Crypto Valley

Blueprint Paper | 09.02.2022

Cybersecurity for Enterprise Blockchain Solutions

Published by CVA's Cybersecurity and Enterprise Blockchain Working Groups

www.cryptovalley.swiss

@thecryptovalley

Contributors

Moritz Kuhn
Adnovum AG

Michel Sahli
Adnovum AG

Gianluca Tordi
Alysidia GmBH, TS Quality & Engineering

Dr. Katharina Lasota Heller
LEXellence Legal Services AG

Natacha Linard
CYSEC SA

Frédéric Ballara
Fortinet SA

Blanca Angela Zutta
International Token Standardization Association (ITSA)

Dennis Flad
Chairman of CVA Enterprise Blockchain Working Group

Table of Contents

1 Introduction

Over the last decades a paradigm change happened in the space of Enterprise Solutions. Traditionally Enterprise Solutions were built to collect, analyze and distribute data for business critical processes within an enterprise. Today, Enterprise Solutions focus more on enabling the data exchange between enterprises. They become networks and in this context more and more enterprises analyze and deploy blockchain and distributed ledger technology (DLT) based solutions and infrastructures. Especially the aspect of decentralized infrastructure and data storage that enables the interconnection between network participants without depending on a central technology intermediary is seen as a key advantage for Enterprise Blockchain Solutions. However, with the new decentralized enterprise solutions the demands on the cybersecurity management are changing too.

In this paper, the Crypto Valley Association's Cybersecurity and Enterprise Blockchain working groups establish a blueprint and check list for organizations to quickly establish the security of their scalable blockchain and DLT infrastructure as a solid baseline. It is aimed at IT development and infrastructure practitioners seeking to establish best practices quickly and may be used by cybersecurity professionals as a jumping off point to dive deeper into developing customized solutions specific to their needs.

This publication focuses on traditional private DLT systems such as Hyperledger, R3 Corda or BigChainDB, which have been built from the ground up to replicate blockchain characteristics for private blockchain deployments. While we observe an increasing adoption of traditionally public blockchain software forked and used for semi-private networks, such as Quorum, Binance Smart Chain as well as side chains or layer-two-scaling solutions, their architecture is sufficiently different to warrant a different approach to scaling and securing them, given their semi-public deployments.

2 Cybersecurity and Enterprise Blockchain Solutions

by Frédéric Ballara

Because a blockchain is distributed and interconnected, it provides several essential services. The first is transparency. The access and exchange of data is an integrated part of a blockchain, or distributed ledger transaction and a copy of the data is not stored on a single but multiple stored and operated database (e.g. on Ethereum, Hyperledger) or on the databases of the involved parties of a data exchange (e.g. on R3 Corda). Depending on the underlying technology the data is transparent to some, or all involved parties. The second is that it is difficult to corrupt the data because altering any unit of information on the blockchain would also modify all subsequent blocks unless huge amounts of computing power are used to override the entire network. In most cases because it is distributed, it cannot be controlled by any single entity. And for that same reason, the possible occurrence of a single point of failure is reduced by design.

2.1 Access control and Privacy

When used by a consortium or private entity, most Enterprise Blockchain Solution will be permissioned. In such blockchains, a governance structure has to be defined. This structure ensures which users can view or update the blockchain, and how they can do it. This establishes a consensus process that is controlled by a pre-selected set of nodes and predefined rules of governance. For example, if you have a financial organization of 25 institutions, you may want to establish a rule requiring that at least 15 of them must sign a block in order for the block to be valid.

While blockchain technology guarantees integrity, security components such as access control and privacy are things that need to be overlaid. It is important that all participants be protected from unauthorized access. So, in a permissioned blockchain, outsiders should not be able to tamper with the ledger. Therefore, the administrator of the permissioned blockchain must minimize its attack surface. In practical terms, this means that every participant is a target, and that traffic to and from participating entities must be protected using policies.

2.2 Secure Key Management

A secure blockchain application requires the secure management of user private keys. Insecure key management can severely impact the confidentiality and integrity of data. Therefore, the same technologies that are typically put in place to address such concerns elsewhere should be used to secure these keys. Blockchain by itself doesn't make establishing this sort of control any easier or harder than with other technologies. The protection of these can be ensured using a variety of methods, including physical access control, network access control, and a key management solution that includes generation, distribution, storage and escrow, and backup etc.

2.3 Distributed Denial of Service (DDoS)

Blockchain transactions can be easily denied if participating entities are prevented from sending transactions. A DDoS attack on an entity or set of entities, for example, can totally cripple the blockchain organization and the attendant infrastructure. Such attacks can introduce integrity risks to blockchain by affecting such things as consensus. Therefore, blockchain architects must work with their security counterparts to ensure the availability of the infrastructure via such methods as building strong DDoS attack mitigation directly into the network.

3 Membership and Identity Management

by Michel Sahli and Moritz Kuhn

Clearly defined membership and verified identities are at the core of Enterprise Blockchain Solutions and differentiate conceptually from solutions based on public blockchains.

	Public Blockchain	**Enterprise Blockchain Solution**
Access of members	Open to everyone	Only registered members (consortium based)

Identity of members	Participants are (pseudo) anonymous	Identity of participants is verified
Storage of transactions	Transactions are public and stored on visible blocks	Transactions are private and data is selectively shared with only in a transaction involved members

Picture 1: Differences between Public Blockchains and Enterprise Blockchain Solutions

Only registered members with a verified identity participate in an Enterprise Blockchain Solution. This applies to organizations as well as to end-users and leads to a number of identity and membership management challenges.

3.1 Challenges

Many traditional approaches to identity management do not work very well for Enterprise Blockchain Solutions. For example:

- A central identity management solution conflicts with the distributed nature of the solution.
- Federated identity solutions do not scale enough for Enterprise Blockchain Solutions with a high number of members.
- In an Enterprise Blockchain Solution it is more difficult to establish a common trust anchor, because control over such a trust anchor should be distributed as well.

3.2 Onboarding, Identity and Privileges

For most Enterprise Blockchain Solutions the onboarding of organisations and end-users requires Know-You-Customer (KYC) compliance and corresponding processes. For organisations this often still involves non-digitalized “offline” processes, for example the signing of membership agreements, or the adherence to specific business rules or terms and conditions.

In this chapter, we focus on the next stage: the “technical” onboarding to the Enterprise Blockchain Solution, which takes place after the “offline” onboarding processes and a successfully completed

KYC process. An Enterprise Blockchain Solution Operator (EBSO) is responsible for "technical" onboarding processes.

For organizations, the "technical" onboarding process normally involves the following steps:

1. Registering the identity of the organization as a member or participant of the Enterprise Blockchain Solution
2. Registering authentication credentials of the new member
3. Issuing credentials that allow other participants to identify the new member
4. Issuing credentials that reflect privileges of the new member

The onboarding process of end-users (e.g. consumers, employees, micro-enterprises) normally includes the steps:

1. Identification of the person often using official identity documents. This step might also happen outside of the Enterprise Blockchain Solution in an "off-chain" process before the actual onboarding process starts.
2. Registration of the person and their authentication credentials on the Enterprise Blockchain Solution.
3. Mapping of the person's identity to an identifier and corresponding credentials.

The participants of a transaction on the Enterprise Blockchain Solution have to be able to verify:

- the identity and authenticity of the counterparty of the transaction,
- that the counterparty of the transactions is an valid member of the solution, and
- that the counterparty has the required privileges and authorizations for the roles they play in the transaction.

The result of such verification checks is that the members can be sure that the counterparty is what it claims to be, for example the participant is a medical doctor, an insurance regulated by the authorities, or a valid AI robot of a service company.

3.3 Protection of Identities

The secure storage of cryptographic keys can not easily be enforced. The principle of usage themselve are cryptographic secure but nothing can certify that an EBSO has not written the private key on a paper notice on their desk.

The Enterprise Blockchain solution should define rules on how to secure usage and storage of cryptographics keys. However, it will not be possible to enforce and certify such actions for each transaction.

Each participant is responsible for the protection of their cryptographic credentials used to authenticate and authorize transactions. The solutions to protect the cryptographic credentials depend on the kind of credentials and authority of the user. For example:

- End-users might use two-factor or multifactor authentication mechanisms to protect access to their private keys.
- Organizations might use conventional solutions to govern and protect access to private keys.
- The cryptographic credentials used as trust anchor for the whole Enterprise Blockchain Solution might be protected by key sharding.

3.4 Identification and Personally Identifiable Information (PII)

Special care has to be taken to avoid and protect Personally Identifiable Information (PII) on Enterprise Blockchain Solutions. PII should never be written to the ledger, because it cannot be removed afterwards. That means only a reference to the person should be written to the ledger. Additionally, this reference should not take the form of a global ID, because this would allow correlating transactions based on the ID. To prevent correlation, persons and organisations might use unique IDs per business relationship. Nevertheless, persons and organisations must be able to prove ownership of their IDs.

3.4.1 Revocation of privileges and offboarding

As for onboarding, the Enterprise Blockchain Solution Operator (EBSO) plays an important role at the end of the identity life cycle off-boarding participants and revoking their privileges.

In the following cases the EBSO has to revoke privileges of participants, block them temporarily or cancel their membership and offboard the participant:

- The EBSO has to offboard a participant, when the participant has terminated their membership.
- The EBSO has to temporarily revoke the privileges of a participant, if the credentials of the participant have been compromised.
- The EBSO has to permanently or temporarily suspend the membership of a participant or revoke their privileges, after a misconduct or a breach of the governance by the participant.

While the process to handle the first case can be planned well in advance of the termination date, the EBSO has to be able to act fast and without the collaboration of the participant in the other two cases to prevent further harm.

3.4.2 Roles

Roles of the organizations and their members participating in the Enterprise Blockchain Solution need to be properly reviewed and agreed upfront. It is important to design the proper architecture for the use case and the type of information the parties will need to share. This means also defining the way the information will be shared, the role of the parties and the level of disclosures each party in the chain will have. This is particularly critical in the cases where sensitive information is shared among the parties for achieving a certain purpose, that might be bank access data, patient sensible information or industrial know-how.

3.5 Solution ideas / components

Self-sovereign Identity (SSI) enables organisations, users and things to have a provable identity which is not bound to a central service but decentralized with the help of DLT.

3.5.1 Self-sovereign Identity as a solution

Onboarding processes and KYC requirements are commonly slow and involve a lot of back and forth communication for “offline” signatures. With SSI, an end-user has multiple Verifiable Credentials (VC) which are information provided and validated by an issuer. An end-user can be onboarded

automatically when they possess all the required and trusted VCs. The EBSO verifies the provided information and gives the end-user a membership VC. The SSI onboarding method completely automates the KYC process and skips the offline onboarding process which makes the whole procedure faster and without human interaction.

Actual centralized solutions store and collect personal data on end-users, sometimes even without their consent. SSI solves this issue by giving the responsibility of personal data back to the end-user. Every time a participant of an Enterprise Blockchain Solution needs data on an end-user, they will send a request to the end-user to be approved. It is also possible to only provide proof to some personal information instead of the whole information. For example, a participant of an Enterprise Blockchain Solution could ask an end-user if they are major and the end-user would send a proof computed from their birthdate. For participants of an Enterprise Blockchain Solution, it significantly reduces processes tied to data protection law. Users also benefit from it with more privacy and control over personal data.

Bigger Enterprise Blockchain Solutions will need different roles for their end-users as their solution grows and needs fine granulated authorization control. In SSI, roles can be represented by VCs. EBSO issues one membership VC to access the solution and will issue new VCs per role or trust VCs from other issuers to add more privileges to rightful end-users. This solution gives a fine granulated control over authorization.

Offboarding and temporary revocation are part of the IAM process and should restrict end-users to perform actions with expired authorization on a service provided by a participant of the Enterprise Blockchain Solution. In case of an incident which needs fast intervention and involves VCs from other issuers, it is possible for the EBSO to revocate the membership VC. Stripping the end-user of the membership VC disables every right that the end-user has. Revocation of the membership VC during offboarding also avoids forgetting to delete user roles.

3.5.2 Self-sovereign Identity Challenges

The first problem arises with the need of regulated issuers of contracts like insurances. One approach could be to ask a regulated member for identity proof before interacting with them. The

insurance would need to be identified by a higher instance that regulates insurances like the FINMA in Switzerland. Everyone could still issue insurance contracts as the nature of SSI is to be decentralized but only the one issued by a Finma certified insurance would be considered valid.

Decentralized systems have a fundamental trust issue. SSI being decentralized as well inherits the same problems. An SSI user has to trust that the other communication party is really the person that the initial user meant to communicate with.
This problem is not only applicable to SSI but to the internet in general. Some years ago, having a SSL certificate meant that the site was trustworthy. This is no longer the case today as anybody with access to a domain name can create a valid SSL certificate.

Currently the SSI concepts are starting to be standardized. Innovative companies have created their first products integrating SSI but they are not universally interoperable as new standards were written during their implementation phase. The next iterations will address this issue and SSI will in a few years become an attractive possibility to ease the identification and authorization process of today's application and enforce data privacy for their users.

4 Data Privacy

by Dr. Katharina Lasota Heller

The following chapter considers key tensions between blockchain technology and regulations concerning data privacy. The contribution will mainly focus on the requirements included in the GDPR[1], though it is worth mentioning that most other data protection regulations follow a similar approach, in particular in relation to the central functions of data controllers and data processors.
Public blockchains are obviously different from private blockchain. While public blockchains are generally available to any node that wishes to download the network, in private blockchains nodes must be granted access in order to participate, view transactions and deploy a consensus protocol, automatically or through identified gatekeepers.

[1] The General Data Protection Regulation (EU) 2016/679

Critics of public blockchains say that, because everyone can download a blockchain and access the history of transactions, there is only very little privacy. On the other hand, since transactions listed on a private blockchain are private, they seem to ensure a higher level of privacy than public ones. In private blockchains the issue of ownership of data also seems clearer. However, private blockchains also face many challenges from the point of view of data privacy related regulations.

4.1 Tensions between blockchain technology and data privacy

The main sources of tension between blockchain technology and data privacy include:

- the identification of data controllers and data processors
- the anonymity and pseudonymity of data
- the immutability of data
- territorial aspects

This chapter focuses on issues related to the identification of data controllers and/or data processors, and on the immutability of the data deployed into the blockchain.

To understand the tensions and related risks, it is first necessary to understand three things:

- What is private data?
- Who is generally responsible for compliance with data protection regulations?
- What is the right to be forgotten?

4.2 What is private data and how is responsible to comply with the regulation?

The GDPR defines private data very broadly as any piece of any kind of information relating to an identified or identifiable individual, for example dynamic IP addresses can be considered as private data too.

The GDPR and many other data protection regulations follow a centralistic approach, meaning that there is a central institution responsible for compliance with its regulations. These institutions are the Date Controller and Data Processor. The data controller determines the purpose of processing the data and the data processor processes the data on behalf of the data controller. The data controller and data processor are responsible for compliance with the data protection regulations.

Those central functions of data controllers and data processors contrast with the decentralized technology of blockchain and make it difficult to decide which party determines the purpose and means of processing the data. This leaves it unclear as to who is ultimately responsible for compliance with data protection regulations.

In a public blockchain there is usually no central operator, which makes it difficult to assign the traditional obligations of data controller and data processor, as each node independently processes the same transaction private data. This might lead to the conclusion that the set of nodes could be treated as joint controllers under the GDPR, which can lead to joint liability for non-compliance with its regulations.

The legal situation in the case of private blockchain is simpler. Here the central EBSO or consortium qualifies as the data controller or joint controllers, because they usually have control over the blockchain system and can determine the purpose and means of the processing of private data. Thus, they must consider the obligations under the relevant data protection regulations and apply them.

4.3 Right to be forgotten

The right to be forgotten - or the right to the erasure of data from a database - concerns the most apparent conflict between the requirements of the GDPR and blockchain technology.
The most important characteristic of a blockchain, and at the same time the most desired future of its security, is the immutability of the data stored on the blockchain, meaning that once stored, the data cannot be changed or erased. Especially not on public blockchains. However, in order to comply with the requirements of the GDPR, there must be a way for private data to be forgotten, i.e. strictly speaking erased.

As strict technical erasure requires at least (i) a reverse deconstruction of the blockchain including the targeted record, and then (ii) the reconstruction of the blockchain from the point of deleted data, the process is extremely costly in terms of time and resources.

Generally, an erasure process is easier to implement in private blockchain (with a central function of data controller and data processor) as the enforcement of stricter rules is easier to achieve than in the case of public blockchains.

Unfortunately, there is no safe approach on how to make blockchain technology fully compliant with the right to be forgotten. There are certain mitigating steps that can be taken, such as limiting the use of private data at all, using technologies which allow limitations of data to certain assets or units, considering whether blockchain technology is the right medium for the anticipated business model, adopting alternative methods of encryption and ensuring the destruction of data to protect personal data.

There are tensions between privacy regulations and blockchain technology. They are due to the fact that the current data protection regulations follow a centralized approach with clear functions of data controller and/or data processor, while blockchain technology is by its nature decentralised.
The most apparent tensions concern the central functions of data controller and data processor and the right to be forgotten.

Compliance with the requirements of data protection (i.e. the GDPR) is easier to achieve in the case of private blockchains.

5 Cryptographic Key Storage

by Natacha Linard

Blockchain is known to protect the integrity of information such as digital asset transactions. Indeed, as mentioned earlier, a public and a private key are needed to utilize your digital assets. So, the assets' safety relies on the protection of your private key. As a matter of fact, once a malicious attacker has your private key, he can authorize the transfer of the assets in and to any wallet. To prevent unauthorized transactions, validations or authentications, securing the private key is required. Several solutions are available to secure keys which can be divided into three parts:

- Software-based,

- Hardware-based, and
- a combination of both.

Any storage solution needs to overcome limitations on key management lifecycle, isolation, encryption, protection, privacy, confidentiality as well as being adapted to the evolution of blockchain crypto curves.

5.1 Software-based solutions

Software solutions may be described through the extensively used Multi-signature (Multisig) and Multi-Party Computing (MPC) solutions. Multisig is a digital signature scheme that enables a group of users to sign transactions. Before using multisig, cryptocurrencies were often stored using a single private key. If someone has obtained this private key, he has access to the wallet associated with this key. Adding Multisig increases the security as an attacker has to obtain all the keys.

More recently, MPC is a cryptographic protocol enabling a distributed computation across several different parties with no one can see the other parties' private data. In this model, the participants are protected from each other. The participants' privacy is the priority because they can't see other participants' secrets.

Gennaro and Goldfeder[2] are one of the first to propose an optimal threshold protocol for Elliptic Curve Digital Signature Algorithm (ECDSA): MPC-GG18. Key generation and signature is the threshold scheme that is done by a communication protocol between the different parties. Gennaro and Goldfeder reduced the number of signature rounds to 9. Until today, this protocol is considered as a "standard" in the industry. Around the same time, Lindell et al[3] introduced another protocol for multi-party ECDSA with one advantage: the reduction of the number of transaction rounds to 8. Doerner et al.[4] proposed a threshold ECDSA with 6 signature rounds.

[2] https://eprint.iacr.org/2019/114.pdf

[3] https://eprint.iacr.org/2018/987.pdf

[4] https://eprint.iacr.org/2018/499.pdf

Last but not least it is to be mentioned that MPC-CMP[5] has reduced the number of signature rounds to 1 which increases the speed of the algorithm to 800% compared to MPC-GG18. To increase security, an automatic refresh mechanism of the key shares has been implemented to prevent the capacity of key reuse.

MPC has more flexibility than Multisig. Indeed, Multisig are pre-set to the wallet, hence they cannot be adjusted according to the changes of the team, for example number of employees required to sign transactions.

5.2 Hardware-based solutions

A Hardware Security Module (HSM) is a tamper resistant physical security solution to manage digital keys widely used in financial services. HSMs are designed to generate key pairs, and to compute cryptographic operations such as encryption and decryption, signature and verification, hash function and more. Moreover the HSM has a secure storage to keep the key inside safe. The use of an HSM alone is vulnerable against internal attacks. If the private key is a complement stored in the HSM and a third party has access to the HSM, he will be able to sign unwanted transactions.

As an add-on the orchestration of digital asset transaction authorization process can be managed within the secure perimeter of a Hardware Security Module (HSM). The HSM may operate a specific firmware or Operating System enabling it to protect the private keys, thus ensuring signatures may only be performed within the context of the execution of a transaction – in compliance with the previously configured authorization flow. For the traditional financial sector institution expanding into blockchain or cryptocurrency — and even for several crypto-native exchanges — HSMs are the usual choice most of all for cold wallet configuration.

5.3 Software and hardware-based solutions

A mix between a software and hardware-based solution is possible, depending on the configuration of wallet temperature. We distinguish between hot and cold wallets. For example, using HSMs for cold wallets enables one to benefit from strong security principles (relying on Hardware security) while having an MPC layer for hot wallets enables one to benefit from the flexibility of software implementation.

[5] https://eprint.iacr.org/2021/060.pdf

Technology	MPC	HSM
Key	Multiple distributed key shared across different parties	One private key
Key Storage	Not physically secure, which implies an attack surface if the user does not secure his key	Key never leaves HSM
Transaction throughput	Fast	Little capacity of automation
Flexibility	Easy to destroy and to create key shared	Needs specific implementation of crypto algorithms to support new types of curves and tokens

Moreover, these different software implementations may benefit from technologies such as secure enclaves or Trust Execution Environment (TEE) that protects code execution as well as sensitive key material. The keys can't be extracted from the TEE by a hacker.

6 Digital Assets and their integrity

by Gianluca Tordi

Digital assets management and respective integrity is a critical matter nowadays. In fact in every industry most of the output of the value chain resides in the data generated by a specific process or pertaining to a specific product. From an industrial standpoint the possibility to digitize data could help speed up decision making and improve quality of product and process.

The integration of technologies such as blockchain, Internet-of-Things (IoT), Radio Frequency Identification (RFID), Cloud, cooperative robotics, could help reach the next level of automation, where processes once designed can be executed almost without the need of human intervention. Use of Machine Learning (ML) and Artificial Intelligence (AI) could help continuously optimize such processes and improve sustainability and resource usage. The same level of automation could possibly be reached in sector finance or bank sectors.

Without going too far in the future, already today all of that data generated are extremely critical assets for the organization who owns them and a loss or damage of such data could lead to huge loss, shut-downs and legal prosecution. It is therefore more and more important to define solutions and adopt technologies able to keep the pace of such shifts toward a fully digitalized world.
Data integrity is critical and mandated by regulatory authorities, for example in the pharma industry as per CFR Part 11, following the ALCOA+ principles, it is important to confirm that a certain data is Attributable, Legible, Contemporaneous, Original, Accurate, Complete, Consistent, Enduring, Available (ALCOA+).

Such principles, despite coming straight from the pharma fields, and GMP (Good Manufacturing Practice) rules should be remembered and considered when designing a solution to manage digital assets. We are in fact seeing more and more the need to protect not only the information which is born digital but also all the information that is coming from the digitalization of physical assets. Such assets might be currencies, knowledge, a piece of art, a barrel of oil or anything that has a digital representation. Blockchain Enterprise Solutions should carefully consider such aspects and help the industry to address them with focused solutions. One of such challenges is affirming the authenticity of the contents rendered both offline and online. A solution to this is the use of hashing. Hashing is an intrinsic principle of every blockchain solution. And can be used to make sure a certain document or data set has not been tampered or modified without the approval of the parties participating in the blockchain enterprise solutions.

One of the main characteristics of a blockchain is decentralization. This means data is not stored on a single location but copied on each node within the system this makes good for storing assets metadata and immutable audit trails of action and transactions among the parties, preventing third parties outside the chain to modify such status. Those characteristics of blockchain can be used to design solutions where the integrity of a certain data set can be checked and assured via the use of DLT technologies.

The above is always true for public blockchains. Private blockchain might assume different forms of data storage based on the type of network and agreements among the parties. A private blockchain

is usually designed to meet the requirements of a pool of entities or at least two entities that need to exchange information or assets in a secure way, under rules and agreements which are defined among them. In a private blockchain which might include less nodes and rules need to be defined and agreed among the parties how exchanges of information or assets are getting processed and logged on the network. Such rules must be decided together in the network and trust each other. Nevertheless, there might always be within a network a node which acts as safeguards for the immutability and safety of the whole network.

Usually, a private blockchain network will contain nodes, a notary and a Trust Root, which can be operated in-house or outsourced to a third party. All nodes in the network are identified by, and transact using, a certificate issued by an appointed Certificate Authority. The Trust Root is the single, long-term cryptographic key which all network certificates root back to and is the basis of trust in the provenance of data, recognized by participants. A notary prevents "double-spends" by attesting that for any given transaction, it has not already signed other transactions that consume the proposed transaction's input states (in other words: if the state in a transaction has been previously spent). Moreover, the networks might also contain an Identity Manager (which can grant and revoke participation certificates, to nodes – based on the Trust Root) and a Network Map (which lists the identities of nodes in the network and maintains the network parameters list and makes this information available to all nodes). We have therefore briefly covered the main ways how entities are identified and recognized when participating in a private blockchain. But what happens when such entities transact digital assets on the constituted network. A digital asset is anything that can be stored and transmitted electronically (using a computer) that can be owned and thus, can have ownership and usage rights associated with it.

The problem of supporting transactions of digital assets can be reduced to the problem of tracking which account is the owner of a particular asset at a given point in time, and to register when the ownership of an asset changes. With these basic operations, one can compute how many assets a person or organisation has and avoid double spending and false claim attacks. The pattern is the same independently of the type of asset, whether it represents the ownership of a real-world object, or a more ethereal value like reputation or credit.

As such, digital assets and their transaction rules in the context of blockchains are defined during *token modelling* (also known as *token design,* or *"tokenomics"*). A *token definition* establishes the digital asset being exchanged, the admissible operations that can be executed (and therefore, need to be validated) on it, and often implicitly, the rights associated with holding it. We add to this also the concept of fungibility. A token is fungible if its individual units are essentially interchangeable, and each of its parts is indistinguishable from another part. A non-fungible token represents a unique entity (or ownership of a unique physical world item), their main goal is to create verifiable digital scarcity. Such Token cannot be divided or combined. Token can only belong to a physical address - to an account - either user's wallet or another smart contract; each token can thus have one (and only one) owner.

Assets like gold, real estate, fine art, or carbon credits are more difficult to transfer, often obligating buyers and sellers to contend with mountains of paperwork and lengthy procedures. By representing physical assets as digital tokens on a distributed digital ledger or blockchain, it's possible to unlock the value of real-world assets and to exchange them in real time[6]. Digitization of assets or also tokenization is a process in which the rights to an asset are converted into a digital token on a blockchain. Ownership rights are transmitted and traded on a digital platform, and the real-world assets on the blockchain are represented by digital tokens. It became then important to define appropriate solutions to link the physical or digital assets to their current owner. This process can include different steps which might still require some burdens especially as physical entities are not native digital assets that can be easily associated with their digital representative, this might involve paperwork and verification steps and the process of conversion might be linked to local regulatory rules.

In case of native digital assets instead the process might be easier as the digital goods (eg. arts, tickets, course, etc..) can be generated already to be then transferred as a token. Few platforms offer right now such service and related safe trade of digital goods and more will be available as the economy is moving toward a more tokenized environment

[6] https://www.ibm.com/thought-leadership/institute-business-value/report/tokenassets

7 Interoperability

by Blanca Anggela Zutta

A key success driver of an Enterprise Blockchain Solution is its interoperability. Interoperability facilitates people to transact, share, access, and see information across various blockchain networks and between blockchains and other emerging and legacy technologies without the need of intermediaries. Since 2015, there has been a growing interest in "Blockchain Interoperability", where the number of research documents will reach more than 200 research papers this year.[7]

7.1 Challenges

The promise of Enterprise Blockchain is to respond to the increasing demand of direct interactions and collaborations between enterprises. However most blockchain networks operate in isolation and they are designed to respond to specific needs. The biggest challenges to blockchain interoperability result from heterogeneity, a diversity of blockchain systems speaking different coding languages, with increasing amounts of data transferred, and process silos. Most businesses operate different types of blockchain networks with different architecture, protocols, governance, regulatory controls, and databases. This leads to increasing integration complexity[8] and further fragmentation. Moreover, the lack of standards resulting from technology differences between blockchains, and a weak network of nodes make blockchains more susceptible to cyberattacks.

7.2 Advantages of Interoperability

The lack of interoperability and the limited scaling are significant barriers for businesses looking to build Enterprise Blockchain Solutions. Organizations want to build flexible and scalable solutions that can grow with them and open options for external collaboration. They look for ways to adapt to market changes and swap to other solutions if required. Solving the interoperability problem will build trust of enterprises and investors in blockchain and distributed ledger technology, boost its adoption in the business space significantly.

[7] Source: Google scholar in November 2021;

[8] The number of integrations required to connect several ledgers grows quadratically with the number of ledgers. If we connect 10 ledgers we expect 50 integration scenarios. This number grows quickly to more than 5000 integration scenarios for 100 ledgers.

For example, Interoperability could ensure the integrity of information exchange, the transfer of value between chains and reduce the costs associated with KYC between blockchains, but it would require a more straightforward execution of smart contracts, new governance models, messaging standards between those networks, and an excellent user experience. Furthermore, interoperability could foster data privacy by allowing enterprises to use sidechain approaches with different privacy requirements resulting in reduced risks.

7.3 Architecture of Interoperability

At the application layer, the interest has been more on technical and semantic aspects of interoperability and less on organizational, legal, and interoperability governance aspects. Several organizations are currently working on standards to drive the interoperability of business model on blockchains, such as the Blockchain Industrial Alliance (BIA), The British Standards Institution (BSI), the Subgroup on Blockchain Governance and Interoperability IEEE P2145[9], the ISO Technical Committee 307 (ISO/TC/SG7)[10], the IETF via the IETF Open digital asset protocol (ODAP)[11], just to name a few.

The Blockchain Interoperability Working Group, for example, elaborates in partnership with the IMF's Digital Advisory Unit recommendations[12] from a business, technology, security, risk and legal perspective. They include for example:

- Recommendations how to address and solve interoperability challenges through a governance group.
- Explorations on the value exchange and information exchange usability between blockchain platforms technically and semantically.
- Security and risk recommendations on the identity, cryptography, level of decentralization, and semantic layers.
- Considerations how to establish a purpose for a blockchain application and the jurisdictions involved and supervising the solution.

[9] https://sagroups.ieee.org/ieee2145/home/p2145-subgroup-on-governance-and-interoperability/

[10] ISO/TC 307 Blockchain and distributed ledger technologies — Vocabulary

[11] https://www.ietf.org/archive/id/draft-hargreaves-odap-01.txt

[12] https://documents1.worldbank.org/curated/en/373781615365676101/pdf/Blockchain-Interoperability.pdf

The standard IEEE 2418.2-2020[13] establishes requirements on data formats for blockchain systems and addresses data structures, data types, and data elements. Other IEEE standards initiatives under development are:

- P3203 - Standard for Blockchain Interoperability Naming Protocol,
- P3204 - Standard for Blockchain Interoperability - Cross Chain Transaction Consistency Protocol,
- P3205 - Standard for Blockchain Interoperability - Data Authentication and Communication Protocol.

At the network layer, most attention has been on cross-chain communication mechanisms[14], raising security issues related to IP address identification, verification of transactions at the consensus layer, and a lack of standards in programming languages used for smart contracts and diverse environments where these contracts operate.

7.4 Blockchain interoperability use cases

There are a variety of scenarios where interoperability can operate, such as:

- Asset swap across networks,
- Asset migration between networks using the same or different technology,
- Querying data from another ledger, or
- Invoking another ledger.

The World Economic Forum designed an interoperability framework[15] addressing the challenges mentioned above at the business, platform and infrastructure level and categorizing interoperability in three groups:

1. Cross-authentication, enabling both parties to cryptographically authenticate transactions without intermediaries,

[13] https://www.en-standard.eu/ieee-2418-2-2020-ieee-standard-for-data-format-for-blockchain-systems-2

[14] https://www.semanticscholar.org/paper/Towards-a-Novel-Architecture-for-Enabling-amongst-Jin-Dai/020bcf6a5808ef3c82f5738c881d542e2cc3b809

[15] https://www3.weforum.org/docs/WEF_A_Framework_for_Blockchain_Interoperability_2020.pdf

2. Oracles, enabling the transfer or external data and requiring trust as the oracle could be a centralized or decentralized solution, and
3. API gateways, requiring each network separately to implement their connector.

Recent studies by Rafael Belchior[16] moves a step further. He designed a Blockchain Interoperability Framework where blockchain use cases are classified into three families:

- Public connectors (PC) - Aiming to provide interoperability between cryptocurrency systems. Focus on exchange instead of a real transfer of assets.
- Blockchain of Blockchains (BoB) - Designed for interoperable blockchains dApps. Not always compatible with legacy systems, network versions, or private networks.
- Hybrid connectors (HC) - Designed to connect public and private networks.

For each one of these categories, there are several techniques used for achieving interoperability:

	Sub-categories	**Blockchain use cases**
Public connectors	Side chains and relays: where the responsibility of the interoperability is delegated to the side chain and not handled on the main chain. Notary schemes: where the notaries are the trusted parties helping participants on one blockchain confirm transactions of another blockchain. Hash time hashlocks (HLTC): requiring a smart contract that is limited in time to do cross-chain atomic operations.	BitXhub-PI Chainlink (Centralised and decentralised exchanges)
Blockchain of Blockchains	This framework provides reusable data, network, contract, or even consensus algorithms that can be used to create new blockchains from scratch, and since different blockchain networks use the same pattern, they can easily interoperate.	Cosmos (uses Tendermint, a consensus algorithm, which is a cross-chain network supporting heterogeneous blockchains) Polkadot (uses a relay chain to connect multiple sidechains (parachains), each parachain being a blockchain)

[16] A Survey on Blockchain Interoperability: Past, Present, and Future Trends ; Rafael Belchior, André Vasconcelos, Sérgio Guerreiro, Miguel Correia, 2021

Hybrid connectors	Blockchain migrators: enable cross-blockchains status migration (data+smart contracts). Agnostic protocols: allows an arbitrary DLT to interoperate with other DLTs and legacy systems via a blockchain abstraction layer. Trusted relays or trusted parties: redirect transactions from one blockchain to another.	Hyperledger Cactus[17] (only data).

7.5 Application layer adaptors

The emergence of new platforms, protocols, and cross-chain programming languages allow integration with public and private ledgers at the application layer. For example, Digital Asset Modelling Language (DAML) based applications use agnostic smart contracts to connect with Corda, Fabric, Sawtooth and other networks. Vottun uses APIs mapped to specific smart contracts to connect with Fabric, Alastria, Quorum, and Ethereum.

As earlier mentioned, Polkadot follows the concept of relay chains and explores bridges to connect with Bitcoin, Ethereum and Tendermint. Hyperledger Cactus already supports Hyperledger Fabric, Besu, Quorum, XDai, and Corda, and some smart contract connectors are being built for Polkadot, Iroha, Sawtooth, etc. The Overledger platform supports Hyperledger Fabric, Corda, Ethere-um, Bitcoin, IOTA, EOS, and Ripple. LiquidApps Java and JavaScript SDKs support EOS, Ethereum, Telos, and other blockchain networks.

Furthermore, new approaches like data views are also being tested to take customized snapshots of a blockchain (Blockchain views[18]) that can be further merged, compared, processed, migrated, audited, and analyzed. In addition, an open-source Publication Subscriber architecture[19] to promote

[17] https://github.com/hyperledger/cactus/blob/master/docs/whitepaper/whitepaper.md

[18] https://www.researchgate.net/publication/346474260_A_Survey_on_Business_Process_View_Integration

[19] https://arxiv.org/abs/2101.12331

blockchain interoperability is also being tested by Telus and is open to anyone interested in adding different blockchains to their network to test their data querying functionality.

7.6 Interoperability is a key success factor

Blockchain interoperability is an important research area raising increasing interest. Still, the growing number of multiple new alternatives, and legacy solutions, could result in further fragmentation if the issues around interoperability are not addressed through a coordinated approach between international organizations, the public, academia, and the private sector. Also, interoperability is based on the assumption of trust between the networks that are interoperating, so there is a need for accountability mechanisms to set the right boundaries, keep track of nodes' actions, and enforce the right behavior in the protocol to make it more secure.

Future work on interoperability could provide the exposure Blockchain needs to integrate standards, new ways of working, hence stimulating greater interoperability. Standards could help increase competition, innovation, autonomy, and flexibility of choice, facilitating adoption by establishing benchmarks aligned to global trade and social policies. Initiatives like the Open cybersecurity Alliance (OCA) or the Accountable Digital Identity Association (ADI Association)[20] could bring to the same table interested stakeholders in the Distributed Ledger Technology arena to develop formats and standardized models to classify threats and help bring trust in this industry.

The business sector could prioritize projects contributing to interoperability and be a catalyst of innovation. Likewise, the academic sector could incentivize research on private/public blockchain interoperability, interoperability standards, identity portability, blockchain migration, and Blockchain of Blockchain approach. Hence, it is up to all stakeholders, including end-users, to promote interoperability and contribute to building a more sustainable, integrated, and effective ecosystem.

[20] https://adiassociation.org

8 Decentralized governance

by Dennis Flad

Historically, enterprise solutions arose from an internal workflow situation. The software solutions helped to better organize operational processes between departments and to distribute important and process-critical data within the company in a value-creating manner. With the growth of bandwidth and digitization, enterprise solutions increasingly found their way into optimizing processes between different legal entities. Central providers often entered the market, developing standards as hubs, platforms, marketplaces, or clearing houses and making multi-entity-wide processes more efficient and effective. These central data hubs have considerable advantages. They allow very efficient workflows, consistent data quality and simple usability. But they have one important weakness: the data is or flows through one central point. This makes the data particularly vulnerable to risks of failure and cyber-crime. Erroneous central IT components can hinder or prevent the stable operations of an entire multi-entity enterprise solution. And there is the risk of internal and external manipulation or fraud. Potential attacks need only succeed at one point-of-access to cause massive damage.

Here, blockchain and distributed ledger technology can help to better control these data risks of enterprise solutions. Data is stored redundantly at multiple nods, reducing the risk of tampering and failure. Also, classic ransom attacks where hackers are blocking data access and releasing it only against payment again are not possible for data stored on blockchains or distributed ledgers. However, switching to an enterprise blockchain solution also contains new risks.

8.1 Counterparty risk in blockchains

The foremost is the so-called counterparty risk. In an enterprise blockchain solution the transfers of information, goods, services, or rights are completed and tracked on a blockchain or in the distributed ledger. Often it requires a settlement of the transfer in the real world to complete the use case. Shipping containers, barrels of oil, or certified luxury watches usually only change hands in exchange for a promise to pay. Enterprise blockchain solutions are mostly classic receive-against-payment or delivery-versus-payment use cases conducted by smart contracts. And that is where

the key essence of the counterparty risk is hidden: The real exchange of goods, services and fiat currencies of an on-chain deal often still happens off-chain. Any enterprise blockchain solution therefore needs clear governance that monitors and regulates the rights and obligations of the network participants.

Critical minds may now say that there is no need for governance with a blockchain because it is a trustless network. In certain business cases, such as the transfer of digital assets, this may seem to be a justified statement. However, one may recall the DAO incident of 2016 on the Ethereum blockchain. Clever programmers had discovered a security leak in the DAO code, changed the code and stolen Ether from the solution. At that time, the community had decided to do a hard fork and restore the situation before the theft. This was an act of governance. The community took corrective action to undo the crime.

8.2 The What and the How in Governance

Enterprise blockchain solutions in particular need governance to ensure cyber security and ensure integrity between the on- and off-chain worlds. Here, we should distinguish between different levels of governance - the What - as well as different models of governance - the How. When asking what belongs under governance, there are three layers:

- the blockchain layer
- the token and smart contract layer
- the business rules layer

The blockchain layer is basically about deciding which type of blockchain to use for which business model. Does a private blockchain make sense? Or rather a public blockchain? Or is a distributed ledger model better after all? Depending on the technology and blockchain choice, we already acknowledge a basic set of governance rules. Such as for example how and by whom a transfer of assets, rights or information is validated on the chain and under which compensation model for the validators. The situation is similar at the token and smart contracts level. Here too, we decide and accept certain technical standards which can significantly influence the business model behind an enterprise blockchain solution. The final governance layer are the business rules. This layer includes all the rights, obligations, and responsibilities around the interaction of business partners on an

enterprise blockchain solution. The business rules determine the workflows and business processes to be followed. This includes, for example, the rules about the tokenization of assets, rights, or information or certification of such tokens by external auditors or quality assessment companies. Or rules on how to settle deals on-chain and off-chain.

The question of the How is equally important to the What in the governance of enterprise blockchain solutions. How are decisions made regarding the various technical standards and business rules? There are various models possible. In the classic model, the technical provider of an enterprise blockchain solution takes over the governance role and defines the rules. Or a group of developers do that like in the Bitcoin network in the beginning. In the most common cases, it is a consortium of users of the enterprise blockchain solution who govern the technological standards, the business rules, and the participant onboarding policies. In such consortiums, especially in the early stage, the main participants of the enterprise solution usually balance each other. Rules are defined by consensus, just as development costs are usually shared. This allows the enterprise solution to evolve quickly from a conceptual stage into a live production. However, after the first successes of gaining additional members, things are getting complicated in consortiums. With the increasing number of participants, the diversity of objectives, needs and requirements increase too. Then it is usually advisable to change the governance model and to establish a democratic governance, where standards, rules and obligations get determined by the majority of members. Enterprise blockchain solutions are decentralized networks and are as such comparable to federal states. Each participating enterprise is like a county, state, or canton in the federal structure. In each federation there are members with stronger economic power and such with less power, but the government and the people have often found rules and procedures to give every member a voice and to equal the voting.

Like in successful democracies, the governance of policies, strategies and legal frameworks must come from the bottom, from the (co-)members of the system. Autocratic or top-down approaches often struggle with the acceptance by all participants, but to reach critical mass and to become a successful solution requires that all participants are committed to an industry-wide adoption. It is wise to think of governance measures which allow a broad evaluation and sounding of proposals and equally balance the decision-making process. The right to submit initiative belongs to such basic

democratic constructs as well as the right of a fair hearing or escalation to an arbitration board if a new right or obligation leads to disputes among the network members.

Finding the right governance model for the technical layers and the business rules of an enterprise blockchain solution needs to evolve with the growth of acceptance and adoption. Unilateral or consortium structures are very efficient and effective during the start phase but swap to the contrary later. Perhaps one of the plenty of interesting decentralized voting systems based on blockchain or distributed ledger technology can help to support the right federal consensus building successful enterprise blockchain solution. It is worth looking at them.

Building the World's Leading
Blockchain Ecosystem
www.cryptovalley.swiss