Crypto Valley

Privacy Techniques for Blockchains and DLTs

Published by CVA's Cybersecurity Working Group

✉ cybersecurity@cryptovalley.swiss

www.cryptovalley.swiss

@thecryptovalley

Contributors

Jean-Philippe Aumasson

Christine McAteer

Ognjen Maric

Markus Perdrizat

Table of Contents

Summary

The Crypto Valley Association presents this **primer document on privacy for blockchains and DLTs**. The main takeaways and recommendations are:

- **The use of a privacy coin is usually insufficient to ensure privacy**, as these are just one piece of the puzzle. A strategy should be established and implemented to ensure adequate privacy controls at different levels and with respect to different notions (such as unlinkability of addresses and confidentiality of personally identifiable information).
- **Recognize the limitations of privacy mechanisms.** Reliable platforms that effectively hide transaction information today may be subject to attacks that could reveal all or part of the transactions' information, often resulting from poor operational security practices. Future technological developments may also enable the compromise of current state-of-the-art privacy mechanisms.
- **Understand the regulatory frameworks** and whether an asset or service has obtained applicable domestic or foreign authorisations. The use of an unregulated service may increase the risk of service disruption, theft or loss of funds. Services should have appropriate governance and transaction transparency.
- **Leverage off-chain privacy controls** to protect the confidentiality of personal data, of the governance model, of wallets' structure, or of your IT infrastructure.
- **Understand how confidential business and personal data will be treated**, as the use of privacy techniques may not be fully mature and may harm internal system transparency, scalability and other important data security considerations.

1 / Introduction

Privacy is a human right as recognized by the United Nations Declaration of Human Rights (UDHR) and is essential to consumer protection and to the adoption of decentralized payment methods. Yet, privacy coins such as Zcash have had a tumultuous road to adoption, at times being delisted from exchanges and branded as high risk by regulators and investors, only to later be actively promoted by licensed services in highly regulated jurisdictions. At the same time, privacy mechanisms that hide IP addresses or a cryptocurrency's transaction history have been exploited by illicit actors to facilitate the sale of illicit goods, human trafficking, weapons proliferation and other criminal activities.

There are many considerations related to the use of privacy-enhancing mechanisms in the context of cryptocurrencies, blockchains and Distributed Ledger Technologies (DLTs). Prior to the adoption of a given token or mechanism to ensure customer privacy, or conversely, prior to the delisting or classification of a wallet or token as high-risk for money laundering, it is critical to understand the basic functionality of each mechanisms in order to determine if they can support competing needs in terms of security and compliance with regulatory requirements. Simply put, a technology that enhances privacy may also enable regulatory compliance. The two may not be mutually exclusive.

With that in mind, the CVA Cybersecurity Working Group has assembled a team of experts to shed light on some of the most relevant topics related to blockchain & privacy by describing the various mechanisms and the main challenges and solutions to address them.

This primer is for security experts, solution architects, lawyers, compliance advisors and executives who currently, or plan to manage digital assets or digitize part of the value chain with permissioned distributed ledger technology.

This report is not only about privacy coins and anonymous transactions. As far as blockchain operations and usage are concerned, the concept of privacy applies to many more elements than just transaction data. We thus cover these challenges, focusing on the technical aspects (e.g. recent developments in zero-knowledge proofs), and covering some operational and legal aspects. We describe some of the main mechanisms adopted in practice to enhance privacy, commenting on their value, as well as their associated risks and maturity level. Many of these mechanisms are arguably in their infancy stage. We can expect further developments as research in cryptography and privacy-preserving protocols evolves.

In the following,

- Section 2 reviews what's at stake, in terms of data protection and regulatory oversight, and describes what privacy means in the context of blockchain.
- Section 3 presents selected privacy mechanisms related to blockchain technology and its use, from a technological perspective.
- Section 4 discusses the example of privacy features in Monero and Zcash, and includes a Q&A with Zcash's VP of Growth.
- Section 5 discusses examples of privacy features in enterprise ledgers.
- Section 6 concludes with some recommendations.

2 / Privacy: A Multifaceted Notion

2.1 Data Protection vs. Transparency

Financial privacy is essential to enabling each person's right to freedom of movement, expression and association. Enterprises equally rely on privacy to protect their customers and competitive business information.

At the same time, efforts to combat fraud, ransoms, extortion, as well as the trafficking of individuals, wildlife and arms, have greatly benefited from the combined efforts of financial institutions and other obliged entities to bring greater transparency to financial transactions by identifying and reporting assets that derive from, or may be used to support such crimes. Steps taken by financial intermediaries, be they professional exchanges, money transfer services, traders of precious gems or custodial cryptocurrency wallet providers, to prevent the integration of criminal assets into the financial system or economy benefits society at large.

Given the advanced capabilities of blockchain analytics services to attribute identities to public blockchain addresses, it is critical to understand whether such personally identifiable information (PII) can and should be protected by means of privacy mechanisms, allowing the industry to move towards greater retail and institutional adoption. Whether these same mechanisms should be accepted by regulated entities, or how their risks might be evaluated may depend on the mechanisms' ability to provide transparency to government officials, law enforcement and financial intermediaries in support of tax or regulatory compliance.

As no two privacy mechanisms are alike, gaining a basic understanding of each service or privacy coin may allow financial intermediaries to better gauge the risk that each represents, as well as determine whether AML/CTF and tax compliance can be supported in parallel with its use.

Globally, approaches towards privacy mechanisms have been met with general skepticism. Several exchanges have cut support for privacy coins in the last years in order to comply with national requirements. However certain jurisdictions have begun taking a cautionary permissive approach by allowing regulated exchanges to list certain privacy coins and support privacy-shielded transactions, where details of such transactions are discoverable in the event of an audit or inquiry.

2.2 The Definitions of Privacy

In the context of blockchain, privacy is often ultimately about keeping certain information secret to non-authorized parties (such as blockchain nodes), and more generally to the public in the case of public blockchains. But this idea of secrecy can take several forms, for it can concern both actual pieces of data as well as operational patterns (activity's nature, time, "social graph", and so on). We consider the following concepts, on which will elaborate in the remainder of this report:

- Confidentiality, or the inability for a passive or active attacker to learn any bit of a given piece of information. For example, if an individual's name is encrypted and stored in a blockchain, the name will remain secret. However, even if a piece of data is encrypted, its context and metadata (time, origin, length, etc.) can reveal key information.
- Anonymity, or the confidentiality of a party's long-term identity (name or personally identifiable information for an individual, equivalent information for an organization). The related notion of pseudonymity covers specifically identifiers that are not official identifiers, but instead ad hoc or application-specific ones (such as an account number).

- Untraceability, or the inability to trace the provenance of funds, for example by tracking Bitcoin's UTXO. This notion of untraceable payments generalizes to untraceable assets managed via smart contracts, in addition to native cryptocurrencies and tokens.
- Unlinkability, or the inability to link distinct transactions involving a same account (as sender, recipient, or other role), and more as having a same confidential attribute in common. In one of its forms, unlinkability includes the inability to link transactions to a given wallet, account or public key. Note that unlinkability does not necessarily imply untraceability.
- Deniability, or plausible deniability, refers to the property that a party cannot be irrevocably held responsible for some operation. Typically, non-deniability is guaranteed through digital signatures for a party identified by their public key, thanks to the non-repudiation property (also referred to as technical power of disposal).

3 / Selected Privacy Mechanisms

We review some of the main privacy mechanisms used in blockchain and DLT applications.

3.1 Blockchain Privacy Features

These mechanisms are inherent, and defined by a blockchain platform.

3.1.1 Privacy Coins

So-called *privacy coins* aim to keep all the blockchain's content (that is, the transactions) public and provide the same security guarantees offered by Bitcoin or Ethereum regarding transactions immutability and double spending, however do so without revealing:

- The sender's identity, address, or other unique identifier
- The recipient's identity, address, or other unique identifier
- The amount transferred

Furthermore, the transactions database as a whole should not be exploitable to reveal such information. It should also be impossible for malicious parties (such as senders or validators) to abuse the protocol in order to reveal hidden information. Untraceability and unlikability are additional common goals of privacy coins.

From a purely technical perspective, privacy coins are at the origins of some of the most fascinating and impactful cryptography research in the latest years, mainly as related to *zero-knowledge proofs*. These are cryptographic protocols that prove that a mathematical statement is true without revealing its details and results. Concretely, researchers created non-interactive and efficient techniques for such proofs to be integrated in blockchain protocols to prove the soundness of transactions, without revealing the sender, recipient, and amount.

zk-SNARKS are such types of proofs pioneered by Zcash, which work by transforming an application-level statement (such as Alice is sending N ZEC coins to Bob) into an arithmetic circuit, which is in turn is converted to an equation from which the proof is derived using a private key. A major benefit of SNARKs is that their size is fixed (3 group elements), achievable thanks to techniques introduced in 2016, and using elliptic curve pairings[1]. The more recent zk-STARKS are a more recent type of proof with different properties.

[1] https://eprint.iacr.org/2016/260.

Zero-knowledge proofs find broader applications, as illustrated for example by the StarkWare project[2] or by Filecoin's "proofs of spacetime". A specific type of zero-knowledge proof is the *range proofs*, which prove that a number lies in a certain range. The Bulletproof range proof protocol[3] was created to address blockchains' needs in terms of efficiency and proof size, and is now used in Monero.

A flipside of privacy coins' innovative mechanism is their complexity, making bugs and security shortcomings (either in protocols or in their implementations) harder to find.

To address compliance needs, certain privacy coins integrate a mechanism to reveal the details of an otherwise obscured transaction, if one has a special type of key. This feature has been exploited by regulated exchanges such as Gemini, in order to allow customers to shield their transactions from public scrutiny, while allowing anti-money laundering due diligence to be conducted for each transaction.

There are other approaches than those of Zcash and Monero. One is based on the MimbleWimble technique[4], as adopted by BEAM and Grin. Another is the *PrivateSend* optional feature of the Dash cryptocurrency, which essentially acts as a Bitcoin UTXO mixing. However, these approach are fundamentally less powerful and reliable than those of the aforementioned protocols

3.1.2 State Partitioning

This approach replaces a global, publicly visible shared database (e.g., a public blockchain) by a number of state partitions that are only visible to a subset of the parties involved in the system. Arranging the partitions such that all parties who see a partition are exactly privy to the data in that partition (including regulators, for example) then ensures privacy.

While partitioning can provide privacy without expensive cryptographic mechanisms, it also brings its own challenges. First, as partitions limit visibility, the system must allow cross-partition operations if it's to serve as a single source of truth. Second, as the data in a partition is only visible to a subset of participants, the liveness of cross-partition operations usually depends on the availability of that subset of participants. Finally, partitions make it difficult to ensure global properties such as a constant money supply, which makes it challenging to implement an "issuer-free" fully decentralized currency on top of a partitioned system.

3.2 Off-Chain Techniques

The following section describes technical mechanisms that are either only indirectly connected to the main ledger, or not connected at all.

3.2.1 Tumblers, Mixers and CoinJoins

Tumblers and mixers are commonly interchanged terms referring to services that use smart contracts to redistribute assets belonging to many people in order to both hide the identity of the original owner and change an asset's transaction history. Concretely, as bitcoin is non-fungible (i.e. the transaction history can be traced and often attributed to a beneficial owner), Alice's transaction history becomes obfuscated when her assets are sent to a mixing service and she receives the same amount (less a fee) at an address she selected and controls from the mixer's own or other incoming funds.

In using such services, Alice must rely on a 3rd party or centralized platform that can steal, lose or misappropriate her assets. She may also unknowingly receive in return "tainted" assets that were previously associated with illicit activities.

[2] https://starkware.co.

[3] https://crypto.stanford.edu/bulletproofs/.

[4] https://scalingbitcoin.org/papers/mimblewimble.pdf.

Risks associated with dishonest 3rd parties are often overcome when individuals meet on billboard-style platforms or dedicated peer-to-peer mixing services that use dapps to manage the mixing conditions and execute a mix (known as a CoinJoin). Here again, trust must be placed in the dapp protocol or smart contract executing the agreed conditions.

As most mixers or tumblers control the flow of funds that are sent to their platforms, the transfer or exchange of assets is seen in many jurisdictions as a form of financial intermediation, an activity subject to authorisation and AML/CTF supervision. Unlicensed services can expect an increase in enforcement activities in the years to come, following in the footsteps of the U.S. Department of Justice, which recently imposed a $60 million civil money penalty to the primary operator of Helix and Coin Ninja mixing services.

3.2.2 Encryption and Hashing

Encryption and hashing can both be used to selectively "redact" privacy-sensitive data from a blockchain. In the blockchain, the (sensitive) data is replaced by a random-looking bitstring derived from the original data. In case of encryption, the random-looking bitstring is derived from the data using an encryption key; the sensitive data can be recovered only by the holders of the corresponding decryption key. In case of hashing, the random-looking bitstring is derived just from the data, but data can in general not be recovered from the bitstring (hashing is a "one-way" function). Both encryption and hashing protect the sensitive data from unauthorized parties, as they only see a random-looking bitstring. Yet the blockchain can be still used as the shared source of truth, as the data can be shared with parties privy to the data, including regulators: by revealing either the decryption key (in case of encryption), or the data itself (in case of hashing)[5].

While encryption and hashing are among the most mature cryptographic techniques, these approaches also bring several challenges. First, the redacted data cannot be checked for integrity by the other blockchain participants without additional mechanisms. These can be based on software methods such as zero-knowledge proofs or homomorphic encryption, or based on secure hardware enclaves, such as Intel's SGX. Both have some drawbacks: software methods are usually computationally expensive, and the last few years have brought many successful attacks on secure enclaves. Second, the blockchain on its own may lose transparency and no longer guarantee or prove that the privy parties really have access to the sensitive data. Third, encryption and hashing on their own might be insufficient to ensure compliance with GDPR and similar regulations; hashes may need to be "peppered" to combine the data with some secret randomness to ensure unlinkability with the data, and the status of encryption is not clear. Fourth, access patterns may still be revealed if the changes to the hashed/encrypted data are publicly visible. Finally, future proofing may be a concern when using encryption; the loss of private keys or advances in quantum computing may render encrypted data visible to unauthorized parties in the future.

3.2.3 Quorum Transaction Signing

Whereas (on-chain) multisignatures may be natively supported by many blockchain platforms, starting with Bitcoin, off-chain mechanisms provide more privacy by hiding the set of possible signers and which persons or systems actually contributed to the signature.

Indeed, off-chain quorum signing, as performed with multi-party computation and threshold signature protocols, enable a set of parties to collectively issue a signature (of a transaction) such that none of the parties has full access to the private key. Instead, the private key is split in shares, and a protocol is run to combine these shares to compute a valid signature. Threshold signature protocols can be configured to support arbitrary t-of-n quorums, whereby at least t+1 participants are required to create a signature.

Such methods are typically used to implement shared control of an account between multiple organizations, or between multiple units or systems within a given organization.

[5] If hashing is done via a hash tree (a.k.a. Merkle tree), one would need to reveal the tree authentication path (a.k.a. proof of membership) in addition to the data itself.

3.3 Operational Privacy Methods

Wallets are the primary means for users to interact with public blockchains. As such, many off-chain privacy techniques have been embedded in crypto wallets. Nevertheless, these techniques can also be embedded in other solutions and services operated by crypto service providers.

3.3.1 Funds Pooling Models

Blockchain custody and transaction service providers may mingle funds of several different clients onto a common address or set of addresses, and manage an off-chain register of ownership. This has the added benefit of obfuscating ownership and transactions. However, clients of the service provider need to give up control over their crypto assets and trust the proper operations of the service provider. Consequently, regulators world-wide typically insist on specific accounting rules and security measures to prevent loss of user funds due to fraud and bankruptcy.

One of the main privacy challenges is that in-flow and out-flow are transparent on the blockchain, and the pooling measures can be reversed using sufficiently advanced data analytics. The strength of this established pattern is in its operational convenience for crypto service providers offering custody of digital assets, and not specifically in achieving strong privacy objectives. This is a frequent differentiating factor to the privacy techniques discussed in 3.2.1 Tumblers, Mixers and CoinJoins.

3.3.2 Avoiding Address Reuse

Since transactions are visible to all by default on public blockchains, it is recommended to not associate all personal and business transactions with the same address, and instead to compartmentalize address usage (i.e. set-up independent addresses). On account based blockchains such as Ethereum, this means using different addresses for different types of transactions. On UTXO based blockchains such as Bitcoin, most wallets support this behavior automatically.

Avoiding address reuse through compartmentalization of addresses improves the privacy resilience against blockchain analytics. On the other hand, from a regulatory perspective, the FATF travel rule expects that every address is associated with a known party, and avoiding address reuse will increase the compliance workload. Additionally, avoiding address reuse requires strict operational procedures to avoid accidentally disclosing relationships between addresses that can be identified using transaction analytics.

The principles of address reuse avoidance and compartmentalization are well understood and belong to the “Blockchain 101”. However, we would argue that support in mainstream wallets can be improved, to simplify following this best practice for beginners and advanced users and institutions alike.

3.3.3 Coin Control

On UTXO chains such as Bitcoin, over time the wallet will have multiple addresses with different amounts of crypto assets due to the avoidance of address reuse (see above). These addresses are often mapped together using analytics of on-chain transactions, allowing address risk-rating services to cluster addresses together and attribute them to the same individual or entity.

Understanding that transactions which pull assets together from various addresses may inadvertently provide attribution information to all associated wallets, a technique often referred to as “coin control” is about avoiding to select funds from multiple different wallet addresses that are not already associated with each other based on past transactions.

Wallets with Coin Control support enable users to pick the sending address. Advanced support for Coin Control prevents users from combining multiple addresses in a sending transaction if the addresses are not already connected from past transactions.

Coin control’s primary benefit is that it improves the privacy resilience against blockchain analytics. And it does so with no direct negative impact to regulatory requirements.

However, strict operational procedures are required to avoid accidentally disclosing relationships between addresses that can be identified using transaction analytics. And although the coin control principles are mature and well understood, support in mainstream wallets is frequently lacking entirely.

3.3.4 Mining Pools

Understanding the lifecycle of a typical cryptocurrency or token transaction puts into context the role of blockchain mining. As a reminder, once a blockchain-based transaction is initiated, it is placed in a memory pool ("mempool") of unconfirmed transactions until a miner (a computer in the network) selects it for validation, after which it is propagated to the network and added to the block of transactions (the blockchain).

Cryptocurrency mining can be broken down into three distinct segments: (a) proprietary mining, where miners operate on their own hardware for their gains; (b) remote hosting, where data centres are used to provide mining services to customers (e.g. operating and maintaining hardware owned or rented by customers); and (c) cloud mining, where customers rent out their own computational power for use by a third party.

Many involved in cryptocurrency mining also join mining pools - groups of miners who collectively use their computational resources to mine new coins and share rewards between participants, according to their respective contributions. As mining pool operators generally do not restrict membership or require only basic registration information, mempools tend to attract criminal miners, especially where no verification of identity or source of funds is conducted.

While mining is not a crime in most jurisdictions, miners may engage in behaviors that ensure their transactions are favorably mined, facilitating the laundering process. In a selfish-mining attack, an individual miner (or network of colluding miners) privately develops a series of transactions that it validates and releases to the network all at once, ensuring that its private transactions represent the longest chain and is added to the blockchain. In such an attack, honest miners waste computational power while the selfish miner's private chain is accepted.

Mining as a Service (MaaS) may also be used to convert tainted coins into newly mined coins with no transaction history, which may sell on the open market for 10 – 20% of their market value. In such a setup, remote hosting or cloud mining service providers exchange payment for mining services (without sufficient due diligence on the origin of assets) in return, send new generated or mined coins to a paying client.

Those tasked with managing financial crime risks may benefit from paying closer attention to cryptocurrency mining transactions and mining pool operators. The detection of suspicious activity connected with mining may include high-risk indicators, such as identifying blockchain addresses with significant part of transactions that transfer significant fees to miner, or addresses receiving newly generated cryptocurrencies from a miner or mining pool that has accepted a high proportion of tainted assets.

3.3.5 IP Address Hiding

One level below the blockchain applications, operating systems can be identified by their IP addresses, which some Bitcoin and Ethereum nodes and analytics services have been suspected to collect in order to create databases matching accounts numbers and IPs. Analysis of the activity of an IP address or range thereof can reveal substantial information, especially when enriched with other information (other identifiers, software fingerprint, activity patterns, and so on). However IP addresses are often used for a number of systems or individuals located within proximity (e.g. a residential apartment), therefore correlation is not always direct.

When interacting with a blockchain network, privacy may be provided by diversifying the IP addresses, ranges, and locations. Typical tools that can help are VPNs and VPN services, as well as anonymity networks such as the onion router (a.k.a "TOR") or the upcoming Nym network[6].

4 / Implementation Examples – Cryptocurrencies

We focus on the two coins that stand out as being among the most widely used and having different technical approaches to provide privacy guarantees. We briefly describe their core cryptographic mechanisms and comment on their adoption, maturity, and ability to address compliance requirements.

4.1 Zcash

"Zcash is a privacy-protecting, digital currency built on strong science" says Zcash's motto on the website[7]. Launched in 2016, Zcash is based on the Zerocoin and Zerocash protocols published and reviewed by academic researchers. Zcash leverages zk-SNARKs (zero-knowledge succinct non-interactive arguments of knowledge), a type of zero-knowledge proof that can be used in the context of cryptocurrencies to prove to verifiers and miners that a transaction is sound (and in particular, is not a double-spend) without revealing the sender, recipient, and amount transferred.

Thanks to zk-SNARKs, Zcash supports so-called *shielded addresses* (or z addresses), which enable private transactions between such addresses, and can also include an encrypted memo field for additional messages and metadata. However, Zcash supports another type of address, the transparent addresses, which are similar to Bitcoin addresses in terms of privacy. Zcash comments that these addresses aim to "to accommodate for wallets and exchanges that don't support private transactions".

Furthermore, Zcash's shielded addresses support viewing keys, to disclose the content of a transaction given a specific per-address key. About this feature, Zcash's website comments: "Selective disclosure features within Zcash allow a user to share some transaction details, for purposes of compliance or audit."

The Zcash team includes experienced and respected researchers and engineers, and is generally recognized for its high technical quality and rigor. Zcash's technology is however among the most complex in the blockchain space, and inevitably suffered several security issues, though without major impact on Zcash users. The Zcash team provides extensive information about past security issues and mitigations[8]. One of the most interesting attacks on Zcash is a remote exploit of timing leaks in Zcash operations, leading to the exposure of transaction data[9], a vulnerability now fixed[10].

[6] https://nymtech.net.
[7] https://z.cash.
[8] https://z.cash/support/security/announcements/.
[9] https://crypto.stanford.edu/timings/paper.pdf.
[10] https://electriccoin.co/blog/new-release-2-0-7-3/.

To learn more about Zcash's approach, please see our Q&A with Josh Swihart, VP of Growth at Electric Coin Company, the company behind Zcash, who kindly accepted to answer our questions regarding Zcash's experience:

Q&A with Zcash's Josh Swihart

CVA: *Zcash has made efforts to address compliance needs, notably regarding AML and FATF Travel Rule, by supporting unshielded transactions as well as "viewing keys" for shielded transactions. Could you summarize how successful this effort has been, and in particular the progress in terms of support by regulated VASPs?*

Zcash: Zcash includes features that address a number of regulatory requirements. All VASPs can comply with the travel rule and fully support Zcash, just as they can with any other coin as part of their normal KYC/AML compliance efforts.

Viewing keys help VASPs and regulators by ensuring that full transaction details for shielded transactions with the exchange can be safely made to law enforcement should the need arise. Another feature that could be useful is the encrypted memo. This enables VASPs to send encrypted information along with a transaction to the counterparty. This uniquely meets Travel Rule requirements and eliminates the need for out-of-band communication for compliance.

Thanks to these kinds of capabilities, highly regulated exchanges like Gemini can support shielded transactions while remaining fully compliant[11].

CVA: *Aside from Gemini's expansion to offer shielded withdrawals, have you noted an openness from other VASPs or regulators in other jurisdictions to support privacy-enhanced cryptos?*

Zcash: There are a couple other exchanges that currently support shielded Zcash including The Rock Trading in Italy and the Waves Exchange. I have seen an openness to supporting privacy-supporting cryptocurrencies, and foresee a future where this option becomes mandated to protect business and user data from surveillance by foreign threats as players come to grips with both the technology and long term implications in its use.

CVA: *You have described Zcash's approach to transaction privacy as "the TLS of cryptocurrency", to convey the expectation that the main cryptocurrencies would all ultimately support private transactions. In the context of regulated asset transfers, the challenges of this approach are well known, but could you elaborate on the benefits such as those related to client information protection?*

Zcash: See this post for a summary but I'm happy to provide more if desired: https://electriccoin.co/blog/privacy-is-normal-safe-and-essential/

CVA: *As one of the pioneers in privacy-oriented cryptocurrency, Zcash has experimented with innovative cryptographic techniques, such as novel zero-knowledge protocols. These are powerful, but some would argue that they're still immature and not "battle-tested" enough. What would you respond to such objections?*

Zcash: It's a fair concern. What's wonderful about this is that the cryptography is tested every time a transaction is made on the network. For Zcash, the current market cap is nearing $1B with millions of dollars of transactions per day. There is a huge financial incentive to break it, and there is a bit of a Lindy effect. Confidence will increase over time as the technology survives, is improved and thrives.

[11] See the following: https://electriccoin.co/blog/gemini-becomes-first-regulated-institution-to-support-shielded-zcash-withdrawals/ and a recap with Gemini's CRO and Perkins Coie attorney and former NYDFS, Dana Syracuse: https://www.youtube.com/watch?v=FxEENDi13Eg.

4.2 Monero

"Monero is cash for a connected world. It's fast, private, and secure. With Monero, you are your own bank. You can spend safely, knowing that others cannot see your balances or track your activity." This is how Monero's website[12] describe the project, started in 2014 based on the earlier CryptoNote protocol.

Like CryptoNote, Monero relies on ring signatures, a type of signature that involves a group of signers, and where a signature can be recognized as valid when it's been issued by a member of the group, yet in such a way that a verifier cannot identify the actual signer. Monero's RingCT[13] (ring confidential transactions) protocol builds on ring signature and Bulletproof range proofs to develop a cryptocurrency that hides transactions' information.

As Zcash, Monero also aims to provide unlinkability and untraceability, but these properties sometimes fail to be guaranteed, because of activity patterns and shortcomings in earlier versions of the protocol.

Monero appears less interested in compliance aspects, although it defined view keys, a type of key that allows to reveal the content of a transaction[14]. However, this mechanism now seems unreliable, as Monero's documentation explains: "outgoing transactions cannot be reliably viewed as of June 2017. Therefore, the balance of a Monero address as shown via a viewkey should not be relied upon."

Compared to other blockchains and cryptocurrencies that are supported by a formal legal entity, such as a corporation or a foundation, Monero is managed by a loosely defined community and relies on donations from its users to fund research initiatives and third-party audits.

Monero's critical security components underwent several audits before being deployed, sometimes by several companies simultaneously. Like Zcash, Monero was found to be vulnerable to remote timing attacks[15], and mitigations were implemented[16].

5 / Implementation Examples – DLT Enterprise Ledgers

In this section, we look at several prominent enterprise-oriented distributed ledger technologies (DLTs), and list which privacy mechanisms they use. For more information on a particular mechanism, please see section 2 above.

5.1 Hyperledger Fabric

[12] https://www.getmonero.org.
[13] https://eprint.iacr.org/2015/1098.
[14] https://web.getmonero.org/resources/moneropedia/viewkey.html.
[15] https://crypto.stanford.edu/timings/paper.pdf.
[16] https://hackerone.com/reports/713321.

IBM's Hyperledger Fabric is the flagship DLT platform of the Hyperledger foundation, providing a permissioned ledger with smart contracts written in Java, Go and Javascript. The basic privacy mechanism in Hyperledger Fabric is partitioning the state into so-called channels. A channel can be thought of as a "lightweight blockchain". The channel contents are visible only to the channel members, a configurable subset of the nodes in a Fabric deployment.

By default, all channel data is visible to all members. This suffices to ensure privacy, as long as the channels can be constructed such that all members are privy to all data in a channel. This can be achieved using very fine-grained channels, one for every possible group of data stakeholders. The issue with that approach is that Fabric doesn't support transactions over data stored on different channels. Beyond channels, Fabric provides two other privacy mechanisms. First, it provides so-called private data collections. These employ the hashing technique of Section 2.2, such that some data in a transaction can be shared out-of-band, and only data hashes are stored in the channel. Second, Fabric's Identity Mixer utilizes zero-knowledge proofs to provide users with anonymous credentials. In Fabric's case, these currently allow a user to convince others that it's a member or an administrator of a certain organization on the Fabric network, without revealing any further details about the user. They also ensure unlinkability between the usages of a credential.

5.2 Corda / R3

Corda is a DLT platform by R3, providing a permissioned ledger with smart contracts written in any JVM-compatible language (with some restrictions on the available language features to ensure determinism).

Corda relies on state partitioning as its main privacy mechanism: Data in Corda is contained in so-called contract states. Like Bitcoin, Corda uses a UTXO model; that is, every Corda transaction consumes some existing states and creates some new states; unlike Bitcoin, states can contain arbitrary data (not just amounts). Contract code specifies how states can be consumed and created and who is required to sign a consumption or creation of the state. By default, Corda nodes have no access created by transactions of other nodes. States are distributed only when needed to conduct a transaction, using so-called Corda flows. First, all the states in the transaction are distributed to all required signers of all states consumed or created. Second, for every consumed state, the entire chain of transactions leading to this state (e.g., the transfer history of a digital banknote) is also shared with all the signers. Third, the transaction and its data are normally shared with a trusted third party called a notary, who validates and confirms the transaction. Finally, the node submitting the transaction might (at its own discretion) decide to notify some further nodes about the transaction. In this case, it normally distributes the transaction as well as the chain of transactions leading up to all states consumed by the transaction.

Corda provides further mechanisms to increase privacy. First, if conducting a transaction requires statements from third parties (e.g., on the current price of a stock), Corda provides so-called transaction tear-offs, which allow the third party to confirm this statement for the transaction while hiding the remaining transaction contents to the third party. Next, the notary can be run in the so-called non-validating mode, where it only gets access to the state identifiers, but not the states themselves. This provides more privacy, but opens the system to so-called denial-of-state attacks, where users can consume states in an unauthorized fashion. As a future alternative, Corda will allow contract states to be encrypted such that the notary can only decrypt the data inside of an SGX hardware enclave, a mechanism we described in Section 2. Finally, since revealing the entire history of an asset is often problematic, Corda allows trusted issuers to do a so-called "reissuance", which periodically truncates the history of the asset.

5.3 DAML/Canton

DAML is a bespoke smart contract language by Digital Asset. Canton is a protocol for executing DAML, which builds a virtual global ledger using many underlying databases (operated by trusted parties) or ledgers (permissioned or permissionless) for data transport simultaneously.

All data in DAML is contained in so-called contracts, where all contracts specify their stakeholders. The Canton protocol then partitions the state of the global ledger according to the stakeholder annotations, such that each node holds only the data of the stakeholders it hosts. A transaction can span multiple such partitions, that is, operate on contracts with different sets of stakeholders. Transactions are atomic, but the full transaction is not shared with all stakeholders of all contracts. Instead, Canton provides so-called sub-transaction privacy. There, each stakeholder automatically receives exactly the part of the transaction that's relevant for the changes to their contracts. For example, in a transaction trading an equity for a cash token, the equity (resp. token) issuer does not learn the traded cash amount (resp. the equity or its amount). The transaction is communicated to the nodes over the underlying databases or ledgers. To provide privacy against the parties to whom the underlying database or ledger is visible, the transaction messages are encrypted with the recipients' public keys. Canton enforces that all recipients receive their part of the transaction, ensuring the transparency of the global ledger, without needing out-of-band communication.

6 / Recommendations

With a base-line understanding of the various methods available to enhance the privacy of public and private DLT transactions, readers are encouraged to consider the following recommendations:

The use of a privacy coin is usually insufficient to ensure high privacy insurance, as these are just one piece of the privacy puzzle. A strategy should be established and implemented to ensure adequate privacy controls at different levels and with respect to different notions (such as unlinkability of addresses and confidentiality of personally identifiable information).

Leverage off-chain privacy controls, in order for example to protect the confidentiality of personal data, of the governance model, of wallets' structure, or of your IT infrastructure.

Recognize the limitations of privacy coins. These may be reliable platforms that effectively hide transaction information now and in the foreseeable future. Further in the future however, these may be subject to attacks that could reveal all or part of the transactions' information, often resulting from or jeopardized by poor operational security practices.

Understand the regulatory frameworks, preferably with the help of experts, according to the applicable regulations and laws. Different industries and jurisdictions regulate blockchain and DLT activities to varying degrees and in different ways. An activity or service may also require authorisations in the jurisdiction in which they are registered, operate and/or directly solicit customers. Appropriate governance and transaction transparency are often not optional.

+ + +

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