Addressing Privacy Challenges in Permissioned Blockchain Adoption For Financial Institutions and Governments

Category: Information Technology

Affiliantion: Parfin.io

Alex Buelau[1]
Ricardo Santos[2]

Resumo

Permissioned EVM (Ethereum Virtual Machine) blockchains are gaining popularity as viable options for permissioned blockchains. However, scalability and privacy remain significant challenges. This article examines the advantages, disadvantages, and risks of current privacy solutions for EVM- based blockchains. It concludes that the best approach is to implement a network topology that ensures sensitive data never leaves the institution responsible for its management. By doing so, organizations can benefit from the advantages of blockchain technology while minimizing the risks associated with privacy breaches.

Palavras-chave: *privacy;* EVM*; blockchain; cryptography; financial institutions; bridges.*

[1] alex@parfin.io
[2] ricardo@parfin.io

1 Introdução

The financial industry has been undergoing significant transformation in recent years, with the increasing adoption of blockchain technology and digital assets. One of the key drivers of this transformation has been the growing interest in institutional and governmental financial applications of permissioned blockchains. In particular, tokenization and Central Bank Digital Currencies (CBDCs) have captured the attention of financial institutions and governments alike. This article explores the benefits and challenges of adopting Ethereum Virtual Machine (EVM) for permissioned blockchains, the way to address privacy concerns, and how a new topology can provide a sound solution to for ensure privacy in financial transactions.

Permissioned blockchains are gaining traction in the financial industry because they offer several advantages over their public, permissionless counterparts. They allow for more control over network participants, enhanced security, and tailored consensus mechanisms. The most notable applications of permissioned blockchains in the financial sector are tokenization and CBDCs. Tokenization allows the conversion of various assets into digital tokens, making them easily tradable and accessible. CBDCs, on the other hand, are digital currencies issued by central banks that can facilitate faster and more efficient payments and settlements.

EVM has become the standard for public permissionless blockchains due to its compatibility, flexibility, and robust community support. Institutions and governments have also adopted EVM for their permissioned blockchains, as it allows them to leverage innovations from the public domain, access a large pool of developers and experts, and benefit from ongoing improvements in the technology. However, while EVM offers numerous advantages, it also poses unique challenges when applied to permissioned blockchains, particularly in the areas of privacy and scalability.

2 Challenges in permissioned blockchains: privacy and scalability

Two widely known challenges faced by permissioned blockchains using utilizing EVM are privacy and scalability. Privacy is a crucial concern for financial institutions and governments, as sensitive information must be protected from unauthorized access. Scalability, on the other hand, is essential for ensuring that the blockchain can handle increasing transaction volumes and maintain high- performance levels.

This article will focus primarily on the privacy challenge, since it is a more general issue for permissioned EVM networks.

A significant privacy challenge in EVM-based permissioned blockchains is that they are account-based, which means all validators on the network can access all the data stored on the blockchain. This poses a problem for financial institutions, especially if they serve as validators, since they could potentially view each other's transactions and account information. This lack of confidentiality could undermine trust among participating institutions and compromise the overall security of the network.

3 Addressing Privacy Concerns In EVM-based Permissioned Blockchains

There are three primary ways to address privacy concerns in EVM-based permissioned blockchains:

a) Data encryption: One approach to ensure privacy is encrypting the data on the blockchain. This prevents unauthorized parties from accessing sensitive information for a period of time.

b) Regulating validators: Another solution is to establish regulations that prohibit validators from accessing certain data and trust that they will comply.

c) Multiple private blockchains: A third option is to adopt a topology with multiple private blockchains, where each financial institution acts as a single validator of their own private blockchain, and these blockchains are connected through bridges.

Each of the above privacy solutions has its advantages and drawbacks:

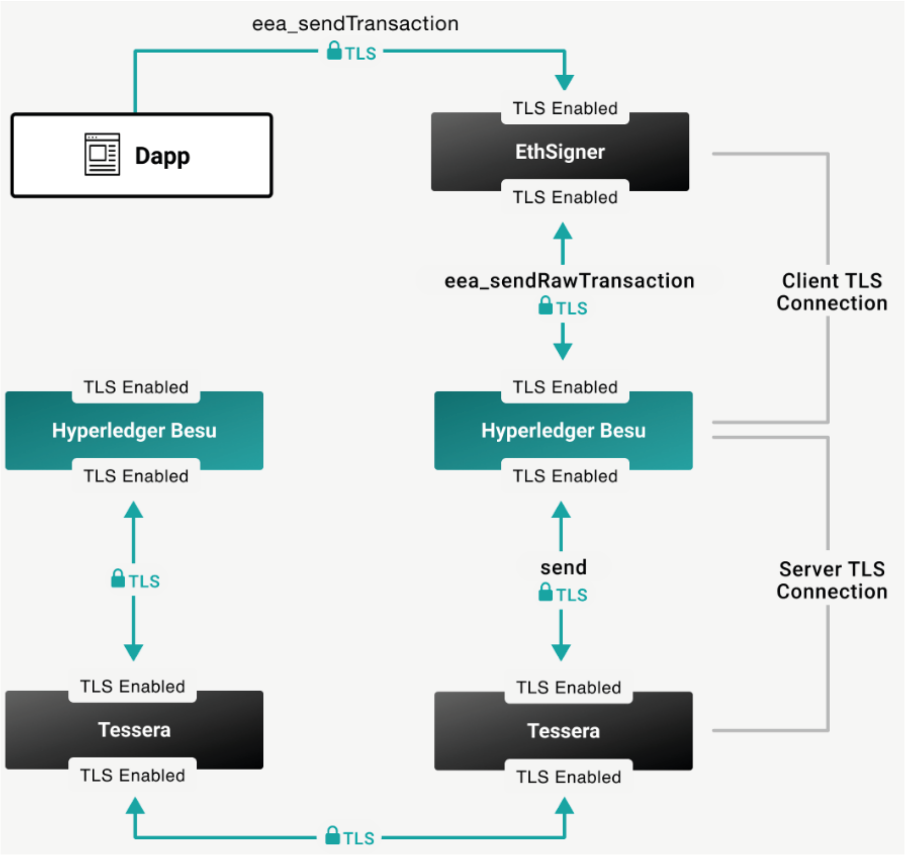
a) Data encryption

There are several solutions that have been created over the years that use encryption to try to provide privacy in EVM blockchains. The first type of solution isconsists of private databases that handle private transactions and stamp hashes on a shared chain. For example, the Ethereum clients Quorum and Hyperledger Besu can work with a private transaction manager called Tessera. Hyperledger Fabric supports the same private transaction pattern through chaincode private collections.

In these scenarios, members of a network can communicate privately using private Ethereum transactions. The way it works is relatively simple. First, a standard Ethereum transaction occurs publicly with an input field containing an enclave key. Then, that enclave key is used to fetch the private transaction. A private transaction is the same as a public Ethereum transaction with additional privacy metadata. The privacy metadata

contains the privateFrom and the *privateFor* or the *privacyGroupId* data.
The privacy group is a complete side chain. Each privacy group can have its own custom genesis. The ramifications of this are that when you interact with a private transaction you are in effect sending two transactions in one; the public marker transaction (with its own sender, nonce etc.) and a private transaction (again with its own sender, nonce, etc.).

Figura 1 - Funcionamento de uma *liquidity pool*



Source: Image: SourceTessera Privacy Solution, ([n.d.)]).

Approaches like these have a few drawbacks, namely:

- No Native Token support: Private transactions either deploy contracts or call contract functions. Native token transfer transactions cannot be private.
- Composability Issue: In order to support private transactions some Ethereum Clients need different parameters in SDK or RPC calls such as the privateFrom and privateFor, or privacyGroupId. These small differences make the usage of the most common libraries in Web3 space quite difficult to use.
- Private State Divergences leading to double-spend attacks: While private transactions may seem to provide a certain level of safety at first glance, their inherent secrecy also has a downside that needs to be addressed. Nodes' private states may diverge, creating the opportunity for a double-spending exploit.

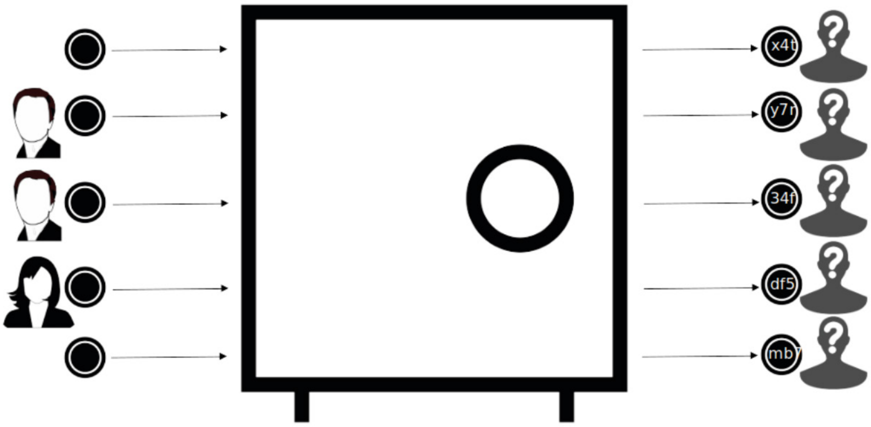
Another popular approach to provide privacy to EVM-based blockchains is to use Zero-Knowledge technology (ZK). Examples include TornadoCash which utilizes ZKP (ZK Proofs), and Polygon Nightfall which employs Optimistic ZK.

In the case of TornadoCash, transactions are made private by asking the sender to send a token to a pool, and this token can only be withdrawn if the receiver presents a valid ZK Proof (TornadoCash, [n.d.]). This approach, however, has many drawbacks:

- Off-chain communication is required between sender and receiver so that the receiver can have the ZK Proof required to withdraw.
- A user's privacy is derived in large part from the simultaneous usage of the pool by many other users. If the pool had only a single user, simple inference would make it obvious from where the withdrawn tokens came (TornadoCash, [n.d.]).
- In order to guarantee privacy, receivers are supposed to wait a period of time before withdrawing which makes this solution difficult to use in real-world applications.
- Since this is a smart contract-based solution, it doesn't solve the issue of validators still being able to see the balances of all accounts.

Polygon Nightfall has a very similar approach and similar limitations as TornadoCash. Transactions can be private to some extent (given the limitations above) but accounts are still transparent to all validators.

Figure 2 – Polygon Nightfall Concept



(Source: Polygon Nightfall Github, [n.d.]

Nevertheless, technologies such as TornadoCash and Nightfall have some interesting use cases outside of regulated financial markets, for example Nightfall might be useful for supply chains as explained by the Polygon Nightfall team themselves: "In fact, we aim at disrupting the $50 Trillion global supply chain industry". (Polygon Nightfall, [n.d.]).

An additional concern that arises when using encryption to try and keep private blockchain data secure over long periods of time is the threat of data harvesting. As explained by ITPRo: "The rise in quantum computing this decade is pushing cyber criminals into stealing encrypted business data with the hopes of cracking it in the future" (Steal Now Crack Later, [n.d.])

In summary, encryption can provide robust protection for sensitive data, but it is not immune to future cryptographic breakthroughs. Validators and malicious attackers could potentially harvest data for future decryption once the cryptographic algorithms have been broken. Additionally, encryption can add overhead to the processing time and complicate data management.

b) Regulation validators

Relying on regulatory compliance and trust is not fool proof, as it leaves room for human error and malicious intent. Ensuring that validators adhere to regulations can be challenging, and breaches may still occur despite strict oversight.

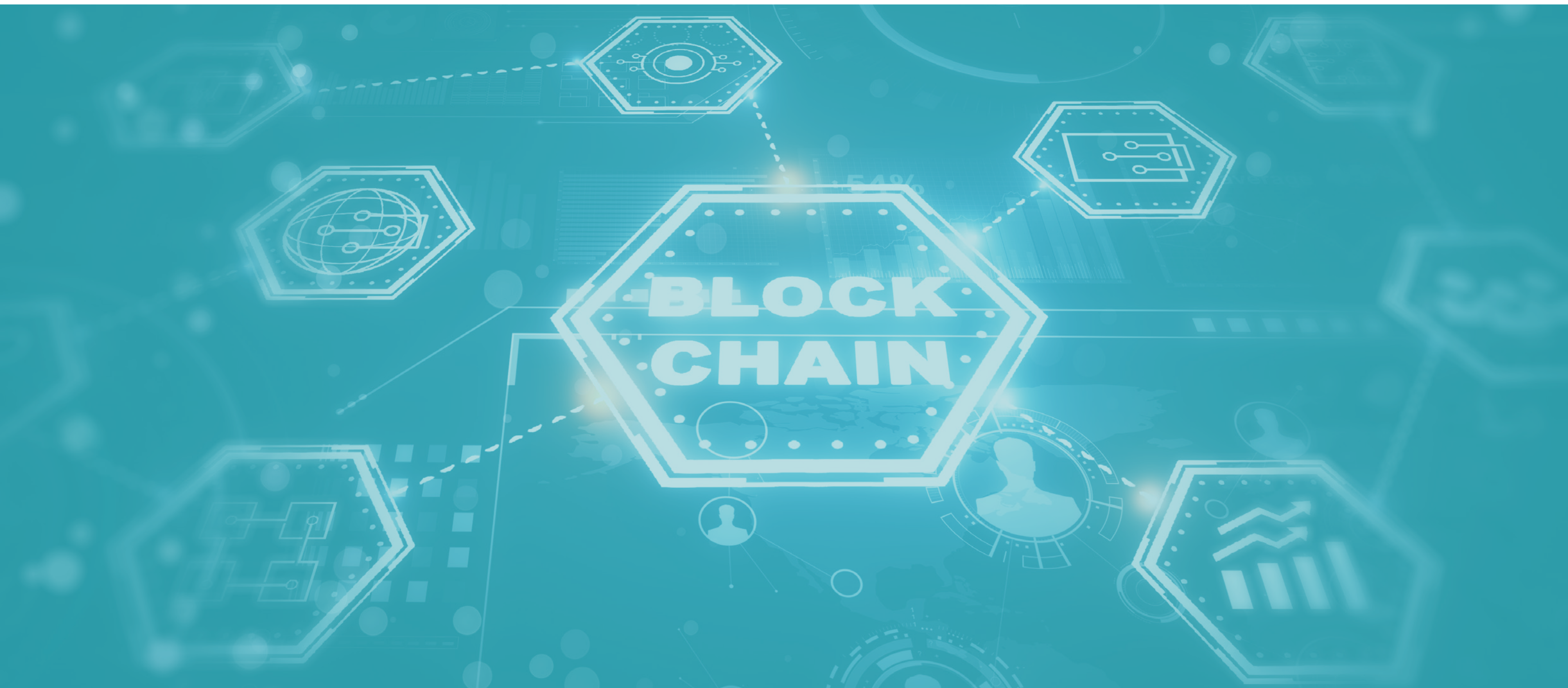
For example, we have seen an increase in the numbers of fines imposed by regulators to companies, including financial institutions, for breaches of compliance with data protection regulations. Data protection authorities in Europe have issued a total of EUR 1.64bn of fines since January 2022 for breach of regulatory obligations (according to the DLA Piper GDRP Fines and Data Breach Survey Report).

Furthermore, this approach is also susceptible to data harvesting as explained in the section above and indeed data breaches at validators could result in data being exploitable even if encrypted and in the case of a financial blockchain with multiple validators, a data breach in one validator could result in the data of all participants being exposed.

c) Multiple private blockchains

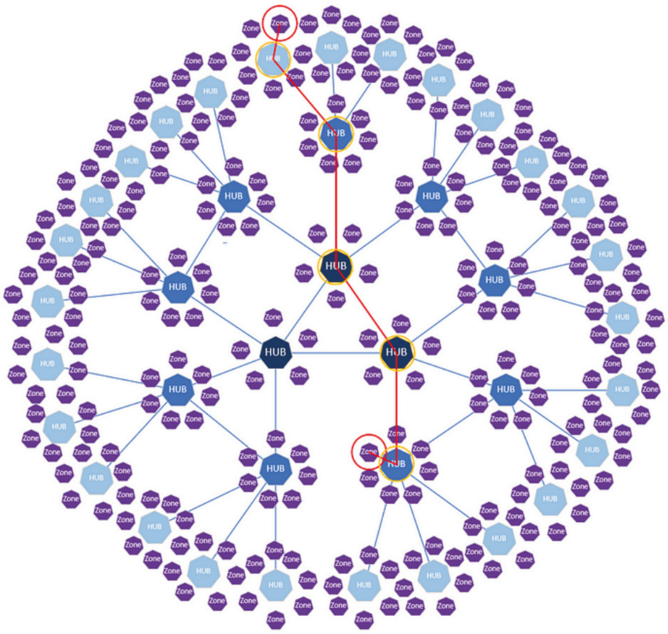
A third option to preserve privacy of financial institutions is for each financial institution to have its own private EVM blockchain, where it can mint proprietary tokens, manage its own client accounts, deploy smart contracts, offer DeFi solutions to its clients all in a completely private and safe environment that it fully control.

A notable challenge for this topology has been ensuring seamless bridges that connect various blockchains. In the past, there have been instances of security breaches involving blockchain bridges; however, these breaches primarily occurred in the context of public decentralized blockchains. When it comes to permissioned blockchains, many requirements associated with decentralization and trustlessness can be set aside, simplifying the process of establishing secure bridges between networks.



Considerable advances have been made in recent months by public permissionless ecosystems such as Cosmos and Polkadot in what are being referred to as ‘Layer Zero’, which means standard protocols that enable seamless communication between blockchain.

Figure 3 – Vision for the Cosmos Blockchain Topology



Source: Cosmos Topology ([n.d.])

A Layer Zero topology has several advantages, such as increased control over data and reduced risk of unauthorized access, interoperability between different blockchains, that don’t even have to rely on the same internal consensus or smart contract machinery.

4 The optimal solution: privacy-preserving layer zero

Considering the pros and cons of the above-mentioned privacy solutions, the most feasible and fail-proof way to ensure privacy in permissioned blockchains is to adopt a layer zero topology where private data never leaves the context of the institution to which the data is private. This approach combines the benefits of multiple private blockchains while addressing their shortcomings.

In this topology, each financial institution or government agency operates its own private blockchain, acting as the sole validator. These private blockchains are connected through secure bridges, which facilitate the exchange of data and transactions between participating institutions. This setup ensures that sensitive data remains confined within the originating institution's private blockchain, preventing unauthorized access and preserving privacy.

This topology allows for the creation of standardized protocols and interfaces to ensure seamless interoperability between the various private blockchains, mitigating the complexity associated with managing multiple blockchains.

5 Conclusion

As the adoption of permissioned blockchains for institutional and governmental financial applications continues to rise, addressing privacy concerns becomes paramount. The Ethereum Virtual Machine (EVM) has emerged as a popular choice for implementing permissioned blockchains, but its inherent privacy challenges must be tackled head-on.

While data encryption and regulatory measures can provide some degree of privacy protection, they are not immune to potential breaches or future advancements in cryptography. The most effective solution is to adopt a new topology in which private data remains within the confines of its respective institution, ensuring the highest level of privacy and security.

By embracing this approach, financial institutions and governments can leverage the power of permissioned blockchains for applications like tokenization and CBDCs, while preserving the confidentiality and trust required for successful implementation.

References

COSMOS TOPOLOGY. **Cosmos** — an early in-depth analysis at the ecosystem of connected blockchains — Part Two. [n.d.]. Available in: https://cryptoseq.medium.com/cosmos-an-early-in-depth- analysis-at-the-ecosystem-of-connected-blockchains-part-two-2d5a9886166.

POLYGON NIGHTFALL. **Introducing Polygon**. [n.d.]. Available in: https://polygon.technology/blog/introducing-polygon- nightfall-mainnet-decentralized-private-transactions-for-enterprise.

POLYGON NIGHTFALL GITHUB. **Nigntfall** – A ZK-Proof Protocol for Entrerprises. [n.d.]. Available in: https://github.com/NightfallRollup/nightfall-docs.

STEAL NOW CRACK LATER. **What is steal now crack later quantum computing**. [n.d.]. Available in: https://www.itpro.com/security/cyber- security/370298/what-is-steal-now-crack-later-quantum-computing.

TESSERA PRIVACY SOLUTION. **Hyperledger Besu Ethereum clien**t. [n.d.]. Available in: https://besu.hyperledger.org/en/stable/private- networks/

TORNADOCASH. [n.d.]. **How does Tornado Cash work?** Available in: https://www.coincenter.org/education/advanced-topics/how- does-tornado-cash-work/