apparently random value between bounded ranges when plotted with respect to the trade and reserve size ratio. That contrasts with Balancer or Uniswap, where the slippage has a functional dependence on the same ratio. Additionally, if the individual reserves of pools $\mathcal{G}_1$ and $\mathcal{G}_2$ were not visible publicly, slippage would appear stochastic and potentially could help making front-running more challenging. For the same volume of liquidity, Balancer and sync-AMM have higher slippage than Uniswap, however, if the reserve sizes were increased by the appropriate factor compared to the reserves in a Uniswap-type AMM, then the average slippage would be comparable between the DEXs, while preserving the improved impermanent loss as discussed in previous sections.

5 Conclusion

With the recent innovations in the DEX industry and decentralized finance more generally, new aspects of risk exposures have emerged for investors providing liquidity to decentralized exchanges. In particular, the impermanent loss, or the risk of loss compared to a buy-and-hold strategy when the spot deviates largely from the LP's entry-point, has been a topic of strong research and development in the field. Up until now, tackling the impermanent loss problem has relied mainly on extra-features which do not modify the intricacies of the AMM itself. In this article, we focused on the underlying mechanisms of the market maker by proposing a new approach combining properties of different CFMMs. Our driving example combines two dual-asset geometric mean markets with symmetric weights and provides an improvement of the impermanent loss in every spot market scenario resulting in an average increase of the returns for liquidity providers. This setup brought us to discuss impermanent loss in geometric mean markets used by well known DEXs, such as Uniswap V2 and Balancer V1 where we provided analytical formulas of the IL for the generic case of $n-$assets with and without trading fees. Our numerical results show that the sync-AMM combined with the usual 0.3% trading fees, lead to positive returns in a large amount of market scenarios, even when the spot deviates drastically from the liquidity providers entry points. Striking examples, are sample paths which lead to an increase or decrease of the asset price by a factor of 150 and where, in that instance and on the paths analyzed, the sync-AMM still provided positive returns, compared to a buy-and-hold portfolio. The symmetrical average slippage makes the proposed DEX suitable for trading in both directions as opposed to Balancer with uneven weights. Finally

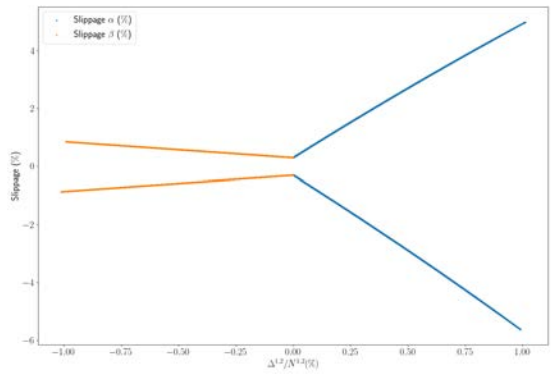


Figure 4.12: Slippage of Balancer with weight $w = 0.9$.

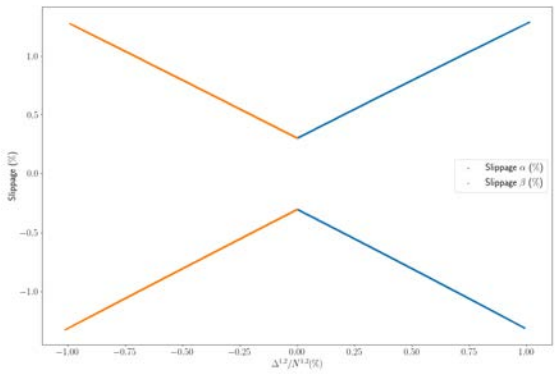


Figure 4.13: Slippage of Uniswap.

this new approach to automated market making could potentially open other research topics on additional improvements of the impermanent loss, reduction of slippage costs as well as new features such as single-sided liquidity provisioning.

References

[1] Defi pulse. https://defipulse.com/.

[2] Deribit. https://www.deribit.com/.

[3] Aave. Aave: Protocol white paper. 2020.

[4] Hayden Z. Adams, Noah Zinsmeister, and Dan Robinson. Uniswap v2 core. 2020.

[5] Hayden Z. Adams, Noah Zinsmeister, Moody Salem, River Keefer, and Dan Robinson. Uniswap v3 core. 2021.

[6] Guillermo Angeris and Tarun Chitra. Improved price oracles: Constant function market makers. In *Proceedings of the 2nd ACM Conference on Advances in Financial Technologies*, AFT '20, page 80–91, New York, NY, USA, 2020. Association for Computing Machinery.

[7] Guillermo Angeris, Alex Evans, and Tarun Chitra. When does the tail wag the dog? curvature and market making. *arXiv: Trading and Market Microstructure*, 2020.

[8] Guillermo Angeris, Hsien-Tang Kao, Rei Chiang, Charlie Noyes, and T. Chitra. An analysis of uniswap markets. *ArXiv*, abs/1911.03380, 2019.

[9] Vitalik Buterin. A next-generation smart contract and decentralized application platform. 2015.

[10] Yan Chen and Cristiano Bellavitis. Blockchain disruption and decentralized finance: The rise of decentralized business models. *Journal of Business Venturing Insights*, 13:e00151, 2020.

[11] Rama Cont and Peter Tankov. *Financial Modelling with Jump Processes*. Chapman & Hall/CRC, 2003.

[12] Dodo team. A next-generation on-chain liquidity provider powered by pro-active market maker algorithm. Technical report, 2020.

[13] Michael Egorov. Stableswap - efficient mechanism for stablecoin liquidity. 2019.

[14] Steve Ellis, Ari Juels, and Sergey Nazarov. Chainlink: A decentralized oracle network. 2017.

[15] Alex Evans. Liquidity provider returns in geometric mean markets. *arXiv: Mathematical Finance*, 2020.

[16] Neil Gandal, JT Hamrick, Tyler Moore, and Tali Oberman. Price manipulation in the bitcoin ecosystem. *Journal of Monetary Economics*, 95:86–96, 2018.

[17] Paul Glasserman. *Monte Carlo Methods in Financial Engineering*, volume 53 of *Stochastic Modelling and Applied Probability*. Springer, 2003.

[18] Martin D. Gould, Mason A. Porter, Stacy Williams, Mark McDonald, Daniel J. Fenn, and Sam D. Howison. Limit order books. *Quantitative Finance*, 13(11):1709–1742, 2013.

[19] Robin Hanson. Combinatorial information market design. *Information Systems Frontiers*, 5(1):107–119, 2003.

[20] Eyal Hertzog, Guy Benartzi, and Galia Benartzi. Bancor protocol. 2017.

[21] Hertzog, Eyal and Benartzi, Guy and Benartzi, Galia. Bancor V2. 2020.

[22] IDEX. Idex 2.0: The next generation of non-custodial trading. 2019.

[23] Antonio Juliano. dydx: A standard for decentralized margin trading and derivatives. 2017.

[24] Robert Leshner and Geoffrey Hayes. Compound: The money market protocol. Technical report, February 2019.

[25] Stefan Loesch and Nate Hindman. Bancor protocol v2.1: Economic and quantitative finance analysis. 2020.

[26] Fernando Martinelli and Nikolai Mushegian. Balancer: A non-custodial portfolio manager, liquidity provider, and price sensor. 2019.

[27] Abraham Othman. Automated market making: Theory and practice. *Ph.D. Thesis. Carnegie Mellon University.*, 2012.

7.7. Risk Management Strategies for Decentralized Networks

AUTHORS:

Luminata Tudose

SEBA BANK

®Risk Management Strategies for Decentralized Networks (Luminita Tudose, September 2023)

INTRODUCTION

Decentralized networks, especially in the realm of Decentralized Finance (DeFi), have experienced an exhilarating surge in growth and innovation in recent years. It's an exciting frontier, but one that comes with its own set of risks. In this article, we will explore risk management strategies for decentralized networks.

Before we dive into risk management, let's get a grasp of what decentralized networks are all about. These networks, powered by blockchain technology, offer financial services without relying on traditional intermediaries like banks. But here's the catch – this very innovation brings forth vulnerabilities.

One of the most significant risks in decentralized networks is the prevalence of high leverage. Users can easily leverage their investments through lending and trading platforms, potentially amplifying their gains. However, this also introduces a considerable amount of procyclicality. When the market takes a turn for the worse, the pressure to reduce debt can force asset liquidations, pushing prices further down. The interconnected nature of DeFi applications can amplify these distress signals, exposing the vulnerability of the system.

To navigate these risks effectively, you need to be vigilant, especially given the unique characteristics of decentralized networks. Staying informed about your exposure levels and maintaining risk buffers are essential precautions to withstand the ebbs and flows of the market.

Ever since I stumbled upon the world of cryptocurrencies a few years back, I've been utterly fascinated by the promise of decentralized networks. Picture a world where you don't need a central authority, like a bank or a big corporation, to validate or oversee transactions. That's the beauty of decentralized networks. It's a world where trust is built on the consensus of many, rather than the word of one.

I personally believe in the transformative power of this technology. It feels like a breath of fresh air, especially when you think about how much control traditional institutions have over our financial lives. With blockchain technology at its core, decentralized networks offer transparency.

Every transaction, every movement, is right there for anyone to verify. It's like an open book, and as this is revolutionary.

Decentralized networks operate based on the principle of distributed control, meaning decision-making is spread across multiple nodes or participants rather than being concentrated in a single entity. In the realm of blockchain technology, this implies that data or transaction verification doesn't rely on a central authority, like a bank, but rather on the consensus of multiple participants in the network.

This structure offers the advantages of increased security, transparency, and resistance to censorship. Since data is stored across multiple nodes, it becomes harder for any single participant or attacker to alter the data without the consensus of the majority. Additionally, transactions and data are transparent to all participants, leading to increased trust and verifiability.

However, decentralized networks aren't without challenges. The lack of a central authority can sometimes lead to slower decision-making processes, and the openness of these networks can make them susceptible to attacks if not properly secured.

In the context of Decentralized Finance (DeFi), these networks are powering a new wave of financial products and services that don't rely on traditional intermediaries. This has opened up financial systems to a broader global audience, reduced fees, and created new innovative financial products. However, as with any new technology, there are risks involved, which is why understanding and implementing risk management strategies is vital.

Now, let's talk about stablecoins – a cornerstone of decentralized networks. They aim to maintain a stable value by pegging them to reserve assets. However, they inherently suffer from liquidity mismatches. These mismatches arise from differences in risk between the underlying collateral and the stablecoin liabilities. It's a vulnerability akin to traditional intermediaries like money market funds, where investors expect immediate redemption at par value.

The extent of these vulnerabilities depends on the design of the stablecoin. Some are backed by short-term securities with illiquid secondary markets, while others rely on volatile collateral like cryptocurrencies. Overcollateralization helps mitigate these risks, but extreme volatility events can erode these buffers, potentially sparking investor runs.

Decentralized networks, particularly in the domain of Decentralized Finance (DeFi), present a transformative approach to financial systems, eliminating the need for traditional intermediaries and providing more transparent and accessible financial services. However, this innovation is accompanied by unique vulnerabilities and risks. Effective risk management strategies, including diversification, due diligence, maintaining risk buffers, real-time monitoring, regulatory compliance, and stress testing, are imperative for participants to navigate this rapidly evolving ecosystem successfully and maximize its potential benefits.

RISK MANAGEMENT STRATEGY

Now, let's dive into the risk management strategies.

The importance of a robust management strategy in the cryptocurrency world cannot be overstated. Cryptocurrencies are notoriously volatile, with price swings of 10%, 20%, or even more in a single day not being uncommon. This volatility stems from factors such as regulatory news, technological advancements, market sentiment, and macroeconomic indicators. Without a clear management strategy, an investor can quickly find themselves in a position of significant loss.

As we all know, unlike traditional financial markets, the cryptocurrency market never sleeps, it operates 24/7. This means that changes can occur at any time of the day or night. An effective management strategy will take this continuous operation into account, ensuring that one is not caught off-guard by sudden market movements during off-hours.

Additionally, the crypto ecosystem is relatively young and still maturing. New projects and coins are continuously being launched, and not all of them have long-term viability. It's crucial for investors to have a strategy that helps them evaluate which projects are worth investing in and which ones might be more speculative or even potentially fraudulent.

Regulatory concerns also play a significant role. The regulatory landscape for cryptocurrencies is constantly evolving, and a sudden change in regulations in a major market can significantly impact cryptocurrency prices. Being aware of potential regulatory shifts and having a strategy to manage investments in light of these shifts is crucial.

Liquidity is another concern. While major cryptocurrencies like Bitcoin and Ethereum are highly liquid, many altcoins might not have the same level of liquidity. This can make it challenging to

exit a position without impacting the price significantly. A sound management strategy will ensure that one is not overly exposed to illiquid assets.

Furthermore, with the rise of DeFi (Decentralized Finance) platforms, there are more opportunities – and risks – than ever before. While these platforms can offer impressive returns, they also come with their own set of vulnerabilities, such as smart contract bugs. Having a management strategy can help in assessing the risk-reward ratio of participating in these platforms.

In the ever-evolving landscape of cryptocurrencies, there have been recent mishaps that emphasize the necessity of a solid management strategy. Take the case of the KuCoin hack in 2020, where the exchange lost an estimated $281 million due to a security breach. This incident reminds us that even well-regarded platforms can be vulnerable.

Another example is the collapse of the Iron Finance stablecoin project in 2021. Marketed as a partially collateralized stablecoin, a sudden and sharp drop in the token's collateral led to a "bank run" scenario. Investors rushed to redeem their tokens, causing the value of the stablecoin to plummet dramatically, and leading to significant losses for many involved.

These instances highlight that while the crypto space offers numerous opportunities, it is also fraught with risks. Exchanges can be hacked, and projects, even those that appear sound on the surface, can collapse due to unforeseen vulnerabilities or market dynamics. It underscores the absolute necessity of a robust and dynamic management strategy for anyone venturing into the world of digital assets.

While the cryptocurrency world offers vast opportunities for growth and diversification, it also presents unique challenges. A well-thought-out and adaptable management strategy is not just beneficial—it's essential for anyone looking to navigate this dynamic and ever-evolving space successfully.

Diversification is one of the golden rules in risk management for decentralized networks. Imagine having a substantial investment in a single DeFi lending platform. If that platform runs into unexpected problems, like a smart contract vulnerability or regulatory challenges, your entire investment could be in jeopardy. To mitigate this, spread your holdings across multiple DeFi platforms. For instance, consider allocating your funds to lending protocols like Aave,

Compound, and MakerDAO. This way, you're diversifying your Diversification, a time-honored principle in traditional finance, finds critical importance in the rapidly evolving world of decentralized networks, particularly in the Decentralized Finance (DeFi) space. As the saying goes, "Don't put all your eggs in one basket," and this is especially pertinent when navigating the dynamic waters of blockchain and smart contract-based platforms.

In the rapidly evolving landscape of cryptocurrencies historical events offer crucial lessons about the perils of over-concentration. The debacle surrounding the Mt. Gox exchange is perhaps one of the most illustrative examples of how things can go terribly wrong when one fails to diversify their investments.

Mt. Gox, once the largest Bitcoin exchange globally, declared bankruptcy in 2014 after a massive security breach. This breach resulted in the loss or theft of approximately 850,000 Bitcoins (following Bloomberg, the amount varies depending on the source between 740,000 and 850,000), a staggering sum equivalent to hundreds of millions of dollars back then. The fallout was immense, with many traders and investors, who had the lion's share of their Bitcoin holdings on this single platform, facing ruinous losses. Their confidence was shattered, and the crypto world received a stern wake-up call about the dangers of centralization and the lack of diversification.

Similarly, while not a bankruptcy, there were concerns in the past surrounding exchanges like Bitfinex when they faced issues related to their tether (USDT) reserves. Some traders and investors who had substantial portions of their holdings in tether on Bitfinex found themselves in a precarious situation.

Bringing our attention to DeFi, the principle remains as relevant. For instance, if one were to invest heavily in a single DeFi lending platform and that platform encountered unexpected issues, such as a smart contract vulnerability or regulatory hurdles, the implications could be disastrous. An illustrative example here would be the various DeFi projects that have been "rug pulled" or had coding vulnerabilities exploited, leading to massive losses for users.

Against this backdrop, the wisdom in diversifying one's crypto holdings becomes abundantly clear. Spreading investments across several platforms and protocols is a sound strategy. Allocating funds to established lending protocols like Aave, Compound, and MakerDAO, in

addition to others, can provide a buffer against the failure of any single platform. Beyond just diversifying across platforms, one should also consider diversifying across various cryptocurrencies, tokens, and even traditional assets.

The essence of diversification is not just a fundamental investment principle; it's an essential protective strategy in the inherently volatile and unpredictable world of cryptocurrencies and DeFi. Embracing diversification can be the difference between safeguarding one's wealth and seeing it vanish in the face of unforeseen market adversities.

In the domain of Decentralized Finance, the risks are exceptionally pronounced. This burgeoning sector is breaking barriers, offering users unprecedented financial freedom, transparency, and opportunities for high returns. But with great opportunities come great risks. Unlike traditional financial institutions that have stood the test of time and are backstopped by regulatory safety nets, many DeFi platforms are relatively young, operating in a space where regulatory clarity is still emerging. This makes them susceptible to a myriad of unforeseen challenges.

Consider the smart contract. It is a marvel of programming, facilitating automated, trustless transactions on the blockchain. But it's also code, and like all code, it's susceptible to bugs and vulnerabilities. A flaw in a smart contract could be exploited, leading to significant financial losses for users. If you've parked all your digital assets in a single DeFi platform and that platform's smart contract is compromised, the consequences could be devastating.

Furthermore, the regulatory environment for DeFi is still a work in progress in many jurisdictions. As governments and regulatory bodies around the world grapple with how to classify and oversee these platforms, DeFi services could find themselves facing legal challenges or operational disruptions. A platform you're heavily invested in might suddenly have to navigate regulatory headwinds, which can introduce uncertainties to its performance and stability.

Given these complexities, diversifying one's holdings across multiple DeFi platforms isn't just wise—it's essential. By spreading your investments, you're not only managing risks associated with individual platforms, but you're also positioning yourself to capture diverse opportunities in the market.

For instance, Aave might offer certain advantages in terms of lending rates or unique financial products, while Compound could provide better liquidity or more collateral options. MakerDAO,

on the other hand, might have its unique governance token dynamics and stability mechanisms. By allocating funds across these platforms, an investor can benefit from the strengths of each, while also ensuring that a mishap in any single platform doesn't spell disaster for their entire portfolio.

Moreover, diversification in the DeFi space isn't just about spreading funds across platforms. It's also about understanding the underlying assets, the collateral types, the governance models, and the community engagement of each platform. A well-diversified DeFi portfolio considers all these variables, ensuring a robust and resilient approach to investment.

As the DeFi landscape continues to evolve, the importance of diversification cannot be overstated. While the allure of high returns and innovative financial products might tempt investors to go all-in on a single platform, the wise strategy lies in diversification. It's a principle that has safeguarded investors for generations and remains a golden rule in the nascent world of decentralized finance. risk and reducing the impact of a single platform's failure on your overall portfolio.

Due diligence is the backbone of smart investing in the DeFi world. Before diving into any platform, protocol, or stablecoin, conduct thorough research. Take a new DeFi project promising high returns, for example. Without due diligence, you might rush in and expose yourself to scams or vulnerabilities. Instead, read the project's whitepaper, analyze independent audit reports, and scrutinize the development team's backgrounds. Assess the security mechanisms they've implemented and understand their governance structure. Armed with this knowledge, you can make informed decisions and manage risks effectively.

Navigating the DeFi landscape can be likened to venturing into a vast, promising, but occasionally treacherous jungle. The allure of high returns can sometimes overshadow the inherent risks, leading to hasty decisions. This is where due diligence comes into play, acting as the trusted guide for anyone journeying through this financial wilderness.

The first and foremost step is to resist the initial urge of diving headlong into any project, especially if it promises moonshot returns. History has shown that in the world of finance, and especially so in DeFi, if something sounds too good to be true, it often is. This isn't to say that

every project with high returns is dubious, but rather that they require a more significant degree of scrutiny.

The DeFi landscape is akin to the wild west of finance: full of opportunities but equally riddled with pitfalls. Over the years, the age-old adage "if it sounds too good to be true, it probably is" has proven its mettle time and again. In the rapidly evolving world of DeFi, this couldn't be truer. A high return might entice even the most seasoned investors, but it's essential to approach such projects with a heightened sense of caution.

For instance, the DeFi project Yam Finance, despite its initial success, faced a severe bug in its code shortly after launch. This flaw in the smart contract led to the protocol being unmanageable and resulted in a loss of confidence. Many users, attracted by the novelty and potential high yields, found themselves caught off guard.

Another case in point is the SushiSwap saga. While not a scam in the traditional sense, it drew significant attention when its anonymous founder sold a large portion of their tokens, causing a sharp drop in the token's value. The event stirred debates around trust, anonymity, and the importance of transparency in DeFi projects.

These examples underscore the inherent risks in the DeFi space. It's essential not only to be enticed by the allure of high returns but to arm oneself with comprehensive knowledge about the project. This involves understanding the project's fundamentals, the team behind it, the technology underpinning it, and its overall viability in the marketplace. And, as these recent cases illustrate, due diligence is not just advisable; it's imperative.

Starting with a project's whitepaper is crucial. This document should lay out the project's goals, architecture, tokenomics, and roadmap. While technical jargon might be overwhelming to newcomers, the whitepaper's clarity and depth can give an initial sense of the project's seriousness and intent. A hastily put-together whitepaper, or one that doesn't adequately explain its mechanics, can be a red flag.

But a whitepaper is just the tip of the iceberg. Independent audit reports are the next checkpoint. These reports, often conducted by reputable firms, dive deep into the project's code and mechanics, identifying potential vulnerabilities and pitfalls. A project that hasn't undergone an audit or, worse, has ignored the recommendations from an audit, can signal potential trouble.

One of the most notorious cases illustrating the dangers of disregarding audits or their recommendations in the DeFi space is the DAO (Decentralized Autonomous Organization) incident. The DAO was a venture capital fund set up on the Ethereum blockchain, where decisions would be made by members holding DAO tokens. It attracted a significant amount of attention and capital, raising over $150 million in a crowdfunding campaign in 2016. It was hailed as a revolutionary step in automating organizational governance and decision-making.

However, the code behind the DAO had vulnerabilities. Although some community members and experts raised concerns about potential attacks, these were largely overlooked or underestimated. Not long after its launch, an unidentified attacker exploited one of these vulnerabilities, draining over 3.6 million Ether (which was worth around $70 million at the time) from the DAO into a "child DAO."

The community was in turmoil. This event was significant not just because of the funds involved, but because it exposed the inherent risks of smart contracts and the dangers of proceeding without thorough, third-party audits. Even if a project undergoes an audit, it's crucial to address the identified vulnerabilities and not just dismiss them.

To remediate the situation and prevent the attacker from accessing the funds, the Ethereum community eventually decided on a hard fork, returning the stolen Ether to the original investors and leading to the split of Ethereum into two blockchains: Ethereum (ETH) and Ethereum Classic (ETC).

The DAO incident is a stark reminder that projects, especially in the nascent world of DeFi, must prioritize security and heed the recommendations of audits. Failure to do so can lead to catastrophic consequences, not just for the project itself but for the broader ecosystem.

Yet even a robust whitepaper and a clean audit report don't give the complete picture. The humans behind the project, the development team, play a pivotal role. Who are they? What's their track record? Have they been involved in other successful projects, or is their history mired in failed ventures or even scams? Knowing who's steering the ship can provide insights into where it might be headed.

Furthermore, understanding the security mechanisms in place is crucial. With DeFi, smart contracts play a pivotal role. Ensuring that these contracts have been thoroughly vetted and that

there are mechanisms in place to address potential breaches can spell the difference between a secure investment and a disastrous one.

Lastly, governance structure shouldn't be overlooked. Decentralization is a key tenet of DeFi, but how decisions are made and who gets to make them can heavily influence a project's trajectory. Understanding whether governance is truly decentralized or if there's potential for manipulation by a few stakeholders can be a determining factor in the project's long-term viability.

In essence, due diligence isn't just a cursory glance at a project's flashy website or its promises of astronomical returns. It's an in-depth, meticulous process that, when done right, offers investors the best possible protection against the inherent risks of the DeFi world. Armed with thorough research and an understanding of a project's intricacies, one can confidently step into the DeFi arena, poised to capitalize on its opportunities while being well-shielded from its potential pitfalls.

Maintaining risk buffers or collateral is a smart strategy for weathering market turbulence. Leverage can amplify your gains, but it also heightens the risk of forced liquidations in unfavorable market conditions. You might find yourself in a situation where your assets are sold off to cover outstanding debt, leading to losses. To safeguard against this, make sure you have enough collateral to absorb market swings without triggering forced liquidations.

Navigating the tumultuous seas of the financial markets, particularly the decentralized finance sector, demands not just foresight but also prudent preparedness. At the heart of this preparedness is the concept of risk buffers or collateral, which act as a safety net for investors venturing into high-volatility terrains.

In the exhilarating world of DeFi, the allure of leverage often tempts many. After all, leveraging, or borrowing funds to amplify potential profits, can significantly magnify one's returns. Picture a scenario where a small price increase in an asset can double or even triple your gains due to the additional funds you've borrowed. Such prospects are undeniably enticing.

However, like the two faces of a coin, with these heightened rewards comes heightened risk. Leverage, while a powerful tool for magnification of returns, also magnifies losses. This dual-edged nature becomes particularly evident during market downturns. A slight decline in asset value can put leveraged positions in danger, and if the value of your investment falls below a

certain threshold, you might be subject to forced liquidations. In simple terms, this means that the platform will sell off your assets, often at a less-than-ideal price, to recover the borrowed amount. Such events can be financially devastating, turning what seemed like a strategic move into a regrettable decision.

Experience in trading or investing plays a pivotal role in shaping how one navigates the complexities and pitfalls associated with financial instruments like leverage. It's akin to a seasoned captain maneuvering a ship through stormy seas, where intuition, knowledge of past storms, and the ability to make calculated decisions become crucial survival tools.

For beginners, the mechanics of leverage can be deceptive. The allure of exponential gains can blindside the inexperienced, making them overlook the proportional risk. An experienced trader, on the other hand, has felt the sting of a bad leveraged position or has witnessed the rapid unraveling of an over-leveraged portfolio. These past experiences, often accompanied by financial losses and the emotional turmoil they induce, imprint valuable lessons. They teach the trader about the significance of risk management, the necessity to set stop losses, and the importance of not overextending oneself.

Furthermore, experienced traders or investors have often developed a keen sense for market sentiment. They've learned, sometimes the hard way, that markets can be irrational longer than one can remain solvent. This understanding makes them wary of over-leveraging, especially during times of extreme market euphoria or pessimism.

Beyond just understanding the mechanics, experience also equips traders with emotional resilience. The psychological toll of watching a leveraged position move against you is immense. Panic can quickly set in, leading to rash decisions like closing a position prematurely or, worse, doubling down in hopes of recovery. An experienced individual, having faced such situations before, is better equipped to manage these emotional roller coasters. They know the importance of sticking to a predefined strategy, being patient, and making decisions based on logic rather than emotion.

Experienced traders are more likely to be aware of the broader market landscape. They might have a better grasp on macroeconomic factors, understand the interplay between different assets, and be more attuned to news or events that could impact their leveraged positions. This holistic

view can be invaluable in preempting potential market downturns or recognizing when a correction is just a temporary blip rather than a prolonged downturn.

Essentially, while tools like leverage level the playing field, allowing both novices and experts to amplify their potential returns, it's the wealth of experience that often determines who sails smoothly and who capsizes. The intricacies of financial markets demand respect, and it's through experience – both the victories and the scars – that traders learn to navigate them with prudence and finesse.

Navigating the financial markets, especially with tools like leverage, is akin to sailing in unpredictable seas. While the promise of greater returns can be tempting, it's crucial to remember that greater rewards often come with increased risks. I've observed that those who approach these waters with respect, armed with experience and knowledge, tend to fare better. In my opinion, leverage should be used judiciously. Like a sharp knife, in the hands of a novice, it can cause harm; but in the hands of an expert, it's a powerful tool. Always prioritize learning and understand the risks before diving deep.

The good news is that unfortunate outcomes, likes the ones previously mentioned, are avoidable. The key lies in maintaining ample collateral. Think of collateral as the anchor that holds a ship steady during a storm. Collateral is a fundamental concept in the world of finance, acting as a safety net for lenders and providing confidence in the lending process. It's an asset pledged by a borrower to secure a loan, ensuring that the lender can recoup their funds should the borrower default.

This mechanism not only facilitates the flow of credit in various markets but also plays a pivotal role in determining the terms of loans, including interest rates and borrowing limits. In today's rapidly evolving financial landscape, especially in decentralized finance, the nuances of collateral have taken on new dimensions, but its core purpose remains the same: to provide security in transactions.

By ensuring that you have an adequate amount of assets or "buffer" in your account, you create a cushion that can absorb the wild swings of the market. This cushion ensures that even if asset values dip temporarily, you aren't immediately at risk of having your assets liquidated.

The amount of collateral held by major exchanges can have a significant impact on the overall cryptocurrency market. If a large exchange faces issues, whether they be technical glitches, security breaches, or regulatory challenges, the vast amount of collateral they manage could be at risk, which could, in turn, affect market sentiment and prices.

While the DeFi world offers unprecedented opportunities, it also demands a new level of vigilance. By understanding the mechanics of leverage and the importance of collateral, investors can strike a balance between pursuing ambitious returns and ensuring that they are shielded from the harshest blows the market might deliver. In this dynamic environment, a well-maintained risk buffer doesn't just offer protection; it provides peace of mind.

Real-time monitoring is a game-changer in decentralized network risk management. With monitoring tools and analytics platforms, you can track your exposure and portfolio performance as events unfold. For instance, if you've provided liquidity to a decentralized exchange and are earning fees, real-time data can help you spot changes in liquidity demand or unexpected protocol issues. This proactive approach empowers you to identify and respond to market conditions swiftly.

In today's rapidly changing decentralized financial landscape, having the ability to monitor events in real-time isn't just a luxury; it's a necessity. The inherently volatile nature of cryptocurrencies and the myriad of intricate operations on decentralized networks mean that situations can change in the blink of an eye. Whether it's a sudden surge in a token's value or an unforeseen vulnerability in a smart contract, events within the blockchain ecosystem can unfold at a blistering pace.

Enter real-time monitoring. The advent of sophisticated monitoring tools and analytics platforms has revolutionized the way investors and stakeholders engage with decentralized networks. These tools offer a live window into the heart of your investments and allow you to observe the nuanced shifts in market dynamics as they happen. No longer do you need to be caught off guard by sudden market changes or await updates that may arrive too late to be of any actionable use.

If we consider the scenario of providing liquidity on a decentralized exchange, a popular activity in the DeFi world. As you contribute assets to a liquidity pool, you're rewarded with fees based on the volume of trade that leverages your liquidity. In such an environment, it's crucial to

understand the demand for liquidity and any changes in that demand. If, for example, there's a sudden spike in trading volume or if a major liquidity provider withdraws a significant amount, the dynamics of the pool can change dramatically. Without real-time insights, you might miss these shifts, potentially leaving your assets exposed to heightened risks.

Moreover, the decentralized nature of these platforms means that they don't have centralized control, making them susceptible to unexpected protocol issues or vulnerabilities. With real-time monitoring, you can be alerted instantly to anomalies or suspicious activities, enabling you to make prompt decisions, such as withdrawing your funds or adjusting your stake.

The beauty of these real-time monitoring tools is that they turn reactive measures into proactive strategies. By always being in the loop, investors can make decisions that are not only timely but also informed by the latest data. As the DeFi space continues to expand and evolve, such vigilant monitoring becomes the linchpin of effective risk management, ensuring that participants can navigate the complexities of decentralized networks with confidence and agility.

Market makers are instrumental figures in the financial landscape, ensuring that assets within a market can be readily bought or sold without triggering dramatic price shifts. Their primary role is to infuse markets with liquidity, creating a smoother trading experience for everyone involved. This function is essential for both traditional financial systems and newer decentralized frameworks.

Within the decentralized finance (DeFi) ecosystem, the role of market makers gets a slight twist. By depositing assets into liquidity pools on these platforms, individuals can earn fees based on the trading activity that utilizes their provided liquidity.

The benefits that market makers bring to the table are manifold:

- They ensure price stability. By maintaining consistent buy and sell orders, market makers act as a buffer against erratic price volatility. This stabilization is particularly valuable in the cryptocurrency domain, which can be subject to rapid price swings.
- Market makers enhance the efficiency of trades. With an ample reservoir of liquidity at their disposal, trades can be executed swiftly without the necessity of waiting for a counterpart. This fluidity is especially crucial in markets known for their quick movements, allowing traders to adapt to changing conditions rapidly.

High liquidity levels, often attributed to active market makers, can act as a beacon, drawing in further participation from traders and investors. When individuals observe that a market is well-liquidated, it fosters confidence, indicating that entering or exiting positions won't be a cumbersome process.

In the context of real-time monitoring within decentralized networks, market makers play a pivotal role. Their constant involvement and provision of liquidity can serve as an early indicator of shifts in market sentiment or demand. Monitoring tools that track liquidity changes or trading volumes can provide insights into the actions and strategies of market makers, offering a more comprehensive understanding of the market's current state. Thus, understanding the movements and decisions of market makers can be a valuable tool for any investor or trader in the decentralized space.

Staying informed about evolving regulations is crucial in the DeFi space. Non-compliance with Anti-Money Laundering (AML) and Know Your Customer (KYC) requirements can lead to legal and financial risks. For instance, using a decentralized exchange that requires KYC verification might seem inconvenient, but ignoring it exposes you to regulatory risks. To mitigate this, align your DeFi activities with regulatory expectations and comply with applicable laws and regulations.

Navigating the intricate labyrinth of decentralized finance requires more than just an understanding of smart contracts or yield farming. At its heart, it necessitates a thorough comprehension of the evolving regulatory landscape that envelops it. As the DeFi space burgeons, so does the regulatory scrutiny, making it imperative for participants to remain on their toes.

Switzerland, known for its progressive stance on financial innovations, has been at the forefront of shaping a regulatory framework conducive for the growth of digital assets and blockchain technologies. While the Swiss authorities have been supportive, they've equally emphasized the significance of robust risk management, particularly in the realm of Anti-Money Laundering (AML) and Know Your Customer (KYC) norms.

These AML and KYC requirements, though they may seem cumbersome, serve a pivotal role in ensuring that the financial systems aren't misused for illicit activities. A decentralized exchange

might offer the allure of swift, permissionless transactions, but when it comes to platforms that mandate KYC verifications, the underlying rationale is to instill a layer of transparency and accountability.

Now, some DeFi enthusiasts might argue that the very essence of decentralized systems is to operate devoid of intermediaries and traditional gatekeepers. But herein lies the conundrum. As the DeFi ecosystem intertwines more with the traditional financial world, the call for regulatory clarity intensifies. Ignoring or bypassing these regulatory mandates doesn't just jeopardize the individual's position but can also cast a shadow over the entire project or platform in question.

In a rapidly evolving environment, where regulatory stances can shift, being oblivious or choosing to remain in the dark is not an option. Legal repercussions, hefty fines, or even criminal charges aren't mere theoretical threats. They hold tangible implications for those who flout the rules.

But it's not just about circumventing risks. Aligning DeFi operations with regulatory norms also fosters trust. For the broader public to embrace decentralized financial products, they need the assurance that these platforms respect and adhere to the same standards of integrity and security as their centralized counterparts.

As the decentralized finance realm continues its ascent, its participants must juggle innovation with compliance. The onus is on them to be proactive, to educate themselves, and to synchronize their activities with the regulatory rhythm. Only by marrying the decentralized ethos with regulatory prudence can the DeFi space truly unlock its transformative potential.

Stress testing is like a safety net for your investments. It involves simulating extreme market conditions to see how your portfolios would perform under adverse scenarios. Imagine a scenario where the prices of assets in your portfolio sharply decline simultaneously. Through stress testing, you can identify weaknesses in your risk management strategy and make informed adjustments to your portfolio.

Stress tests, by their nature, are hypothetical scenarios designed to gauge the resilience of financial institutions and portfolios under extreme conditions. Their efficacy is a topic of some debate among financial experts, especially when drawing parallels between the decentralized

finance (DeFi) space and traditional financial markets. In traditional financial markets, stress tests became particularly significant after the 2008 global financial crisis.

Regulatory authorities, especially in the U.S. and Europe, introduced rigorous stress testing for banks to ensure they held enough capital to weather severe economic downturns. These tests have been credited with bolstering the banking system by forcing institutions to maintain higher capital reserves and rethink certain risk-prone strategies.

However, there are criticisms. Some argue that these tests can give a false sense of security. They contend that it's nearly impossible to accurately predict every possible adverse scenario and that the very nature of black swan events — rare and unpredictable occurrences — means they often fall outside the parameters of most stress tests. This sentiment was echoed during the onset of the pandemic, a stressor not accounted for in many models, which caused significant financial turmoil.

Furthermore, the effectiveness of stress tests in traditional markets is closely tied to the accuracy of the models used and the assumptions underpinning them. If the models are too optimistic or if they don't capture all potential risks, the stress tests can be misleading.

Stress testing is the financial world's equivalent of strapping into a rollercoaster, without the fear of gravity pulling you down. It's the "what if" game we play with our investments, thrusting them into a series of hypothetical tempests to see if they'll weather the storm or crumble like a cookie in milk. Think of it as taking your portfolio for a trial run in the worst-case scenario Olympics.

Now, imagine you're holding a basket of stocks, and each stock is like an egg. Stress testing is like shaking that basket vehemently to see if any of those eggs crack. If they do, well, you might want to reconsider placing all your eggs in that particular basket. And let's be honest, nobody wants scrambled investments.

The beauty of stress testing is that it exposes the chinks in our financial armor. It reveals those assets in our portfolio that might not be as resilient as we thought they were. In many ways, it's a reality check, a financial mirror that reflects back our over-optimism or under-preparedness.

Stress testing is a bit like a financial horoscope - it predicts a potential future, but it's up to you whether you believe it or act on it. But unlike horoscopes, it's always better to take the results of a

stress test seriously. After all, Saturn retrograde might mess with your mood, but it won't impact your Bitcoin!

In my opinion, while stress testing might seem like a tedious process, it's an essential tool in the investor's toolkit. It pushes us to be more proactive and less reactive. It challenges us to think beyond the rosy predictions and confront the possible financial nightmares head-on. By doing so, we not only strengthen our investment strategy but also bring a sense of confidence and clarity to our financial journey.

Now, let's look forward to some emerging trends and developments in decentralized networks.

One exciting development is Decentralized Identity (DID), which gives individuals full control over their digital identities. This reduces reliance on centralized entities for identity verification, and we can expect widespread adoption across various applications.

Efforts are underway to enhance cross-chain communication, breaking down the barriers between different blockchain ecosystems. This will open up new possibilities for DeFi and other applications.

Layer 2 scaling solutions like Optimistic Rollups and zk-Rollups are gaining traction, promising more efficient and affordable decentralized networks.

Decentralized Autonomous Organizations (DAOs) are on the rise, allowing participants to have a direct say in network upgrades and changes. Expect to see more community-driven projects.

Regulations are evolving, impacting how participants engage with decentralized networks. Staying informed will be essential for risk management.

Non-Fungible Tokens (NFTs) are expanding beyond art and entertainment, finding applications in real estate, intellectual property rights, and virtual reality.

DeFi will continue to evolve with improved user experiences, enhanced security measures, and a broader range of financial products.

Environmental concerns related to blockchain energy consumption are gaining attention, pushing for more eco-friendly practices.

CONCLUSION

As decentralized networks continue to evolve, staying ahead of these trends and adapting your risk management strategies accordingly will be vital. It's an exciting journey, but one where careful risk management is your compass to navigate the terrain successfully. Decentralized networks are here to stay, and with the right approach, they can transform the financial landscape while ensuring trust and security.

As we could see all through this paper, in the rapidly shifting sands of the decentralized ecosystem, agility and foresight are not just virtues but necessities. With every innovation in DeFi and blockchain technology, new opportunities emerge, but so do potential pitfalls. The decentralized world is much like an unfolding chapter in the annals of financial history, rich with potential yet fraught with complexities.

Risk management, in this context, is more than just a safeguard; it is a lens through which investors and participants can evaluate decisions, measure potential outcomes, and determine the best courses of action. By continually updating and refining these strategies in response to new developments, one can ensure that they are not merely reacting to the market's ebb and flow but proactively charting a course through it.

As decentralized networks gain more traction and acceptance, their influence on global finance will undoubtedly expand. Traditional financial structures might soon find themselves adapting to or even adopting some of the principles that underlie decentralized systems. The promise of decentralization, after all, is a more inclusive, transparent, and efficient financial ecosystem.

We should keep in mind that with this promise comes a responsibility. Every stakeholder, from developers to investors, has a role to play in ensuring that these networks remain trustworthy. While decentralization champions autonomy and reduced intermediation, it also calls for heightened diligence. The absence of a centralized authority means that the onus of security, transparency, and ethical behavior lies with the community.

As we stand on the cusp of what might be a monumental shift in the way we perceive and interact with financial systems, it is essential to move forward with both optimism and caution. The decentralized future beckons, offering a horizon filled with possibilities. Embracing it with a well-calibrated compass of risk management ensures not only individual success but the

collective prosperity and integrity of the entire ecosystem. After all, in the world of decentralization, every node, every participant, and every decision contributes to the strength and resilience of the network.

Navigating the choppy waters of cryptocurrency can feel overwhelming, and you're not alone in feeling this way. Even seasoned traders from traditional markets often hesitate to dip their toes into the crypto pool, wary of its unpredictable currents. It's essential to remember that this market isn't just about quick wins; it's about understanding and respecting its unique challenges. Dive in with both eyes open, and only invest what you're genuinely prepared to part with. The crypto world can be rewarding, but it's definitely not for everyone. Stick with what you're comfortable with, and always prioritize your financial well-being. Remember, everyone's investment journey is personal, so tread at your own pace… and remember don’t trust verify!

References

Johnson, A. (2022). Decentralized Finance: Risks and Rewards. Blockchain Journal, 18(3), 45-58.

Smith, L. (2021). Due Diligence in Decentralized Finance: A Comprehensive Guide. DeFi Insights, 12(2), 33-46.

Turner, R. (2020). Risk Buffers and Collateral Management in DeFi. Crypto Risk Management, 8(1), 19-27.

White, S. (2021). Real-Time Monitoring in Decentralized Finance: Tools and Techniques. DeFi Analytics, 15(4), 65-79.

Regulatory Authority for Decentralized Finance (2022). AML and KYC Guidelines for DeFi Participants. Retrieved from [URL]

Brown, J. (2020). Stress Testing Strategies for Decentralized Portfolios. DeFi Risk Assessment, 9(3), 55-68.

Martin, D. (2022). The Psychological Aspects of Investing in Volatile Markets. Behavioral Finance Journal, 20(5), 78-85.

Zhao, C. (2019). The Transformative Role of Decentralized Exchanges in Traditional Finance. DeFi Reviews, 7(8), 42-51.

Garcia, E. (2023). A Comparative Analysis: Traditional Market Savvy Traders vs. Crypto Enthusiasts. Modern Finance, 13(4), 30-41.

Bibliography

Buterin, V. (2013). Ethereum: A Next-Generation Smart Contract and Decentralized Application Platform. Retrieved from [URL]

Antonopoulos, A. M. (2014). Mastering Bitcoin: Unlocking Digital Cryptocurrencies. O'Reilly Media.

Peterson, J. (2020). DeFi Explained: A Comprehensive Guide to Decentralized Finance. Packt Publishing.

Gensler, G. (2021). Digital Finance: New Challenges and Risks. Harvard Business Review, 87(6), 112-128.

PwC Global. (2023). Crypto Regulation Report. PricewaterhouseCoopers.

Tapscott, D., & Tapscott, A. (2016). Blockchain Revolution: How the Technology Behind Bitcoin Is Changing Money, Business, and the World. Penguin.

Casey, M.J., & Vigna, P. (2018). The Truth Machine: The Blockchain and the Future of Everything. St. Martin's Press.

DeFi Alliance. (2022). Transitioning from Traditional Finance to DeFi: A Practitioner's Guide. DeFi Alliance Publications.

7.8. Risk-Adjusted Returns of Concentrated Liquidity Automated Market Maker Liquidity Provider Positions and Forecasting Metrics for Market Simplicity.

AUTHORS:

Henry R. Fudge

Nicolas Alioth

Risk-Adjusted Returns of Concentrated Liquidity Automated Market Maker Liquidity Provider Positions and Forecasting Metrics for Market Simplicity.

Authors: Henry R. Fudge, Nicolas Alioth,

Abstract

In Concentrated Liquidity Automated Market Makers (CLAMM), such as Uniswap, Liquidity providers (LPs) deposit crypto assets. These positions often incur significant risk, including but not limited to contract risk, execution risks, and impermanent loss risk. This paper attempts to discover whether CLAMM systems deliver a fair market risk-adjusted return for LPs and generate a metric called the Fudge-Alioth ratio by which a typical investor can forecast the risk-adjusted returns of a potential allocation, using historical data.

Table of Contents

1: Introduction to Automated Market Makers

Decentralised Exchanges (DEX) come in many forms, with the largest by volume being Uniswap with 3.24 Bn in Total Locked Value as of 20th September 2023 (DeFiLlama, 2023). In March 2021, Adams, Keefer, Zinsmeister, Robinson & Salem released the Uniswap v3 core whitepaper, developing the first Concentrated Liquidity Automated Market Maker (CLAMM), which led to the release of the Uniswap v3 DEX in May 2023. Concentrated Liquidity Automated Market Makers differ from Constant Function Automated Market Makers (CFAMM) in that a liquidity provider can select a set price range (P_L to P_H) over which to provide liquidity rather than over the entire range (0, Infinity). This comes with some benefits and drawbacks.

According to Adams et al. (2021), the CLAMM system allows for deeper virtual reserves of a liquidity pool, which is reflected in tighter spreads and lower slippage compared to traditional CFAMM systems. Fritsch (2021) also demonstrates that CLAMM generates higher returns from trading fees than its CFAMM counterpart, even when accounting for bad strategies.

However, as Heimbach, Schertenleib and Wattenhofer (2022) point out, CPAMM also increases impermanent loss (divergence loss) if P_L and P_H aren't set to cover the entire price range. The trading fees generated are also disproportionately distributed around tighter price ranges, which disincentivises providing deep liquidity. Lastly, the authors conclude that the switch from CFAMM to CLAMM added complexity, creating a barrier to entry for retail participants by making profitable returns more challenging.

2: Concentrated Liquidity Automated Market Makers

Unlike CFAMM systems, CLAMM systems allow users to deploy liquidity over a set price range, extending from the lower bound (P_L) to the higher bound (P_H). The system of a CLAMM then allows a trading pair to exchange across a virtual reserve range as if it was a CFAMM pool with larger reserves, as shown in Figures 2 and 3 (Adams, Keefer, Zinsmeister, Robinson, & Salem, 2021).

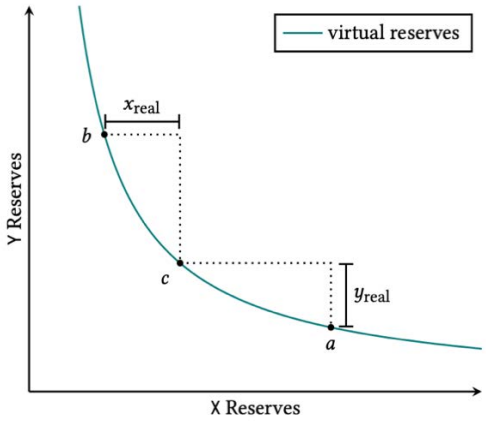


Figure 1: Simulation of Virtual Liquidity

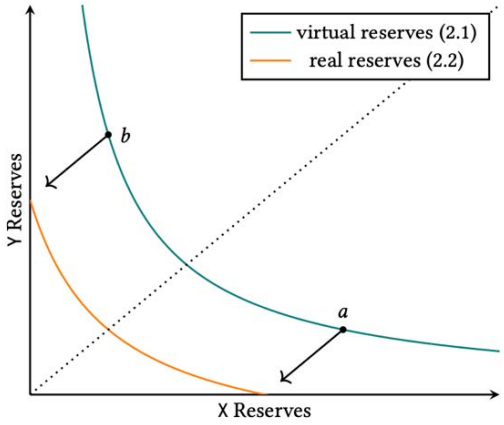


Figure 2: Real Reserves

The Uniswap v3 core whitepaper (2021) states that the real liquidity of this position, measured by value L, can be calculated as follows:

$$\left(x + \frac{L}{\sqrt{P_H}}\right)\left(y + L\sqrt{P_L}\right) = L^2 \tag{2.1}$$

Where x and y are the respective reserves of asset X and Y. To calculate x and y within the price range (P_L, P_H) the equation (2.1) can be simplified as follows:

$$x = L\,\frac{\sqrt{P_H} - \sqrt{P}}{\sqrt{P}\cdot\sqrt{P_H}} \tag{2.2}$$

$$y = L(\sqrt{P} - \sqrt{P_L}) \tag{2.3}$$

If the price moves outside of the range (P_L, P_H), the position will be entirely held in asset X or Y, which means that either x or y is 0 and the position is earning no fees. This allows us to calculate x and y regardless of the current price P when the position is out of bounds:

$$\text{When } P > P_H\text{: } y = L\left(\sqrt{P_H} - \sqrt{P_L}\right) \text{ and } X = 0 \tag{2.4}$$

$$\text{When } P < P_L\text{: } x = L\,\frac{\sqrt{P_H} - \sqrt{P_L}}{\sqrt{P_L}\cdot\sqrt{P_H}} \text{ and } Y = 0 \tag{2.5}$$

The value of the real liquidity can also be solved for each respective asset L_x and L_y from equations (2.2) and (2.3) with the following formulas:

$$L_x = x \frac{\sqrt{P} \cdot \sqrt{P_H}}{\sqrt{P_H} - \sqrt{P}} \tag{2.6}$$

$$L_y = \frac{y}{\sqrt{P} - \sqrt{P_L}} \tag{2.7}$$

The liquidity L_x and L_y are directional at each point, depending on whether the price P is on an upward or downward trend. But the general real liquidity L can be calculated for both directions using a combination of (2.6) and (2.7) as follows:

$$L = \min(L_x, L_y) \tag{2.8}$$

When allocating liquidity, it should be optimised for full utilisation of the assets in question. Using the equations (2.6), (2.7), and (2.8), with a known current market price P, a known value of x and y and a variable upper bound P_H can be calculated the corresponding lower bound P_L, which ensure the full utilisation of assets X and Y at the beginning of the positions (t_0).

$$P_L = \left(\frac{y}{\sqrt{P_H} \cdot x} + \sqrt{P} - \frac{y}{\sqrt{P} \cdot x} \right)^2 \tag{2.9}$$

Elsts (2021) also introduces the concept of 'tick mathematics'. Uniswap v3 maps the continuous space of all possible prices to a discrete subset indexed by ticks (Adams, Keefer, Zinsmeister, Robinson, & Salem, 2021). A tick has unique relation with price, defined by the tick base parameter, which is equal to 1.0001 in Uniswap v3. The price corresponding to the i-th tick is as follows:

$$P_i = 1.0001^i \tag{2.10}$$

To make this easier to read in the following equations, the tick prices quoted in (2.10) is adjusted for the number of decimals of each asset using the formula below:

$$P_{adjusted} = P \cdot 10^{Decimals\ y - Decimals\ x} \tag{2.11}$$

As an example, the equation (2.11) is used with the ETH-USDC pair. ETH (used for *x*) has 18 Decimals, and USDC (used for *y*) as 6 decimals. This would result in a price system of:

$$P_{Adj.ETH} = \frac{P_i}{10^{12}} \tag{2.12}$$

The equation (2.12) expresses the price of asset X in asset Y, which in this example is USDC in ETH terms. To find the price of ETH in USDC terms, the following equation can be used:

$$P_{\$} = \frac{1}{P_{Adj.ETH}} \tag{2.13}$$

3: Portfolio Values and Impermanent Loss.

This paper proposes the following equation to calculate the portfolio value *V* of a liquidity pool, composed of a volatile asset *x* and a stablecoin *y*, over a time period (0,1), with *P* being the price of *x* denominated in terms of *y*:

$$V_0 = P_0 x_o + y_0 \tag{3.1}$$

$$V_1 = P_1 x_1 + y_1 \tag{3.2}$$

However, as demonstrated by Fritsch (2021,) *x* and *y* will change at differing rates in CLAMM, depending on the range chosen (P_L, P_H), incurring impermanent loss (IL). To better illustrate this relationship, see Figure 3, which is a graphic representation of a simulated ETH-USDC pool showing the portfolio values calculated using a selected set of price ranges for the CLAMM LP positions over a range of ETH prices ($1334 to $3000) starting from an initial price (P_0) of $2000 per ETH, under the set condition of optimal liquidity utilisation using equation (2.9).

From this simulated market, it can be observed that the smaller the price ranges (P_H-P_L), the more severe the impermanent loss of the LP position for each relative move in ETH Market price. The impermanent loss can be seen in Figure 3 by the distance between the straight line (V^{Tilda}) and the respective curves for each price range LP position.

It is also recognisable that when the market price of ETH is above the P_H, the entire position is in USDC, giving a horizontal line against further price increases, while below P_L, the entire portfolio is in ETH, giving a directly proportional price change relative to the price of ETH below this point.

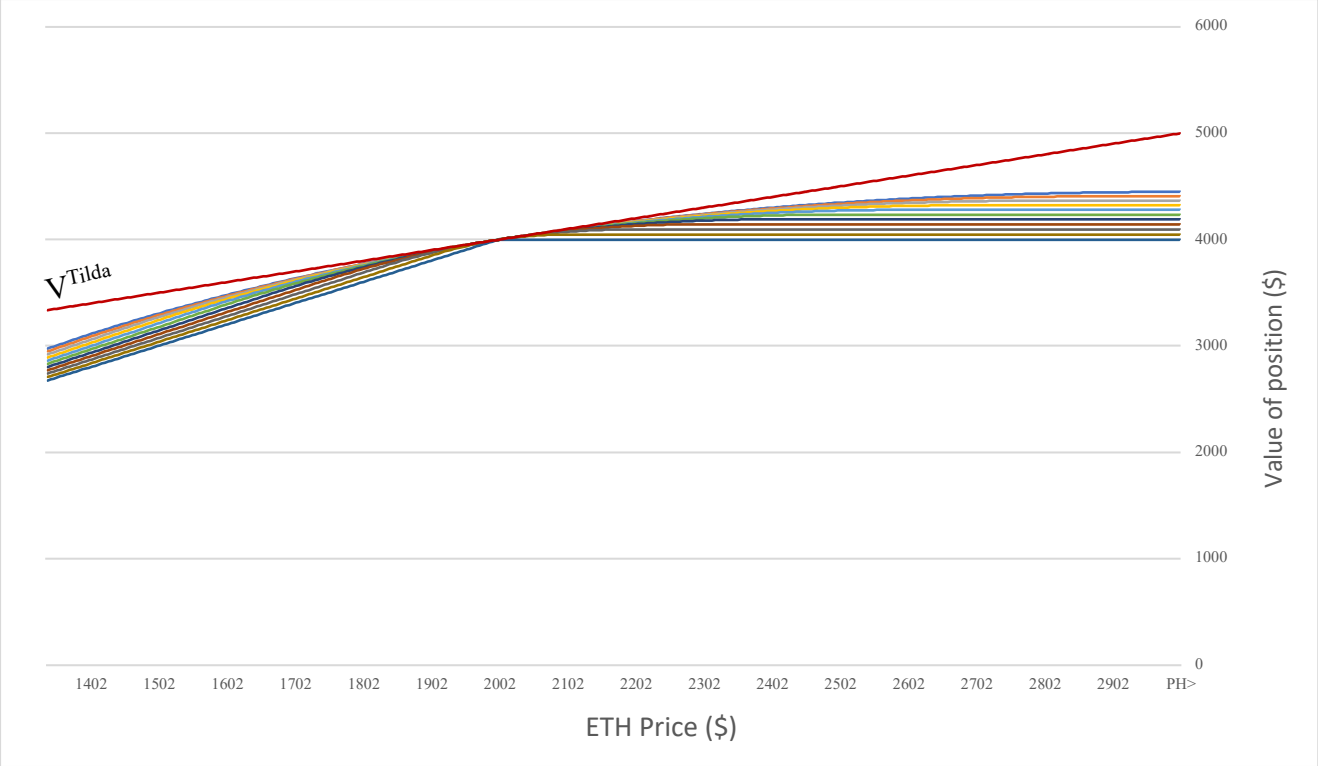


Figure 3: Impact of price ranges on the value of an LP position

It can also be seen that when the market price of ETH is above the P_H, the entire portfolio is in USDC, giving a horizontal line against further price increases, while below P_L, the entire portfolio is in ETH, giving a directly proportional price change relative to the price of ETH below this point.

This deviation in value (impermanent loss) can be expressed by the following equation:

$$IL = \frac{P_1 x_1 + y_1}{P_1 x_0 + y_0} - 1 \tag{3.3}$$

Inserting all relevant equations from (2.2), (2.3) and (2.8) factors into (3.3) for a change in price from P_0 to P_1 under the constraint of optimal liquidity utilisation from (2.9) in the initial position of X_0 and Y_0 and a known P_H, in terms of X_0 and Y_0 this becomes:

$$IL_{(0,1)} = \frac{P_1\left(L\frac{\sqrt{P_H}-\sqrt{P_1}}{\sqrt{P_1}\cdot\sqrt{P_H}}\right) + L\left(\sqrt{P_1} - \left(\frac{y_0}{\sqrt{P_H}\cdot x_0} + \sqrt{P_0} - \frac{y_o}{\sqrt{P_0}\cdot x_0}\right)\right)}{P_1 x_o + y_0} \quad - \quad 1 \tag{3.4}$$

The equation (3.4) also operates with the assumptions that the price P_0 and P_1 stay within the set price range, which we denote as follows:

$$P_1 \in (P_L , P_H) \tag{3.5}$$

$$P_0 \in (P_L , P_H) \tag{3.6}$$

4: Risks in DEX trading systems and approaches to risk mitigation

There are numerous sources of risk when trading on DEXs. Smart contract risk stems from the failure of the system due to technical or security concerns, often from front end traffic interception, re-entrancy attacks, flash-loan attacks and more (Sun, Lin, Sjöberg, & Jie, 2021). Execution risk, best known as Maximum Extractable Value (MEV) attacks, are a result of front running, back running, and sandwich attacks, which effect the execution price for traders in these systems (Yang, et al., 2023). However, this paper will focus strictly on the mathematical and financial impact of the proper operation of these systems, namely, impermanent loss.

4.1: Current approaches to risk hedging

Several studies have proposed radical systems for hedging impermanent loss such as using weighted variance swaps in Constant Product Automated Market Makers (CPAMM) (Fukasawa, Maire, & Wunsch, 2023) or creating long option straddles with strikes at the market price for CLAMM (Elsts, Liquidity Provider Strategies for Uniswap v3: Options, 2023).

However, there are many issues in the real-world implementation of these methodologies: Their applications thus far have been limited to constant product automated market makers, where impermanent loss across the price range 0 to infinite, is lower than a non-zero low price threshold or non-infinite high price threshold within CLAMM systems. The proposed systems for CPAMM systems, do not cover the greater IL risk in CLAMM systems without leverage or intensive additional structuring (0xDanr, 2022).

Both proposed models enhance other real-world risk metrics, namely in counterparty risk, relying either on external issuers of options contracts or gamma swaps, while theoretically possible, accurately calculating a real-world metric for how much risk is hedged compared to added by using such strategies is difficult to measure.

Liquidity and availability of strategy components is questionable; while options markets exist for major listed assets such as BTC and ETH, smaller market cap assets often lack derivatives coverage or sufficient coverage to offer significant proportions of LP participants in these assets to engage in hedging, meaning such strategies if functional in the real world, are thoroughly limited to pools of the largest assets, while all other pools still face these risks.

This is true for CPAMM systems and intensified in CLAMM systems, as a countably infinite range of price boundaries able to be selected over discrete intervals (ticks) creates LP positions with unique IL properties relative to the underlying, unique Delta and Gamma attributes. Even under a theoretical approach to risk hedging, gamma-swaps in CLAMM systems would struggle to have continuous market pricing for the underlying positions taken by LPs without securitisation of several discrete swaps executed for each individual CLAMM LP position covered by such a swap into a broader portfolio, or a pure peer to peer market for individual gamma swaps for all CLAMM LP Positions, a huge barrier to real-world implementation.

While Fukasawa, Maire & Wunsch (2023) and Elsts (2023) have shown that it is theoretically possible to hedge impermanent exposures, there has been little discussion on the effective returns of hedged positions. When yields from crypto-stable pools can often exceed 20% pa (DeFiLlama, 2023), little is mentioned about the total cost of options straddle strategies or gamma swaps and whether they may exceed the potential yields (total fees) generated in these strategies. In such a case where the effective cost of hedging position exceeds the fees, there is no economic logic to engage in a hedged LP position rather than simply hold the initial assets intended to be supplied as an equally weighted portfolio.

4.2: A new approach

As this paper has shown in the previous section, while theoretical approaches to hedging principal risk in DEX systems do exist, their real-world applications are sparse, their returns require further study and are often not applicable to CLAMM systems specifically. The approach of this paper is to measure the effective risk-return profiles of pool positions as a guidance metric for investors in a simplified fashion.

4.3: Risk Reward Strategy in CLAMM systems

As outlined in the Uniswap v3 core whitepaper (Adams, Keefer, Zinsmeister, Robinson, & Salem, 2021), fees from CLAMM systems are distributed across tick ranges proportionally to all LPs liquidity within the bounds of the current tick range, with fees ranging from 0.01% to 1% for different pairs in Uniswap v3. When deploying liquidity initially, the liquidity of an LP position is deployed across all tick ranges proportionally between the set high price P_H and low price P_L threshold set by an individual LP.

This creates an interesting game set-up for LPs competing for fee revenues in a pool. Running tighter boundaries of P_L and P_H focuses your liquidity on a fewer number of price ticks around the current market trading price, and proportionally generates higher relative fees, than wider ranges of P_L and P_H (Fritsch, 2021). However as seen in the previous section, impermanent loss for tighter ranges is far more severe, and if market price moves outside of this price range, the position is entirely in one asset and generates no fees.

LPs when considering their positions, must work on the trade-off of tighter price ranges for higher fees, but accept higher impermanent loss and a higher chance of the position falling out of range and generating no fees.

Fees themselves are generated from trading volumes but they exhibit weak correlation with volatility (Heimbach, Schertenleib, & Wattenhofer, Risks and Returns of Uniswap V3 Liquidity Providers, 2022), meaning for the purposes of this paper, fees are treated as an exogenous factor in our analysis.

The difficulty of such a system, is the competition for fees is to find a stable market equilibrium. A trader selects a set price range, under the assumption exogenous and predictable fees, within his own risk preference. When another trader enters as an LP with a different risk preference and price range, it will change the effective risk-reward of the initial trader's position.

Under the pretext of this 'game', Nash equilibria in the system of CLAMM would exist only under the assumption of uniform risk preferences amongst the LPs, or perfect information on the risk preferences of the other participants, and total asset allocation of all potential LPs.

A better solution may be found in the simplifying assumption that in any area where the risk-adjusted return of allocating capital as an LP in a CLAMM system is seen as fair compared with other risk markets on measurable factors with an addition for the difficult-to-quantify additional risks from the protocol to find its fair place on the efficient frontier.

In this chain of thought, the paper sees a better way forward for assessing short-term CLAMM LP positions: creating a simple metric to quantify and relatively qualify positions, a Sharpe ratio equivalent for CLAMM positions, which this paper will call the Fudge-Alioth ratio.

4.4: Defining the Fudge-Alioth Ratio

This paper suggests that the expected returns are comprised of the net result of expected impermanent loss and the expected fees generated as fair yield and can be described as follows:

$$\mathrm{E}[F] \approx \frac{\mathrm{E}[TF_d]\cdot(T_1-T_0)}{\mathrm{E}[TVL]\cdot\left(\frac{P_H-P_L}{P_L}\right)} \cdot \rho_{In\ range} \tag{4.4.1}$$

With $\mathrm{E}[F]$ being expected fees generated for the LP, $E[TF_d]$ being the expected Trading Fees for the entire pool, $\mathrm{E}[TVL]$ being the expected Total Value Locked (TVL) in the pool and $\rho_{In\ range}$ is a probability score using the normal distribution based on the statistics of the risk asset X where the price is over the P_H threshold or below the P_L meaning no fees would be generated by the position. The bounds are still contingent on optimal liquidity utilisation as laid out in equation (2.9).

As pointed out by Fritsch (2023), fees generated are inversely proportional to the spread of the range around the current market trading price, which is why an adjustment factor is created that as this spread increases, our relative fees decrease for the position, and as it decreases the fees relatively increase as a crude estimator of fees generated for the position.

When applying the above estimator to the current market situation as of 17th October 2023, even with the increased risk weighting of tighter price boundaries, reducing the boundaries of the position does offer increasing marginal returns to investors, as shown in Figure 4.

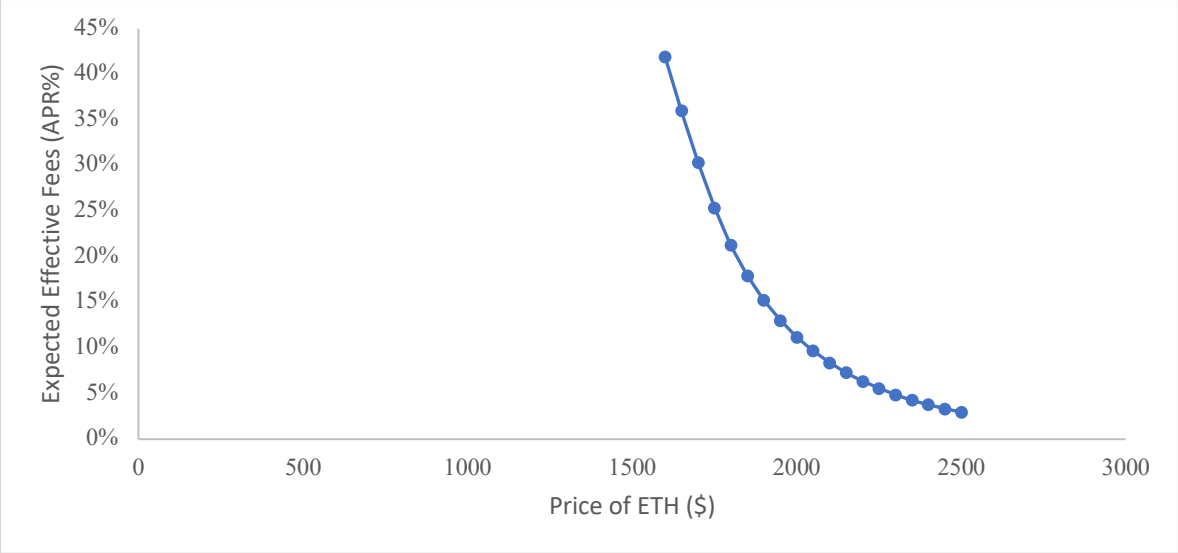


Figure 4: Expected Effective Fees by Upper price bound (ETH-USDC 17th October 2023)

For the expectation of impermanent loss, we simply need an expected value for V^1, and its composition, all taken from the future price expectation of the risk asset.

$$\mathrm{E}[V^1] = \mathrm{E}[P_1]\left(L\,\frac{\sqrt{P_H}-\sqrt{\mathrm{E}[P_1]}}{\sqrt{\mathrm{E}[P_1]}\cdot\sqrt{P_H}}\right) + L\left(\sqrt{\mathrm{E}[P_1]}-\sqrt{P_L}\right) \tag{4.4.2}$$

The generated capital appreciation can either be submitted by the user based on their own analysis for a price target, it can be estimated from historical returns, or run a Monte-Carlo simulation. For the purposes of a simple example, this paper will stick to historical returns to show the basic principles.

To generate a simple portfolio return we simply combine the equation (4.4.2) into the following formula based on Treynor (1962):

$$\mathrm{E}[R^P] = \frac{\mathrm{E}[V_1]+\mathrm{E}[F]-V_0}{V_0} \tag{4.4.3}$$

The equation (4.4.3) represents a simplistic percentage return expected from a portfolio position. After full substitution the resulting equation is:

$$\mathrm{E}[R^P] = \frac{\mathrm{E}[P_1]\left(L\,\frac{\sqrt{P_H}-\sqrt{\mathrm{E}[P_1]}}{\sqrt{\mathrm{E}[P_1]}\cdot\sqrt{P_H}}\right)+L\left(\sqrt{\mathrm{E}[P_1]}-\sqrt{P_L}\right)\;+\left(\frac{\mathrm{E}[TF_d]\cdot(T_1-T_0)}{\mathrm{E}[TVL]\cdot\left(\frac{P_H-P_L}{P_L}\right)}\right)\cdot\rho_{In\,range}-(P_0x_o+y_0)}{P_0x_o+y_0} \tag{4.4.4}$$

To fit this into a Sharpe ratio and, subsequently a Fudge-Alioth ratio to effectively position its risk reward rating, we must also derive the effective volatility of the position. However, given the underlying adjustments in the LP holdings are conditional on the price development, this paper will take a simplification from the world of options.

As pointed out in a previous chapter by Elsts (2023), the Pay-off structure of LP positions is very similar to a short put position, which is represented in Figure 5.

Figure 5: Ethereum Short Put Pay off Vs. CLAMM LP ETH-USDC pa off

With this simple approximator available, a fair market estimation of a comparable asset's volatility by referencing the implied volatility of 12-month puts on Ethereum can be pulled. Using live data from Deribit (2023), it can be seen that At the Money options, on an annual basis, are trading with an implied volatility of 46.1%, which will be used for the basis of the Fudge-Alioth ratio metric.

The original Sharpe ratio as proposed by Sharpe (1996) is described as follows:

$$Forecasting\ Sharpe\ Ratio = \frac{\mathrm{E}[R^P] - R^F}{\sigma^P} \qquad (4.4.5)$$

The Fudge-Alioth (*FA*) ratio specific to CLAMM LP positions is obtained by substituting equation (4.4.4) into equation (4.4.5) and results in:

$$\boldsymbol{FA} = \frac{\left(\frac{\mathrm{E}[P_1]\left(L\frac{\sqrt{P_H}-\sqrt{\mathrm{E}[P_1]}}{\sqrt{\mathrm{E}[P_1]}\cdot\sqrt{P_H}}\right)+L\left(\sqrt{\mathrm{E}[P_1]}-\sqrt{P_L}\right) + \left(\frac{\mathrm{E}[TF]}{\mathrm{E}[TVL]\cdot\left(\frac{P_H-P_L}{P_L}\right)}\right)\cdot\rho_{In\ range}-(P_0x_o+y_0)}{P_0x_o+y_0} \right) - R^F}{\boldsymbol{IV_x}} \quad (4.4.6)$$

As of October 17th 2023, under the assumption of constant TVL, and uncorrelated and normally distributed volumes and therefore fees, equation (4.4.6) can be used to run a simple forecast Fudge-Alioth analysis of a ETH-USDC position with a high bound set at 3000 and low bound set according to (2.9), for a 12 month duration position, using current ATM put options Implied Volatility sourced from Deribit (2023), a forecasted Fudge-Alioth approximation of 0.2376 is generated.

Fitting with the analysis conducted by Heimbach, Lioba, Schertenleeib & Wattenhofer (2022), CLAMM positions investor returns are relatively poor compared to traditional finance peers. When analysing this same hypothetical position on a daily interval using forecast mechanic, the results for the forecast Fudge-Alioth ratio (FFAR) shown in Figure 6 are obtained.

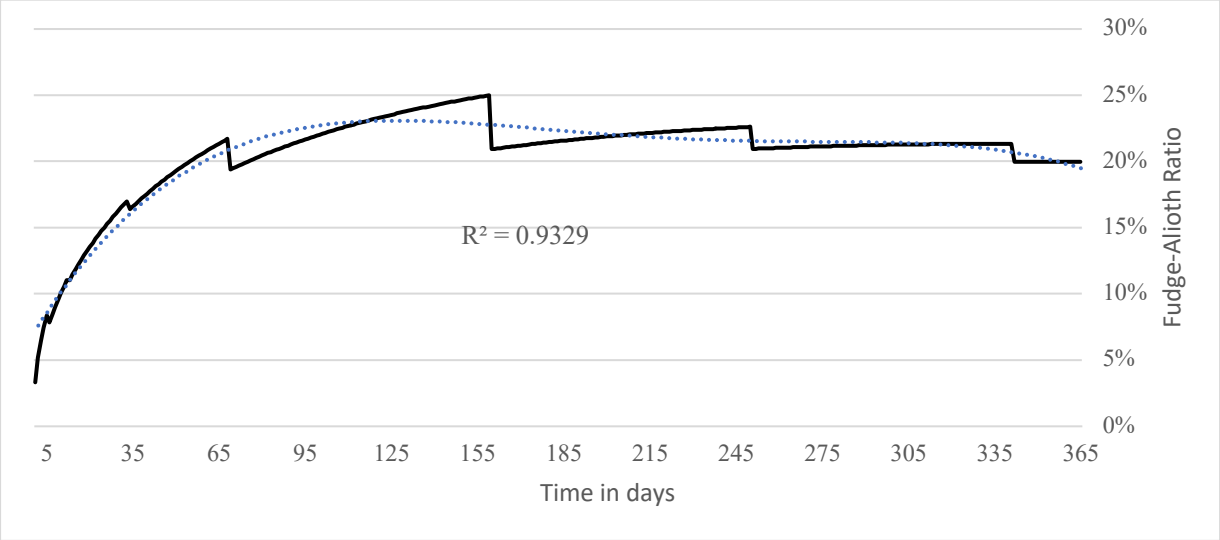


Figure 6: Forecast Fudge-Alioth Ratio of a P_H 3000 Position over time

An interesting relationship begins to form, partially driven by risk pricing in the options market, where there is a lack of continuous data available, leading to cliffs available where a fair market pricing the volatility surface over continuous periods. But in its place, it can be seen that a simple relationship emerges, where optimal liquidity provision time for risk-return for a given price range, without re-adjustment based on the current IV of Put options taken from Deribit (2023), is 159 days. However, under the context of a continuous volatility surface, as modelled in a simplistic manner, the highest effective Fudge-Alioth ratio can be found at approximately 120 days, but is still a sub-optimal investment relative to peers on a risk-adjusted basis when managed passively.

When taking these findings of approximately optimal time ratings, it can be analysed in a simplified manner, under the conditions of optimal barrier prices according to equation (2.9), using a position length of 150 Days. The results are shown in Figure 7.

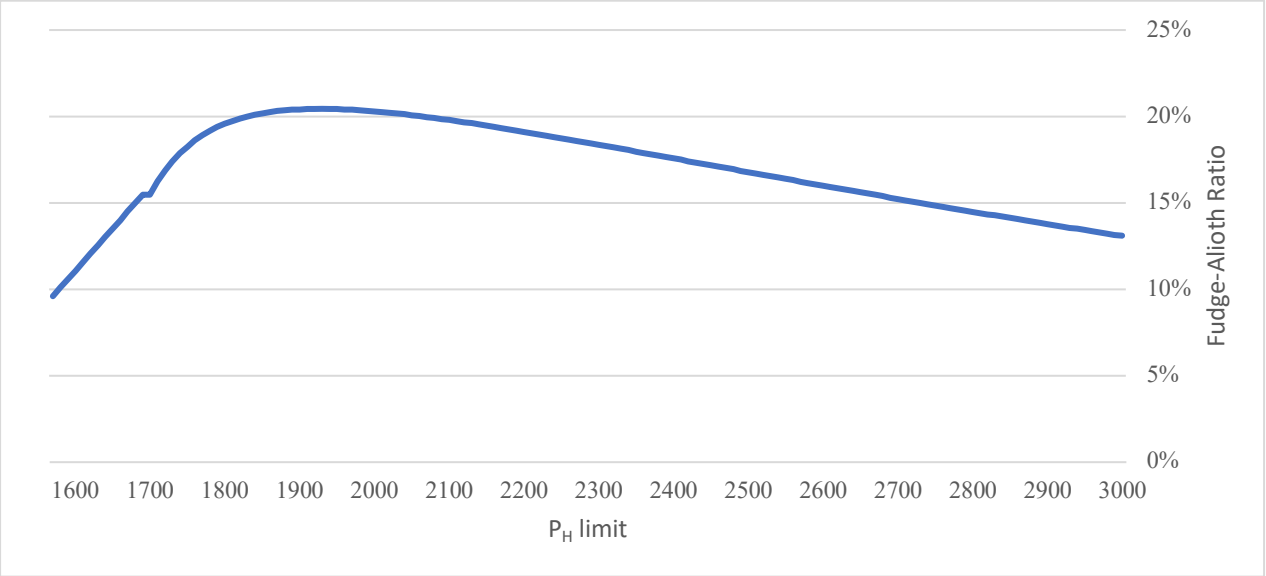


Figure 7: Forecast Fudge-Alioth Ratio

Optimal bounds can be found at $1930 – $1262, producing a forecast Fudge-Alioth ratio at 0.3284 under the aforementioned conditions. While an improvement, we still see a less than optimal Fudge-Alioth ratio.

Effectively this paper proposed a new metric where for any selected pair consisting of a volatile asset and a stable coin, using simplified analysis techniques and historical data, a critical number of issues in the LP market can be solved.

The lack of ability for LPs to directly compare risk reward in pairs, leading to sub optimal returns and lower total allocations to LP positions can be mitigated using the FFAR. It also simplifies the increasing complexity of CLAMM systems, giving better actionable information to potential LPs.

By using the process in reverse, a user can either find the optimal time length of their positions under the pre-set assumptions, or the optimal price range for their position given a desired time in a market position.

Given a price expectation on the volatile asset X in question, a desired position time and price barrier range, LPs can see the payoffs of their desired allocation, and compare them simply with the passive portfolio under their price estimations or directly against other asset classes risk adjusted returns historically.

4.5: Limitations of the accuracy of the FFAR and Historical Testing

While a useful tool for traders to be able to directly compare pools of various crypto assets against stable coins, a number of issues exist in the quality of its predictive power.

As outlined by Punzo & Bagnato (2021), crypto-asset returns do not perfectly fit the normal distribution, they are arguably closer to a Laplace distribution. This can lead to the results of being an LP given what under normal market estimation could be called a ‘black swan’ either greatly exceeding or greatly under-performing the expected returns. This is especially true when prices become inaccurate during periods of high volatility as shown by Heimbach, Schertenleib & Wattenhofer (2022).

There is a lack of continuous volatility surfaces for liquid options markets on crypto assets in question leads to cliffs and jumps at critical dates around common expiries in traditional options markets.

A lack of options pairs for smaller market cap crypto-assets limits the range of assets the Fudge-Alioth ratio can fairly analyse, outside of using their beta against larger cap assets with fair and

liquid options markets and using an approximation which would introduce greater inaccuracies into the modelling.

There is naturally a strong and logical correlation between total fees and TVL (DeFiLlama, 2023), the core economic logic being, that should the volumes in a pool increase, ceteris paribus, the yield available will increase, changing the risk reward dynamic for this asset relative to peers, and lead to new LPs engaging in the market, increasing TVL rapidly to capture these higher fees.

The issue of superior strategies existing is common in the market, where professional traders, with better access to information, and better trading systems, can continuously run shorter-dated positions to generate superior fees. Under the hypothesis of a 'perfect game' between a trader using this related metric or a professional trader running short-dated positions re-adjusting on a daily or even hourly basis with much tighter price ranges, would predictably always beat on fee revenues using this shorter-dated rapid adjustment strategy compared to even an optimised medium-term position.

The risk returns measured by the FFAR currently exclude any additional risk factors, such as smart contract and execution, as outlined in Chapter 4. Still, they are relatively low compared to several traditional market assets. This is either a fitting explanation for the relatively small size of the markets TVL compared to the total value of the crypto market, at $38.296bn in total TVL on 22nd October 2023 (DeFiLlama, 2023), compared to a total crypto market capitalisation of 1.13 Trillion (Coinmarketcap, 2023) or 3.38% of total crypto assets by value actively deployed into LP positions, where we can assume the majority are deployed by professionals engaging in short term rapid rebalancing strategies to capture far higher potential fees as retail users have been 'pushed out' by continuously receiving below fair returns for their risk in participating as LPs.

5: Conclusion

This paper analysed the risks and benefits of CLAMM systems like Uniswap v3 and proposed the Fudge-Alioth Ratio as a metric for forecasting the risk-adjusted returns of potential allocations. While CLAMM systems offer deeper virtual reserves, tighter spreads, and lower slippage compared to CFAMM systems, they also come with significant risks such as impermanent loss and disproportionately distributed trading fees. Therefore, this paper

concludes that investors must carefully consider the risks before allocating their assets to CLAMM systems. By using FFAR, investors can make more informed decisions.

Further study beyond the scope of this paper, including a rebalancing portfolio for a fair comparison, could enhance the FFAR and show where superior returns could be generated with simple automated strategies that adjust the price range as soon as it leaves the previous range set, which could become the basis of passive LPs participating with guidance by an automated platform, which could re-introduce the ability of retail to participate with fair risk-reward in future.

Bibliography

DeFiLlama. (2023, October 23). *Uniswap*. Retrieved from DeFiLlama: https://defillama.com/protocol/uniswap

Adams, H., Keefer, R., Zinsmeister, N., Robinson, D., & Salem, M. (2021, March). *Uniswap v3 core*. Retrieved from https://uniswap.org/whitepaper-v3.pdf

Heimbach, L., Schertenleib, E., & Wattenhofer, R. (2022). *Risks and Returns of Uniswap V3 Liquidity Providers.* ETH Zürich.

Fritsch, R. (2021). *Concentrated Liquidity in Automated Market Makers.* ACM CCS Workshop on Decentralized Finance and Security.

Sun, X., Lin, S., Sjöberg, V., & Jie, J. (2021). *How to Exploit a DeFi Project.* Financial Cryptography and Data Security.

Yang, S., Zhang, F., Huang, K., Chen, X., Yang, Y., & Zhu, F. (2023). *SoK: MEV Countermeasures: Theory and Practice.* Cryptography and Security.

Fukasawa, M., Maire, B., & Wunsch, M. (2023). *Weighted variance swaps hedge against impermanent loss.* Quantitative Finance.

Elsts, A. (2023, July 24). *Liquidity Provider Strategies for Uniswap v3: Options*. Retrieved from Medium: https://atise.medium.com/liquidity-provider-strategies-for-uniswap-v3-options-ce6748c5b1b4

Elsts, A. (2021). *Liquidity Math in Uniswap v3.* Elektronikas un datorzinātņu institūts.

0xDanr. (2022, June 22). *GammaSwap Protocol*. Retrieved from GammaSwap: https://gammaswap.com/blog/gammaswap-protocol

DeFiLlama. (2023, October 16). *Stablecoin - DeFiLlama Yield*. Retrieved from DeFiLlama: https://defillama.com/yields/stablecoins

Treynor, J. L. (1962). *Toward a Theory of Market Value of Risky Assets.* Independent.

Deribit. (2023, October 17). *Deribit Metrics - Deribit*. Retrieved from Deribit: https://metrics.deribit.com/options/BTC

Sharpe, W. F. (1966). *Mutual Fund Performance.* The Journal of Business.

Punzo, A., & Bagnato, L. (2021). *Modeling the cryptocurrency return distribution via Laplace scale mixtures.* Physica A: Statistical Mechanics and its Applications.

Heimbach, L., Schertenleib, E., & Wattenhofer, R. (2022). *Exploring Price Accuracy on Uniswap V3 in Times of Distress.* ETH Zürich.

7.9. Stablecoins and Systematic Risks: Anchoring Crypto Markets in Turbulence

AUTHORS:

Mauro Casellini

vision&

Stafano Frick

BDO

"Stablecoins and Systematic Risks: Anchoring Crypto Markets in Turbulence"

1. Introduction

The introduction of cryptocurrencies marked a paradigm shift in the world of finance. The concept of a decentralized digital currency, free from the control of central banks and traditional financial institutions, was first introduced by the pioneer cryptocurrency "Bitcoin". While this concept remains a major advantage, it is important to note that cryptocurrencies like Bitcoin still witness strong volatility spikes making them less ideal for day to day transactions and as thus a stable store of value.

But where does all the volatility come from? Volatility spikes come from various sources, such as speculative trading, market sentiment, and limited adoption. The result is obvious; extreme price swings, even within a single day. The ongoing volatility stipulates the need for a stable medium of exchange,equivalent to traditional means of payment (Kamsky, 2023).

To address this issue, stablecoins have emerged as a solution that combine the advantages of cryptocurrencies (such as speed, security, and borderless peer to peer transactions) with the stability of traditional fiat currencies. As the name indicates, stablecoins aim to maintain stable value by pegging against external assets like fiat currencies, commodities, or even algorithms that automatically adjust the supply based on market demand (DeMatteo, 2022).

2. Purpose and Scope

The purpose of this paper is to examine the complex relationship between stablecoins and the systemic risk within cryptocurrency markets. The scope of our exploration is broad and encompasses the following key areas:

- **Mechanisms and Classifications of Stablecoins**: In this paper, we will provide an overview of mechanisms and classifications of stablecoins, with an understanding of their operation and significance within the cryptocurrency ecosystem.
- **Systemic Risks Associated with Stablecoins**: We will identify and assess the potential systemic risks such as market concentration, regulatory challenges, technological vulnerabilities, and the potential for market manipulation.
- **Risk Management Strategies**: We will explore existing risk management practices and strategies within the stablecoin ecosystem, evaluating their effectiveness in mitigating the identified threats.

- **Recommendations for Stakeholders**: We will propose recommendations and insights for regulators, market participants, and investors to mitigate the systemic risks associated with stablecoins.

3. The Significance of Stablecoins

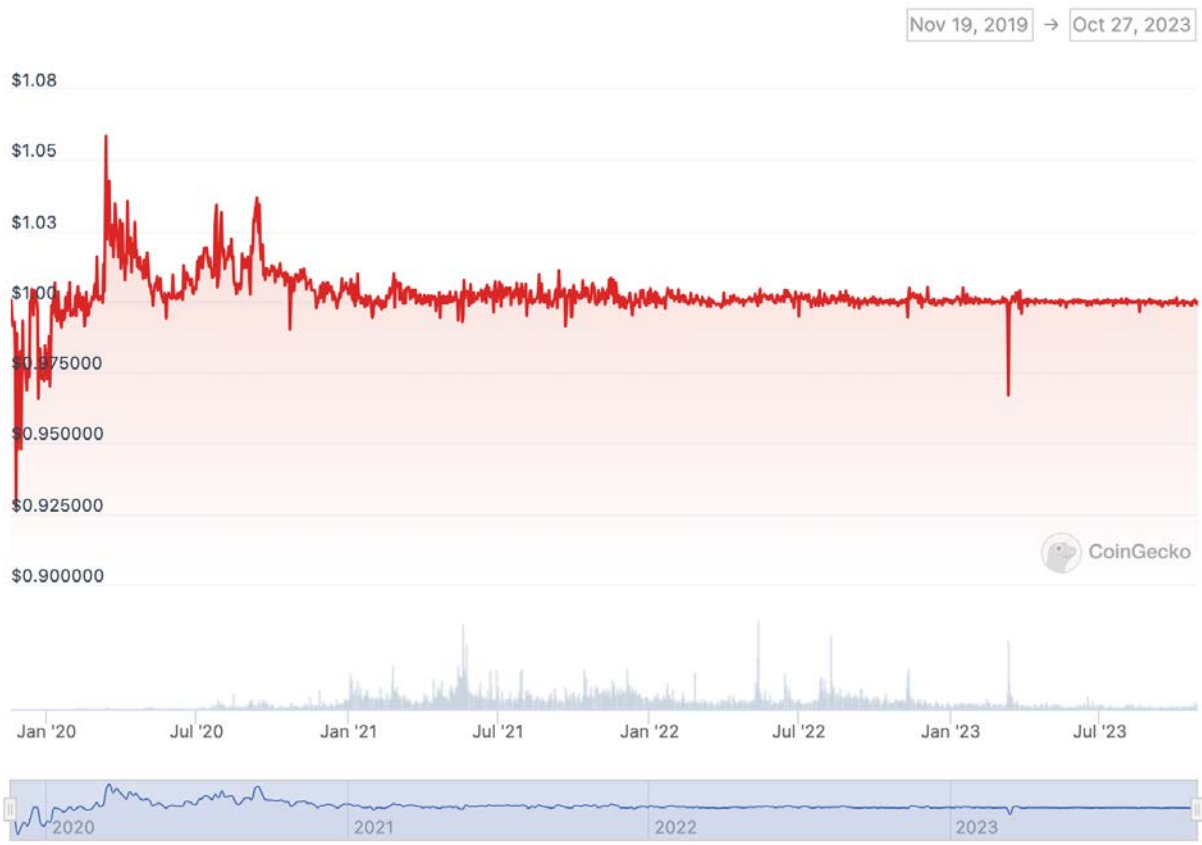
3.1 Understanding Stablecoins

Stablecoins play a pivotal role within the cryptocurrency ecosystem, serving as a critical bridge between the inherent volatility of cryptocurrencies like Bitcoin and the desire for stability often associated with traditional financial assets. These digital assets are designed to maintain a consistent value over time, leveraging a variety of mechanisms to achieve this objective. Understanding these mechanisms is crucial for comprehending the significance and diversity of stablecoins.

3.1.1 The Versatility of Collateralized Stablecoins

Among the most prominent categories of stablecoins are collateralized tokens, which maintain their stability by backing each unit with a reserve of assets. These assets can encompass fiat currencies like the US dollar, cryptocurrencies such as Ethereum, or even tangible commodities like gold. Their stability hinges on the ratio of stablecoins in circulation to the value of the collateral (Hussey & Chipolina, 2023). A prime example is USD Coin (USDC), maintaining a 1:1 peg to the US dollar by holding an equivalent amount of USD in reserves, fostering trust by enabling users to redeem USDC for USD on demand.

Another collateralized stablecoin with a different approach is DAI from MakerDAO (MakerDAO, 2018). DAI is a collateralized stablecoin in the cryptocurrency ecosystem, backed primarily by Ethereum and designed to maintain a stable value, typically pegged to the US dollar. Users lock up cryptocurrency, like ETH, as a collateral to generate DAI. An autonomous system of smart contracts on the Ethereum blockchain regulates the supply to ensure stability and maintain a target value.



Note. Price Stability of DAI since inception, October 2023, www.coingecko.com

3.1.2 Algorithmic Control: Navigating Without Collateral?

Algorithmic stablecoins, on the other hand, chart a different course, forsaking traditional collateralization. They rely on algorithmic mechanisms to control the supply of the stablecoin, making real-time adjustments based on market demand and deviations from the target price (Simon, 2020). For instance, if the price of an algorithmic stablecoin exceeds its peg, the algorithm may mint new tokens to increase supply and restore the desired price level. TerraUSD (UST), a prime illustration of this trend, commenced its mainnet operations in 2019, utilising autonomous smart contracts to keep a stablecoin stable at 1 USD value. It gained substantial attention within the crypto market, even if it was still quite experimental at this point. However, the events of May 2022 underscored the extent of its experimental status, as it suffered a dramatic collapse. This collapse led to the swift evaporation of $45 billion in market capitalization in just a few days and contributed to substantial losses across the broader crypto landscape.(Miller, 2022).

3.1.3 Adaptability and Resilience: The Strength of Stablecoins

The significance of stablecoins extends beyond their mechanisms. They demonstrate adaptability and resilience by utilizing these diverse mechanisms. Collateralized stablecoins offer a tangible link to real-world assets, bolstering stability and trust (Zawieja & Kazmierczak, 2023). In contrast, algorithmic stablecoins provide flexibility and automatic adjustments, making them suitable for decentralized finance (DeFi) platforms where collateral might be scarce or undesirable.

Additionally, stablecoins exhibit adaptability by being compatible with various blockchain platforms. They are issued on Ethereum, Tron, Solana, Binance Smart Chain, and others, enabling users to select a platform that aligns with their preferences for security, scalability, and cost-effectiveness.

3.1.4 The Expanding Role of Stablecoins Beyond Crypto and DeFi

Stablecoins have evolved far beyond their initial utility within the crypto and DeFi spheres. They have now established themselves as a peer-to-peer, borderless means of payment. Notably, they are gaining prominence outside of the United States, finding utility in various global financial ecosystems (Zawieja & Kazmierczak, 2023).

3.2 Stablecoins: Enhancing Financial Stability Amidst Crypto Volatility

Stablecoins have transcended their origins in the crypto and DeFi spheres to become a peer-to-peer, borderless means of payment. This evolution is especially notable as they gain prominence beyond the borders of the United States, finding utility in diverse global financial ecosystems (Young, 2023). Stablecoins are no longer just stabilizers within the crypto market. They have become a vital bridge connecting traditional financial systems with the world of cryptocurrencies, offering an array of benefits that enhance their significance in the crypto landscape.

Traditional cross-border transactions often entail substantial fees and lengthy settlement times, causing inconvenience and financial strain. In stark contrast, stablecoins like USDC and USDT offer a rapid and cost-effective alternative. The World Bank reports that the global average cost of sending a remittance is approximately 6.2% of the transaction amount (The World Bank Group, 2023). Stablecoins, conversely, facilitate cross-border transfers with fees often less than 1% (with Gas Fees) and settlement times of merely/a few seconds or

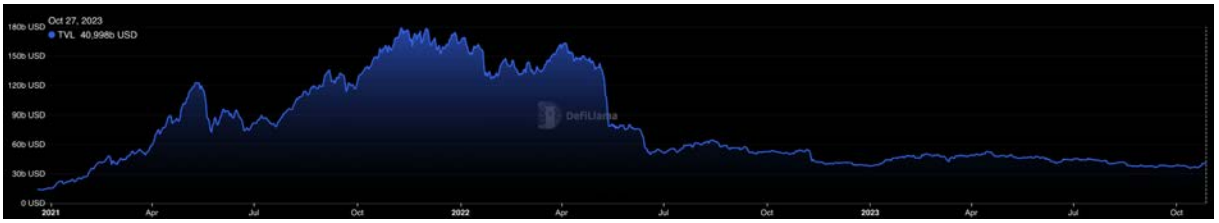
minutes,not days. These figures highlight the significant cost and time savings facilitated by stablecoins, making them the preferred choice for international money transfers.

3.2.1 Stablecoins: A Sanctuary Amid Market Turbulence

The inherent volatility of cryptocurrency markets can result in substantial losses for investors during market downturns. In times of uncertainty, stablecoins emerge as a safe haven, offering a sanctuary for investors to protect their capital, while staying within the crypto space, without the need to revert to fiat.. Data reveals that during periods of market crashes, trading volumes for stablecoins surge more than 200% (Faridi, 2018). This observation underscores the pivotal role stablecoins play in risk management during turbulent times.

3.2.2 Empowering Decentralized Finance (DeFi) Platforms

Decentralized finance (DeFi) has experienced explosive growth, and stablecoins are at its core. They provide the essential liquidity needed for lending, borrowing, trading, and yield farming on DeFi platforms. As of 27. October 2023, the total value locked (TVL) in DeFi protocols exceeded $41 billion, with stablecoins forming a substantial portion of this value (DefiLlama, 27.10.2023). This TVL demonstrates how stablecoins underpin the DeFi market, acting as a catalyst for growth.



Note. Total Value Locked in DeFi, October 2023, www.DeFiLlama.com

3.2.3 Stablecoins: A Tool for Everyday Transactions

Beyond their role as a refuge during market turbulence, stablecoins find utility in everyday transactions. Their stable value makes them suitable for various use cases, from purchasing goods and services to facilitating international fund transfers.

Imagine a scenario where a freelancer based in one country receives payment in stablecoins, which can be seamlessly converted into their local currency without concerns about the significant price fluctuations that often affect traditional cryptocurrencies. Individuals can

choose to remain in the more stable USD for as long as they wish, especially when compared to their often much more volatile local currencies. This stability encourages the widespread adoption of cryptocurrencies in everyday financial activities (James, 2023).

4. Regulation and Compliance

4.1 Regulatory Landscape

Stablecoins, the backbone of financial stability in the crypto realm, find themselves navigating a complex and rapidly evolving regulatory landscape. Governments and regulatory bodies worldwide are grappling with how to classify and oversee these digital assets. In this chapter, we embark on a journey through the intricate regulatory environment of the European Economic Area (EEA) and Switzerland. We explore how these two distinct jurisdictions are approaching stablecoin regulation, shedding light on the challenges that this presents for both issuers and users.

Government entities and traditional financial institutions play pivotal roles in shaping the stablecoin ecosystem. The level of government involvement, ranging from cautious monitoring to outright bans, impacts the adoption and development of stablecoins. We will investigate the roles these entities play in shaping the regulatory framework and their influence on the stability of stablecoins.

4.2 European Union

The Markets in Crypto-Assets Regulation (MiCAR) will introduce a new regulatory framework for European crypto-assets. Critically, MiCAR aims to protect investors and ensure financial stability while allowing innovation and fostering the attractiveness of the crypto-asset sector.

The Regulation came into force on the 30th of June 2023, 20 days after the publication in the official journal. The provisions in Titles III and IV regarding Asset-Referenced Tokens (ARTs) and E-Money Tokens (EMTs) will begin to apply already on the 30th of June 2024, 12 months after entry into force.

MiCAR will bring issuers of certain types of crypto-assets into the regulatory framework. Specifically, MiCAR will establish new rules for those types of crypto-assets known as "stablecoins" including ARTs, EMTs and utility tokens. MiCAR distinguishes stablecoins by defining ARTs as being linked to multiple currencies, commodities or crypto currencies and

EMTs as being linked to a single currency. Utility tokens are intended to provide access to a good or service that will be supplied by the issuer of that token.

Issuers of ARTs and EMTs will be required to be authorised by their respective national supervisory authority and to publish a white paper which will contain information for investors. They will also be required to build up a sufficiently liquid reserve with a 1/1 ratio and meet other regulatory requirements. MiCAR recognises that some ARTs or EMTs may be significant due to their size and other factors and as a result may present an increased risk. The European Banking Authority (EBA) will have supervisory responsibilities for issuers of significant ARTs and EMTs.

Subject to intense debate, MiCAR introduces restrictions on the daily average number of transactions and trading volume associated with EMTs and ARTs when used as a means of exchange according to MiCAR Art. 23 and Art. 58. It sets a limit of 1 million transactions and EUR 200 million in trading volume. However, it is essential to note that these limitations apply primarily to EMTs denominated in a currency that is not an official currency of an EU member state.

Concerns have arisen that these regulations could potentially stifle the usage of popular USD-pegged stablecoins like Tether's USDT and Circle's USD Coin in the EU due to their substantial trading volumes. However, it is important to highlight that regulation offers clarity by distinguishing that not all types of transactions will be classified as linked to the use as a medium of exchange. Interestingly, this regulatory framework may boost the adoption of EUR-backed stablecoins, opening new opportunities and dynamics within the European market.

4.3 Switzerland

Regarding stablecoins in Switzerland, no general statement is possible whether financial market activities in connection with such coins require any financial market licence. The supervisory classification of stablecoins by FINMA follows the following three principles: “substance over form”; “same risks, same rules”; and “case-by-case analysis taking into account the specific circumstances of the individual case” (FINMA, 2019). No specific regulations for stablecoins exist in Switzerland. Depending on their design features, stablecoins must therefore be analysed on a case-by-case basis to determine whether any such licence is required. Design features such as (i) whether a single underlying or a basket of underlyings is used, (ii) the type of underlying, as well as (iii) if the stablecoin in question

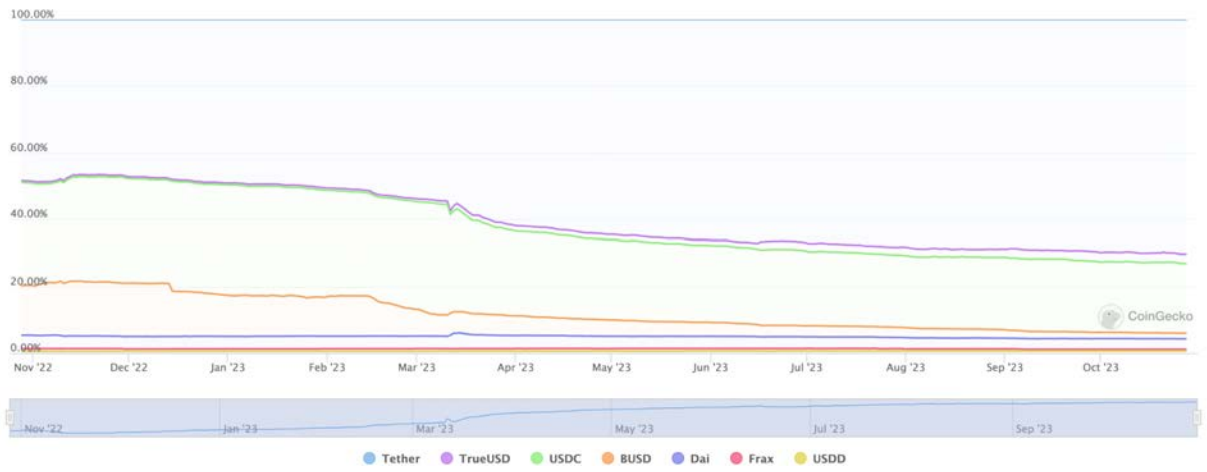
gives the holder a contractual redemption claim with regard to the underlying(s), respectively, the value of the underlying(s), or if the token merely fulfils the function of evidencing an ownership position with regard to the underlying(s), may be decisive (FINMA, 2019). In particular, a banking licence may be required. For example, according to the FINMA Supplement, in particular issuers of stablecoins that are linked to (i) fiat currency applying a fixed ratio (*e.g.*, 1 token = 1 USD), or (ii) so-called precious metal of banks that provide for a contractual claim for the respective underlying, may require a banking licence.

5. Systematic Risks and Mitigation

Systematic risks within the stablecoin ecosystem are pivotal factors that warrant thorough examination due to their potential to impact not only the stablecoin market but also the broader financial system. To develop effective strategies for risk mitigation, it is important to identify and assess these risks comprehensively. Let us dive into some of these systematic risks and their sources:

5.1 Market Concentration

Market concentration is a substantial systematic risk stemming from the dominance of a single stablecoin. For instance, the two largest stablecoins, USDT and USDC, collectively account for 88% of the market capitalization, with USDT alone holding 67% of the total market capitalization, while USDC constitutes just 21% (Coinmarketcap.com, 26.10.2023). Market concentration implies vulnerabilities, as the stability and regulatory issues of a dominant stablecoin can have far-reaching consequences. To mitigate this risk, diversification of stablecoin options becomes crucial, ensuring that market reliance on a single player is reduced, thus making the ecosystem more resilient.



Note. Stablecoin Market Dominance, October 2023, www.coingecko.com

5.2 Regulatory Challenges

The ever-evolving regulatory landscape poses a significant systematic risk. Inconsistencies or overly stringent regulations across jurisdictions can disrupt stablecoin operations and erode user confidence. Governments are actively pushing for regulatory clarity and harmonization to safeguard end-users and companies (*Pathways to the Regulation of Crypto-Assets: A Global Approach*, *WEF,* 2023). In Europe, MiCAR has taken a proactive stance on regulating stablecoins, proposing restrictions on foreign currency-denominated stablecoins that could impact the market significantly. Meanwhile, the regulatory approach in the United States, marked by uncertainties, further complicates matters. Rapid regulatory changes can also have adverse effects, meaning that active legal use cases today could potentially turn into legal issues tomorrow. Such a dynamic environment emphasises the need for international collaboration and clear guidelines to ensure stablecoin stability and growth.

5.3 Technological Vulnerabilities

Stablecoins heavily rely on blockchain technology, which inherently exposes them to technological risks. Vulnerabilities in smart contracts, network congestion, and software bugs can lead to severe disruptions and financial losses (Li, 2023). This risk is further compounded by the increasing complexity of the stablecoin landscape, as stablecoins are not limited to a single blockchain but are active across multiple blockchains. Each provider must navigate various technologies, bridges, and interoperability challenges, adding another layer of complexity to risk management. To address this multifaceted risk, regular and rigorous security audits and updates are of paramount importance. By continually fortifying the underlying technology and adapting to the complexities of a multi-chain environment, stablecoins can enhance their resistance to technological vulnerabilities, ensuring greater stability and reliability.

5.4 Market Manipulation

Market manipulation poses a systemic risk, especially within centralized exchanges. Activities like price manipulation, wash trading, and insider trading can significantly undermine market integrity and, consequently, the stability of these assets (Kharif & Bronner, 2023). While the blockchain itself is fundamentally transparent, making it challenging to

manipulate on-chain data, stablecoins are still vulnerable to market manipulation and wash trading.

However, it is important to note that market manipulation can also impact stablecoins, affecting their prices and stability. Therefore, robust surveillance mechanisms and effective enforcement measures are essential to maintain market integrity. Regular monitoring and stringent enforcement of market rules and integrity can act as powerful deterrents against manipulation, safeguarding the stability of the stablecoin ecosystem. This becomes even more critical as stablecoins continue to play a pivotal role in various crypto transactions and decentralized finance (DeFi) activities.

6. Risk Mitigation Strategies in the Stablecoin Ecosystem

Risk mitigation is key to ensure a stable and reliable stablecoin ecosystem. This chapter delves into a spectrum of strategies employed within the stablecoin ecosystem to effectively manage and reduce risks. These strategies encompass collateralization, algorithmic controls, and reserve management, and we will examine their roles and suitability across various stablecoin models.

6.1 Collateralization: A Foundation of Stability

Collateralized stablecoins derive their stability from a reserve of assets, which can encompass a spectrum of assets, spanning from fiat currencies to cryptocurrencies. A notable feature of asset-backed stablecoins is the utilization of over-collateralization, a risk-mitigation strategy that creates a protective cushion against market volatility. The effective management of collateral resources is indispensable for the maintenance of stability and the mitigation of risks associated with these underlying assets.

In an over-collateralized system, the total value of assets held in reserve surpasses the combined value of the stablecoins in circulation. For instance, if a stablecoin issuer has issued $100 million worth of stablecoins, they may secure them with assets like Ether worth $150 million (Kohli, 2019). This approach acts as a robust safety net, serving to buffer against market fluctuations and potential declines in the value of the underlying assets.

Effective collateral management practices are pivotal to uphold stability and counter risks tied to the underlying assets. These practices encompass a regimen of regular audits to ensure that the collateral reserves correspond accurately to the total supply of stablecoins. Additionally, issuers must prudently oversee their collateral in response to the prevailing market conditions

to avert scenarios where the asset value falls below the aggregate value of the stablecoins in circulation, which could lead to potential insolvency. The requisite Loan to Value (LTV) ratio for securing the stablecoin varies depending on the market situation, highlighting the need for adaptability and vigilance in the face of dynamic market dynamics.

6.2 Algorithmic Controls: Code-Based Resilience

Algorithmic stablecoins represent a pioneering approach to stability management by harnessing the power of smart contracts and algorithms (Cointelegraph, 2022). Unlike collateralized stablecoins that heavily rely on physical assets, algorithmic stablecoins pivot towards code-based mechanisms that autonomously adapt the stablecoin's supply to align with market demand. This innovative strategy minimizes dependence on traditional collateral, rendering algorithmic stablecoins more resilient and less susceptible to the risks associated with asset holdings.

In essence, algorithmic stablecoins maintain their peg to a target value, often $1, through an intricate interplay of algorithmic rules and market dynamics. When the stablecoin's price drifts away from its intended value, the smart contract governing it intervenes, executing predefined actions to restore equilibrium. For instance, if the stablecoin's price surpasses $1, the smart contract may incentivize users to mint new stablecoins or burn existing ones, thereby influencing the supply to reduce the price. Conversely, if the price dips below $1, the contract might incentivize users to purchase and hold stablecoins, increasing demand and propelling the price back to the target.

This code-driven resilience offers a distinct advantage by reducing the reliance on physical assets, mitigating collateral-associated risks, and increasing the flexibility of stablecoins to adapt to changing market conditions. However, it also introduces unique challenges, such as the need for robust auditing and the necessity to fine-tune algorithmic parameters to maintain stability. As witnessed with Terra Luna and UST, this sector is still in its infancy, and its experimental nature cannot be overstated. Currently, risks outweigh the advantages, and the future development of this field remains uncertain. It will be intriguing to observe how this area evolves in the coming years.

6.3 Reserve Management: Ensuring Solvency

Reserve management is a cornerstone of stablecoin operations. Issuers must carefully manage their reserves to ensure they can cover the total supply of stablecoins in circulation.

Inadequate reserve management can result in insolvency risks, underscoring the critical importance of effective reserve practices.

Effective reserve management is vital to ensure the solvency of stablecoin issuers. These digital assets rely on reserves of underlying assets, such as fiat currencies or cryptocurrencies, to back their value. It is crucial that these reserves are not only adequate but also sufficiently liquid to meet redemption demands. Inadequate liquidity can lead to significant problems, akin to a traditional bank run, potentially causing the insolvency of the stablecoin issuer.

These systematic risk mitigation strategies, when complemented by transparent operations and governance, form the foundation of a stable and dependable stablecoin ecosystem. Continuous evaluation and adaptation are essential in addressing the ever-evolving challenges and opportunities present in the dynamic cryptocurrency landscape.

6.4 Auditing and Transparency Standards: Safeguarding Trust

Transparency and robust auditing standards are essential for mitigating risks within the stablecoin ecosystem. Stablecoin issuers wield significant influence, and it is crucial to prevent any potential misuse of this power. Consequently, just as in the traditional financial world, the implementation of monitoring, audits, controls, and supervision is highly advisable to ensure the integrity and stability of stablecoins.

6.4.1 Transparency in Operations

Transparency in stablecoin operations is of immense importance. It is essential that users and more and more also regulators and other important third parties like auditors have access to real-time transaction data, reserve composition, and issuance records. Transparent operations not only build trust among stakeholders but also enable the swift identification of any issues that may arise.

6.4.2 Third-Party Audits

The verification of stablecoin reserves through third-party audits is a cornerstone of trust. Independent auditors rigorously assess the issuer's holdings to ensure they match the outstanding stablecoin supply. This process provides a high degree of assurance to users and regulators alike.

In today's digital age, with optimized banking connections and accessible APIs, the process of conducting third-party audits has become more streamlined and efficient. However, it is worth noting that some providers still face challenges. It is crucial to place significant emphasis on this aspect, especially if stablecoins are to gain wider use cases and broader industry adoption. Ensuring that audits can be conducted seamlessly and with the utmost transparency is essential for the continued growth and credibility of stablecoins in the financial landscape.

6.4.3 Disclosure Standards

Stablecoin issuers should adhere to disclosure standards akin to those in traditional finance. Comprehensive financial reporting, including balance sheets and income statements, plays a pivotal role in enabling users and regulators to evaluate the financial health and stability of stablecoin issuers.

The implementation of stringent auditing and transparency standards serves as a vital safeguard, enhancing trust, and bolstering the stability of the stablecoin ecosystem. These measures are crucial for ensuring that stablecoin users can have confidence in the integrity and reliability of these digital assets.

7. The Future of Stablecoins: Trends, Challenges, and Opportunities

The future of stablecoins is indeed an intriguing landscape marked by various trends, significant challenges, and exciting opportunities. As cryptocurrencies continue to influence traditional finance and gain mainstream recognition, stablecoins play a vital role in bridging the worlds of fiat currencies and digital assets.

One prominent trend is the expanding use of stablecoins beyond the realm of cryptocurrencies and DeFi. We are witnessing stablecoins increasingly being integrated into various industries, especially in the context of Industry 4.0 (Nuttah et al., 2023). These digital assets are optimizing supply chains, enhancing transparency, and facilitating seamless cross-border transactions. This expansion into traditional industries indicates the growing trust and adoption of stablecoins in broader economic contexts.

The integration of blockchain enhancements is another key trend. The underlying technology of stablecoins, blockchain, is continually evolving. New consensus mechanisms, scalability solutions, and interoperability protocols are being developed to address the limitations of

early blockchain networks. These advancements contribute to increased efficiency, reduced transaction costs, and improved scalability, all of which benefit stablecoins.

Moreover, the integration of stablecoins with central bank digital currencies (CBDCs) is on the horizon (*Central Bank Digital Currency Tracker*, 2023). Governments and central banks are exploring the issuance of digital versions of their national currencies. The synergy between CBDCs and stablecoins could revolutionize the way we transact, potentially leading to more efficient, cost-effective, and secure financial systems.

Challenges also accompany these opportunities (Nuttah et al., 2023). Striking the right balance between fostering innovation and ensuring regulatory compliance is a paramount challenge. Regulators around the world are closely scrutinizing stablecoins due to concerns about potential risks, such as money laundering, financial instability, and consumer protection. Achieving this balance is crucial to provide a secure environment for innovation while addressing these concerns.

Additionally, the stablecoin ecosystem should consider the implications of regulatory actions on both centralized and decentralized stablecoins. Regulatory clarity and harmonization are essential to prevent fragmentation and regulatory arbitrage, ensuring a level playing field for all market participants.

In conclusion, the future of stablecoins is teeming with promise and potential. Their versatility and stability make them essential components of the evolving financial landscape. As they continue to evolve, finding the right equilibrium between innovation and regulation will be key to unlocking their full potential and ensuring a secure and resilient financial system that benefits all stakeholders.

8. Recommendations for the Stablecoin Ecosystem

The stablecoin ecosystem stands at a crossroads, navigating evolving regulations and the pursuit of innovation. To ensure its continued growth and success, here are some recommendations:

Proactive Regulatory Engagement: Engaging with regulators to help shape sensible regulations, demonstrating a commitment to compliance and transparency. Proactive dialogue, information sharing and education can demystify the stablecoin industry for regulators,

fostering understanding rather than fear. Collaboration with regulatory authorities can lead to well-informed, balanced policies that support innovation while safeguarding the ecosystem.

Self-Regulatory Standards: Consider establishing industry standards for transparency, reserve management and operational practices. This proactive approach can demonstrate to regulators that the market is capable of effective self-regulation, potentially mitigating the need for more stringent oversight. By setting and adhering to high standards, the stablecoin ecosystem can foster a collaborative environment that encourages responsible growth and innovation.

Innovation Focus and Collaboration for Adoption: Continuously invest in innovation to unlock the full potential of stablecoins in revolutionizing finance and payments. Collaborate within the industry, partnering with key players like payment processors and financial institutions, to drive mass adoption while ensuring regulatory compliance and transparency.

User Education and Protection: As the stablecoin ecosystem continues to evolve, it is important to prioritize user education and protection. Issuers and industry associations should invest in educational resources to help users understand the risks and benefits of stablecoins. Providing clear information about how stablecoins work, their use cases, and the importance of conducting due diligence can empower users to make informed decisions. Additionally, implementing safeguards, such as insurance and reserve audits, can enhance user protection.

Transparency Initiatives: In addition to transparency in operations, stablecoin issuers should consider launching initiatives that provide real-time transparency into their operations. This can include publishing reserve data on blockchain ledgers, providing live updates on transaction volumes, and sharing key operational metrics. Enhanced transparency builds trust and allows users and regulators to monitor the stability of stablecoins continuously.

Contingency Planning: it is crucial for stablecoin issuers to develop comprehensive contingency plans for various scenarios. These plans should include strategies for addressing market volatility, liquidity crises, and regulatory changes. By having contingency plans in place, issuers can respond swiftly to unexpected events, ensuring the stability and solvency of their stablecoins.

In conclusion, the stablecoin ecosystems continuous success relies on proactive engagement with regulators, self-regulatory standards, innovation, user education, transparency, and robust contingency planning. These recommendations provide a roadmap for ensuring stability, growth and responsible development within the industry.

References

Central Bank Digital Currency Tracker. Atlantic Council. Retrieved October 27, 2023, from https://www.atlanticcouncil.org/cbdctracker/

Cointelegraph. (2022). *A beginner's guide on algorithmic stablecoins*. Cointelegraph. Retrieved October 27, 2023, from https://cointelegraph.com/learn/a-beginner-s-guide-on-algorithmic-stablecoins

DefiLlama. (2023). DefiLlama - DeFi Dashboard. Retrieved October 27, 2023, from https://defillama.com/

DeMatteo, M. (2022, September 16). *What's the Point of Stablecoins? The Reasons, Risks and Types to Know*. CoinDesk. Retrieved October 26, 2023, from https://www.coindesk.com/learn/whats-the-point-of-stablecoins-understanding-why-they-exist

Faridi, O. (2018, November 19). *As Crypto Markets Lose Billions in Market Cap, Stablecoin Trading Volumes Surge Over 200%*. CryptoGlobe. Retrieved October 27, 2023, from https://www.cryptoglobe.com/latest/2018/11/stablecoin-trading-volumes-surge-by-over-200-in-past-24-hours-as-crypto-market-sheds-billions/

Hussey, M., & Chipolina, S. (2023, October 25). *What Are Stablecoins and How Do You Use Them?* Decrypt. Retrieved October 26, 2023, from https://decrypt.co/resources/stablecoins

James, A. (2023, September 28). *What is a stablecoin and how does it work?* The Block. Retrieved October 27, 2023, from https://www.theblock.co/learn/251862/what-is-a-stablecoin-and-how-does-it-work

Kamsky, A. (2023, October 5). *A Comprehensive Guide To Why Is Bitcoin Volatile*. CCN.com. Retrieved October 26, 2023, from https://www.ccn.com/education/why-is-bitcoin-volatile/

Kharif, O., & Bronner, E. (2023, September 12). *Wash Trading Rampant on Decentralized (DeFi) Crypto Exchanges, Solidus Labs Says*. Bloomberg.com. Retrieved October 27, 2023, from https://www.bloomberg.com/news/articles/2023-09-12/wash-trading-is-rampant-on-decentralized-crypto-exchanges#xj4y7vzkg

Kohli, K. (2019, March 11). *What's MakerDAO and what's going on with it? Explained with pictures.* HackerNoon. Retrieved October 27, 2023, from https://hackernoon.com/whats-makerdao-and-what-s-going-on-with-it-explained-with-pictures-f7ebf774e9c2

Li, H. (2023, June 30). *A Review of Approaches for Detecting Vulnerabilities in Smart Contracts within Web 3.0 Applications*. MDPI. Retrieved October 27, 2023, from https://www.mdpi.com/2813-5288/1/1/2

MakerDAO. (2018, December 12). *Stablecoins: Collateralization Types | by MakerDAO*. Medium. Retrieved October 26, 2023, from https://medium.com/@MakerDAO/stablecoins-collateralization-types-2a860624dcd3

Miller, H. (2022, May 14). *Terra's $45 Billion Face Plant Creates a Crowd of Crypto Losers*. Bloomberg.com. Retrieved October 26, 2023, from https://www.bloomberg.com/news/articles/2022-05-14/terra-s-45-billion-face-plant-creates-a-crowd-of-crypto-losers

Nuttah, M. M., Roma, P., Lo Nigro, G., & Perrone, G. (2023, June). *Understanding blockchain applications in Industry 4.0: From information technology to manufacturing and operations management*. Science Direct. Retrieved October 27, 2023, from https://www.sciencedirect.com/science/article/abs/pii/S2452414X23000298

Pathways to the Regulation of Crypto-Assets: A Global Approach. (2023, May). WorldEconomicForum. Retrieved October 27, 2023, from https://www3.weforum.org/docs/WEF_Pathways_to_the_Regulation_of_Crypto_Assets_2023.pdf

Simon, B. (2020, December 21). *Stability, Elasticity, and Reflexivity: A Deep Dive into Algorithmic Stablecoins*. Mechanism Capital. Retrieved October 26, 2023, from https://www.mechanism.capital/algorithmic-stablecoins/

Top Stablecoin Tokens by Market Capitalization. (2023, October 26). CoinMarketCap. Retrieved October 27, 2023, from https://coinmarketcap.com/view/stablecoin/

The World Bank Group. (2023, June). Remittance Prices Worldwide Quarterly. https://remittanceprices.worldbank.org/sites/default/files/rpw_main_report_and_annex_q223.pdf

Young, M. (2023, August 8). *Circle CEO: 70% of USDC adoption comes from outside the US*. Cointelegraph. Retrieved October 26, 2023, from https://cointelegraph.com/news/circle-ceo-usdc-adoption-emerging-developing-markets

Zawieja, K., & Kazmierczak, M. (2023, July 13). *Stablecoins Report: The Ultimate 2023 Market Overview*.

7.10. DAOs - A Risk Management Approach

AUTHOR:

Ramona Tudorancea

JupiterBlock

DAOs - A Risk Management Approach

- a preliminary research paper with practical implications -

Introduction

Decentralized Autonomous Organizations (DAOs) can be seen as a multitude of experiments in decision-making and organization of work across national borders[1], based on the key principles of blockchain: decentralization, transparency, and authenticity. DAOs are "collectives" with variable and free-floating membership and levels of activity[2], and relatively stable but evolving goals and structural design, tied to a set of blockchain-based tools and automated systems. A brief review of the existing literature uncovers several key characteristics and issues, but research is still very fragmented[3]. Additional difficulties arise from the fact that a large number of projects call themselves DAOs without in reality being decentralized, and that DAOs generally span a large spectrum of human activities - from social clubs to associations to professional guilds to support activities, etc.[4] As in all pioneering industries, a mix of visionaries and opportunistic

[1] See *Decentralized Autonomous Organization Toolkit*, published by the World Economic Forum (WEF) in January 2023, which looks at DAOs as "potentially a significant innovation in organizational structures", "engaged in nothing less than an experiment to reimagine how we all connect, collaborate and create".

[2] In this respect, DAOs are clearly distinctive from cooperatives and associations, which have clear roles / levels of participation and benefits available for their members. We would argue that the variability of participation is in itself a DAO characteristic, even if this point has not been emphasized in the existing literature.

[3] Because DAOs are an emerging phenomenon, the current body of literature on DAOs is often focusing on isolated elements, *i.e.* technical architecture and smart contracts, without a comprehensive approach. One of the first papers to discuss DAOs in the context of organizational theory, Beck et al. (2018) argue that the emergence of the blockchain economy demands a rethinking of governance and may bring radical changes once the industry matures. Some of the themes which the authors felt needed to be explored in this context were: (i) cost-benefit analysis of centralized vs. decentralized decision-making, and the mechanisms of transition from one to the other; (ii) how decision-making worked in DAOs, and the separation between management rights and control rights; (iii) consequences of forking; (iv) the role of blockchain economy ownership; (v) business models for providing public goods; and (vi) how to predict the needs and incentives of network participants.

[4] Hassan and De Filippi (2021) offered a good overview of the history of DAOs and the multiplicity of viewpoints and definitions of DAOs in the existing literature. Not going into any details, we note that the early concept of the Decentralized Autonomous Corporation (DAC) was described by early crypto enthusiasts as "a new corporate governance form, using tokenized tradable shares as a means of providing dividends to shareholders". Authors are finally settling on the definition of DAO as a concept: a system based on a set of self-executing rules deployed on a blockchain, allowing people to coordinate among themselves for a common goal and thus leading to decentralized governance. (It should be noted that not all DAOs are tied to a certain blockchain protocol and many operate on the basis of blockchain-based tooling built by other projects.) The exact definition adopted by Hassan and de Filippi (2021) was "DAO is a blockchain-based system that enables people to coordinate and govern themselves mediated by a set of self-executing rules deployed on a public blockchain, and whose governance is decentralized (*i.e.*, independent from central control)." On this basis, several characteristics were identified which are specific to DAOs, including blockchain-based governance mechanisms, transparency, and above all decentralization. See also the World Economic Forum (WEF) definition in the *Decentralized Autonomous Organization Toolkit*: "organizational structures that use blockchains, digital assets and related technologies to direct resources, organize activities and make decisions."

actors have led to high failure rates and unscrupulous and even criminal behaviors, which have brought much disrepute to crypto generally. Even without going into a deep dive, it is therefore evident that DAOs are for the time being highly experimental and the level of decentralization is relative and depending on the maturity[5] of the project. It is also clear that DAOs present a large number of risks, some of which are yet unknown[6], starting with the long-term viability of the project (many DAOs are yet unclear as to their value proposition), legal and regulatory risks related to the activities carried out, and of course technical risks related to the blockchain-based operating systems, smart contracts, as well as underlying protocol and DAO tooling used. Yet, by combining blockchain technology with traditional "corporate" benefits (such as limited liability for members, legal personality and ability to contract, and governance mechanisms in line with best practices in organization theory), DAOs which are attached to a "legal wrapper"[7] could lead to an evolution and paradigm shift of corporate and social structures[8]. In particular, it is said that DAOs could solve a certain number of problems which are currently plaguing corporations[9].

At the same time, even the most enthusiastic DAO participants should acknowledge that most regulatory frameworks for organizations have been developed over time based on the classical agency theory where ownership and control are separate, requiring management of the potential conflict of interest between agent and principal and the protection of passive investors[10]. DAOs,

[5] Appel and Grennan (2023) found that over time the number of DAO proposals and active members increases and the control exerted by a small number of actors is eroded by community participation. Accordingly, we can view DAOs suffering from a lack of decentralization as "immature" or "young" DAOs.

[6] Some of the emerging risks are discussed below in **Part I**, but additional research is needed on this.

[7] There is no reason why DAOs would be unable to create a constellation of legal entities in various jurisdictions to serve their purposes, all tied into a common governance mechanism linked to the DAO. Simply, the industry is just now maturing and only a few projects are big and sophisticated enough to take advantage of such complex organizational structures.

[8] Our position in this respect is based on the seminal work for organizational theory which is "The Nature of the Firm" by Ronald Coase, published in 1937, arguing that corporations exist because they are more efficient compared to peer-to-peer transactions, which have higher "transaction costs" (finding a counterparty, negotiating and enforcing contracts, and information costs). As demonstrated by the rise of the sharing economy (AirBNB, Uber, etc.), technology has the potential of changing business models. With DAOs, the new economic models could lead to peer-to-peer transactions becoming less costly compared to organizations. This is for example the value proposition of Decentralized Finance (DeFi), subject to important limits and constraints such as the knowledge barrier, the costs related to smart contract audits, as well as on-chain governance. Coase is a useful benchmark which allows us to reframe the discussion as the competition between DAOs vs. corporations in the evolution of organizations.

[9] It is said that DAOs are addressing a "democratic deficit" in organizations by reuniting ownership and control, and changing the capitalist model. See WEF (2023), the *Decentralized Autonomous Organization Toolkit*: "DAOs seek to restructure hierarchical management set-ups and the classical separation of ownership and control by broadening participation in governance and aligning rewards with labor, contribution and participation." As experiments in organization theory, it is true that DAOs are live laboratories with thousands of participants and real world assets. However, from a less human-centric approach, DAOs can also be compared to neural networks (the "hive mind" theories), and some authors speak of multi-agent systems with digital humans (*i.e.*, AI) and of the rise of cybernetic organisms (Qin et al., Li et al., 2023).

[10] See Fama and Jensen (1983) and Shleifer & Vishny (1986) for example. This separation of ownership and control in modern corporations has major implications for investor protection and corporate governance mechanisms, which include securities laws and the role of the Securities and Exchange Commission (SEC) in the United States and similar market authorities, etc. .

which essentially disrupt this model, represent a challenge[11]. Because of this inability of DAOs to fit into current legal and regulatory models, some projects attempt to use offshore legal structures such as trusts, corporations or foundation companies[12] in order to attach the DAO to a "legal wrapper" which would hopefully ensure some protection against regulatory uncertainty[13], as well as the protection of the most active members of the DAO[14], taking into account recent enforcement actions[15]. Some jurisdictions started to adapt their legislation to accommodate legal structures which could be used by DAOs[16].

DAOs using offshore legal structures are motivated by complex factors, including the possibility to tie corporate governance to DAO consensus mechanism, the simplicity and pragmatism of offshore rules which have been successfully used by traditional actors over several decades[17], and the fact that the value resulting from community growth is not attributed or taxed in certain countries or to certain individuals, and can accrue to the benefit of the project or protocol[18]. However, there are many unknowns in this approach, and offshore legal structures in the context of DAOs have not yet been addressed by courts or regulatory agencies.

[11] See especially in the context of U.S. securities laws which are based on the idea of making profit from other people's efforts (the famed *Howey Test*), which explains why the Securities and Exchange Commission (SEC) is literally unable to issue uniform rules or guidance regarding tokens and insists on a case-by-case facts and circumstances approach.

[12] The most commonly used structures are Cayman Islands, and to a much smaller extent Bahamian or Panamanian foundation companies, trusts in various offshore jurisdictions, and LLCs and corporations. For the purposes of this research paper, we will illustrate issues arising when DAO is tied to a Cayman Islands foundation company.

[13] It should be noted here that protection against regulatory uncertainty is not always protection against legal uncertainty and that none of the offshore legal structures have been tested in a major dispute or enforcement action, and we are still very early in the process of designing bespoke governance models which would seamlessly work with the DAO decentralized governance rules.

[14] In the absence of a legal entity, in many jurisdictions the DAO members may be considered as having formed a common law partnership, leading to many legal consequences and especially unlimited liability. For this reason, we believe that the absence of a legal entity attached to a DAO project is one of the major Participant Risks (see below proposed **Risk Taxonomy for DAOs**)..

[15] In September 2022, the CFTC filed an enforcement action in federal court against Ooki DAO (bZeroX, LLC's successor) for failure to register as a futures commission merchant (FCM) and derivatives contract market (DCM) for activities that included offering leveraged and margined retail commodity transactions in digital assets. See Boniel (2023) for a full discussion.

[16] The states of Wyoming, Tennessee and Vermont in the United States, Malta and the Marshall Islands. See for a full discussion *Decentralized Autonomous Organization Toolkit*, published by the World Economic Forum (WEF) in January 2023.

[17] The Cayman Islands, for example, are the first offshore jurisdiction for investment funds and a major contributor to the traditional financial markets, as well as home to many public companies listed in the United States on NASDAQ or the NYSE. Offshore entities have been used by the traditional financial markets for decades - investment funds, asset managers, and securitization / bankruptcy-remote vehicles. This allowed for wealth-accumulation and tax optimization and enabled the international monetary flows which are supporting the current economy. The international push towards more transparency of offshore jurisdictions led to their becoming more accessible to smaller projects, including startups receiving venture capital or private equity funding, holding companies, and now DAOs. At the end of March 2023, there were close to 650 foundation companies incorporated in the Cayman Islands for example.

[18] This is achieved via incorporation of ownerless or "orphan" foundation company structures for example, without members, and which designate the underlying protocol, community, DAO or token holders as beneficiaries of the foundation company. This can also be achieved via a trust mechanism, subject to the appointment of a trustee.

The goal of this research paper is to advance the understanding of the risks, risk management approaches and governance issues for DAO projects generally, including with respect to offshore legal structures. First, a brief literature review was carried out to understand the state-of-the-art thinking in terms of governance and risk management, including on the continued relevance of agency theory[19], and decentralization generally. On this basis, we then presented several modern risk management concepts and methods and how they can be adapted for DAOs, including in the context of offshore legal structures, and proposed a *Risk Taxonomy for DAOs* (**Part I**). This analysis then served as a starting point to open a discussion on what a *Risk Management Framework for DAOs* could look like, and offer a few practical suggestions (see **Part II**).

Part I:

Risk management as a formal discipline dates back to the post-World War II era, with initial methods often developed in the fields of engineering and insurance (Dionne, 2013). Over the years, it evolved towards more structured approaches, such as the development of the risk-based approach (RBA) based on a Risk Matrix, Value-at-Risk (VaR) models in finance, Failure Modes and Effects Analysis (FMEA) in engineering, etc. Corporate risk management, *i.e.* risk management in organizations, first began as a siloed function aimed to prevent losses, often confined to health & safety, environmental and financial risks[20]. Later, the scope expanded to include operational, project, strategic, and reputational risks, etc. With the advent of technology and increasing complexity of operations, new methodologies emerged, such as Enterprise Risk Management (ERM)[21], which is an integrated, holistic approach to understanding and managing risks and opportunities, a framework that aligns risk appetite and management with the strategy

[19] Agency theory for DAOs can be a lens to view allocation of decision rights, determine how parties are to be held accountable, and how incentives can be used to overcome diverging goals (see Beck et al., 2018 citing the classics Jensen & Meckling, 1976, Fama & Jensen, 1983 and Eisenhardt, 1989). In fact, DAOs are not just a technological advancement but also a conceptual one, challenging established theories in economics, organizational behavior, and governance.

[20] For example, the two best-known internal risk management models were developed by JP Morgan as late as 1994 and 1997 —RiskMetrics for market risk and CreditMetrics for credit risk, and it was the publication of the RiskMetrics model which prompted the dissemination of the Value-at-Risk (VaR) concept. Adequate capital reserves for banks only became a concern in the early 2000s following the Enron bankruptcy in 2001. See Dionne (2013) for the main risk management milestones in finance.

[21] ERM is based on a set of standardized principles published by the Committee of Sponsoring Organizations of the Treadway Commission (COSO) in the United States in 2017. See also the guidance by Airmic and the Institute of Risk Management (IRM) – '*A structured approach to ERM and the requirements of ISO 31000*'. For an interesting discussion of the limitations of ERM in the context of integrated systems such as supply chains, see Sutton (2006) who argues that enterprise systems applications are redefining the boundaries of the entity in terms of risk management.

and objectives of an organization. One of the critical factors shaping the ERM perspective is the definition of risk moving away from "pure risk" or loss. Since Knight's *Risk, Uncertainty and Profit* was published in 1921[22], risk has been defined as the effect of uncertainty on objectives, meaning that risk could be positive, negative or both, resulting in both threats and opportunities. Risk management, therefore, is not about eliminating risk, which would be impossible as well as wasteful, but about anticipating uncertainty.

To our knowledge, risk management practices for DAOs and blockchain projects follow the siloed approach instead of the more modern ERM approach[23]. However, the blockchain economy is an opportunity for rethinking of risk management concepts and methods. For DAOs, risk management systems embedded in the tooling[24] could be designed, and therefore this research paper simply opens the conversation on these important issues, with much more work needing to be done (see **Part II**). Based on current best practices for identifying emerging risks, we believe that four methods could be most useful for risk identification in DAOs: SWOT (Strengths, Weaknesses, Opportunities, and Threats), the Delphi Method (a forecasting technique based on expert input), Scenario Planning, and the PEST (Political, Economic, Social and Technological Factors) Analysis. We will briefly review each in turn.

SWOT is an established and well-known method[25] for strategy formulation, which has already been suggested for DAOs[26], and which allows for collective input from DAO participants. While

[22] Discussed by Brooke (2010), two different concepts of "uncertainty" were developed in Frank Knight's seminal work *Risk, Uncertainty and Profit* published in 1921: the possibility of insuring against a certain outcome and subjective expectations about the future. This shapes modern risk management perspectives.

[23] As in all industries, risk management for DAOs started to develop around specific risks.

[24] The idea of embedding risk management in organizational architecture has already been discussed. See Barateiro et al. (2012) proposing an alignment between Risk Management, Governance and Enterprise Architecture activities. Almeida et al. (2019) found that enterprise architecture (EA) models and tools can help reduce the complexity of the ISO 31000 standard and improve the communication between stakeholders. See also Bąk (2023) for a study of 107 listed companies in the sectors of financial services, construction, and IT and seeking to determine how risk management was embedded in systems.

[25] See Helms and Nixon (2010) for a comprehensive review of the literature on SWOT analysis.

[26] See Boss (2022) who uses SWOT extensively to test whether DAOs can serve as organization structures for a larger range of activities including in traditional industries. For a specific project, strengths may include an active community, an advanced technical architecture, having successfully completed a smart code audit, etc., while opportunities might range from potential collaborations to new utility functions for tokens. Weaknesses of a specific project could be governance bottlenecks or legal ambiguity, and threats often arise from regulatory landscapes and competition. For DAOs generally, Boss (2022) identifies the following strengths and opportunities: flexibility in governance structures and voting processes, benefits of digital assets including easy onboarding of new members via governance token acquisition and on-chain control of assets, transparency, participatory nature leading to increased engagement, disintermediation leading to reduced transaction costs, and high potential for innovation, and as weaknesses and threats: the need for DAO members to invest considerable time and effort to effectively participate in decentralized governance, the absence of legal recognition of DAOs leading to personal liability and/or complicated structures for legal wrappers, anonymity of DAO members, absence of accepted codes of conduct, security issues, and the volatility of digital asset prices

SWOT is considered vague and simplistic in certain circles, it is also widely known and can be easily understood by DAO participants generally, providing a useful starting point for strategy planning[27]. In the blockchain economy, SWOT could be an ongoing and participatory process, where multiple stakeholders could weigh in on various aspects in real time.

The Delphi Method is a forecasting technique based on successive anonymous inputs on a certain topic by a diverse panel of experts. An example of its application in the context of blockchain is Schwerin (2018) addressing how blockchain is affected by privacy regulation and vice versa[28]. In DAOs, the community or a subset of DAO members could act as a panel, subject to maintaining anonymity of submissions, allowing for a consensus to be reached after several iterations. We believe that the Delphi Method can be aligned with decentralized governance models without compromising its efficacy and can be leveraged for strategic decisions, risk assessment, or even setting development priorities.

Scenario Planning serves to navigate uncertainty and anticipate possible futures[29], which is vital given the fast-paced evolution of the digital assets industry. Market trends, potential regulatory changes, and even changes in user behavior could be modeled, allowing DAOs to prepare for multiple eventualities, and become more resilient. For example, a project might use scenario planning to explore what would happen if a particular jurisdiction (where many of its members reside) suddenly imposes restrictive regulations negatively impacting DAO activities.

Finally, PEST is a management tool used to assess external macro-environmental factors to identify strategic risks impacting an organization[30]. Understanding these external forces is

[27] See also in **Part II** why we believe most DAOs are confronted with a "strategic gap" in terms of risk management. From this perspective, SWOT can be a useful tool for engaging the community in risk management and strategy investigations. Moreover, the success of a SWOT analysis generally depends on the thoroughness of investigation which is a function of time, number of experts, and the level of consensus, meaning that it is particularly adapted to community environments.

[28] After an initial literature review, the authors asked a panel of 25 experts to find opportunities, limitations and general suggestions about both topics (*i.e.* blockchain and privacy). In a first round, the panel received semi-structured questions related to the initial research hypotheses. In a second round, the initial responses were aggregated and the panel was given the opportunity to rank the issues, allowing for additional comments. Because the research topic was complex and future-focused, drawing from opinions of predictive and subjective nature, an optional round three in the form of a mini-workshop was suggested to discuss resulting frameworks and recommendations in a face-to-face setting. This was an exception to the traditional Delphi Method where experts cannot know each other's responses to avoid influencing their submission.

[29] Organizations can gain more clarity in their strategic approach by using scenario planning to strategize in a way that allows them to prepare for multiple futures, with multiple strategies. Essentially, this allows participants to be "mentally prepared" for turbulence and uncertainty. See Oliver and Parrett (2017) for a discussion of this method.

[30] PEST is centered around the idea of understanding external factors and evaluating how business models will have to evolve to adapt to their environment. PEST is often used in conjunction with SWOT and works well when the environmental factors are

paramount: DAOs exist in a universe of ambiguity, lacking a physical jurisdiction, but exposed to diverse political risks[31] based on membership base and operations. Digital assets are marked by extreme volatility[32]. DAOs - as community-driven entities - must understand societal trends and cultural shifts or risk reduced participation and loss of engagement from DAO members. Regular dialogue within the community can help identify and address potential social risks. Finally, technology is the backbone of DAOs, but this also means that DAOs are more exposed to risks related to rapid technological advancements. Due to their free-floating membership, DAOs must always stay ahead of technological trends, investing in research and development, and ensuring their systems are both secure and at the forefront of innovation.

Based on these methods, as well as a brief review of existing literature, we propose the following Risk Taxonomy for DAOs built around nine dimensions of risk:

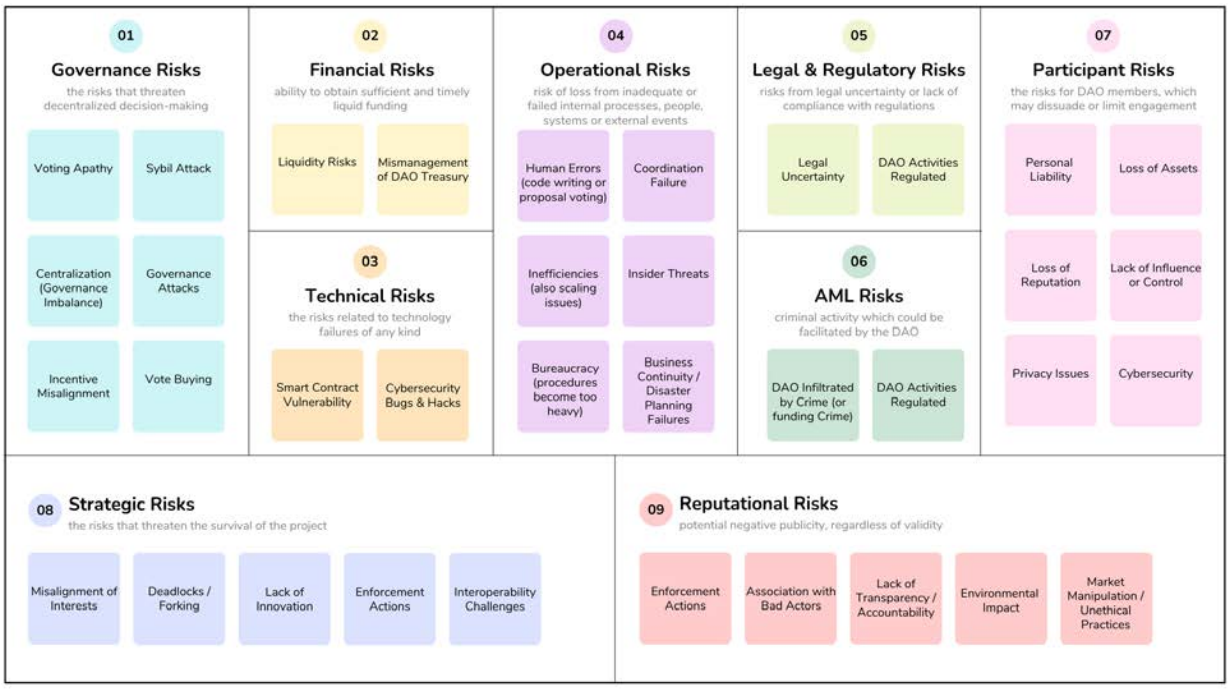


Table 1: Proposed Risk Taxonomy for DAOs

analyzed from the perspective of an organization's resources, capabilities, and core competences. PEST has five main stages: identifying PEST factors, analyzing possible effects on the organization, categorizing into opportunities and threats, prioritizing, and developing corrective or preemptive strategic action. See Sammut‐Bonnici and Galea (2015).

[31] It could be argued that this is the equivalent of a multinational company needing to monitor different countries for regulatory crackdowns, policy changes, or shifts in government stances.

[32] Economic downturns, inflation rates, and changes in cryptocurrency values can significantly affect DAO treasury and therefore operations.

Extensive research and work has been carried out on smart code vulnerabilities, tokenomics and design issues, in the categories of Financial[33] and Technical Risks[34]. These are outside the scope of this research paper. It will also be noted that we did not include Default or Counterparty Risk[35] or Market Risk. This is because these risk categories are not specific to DAOs; however, they should not be ignored. To the extent a DAO has significant exposure to such risks, we believe that they belong in the Financial Risks or the Strategic Risks categories.

"*DAOs are an experiment in governance.*"[36] In our view, Governance Risks are some of the most significant for DAOs[37]. For their analysis, it is of capital importance to distinguish between DAOs as cybernetic organisms with automated functions and minimal human participation[38], vs. DAOs as "collectives" of individuals using blockchain-based governance systems to participate in decentralized decision-making[39]. In the first case, risk management is a design issue[40], a novel engineering problem[41]. In the latter case, risk management is a human issue, and we have plenty of examples from existing organization theory, ranging from startups and regular corporate structures, to associations and trade guilds, to cooperatives, to public companies, to democratic

[33] Many DAOs related to Decentralized Finance (DeFi) and stablecoin projects have implemented monitoring of certain key metrics designed to address Financial Risks. We have listed *Liquidity Risk* and *Mismanagement of DAO Treasury* as the most significant risks DAOs face, but depending on the activity, there will be many others, and we leave this analysis to specialists. We note in passing that certain Financial Risks may be amplified due to the presence of pseudonymous actors, such as rent extraction through grants (Goldberg and Schär, 2023).

[34] The literature regarding Technical Risks for DAOs is equally extensive, and this research paper specifically does not address these. We listed *Smart Contract Vulnerability* and *Cybersecurity* issues as the most significant at a high level.

[35] This covers probability of default, recovery rate, exposure at default.

[36] *Decentralized Autonomous Organization Toolkit*, published by the World Economic Forum (WEF) in January 2023.

[37] Starting from the assumption that decentralized decision-making is the key characteristic of DAOs, it can be argued that risks which threaten this deserve their own category.

[38] Certain researchers view DAOs as cybernetic organisms which can become self-sustaining in the long term, including via including robots and "digital humans" or AI which would guide humans (Qin et al., Li et al., 2023).

[39] Boss (2022) distinguishes between DAOs based on algorithmic structures (underlying smart contracts dictate the entire functionality of the DAO, *i.e.* fully automated systems), vs. DAOs based on a participatory structure and distributed consensus, (smart contracts are merely used to aggregate the votes or preferences of the members). Arguably the latter model has significant advantages insofar as it prevents developers from taking actions that would not benefit users/DAO members, and allows more flexibility for the project to comply with regulatory requirements and emerging risks (Wright, 2021).

[40] It could be argued that even in participatory DAOs the separation of decision management and decision control rights to avoid self-monitoring, self-reward, and self-punishment - Beck et al. (2018) - is a design issue. Decision management rights are for example generating DAO proposals, and executing or implementing decisions. Decision control rights allow ratification of decisions (deciding whether decisions are to be implemented) and also relate to the monitoring functions. Most regulators require segregation of duties to avoid conflicts of interest in regulated entities. To the extent that DAOs want to implement best practices, these rules should be used in the design of the DAO governance mechanisms.

[41] See for example Onjewu et al. (2023) who argue that most of the well-known agency-principal issues in organization theory are not applicable to blockchains.

decision-making[42]. This ties into the well-known distinction made in literature between on-chain and off-chain governance of DAOs[43].

Many DAOs have already addressed certain types of Governance Risk, and a body of research has slowly developed around *Sybil Attacks*[44], *Governance Attacks*[45], etc. Governance Risks can also have significant overlap with Technical and Operational Risks, as well as Strategic Risks. We also listed *Voting Apathy* here because the risk of low participation in governance decisions can lead to decision-making power being concentrated among a small group and/or paralyze the DAO if the participation is lower than the quorum[46]. It can also leave the DAO vulnerable to *Governance Attacks*. If DAO members become disengaged and do not participate in governance decisions, then the overall system is weakened and also the DAO loses part of its purpose which includes decentralized decision-making[47]. Certain projects attempt to resolve this problem by designing working groups voting on specific issues within a DAO, with public votes reserved for major decisions only, but this could lead to an erosion of decentralized decision-making.

---

[42] Our position is that DAOs are mostly a collection of individuals using automated systems for governance and decision-making to reach common goals. Therefore agency issues are still very much relevant. As highlighted by Jensen and Meckling (1976), agency problems arise due to the misalignment of interests between agents (managers or decision-makers) and principals (owners or stakeholders). DAOs, while decentralized, are not immune to such conflicts. Token holders (principals) might not fully understand actions taken by core developers (agents), leading to issues of trust and potential misuse of power. See also Eisenhardt (1989) for further perspectives on how internal controls can minimize these risks. Filippi et al. (2020) argue that blockchain in reality shifts trust from centralized intermediaries to code and network participants, which implies that governance issues are critical. According to the authors, decentralization creates unique governance hurdles, like achieving consensus across diverse and dispersed stakeholders and the difficulty of updating or rectifying mistakes.

[43] Hsieh et al. (2017) distinguish between internal and external governance features, and argue that internal governance is tied to the design of incentives, while the effectiveness of external governance depends on the influence exerted by the community, the media, and the general public over the organization. Our proposal is to include the community factors within the Governance Risks analysis, and the media and general public in the Reputational Risks analysis.

[44] In a Sybil Attack, a participant creates multiple identities to gain undue influence over a system, for example multiple wallet addresses to skew voting outcomes. For this reason decentralized systems cannot rely on "one person, one vote" schemes unless they verify identity, leading to the "weak identities problem" (Goldberg and Schär, 2023). Measures protecting against a Sybil Attack include Proof-of-Stake (PoS), identity verification (cryptographic methods and zero-knowledge proofs, Gitcoin's proof of humanness, etc.), limits on participation or cooldown periods, tying participation to certain actions, or electing a set of trusted delegates. See also Douceur (2002) for a very early discussion.

[45] Garimidi et al. (2022) cite the example of Steem, subject to a governance attack by Justin Sun who wanted to merge Steem into Tron and acquired 30% of the total token supply in a private deal. Steem initially froze Sun's tokens, which led to a public to control enough tokens to change top 20 witnesses controlling the network and reverse the decision. They also cite a different type of governance attack in Beanstalk, when a wallet took out a flashloan to acquire enough governance tokens to pass a malicious proposal allowing them to seize $182 million reserves. Due to the flashloan mechanism, this was over before anyone had time to react. The authors suggest that the main cause of Governance Risks is that "market mechanisms for token allocation fail to distinguish between users who want to make valuable contributions to a project and attackers who attach high value to disrupting or otherwise controlling it", and propose a framework for assessing and addressing vulnerability based on a three-prong strategy designed around decreasing the value of attacks, while increasing the cost of acquiring voting power and of executing attacks

[46] This is a problem encountered in democracies everywhere, as well as public companies. Simply giving DAO participants more incentives to vote (or penalizing absenteeism) is not in itself sufficient to protect against Governance Risks if they just follow the majority vote or delegate their voting power. Many DAO projects are experimenting with weighted or quadratic voting.

[47] See also Hsieh et al. (2017), who argue that decentralization distinguishes blockchain-based corporate governance from the traditional model based on hierarchies. Accordingly, in the absence of decentralized decision-making, there is no DAO.

In existing literature, Beck et al. (2018) found that even if smart contracts allow for decentralized governance mechanisms, the blockchain economy was still characterized by a high degree of centralized decision-making, which in the opinion of the authors is necessary in the early stages of a project for effective system design[48]. This is in line with the findings of a later study by Appel and Grennan (2023) who reviewed 10,639 proposals across 151 DAOs and concluded that a small number of entities effectively influenced or determined most decisions. Both articles placed DAOs squarely in scope of agency theory, with Appel and Grennan arguing that when ownership is dispersed, individuals have very weak incentives to monitor performance and/or compliance (effort to monitor > utility gained) and to participate in decision-making[49]. Goldberg and Schär (2023), in the first study focused on the metaverse decision-making, analyzed Decentraland data from Ethereum and snapshot.org including all submitted proposals, wallets and votes[50]. They found strong empirical evidence that many proposals were effectively decided by few individuals and concluded that many of the issues identified as Governance Risks were really a consequence of pseudonymous token-based voting, suggesting future improvement would be possible via adoption of a bicameral system (pseudonymous token-based voting plus known delegates) to mitigate the "weak identities problem".

Filippi et al. (2020) argue that instead of the promised disintermediation of blockchain, in reality new intermediaries have emerged, such as miners in Proof-of-Work (PoW) or validators in Proof-of-Stake (PoS) systems, with their own interests which can sometimes conflict with those of the broader community, so we must add *Incentive Misalignment* here[51]. Overall, Governance

[48] The study argues that incentives are crucial for the blockchain economy to function effectively, because of their role in the formation of consensus among the nodes/validators of the blockchain. This points to tokenomics being an area of strategic risk for DAOs (see below *Risk Taxonomy for DAOs*). Beck et al. (2018) illustrates well one of the risks of the current forms of DAOs, which are in the process of being decentralized but still somewhat guided by their founders, namely the risk that the founders team does not relinquish control, but instead add milestones to the initial vision, seeing themselves as instrumental to maintain the goals and the quality of the project. Irrespective of whether this is a valid concern in practice, it opens the project to additional risks resulting from the lack of sufficient decentralization - the risk of legal enforcement action based on securities laws, the risk of non-compliance with regulatory requirements applicable to centralized business models, etc. See also the definition of sufficient decentralization proposed by Axelsen et al. (2022): "a verifiable state, where (1) the design of the DAO is collusion resistant and based on long-term equilibrium; (2) its governance processes have unrestricted and transparent access".

[49] This is a similar problem to the absenteeism of small stakeholders in large public companies - the effort to participate in proxy voting is greater than the utility gained, especially if the shares are held for investment purposes. In the context of DAOs, due to the critical importance of decentralization as well as a number of legal and regulatory risks related to the absence of decentralization we would place absenteeism among the high risk factors for DAOs, which should be included in the Risk Dashboard and carefully monitored.

[50] 1,414 proposals submitted by 789 Ethereum addresses between May 24, 2021 and December 08, 2022, and 45,333 cast votes submitted by 4,345 addresses.

[51] But see also the discussion below on Strategic Risks.

Risks should be reviewed from a systems thinking perspective, including identifying key players[52]. This is also connected to the *Centralization (Governance Imbalance)* risk[53].

We have listed *Inefficiencies* as part of the Operational Risks of DAOs, but it should be stated also that a certain level of inefficiency is embedded in the DAO design due to decentralization[54]. The analysis of how value is created in organizations has so far focused on startups and entrepreneurship or intrapreneurship[55]. Decentralized organizations depart from this wisdom - instead, the value proposition is that large, intelligent, self-organizing cybernetic collectives may be slow to learn and act at the beginning but have more sustainability, fairness and resilience in the long term due to the advantages of blockchain technology and constant improvement[56].

Due to their decentralized nature, DAOs face many operational challenges, including recruiting and onboarding contributors, establishing relationships in the traditional economy, and payments in *fiat currency* to external service providers. Some DAOs limit themselves to cryptocurrencies payments only, which places them at a strategic disadvantage and opens them to additional *Market Risk*. Alternatively, they manage operations via smaller structures (including operational subsidiaries or sub-DAOs), or delegating specific tasks to certain DAO participants or third party service providers, leaving themselves open to *Counterparty Risk*.

One of the most revolutionary aspects of DAOs is their ability to operate beyond national borders, which represents both an opportunity and a challenge. Work organization is often fluid, with contributions coming from multiple members, each perhaps specialized in different tasks[57].

---

[52] Certain actors (proposal creators or significant token holders) can emerge as influential figures, and from a systems thinking perspective their roles and motivations need to be understood in the context of the DAO's overall governance.

[53] For example, Atzori (2015) argues that scalability leads to a natural process of centralization for any Proof-of-Work (PoW) network, due to the decrease of the number of miners and growing costs.

[54] In modern corporate structures, decision-making is often hierarchical or centralized because of the efficiency gains (Beckhard, 1966). See also Hsieh et al. (2017) who argue that there is a trade-off between decentralization and efficiency. In this respect, King (1984) on centralization vs. decentralization is still relevant today and provides insights into the operational challenges that can arise for DAOs. The study by Christie, Joye, & Watts (2003) also shows how decentralization can complicate communication and make governance less efficient.

[55] "The Founder's Mentality", a concept popularized by Chris Zook and James Allen in their book of the same name, focuses on the core principles that fuel successful startups, and how these can be harnessed in more complex organizations.

[56] See also Beckhard (1966) focusing on the challenges and opportunities presented by decentralized organizational structures. Insights regarding the difficulties of implementing change in decentralized organizations are relevant for DAOs and suggest a nuanced approach that involves both "hard" rules and "soft" influences.

[57] This modularity and flexibility in labor division could be aligned with traditional theories that talk about goal partitioning in organizations (Freeland & Baker, 1975) and about sustainable collaboration (Kumar & Dissel, 1996).

From a governance perspective, this organization of work may introduce a sort of "polycentric governance" where multiple centers of decision-making exist[58].

We have included *Insider Threats*[59] as part of Operational Risks because typically this relates to a systems failure (*i.e.* failure to implement controls or malicious behaviors), but it could also be a design issue. For the same reason, we propose that *Business Continuity / Disaster Planning Failures* should be included as part of Operational Risks[60], but it is obvious that the lack of a clear business model and value proposition is also part of the Strategic Risks.

Due to the legal uncertainty surrounding DAOs and related projects, we have included Legal & Regulatory Risk as a distinct category, also taking into account that the expertise needed to monitor and address these risks is lacking among DAO participants. We have highlighted *Legal Uncertainty* and the specific risks when the DAO activities fall under scope of regulations (for example, Decentralized Finance (DeFi) projects)[61]. Using legal offshore structures as a "legal wrapper" may help mitigate legal uncertainty and regulatory risks for the DAO and its members, but brings a different set of challenges[62]. Historically, offshore legal structures have been used (and they have been designed for) sophisticated users[63]. For DAOs, there is much learning to be done. From a risk management perspective, there could be a significant lack of understanding about how offshore legal structures actually work, significant misperception and misalignment. Additionally, not many offshore service providers are able to work with individual users such as

[58] This is also one of the reasons which explain why offshore legal structures can be used effectively for DAOs.
[59] See as an example, a discussion regarding the abuse of Admin privileges on Coordinape - https://forum.bankless.community/t/regarding-the-previous-dao-wide-coordinape-admin-whales/4958
[60] Atzori (2015) discusses the major risks related to business continuity of blockchain protocols and DAO-type structures - first, DAO members may not be motivated to continue, and second connectivity issues.
[61] Starting with Beck et al. (2018), authors have discussed another type of legal and regulatory risk - if DAO members engage in business activities via a peer-to-peer platform, they will likely fall in scope of regulations themselves (if they are not agents of the DAO), or the DAO will be considered a partnership and engaging in business activities. While most regulatory frameworks have not been designed for decentralized business models, it will not take long for regulators to adapt them to the new blockchain economy. This misunderstanding by DAO members of the consequences of carrying out business activities as part of a DAO can be dangerous. From this perspective, incorporating offshore does not help except in cases of "reverse solicitation" where allowed, and some legislations do not even allow for this exception (such as the United States).
[62] The treatment of an offshore legal structure attached to a DAO cannot be guaranteed. It is likely that any judge would adopt a facts and circumstances approach - the existence of any type of legal structure attached to the DAO does not entirely eliminate the Participant Risks, especially if DAO members act outside of the objectives set out in the Memorandum and Articles of Association (or similar document) and/or outside the knowledge of the Board of Directors. It would still be possible for a court to determine that a certain DAO member has acted as a de facto manager or director, or that a partnership has been established with respect to certain activities and operations.
[63] Typically, high net worth individuals (HNWIs), family offices, investment funds, and multinational companies.

DAO members[64], who typically require more guidance and support, and take longer to reach consensus because of decentralized decision-making and the need for transparency. DAO members rely on the information presented in the DAO proposals, which may be incomplete, or, despite much transparency in sharing information at the outset, there may be little understanding of the interdependencies which would need to develop between the DAO and the offshore legal structure[65]. For this reason, it becomes necessary to review several levels of Legal and Regulatory Risks: for participants, for the DAO, for the Board of Directors of the offshore legal structure, for technical committees and multisig signatories. Due to the pseudo-anonymous nature of blockchain, we also believe that risks related to money laundering and terrorist financing (AML Risks) should be understood, assessed and monitored separately[66]. For DAOs using offshore legal structures as "legal wrappers", there are additional considerations related for example to the automatic applicability of standard Proceeds of Crime legislations, or the legal requirements imposed by offshore jurisdictions on service providers working with DAOs[67].

We suggest that Participant Risks should be an entirely new category, specific to DAOs. Most risk management frameworks are not concerned with the risk to stakeholders beyond monitoring health and safety and environmental concerns. In our view, due to the nature of the DAOs as free-floating "collectives", projects must understand and address these issues in order to attract good-quality contributions and membership. One of the most significant Participant Risks is related to personal liability for DAO activities and operations. To the extent that these fall within scope of existing regulations (for example, Decentralized Finance (DeFi) projects[68]), token holders can be exposed to personal liability as well as enforcement actions.

---

[64] While DAO-specific service providers have started to grow in destinations such as the Cayman Islands, they are still a scarce resource.

[65] See in **Part II** the discussion regarding the role of the Board of Directors in risk management.

[66] They are closely tied into Legal & Regulatory Risks in those cases when DAO activities fall under scope of regulations. However, they also tie very closely into Reputational Risks and Strategic Risks.

[67] To illustrate, the Cayman Islands foundation company, which is often used by DAOs, is required to have a Secretary appointed which is a local service provider with a company license regulated by the Cayman Islands Monetary Authority (CIMA). This Secretary has its own requirements with respect to AML Risks, but also specifically is tasked with monitoring AML Risks for the foundation company structure, especially in the context of contributions made and gifts received. The Board of Directors cannot accept such contributions and gifts without receiving a "notice of no objections" from the Secretary. These requirements are not always properly understood by DAOs.

[68] For example, Blockscience (2022), analyzing vulnerabilities for LIDO, states "LDO token holders are the owners/managers of the platform". If this statement is true, then the LDO token holders may be subject to additional risks if they hold sufficient tokens or are sufficiently active in the network. This example shows why it is important for a DAO to correctly identify, assess and manage Participant Risks. Failure to do so may result in lower participation and DAO members disappearing in crisis situations or if threatened with enforcement actions.

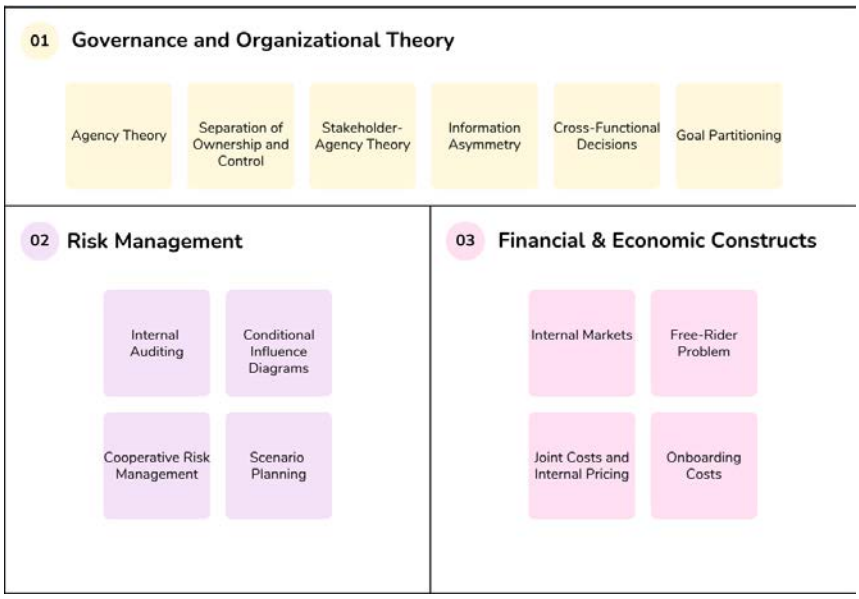
DAOs and underlying blockchain projects are under a lot of scrutiny from regulators and the public. For this reason, we argue that mature DAOs need to carefully monitor and address their Reputational Risks, and we have included here a wide range of risks from *Enforcement Actions*, *Association with Bad Actors*, *Lack of Transparency / Accountability*, *Environmental Impact*, to *Market Manipulation* and other *Unethical Practices*[69]. Transparency is key for DAOs because as we saw earlier using tokens to incentivize participation in decision-making does not eliminate the principal-agent problem. Information asymmetry[70] can still exist, which leads to the need to create transparent protocols for decision-making and financial transactions. Still, large token holders or founding members might have more information than smaller actors, creating an imbalance in decision-making power and risk exposure[71].

Finally, one last dimension of risk which must be analyzed carefully is linked to risks which could potentially threaten the continued existence of the DAO. We consider that the most significant Strategic Risks are linked to *Misalignment of Interests* between DAO members (which ties into the importance of incentives in the blockchain economy), *Deadlocks and Forking*[72], *Lack of Innovation*, *Enforcement Actions* and finally *Interoperability Challenges* (which also include user experience issues).

One important aspect to consider here is the **interconnectedness** of these dimensions of risk. As highlighted by Hsieh et al. (2017), decentralized governance relies on the proper functioning of consensus algorithms and smart contracts, and the correct design of tokenomics, but these are only a few aspects to be considered. We suggest that multi-layered risk management strategies specific for DAOs should be developed from traditional models, embedded directly in DAO tooling[73] and reinforced by internal audits. Hong and Apostolakis (1993) discuss the use of

[69] See also Atzori (2015) who argues that decentralization is not always the best choice for all organizations and that smart contracts are not meant for policy-making and areas of activity which should remain human-centric and focused on ethics.
[70] Atzori (2015) argues that Bitcoin stakeholders lack essential information on security issues, because of a strong information asymmetry between core developers, pool managers and users. See also Mishra, Heide, & Cort (1998).
[71] On the systemic consequences of information asymmetry, see also Dionne (2013).
[72] Decentralized and open-source architecture allows the community or a dissenting minority to effectively clone and deploy another instance of the blockchain, with an alternative governance system (Goldberg and Schär, 2023). While we list *Forking* as a Strategic Risk, it could be argued that the threat of *Forking* and its consequences for the survival of the DAO may keep dominant actors in check and ameliorate the problem of *Governance Imbalance* (see above in Governance Risks).
[73] DAO tooling for risk management purposes is taking shape. See https://github.com/defi-defense-dao/defi-risk-tools-list which includes resources for several categories of risks including Financial Risks, Smart Contract Risks, and Centralization Risks. Embedding risk management in DAO tooling would also have the advantage of ensuring implementation irrespective of the diligence of DAO members at a certain point in time. For context, Dionne (2013) argued that many investors lost large amounts

conditional influence diagrams in risk management, an approach that could be useful to DAOs as well. A list of useful concepts from traditional literature is included in Table 2 below:



Part II:

Based on the analysis carried out in **Part I**, we propose a few basic principles for a Risk Management Framework for DAOs, in alignment with modern practices and ISO 31000:2018, the international standard for risk management[74]. At a minimum, we suggest that two simple strategies for risk management at the DAO level could easily be implemented while further research is carried out: first, promoting organization-wide learning - potentially via allocating additional tokens or voting power to DAO members who are willing to learn and participate; second, creating "Guardian Roles" within the community for people with specialized skills in risk management and who will be able to spot risk-generating activities or behaviors.

during the financial crisis for three reasons: lack of clear definition of risk appetites, absence of an integrated approach to risk management, and independent risk management policies not being supported by top management.

[74] We wanted to mention the ISO standards but of course the full detail is outside the scope of this research paper. In practice, the concept of a framework is used to refer to all the policies, procedures, processes, and tools which are used for an organization's risk management activities, which provide a coherent structure for the management of risks.

A typical Risk Management Framework (RMF) is comprised of a risk appetite statement (RAS)[75], a three lines of defense (3 LOD) (or similar defense in-depth) model designating the roles and responsibilities of several categories of stakeholders with regards to risk management, and a set of processes and tools for risk identification and monitoring (taxonomy, key risk indicators (KRIs), etc.) and management of risk. In a typical corporate structure, the Board of Directors, management, the Risk and Compliance Team, as well as regular stakeholders all have different roles in risk management. The Board of Directors, for example, is responsible[76] for the annual (or more frequent) overview of major risks, the amount of risk the organization is willing to accept to achieve its objectives, as well as strategic discussions as to where engagement of different stakeholders[77] is needed to mitigate the risks identified. Because of the decentralized decision-making in DAOs, it is typical that even if the DAO is tied to a "legal wrapper" the role of the Board of Directors is greatly reduced[78], so the strategic review should also be carried out at the DAO level. Consequently, a Risk Management Framework for DAOs needs to specifically address the strategy and oversight function, how it could be delegated as part of the DAO design, and the necessary interactions with the Board of Directors of any legal structures used.

Arguably, the early contributors in a DAO, and especially the original founders of a project, are the first engineers of the DAO strategy. In the early stages, they often maintain control or at least the possibility of exercising control, so that the project maintains coherence in alignment with

[75] This is a high-level indication of how much risk an organization is willing to take, accept or tolerate to achieve its goals and objectives. DAOs are generally risk-seeking organizations with a high tolerance of risk; however, among the different categories of DAOs and areas of activity there should be different risk appetites. For instance, stablecoin and DeFi projects should have low risk appetites, whereas gaming and Web3 projects could have higher risk appetites. To our knowledge, no review of DAO risk appetite profiles exists, so we note this as another area of research.

[76] In DAOs attached to a "legal wrapper", the Board of Directors has a fiduciary duty to maintain this role. For a Cayman Islands foundation company, for example, Directors have certain fiduciary duties as well as a general duty of care, skill and diligence, irrespective of the limitations and restrictions tied to the need to follow the DAO consensus mechanisms. The fiduciary duties require Directors to act loyally, honestly and in good faith in the best interests of the company (the duty is owed to the company itself); exercise their powers only for the purpose for which they were conferred and not for any personal or collateral purpose; maintain confidentiality; avoid a potential conflict of interest (if any, it needs to be disclosed, and no personal profits may be drawn from it); act in a manner likely to promote the success of the company; exercise independent judgment (and not compromising or restricting their ability to exercise independent judgment - this is particularly relevant for DAOs); not retain for their own benefit or passing to third parties property of the company; not act beyond the powers allocated to them; and act in accordance with the Memorandum and Articles of Association. Any Director must act with the skill, care and diligence that might reasonably be expected of them based on the circumstances. In practice, this implies a certain level of competence, a sufficient knowledge and understanding of the DAO, as well as a proactive attitude. If Directors are appointed for the foundation company from among community members, best practices in terms of risk management require additional training for them, with respect to their role in risk management and other legal obligations.

[77] Under the stakeholder-agency theory outlined by Hill and Jones (1992), stakeholders are not just token holders but can also include developers, regulators, and even entities interacting via smart contracts. It can be argued that a multi-faceted governance approach that accounts for these different stakeholders could make DAOs more robust and adaptable.

[78] In some cases, Directors may not receive sufficient information unless they also actively participate in the DAO forums.

the original vision and objectives. This is often problematic and advised against by scores of lawyers, due to potential personal liability, tax, and securities laws issues. The pressure from the public, the community as well as the regulators is to decentralize as fast as this is feasible. Thus, most DAOs have a "strategic gap" when it comes to risk management and how risk informs strategy. To understand the importance of this issue, we need to dive deeper into management roles. In an article entitled "*Blockchain and the Chief Strategy Officer*", Sandberg et al. (2019) explain that the role of strategy is to future-proof the organization, which includes "identifying growth opportunities, managing the strategic-planning process, monitoring long-term trends, and maintaining competitive intelligence". DAOs mostly rely on the collective intelligence of their most active contributors to carry out this function, with the understanding that such contributors will make proposals in line with the goals of the organization and generate enough momentum to allow for the adoption by the relevant consensus mechanisms. This is an unstructured approach, akin to the early stages of the strategy function in corporate organizations, and we argue that it is not sufficient to enable DAOs to become better organizations.

Setting aside strategy and oversight roles, management plays a critical role in a typical Risk Management Framework. In line with modern practices, management should have a holistic view of the risks at any given time for risk-informed planning and decision-making, the ability to set up commensurate controls and mitigation measures, the ability to prioritize and raise awareness of the most significant risks so that resources are allocated efficiently, the ability to address and document risks and opportunities in a structured and systematic way, and the ability to involve staff for execution. It is very difficult to find the right DAO contributors who would be able and willing to serve in this capacity for the simple reason that they would risk being considered in control of the DAO. Because of its decentralized nature, a DAO is therefore forced to rely on either third-party service providers who would serve as risk monitors, or on individual DAO contributors participating in Risk Core Units, knowing that these DAO contributors would still have to go through the proposal and voting mechanisms to execute on their findings. It follows that in addition to the "strategic gap" when it comes to risk management, DAOs also have a "management gap". This requires a much more methodical and systematic approach to risk management, so that different DAO contributors can be allocated and effectively cover all relevant areas of risk identification, monitoring and management. This is why we believe that

developing the Risk Taxonomy of DAOs is of capital importance, together with the creation of specialized roles and functions, and educating the DAO community. In addition, market-based risk management mechanisms could be developed to prioritize risks and allocate resources[79].

Finally, in a typical Risk Management Framework, a significant role is played by the Risk and Compliance Team (the equivalent in a DAO would be a Risk Core Unit[80]), which develops common language and minimum standards, ensures that risk approaches within the organization are coherent and in line with the risk appetite, and is able to provide guidance and training as well as advice and assistance to staff. We argue that as part of a Risk Management Framework for DAOs this specialized team of contributors should play a more active role to cover portions of the "strategic gap" and "management gap".

Two strategies which we propose as pillars of a Risk Management Framework for DAOs, taking into account decentralization needs, are Risk Dashboards and Guardian Roles.

Risk Dashboards are increasingly becoming a cornerstone in risk management, particularly for allowing Boards of Directors to have a high-level view of the most significant risks which shape an organization's strategy. Risk Dashboards are real-time, interactive tools that compile and display essential risk-related metrics, providing a unified view of the organization's risk profile. In the context of DAOs, Risk Dashboards would allow community members to have a better understanding of the risks without the need to invest a lot of time and effort. This paper argues that this will improve transparency and increase confidence in the DAO, as well as participation.

[79] For example, Kouvelis and Lariviere (2000) discuss intra-company coordination through internal markets, a concept that DAOs and coalitions of DAOs can easily adapt for resource allocation. Previously, Shubik (1962) discussed the role of internal pricing as a way to allocate resources and costs within a firm, essentially as a control mechanism.

[80] As an example, MakerDAO includes a Risk Core Unit, which developed their own internal framework for risk assessment, including qualitative and quantitative risk metrics of crypto collateral assets. The Risk Core Unit also has community outreach functions including interacting with and educating DAO members. The MakerDAO Risk Core Unit is focused on financial risks of the protocol (with metrics such as VaR (Value at Risk), Debt Ceiling (IAM), Liquidation Ratio, Surplus Buffer, etc.), while smart contract risks are addressed by Smart Contract Core Units. This corresponds to the siloed approach to risk management, which is the initial stage before moving towards a more integrated approach to risk management. This approach is still effective as demonstrated by Kjäer et al. (2021) who reviewed the stability of the MakerDAO protocol, based on its operations from November 2019 to 2020, including the cryptocurrency crisis in March 2020, based on the publicly available data of Ethereum.

A unique but promising strategy for risk management in DAOs is the concept of "Guardian Roles"[81]. Guardians could be specialized strategy, risk management and governance roles within a DAO structure, tasked with overseeing specific risk areas such as legal compliance, financial stability, or cybersecurity. Guardians could be elected by the community and could be given additional voting power (weighted voting) in their area of expertise. We suggest that Guardians could bring a layer of expertise and insight above the average DAO participant, and could be instrumental in a crisis scenario, when DAO members are likely to get overwhelmed and not have sufficient knowledge to act in the best interests of the project in the long term.

Of course, both Risk Dashboards and Guardian Roles have their limitations. In particular, Risk Dashboards are unlikely to capture qualitative aspects of risk, and are limited by the quality of the underlying data. They may be susceptible to faulty design and even manipulation. Guardian Roles might contribute to concentrating power in a few hands, thus diminishing decentralization. Because DAOs are still in their experimental phase, it is unlikely that current risk management solutions are mature enough to deal with the emerging risks and complexities from this paradigm shift. An essential part of DAO risk management is therefore continuous learning from other projects, education of DAO community members, and testing of new approaches.

[81] DAOMeter includes "community stewards" in its review methodology,a related concept although not quite identical. See Ziegler and Zehra (2023) for a comprehensive review of existing DAO studies and scoring methodologies.

Conclusion

In the blockchain economy, mobility and fluidity are key. DAO members gravitate towards the projects that are a good fit for them, requiring DAOs to remain open, evolving systems[82]. As mentioned in **Part II**, in traditional risk management theory, banks and other financial institutions apply the principles of defense in-depth, or lines of defense (LOD). For DAOs, this could mean employing a mix of risk management strategies, either embedded in design or participatory, and functioning synergistically. This multi-layered approach would increase the resilience of DAOs, making them more robust against various types of risks and uncertainties. At the most granular level, DAO members already engage[83] in due diligence, vote responsibly, and participate in governance proposals. Collective strategies like Risk Dashboards and Guardian Roles could come into play as structured mechanisms for managing risks. Industry-wide best practices could be developed via service providers, industry associations, or DAOs providing tooling or specialized expertise, offering another layer of risk management solutions as well as potential candidates for Guardian Roles. Finally, in the long term, regulatory frameworks will play a critical role in establishing industry risk management best practices.

[82] DAOs are dynamic entities that need to constantly evolve. Lessons can be drawn from traditional organizations - see for example Beckhard (1966) and Freeland and Baker (1975). This begs the question whether having categories of DAO members would not be beneficial - from visitors / users to technical group members to core team - with concentric circles of access and attributions.

[83] High engagement and better quality could be achieved by adding incentives for certain value-adding or risk-reducing activities.

REFERENCES

Adams, M. (1994). Agency theory and the internal audit. Managerial Auditing Journal, 9(8), 8-12. https://doi.org/10.1108/02686909410071133

Almeida, R., Teixeira, J. M., Silva, M. M. d., & Faroleiro, P. (2019). A conceptual model for enterprise risk management. Journal of Enterprise Information Management, 32(5), 843-868. https://doi.org/10.1108/jeim-05-2018-0097

Appel, I. and Grennan, J. (2023). Control of decentralized autonomous organizations. AEA Papers and Proceedings, 113, 182-185. https://doi.org/10.1257/pandp.20231119

Atzori, M. (2015). Blockchain technology and decentralized governance: is the state still necessary?. SSRN Electronic Journal. https://doi.org/10.2139/ssrn.2709713

Axelsen, H., Jensen, J. R., & Ross, O. (2022). When is a dao decentralized?. Complex Systems Informatics and Modeling Quarterly, (31), 51-75. https://doi.org/10.7250/csimq.2022-31.04

Bąk, S. (2023). The embedment of risk management in enterprise management system. International Journal of Contemporary Management, 59(2), 1-16. https://doi.org/10.2478/ijcm-2022-0014

Barateiro, J., Antunes, G., & Borbinha, J. (2012). Manage risks through the enterprise architecture. 2012 45th Hawaii International Conference on System Sciences. https://doi.org/10.1109/hicss.2012.419

Beck, R., Müller-Bloch, C., & King, J. L. (2018). Governance in the blockchain economy: a framework and research agenda. Journal of the Association for Information Systems, 1020-1034. https://doi.org/10.17705/1jais.00518

Beckhard, R. (1966). An organization improvement program in a decentralized organization. The Journal of Applied Behavioral Science, 2(1), 3-25. https://doi.org/10.1177/002188636600200102

Boniel, M. (2023). From Code to Consequence: CFTC Obtains Default Judgment Against Ooki DAO for Commodity Exchange Act Violations, available at https://www.blockchainandthelaw.com/2023/07/from-code-to-consequence-cftc-obtains-default-judgment-against-ooki-dao-for-commodity-exchange-act-violations/

Boss, S. (2022). DAOs and the future of governance. Master's Thesis Economics. Nijmegen School of Management. https://theses.ubn.ru.nl/items/52d8c11a-6b93-40d3-b300-230699d61671

Brickley, J. A., Coles, J. L., & Terry, R. L. (1994). Outside directors and the adoption of poison pills. Journal of Financial Economics, 35(3), 371-390. https://doi.org/10.1016/0304-405x(94)90038-8

Brooke, G. (2010). Uncertainty, profit and entrepreneurial action: Frank Knight's contribution reconsidered. Journal of the History of Economic Thought, 32(2), 221-235. https://doi.org/10.1017/s1053837210000179

Coase, R. H. (1937). The nature of the firm. Economica, 4(16), 386-405. https://doi.org/10.1111/j.1468-0335.1937.tb00002.x

Christie, A. A., Joye, M. P., & Watts, R. L. (2003). Decentralization of the firm: theory and evidence. Journal of Corporate Finance, 9(1), 3-36. https://doi.org/10.1016/s0929-1199(01)00036-0

Dionne, G. (2013). Risk Management: History, Definition and Critique. Risk Management and Insurance Review 16, 2, 147-166, 2013, http://dx.doi.org/10.2139/ssrn.2231635

Douceur, J. R. (2002). The Sybil Attack. Peer-to-Peer Systems, 251-260. https://doi.org/10.1007/3-540-45748-8_24

Eisenhardt, K. M. (1989). Agency theory: an assessment and review. Academy of Management Review, 14(1), 57-74. https://doi.org/10.5465/amr.1989.4279003

Fama, E. F. (1980). Agency problems and the theory of the firm. Journal of Political Economy, 88(2), 288-307. https://doi.org/10.1086/260866

Fama, E. F., & Jensen, M. C. (1983). Separation of Ownership and Control. The Journal of Law and Economics, 26(2), 301-325. https://doi.org/10.1086/467037

Freeland, J. R. and Baker, N. R. (1975). Goal partitioning in a hierarchical organization. Omega, 3(6), 673-688. https://doi.org/10.1016/0305-0483(75)90070-5

Goldberg, M. and Schär, F. (2023). Metaverse governance: an empirical analysis of voting within decentralized autonomous organizations. Journal of Business Research, 160, 113764. https://doi.org/10.1016/j.jbusres.2023.113764

Hart, O., & Grossman, S. J. (1980). Takeover bids, the free-rider problem, and the theory of the corporation. The Bell Journal of Economics, 11(1), 42. https://doi.org/10.2307/3003400

Hassan, S. and de Filippi, P. D. (2021). Decentralized autonomous organization. Internet Policy Review, 10(2). https://doi.org/10.14763/2021.2.1556

Helms, M. M. and Nixon, J. (2010). Exploring swot analysis – where are we now?. Journal of Strategy and Management, 3(3), 215-251. https://doi.org/10.1108/17554251011064837

Hill, C. W. L., & Jones, T. M. (1992). Stakeholder-agency theory. Journal of Management Studies, 29(2), 131-154. https://doi.org/10.1111/j.1467-6486.1992.tb00657.x

Hong, Y., & Apostolakis, G. (1993). Conditional influence diagrams in risk management. Risk Analysis, 13(6), 625-636. https://doi.org/10.1111/j.1539-6924.1993.tb01324.x

Jensen, M. C. and Meckling, W. H. (1976). Theory of the Firm: Managerial Behavior, Agency Costs and Ownership Structure. Journal of Financial Economics, 3(4), 305-360. https://doi.org/10.1016/0304-405x(76)90026-x

King, J. L. (1983). Centralized versus Decentralized Computing: Organizational Considerations and Management Options. ACM Computing Surveys, 15(4), 319-349. https://doi.org/10.1145/289.290

Kjäer, M., Angelo, M. d., & Salzer, G. (2021). Empirical evaluation of makerdao's resilience. 2021 3rd Conference on Blockchain Research &Amp; Applications for Innovative Networks and Services (BRAINS). https://doi.org/10.1109/brains52497.2021.9569811

Kumar, K. R. & Dissel, H. G. v. (1996). Sustainable collaboration: managing conflict and cooperation in interorganizational systems. MIS Quarterly, 20(3), 279. https://doi.org/10.2307/249657

Kouvelis, P. and Lariviere, M. A. (2000). Decentralizing Cross-Functional Decisions: Coordination Through Internal Markets. Management Science, 46(8), 1049-1058. https://doi.org/10.1287/mnsc.46.8.1049.12022

Laatikainen, G., Li, M., & Abrahamsson, P. (2023). A system-based view of blockchain governance. Information and Software Technology, 157, 107149. https://doi.org/10.1016/j.infsof.2023.107149

Li, J., Qin, R., & Wang, F. (2023). The future of management: dao to smart organizations and intelligent operations. IEEE Transactions on Systems, Man, and Cybernetics: Systems, 53(6), 3389-3399. https://doi.org/10.1109/tsmc.2022.3226748

Manfredo, M. R., & Richards, T. J. (2003). Cooperative Risk Management: Rationale and Effectiveness. https://doi.org/10.22004/ag.econ.28540

McShane, M. K. (2018). Enterprise risk management: history and a design science proposal. The Journal of Risk Finance, 19(2), 137-153. https://doi.org/10.1108/jrf-03-2017-0048

Mishra, D. P., Heide, J. B., & Cort, S. G. (1998). Information Asymmetry and Levels of Agency Relationships. Journal of Marketing Research, 35(3), 277-295. https://doi.org/10.1177/002224379803500301

Nadler, D. A. & Tushman, M. L. (1980). A model for diagnosing organizational behavior. Organizational Dynamics, 9(2), 35-51. https://doi.org/10.1016/0090-2616(80)90039-x

Nilakant, V., & Rao, H. R. (1994). Agency theory and uncertainty in organizations: an evaluation. Organization Studies, 15(5), 649-672. https://doi.org/10.1177/017084069401500501

Oliver, J. J. and Parrett, E. (2017). Managing uncertainty: harnessing the power of scenario planning. Strategic Direction, 33(1), 5-6. https://doi.org/10.1108/sd-09-2016-0131

Onjewu, A. E., Walton, N., & Koliousis, I. (2023). Blockchain agency theory. Technological Forecasting and Social Change, 191, 122482. https://doi.org/10.1016/j.techfore.2023.122482

Ouchi, W. G. (1979). A Conceptual Framework for the Design of Organizational Control Mechanisms. Management Science, 25(9), 833-848. https://doi.org/10.1287/mnsc.25.9.833

Pilling, B. K., & Zhang, L. (1992). Cooperative exchange: rewards and risks. International Journal of Purchasing and Materials Management, 28(2), 2-9. https://doi.org/10.1111/j.1745-493x.1992.tb00558.x

Qin, R., Ding, W., Li, J., Guan, S., Wang, G., Ren, Y., … & Qu, Z. (2023). Web3-based decentralized autonomous organizations and operations: architectures, models, and mechanisms. IEEE Transactions on Systems, Man, and Cybernetics: Systems, 53(4), 2073-2082. https://doi.org/10.1109/tsmc.2022.3228530

Sammut‐Bonnici, T. and Galea, D. (2015). pest analysis. Wiley Encyclopedia of Management, 1-1. https://doi.org/10.1002/9781118785317.weom120113

Sims, A. (2019). Blockchain and Decentralised Autonomous Organisations (DAOs): The Evolution of Companies? SSRN Electronic Journal. https://doi.org/10.2139/ssrn.3524674

Shleifer, A., & Vishny, R. W. (1986). Large shareholders and corporate control. Journal of Political Economy, 94(3, Part 1), 461-488. https://doi.org/10.1086/261385

Shubik, M. (1962). Incentives, decentralized control, the assignment of joint costs and internal pricing. Management Science, 8(3), 325-343. https://doi.org/10.1287/mnsc.8.3.325

Schwerin, S. (2018). Blockchain and Privacy Protection in Case of The European General Data Protection Regulation (GDPR): A Delphi Study. The Journal of The British Blockchain Association 1 (1). https://doi.org/10.31585/jbba-1-1-(4)2018

Sutton, S. G. (2006). Extended‐enterprise systems' impact on enterprise risk management. Journal of Enterprise Information Management, 19(1), 97-114. https://doi.org/10.1108/17410390610636904

Thiel, A. (2023), 'Polycentric Governing and Polycentric Governance', in Polycentrism: How Governing Works Today (Oxford Academic), https://doi.org/10.1093/oso/9780192866837.003.0005

Wright, A. (2021). The Rise of Decentralized Autonomous Organizations: Opportunities and Challenges. Stanford Journal of Blockchain Law & Policy. https://stanfordjblp.pubpub.org/pub/rise-of-daos/release/1

Ziegler, C. and Zehra, S. R. (2023). Decoding decentralized autonomous organizations: a content analysis approach to understanding scoring platforms. Journal of Risk and Financial Management, 16(7), 330. https://doi.org/10.3390/jrfm16070330

7.11. A Decentralized Mechanism for Know-Your-Transaction Compliance

AUTHOR:

Thomas Locher

DFINITY

A Decentralized Mechanism for Know-Your-Transaction Compliance

Thomas Locher, DFINITY Foundation
thomas.locher@dfinity.org

Extended Abstract

Know-your-transaction (KYT) compliance mandates the use of control mechanisms that identify suspicious customer actions in an effort to combat and prevent financial crimes such as money laundering. This type of regulation also affects cryptocurrency exchanges, which, in addition to know-your-customer (KYC) verification, also utilize services to perform KYT checks. Since Bitcoin is by far the largest cryptocurrency with respect to market capitalization, it is the focal point of KYT, and multiple companies such as Chainalysis, Elliptic, and CipherTrace provide services to classify bitcoins based on their transaction history. Concretely, these KYT service providers offer subscription-based APIs that, given a Bitcoin address or a specific transaction output, return their classification measuring the "exposure" to fraudulent activity. If there is any exposure, the Bitcoin address or transaction output is considered "tainted". If a reputable exchange and financial institution receives tainted bitcoins through a customer transfer, the incident is reported and the bitcoins in question are likely to be confiscated. While the crypto community may see Bitcoin as a fully fungible token, this is not the case in practice.

Bitcoin users who trade exclusively on centralized exchanges are typically oblivious to KYT checks running in the background, and they are unlikely to ever receive tainted bitcoins because the exchanges monitor their funds vigilantly. However, decentralized marketplaces and other decentralized finance (DeFi) products bring about new risks for users. DeFi applications usually do not perform any kind of KYT checks for multiple reasons.

First of all, decentralized applications (dapps) are normally not classified as virtual asset service providers and therefore not obliged to adhere to regulatory requirements. Moreover, dapps executed on self-contained blockchain platforms simply lack the capability to perform KYT checks. The risk for a user is that bitcoins obtained from such dapps may be considered tainted by exchanges, causing trouble for the user after transferring the tainted funds to an exchange.

This article presents the first decentralized dapp that is KYT-compliant, significantly reducing the aforementioned risk for all users. The dapp is the so-called chain-key Bitcoin (ckBTC) minter, a smart contract that handles the conversion between bitcoins and ckBTC, a token on the Internet Computer that is backed 1:1 by bitcoins such that 1 ckBTC can always be redeemed for 1 bitcoin and vice versa. Since ckBTC tokens can be transferred within 1-3 seconds and each transfer merely costs the equivalent of 10 satoshi, ckBTC provides a fast, inexpensive, and decentralized way to trade bitcoins, and is therefore appealing to frequent traders.

The Internet Computer has a unique feature in the crypto space that makes KYT checks possible for dapps: Smart contracts can issue HTTPS calls to regular web servers and process the responses. This feature is used in a specific smart contract that interacts with a KYT service provider to classify Bitcoin addresses and transaction outputs. The ckBTC minter calls this smart contract to perform KYT checks for both deposits and withdrawals. More precisely, it requests a KYT check for the corresponding unspent transaction output from the KYT smart contract before accepting a deposit, and asks the KYT smart contract to verify that the Bitcoin address where funds are meant to be transferred is "clean" for withdrawals, ensuring that ingress and egress flows are protected.

In this article, we describe this decentralized KYT mechanism in depth. We discuss advantages of this approach as well as challenges that open up interesting avenues for future work.

1 Web3 Services & KYT Compliance

Web3 is often touted as the "next generation" of the World Wide Web, augmenting the current Web2 with concepts such as decentralization and token-based economics ("tokenomics") that enable creators to retain ownership and control over their content, thereby reducing the power of centralized tech companies. Due to Web3's potential to democratize the digital space, interest in Web3 services has been on the rise for several years. In fact, Web3 equivalents for a plethora of Web2 platforms have emerged in numerous areas including gaming, social media, and, most prominently, financial services. Tokenomics play a pivotal role in Web3 as many services manage or interact with virtual assets, typically in the form of tokens. Classic examples are decentralized exchanges (DEXs), rivaling their centralized counterparts and attracting users with low fees, and decentralized market places for digital goods. DEXs started out as simple automated market makers, using liquidity pools of crypto tokens for trading, but full order-book DEXs are emerging on the market, nearing feature parity with CEXs.

Apart from the lack of centralized control (and possibly lower fees), a crucial difference between CEXs and DEXs is that DEXs generally lack regulatory oversight, which entails a substantially higher risk of financial crimes including money laundering. In the Web2 world, companies such as Chainalysis [1], Elliptic [2], and CipherTrace [3] that track cryptocurrency flows and link them to criminal activities have established themselves as business partners of CEXs and financial institutions in general. These companies provide APIs to their (paying) customers to check if any source or destination address has had direct or indirect exposure to any recorded illicit activity, enabling the customers to accept funds or approve outflows in accordance with legal standards and regulations. While presumably all major CEXs implement a KYT strategy, the opposite is true for DEXs and other services in the Web3 space.

The Financial Action Task Force (FATF) defines a virtual asset service provider (VASP) as a business that engages in the management, safekeeping, exchange, and transfer of virtual assets [4]. This definition includes cryptocurrency services such as exchanges, wallet custodians, and many others. It is important to note that, if there is a transfer of value, even a decentralized application (dapp)

and/or its owner/operator(s) may be considered VASPs with obligations to carry out KYC and KYT checks. However, if a dapp does not have an operator, it is unclear what party should be considered the corresponding VASP, if any. What is more, most blockchains are self-contained systems that cannot initiate any interaction with external entities. Consequently, it is usually infeasible or undesirable for a dapp to perform such checks. A cumbersome approach would be to keep all transactions pending until they are fetched by an external oracle service that passes them on to a KYT service provider for verification before returning the verification results to the dapp. In this approach, the dapp becomes entirely dependent not only on the KYT service provider but also on the oracle service, increasing the complexity and costs of the dapp while severely hampering both performance and decentralization. On the other hand, the absence of KYT checks puts the owners or operators of the dapp in a legal gray zone—and the users may not be fully aware of the risk that they are exposed to when interacting with the dapp.

2 The Internet Computer & HTTPS Outcalls

As mentioned in the previous section, a crucial shortcoming of most blockchain platforms is the lack of any means to access information external to the blockchain. This shortcoming is due to the fact that blockchains are deterministic replicated state machines, where the same changes must be applied in the same order to ensure that any state transition leads to the same new state. If the machines running the blockchain obtained different results when querying the same external data source, consensus would have to be reached first as to which result to use for the state update.

The only blockchain platform that offers such a feature is the Internet Computer [5], a general-purpose blockchain-based platform that has several unique capabilities [6]. The main feature of interest for this article is the capability to make HTTPS outcalls [7] from inside smart contracts. The function `http_request` that any smart contract can call to access data from the web is defined as follows:

```
type http_response = record {
  status: nat;
  headers: vec http_header;
  body: blob;
};

http_request : (record {
    url : text;
    max_response_bytes: opt nat64;
    method : variant { get; head; post };
    headers: opt http_header;
    body : opt blob;
    transform : opt record {
      function : func (record {
        response : http_response; context : blob})
        -> (http_response) query;
      context : blob
    };
  }) -> (http_response);
```

The request must contain the targeted URL in the `url` field. Additionally, the access method must be specified, which is either, `get`, `head`, or `post`. In addition to the status, the response contains the result in the `body` field in the form of a byte array (`blob`). As the definition shows, there are more fields in the request and response. Since this is not the core topic of this article, we dispense with a more detailed description and refer the interested reader to online documentation [8]. It is worth noting, however, how the Internet Computer ensures deterministic state transitions given that the machines may receive different responses. In short, the protocol simply verifies that at least two thirds of all responses are identical. If this is the case, the response is accepted and returned to the calling smart contract. Otherwise, an error is returned. Since responses from web servers can contain various metadata such as unique request identifiers, timestamps, and other data that is likely to change with every request, a transform

function can be specified that extracts the relevant piece of information from the response before comparing for equality, thereby greatly increasing the chances of getting an agreed-upon response.

Obviously, HTTPS outcalls cannot be used to access rapidly changing data because the machines would rarely be able to reach consensus. Fortunately, KYT data does not change quickly, which makes it possible to utilize this feature to implement a decentralized KYT mechanism.

3 Chain-key Bitcoin & KYT Verification

Bitcoin is still the commanding force in the cryptocurrency space, yet it is seldom used for decentralized finance (DeFi) applications due to its lack of programmability, high transaction fees, and low transaction speed. While the Lightning network [9] is intended to reduce fees and improve transaction throughput, several projects such as Stacks [10], Rootstock [11], and chain-key Bitcoin (ckBTC) [12] that enable more general-purpose smart contracts to be built on Bitcoin have recently grown in popularity.

In this article, we focus on ckBTC, a token on the Internet Computer that is backed 1:1 by bitcoins (BTC) and that addresses the aforementioned drawbacks: ckBTC can be used inside smart contracts implementing arbitrary business logic, every transaction costs the equivalent of 10 satoshi, i.e., 0.0000001 BTC, and transactions settle with finality typically after 1-3 seconds.

Naturally, a 1:1 peg can only be maintained by guaranteeing that 1 ckBTC can always be redeemed for 1 BTC and vice versa (minus fees). To this end, the ckBTC functionality is split into two main smart contracts:

1. The *ckBTC minter* is responsible to mint ckBTC when a user deposits BTC and burn ckBTC when a user retrieves BTC.

2. The *ckBTC ledger* executes all ckBTC transactions. Moreover, it mints and burns ckBTC as instructed by the ckBTC minter.

The ckBTC minter makes use of another unique capability of the Internet Computer, its bridgeless integration with the Bitcoin network [13] that enables a

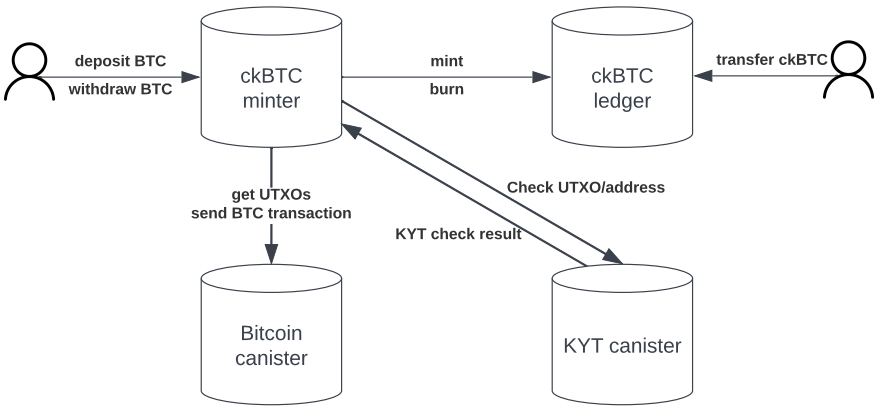


Figure 1: An overview of the interactions between users and the smart contracts that together provide the ckBTC functionality.

smart contract to hold, receive, and send real bitcoin. Since no bridge is required to connect the two networks, it is a more secure alternative to using wrapped tokens such as WBTC on Ethereum [14]. The ckBTC minter effectively takes all received bitcoins under custody and instructs the ckBTC ledger to mint and burn ckBTC tokens whenever bitcoins have been deposited and retrieved, respectively. A high-level overview of the architecture is shown in Figure 1.

In the lower left corner, the *Bitcoin canister* is the system-level functionality that provides read and write access to the Bitcoin blockchain through endpoints that return the unspent transaction outputs (UTXOs) and balances of Bitcoin addresses (read access) and accept Bitcoin transactions from smart contracts, which are then advertised in the Bitcoin network for inclusion in a block (write access). Note that a smart contract executed on the Internet Computer is referred to as a *canister*, which is a bundle of the smart contract logic and the data that holds the smart contract's state.

It is worth noting that another technical feature is required: A smart contract must be able to have at least one Bitcoin address and it must be able to securely sign transactions to spend funds associated with its addresses. This functionality is enabled through threshold ECDSA [15], another feature available on the Inter-

net Computer: Smart contracts can obtain one or more ECDSA public keys and request signatures for a given piece of data and one of these keys. Since several types of Bitcoin addresses simply encode an ECDSA public key and spending bitcoins requires signatures for the encoded public keys, threshold ECDSA indeed provides the required functionality.

We are now in the position to return to the main topic of KYT compliance. This part is covered by the *KYT canister* shown in the lower right corner, a smart contract used by the ckBTC minter as follows. When the ckBTC minter receives a new UTXO, it sends a request to the KYT canister to perform a KYT check on the UTXO. Similarly, when there is a BTC retrieval request to a certain destination address, the ckBTC minter asks the KYT canister for a KYT check on the Bitcoin address. Since KYT checks are performed when bitcoins are received and transferred out, both ingress and egress flows are protected.

The KYT canister cannot answer the requests itself. Instead, it uses the HTTPS outcalls feature to make requests for KYT checks to a KYT service provider. The response of the KYT service provider is then simply returned to the ckBTC minter. The response may contain a list of alerts associated with the given UTXO or address with each alert having a certain severity level. The ckBTC minter treats alerts conservatively in that it marks UTXOs and addresses as tainted if there is any alert, regardless of severity. If a UTXO is tainted, it is quarantined and no ckBTC are minted. This UTXO is then "stuck" in the ckBTC minter since there are currently no clear guidelines as to how tainted bitcoins are to be treated. If a Bitcoin address is tainted, on the other hand, the request to send bitcoins to this address is simply declined and the user who made the request retains his or her funds in ckBTC.

An important technicality that must be considered is the fact that KYT providers offer paid subscription services. Since smart contracts cannot purchase subscriptions using fiat currencies, there is a need to introduce the role of a *maintainer*, which is an entity that has acquired a subscription and registered the corresponding API key (required to gain access to the KYT service) with the KYT canister. When registering an API key, the KYT canister uses the API key to make a KYT request against the KYT provider to verify that the key is valid before accepting the maintainer. For each request, the KYT canister picks a reg-

istered maintainer and uses the maintainer's API key to make the request to the KYT provider. For each successful request—irrespective of the outcome of the request—, the maintainer gets awarded a KYT fee of 0.00002 ckBTC. The ckBTC minter remunerates the maintainers with a daily lump-sum payment into their accounts on the ckBTC ledger. These payments are meant to offset the cost of purchasing the subscription. The user depositing or withdrawing bitcoins must pay the KYT fee, in addition to the Bitcoin network fee and a small fee that goes to the ckBTC minter as compensation for the cost incurred to send the Bitcoin transaction.

When looking at the figure, the KYT mechanism appears deceptively simple but multiple complex features need to interact seamlessly and several technical details need to be considered to make the whole process work.

4 Open Challenges

Overall, the mechanism described in the preceding section makes it possible to use ckBTC as a fast and cost effective "twin" of Bitcoin with confidence that every ckBTC token is worth one bitcoin because a) the underlying asset is held by the ckBTC minter itself and b) every accepted UTXO underwent a KYC check. It is therefore improbable that a user would ever run into issues when sending retrieved bitcoins to a centralized exchange or a financial institution.

However, there are some open challenges. First of all, only one KYT provider is used currently. The damage this KYT provider could cause is limited in that it does not have control over any funds. In the worst case, the KYT provider would return erroneous information, causing the ckBTC minter to accept tainted UTXOs or send bitcoins to tainted addresses, or reject UTXOs and addresses even though the UTXOs and addresses are clean. In the latter case, the KYT provider would disrupt the minting and burning process but regular ckBTC transfers would not be affected. The KYT provider constitutes a single point of failure in an otherwise decentralized architecture. Fortunately, the risk of this scenario is low because a reputable KYT provider can be expected to reliably provide correct data. More importantly, in the unlikely event that the KYT provider ceases to provide its

service, the decentralized governance system of the Internet Computer can be used to upgrade the KYT canister in order to switch to another KYT provider, i.e., this dependency cannot make the ckBTC minter inoperable. Clearly, the KYT process can be decentralized in the future by having the KYT canister interact with various KYT providers, at the expense of (linearly) increased fees.

Another challenge pertains to maintainers: The process of registering maintainers and API keys is already fully decentralized. The challenge is to find maintainers willing to make the initial investment in fiat currency to get a subscription and to get reimbursed through daily ckBTC payments. Since the KYT fee is a fixed ckBTC amount, a maintainer can only turn the investment to profit if there is a substantial number of deposits and withdrawals coupled with a sufficiently high Bitcoin price. Therefore, it is expected that entities building their businesses around ckBTC are primarily interested in becoming maintainers. As there is no centralization concern if there is merely a single maintainer, it is therefore only required for the community to ensure that such a maintainer is always available.

Lastly, the management of API keys is another challenge because the machines running the KYT minter store the API keys. In theory, that puts the operators into a similar position as the KYT providers in that they could attempt to read out the API keys and try to deplete their quotas, which would make the mint and burn operations fail. Again, the risk of such an attack is deemed low because it is quite an effort to read out this information for little gain as the maintainers can use a single function call to replace their API keys. Furthermore, due to the scalable nature of the Internet Computer, only a small set of machines scattered around the world host the KYT canister. Consequently, it is not as easy to get access to such internal state information as it would be on other blockchain platforms. Nevertheless, even if the risk is low, it would be beneficial to have better protection of API keys in place. Since the API keys are used as part of the URL in HTTPS outcalls, it appears to be infeasible to hide the keys from the smart contract itself. Currently, the best available solution is to protect the entire smart contract by running it in an encrypted virtual machine. Since more and more machines are equipped with support for AMD's secure encrypted virtualization-secure nested paging (SEV-SNP) technology [16], it will be possible to add this layer of security in the near future.

5 Conclusion

To the best of our knowledge, the presented decentralized mechanism for KYT compliance is the first of its kind. As more and more funds are transferred in and out of dapps, it will become increasingly important to provide the means to protect users from financial crimes and having KYT checks baked into smart contrast is a step in that direction. As pointed out in this article, there are still challenges to overcome but we believe that we have only scratched the surface of what is possible. It is not unthinkable that full KYT services will eventually run on-chain, competing for users and providing KYT data to smart contracts directly in a more affordable, direct way without any sacrifices in terms of security or decentralization. Naturally, services for other types of compliance checks can emerge as well, making it possible for smart contracts to choose which checks are necessary for their use cases. Due to ckBTC and its KYT mechanism, decentralized compliance verification has just entered its infancy.

References

[1] Chainalysis. `https://www.chainalysis.com`.

[2] Elliptic. `https://www.elliptic.co`.

[3] CipherTrace. `https://ciphertrace.com`.

[4] Updated Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers. `https://www.fatf-gafi.org/en/publications/Fatfrecommendations/Guidance-rba-virtual-assets-2021.html`.

[5] Internet Computer. `https://internetcomputer.org`.

[6] Internet Computer capabilities. `https://internetcomputer.org/capabilities`.

[7] Internet Computer HTTPS Outcalls. `https://internetcomputer.org/https-outcalls`.

[8] HTTPS Outcalls: Technical Wiki Page. https://wiki.internetcomputer.org/wiki/HTTPS_outcalls.

[9] Lightning. https://lightning.network.

[10] Stacks. https://www.stacks.co.

[11] Rootstock. https://rootstock.io.

[12] Chain-key Bitcoin. https://internetcomputer.org/ckbtc.

[13] Internet Computer Bitcoin Integration. https://internetcomputer.org/bitcoin-integration.

[14] Wrapped Bitcoin. https://wbtc.network.

[15] Threshold ECDSA: Chain-key Signatures. https://internetcomputer.org/docs/current/developer-docs/integrations/t-ecdsa.

[16] AMD SEV-SNP. https://www.amd.com/en/processors/amd-secure-encrypted-virtualization.

7.12. Blockchain in China: A Shift from Disruption to Integration

AUTHOR:

Lei Hao

University of Nottingham
UK | CHINA | MALAYSIA

Blockchain in China: A Shift from Disruption to Integration

Lei Hao
Lei.hao@nottingham.edu.cn

Abstract

In China, blockchain's evolution presents a narrative aligned with state initiatives, diverging sharply from its disruptive and decentralizing roots in Western societies. Within China's governance framework, blockchain becomes an integral part of regulatory and socio-economic policy, notably in areas of identity verification and data protection. Through the application of Actor-Network Theory, this study dissects how the Chinese government's stringent regulations, alongside incentives for innovation and the market's demand, coalesce to inform and direct the progression of blockchain technology.The research uncovers a distinctive model of power dynamics in China's blockchain implementation, where the state not only guides its development but also fosters an environment conducive to innovation. This approach aligns with commercial interests, particularly in sectors prioritizing data security and identity management. Such a model illustrates a unique amalgamation of centralized governance with blockchain's decentralized ethos, providing a contrast to the Western model of blockchain adoption. By exploring this unique trajectory, the study sheds light on the intricate role blockchain plays in societal and cultural shifts within China, offering insights into the broader implications of technology's assimilation into different governance structures worldwide. This contributes to a deeper global discourse on how political context shapes the adoption and impact of transformative technologies like blockchain.

Keywords: Blockchain, China, Actor-Network Theory, Governance, Innovation

Introduction

Blockchain technology, originally emerging as a disruptive symbol within the Western world, promised to revolutionize financial systems through decentralization. It was conceived as a tool to undermine traditional financial structures, offering an alternative asset class that was beyond the influence of centralized state control. Yet, in the variegated landscape of global technology adoption, the trajectory of blockchain has diverged significantly, particularly in China.

In China, the technology has been co-opted into a state-driven framework, serving to enhance state governance through improved identity verification and robust data security practices—key components of China's regulatory and socio-economic

objectives. Rather than disrupting, blockchain in China is a model of technological integration, meticulously aligning with the nation's established systems (Xi, 2019).

This paper conducts a comprehensive analysis of the nuanced adaptation of blockchain within China, juxtaposing it against its initial Western conception as a harbinger of financial autonomy. Here, blockchain's promise of decentralization and its countercultural roots are contrasted with its strategic alignment within China's centralized framework. This divergence is not merely a tale of two paths but a narrative rich in convergence, where China's rigorous regulatory structures, fervent drive for innovation, and the dynamism of the market coalesce.

Through the analytical lens of Actor-Network Theory, (Latour, 2005). this exploration delves into the shifts in structural agency and power relations engendered by blockchain in China. The theory elucidates how state-centric oversight has been able to sculpt blockchain's development without curtailing the innovative dynamism that the technology naturally brings. A qualitative approach on the implementation of blockchain in China reveals a development paradigm where state control is integral to blockchain's design, yet innovation thrives (Zheng et al., 2018).

The study's findings highlight a dual role for blockchain in China—as a tool for governance and as a beacon for innovation. This dual role illustrates the complex nature of technology as it interacts with and shapes socio-political landscapes, contributing to a global understanding of how technological advancements are integrated within different governance models.

The Genesis of Blockchain as a Disruptive Force

Blockchain technology's roots can be traced back to the early 1990s with the work of Stuart Haber and W. Scott Stornetta, who first proposed a cryptographically secure chain of blocks to secure digital documents from tampering (Haber & Stornetta, 1991). However, it was not until 2008 that the concept of blockchain as it is known today was popularized by an individual (or group) under the pseudonym Satoshi Nakamoto. Nakamoto (2008) introduced Bitcoin as "a new electronic cash system that's fully peer-to-peer, with no trusted third party," which leveraged blockchain to facilitate and record transactions in a decentralized manner.

The decentralizing potential of blockchain comes from its inherent design as a distributed ledger technology (DLT) that allows data to be stored across a network of computers. This ensures that no single entity has control over the entire dataset, and all participants in the network have access to a shared version of the truth (Nakamoto, 2008). The cryptographic principles underlying blockchain, such as hash functions and digital signatures, provide security and trust without the need for

centralized authority, fundamentally challenging the traditional financial systems which are reliant on trust in central institutions (Antonopoulos, 2014).

In the Western financial landscape, blockchain technology was quickly identified as a tool that could disrupt the status quo. The global financial crisis of 2007–2008 had eroded public trust in banks and financial institutions, setting the stage for an alternative financial system that blockchain promised to provide. Tapscott and Tapscott (2016) argued that blockchain technology presented an opportunity to overhaul existing financial systems, which are often seen as opaque, inefficient, and exclusionary.

As blockchain technology evolved, it enabled the creation of various cryptocurrencies, smart contracts, and decentralized applications (dApps), extending its disruptive potential beyond mere currency to a wide array of financial services (Buterin, 2014). The emergence of initial coin offerings (ICOs) as a means of crowdfunding further exemplified the technology's ability to democratize access to capital (Adhami, Giudici, & Martinazzi, 2018).

The adoption of blockchain in Western societies has been a mix of grassroots movements and institutional interests. While cryptocurrencies like Bitcoin became a symbol of anti-establishment sentiments, enterprises and governments also began to explore the technology's potential to streamline processes and reduce fraud (Mougayar, 2016). Financial institutions, once skeptical, started investing in blockchain research, recognizing the efficiency gains and cost reductions it could offer (Iansiti & Lakhani, 2017).

Blockchain's Realignment in the Chinese Context

China's strategic pivot towards blockchain technology is firmly embedded within its broader agenda for digital transformation, where blockchain is not only seen as a tool for technological innovation but also as an instrument for advancing economic reform and enhancing governance. Recognizing the potential of blockchain, the Chinese government has specifically identified it within the 13th Five-Year Plan (2016-2020) as a key area of development, which has subsequently received significant state investment and robust policy support (Xia, Gao, & Zhang, 2023). President Xi Jinping's explicit endorsement of blockchain development has underscored the nation's commitment to harnessing the technology for industrial transformation and bolstering China's standing in the global economic arena (Xi, 2019).

The integration of blockchain into China's regulatory fabric is exemplified by the deployment of the technology in the identity verification sector. The Blockchain-based Service Network (BSN), spearheaded by the State Information

Center of China, is a testament to the strategic integration of blockchain into the fabric of state operations, using it to reinforce the digital identity ecosystem for both citizens and businesses (Zheng et al., 2018). This initiative reflects a deliberate move to enhance the security and efficiency of identity management systems, which are foundational for a broad spectrum of services, from financial dealings to access to public services (Huang et al., 2022).

In parallel, the concern for data security in an increasingly digitalized economy has led to the Cyberspace Administration of China's (CAC) adoption of blockchain standards to bolster data integrity and traceability. Such measures are designed to mitigate risks associated with data tampering and unauthorized access, establishing a more resilient digital infrastructure (Wang et al., 2019). Alibaba's use of blockchain for logistics and supply chain integrity is indicative of the broader industry trend to utilize blockchain for ensuring the authenticity and permanence of transaction records (Kang et al., 2019)

Moreover, the regulatory environment in China has also shaped blockchain's role in intellectual property (IP) protection. The China National Intellectual Property Administration (CNIPA) is proactively looking into blockchain-driven solutions to create a more transparent and immutable system for IP rights management, reflecting a strategic alignment with China's rapid innovation growth and the need to protect the fruits of this growth (Zhang, Zhong, Wang, Chao, & Wang, 2020)

China's unique approach to blockchain regulation and integration demonstrates a nuanced understanding of the technology's potential. The multifaceted strategy employs rigorous regulatory mechanisms, a proactive stance on technological innovation, and a responsive market landscape, all of which synergize to repurpose blockchain technology from its original disruptive intent to a tool of state-led integration, thus supporting national development strategies and leveraging it for government and commercial benefit.

Actor-Network Theory and Blockchain in China

Actor-Network Theory (ANT), initially developed by scholars such as Bruno Latour, Michel Callon, and John Law during the mid-1980s, offers a novel and robust lens for examining the interplay of technology and society (Latour, 1987; Callon, 1984; Law, 1992). ANT posits that society is composed of networks of both human and non-human 'actors' or 'actants.' These actants interact within a network, influencing each other and shaping developments in a non-hierarchical manner (Latour, 2005).

The relevance of ANT to the study of technology arises from its foundational argument that technological artifacts must not be seen in isolation but as part of a

wider network of relations that give them meaning and potency (Law, 1992). In the context of blockchain technology, ANT provides a framework to understand how various stakeholders - including policymakers, developers, commercial entities, and the technology itself - co-construct the technology's role within the Chinese socio-economic ecosystem.

ANT's analytical utility in assessing blockchain's integration in China comes from its agnosticism to the classification of actors. It allows equal importance to both human actors, such as government officials or developers, and non-human actors, such as the blockchain protocols and algorithms (Latour, 2005). This approach is particularly useful in discerning how blockchain, as a non-human actor, participates in networks that include state regulation, market dynamics, and social practices.

In applying ANT to the study of blockchain in China, it becomes possible to map out the intricate relationships that contribute to the technology's evolving identity. ANT allows for a detailed examination of the processes through which blockchain becomes an integrated component of governance and commerce. This encompasses tracing the translations that occur as blockchain moves from a concept on the periphery to a central technology within China's digital landscape (Latour, 1987).

Case Studies and Applications

In China, blockchain technology's applications span across diverse sectors, providing a rich tapestry of case studies that illustrate the delicate balance between state oversight and the fostering of innovation.

Finance Sector: Digital Currency Electronic Payment (DCEP)

One of the most significant applications of blockchain in China is the development of the Digital Currency Electronic Payment (DCEP) system by the People's Bank of China (PBoC). This system represents the first state-backed digital currency initiative, designed to streamline the monetary system while providing the state with new mechanisms for monitoring the financial system and managing economic policies(Goodell & Nakib, 2021; Wu & Chen, 2021). The DCEP leverages blockchain's distributed ledger technology to ensure transaction security and counteract fraud, illustrating the state's role in directing blockchain's application towards large-scale financial infrastructure.

Media Sector: Content Authentication

In China, the conversation around enhancing media content management is gaining momentum with the proposed integration of ChinaDRM and blockchain technology.

iQIYI, a prominent Chinese online content platform, is advancing this dialogue by not only contemplating the use of blockchain for a robust intellectual property rights management system but has also taken concrete steps by launching a blockchain-based copyright certification function. (Jiang, Sui, Lin, & Han, 2020) This function harnesses both blockchain and AI technology, representing a stride towards transparent and secure content management. It is designed to grant content creators increased autonomy and fair compensation, thus driving the industry towards a more innovative and equitable future. (Jiang, Sui, Lin, & Han, 2020)

ChinaDRM, China's digital rights management solution, is poised to play a key role in this transformation. It already provides robust protection for various digital content formats, and its potential integration with blockchain promises to enhance its encryption, authorization, and access control capabilities. (Shang & Yu, 2023)

The proposed architecture would combine consortium and public blockchains to establish a trustworthy environment for distributing audio-visual content. Through this architecture, media content providers and regulatory bodies could reach consensus via the consortium blockchain, while the public blockchain would handle transparent interactions between users and content providers. This forward-thinking approach to merging ChinaDRM and blockchain indicates a strategic move towards strengthening copyright protection and content security, and if implemented, could significantly advance digital rights management and content distribution in China.

Dual Function of State Oversight and Innovation

Each of these cases reflects the dual function of state oversight and innovation promotion. The DCEP initiative is closely monitored and regulated by the PBoC, ensuring alignment with national monetary policies while pioneering the use of blockchain in central banking. The media sector's use of blockchain for content authentication aligns with state efforts to protect intellectual property rights and promote a healthy digital content industry.

Comparative Analysis

A comparative analysis between the role of blockchain in China and the West reveals divergent trajectories based on differing socio-political motivations and economic structures.

Blockchain in the West: The Disruptive Paradigm

In the West, blockchain's emergence was intertwined with the ethos of decentralization, challenging traditional power structures, particularly within the

financial sector. The foundational philosophy was to create a system that operates outside of and resists the control of central authorities, exemplified by cryptocurrencies like Bitcoin (Nakamoto, 2008). This was seen as a democratizing force, offering financial inclusion and empowering individuals by removing intermediaries and reducing transaction costs (Tapscott & Tapscott, 2016).

Blockchain in China: The Integrative Approach

Contrastingly, in China, blockchain technology is being integrated into state operations and aligned with existing socio-political frameworks. China's strategic approach does not view blockchain as a disruptor but as an enabler that can be harnessed to optimize governance, improve public services, and enhance data security (Xi, 2019). The technology is employed in ways that reinforce the role of central authorities and existing institutions, as seen with the DCEP. This reflects a nuanced understanding that technology can be a force for societal improvement when guided by and integrated within a structured regulatory environment (Zheng et al., 2018).

Technology's Societal Impacts

China's application of blockchain technology reveals a nuanced understanding of its societal impacts. By incorporating blockchain into state governance, China aims to leverage the technology's capabilities for societal benefit, such as enhancing the transparency and efficiency of public services, while also ensuring alignment with national regulatory and security concerns (Zheng et al., 2018).

For instance, China's development of the DCEP not only innovates in the realm of digital currencies but also serves as a tool for monetary policy and economic surveillance, showcasing the state's proactive role in shaping the societal impact of blockchain technology (Jin, 2023).

Comparative Analysis

The comparative analysis of blockchain's role in China versus the West thus highlights differing ideological underpinnings and societal objectives. While the West values blockchain for its ability to democratize and decentralize, China sees it as a means to centralize and strengthen state efficiency and oversight. This dichotomy underscores the flexibility of blockchain as a technology that can be molded to fit varying societal needs and governmental strategies.

Implications for Governance and Innovation

The interplay between governance and innovation within China's blockchain strategy encapsulates a critical balancing act. The Chinese government has positioned blockchain as a transformative technology under the aegis of state supervision, while simultaneously nurturing a burgeoning innovation ecosystem.

State Oversight and Blockchain Innovation

In China, the strategic balance between rigorous state control and the encouragement of innovation is evident in the blockchain domain. The government's assertive role in shaping blockchain's application is designed to enhance national governance. This intent is reflected in the regulatory principles outlined in the "China Financial Stability Report" by The People's Bank of China, which provides a comprehensive overview of the country's direction for financial technologies, including blockchain. (Yu, Gong, & Sampat, 2022)

China's regulatory approach to blockchain features a bifurcated system. It enforces strict prohibitions in certain areas of blockchain, such as peer-to-peer lending, initial coin offerings, and cryptocurrency. Concurrently, there is a flexible regulatory scheme for blockchain within FinTech enterprises, highlighted by innovative regulation pilots in select cities—akin to regulatory sandboxes—which operate under the guidance of the People's Bank of China's "FinTech Development Plan." (Yu, Gong, & Sampat, 2022) This regulatory framework underscores a comprehensive governance strategy, ensuring that blockchain's potential is harnessed effectively while maintaining financial stability and security within China's rapidly evolving digital economy.

Blockchain's Influence on Power Dynamics

Blockchain technology in China is not just a tool for economic advancement but also a means to reshape power dynamics. Through blockchain, the Chinese government is exploring new forms of regulatory control and citizen engagement. The technology's potential for traceability and transparency is leveraged to create new governance models, as seen in the pilot blockchain projects in local government administrations for public services (Zhang, Li, Li, et al., 2018).

In the private sector, blockchain is enabling new forms of structural agency. Companies are utilizing blockchain to create decentralized networks that are nevertheless capable of aligning with the state's regulatory expectations. This has implications for the power dynamics between the state, corporations, and consumers, as each actor negotiates their space within the blockchain-enabled digital landscape (Xu, Li, Zeng, Cao, & Jiang, 2022)

Conclusion

The paper has traversed the landscape of blockchain technology in China, highlighting the country's unique approach to adopting what was initially a disruptive technology in the West. Through detailed analysis, it becomes evident that China has recontextualized blockchain within its socio-political framework, leveraging it as a tool for state-led governance and innovation.

The key findings indicate that China's blockchain strategy is multifaceted, involving a nuanced interplay between regulatory oversight and fostering innovation. Unlike the Western model that champions decentralization and disruption, China's model focuses on integration and enhancement of existing systems. This approach is exemplified by the state-backed Digital Currency Electronic Payment (DCEP) system, and various initiatives across sectors such as media that bolster data security and intellectual property management.

The transformative potential of blockchain in China has significant implications within the global context. As China continues to expand its blockchain initiatives, it sets new standards for how technology can be integrated into different facets of society and governance. This has prompted international discourse on blockchain's capabilities and limitations, influencing global trends in technology adoption and regulation (Campbell-Verduyn, 2017).

For further research, there are several promising areas. One would be the longitudinal study of blockchain's economic and social impact, as the technology matures and becomes more deeply integrated into China's digital infrastructure. Another area would be comparative international studies on blockchain regulation, particularly examining how different regulatory approaches impact innovation and market dynamics.

References

Adhami, S., Giudici, G., & Martinazzi, S. (2018). Why do businesses go crypto? An empirical analysis of initial coin offerings. *Journal of Economics and Business, 100*, 64-75.

Antonopoulos, A. M. (2014). *Mastering Bitcoin: Unlocking Digital Cryptocurrencies*. O'Reilly Media.

Buterin, V. (2014). A next-generation smart contract and decentralized application platform. *White Paper*.

Callon, M. (1984). Some elements of a sociology of translation: Domestication of the scallops and the fishermen of St Brieuc Bay. *The Sociological Review, 32*(1_suppl), 196-233. https://doi.org/10.1111/j.1467-954X.1984.tb00113.x

Campbell-Verduyn, M. (2017). *Bitcoin and Beyond: Cryptocurrencies, Blockchains, and Global Governance*. RIPE Series in Global Political Economy. Routledge.

Chen, Y. (2018). Blockchain and financial market innovation. *Economic Modelling, 79*, 154-162.

Cyberspace Administration of China. (2019). Regulations on the Management of Blockchain Information Services. Retrieved from [official CAC website].

Haber, S., & Stornetta, W. S. (1991). How to time-stamp a digital document. *Journal of Cryptology, 3*(2), 99-111.

Goodell, G., & Nakib, H. D. A. (2021). The development of central bank digital currency in china: An analysis. *arXiv preprint arXiv:2108.05946*.

Huang, C., et al. (2022). Blockchain-Assisted Transparent Cross-Domain Authorization and Authentication for Smart City. *IEEE Internet of Things Journal, 9*(18), 17194–17209. https://doi.org/10.1109/JIOT.2022.3154632

Iansiti, M., & Lakhani, K. R. (2017). The truth about blockchain. *Harvard Business Review, 95*(1), 118-127.

Jin, Z. (2023). Digital RMB and its predecessor: A comparison with mobile payment platforms. *Frontiers in Business, Economics and Management, 7*(2), 155–158. https://doi.org/10.54097/fbem.v7i2.4885

Jiang, T., Sui, A., Lin, W., & Han, P. (2020). Research on the Application of Blockchain in Copyright Protection. *2020 International Conference on Culture-oriented Science & Technology (ICCST)*, 616-621. https://doi.org/10.1109/ICCST50977.2020.00127

Kang, J., et al. (2019). Blockchain for Secure and Efficient Data Sharing in Vehicular Edge Computing and Networks. *IEEE Internet of Things Journal, 6*(3), 4660–4670. https://doi.org/10.1109/JIOT.2018.2875542

Kostka, G. (2019). China's social credit systems and public opinion: Explaining high levels of approval. *New Media & Society, 21*(7), 1565-1593. https://doi.org/10.1177/146144481982640

Latour, B. (1987). *Science in action: How to follow scientists and engineers through society*. Harvard University Press.

Latour, B. (2005). *Reassembling the social: An introduction to actor-network-theory*. Oxford University Press.

Law, J. (1992). Notes on the theory of the actor-network: Ordering, strategy, and heterogeneity. *Systems Practice, 5*(4), 379-393.

Li, M. (2018). Made in China 2025: The making of a high-tech superpower and consequences for industrial countries. *Mercator Institute for China Studies Papers*, (8), 1-32.

Mougayar, W. (2016). *The Business Blockchain: Promise, Practice, and Application of the Next Internet Technology*. Wiley.

Nakamoto, S. (2008). Bitcoin: A peer-to-peer electronic cash system. Retrieved from https://bitcoin.org/bitcoin.pdf

National Development and Reform Commission (NDRC). (2020). Increase the intensity of digital economy policy innovation. Retrieved from https://www.ndrc.gov.cn/wsdwhfz/202205/t20220507_1324362.html

Shang, W., & Yu, Z. (2023). A new media content trusted dissemination architecture based on AV-blockchain and ChinaDRM. *Intelligent and Converged Networks, 4*(2), 142-157. https://doi.org/10.23919/ICN.2023.0015

State Council of the People's Republic of China. (2016). The 13th Five-year Plan for Economic and Social Development of the People's Republic of China (2016-2020). Retrieved from https://en.ndrc.gov.cn/policies/202105/P020210527785800103339.pdf

Tapscott, D., & Tapscott, A. (2016). *Blockchain Revolution: How the technology behind bitcoin is changing money, business, and the world*. Penguin.

Wang, H., Song, Y., & Hamilton, C. (2018). Blockchain-enabled EMR: Improving patient data sharing in China's hospitals. *Health Information Science and Systems, 6*(1), 12.

Wang, Y., Han, J. H., & Beynon-Davies, P. (2019). Understanding blockchain technology for future supply chains: a systematic literature review and research agenda. *Supply Chain Management: An International Journal, 24*(1), 62-84.

Wang, Q., Zhu, X., Ni, Y., Gu, L., & Zhu, H. (2020). Blockchain for the IoT and industrial IoT: A review. *Internet of Things, 10*, 100081. https://doi.org/10.1016/j.iot.2019.100081

Wu, T., & Chen, J. (2021). A study of the economic impact of central bank digital currency under global competition. *China Economic Journal, 14*(1), 78-101. https://doi.org/10.1080/17538963.2020.1870282

Xi, J. (2019). Xi stresses development, application of blockchain technology. *Xinhua Net*. Retrieved from http://www.xinhuanet.com/english/2019-10/25/c_138503254.htm

Xia, H., Gao, Y., & Zhang, J. Z. (2023). Understanding the adoption context of China's digital currency electronic payment. *Financial Innovation, 9*(1), Article 63. https://doi.org/10.1186/s40854-023-00467-5

Xu, Y., Li, X., Zeng, X., Cao, J., & Jiang, W. (2022). Application of blockchain technology in food safety control: Current trends and future prospects. *Critical Reviews in Food Science and Nutrition, 62*(10). https://doi.org/10.1080/10408398.2020.1858752

Yu, P., Gong, R., & Sampat, M. (2022). Blockchain Technology in China's Digital Economy: Balancing Regulation and Innovation. In P. M. Tehrani (Ed.), *Regulatory Aspects of Artificial Intelligence on Blockchain* (pp. 132-157). DOI: 10.4018/978-1-7998-7927-5

Zhang, J., Zhong, S., Wang, T., Chao, H.-C., & Wang, J. (2020). Blockchain-based systems and applications: A survey. *Journal of Internet Technology, 21*(1), 1–14.

Zhang, G., Li, T., Li, Y., et al. (2018). Blockchain-Based Data Sharing System for AI-Powered Network Operations. *Journal of Communications and Information Networks, 3*, 1–8. https://doi.org/10.1007/s41650-018-0024-3

Zheng, Z., Xie, S., Dai, H.-N., Chen, X., & Wang, H. (2018). Blockchain challenges and opportunities: A survey. *International Journal of Web and Grid Services, 14*(4), 352–375.

7.13. Fully on-chain DAOs on the Internet Computer

AUTHORS:

Björn Assmann

DFINITY

Lara Schmid

DFINITY

Fully on-chain DAOs on the Internet Computer

Björn Assmann* Lara Schmid†
DFINITY Foundation DFINITY Foundation

October 25, 2023

Abstract

Decentralized autonomous organizations, or DAOs, are governance systems implemented as smart contracts on blockchains, enabling decentralized communities to make verifiable decisions on a public ledger. Early blockchains, like Bitcoin, lack built-in governance systems that we now associate with DAOs. To upgrade the blockchain, all node operators jointly agree on doing so by individually upgrading their nodes. This requires a lot of costly off-chain coordination and does not benefit from the verifiability of on-chain activities. Newer platforms like Ethereum introduced smart contracts and enabled DAOs for various decision-making processes. Typically only a few of these decisions are executed automatically on-chain and the DAO must trust off-chain individuals to do so.

The Internet Computer blockchain (ICP) addresses these off-chain dependencies through its Network Nervous System (NNS), a fully on-chain DAO that governs the entire ICP. The NNS automates all system upgrades, including those of the protocol and the NNS DAO itself. Furthermore, DAOs on the ICP control whole decentralized applications—covering their stored data, assets, and frontends.

In this paper, we detail how these fully automated, on-chain governance systems are facilitated by the ICP platform's unique design. It includes upgradable smart contracts called ”canisters”, low transaction and storage costs compared to other platforms, a distinct separation between governance participants and node operators, and protocol-embedded node upgrades.

*bjoern.assmann@dfinity.org
†lara.schmid@dfinity.org

I. Introduction

A. What is a DAO?

A governance system is a framework that allows people to jointly make decisions. The governance system defines, for example, who can contribute to decisions and how voting on decisions is organized. Decentralized Autonomous Organizations, DAOs, are governance systems that are implemented on blockchain platforms. The governance system, what decisions can be made, and what their effects are, are defined by smart contracts and enforced using software. According to some definitions [Buterin, 2014], smart contracts are only considered DAOs if they hold internal capital that they govern over.

B. A Short History of DAOs

The term DAO, and similar concepts such as Decentralized Autonomous Corporations (DACs), were introduced around 2013/2014. In 2016, a famous DAO "The DAO" was launched as a decentralized venture capital fund, where members could vote on investment decisions. A hack drained around a third of the DAO's funds, which led to a hard fork of the Ethereum blockchain as the funds were returned in one version (Ethereum) but not in the other one (Ethereum Classic). Since then, many different forms of DAOs have emerged, governing funds, full blockchains, or even real life assets. An example for the latter is the ConstitutionDAO which was formed in 2021 to purchase an original copy of the United States Constitution, but ended up losing the auction to a higher bidder [Matthews, 2021].

C. Why are DAOs useful?

DAOs are not very useful for organizations where there are few, centralized, decision makers and the decision process need not be public.

Rather they are useful for organizations where a decentralized group of people, with potentially different interests, collaborate and collectively make decisions. Since the governance rules and the decisions are encoded in smart contracts, they are publicly verifiable by all DAO members and do not require members to trust the governance system or other members.

D. The Disadvantages of Off-chain Actions

Autonomy and decentralization of trust are two central goals of DAOs. However, in many DAOs decision making satisfies these goals but the decisions are then executed off-chain. For example, the DAO decides on some protocol changes or payments to parties that are then executed by an individual off-chain. Trust in centralized parties who must execute decisions

according to what and when they are made by the DAO contradicts the aim that a DAO should be decentralized. The risk of this is illustrated, for example, by a case where ARB tokens were already spent while the respective vote was still ongoing and even had 75% of voters against it [White, 2023a]. Moreover, the fact that a DAO requires off-chain executions contradicts the goal of autonomy and has the disadvantage that the off-chain component may not be publicly verifiable. For instance, a DAO community was tricked to pay 76 ETH to an attacker who entered their wallet into a hidden row of a spreadsheet that was used to collect payments [White, 2023b].

Another kind of decision that is not executed fully automatically on many blockchains is the upgrade of the blockchain itself. Many popular blockchains, such as Bitcoin or Ethereum, are upgraded by all computers or node providers agreeing on a new protocol version and then upgrading to this new version at roughly the same time. To ensure that a blockchain is available at all times, this requires a lot of off-chain coordination.

In this paper, we present the DAOs on the Internet Computer (ICP) [DFINITY, 2022] that enable decisions that are executed fully on-chain, including upgrades of the DAOs and the blockchain protocol itself. We first present the DAO that governs the Internet Computer which is called Network Nervous System, NNS, then explain the ICP's architectural components, and finally point out distinctive features that enable the NNS DAO and other DAOs that are hosted on the ICP.

II. The DAO that governs the Internet Computer

A. On-chain Governance via the Network Nervous System (NNS)

The Network Nervous System, NNS, is the DAO that governs the Internet Computer. It is permissionless and facilitates continuous upgrades of the blockchain protocol through voting of ICP utility token holders. Unlike blockchains like Ethereum, governance is embedded and enacted fully on-chain, avoiding complicated coordination and the risk of forks. The NNS is a stake-based voting system: any ICP token holder can participate in governance by staking ICP in a "neuron" and their voting power is dependent on the staked amount. Proposals for protocol-level changes can be submitted by any ICP token holder and, upon approval through a predetermined voting threshold, are autonomously executed by the NNS on-chain. ICP token holders can vote on upgrades to new protocol versions, replacement of node machines, changes to the governance & tokenomics and much more.

B. Liquid Democracy: Inclusivity in Decision-Making

The governance model of the Internet Computer is built around a concept known as liquid democracy, that combines aspects of direct and representative democracy. For each proposal, DAO members can vote directly or delegate their voting power to trusted entities or experts. This creates a democracy where voting power is dynamically allocated for each proposal, ensuring a balance between expert input and general participation.

III. Internet Computer Architecture

A. Nodes: The Foundational Units

The Internet Computer runs on physical node machines, the foundational building blocks of its architecture. These machines execute the protocol and store blockchain state. Node machines are high specification servers, standardized for optimal performance. They are distributed across independent data centers worldwide.

Node providers are the entities responsible for the physical hardware and overall maintenance of nodes. They undergo a governance onboarding process by the NNS, which involves providing verifiable proof of identity and resources. The Internet Computer features a diverse set of many independent node providers.

B. Subnets: Striking a Balance between Scalability and Security

A subnet is a collection of nodes that run their own instance of the consensus algorithm to produce a subnet blockchain that interacts with other subnets of the Internet Computer. This concept is similar to shards on other blockchains. Subnets play a pivotal role in striking the balance between scalability and security.

- Scalability: Replication is expensive. In a system with thousands of applications that can each have a large state, it is impossible to store all this information on every single node.
- Security: Applications must run on enough nodes to guarantee data integrity and uninterrupted uptime, even in the byzantine setting where nodes can fail or be malicious.

C. Canisters: Bundling Code and State

Subnets host smart contracts, which are called “canisters” on the Internet Computer. These are computational units which bundle together code and state. Unlike on other blockchains, canister smart contracts have a range of control settings from immutable to mutable. Each

mutable canister defines a controller who can update the canister code. This allows developers to build full decentralized applications (dapps) on-chain, even if the dapps must be adjusted over time to user needs. Canisters also have the ability to make http calls and can thus be integrated with web2 components. They can also directly integrate with other blockchains.

D. Chain-Key Cryptography: Efficiency and Decentralized Security

One of the Internet Computer's key features that enable subnets is an advanced cryptographic technique called chain-key cryptography. At the heart of chain-key cryptography lies a threshold signature scheme. This scheme resembles a standard digital signature, but with a twist: the secret signing key is distributed across all nodes within a subnet. This distribution ensures that a signature can only be produced if sufficiently many nodes agree on it.

The benefits of this sophisticated cryptographic technique include:

- Consistent Public Key: When interacting with the Internet Computer, clients and dapps only need to know one root public key. They can verify messages from any subnet by using this key.
- Inter-Subnet Communication: Similarly to the clients, subnets can use chain-key cryptography to authenticate the legitimacy of the incoming messages from other subnets.
- Adaptable Node Topology: The Internet Computer's network can evolve autonomously. Nodes and subnets can be added and removed from the Internet Computer's network due to the fact that chain-key cryptography allows dynamic resharing of the distributed secret key.

E. The Reverse Gas Model: Developer and User Friendly Fueling

The Internet Computer utilizes a reverse gas model. Instead of users bearing the computational cost, developers pre-charge canisters with "cycles" by burning ICP tokens. These cycles are expended for the canister's computations and storage needs. The primary benefit of this approach is twofold: users engaging with dapps housed in canisters are not burdened with transaction fees, and they do not require specialized wallets. As a result, user interaction with dapps mirrors the experience of using traditional applications and websites.

F. The Network Nervous System's Architectural Role

The NNS DAO itself is realized by a set of canister smart contracts, situated on a special subnet. It orchestrates the organization of the entire blockchain. New node providers are approved

by the NNS DAO and are granted permission to add a limited number of nodes. The NNS DAO then determines how the available nodes are grouped into subnets. Moreover, the NNS specifies the code that is run on the nodes. When the blockchain protocol requires an update, the NNS first approves a new code version that should be run by the nodes. After that, the NNS determines which nodes should be updated to this new version, making these decisions at the subnet level.

To make this process seamless, a "registry" on the chain holds all pertinent details, including information about the nodes, their arrangement into subnets, and their respective software versions. When the NNS makes a decision, such as updating the nodes of a subnet to a new version, the protocol automatically updates this registry. Nodes then periodically access the registry, determining when to upgrade and to which version without the need for any action from node operators.

The NNS also oversees the Internet Computer's tokenomics, managing aspects such as the cost in cycles of computation & storage and token-related incentives.

IV. Internet Computer Platform properties facilitating DAOs

A. The Network Nervous System: the DAO governing the blockchain

The NNS heavily relies on the unique design aspects of the Internet Computer's Architecture.

NNS canisters are mutable smart contracts that can be updated by their controller. In order to ensure that they can only be updated according to NNS DAO decisions, the NNS canisters are set up to control each other. This design allows governance rules to evolve iteratively, adapting to the needs and optimizations of the network.

As detailed in Section III, the reverse gas model of the Internet Computer allows users to interact with dapps without incurring transaction fees. This model benefits NNS DAO members, enabling them to vote on numerous proposals at no cost. Operations on the NNS subnet are exempt from charges, ensuring that governance activities are not hindered by operational costs. This zero-cost operational model for the NNS is cross-subsidized by other subnets. This is possible due to the low computation and storage costs on the Internet Computer compared to other platforms. The affordability means the NNS can process and store a high volume of votes and proposals and also carry out decisions on the chain autonomously.

On the Internet Computer, a clear distinction is maintained between governance participants and node providers. Governance participants (ICP token holders) have the power to decide on the trajectory of the blockchain without being directly involved in its technical maintenance. Conversely, node providers, who contribute to the blockchain's stability and security, do not have influence over governance decisions, unless they become governance participants

by staking ICP and thereby becoming committed to the Internet Computer.

The Internet Computer's native capability for protocol-embedded node upgrades enables the NNS to update the protocol seamlessly without necessitating any manual steps by node operators and without the risk of forks. When the NNS approves a proposal for a protocol upgrade on a subnet, it is automatically deployed across all nodes. This automated upgrade mechanism minimizes the risk for disruptions due to operational error and maintains a high degree of network integrity and security.

B. Service Nervous Systems: System-provided DAOs

Many of the previously mentioned features that enable the NNS also facilitate other applications on the Internet Computer, including DAOs that govern individual dapps.

- Low Barriers for Governance Participation: The reverse gas model ensures that there is a low entry barrier for governance participation, as costs are minimal or even waived entirely for end-users.
- Fully On-Chain Dapp Hosting: The Internet Computer's affordability in terms of computation and storage permits dapps to be hosted entirely on-chain. This includes not just the backend but also the frontends with all their related assets. Combined with the upgradable nature of canister smart contracts, this enables dapps that are fully decentralized and DAO-controlled.
- On-chain Proposal Execution: The low costs enable all DAO decisions to be executed directly on-chain. For example, dapp canisters can be automatically updated to new code and other execution can be triggered by DAO decisions.

These advantages facilitate a variety of possible DAOs on the Internet Computer. A prime example is the built-in Service Nervous System (SNS) framework. This framework allows any dapp developer to decentralize their dapp's control by initiating an NNS proposal which launches a new SNS DAO and assigns the dapp's control to it. A successful SNS launch entails the creation of the SNS, the collection of initial funds in exchange for governance control, and the consequent transfer of the dapp's control to the nascent SNS.

In terms of architecture, an SNS DAO mirrors the NNS, featuring a stake-based governance system to facilitate decision making and governing the dapp. Moreover, it possesses a ledger that defines a unique governance token for each SNS. For easy verifiability and user adoption, all SNSs run the same canister code. However each SNS community can choose the governance rules, tokenomics, and the supported proposals according to their needs.

V. Conclusion

The Network Nervous System (NNS) DAO on the Internet Computer facilitates fully on-chain governance, including upgrades to the protocol itself. This eliminates concerns related to off-chain trust and enhances the autonomy and decentralization that DAOs promise.

Four key features of the Internet Computer's architecture empower these advancements:

- Mutable Canisters: Offering flexibility in dapp development by allowing updates to be made over time.
- Reverse Gas Model: Streamlining user interactions with dapps without the burden of transaction fees.
- Governance and Node Operation Separation: Ensuring unbiased governance, where decision-making and technical operations are distinctly separated.
- Protocol-Embedded Node Upgrades: Facilitating automatic, disruption-free protocol upgrades with increased security.

This architecture not only sets the foundation for the NNS DAO but is also indispensable for the development of decentralized applications (dapps) with canisters. Furthermore, it paves the way for the creation of DAOs that can govern these dapps comprehensively. Due to the Internet Computer's architecture, a DAO can exert full control over a dapp, including all its components such as a web frontend, and execute DAO decisions autonomously on-chain.

The Internet Computer's approach to DAOs holds the potential to redefine the blockchain landscape. Since the start of this year, more than ten SNSs have been successfully launched on the Internet Computer, raising a total of 15M USD [Lawrence, 2023]. We eagerly anticipate the evolution and future of DAOs on the Internet Computer, convinced of its potential to advance decentralized governance.

References

[Buterin, 2014] Buterin, V. (2014). Daos, dacs, das and more: An incomplete terminology guide. https://blog.ethereum.org/2014/05/06/daos-dacs-das-and-more-an-incomplete-terminology-guide.

[DFINITY, 2022] DFINITY (2022). The internet computer for geeks. https://internetcomputer.org/whitepaper.pdf.

[Lawrence, 2023] Lawrence, C. (2023). Web3 platforms are successfully fundraising without a vc in sight raising $15m. https://tech.eu/2023/09/15/web3-platforms-continue-fundraising-without-a-vc-in-sight/.

[Matthews, 2021] Matthews, K. (2021). Rare first printing of us constitution sells for record $43m. https://apnews.com/article/cryptocurrency-technology-lifestyle-business-arts-and-entertainment-b0ab721a52cf20

[White, 2023a] White, M. (2023a). First arbitrum dao vote spirals into disaster: Dao rejects $1 billion spending proposal, but arbitrum already started spending. https://web3isgoinggreat.com/?tech=dao&id=first-arbitrum-dao-vote-spirals-into-disaster.

[White, 2023b] White, M. (2023b). Peopledao loses $120,000 after payment spreadsheet is shared publicly. https://web3isgoinggreat.com/?tech=dao&id=peopledao-loses-120000-after-payment-spreadsheet-is-shared-publicly.

7.14. User-Centric Authentication in Web 3.0

AUTHOR:

Björn Tackmann

DFINITY

User-centric authentication in Web 3.0

Björn Tackmann, DFINITY Foundation

Abstract

Humans are notoriously bad at managing secrets, which may be best witnessed by the ubiquity of problems with passwords in Web 2. The seed phrases used by most Web 3 wallet software, however, only amplify the problem. Seed phrases, unlike passwords, are practically non-memorable, so they have to be managed explicitly outside of the user's brain. On most blockchain platforms, there are also no built-in methods for key recovery or rotation, so failures in safely and securely managing the secrets are immediately catastrophic. So how can we enable non-expert users to safely participate in Web 3?

Internet Identity is a non-custodial and self-sovereign blockchain authentication system on ICP, which enables users to securely manage their identity across multiple devices without ever explicitly touching cryptographic secrets. Internet Identity achieves this by building on two main technical foundations:

- Web authentication: Modern devices support secure management of cryptographic key material using the FIDO and web authentication standards. Instead of remembering different passwords for each service, the user only requires a secure mechanism for unlocking their device, and the device securely manages the secrets.
- Chain-key cryptography: The cryptographic mechanisms implemented in ICP allow to untangle the single, static cryptographic key that represents the user's identity on the blockchain from the multiple, more ephemeral cryptographic keys held on the users devices and used for authentication.

The user experience of Internet Identity revolves around the user's *identity* to which a user can associate multiple devices or recovery mechanisms. The user can then use any one of their associated devices to authenticate toward dapps in a user flow resembling the smooth "sign in with Y" products in Web 2, while maintaining self-sovereignty.

This article describes the Internet Identity blockchain authentication system, its technical foundations, and the vision for future development. The article also discusses experiences from more than two years of production use.

1 Introduction

Transactions in blockchain networks are authenticated using digital signatures. Hereby, a digital signature scheme refers to a cryptographic mechanism in which a client signs a message using their private cryptographic key. The verification of the signature and thus the authenticity of the message, by contrast, is performed relative to a public key, which is derived from the client's private key. Digital signature schemes were first proposed by Diffie and Hellman as *one-way authentication schemes* in their seminal paper introducing public-key cryptography [Diffie and Hellman, 1976].

Assets on a blockchain are associated with an *address* of the user (or the smart contract) that holds the asset. For user-held assets, the address is derived from the user's public key. As a user's assets on a blockchain are controlled through transactions that are authorized via digital signatures, the security and accessibility of a user's assets is directly dependent on the user's ability to keep the private signature key both secure and accessible. If a user's private key was stored insecurely and exposed to some external party, that party would immediately be able to transfer the user's assets. Likewise, when a user loses access to their private key, they also lose the capability of controlling their assets.

The device or program used to store the user's private key is usually referred to as a *wallet*. There are two fundamentally different types of wallets:

- In the case of *custodial wallets*, the user delegates the management of cryptographic keys to a third party, the custodian. When the user intends to send

a blockchain transaction, they have to interact with the custodian. During this interaction, the custodian usually authenticates the user. This authentication can be performed using with various methods ranging from standard Web 2 mechanisms (e.g., username and password) to video calls in which the custodian verifies the intent of the transaction with the user.

- A *non-custodial wallet* is a piece of software or hardware that is under control of the user and stores the cryptographic key. Examples of non-custodial wallets include browser extensions such as MetaMask[1] or hardware devices such as the Ledger Name[2] line of devices.

Custodial and non-custodial wallets have different characteristics and use cases, which are not further discussed in this article. This article focuses on the case of non-custodial wallets.

1.1 The problem of managing secrets

A non-custodial wallet, at its core, stores the user's private signature key. Since the key may have significant assets linked to it, the management of this key has two somewhat conflicting requirements: First, the key must be kept *secure*, meaning that it must be protected from access by people other than the legitimate owner. Second, the key must be kept *accessible*, meaning that the owner must still be able to access or recover the key even in case they, e.g., lose or break their devices that store the key.

For backup purposes, most wallets support a standard called BIP-0039.[3] Following this standard, a secret seed from which the cryptographic keys are derived is encoded as a phrase consisting of 12 or 24 common words. Upon replacing their device, the user initializes the new device using the seed phrase, the device decodes the seed and computes the cryptographic keys from it. The mechanism was invented for Bitcoin but is nowadays supported universally in the Web 3 ecosystem.

[1] `https://metamask.io/`

[2] `https://www.ledger.com/`

[3] `https://github.com/bitcoin/bips/blob/master/bip-0039.mediawiki`

The problem with BIP-0039 is that it requires the user to record the seed phrase in a way that is:

1. protected from access by other people, but
2. can be reliably retrieved in case the user needs to recover the wallet after a software upgrade or on a different device.

For tech savvy users that set up a system for high-value transactions, this is usually not a problem. The user will prepare a sheet of paper (or a more durable material such as metal), which will later be stored in a safe or a bank locker for backup access after the seed phrase has been recorded. For more casual use, however, the seed phrase flow is a major obstacle: users that spontaneously set up a new wallet may not have a way to record the seed phrase in that moment at all, or they may record the phrase in a way that is either not properly protected and can be stolen or (more likely in practice) they will not remember where they kept the seed phrase when they need to recover it later.

What is thus needed is a method that is easy to set up and maintain and does not require the user to explicitly manage cryptographic key material. Internet Identity (in short: *II*), the blockchain authentication system described in this paper, solves this problem based on web standards as well as the features of the ICP blockchain.

Outline

Section 2 introduces basic terminology required for the main part of the paper. Section 3 describes the user perspective on Internet Identity; how an identity is created, used, and maintained. The system architecture is then detailed in Section 4, before Section 5 provides a high-level overview of the cryptographic protocols. Section 6 describes some security properties of Internet Identity. Section 7 contains insights from more than two years of production use, and Section 8 lists planned extensions and improvements for future releases.

2 Background

2.1 Web authentication and FIDO

Web authentication[4] is a standard published by the W3C that enables web applications to access secure cryptographic authentication mechanisms. Web authentication was initially designed in the context of two-factor authentication (2FA), where the first authentication factor—typically a password—is complemented with a second factor—typically a device that the user holds. This device could be the user's mobile phone or computer, or a dedicated security device that is attached to the user's phone or computer via USB or NFC.

Web authentication is particularly well-suited to counter phishing attacks, in which a user is tricked into entering their credentials for some trusted web site into a fraudulent web site owned by an attacker. The attacker records the user's credentials, and can subsequently use them to perform malicious transactions on the user's behalf. Web authentication prevents this attack by binding the 2FA authenticator to the domain of the web site: As long as the attacker cannot obtain a valid TLS certificate for the domain of the trusted web site, the binding reliably prevents the user from accidentally using the authenticator on the attacker's fraudulent web site.

The cryptographic keys used in web authentication were initially thought of as being tied to the authenticator device. Services offering 2FA would then offer a method for replacing the authenticator to deal with the case In which the device got lost or stolen. Since Apple and Google developed protocols for securely synchronizing these cryptographic keys across multiple devices, web authentication has recently been suggested as primary user authentication mechanism, replacing the password entirely. In this context, the web authentication keys are often referred to as *passkeys*, which is also the terminology we adopt in the remainder of this work.

[4] `https://www.w3.org/TR/webauthn-2/`

2.2 Threshold cryptography

In a *threshold cryptosystem*, a group of n parties jointly maintains a cryptographic key in a way that for some specified value $t \leq n$, referred to as *the threshold*, any t-out-of-n parties can jointly perform cryptographic operations, but any less-than-t parties cannot. A *threshold (digital) signature* is a cryptographic protocol in which n parties jointly hold a private key, such that for a given threshold t, any t-out-of-n parties can jointly sign a message, but any less-than-t cannot. The concept of threshold signature dates back to [Desmedt and Frankel, 1991].

2.3 ICP and chain-key cryptography

ICP—the Internet Computer Protocol [The DFINITY Team, 2022]—is a blockchain protocol that makes heavy use of threshold cryptography, especially the BLS cryptosystem proposed by [Boneh et al., 2004] and its threshold variant proposed by [Boldyreva, 2003]. A practical deployment of threshold signatures, however, requires a lot more than a bare threshold signature scheme: it also needs protocols for securely generating the key shared among the participants in a way that no single party ever controls the key, as well as for re-sharing the key upon membership changes as old nodes disappear and new nodes come online. Such protocols can be built based on *distributed key generation* protocols such as the one originally proposed by [Pedersen, 1991]. In the context of ICP, the entire suite of protocols used for maintaining and using the threshold signature key is usually referred to as *chain-key cryptography*, alluding to the fact that the blockchain protocol maintains the private signature key.

One main consequence of chain-key cryptography is that external parties do not need to maintain a copy of the entire blockchain to validate artifacts processed by the chain, such as output values computed by smart contracts. Everything the external parties need in order to validate an artifact is the public key of the chain and a signed certificate for the artifact. In a bit more technical detail, after processing one round of transactions, ICP nodes threshold-sign the computed state, which includes the outputs computed by all canisters. (For efficiency, individual outputs computed, e.g., in the same round can be authenticated together by

means of a Merkle tree [Merkle, 1987]. The certificate then contains the threshold signature and the Merkle tree path for the relevant artifact.) This not only enables blockchain applications that achieve full security while running on constrained devices or within a web browser, it also enables horizontal scaling of the blockchain protocol: The ICP network consists of multiple subnets, each of which is based on its own blockchain, and these subnets can interact securely with very low overhead.

2.4 Terminology

To remain consistent with existing literature on ICP, we adopt the same terminology. Smart contracts on ICP are referred to as *canisters*. Canisters do have more general properties than smart contracts on other platforms, such as an explicit notion of controller, but these differences will not be relevant in the context of this paper. The API of a canister consists of functions that can be called with arguments. Transactions sent to ICP are referred to as *(ingress) messages*. Each ingress message invokes a function on a canister with a specified argument. Each user and canister has a *principal*, which is the same concept often referred to as *address* in other blockchain platforms. The principal of the *caller* of a function, which may be a user or another canister, is exposed to the invoked canister.

3 The user perspective

The user experience of Internet Identity resembles the one known from Web 2. The user's internet identity, which is identified by a sequence number, looks and feels almost like an account in Web 2. This is despite the fact that II is a fully self-sovereign method of authentication, with the record of the user data relevant for verifying the authenticity of the user stored on the blockchain. More technically, the user's record contains the public keys corresponding to each of the user's passkeys. The user can use the II frontend[5] to manage their internet identity, or rather the record of their data stored on the blockchain. For instance, the user can

[5] `https://identity.ic0.app/`

add or remove additional passkeys or account recovery mechanisms to or from the user record. The frontend also allows to recover the account using any one of the registered mechanisms.

3.1 The creation flow

A user that visits the II frontend for the first time is asked to create a new internet identity. This involves, as a first step, the creation of a new passkey on the user's device. In this process, the device will prompt the user to provide an authentication gesture, which may be presenting the face or a fingerprint or simply touching an external security device. As a next step, the user is prompted to solve a simple CAPTCHA, which serves as a simple countermeasure against bots. Finally, the user is presented a (currently 7-digit) number, which serves as the identifier of the user's internet identity. The creation flow is usually completed in less than one minute.

3.2 The authentication flow

Web applications that support authentication via II generally display a button labeled "sign in with Internet Identity," or similar. Upon clicking the button, the II frontend opens in a new browser tab, in which the user then approves the authentication attempt as well as the use of the passkey. Using the passkey will require the user to provide the same authentication gesture as creating it (cf. Section 3.1). After the user is authenticated, the browser tab with the II frontend closes and the user is directed back to the application.

3.3 The management flow

If a user's internet identity is controlled through a single passkey, accessing this identity may be impossible if the device on which the passkey is stored is lost or stolen. Therefore, it is strongly suggested to add multiple passkeys or a recovery mechanism to the identity.

Users can maintain their internet identities by visiting the II frontend. After selecting the desired identifier, the user is asked to approve the use of the associ-

ated passkey, after which the user is forwarded to a management page displaying the currently registered passkeys and recovery mechanisms. On this page, new passkeys or recovery devices can be added, which is described in Section 3.4. Passkeys and recovery devices that are no longer functional or needed can be deleted.

3.4 The device addition flow

In case a user's passkeys are not automatically synchronized across all the user's devices, multiple passkeys can be associated to the same identity. All passkeys have equivalent capabilities, which implies that the user can use web applications from all registered devices seamlessly. The flow for adding a new passkey can be initiated from the II frontend on either (i.e., existing or new) device. When initiated from the existing device, a link (and QR code) is displayed that needs to be visited on the new device. Upon visiting the link, the new device generates a new passkey (authenticating the user in the process) and displays a 6-digit code, which then has to be entered on the existing device. Once this step is completed, the internet identity can be accessed from both devices.

II urges the user to additionally add a *recovery mechanism*. Currently, two types of mechanisms are supported. The first type is using an additional passkey, such as one stored on an external security device. The second type is using a BIP-0039 seed phrase, which is generated in the II frontend.

Supporting BIP-0039 seed phrases as recovery mechanisms may seem surprising; wasn't one goal of II to liberate the user from the burden of maintaining seed phrases? Indeed, and the addition of a seed phrase is entirely optional, the identity can be safely maintained via multiple passkeys. Also, the recovery seed phrase can be set up and replaced at any point in time, whenever it is convenient for the user.

4 System architecture

The II blockchain authentication system consists of three core software components: The *backend*, a canister smart contract running on ICP; the *frontend*, which

runs as a web application in the user's browser; and the *authentication client*, a library used by web applications that support authentication with II.

The backend canister. The backend canister stores all data relevant for user authentication, which includes the public keys associated with the users' passkeys and some additional metadata (e.g., whether a passkey is used for authentication or recovery). The backend canister serves as smart contract that encodes the rules for modification of a user's records. The canister also serves the frontend application into the user's browser.

The frontend application. The II frontend runs in the user's web browser. It enables the user to modify the data in the backend canister, such as by adding or removing passkeys and recovery mechanisms. The frontend also supports the authentication flow used by applications. Passkeys used for II are associated with the URL of the II frontend, `https://identity.ic0.app/`.

The authentication client. Web applications that integrate with II can use a library referred to as authentication client. The library offers a simple interface for application developers and manages the in-browser interaction with the II frontend during the authentication flow.

5 The Internet Identity protocol

As described in Section 1, blockchain transactions are authenticated by digital signatures, and the principal of the user sending the transaction is derived from the cryptographic key used to sign the transaction. This means that assets and capabilities are bound to the cryptographic keys that the transactions are signed with. In order to support the control of assets from multiple devices with (potentially) different passkeys, II has to dissociate the passkey stored on the user's device from the principal used to control assets on chain.

II achieves this dissociation by introducing a layer of indirection: The passkeys stored on the user's devices serve as a means of authentication toward the II backend canister. All the user's assets are then associated to a principal that is under

the control of that backend canister. The remainder of this section describes how the II protocol enables the backend canister to achieve its functionality.

5.1 Canister signatures

ICP subnets use threshold signatures to certify the state of the subnet after each round of computation (cf. Section 2.3). The subnet state contains so-called *certified variables* that can be written by canisters. A certified variable can then be efficiently verified by anyone using the subnet public key and the certificate for the variable written by a canister.

Certified variables can be used to define a (pseudo-)signature scheme for canisters, which is referred to as *canister signature*[6]: The canister writes the message it intends to sign into a certified variable, and the certificate for the variable becomes the digital signature in the signature scheme. The public key relative to which this new signature can be verified consists of the subnet's public key and the signing canister's principal, along with some canister-chosen auxiliary data.

Canister signatures can be used to authenticate ICP transactions. The caller principal of such a transaction is derived from the canister principal and the specified auxiliary data. Looking forward, the auxiliary data allows the II backend canister to generate different principals for different users and different contexts. Beyond that, however, the functionality of signing transactions by itself may not seem particularly useful; in the end, a canister can send messages to other canisters directly on chain, so why would it be helpful for the canister to sign a transaction? This becomes clear in the following section.

5.2 Delegations

Recall that the caller principal of an ingress message is derived from the signature public key that the message is signed with. ICP additionally supports a notion of *delegation* from one public key A to a second public key B. This allows the user to sign a message with public key B and send it to the blockchain together with

[6] `https://internetcomputer.org/docs/current/references/ic-interface-spec#signatures`

the delegation from A to B, which will result in the call being executed with the caller being set to the address derived from public key A.

The II backend canister uses the concept of delegation to delegate from the canister-controlled user (pseudo) public key to an actual key controlled by the web application running in the user's browser. Prior to the authentication flow, the web application generates a fresh signature key pair that corresponds to key B above. During the authentication flow, this session key is sent to the II backend canister, which signs a delegation from the (pseudo) public key associated with the user (which corresponds to key A above) to the session key. The delegation is returned to the web application, which can then sign further ingress messages with the session key.

5.3 Protocol flow

The complete protocol flow (on an abstract, cryptographic perspective) is then as follows:

- The user visits the web application. Upon the user clicking the button "sign in with Internet Identity," the II frontend opens in a new browser tab. The application generates a fresh signature key pair, holds the private key in the browser memory, and sends the public key to the II frontend via an in-browser message passing protocol.

- The II frontend generates a message that includes the newly generated public key. Upon the users approval, the message is signed using web authentication and sent to the II backend canister.

- The II backend canister validates the authority of the user and signs, using canister signatures with the public key associated to the user, a delegation toward the session public key provided in the ingress message.

- The II frontend retrieves the signed delegation from the II backend canister and forwards it to the application, again using the in-browser message passing protocol.

- The application signs blockchain transactions with the session public key, and includes the delegation from the II backend canister. This ensures that the *caller* attribute of the respective transactions is set to the user's identity that is controlled through the II backend canister.

6 Security

While a full analysis of the security if Internet Identity is beyond the scope of this paper, a few relevant security properties should be pointed out.

Isolation between different applications. As described in Section 5, an application that supports authentication with II receives, as result of the authentication flow, a delegation that allows the application to send messages using the user's principal to canisters on ICP. If multiple applications were to use the same user principal, security problems would arise: Suppose one of the applications is entrusted with maintaining valuable assets, while some other one is not. The second application, however, would have equal access to all assets maintained by the first application. Therefore, II derives a different principal for each application even for the same user. This is achieved by including the domain name of the application in the auxiliary data mentioned in Section 5.1. The use of the domain name as a separating property between different applications is consistent with the browser security model, which determines access based on the notion of *origin* that also includes the domain name.

The use of different user principals for different applications also impedes traceability of the same user across multiple devices and thus provides a certain level of privacy.

Storage of cryptographic keys. Devices that support web authentication generally store passkeys in specific secure chips, and the private keys cannot be exported to the operating system or even applications. Assuming the security of the secure hardware chips, the passkeys cannot be extracted even if the user's device gets infected with malware or stolen.

The fact that keys are stored securely does, however, not entirely rule out attacks via malware: As the user has no possibility to securely validate the message that is signed, malware on the user's device could replace a legitimate message that a user intends to sign with a fraudulent one before it is signed by the secure chip. In that sense, the security level is lower than with specialized hardware wallets that allow the user to validate the transaction details.

Security of the II canister. The II backend canister is developed as open-source software,[7] and upgrades to the canister are rolled out through ICP's decentralized governance system. This process ensures a high level of transparency.

7 Practical experience

Internet Identity was developed by the DFINITY Foundation and launched in May 2021 together with the ICP blockchain. Since then, the II canister is controlled through ICP's decentralized governance system. The further development of the Internet Identity protocol and its implementation is performed by DFINITY in collaboration with the ICP community. The subsequent paragraphs describe a few of the learnings the DFINITY team made since then.

Apple devices deleted web authentication keys. In Apple's implementation of web authentication up to iOS 15, cryptographic keys used in web authentication were strictly bound to the device on which they were generated. Somewhat surprisingly, upon clearing the browser history and cache, the web authentication keys would also get deleted. The effect of this behavior was that users would get locked out of their internet identities, requiring recovery.

The treatment of these keys changed completely in iOS 16 with Apple's introduction of the term *passkey*. Since then, the keys are synchronized between different devices via iCloud. They are also no longer deleted upon clearing the browser history and cache.

[7] `https://github.com/dfinity/internet-identity/`

Windows is different. Most platforms, including iOS, macOS, Android, as well as external security devices, generally use the ECDSA signature scheme, which is nowadays used ubiquitously on the web. Microsoft's Windows Hello, by contrast, is based on the older RSA signatures, whose use is otherwise generally discouraged. RSA signatures were not supported in the initial deployment of II, support was added in a later release.[8]

Users do not read warnings. Initial revisions of the II frontend supported unsafe operations such as the removal of all passkeys from an internet identity. While these operations were only performed after the user acknowledged multiple warnings about the deletion of the current and last passkey, several users contacted DFINITY for help after still performing these actions. Current revisions instead entirely block such unsafe behavior.

8 Future directions

Internet Identity has seen significant improvements since the first release in 2021, especially in terms of user experience. Several further features are currently planned or under development.

Attribute support. The II protocol as discussed in this paper is an authentication mechanism, but it currently falls short of being a full *identity* solution: The reason is that no attributes (such as age, nationality, academic credentials) can currently be assigned to the user's principal. Canisters can rely on the *caller* attribute of transactions to be set securely, but they do not know anything else about the user. Work toward supporting W3C verifiable credentials[9] in II is underway and close to completion.

Cryptographic privacy. As discussed in Section 6, the same user has different principals when using different applications. While this impedes traceability

[8] `https://medium.com/dfinity/windows-hello-support-added-to-internet-identity-e9021f74afe9`
[9] `https://www.w3.org/TR/vc-data-model/`

across different applications, it does not achieve anonymity in a strong, cryptographic sense. Based on advanced threshold cryptography that is currently being integrated in ICP, full cryptographic anonymity will be possible in the future [Cerulli et al., 2023].

Additional recovery mechanisms. The currently supported recovery operations (designated passkey, seed phrase) achieve a high level of self-sovereignty, but come at the cost of shifting significant operational responsibility to the user. Additional mechanisms such as social recovery (delegating authority to one or more friends) or support for professional recovery providers can be added to the protocol without major technical complications. By keeping the use of such features optional, II can serve both the (technically more proficient) users that have a preference for full self-sovereignty and the users that are willing to compromise on self-sovereignty for the benefit of easier management.

Acknowledgment

I would like to thank all researchers and engineers that contributed to the protocol and code, including Bartosz Przydatek, Christoph Hegemann, Frederik Rothenberger, Islam El-Ashi, Joachim Breitner, Mary Dwyer, Michel Abdalla, and Nicolas Mattia.

References

[Boldyreva, 2003] Boldyreva, A. (2003). Threshold signatures, multisignatures and blind signatures based on the gap-diffie-hellman-group signature scheme. In Desmedt, Y., editor, *Public Key Cryptography*, volume 2567 of *Lecture Notes in Computer Science*, pages 31–46. Springer.

[Boneh et al., 2004] Boneh, D., Lynn, B., and Shacham, H. (2004). Short signatures from the weil pairing. *J. Cryptol.*, 17(4):297–319.

[Cerulli et al., 2023] Cerulli, A., Connolly, A., Neven, G., Preiss, F.-S., and Shoup, V. (2023). vetKeys: How a blockchain can keep many secrets. Cryptology ePrint Archive, Paper 2023/616. https://eprint.iacr.org/2023/616.

[Desmedt and Frankel, 1991] Desmedt, Y. and Frankel, Y. (1991). Shared generation of authenticators and signatures (extended abstract). In Feigenbaum, J., editor, *CRYPTO*, volume 576 of *Lecture Notes in Computer Science*, pages 457–469. Springer.

[Diffie and Hellman, 1976] Diffie, W. and Hellman, M. E. (1976). New directions in cryptography. *IEEE Transactions on Information Theory*, 22(6):644–654.

[Merkle, 1987] Merkle, R. C. (1987). A digital signature based on a conventional encryption function. In Pomerance, C., editor, *CRYPTO*, volume 293 of *Lecture Notes in Computer Science*, pages 369–378. Springer.

[Pedersen, 1991] Pedersen, T. P. (1991). A threshold cryptosystem without a trusted party (extended abstract). In Davies, D. W., editor, *EUROCRYPT*, volume 547 of *Lecture Notes in Computer Science*, pages 522–526. Springer.

[The DFINITY Team, 2022] The DFINITY Team (2022). The internet computer for geeks. Cryptology ePrint Archive, Paper 2022/087. https://eprint.iacr.org/2022/087.

BLOCKCHAIN EXECUTIVES

1-1

8.1. Marcos Benitez - Copper.co

Can you provide a brief overview of your professional background and experience in your industry?

I studied law in my country and gained experience at one of the largest regional law firms, dealing with large corporations and decision-makers. However, I later shifted my focus to business and finance, where I found the perfect combination of finance and interpersonal skills, allowing me to build trust-based relationships. In 2009, I began my career in the FX industry, but unfortunately, I spent too much time on MetaTrader4 forums and missed out on learning about Bitcoin. Nevertheless, I gained exposure to trading platforms and launched my own money management platform with some colleagues for Iberoamerica, where I consulted with various clients. In 2015, I moved to Switzerland and began working for Morgan Stanley in Zurich. From there, I made decisions that brought me closer to the blockchain space, including co-founding the Crypto World Zug Association and consulting for companies like SmartContainers and Geeq.io. At the end of 2018, I was offered the opportunity to become the first employee of Gazprombank Switzerland's Crypto and Blockchain Department. Together with the Head, we helped the bank integrate new technology into their existing processes, which required significant changes. If it weren't for the war, they could have become a serious competitor to other banks offering similar services.

How have your past experiences prepared you for the challenges and opportunities in the evolving landscape of Web3?

As a former consultant for PwC and one of the largest Swiss Banks, I was first introduced to the world of Bitcoin and blockchain technology back in 2017. Since then, I have delved deep into the subject matter and realized the immense potential that Blockchain has to offer. As a former Law student, I understand the importance of the rule of Law in Western societies, and blockchain technology can help rewrite our societal contract and shift from centralization to decentralization. Having grown up in a developing country where poorly managed currency policies have caused significant damage, I also see the potential for Blockchain to offer the general audience a viable alternative.

With my background in Law and finance, I gained a unique perspective on how Blockchain can revolutionize various industries, from peer-to-peer payments to settlements and client position netting. Of course, I am not alone in this journey, and I have met many like-minded individuals who are motivated by the same topics, which will shape the future of our

economy and the way we understand not only wealth but power. Additionally, my consulting work has helped me establish a strong network of venture capital players, allowing me to participate in angel investments and get involved on a personal level with emerging technologies in the blockchain space. Overall, it is this unique amalgamation of personal experience that puts you in the right place (Crypto Valley) at the right time, and I have that conviction that there is no other place or industry I would like to be in. I can imagine many people share that feeling, and during the Web2 revolution, it was the same for many.

Blockchain and Web3 Expertise:

a. What do you see as the most significant developments or trends in blockchain technology and Web3 over the past year, and how have these impacted the industry?

Over the past year, there have been considerable advancements and trends in blockchain technology and Web3. As someone who closely follows the trading ecosystem at Copper, I've noticed a significant shift in sentiment towards centralization, especially after FTX. Additionally, there has been a lack of trust among certain counterparties, which has resulted in several clients suffering losses and some even going out of business. Moreover, the crypto ecosystem saw the closure of a few US banks like Signature and Silvergate, which were the backbone of the industry. This combination of bearish sentiment and lack of trust in institutions has led to a significant decline in capital inflows in the industry.

However, the industry has responded to these challenges by doubling down on solving these problems. Off-exchange Settlement solutions (OES) have seen a significant increase in popularity, and Copper, for instance, has been working on their product ClearLoop for about 4 years. It was the first off-exchange settlement network to market. We have seen a shift in motion, with clients reaching out to exchanges and asking them to integrate with us. This is one of the most significant shifts in the industry in the past year, and it is expected to continue for a while. Off-exchange solutions have emerged as the preferred option when it comes to dealing with centralized exchanges. Although decentralized exchanges may be the way of the future, it will take a while for institutions to consider DeFi as a viable alternative.

b. Can you share a specific project or initiative related to blockchain or Web3 that you've been involved in and the outcomes achieved?

Following up on the previous question, ClearLoop has been our primary focus. This is an initiative owned by Copper, and we have taken the lead in collaborating with other custodians to help them offer this solution to their clients.

Recently, we announced a partnership with Komainu, a UK-based FCA-regulated firm backed by Nomura, and, Bitgo, one of the largest US-based custody providers. Clients of these firms will soon benefit from ClearLoop's off-exchange settlement solution.

We are committed to assisting the ecosystem for the benefit of all. This is an excellent example of how companies can succeed by collaborating with the whole ecosystem, even

with their competitors. Bad actors can undermine the trust of institutional players in the system, which impacts us all. Therefore, we are determined to assist the ecosystem in expanding and setting standards, which will, in turn, bring more trust and, therefore, growth for every market participant, regardless of their size or expertise.

Risk Management in Web3:

a. How do you define and approach risk management in the context of Web3?

When it comes to digital assets, like those used in Web3, risk management is essential. Many traditional players may not be familiar with this new asset class, so it is crucial to bring them up to speed if we want widespread adoption of these solutions. Risk managers face numerous unknown risks, especially when it comes to investors looking to gain an extra yield while holding a position, such as staking ETH. To be comfortable with these new risks, investors must study the underlying technology. For example, slashing is not something an investor can control; it is tied deeply to the staking provider partner chosen. From there, investors need to understand their partner's setup, risks, processes, insurance, and more. There are many approaches to this new space, depending on an investor's strategy. Active management strategies and long-only strategies are the most significant differentiators.
To manage these risks effectively, investors must analyze the following types of Risk: Technological Risk, Regulatory Risk, Market Risk, Operational Risk, Reputational Risk, Financial Risk, and Third-Party Risk. While each type of Risk requires a deep dive, naming them can give an idea of the complexity of the approach.
In summary, defining your goals is the first step, and then you can set yourself or adopt a risk management approach tailored to your objectives.

b. What challenges do you believe are unique to risk management in blockchain and Web3 in particular in your industry?

As mentioned in the last question, we have identified quite a set of parameters unique to Web3 to analyze and understand. This is not a knowledge base that can be built overnight. Having faced many Funds of Funds and sizable Funds, we know first-hand that many have gone through a multi-year exercise before even considering opening up to external investors. It is always easier to lose your own money than someone else's. Hence, most TradFi shops would come at the end of a multi-year experiment led by the vanguardists. If you look into our Web3 ecosystem, there is a repetitive pattern. Crypto native or former TradFi investors, or a group of them, create an investment thesis that works in a contained environment. Once the validity of their approach is established, they believe it would be beneficial to offer the opportunity to others. However, this marks the end of self-custody as a viable option. Some of their strategies may be ineffective due to the market size, impacted

by the inflow of a more sizable position, or the lack of institutional providers capable of accommodating their setup.
The venture funds and liquid funds that invest in the top 50 or top 100 assets based on market cap have matured over time. However, when it comes to the thousands of assets that cater to retail and are relatively unknown to mature investors, there is still much uncertainty. In the world of Web3, launching a project is much easier than in traditional finance. A simple whitepaper or even less can be enough to create a project worth millions of dollars overnight. What is even more surprising is that such projects can become successful without even being adequately listed. DeFi is revolutionizing the way things work in this regard. Most of the trade volumes in DeFi are from retail investors, qualified investors (known as "whales"), proprietary trading firms, and market makers. These players are also present in centralized exchanges, but in DeFi, they are breaking all the molds.
When it comes to managing risk, combining the aforementioned risk management strategy with the dynamic realm of Web3 and DeFi can be an enjoyable but potentially stressful experience. Hence, it will be best to consider the experience of Institutional providers who have gone through the process already with other clients.

Improving Risk Management in Web3:

a. What are your thoughts on the current state of risk management practices in Web3, and what areas do you believe need the most improvement?

In the current state of risk management practices in Web3, it is essential to note that the technology is still in its early stages of adoption. While the potential for revolutionary change is great, there is a steep learning curve associated with it. It took several iterations and failed technologies to bring us to where we are in the Web2 space after 30 years of development, and even with all that progress, we still see non-stop data leaks from big corporations. Due to the inherent nature of decentralization, risk is an ever-present enemy that must be tackled appropriately.
To address this, companies like Copper are working tirelessly to build new standards for Digital Assets. However, at this early stage, more standardization is needed. It is important to note that adopting Web3 technology is a complex process and requires patience and perseverance. The industry must embrace the idea of continuous improvement and learn from past mistakes to build a more robust and secure ecosystem.
So, while the risk management practices in Web3 are still in their infancy, we must remain vigilant and take the necessary steps to ensure the safety and security of the ecosystem. The industry must work towards standardization, embrace continuous improvement, and learn from past mistakes to build a more resilient and secure system.

b. If you could suggest one innovation or change to enhance risk management within the Web3 space, what would it be?

Counterparty risk mitigation has become increasingly important in light of recent events. FTX, Alameda, Three Arrows Capital, Celsius, BlockFi, and many others have taught us that we need to be cautious when it comes to transferring funds from our wallets, even if we are chasing high yields. It is imperative that we engage in better Due Diligence practices with our counterparties, implement Operational DD practices and governance, and have a minimum set of internal policies in place. By doing this, we can have peace of mind knowing that we are ticking all the boxes, and that although there may be things out of our control, we have done everything we can to mitigate risk. It is sometimes better to forego a potential 8% APR than to risk losing 100% of our underlying investment. In the past, many players in our industry have invested based on the trust they had in the names that came before them. However, it has become clear that even the smartest investors can make mistakes. Therefore, we should not blindly trust, but instead, verify!

Collaboration and Ecosystem Resilience:

a. How important is collaboration and information-sharing among blockchain and Web3 projects for overall ecosystem resilience? Can you share an example where collaboration mitigated a potential risk?

Collaboration is key in this industry. By working together, companies can address challenges and create a larger market, benefiting all players. Once established, players can focus on gaining market share with unique value propositions. Balancing collaboration and competition is essential for success. This industry is still too small to even bother about serious competition. Hence, even layer ones should be key for supporting new technologies that other players can use to benefit the whole ecosystem. For retail security, I have witnessed how some players, i.e., MultiversX (formerly Elrond), have created the first 2FA verification built on-chain to safeguard assets. Since you can also store other blockchain assets on that wallet, this also benefits other chains. Also, they have integrated with Google to create a Web3 single-sign without asking the user to get familiarized with blockchain self-custody. At Copper, we prioritize security and risk management as crucial elements for widespread adoption of cryptocurrency as an asset class, particularly in the Web3 arena. As a user, I love when I can easily double-tap the side button of my iPhone to pay for things or even log in securely to a new website, which I may trust by obfuscating my identity via an Apple layer (identity relay). Hence, when we reach that level of second-layer security, without asking for retail to have to iron-brass their 24-word passphrase, then we would have achieved the starting point.

Many people talk about TPS and network usage to measure the success of blockchain technologies, which is understandable. Nevertheless, what is the point of scaling if we still need to get the users' attention? We must make Blockchain a widely used tool on the never-ending road of decentralization and sovereign identity.

8.2. Philipp Dettwiler - Blockchain & Finance Executive

Can you provide a brief overview of your professional background and experience in your industry?

I have been working for 20 years for Credit Suisse and UBS in different leadership roles in Europe and Asia in "TradFi", basically spanning across the entire value chain in banking, incl. relationship management, investment advising, global large-scale programs, product and service ownership roles. Since 2016 I have been interested in Web3 or what you rather called DLT or "crypto" at that point of time. Seeing the multisided application possibilities and potential as well as the inertia of incumbent players, I joined SEBA Bank AG in the beginning of 2019 as one of the first employees to secure one of the globally first crypto bank banking licenses. Next to my role as Head Custody, I was also building up the custodian bank and introducing a debit card scheme. After SEBA, I was taking on the role as COO of a metals tokenization platform.

How have your past experiences prepared you for the challenges and opportunities in the evolving landscape of Web3?

It might be an old saying, but the more I know, I know how little I know. This motivates me to continuously learn to embrace the challenges, not losing sight of the massive potential of our industry.

Blockchain and Web3 Expertise:
a. What do you see as the most significant developments or trends in blockchain technology and Web3 over the past year, and how have these impacted the industry?

The rise of decentralized finance (DeFi): The rise of DeFi has made it possible for people to access financial services without the need for banks, which has opened up new opportunities for people in developing countries and for those who are unbanked.
The increasing adoption of non-fungible tokens (NFTs): The increasing adoption of NFTs has created new markets for digital art and collectibles, and it has also opened up new ways for creators to monetize their work.
The development of the metaverse: The development of the metaverse has the potential to revolutionize the way we interact with the internet and with each other.

Layer 2 scaling solutions: Scalability challenges on major blockchains like Ethereum led to the development and adoption of Layer 2 solutions, including optimistic and zero knowledge (zk) rollups.Succinct Non-interactive ARguments of Knowledge (SNARK), Scalable Transparent ARgument of Knowledge (STARK), Succinct Non-interactive ARGuments (SNARG), Bulletproofs, Verifiable Polynomial Delegation (VPD) are interesting approaches for non-interactive zk protocols. Currently, we read particularly from EVM compatible and SNARK based zkSync (Matter Labs) and EVM equivalent and STARK/SNARK based zkEVM (Polygon).
DAOs: Decentralized Autonomous Organizations (DAOs) became increasingly important in governing blockchain networks and making decisions collectively. They represent a key aspect of Web3, where decentralized applications (dApps) are governed by the community.
Regulatory developments: Governments and regulatory bodies worldwide continue taking a closer look at cryptocurrencies, NFTs, and DeFi. The industry saw discussions on how to regulate these technologies while balancing innovation and investor protection.
Cross-chain compatibility: Projects like Polkadot, Cosmos, and interoperability-focused protocols gained attention for their efforts to connect different blockchain networks, enabling assets and data to move seamlessly between them.
Corporate adoption: More established companies, including financial institutions and tech giants, continue exploring blockchain technology for various use cases, such as supply chain management and digital identity.
Law enforcement: Authorities have beefed up their capabilities to prosecute criminal actors, protecting industry participants.
There is no doubt that these technologies will continue to have a major impact on the world in the years to come.

b. Can you share a specific project or initiative related to blockchain or Web3 that you've been involved in and the outcomes achieved?

The importance of cash is often underestimated. What we use as "cash" or the means of payment drives liquidity; we want neither too many forms of cash, as there were in the US in the 1800s, or cash in too many places. We also want to achieve a singleness of money, in other words the exact opposite of the US case. That singleness and single pool happens when the means of payment is programmable and interoperable. The means of payment should also be a regulated liability. As such, I see various drawbacks in current stablecoins as well as in the recently more en vogue deposit tokens. Therefore, I am currently looking into a faster, cheaper and better version of digital cash.

Risk Management in Web3:

a. How do you define and approach risk management in the context of Web3?

Risk management generally goes along the process of identifying, assessing, and mitigating risks. In Web3 these risks are usually related to technologies and applications and are probably in most cases related to the following risks:

Smart contract vulnerabilities: Smart contracts are self-executing contracts that are stored on a blockchain. They can be used to create a wide variety of applications, but they are also complex and can contain vulnerabilities. If a smart contract vulnerability is exploited, it could lead to the loss of funds or other assets.

Hacking and fraud: Web3 applications are vulnerable to hacking and fraud, just like any other software application. However, the decentralized nature of Web3 makes it more difficult to track down and prosecute hackers and fraudsters.

Regulatory uncertainty: There is currently a lack of clear regulation for Web3 technologies and applications. This could lead to legal and regulatory risks for users and developers.

Market volatility: The Web3 market is still very volatile, and the value of cryptocurrencies can fluctuate wildly. This could lead to financial losses for investors.

To mitigate these risks, it is important to have a comprehensive risk management plan in place. After identifying risks, you assess likelihood and impact of each to prioritize mitigation strategies such as using technical safeguards (e.g. smart contract security audits and bug bounties) or implementing operational procedures (e.g. user authentication and access control). It is important to monitor the risks on an ongoing basis and to update your risk management plan as needed.

On a private level, of course, follow the valid mantra “do your own research”.

What challenges do you believe are unique to risk management in blockchain and Web3 in particular in your industry?

Blockchain and Web3 present a number of unique challenges for risk management, including:

Complexity: Blockchain technology and Web3 applications are complex and can be difficult to understand. This can make it difficult to identify and assess all of the potential risks involved.

Decentralization: There is often no central authority that can be held accountable for security or fraud. This can make it difficult to track down and prosecute hackers and fraudsters.

Regulatory uncertainty: There is currently a lack of clear regulation for blockchain and Web3 technologies and applications. This can lead to uncertainty about the legal and regulatory implications of using these technologies.

Market volatility: The Web3 market is still very volatile, and the value of cryptocurrencies can fluctuate wildly. This can lead to financial losses for investors.

In addition to these general challenges, there are also some specific challenges to risk management in the blockchain and Web3 industry. For example, the following are some of

the challenges that financial institutions face in managing the risks associated with blockchain and Web3 technologies:
Integration challenges: Financial institutions need to integrate blockchain and Web3 technologies into their existing systems and processes. This can be a complex and challenging task.
Compliance challenges: Financial institutions need to comply with all applicable laws and regulations when using blockchain and Web3 technologies. This can be challenging given the lack of clear regulation for these technologies.
Cybersecurity challenges: Financial institutions need to protect their systems and data from cyberattacks. This can be challenging given the unique security risks associated with blockchain and Web3 technologies.
You might want to alleviate these risks by investing in education and training of your employees, implementing a robust risk management framework, using technology to your advantage and working with trusted partners.

Improving Risk Management in Web3:

a. What are your thoughts on the current state of risk management practices in Web3, and what areas do you believe need the most improvement?

There is a need for significant improvement in risk management practices in Web3. Awareness of this seems growing. Generally speaking, there is a lack of standardized practices and tools. Improvement potential revolves around the same topics mentioned above, namely smart contract security (robust process for identifying and fixing vulnerabilities), hacking and fraud (security measures to protect users), regulatory uncertainty (stay up-to-date on the latest regulatory developments).
Standardized practices and tools, however, does not mean applying a one-size-fits-all solution. The specific risks faced by a particular Web3 application or project will vary depending on a number of factors, such as the type of application, the technologies used, and the user base. Risk managers need to carefully assess the specific risks faced by their organization and develop appropriate risk management strategies.
As a community, we should keep developing standardized practices and tools, investing in education and training and promoting collaboration.

b. If you could suggest one innovation or change to enhance risk management within the Web3 space, what would it be?

The development of a comprehensive risk management framework that is tailored to the specific needs of the Web3 industry. This framework should be based on best practices from other industries, but it should also take into account the unique risks associated with Web3 technologies and applications.This would help organizations and individuals to better

understand and manage the risks associated with Web3 technologies and applications and make Web3 a safer and more secure environment for everyone.
Furthermore, I would appreciate to see a privacy preserving government supported Digital Identity initiative that facilitates easier onboarding and connections to services.

Collaboration and Ecosystem Resilience:

a. How important is collaboration and information-sharing among blockchain and Web3 projects for overall ecosystem resilience? Can you share an example where collaboration mitigated a potential risk?

Collaboration and information-sharing among blockchain and Web3 projects is essential for overall ecosystem resilience. When projects work together, they can better identify, assess, and mitigate risks. They can also share knowledge and resources, which can help them to develop more robust and secure products and services.
Collaboration and information-sharing in the blockchain and Web3 space can lead to reduced risk, improved security, increased innovation and faster adoption. Collaboration and information-sharing are essential for the resilience of the blockchain and Web3 ecosystem. There are multiple ways to do so, e.g. attending industry events, joining online communities, contributing to open source projects or simply sharing your knowledge.
In 2017, as an example, a group of researchers discovered a vulnerability in the Ethereum protocol that could have allowed attackers to steal millions of dollars worth of ETH. The researchers immediately disclosed the vulnerability to the Ethereum Foundation, which worked quickly to fix the vulnerability before it could be exploited.

8.3. Christian Ribeiro - CEO SulPayments

Can you provide a brief overview of your professional background and experience in your industry?

I have been actively involved in the cross-border industry for Latin American markets since 2006, accumulating valuable experience in this sector. My journey in the cross-border payments industry began with a focus on providing local payment solutions for international companies operating in Latin America. Essentially, my company acted as a local payment provider for international merchants.

In 2004, when I embarked on this path, the cross-border payments industry was relatively uncharted territory, and I recognized the significant opportunities it presented. My initial foray into this sector took shape while I was a university student, where I had a strong interest in online gaming. I observed a growing trend of students and users in Latin America engaging in online gaming, particularly with a game developed by Cipsoft, known as tibia.com.

Tibia.com offered both a free mode and a premium account, and it was clear that most Brazilian users were opting for the free version. This prompted me to investigate why users were not accessing the paid accounts. With the help of my father, I gained access to a professional gaming account, and the experience was so compelling that I began sharing it with my friends. To my surprise, many of them expressed a desire to purchase these accounts, but they encountered a common challenge—lack of international credit cards.

In response to this demand, I started offering professional gaming accounts to fellow students, and the demand quickly expanded beyond the university level to encompass the entire city. This endeavor eventually evolved into a formal company, which I later sold. My involvement in this space drew the attention of key players in the gaming industry, including Cipsoft, who invited me to GamesCom in Germany. Subsequently, I collaborated with industry giants like Blizzard and Valve Corporation to facilitate their entry into the Brazilian market.

Presently, I hold the position of CEO at SulPayments AG, a Swiss company specializing in instantaneous payment methods. Our focus extends across diverse areas, including gaming websites, in-game purchases, and serving as a fiat on/off ramp for cryptocurrency exchanges. Furthermore, our company is actively engaged in payment processing for USDT (Tether), a prominent stablecoin in the cryptocurrency ecosystem.

In summary, my professional background is rooted in the cross-border payments and gaming industries, and I have leveraged my experience to establish and lead SulPayments AG, a company at the forefront of innovative payment solutions for various sectors, including the burgeoning cryptocurrency market.

How have your past experiences prepared you for the challenges and opportunities in the evolving landscape of Web3?

My experience dating back to 2004 has consistently revolved around collaborations with local banks, primarily driven by the challenges posed by international payments. During that period, the landscape of purchasing games differed significantly from what is common today. Banks, in their caution, often questioned the nature of these game purchases, requesting extensive documentation and proof of the gaming transactions. This was especially true when considering in-game purchases, as banks struggled to grasp the concept of acquiring digital items within a game. In the context of 2004, this concept was quite foreign, and I often encountered perplexed reactions.

Fast forward to the present, and we can draw parallels to the challenges encountered in international remittances. When seeking to send money across the globe, particularly in connection with countries like Brazil and other Latin American nations, banks in Europe, for instance, still grapple with difficulties when it comes to accepting funds originating from outside of Europe. The onboarding process and transaction procedures remain heavily manual, often characterized by outdated bank technology. This outdated infrastructure contributes to the enduring problems of international payments being slow and costly.

The delay in these international transactions can be attributed to several factors, including legacy systems and stringent verification processes. It is imperative that the banking industry embraces more efficient and modern technologies to streamline international remittances, ensuring they are both timely and cost-effective.

Blockchain and Web3 Expertise:

a. What do you see as the most significant developments or trends in blockchain technology and Web3 over the past year, and how have these impacted the industry?

In the context of real-time transaction confirmation, a significant volume of communication is traditionally required between international banks. European banks must establish contact with local banks to confirm and validate the transaction. However, in today's landscape, blockchain technology has revolutionized this process by enabling automatic confirmation and funds transfer, obviating the need for intermediaries to vouch for the transaction's legitimacy.

Blockchain operates as a highly efficient mechanism for verifying critical transaction elements, including the identity of the sender, the recipient, and the availability of funds. Moreover, it accomplishes the instantaneous transfer of funds. This transformative approach has addressed a substantial challenge in Latin America's financial landscape, where timely and secure transactions were often elusive.

The key advantages of blockchain lie in its inherent trustworthiness, reliability, and cost-effectiveness. As a technology, it has disrupted the traditional financial ecosystem by providing a transparent and decentralized framework for transactions, ultimately enhancing efficiency and reducing associated costs.

b. Can you share a specific project or initiative related to blockchain or Web3 that you've been involved in and the outcomes achieved?

SulPayments AG stands as a pioneering global provider of stablecoin settlement solutions. Our core expertise lies in facilitating cross-border transactions through stablecoins, which presents a significant advancement in the world of digital finance.
Stablecoin settlement refers to the process of utilizing stablecoins, such as USDT (Tether), to settle financial transactions. Stablecoins are a subset of cryptocurrencies that are designed to maintain a stable value, often pegged to a reserve of traditional assets like the US dollar. USDT, in particular, is one of the most well-known stablecoins, and it is typically valued at one US dollar. This stability makes it a suitable digital asset for facilitating transactions.
USDT, or Tether, is widely used for several reasons. Firstly, its value is consistently tied to a well-established fiat currency, providing a reliable and predictable value. Secondly, it operates on blockchain technology, which ensures fast and secure transactions. Lastly, USDT offers a global reach and is widely accepted, making it a practical choice for merchants conducting business internationally.
The significance of using USDT and stablecoin settlement lies in the ability to pay merchants globally without the limitations that can accompany traditional banking systems. These solutions facilitate borderless and efficient financial transactions, transcending geographical and regulatory barriers. Additionally, stablecoins like USDT are highly transparent and audited to ensure their stability, which further enhances trust and confidence in cross-border financial operations.

Risk Management in Web3:
a. How do you define and approach risk management in the context of Web3?

Risk management in the context of Web3, particularly concerning payments, is a critical and evolving aspect of the digital economy. Web3, with its decentralized and blockchain-based technologies, presents unique opportunities and challenges that require a different approach to traditional risk management. Here's a breakdown of how risk management is defined and approached in the context of Web3 payments:
Smart Contract Risk: Web3 payments often involve smart contracts, self-executing agreements with code on the blockchain. Risk in this context includes vulnerabilities in smart contract code that can lead to financial losses.

Market Volatility: Cryptocurrencies are highly volatile, and their value can fluctuate significantly. Risk management involves accounting for price volatility when making payments in cryptocurrencies.
Counterparty Risk: In decentralized systems, there might be risks associated with dealing with unknown or pseudonymous parties. Trust in counterparty interactions is a key risk to manage.

Regulatory and Legal Risks: The evolving regulatory environment around Web3 and cryptocurrencies can introduce legal risks for payment services. Complying with regulations is essential.

In conclusion, risk management in the context of Web3 payments requires a proactive and multifaceted approach. It involves addressing security, market volatility, legal compliance, trust-building, and staying updated on the rapidly evolving landscape of decentralized finance. By embracing these principles, businesses and individuals can navigate the unique risks and opportunities presented by Web3 payments more effectively.

b. What challenges do you believe are unique to risk management in blockchain and Web3 in particular in your industry?

In the realm of blockchain payments, several critical factors demand vigilant attention to ensure the safety and accuracy of transactions. Firstly, it is imperative to validate that the public key, which serves as the recipient's address, is always correct. Any inaccuracies in the public key can result in the irreversible loss of funds. Secondly, verifying that the transaction occurs on the same blockchain network is of paramount importance. Attempting to transact across different blockchain networks can lead to funds being lost in the digital void.
Merchants engaging in blockchain payments must take an active role in managing their own wallets. This includes safeguarding their wallet's private keys and passwords with the utmost diligence. The loss or compromise of these credentials can lead to the irretrievable loss of assets and significant security risks.
In this decentralized and trustless environment, independence is a fundamental principle. However, it must be accompanied by a profound sense of responsibility. Each participant in the blockchain ecosystem, whether individuals or businesses, is entrusted with the duty to exercise prudent practices in securing their assets and conducting transactions accurately. In the world of blockchain, independence indeed comes with responsibility.

Improving Risk Management in Web3:

a. What are your thoughts on the current state of risk management practices in Web3, and what areas do you believe need the most improvement?

User Experience in Blockchain Transfers: Blockchain technology holds enormous potential, but the user experience for many remains far from ideal. One of the major pain points is complexity. Sending or receiving digital assets often involves dealing with long, alphanumeric wallet addresses, which can be intimidating and prone to errors. This complexity is a significant barrier to entry for newcomers.

Moreover, transaction speed is a common concern. Many popular blockchains face scalability issues, leading to slower confirmation times. Users may find themselves waiting longer than desired for their transactions to be validated, which can be frustrating.

Another challenge is the lack of user-friendly tools. Most blockchain interfaces and wallets are designed with technical users in mind. This can be a deterrent for individuals who lack a technical background, making blockchain technology less accessible to a broader audience.

Experienced and Trustworthy Companies:In the blockchain space, the presence of experienced and trustworthy companies is crucial. Security is of utmost importance when it comes to handling digital assets, and users need confidence in the entities providing services such as wallets, exchanges, and payment processors.

Regulatory compliance is another concern. Blockchain companies must navigate a rapidly evolving regulatory landscape, and users need assurance that the services they use adhere to the necessary legal standards. Trustworthy companies proactively address these compliance issues, ensuring users that their operations are both legal and secure.

Additionally, customer support plays a vital role. As the blockchain ecosystem grows, users require responsive customer support to assist with their inquiries and concerns. Established companies often provide robust support systems to cater to their user base.

To address these concerns and improve the blockchain ecosystem, a multifaceted approach is required. This includes designing more user-friendly interfaces, implementing scalability solutions, collaborating with regulators to create a conducive environment, educating users about the blockchain space, fostering transparency in operations, and encouraging innovation and collaboration within the industry.In essence, these improvements are pivotal in making blockchain technology more accessible, secure, and trustworthy for a wider user base. They are essential steps for the continued development and maturation of the blockchain industry.

b. If you could suggest one innovation or change to enhance risk management within the Web3 space, what would it be?

The emergence of new companies dedicated to enhancing the safety and usability of wallet creation, transaction sending, and fund reception represents a significant advancement in the blockchain and cryptocurrency ecosystem.

One of the primary objectives of these companies is to prioritize the security and safety of end users. They often employ robust security measures, including advanced encryption techniques and multi-factor authentication, to safeguard users' digital assets. As a result, users can feel more confident in their interactions with blockchain technology.

The process of creating a cryptocurrency wallet can be intimidating for newcomers. These companies have invested in developing intuitive and user-friendly interfaces that simplify the wallet creation process. This user-centric approach lowers the barrier to entry, making it accessible to a broader audience.

Sending cryptocurrencies often involves complicated wallet addresses and transaction fees. New companies are simplifying this process, providing users with straightforward mechanisms to send funds securely and efficiently. This simplification can reduce the likelihood of errors and enhance the overall user experience.

Receiving digital funds is a critical aspect of using cryptocurrencies, and these companies are committed to making this process safer and more convenient. They may offer features like customizable payment request links, ensuring that users receive funds in a secure and hassle-free manner.

In a professional context, the role of these companies in improving user safety and usability is of utmost significance. They contribute to the growing trust and adoption of blockchain and cryptocurrencies by offering user-centric solutions. Their commitment to security, ease of use, and efficiency in wallet creation, transaction sending, and fund reception aligns with the broader industry goals of making blockchain technology more accessible and reliable for a diverse user base. As the blockchain ecosystem continues to evolve, such companies play a vital role in shaping its future.

Collaboration and Ecosystem Resilience:

a. How important is collaboration and information-sharing among blockchain and Web3 projects for overall ecosystem resilience? Can you share an example where collaboration mitigated a potential risk?

Collaboration between companies in the Web3 industry plays a fundamental role in bolstering the safety and resilience of the ecosystem. This collaborative approach emphasizes the importance of working together rather than viewing each other as competitors. Here's how this collaboration contributes to a safer and more resilient Web3 industry:

1. Technology Standardization: When companies collaborate and use the same technology standards, the Web3 ecosystem becomes more unified and compatible. Standardization simplifies interoperability, reducing the risk of technical issues and enhancing overall resilience.
2. Knowledge Sharing: Collaboration creates a space for companies to openly discuss challenges, exchange ideas, and share valuable information. This collective sharing of knowledge leads to a deeper understanding of risks and paves the way for innovative solutions.
3. User-Centric Approach: By focusing on the end-user experience through collaboration, companies can collectively design more user-friendly solutions and services. This emphasis on user satisfaction builds trust and drives wider adoption of Web3 technologies.
4. Streamlining International Transfers: Collaborating companies can streamline international transfers by working together to create standardized processes. This simplifies cross-border payments, making them more efficient and less prone to complications.

8.4. Paolo Guarnerio - SDX SIX Digital Exchange

Can you provide a brief overview of your professional background and experience in your industry?

I have had the privilege of working in the blockchain and cryptocurrency industry for several years. My journey in this industry began in 2018 when I joined ShapeShift, one of the first cryptocurrency exchange. During my time at ShapeShift, I gained invaluable insights into the dynamics of the crypto market and the evolving landscape of digital assets.
In 2019, I embarked on an exciting new chapter of my career by joining SEBA Bank, a Swiss financial institution. At SEBA Bank, I served as the Digital Custody Services Manager. It was a remarkable experience as I was involved in the bank's journey to obtain a banking license, becoming the first fully regulated crypto bank in Switzerland. I was fortunate to be part of the team that made this pioneering venture fully operational, which involved navigating complex regulatory challenges and ensuring robust risk management practices in the digital asset space.
More recently, in the present year, I decided to take on another challenge in my professional career. I joined SIX Digital Exchange, a subsidiary of SIX Group, as a Senior Business Development Manager with a specific focus on the Web3 business. SIX Digital Exchange is a leading player in the global financial industry, and it has been actively exploring the opportunities and challenges presented by Web3 technologies.

How have your past experiences prepared you for the challenges and opportunities in the evolving landscape of Web3?

My past experiences have uniquely prepared me for the challenges and opportunities in the evolving landscape of Web3. Working in the crypto and blockchain industry for several years has equipped me with a strong foundation in understanding the core principles of decentralized technologies and the associated risks and opportunities.
My role as the Digital Custody Services Manager at SEBA Bank was pivotal in preparing me for the challenges of crypto. SEBA Bank was a pioneer in embracing digital assets and becoming a fully regulated crypto bank in Switzerland. The journey to obtain a banking license and operate within a highly regulated financial environment gave me a deep understanding of regulatory compliance, a skill that is essential in Web3 where regulatory

frameworks are rapidly evolving. Furthermore, managing digital custody services at the bank exposed me to the complexities of safeguarding digital assets and managing risk in a rapidly changing crypto landscape.
Joining SIX Digital Exchange as a Senior Business Development Manager with a focus on Web3 has allowed me to leverage this extensive experience to navigate the opportunities and challenges presented by Web3 technologies. The knowledge and insights gained from my previous roles in the crypto and banking sectors are invaluable in identifying, assessing, and managing risks while harnessing the potential of Web3 solutions.
Blockchain and Web3 Expertise:
What do you see as the most significant developments or trends in blockchain technology and Web3 over the past year, and how have these impacted the industry?

The past year has seen several significant developments and trends in blockchain technology and Web3 that have had a profound impact on the industry. Here are some of the key highlights:
Institutional Adoption in Switzerland and Europe: Switzerland and Europe have emerged as strong advocates for blockchain and cryptocurrencies, with a focus on enabling institutional adoption. Several banks and financial institutions in Switzerland and the broader European region have recognized digital assets as a new asset class. They are actively working to provide custodial and trading services for cryptocurrencies, which is a significant shift in the financial landscape. The regulatory clarity and progressive approach in these regions have played a pivotal role in attracting institutional interest.
Non-Custodial Solutions: Non-custodial solutions have gained traction as a viable alternative to traditional legacy systems. These solutions emphasize user sovereignty and control over digital assets. DeFi platforms, decentralized exchanges, and wallet providers have enabled users to manage their assets without relying on intermediaries. This trend aligns with the ethos of Web3, which empowers individuals and underscores the 'Don't Trust, Verify' principle. Non-custodial options have introduced a new paradigm for secure and transparent asset management.
Layer-2 Solutions on Bitcoin: Layer-2 solutions, such as the Lightning Network, have gained prominence on the Bitcoin network. These solutions aim to improve scalability and reduce transaction fees on the Bitcoin blockchain. By enabling faster and cheaper transactions, they enhance Bitcoin's utility as a digital currency for everyday use.

b. Can you share a specific project or initiative related to blockchain or Web3 that you've been involved in and the outcomes achieved?

One of the most significant projects I had the privilege of being involved in was during my work experience at SEBA Bank, where I served as the Digital Custody Services Manager. SEBA

Bank embarked on an ambitious journey to become the first fully regulated crypto bank in Switzerland.

The project's core objective was to obtain a banking license that would allow SEBA Bank to offer a comprehensive suite of services for digital assets, including cryptocurrencies. This involved a multi-faceted approach that required close collaboration with Swiss regulatory authorities, particularly the Swiss Financial Market Supervisory Authority (FINMA).

Navigating the regulatory landscape was a complex process that demanded a deep understanding of compliance and risk management in the digital asset space. We engaged in extensive and constructive dialogues with regulators, educating them about the unique features of cryptocurrencies and blockchain technology, and demonstrating our commitment to upholding high standards of security and transparency.

The successful outcome of this initiative was the granting of a full banking license to SEBA Bank, making it the first fully regulated crypto bank in Switzerland.

As a result of SEBA Bank's pioneering efforts, we witnessed a remarkable ripple effect in Switzerland's financial sector. Today, dozens of different banks, both large and small, in Switzerland offer cryptocurrency services to their clients. This project not only shaped the trajectory of SEBA Bank but also set a precedent for other financial institutions in Switzerland and Europe to embrace digital assets as a legitimate and regulated asset class.

Risk Management in Web3:

a. How do you define and approach risk management in the context of Web3?

Risk management in the context of Web3 requires a comprehensive approach. Web3, with its decentralized and trustless nature, introduces unique risk factors that demand specialized attention. Here's how I define and approach risk management in this context:

Comprehensive Understanding: The first step is to thoroughly understand the specific risks associated with Web3. This includes technological risks such as smart contract vulnerabilities, consensus algorithm weaknesses, and the potential for network forks. It also encompasses regulatory risks, market risks, and even reputational risks given the public and transparent nature of many blockchain networks.

Proactive Mitigation: Web3 risk management is about being proactive. It involves the implementation of best practices and robust security measures. This includes code audits for smart contracts, ongoing vulnerability assessments, and employing the latest security technologies to protect digital assets.

User Education: Users play a crucial role in risk management. Educating users on best practices, security measures, and the importance of self-custody can help reduce risks related to user errors and vulnerabilities.

Community and Industry Collaboration: Collaboration with the broader Web3 community and the industry as a whole is instrumental. Sharing insights, best practices, and threat intelligence can collectively enhance the resilience of the ecosystem.

b. What challenges do you believe are unique to risk management in blockchain and Web3 in particular in your industry?

Risk management in the blockchain and Web3 industry presents unique challenges, some of which include:
Regulatory Uncertainty: The regulatory landscape for blockchain and Web3 is constantly evolving. Navigating this uncertainty, especially in the context of global operations, can be challenging. Adhering to compliance while staying innovative is a delicate balance.
Irreversible Transactions: Blockchain transactions are typically irreversible. Mistakes can be costly, emphasizing the importance of user education and preventive measures.
Lack of Intermediaries: While the removal of intermediaries is a strength of Web3, it can also lead to a lack of recourse in the event of disputes, hacks, or losses.
Rapid Technological Evolution: The fast pace of technological advancements in the blockchain space means that risk management practices must constantly adapt to new threats and solutions.
Addressing these challenges requires a combination of proactive risk management strategies, collaboration with industry peers, engagement with regulators, and a deep understanding of the evolving technology and its implications for the industry.

Improving Risk Management in Web3:
a. What are your thoughts on the current state of risk management practices in Web3, and what areas do you believe need the most improvement?

The current state of risk management practices in Web3 has made significant progress, but there is still room for improvement. While some aspects are well-developed, there are specific areas that need more attention and enhancement.
Regulatory Clarity: Regulatory frameworks around the world are still evolving. Clarity in regulations and international standards would provide more certainty and facilitate compliance for businesses operating in the Web3 space.
Interoperability: With the rise of cross-chain interactions, ensuring the security and interoperability of different blockchain networks is a critical area that requires more attention.
Decentralized Identity: As decentralized identity solutions gain prominence, ensuring the privacy and security of user data is an ongoing challenge.

b. If you could suggest one innovation or change to enhance risk management within the Web3 space, what would it be?

If I could suggest one innovation to enhance risk management within the Web3 space, it would be the development of a standardized regulatory compliance protocol. By implementing a standardized regulatory compliance protocol, the Web3 ecosystem would promote responsible and compliant behavior, reduce regulatory risks, and create a more transparent and accountable environment for users and businesses.

Collaboration and Ecosystem Resilience:
How important is collaboration and information-sharing among blockchain and Web3 projects for overall ecosystem resilience? Can you share an example where collaboration mitigated a potential risk?

Collaboration and information-sharing among blockchain and Web3 projects are equally crucial in the context of institutional adoption. Here's an example of how collaboration helped mitigate a potential risk in this domain:
In 2021, as institutional interest in cryptocurrencies and blockchain technology surged, a potential risk emerged related to custodial services for digital assets. Institutions required secure and regulated custody solutions to enter the crypto space confidently. However, the industry lacked well-established standards and practices for custodial services tailored to institutional needs.
Recognizing the need to address this risk and foster institutional adoption, several blockchain and crypto firms collaborated. They formed a consortium focused on creating industry-wide standards for institutional-grade custody services.
This consortium included representatives from various blockchain projects, crypto exchanges, and financial institutions, all working together to establish best practices, security standards, and regulatory compliance frameworks. They shared their insights and experiences to develop a comprehensive set of guidelines for secure custody of digital assets.

8.5. Michele Federici - Founder Sig9 IT Security

Can you provide a brief overview of your professional background and experience in your industry?

I've always been a tech enthusiast and particularly intrigued by the security aspects of IT. Largely thanks to my nerd granddad, I began coding at a very early age, around 10. My involvement with the open-source community has also been constant, and that made me discover Bitcoin very early too, immediately falling in love with its principles and the technology behind it, and broadcasting my first transactions to the network in 2011.

I started my professional journey as a developer, specializing in secure coding and spending the initial years working on traditional payment gateways and biotech software. In 2019, I relocated to Switzerland to join the core team of SEBA Bank, which was still a startup at the time. As their Head of Blockchain Engineering, I oversaw the blockchain and custody sections of the bank for slightly more than 3 years. Notably, during that period, I also contributed to Bitcoin Core by identifying and helping to solve a critical bug. After departing from the bank, and after a shorter interlude as Head of IT Security at Dialectic, I chose to follow my own path.

I then established my cybersecurity consulting firm sig9.ch, co-founded the decentralized escrow protocol unicrow.io, while also serving as "CTO-as-a-service" for the Dubai-based VAF Compliance, a crypto compliance entity specializing in risk scoring and blockchain intelligence.

b. How have your past experiences prepared you for the challenges and opportunities in the evolving landscape of Web3?

The web3 ecosystem is a very dynamic amalgamation of different technologies, with security standing (not always, unfortunately) as a paramount component. I'm confident that the diverse skill set, flexibility, and security-centric approach of my team and myself align well within this domain.

In IT, maintaining a comprehensive understanding of every layer involved when constructing an application or platform is vital. Unfortunately, I've seen this holistic perspective fading over the years, as more and more professionals tend to specialize exclusively in a restricted set of skills, often on a single layer, not being able to spot or understand when something is going wrong, for example on a lower layer. While such narrow specialization can occasionally enhance productivity throughput, this assembly line approach has often been detrimental to companies, particularly at the expense of security.

Blockchain and Web3 Expertise:

a. What do you see as the most significant developments or trends in blockchain technology and Web3 over the past year, and how have these impacted the industry?

Over the past year, some of the technologies that have advanced and gained traction, ones that I'm particularly interested and enthusiastic about, include: ZK cryptography based projects, the Bitcoin Lightning Network and Layer 2 chains in general, and MPC (Multi-Party Computation) solutions.

Zero-Knowledge (ZK) cryptography has the potential to drastically improve scalability and privacy. In this context, I'm a member of the board of advisors of the promising crypto valley startup, Triton. They are developing Neptune, a new ZK-based Layer 1 blockchain, a very interesting project backed by an exceptional team. They recently launched their alpha network. Many other projects and players are emerging in this area and some ideas and advancements are truly noteworthy. I'm eager to be part of and observe how this will further evolve over time.

Speaking of the Bitcoin Lightning Network, while it's not something new, recent improvements in its protocol, tooling and overall UX have boosted its traction and user base. Personally, I'm using it much more frequently than before. The integrations shipped into various platforms, like the clients of the social network Nostr, are very smooth. It's remarkably easy and quick to "tip" a content creator in mere seconds and with negligible fees. At the same time, other Layer 2 solutions, for example within the Ethereum ecosystem, have greatly benefitted dapp developers and their users by dramatically reducing fees compared to mainnet, making them more accessible for a broader range of users and use cases.

Lastly, Multi-Party Computation (MPC) mechanisms, a rapidly progressing domain, promise to redefine custody and the way transactions are signed, offering, when implemented correctly, both improved security and flexibility.

b. Can you share a specific project or initiative related to blockchain or Web3 that you've been involved in and the outcomes achieved?

This year has definitely been quite busy for me, and I had the chance to engage in a multitude of fascinating projects and interesting initiatives in the Web3 space.

Due to its sensitive nature, there's unfortunately not much I can disclose on the work we have done at my cybersecurity consulting firm sig9.ch, but I'm happy to spend a couple more words on my other projects I mentioned previously:

unicrow.io is a smart contract based decentralized escrow system, designed to be unstoppable and trust-minimized. It's a project I co-founded with a friend and an idea we

were both, unbeknownst to each other, thinking about for maybe years. We aimed to fill what we considered a gap in the ecosystem, envisioning our platform as a sort of crypto version of Stripe in terms of integration ease. Everything about unicrow.io is transparent and open source, we didn't add any control over the contracts (ownership, upgradeability), and we released an SDK that allows anyone to integrate the system in their own e-commerce and start accepting crypto with just few JavaScript/TypeScript lines, without any onboarding and without having to manage custody and web3 integration.

Regarding VAF Compliance, we launched a Telegram bot (@VafComplianceBot) that combines the multitude of data sources offered by many crypto forensic companies and OSINT, to produce comprehensive risk reports and scoring for crypto addresses. This seems to be another ever growing field, especially as more heavily regulated players are joining the market.

Lastly, it's worth reiterating my endorsement for Neptune and its team, I believe they have the potential to make significant waves in the domain.

Risk Management in Web3:
a. How do you define and approach risk management in the context of Web3?
The main areas I focus on when drawing the risk profile of a Web3 project usually are:

Key management and custody risk: whenever custody, asset, or platform management is involved, the design of the key ceremonies (how the cryptographic keys are generated) and how keys are stored and used is of course critical. Key questions include: Is there a multisig in place for important management operations? Is there a single point of failure if a certain key or a set of keys are lost? How are backups managed?
Centralized infrastructure: no matter how decentralized a dapp can be, the reality is that we, most of the times, still need some centralized components. Considerations include: how is the frontend served and from where? How is it managed and deployed? A takeover of the frontend's hosting infrastructure often means that a malicious actor could tamper with the served code and potentially misdirect user transactions, resulting in theft.
Smart contracts: it's critical to review and audit smart contract code thoroughly. Beyond the risks posed by bugs that can lead to exploits or loss of funds, other concerns include aspects like contract ownership and upgradeability. Namely, the power to alter contract settings or even redeploy the contract itself.
Code development workflow and personal security: consider the damage a malicious actor could cause by compromising a team member's machine or wallet keys. What measures does the team take (e.g., multisig for certain operations, treasury management, deployments, etc.)? What security measures do individual developers implement?

Side channels: does the platform rely on external products, technologies, or hardware? Are these dependencies verifiable? Having an unverifiable, closed-source dependency is often a red flag.
Financial risk: does the application operate in illiquid or highly volatile markets? Is its financial model and or tokenomics sustainable?

b. What challenges do you believe are unique to risk management in blockchain and Web3 in particular in your industry?

Three challenges immediately come to mind:
Key management and custody: a copied seed leaves no trace, so generating the keys and backing them up following a proper design, planning, and in the right environment already covers a significant portion of common risks. Custody is a great power, but every great power comes with great responsibility.

Irreversibility: another fairly unique trait of the field. Unlike the traditional payment systems, any error, whether human or the result of a bug, can lead to irreversible and potentially catastrophic outcomes. This underscores the importance of treating the code involved as critical code.
Complexity and evolution of the technology: the rapid evolution of Web3 technologies means the environment is constantly shifting, as security paradigms and threat vectors change or evolve quickly, alongside the technology.

Improving Risk Management in Web3:
a. What are your thoughts on the current state of risk management practices in Web3, and what areas do you believe need the most improvement?

Security awareness in the space has steadily improved throughout the years, but there's still a lot of room for improvement. The uniqueness of many concepts has created a whole new set of approaches to risk mitigation, and the rapid technological advancement often means that adequate assessments and security practices lag behind, making the terrain fertile for hacking, especially when valuable assets are at stake.
Education is always one of the fundamental factors, and something that can always be continuously improved. Many stakeholders, users but also developers, often jump into this space, maybe even just for FOMO and without a comprehensive understanding of its inherent risks. Strengthening education around security practices and the fundamental principles of blockchain technology would considerably reduce the risks for human errors. Think about the evergreens keys and backups management, but also how to properly check the content of a transaction before signing and broadcasting. I find the latter a very interesting problem, since it’s often not possible to methodologically parse the entirety of

transactions contents to human readable information. Luckily though, today we have very helpful tools in this regard, for example to simulate transactions on local forks and see the outcomes (VM state changes) before actually sending the transaction to the real network.
User interface and user experience (UI/UX): a significant number of incidents are still caused by human errors, often due to confusing interfaces, processes or information. The ecosystem still has a long way to go for its abstraction layers to be simple enough to be understood, used and trusted by non-technical users, allowing them to fully benefit from these technologies. Clarity is critical, especially for tasks associated with high risks, and society already mass adopted many highly complicated systems in a much smoother way than what we can see in this domain today.
Monitoring and auditing: given the immutable nature of blockchain, regular audits and monitoring are crucial. Many projects do initial “checkbox audits”, but fail to follow up and keep auditing new code and features. Security should be a constant work. Monitoring systems and emergency switches/measures that account for this evolving threat landscape are often neglected.

b. If you could suggest one innovation or change to enhance risk management within the Web3 space, what would it be?

As previously mentioned, one thing I think we miss, at least in most chains, is a proper standard for transaction parsing. This, in my opinion, is one of the elephants in the room, but I don't see as much discussions around it as I'd expect, even though it has a lot of risk potential. Users are often blindly signing transactions without knowing exactly what operations they contain.
I can't help but mention the oldest pain point too: key generation, management and backup. I still feel we haven't found the final approach yet. What I foresee for the future are smoother systems for social recovery and easier, more flexible multisig setups. Technologies like MPC are promising in that sense, but I feel we still need to reach proper and more mature, battle-tested, implementations.
Another component, still missing, is a "web of trust" for crypto. The users of most of the dapps today could be easily tricked to sign rogue txs if a dapp frontend is hacked. A proper address book, maybe socially maintained, could greatly reduce that risk. Most wallets already support address books, but maintained by the user, which is good but not optimal, especially as protocols get more and more complicated, also increasing the number of contracts our wallets are requested to interact with.

Collaboration and Ecosystem Resilience:

a. How important is collaboration and information-sharing among blockchain and Web3 projects for overall ecosystem resilience? Can you share an example where collaboration mitigated a potential risk?

Information-sharing and collaboration, especially on tooling, standards, and common issues, is always undoubtedly valuable for everyone's security, in IT in general but particularly in decentralized contexts, where centralized controls are absent and the system depends on a collective, community-driven approach.

An example is the responsible disclosure of vulnerabilities, where researchers and developers report potential security threats to platforms before they can be exploited. In the blockchain space, such collaboration takes on even more urgency due to the real-time, irreversible nature of transactions.

Another example is the proactive sharing of intelligence among exchanges and forensic companies after incidents and security breaches. By pooling their resources and insights, these entities can sometimes manage to trace illicit fund flows, isolate threat vectors, and even help recover stolen assets in certain scenarios. Similarly, being part of specific communities and chat groups, as well as subscribing to real-time alerting systems can act as an early warning mechanism, enabling swift countermeasures and reactions against potential threats.

Moreover, open-source contributions represent a unique aspect of collaboration in the broader IT landscape. By openly sharing tools, platforms, and protocols, the community not only encourages innovation but also subjects these works to rigorous peer review. This transparency ensures that many issues and vulnerabilities in the code are identified and addressed by a diverse group of experts, enhancing the security and robustness of the overall ecosystem.

CVA RESEARCH JOURNAL 2023
DON'T TRUST, VERIFY. RISK MANAGEMENT IN WEB3.

CRYPTO VALLEY ASSOCIATION, SWITZERLAND
PULISHED NOVEMBER 27TH, 2023
www.cryptovalley.swiss