Welcome to the DSF Science Notes

Contents

DSF Science Notes consists of high-quality technical research content focused on blockchain technology. The topics covered fall in these three major categories, namely;

1. **Academic Insights**: This category will feature science notes that highlight academic research findings related to blockchain technology, cryptography, distributed ledger technology (DLT), and other relevant topics. Science notes in this category with include a comprehensive overview of recent research papers in a subject-area. and will be findings-focused.
2. **Industry Perspectives**: This category will include science notes that provide findings and insights focused on the industry applications of blockchain-related subject matters.
3. **Innovation & Ideation**: This category will focus on highlighting innovative ideas, concepts, and use cases related to blockchain technology. It will feature blog posts that explore potential applications of blockchain in various industries, such as finance, supply chain, healthcare, and more.

Download Science-Notes as a pdf

DSF Science Notes Editorial Board

Dr Jiahua Xu, DSF Head of Science
Dr Carlo Campajola, DSF Senior Research Fellow

Governance In DeFi

Academic insight

Key Insights

- The voting power in DeFi protocols becomes increasingly concentrated among a percentage of token holders over time in decentralised exchanges, lending protocols and yield aggregators.
- The paramount wallet addresses ranking within the top 5, 100, and 1000, exercise predominant influence over the voting power in the Balancer, Compound, Uniswap, and Yearn Finance protocols, with Compound displaying the least evidence of decentralisation.
- The most significant governance challenges identified by DeFi users are voter collusion, low participation rates, and voter apathy.
- To address vulnerabilities in DeFi governance, a novel voting mechanism resistant to sybil attacks called bond voting has been proposed.
- To enhance the manual parameter section, an AI-enabled adjustment solution has been demonstrated to automate governance mechanisms.

Decentralised finance (DeFi) has emerged as a potential substitute for traditional financial institutions, offering peer-to-peer transactions and a diverse range of services that democratise finance by enabling users to participate in protocol governance. However, several studies have suggested that the current governance mechanisms require improvements. This article provides an overview of findings associated with DeFi governance.

Centralisation of Governance in DeFi Protocols

Centralisation in DeFi has become a growing concern among researchers with several studies identifying a significant level of centrality in the governance mechanisms of DeFi protocol. Barbereau et al., [BSP+22a] found that the decentralisation of voting is significantly low with a majority of the voting power concentrated among a percentage of governance token holders. As evidenced by their findings, there was a significant degree of centrality, in lending protocols, decentralisd exchanges and yield aggregators. This research work employed case studies to comprehend the governance mechanisms of these protocols.

Similarly, result by Jensen et al. [JvWR21] demonstrate centrality in voting power with the protocols top 5, top 100, and top 1000 wallet addresses controlling majority of the voting power in Balancer, Compound, Uniswap and Yearn Finance protocols. In this study, the token holdings and users' wallets of protocols were analysed; Compound displayed the most evidence of centrality and Uniswap the least with the top 5 wallet addresses accounting for 42.1% and 12.05%, respectively.

Barbereau et al. [BSP+22b] ascertained that DeFi protocols become more centralised over time. In this longitudinal study, voting patterns demonstrated changes in the power dynamics as time progressed. The tendency for this centralisation of DeFi protocols is shown in [Fig. 1]. Furthermore, in analysing the governance structures of DeFi protocols, Stroponiati et al. [S+] ascribed reward-based economic incentives as the significant cause behind the development of centralised structures.

Lending Protocols

Lending Protocols are DeFi applications built on top of blockchain technology that allow users to lend and borrow cryptocurrency assets without the need for intermediaries such as banks or traditional financial institutions.

Decentralized Exchanges

Decentralized Exchanges (DeXs) are peer-to-peer trading platforms built on top of a blockchain that enable the direct exchange of cryptocurrency assets without the need for a central authority or intermediary.

Yield Aggregator

Yield Aggregator are DeFi applications that automate the process of seeking out the best yield opportunities for cryptocurrency assets, and provide users with a way to optimize their returns on investment.

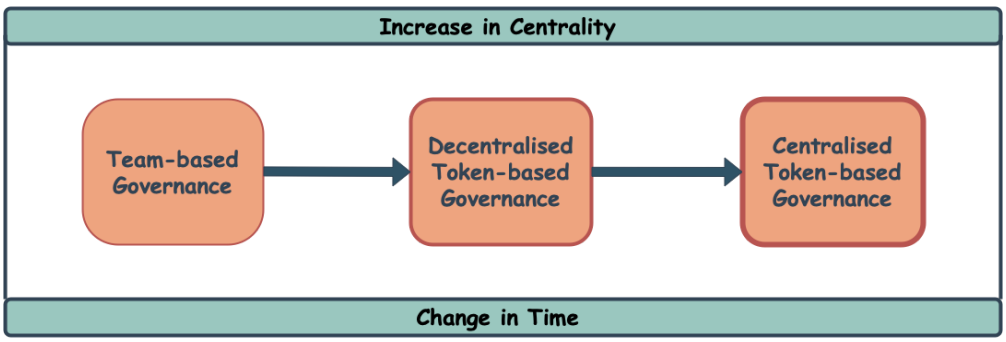


Fig. 1 The Tendency for Centralisation in DeFi Governance.

Challenges & Vulnerability In DeFi Governance

In investigating governance challenges, Ekal et al., [EAw22] identified voter collusion, low participation rates, and voter apathy as the most significant challenges. This empirical investigation utilised an interview survey approach to collect data from protocol users. Furthermore, to address voter concentration vulnerabilities, Mohan et al. [MKB22] proposed a novel voting mechanism called bond voting which is resistant

Voter Collusion

Voter Collusion refers to a situation where a group of voters collude together to manipulate the outcome of a voting process in their favor, typically by coordinating their votes to create a super majority.

tokens, for a time period to gain voting power. Therefore, by combining this time commitment with weighed voting with a time commitment, sybil attacks are more difficult. Quadratic voting, another solution to voting concentration, allows participants to convey both their preferences and the intensity of those preferences, however, the drawback of this mechanism is its vulnerability to sybil attacks, voter collusion and voter fraud [KL22].

Voter Apathy

Voter Apathy refers to a situation where token holders or members of the organisation do not actively participate in the voting process due to a lack of interest

Sybil Attack

Sybil attacks occur when an attacker generates multiple false identities to gain significant network control, thereby allocating more votes than expected.

AI-enabled On-chain Governance

To enhance and automate governance mechanisms, Xu et al., [XPFL23] demonstrated an AI-enabled parameter adjustment solution which is more efficient than current implementations. Specifically, the study employed Deep Q-network (DQN) reinforcement learning to investigate for automated parameter selection in a DeFi environment. Although a lending protocol was employed in the study, the model's application can extend to other categories of DeFi protocols as well. In investigating DAOs, Nabben [Nab23] observes that GitcoinDAO also employs algorithmic governance in various organisational components such as monitoring the compliance with rules of the organisation.

Conclusion

The vision of DeFi is to foster a democratic process of governance and sustain high levels of decentralisation. However, recent studies have highlighted significant centrality in DeFi governance mechanisms, indicating the need for improvements in the existing governance models. The studies analysed in this article have revealed that the majority of the voting power in several protocols is concentrated among the top token holders, with evidence of increasing centralisation over time. Moreover, DeFi has been found to face challenges in the voting and governance process. In view of some of these challenges, researchers have proposed novel solutions such as a bond voting and an AI-enabled parameter-selection solution to improve the current mechanisms. Given the importance of decentralisation in the underlying philosophy of DeFi, proposing more solutions to governance challenges is crucial for creating a more inclusive and democratic financial ecosystem. Therefore, continued research and development will certainly be required.

Yimika Erinle
April 2023

References

[BSP+22a] Tom Barbereau, Reilly Smethurst, Orestis Papageorgiou, Alexander Rieger, and Gilbert Fridgen. Defi, not so decentralized: the measured distribution of voting rights. *Hawaii International Conference on System Sciences (HICSS)*, 2022.

[BSP+22b] Tom Barbereau, Reilly Smethurst, Orestis Papageorgiou, Johannes Sedlmeir, and Gilbert Fridgen. Decentralised finance's unregulated governance: minority rule in the digital wild west. *Available at SSRN*, 2022.

[EAw22] Hassan Hamid Ekal and Shams N Abdul-wahab. Defi governance and decision-making on blockchain. *Mesopotamian Journal of Computer Science*, 2022:9–16, 2022.

[JvWR21] Johannes Rude Jensen, Victor von Wachter, and Omri Ross. How decentralized is the governance of blockchain-based finance: empirical evidence from four governance token distributions. *arXiv preprint arXiv:2102.10096*, 2021.

[KL22] Aggelos Kiayias and Philip Lazos. Sok: blockchain governance. *arXiv preprint arXiv:2201.07188*, 2022.

[MKB22] Vijay Mohan, Peyman Khezr, and Chris Berg. Voting with time commitment for decentralized governance: bond voting as a sybil-resistant mechanism. *Available at SSRN*, 2022.

[Nab23] Kelsie Nabben. Governance by algorithms, governance of algorithms: human-machine politics in decentralised autonomous organisations (daos). *puntOorg International Journal*, 8(1):36–54, 2023.

[XPFL23] Jiahua Xu, Daniel Perez, Yebo Feng, and Benjamin Livshits. Auto. gov: learning-based on-chain governance for decentralized finance (defi). *arXiv preprint arXiv:2302.09551*, 2023.

Blockchain Bridge Security

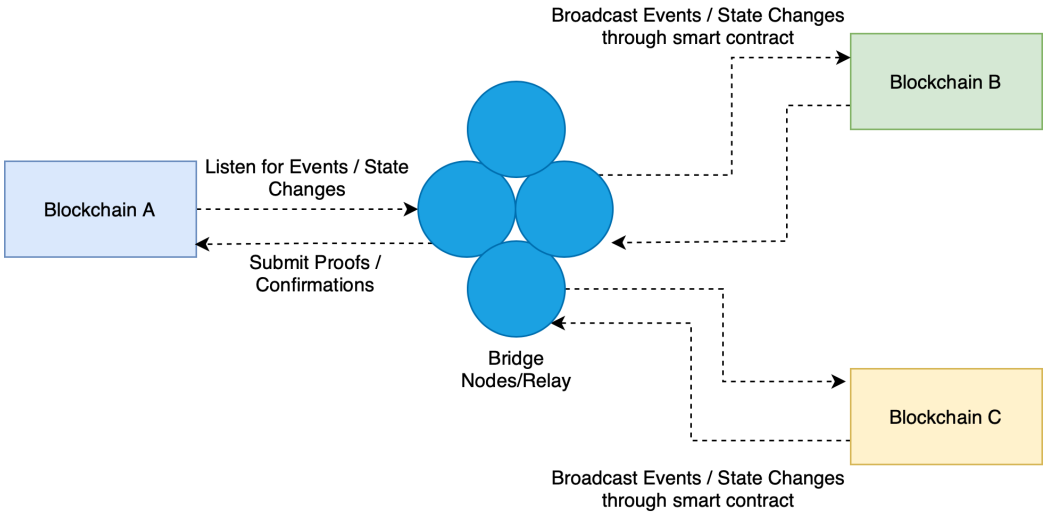
Academic insight

Key Insights

- To mitigate security risks, a cross-chain bridge leveraging zk-SNARK technology to provide a secure, trustless cross-chain bridge, marking the first implementation of Zero-Knowledge Proofs (ZKP) in a decentralized trustless bridge system has been proposed.
- To facilitate secure cross-chain interoperability, a Hash time-lock scheme which does not rely on external trust ensuring transaction security is introduced.
- High security and highly scalability option which supports the interoperability of multiple objects is sidechains/relay scheme.
- To mitigate token transfer risks, a series of protocols “TrustBoost” using smart contracts to achieve a ‘consensus on top of consensus’ mechanism, bolstering trust across multiple blockchains and with promising prospects for future applications is proposed.
- To enhance interoperability, a novel framework mitigating security risks in cross-blockchain technology is proposed. It facilitates the identification of key assumptions and characteristics. It improves decision-making, minimizes design errors, and aids in integrating various blockchain applications, thus promoting effective interoperability.
- Cryptographic techniques remain central to ensuring security in blockchain bridges. A balance between scalability and security is crucial for the future of blockchain bridges.

Introduction

Blockchain technology has been lauded for its potential to disrupt various industries, given its unique properties such as decentralization, transparency, and security. One recent advancement in this area is the development of blockchain bridges, which enable interoperability among different blockchains. Bridges facilitate communication between two blockchain ecosystems through the transfer of assets and information. However, as with any innovative technology, these bridges pose new security challenges. In this science note, we delve into the current academic landscape surrounding the security of blockchain bridges and summarize the recent research findings.



Communication through a Blockchain Bridge

Interoperability and Security Challenges

Interoperability in blockchain environments brings forth a series of unique security challenges. Trustless, interoperable, cryptocurrency-backed assets can be subjected to various threats. In April 2022, attackers were able to obtain five of the nine validator keys, through which they stole 624 million USD by exploiting Ronin bridge, making it the largest attack in the history of DeFi (Sam Kessler and Sage D. Young, 2022). According to blockchain analytics firm Chainalysis, until August 2022 recurring attacks against bridges have cost users around 1.4 billion USD (Ryan Browne, 2022). In 2022 attacks on bridges accounted for 69% of total funds stolen (Chainanalysis, 2022).

Zero-Knowledge Proofs

A zero-knowledge proof (ZKP) is a cryptographic technique that enables one party, the prover, to convince another party, the verifier, of the validity of a statement or the possession of a secret without revealing any additional information about the underlying secret or data.

zk-SNARK

Zk-SNARK is an acronym that stands for "Zero-Knowledge Succinct Non-Interactive Argument of Knowledge." A zk-SNARK is a cryptographic proof that allows one party to prove it possesses certain information without revealing that information.

This calls for novel security models and protocols that can protect against possible attack vectors introduced by cross-chain communication. This is particularly true for blockchain bridges that need to uphold the integrity and security of transactions across disparate networks. Most existing solutions rely on trust assumptions of committees, this lowers the security significantly.

Xie et al. proposed a solution by introducing "zkBridge" an efficient cross-chain bridge that guarantees strong security without external trust assumptions. The main idea is to leverage zk-SNARK, which are succinct non-interactive proofs (arguments) of knowledge as a result security is ensured without relying on a committee. zkBridges uses zk-SNARK protocol to achieve both reasonable proof generation time and on-chain verification cost. zkBridge is "trustless" as it does not require extra assumptions other than those of blockchains and underlying cryptographic protocols. It is the first to use Zero-Knowledge Proofs (ZKP) to enable a decentralized trustless bridge.

Pillai et al. proposed a novel cross-blockchain integration framework designed to guide the integration of cross-blockchain technology. The framework aids in identifying crucial assumptions and characteristics, mitigating security risks, enhancing the decision-making process, minimizing design mistakes and performance issues. It recognizes the integration system as the fundamental unit of cross-blockchain technology, providing comprehensive analysis and addressing security concerns. Moreover, the framework supports businesses in designing and integrating various blockchain applications, while enabling a more accurate evaluation of security assumptions. Thus, it paves the way for effective interoperability among multiple blockchains.

The Role of Cryptography in Blockchain Bridge Security

Securing blockchain bridges is greatly dependent on the strength of the cryptographic techniques deployed. The fundamental study by Kiayias et al. on proof-of-stake blockchain protocols is of significant relevance. They outlined a novel cryptographic mechanism that provides transactional security while ensuring transparency.

Sidechain

Sidechain is a blockchain that communicates with other blockchains via a two-way peg. It stems from the main blockchain and runs in parallel to it.

Cryptographic Protocol

A cryptographic protocol is an abstract or concrete protocol that performs a security-related function and applies cryptographic methods, often as sequences of cryptographic primitives. A protocol describes how the algorithms should be used and includes details

To overcome the external trust assumption, Li et al. in their paper proposed a Hash time-lock scheme, which utilizes a hash function and time-lock features to achieve cross-chain interoperability. The security of the Hash time-lock scheme is based on cryptographic hardness assumptions. The asset receiver is forced to determine the collection and produce proof of collection to the payer within the cut-off time, or the asset will be returned via hash locks and blockchain "time" locks. The proof of receipt can be used by the payer to acquire assets of equal value on the recipient's blockchain or trigger other events. However, this scheme only supports monetary exchange and thus has low scalability.

interoperable versions of a program.

sidechains/relay scheme which supports the interoperability of multiple objects such as assets and other data, thus having high scalability. In particular, the two-way peg is a mechanism that allows bidirectional communication between blockchains. An example of a two-way peg is simplified payment verification (SPV) in Bitcoin. Relays represent a mechanism that enables a blockchain network to authenticate data from other blockchain networks, eliminating the need for external third-party sources. Operating as a light client on a network, a relay system incorporates a smart contract and records block header information from different networks (Frauenthaler et al., 2020). A trade-off of the sidechain implementation is that the vulnerability might increase in the main chain or other sidechains if there is a compromised sidechain in the network (P. Sztorc, 2019).

Ding et al., proposed a framework for connecting multiple blockchain networks via an intermediary structure known as the InterChain. The InterChain possesses its own validation nodes, while SubChain networks are linked to this InterChain via gateway nodes.

Hardjono et al., discussed blockchain interoperability by drawing parallels with the design principles of Internet architecture. Just as the internet uses routers to guide message packets across its network at a mechanical level, they propose the use of gateways to direct messages between different blockchain networks.

Such cryptographic protocols can serve as a guiding light for the development of security measures in the context of blockchain bridges.

Scalability and Security

As important as security is for blockchain bridges, it should not compromise the scalability of the systems. Zamyatin et al. discussed the scalability-security trade-off in their study on interoperable assets. There is need for a balance that allows for scalability without jeopardizing security. Future research in blockchain bridge security needs to address this delicate balance, ensuring the development of robust and efficient interoperable systems.

Zhang et al. introduced a method that facilitates asset exchange between inter-firm alliance chains and private chains. Users from both the sending and receiving chains authenticate their identities and secure a certificate by interacting with the alliance chain. When a cross-blockchain transfer request is initiated, the alliance chain validates the ownership of the users over the assets, then proceeds with the asset transfer through a cross-blockchain interaction process.

Maintaining Sovereignty of blockchains

Existing solutions to boost the trust using a stronger blockchain, e.g., via checkpointing, requires the weaker blockchain to give up sovereignty. Wang et al. in their paper present a series of protocols known as “TrustBoost” designed to bolster trust across multiple blockchains without compromising their sovereignty. These protocols function through smart contracts, achieving a “consensus on top of consensus” that avoids changes to the blockchains’ consensus layers. TrustBoost operates by allowing cross-chain communication via bridges, facilitating the sharing of information across smart contracts on different blockchains. This system maintains its security as long as two-thirds of the participating blockchains are secure. Furthermore, TrustBoost shows potential in mitigating risks associated with cross-chain token transfers and exhibits promising prospects for future applications, especially as heterogeneous blockchain networks continue to mature.

Conclusion

Blockchain bridges represent an important evolution in blockchain technology, facilitating crucial interoperability. However, the security aspects of these bridges are complex and multifaceted, requiring rigorous academic and industry attention. The body of research surrounding blockchain security provides critical insights that can help guide the development of secure and efficient blockchain bridges. As this field continues to evolve, a focus on understanding and mitigating security risks while maintaining scalability will be paramount.

Ali Kathia
May 2023

Chainanalysis (2022) Cross-chain bridge hacks emerge as top security risk, Chainalysis. Available at: https://blog.chainalysis.com/reports/cross-chain-bridge-hacks-2022/ (Accessed: 22 May 2023).

D. Ding, T. Duan, L. Jia, K. Li, Z. Li and Y. Sun, "Interchain: A framework to support blockchain interoperability", Proc. 2nd Asia–Pacific Work. Netw., pp. 1-2, 2018.

J. Zhang, Y. Liu and Z. Zhang, "Research on cross-chain technology architecture system based on blockchain", Proc. Int. Conf. Commun. Signal Process. Syst., pp. 2609-2617, 2019, [online] Available: https://link.springer.com/chapter/10.1007/978-981-13-9409-6_318.

Kiayias, A. et al. (2017) 'Ouroboros: A provably secure proof-of-stake Blockchain Protocol', Advances in Cryptology – CRYPTO 2017, pp. 357–388. doi:10.1007/978-3-319-63688-7_12.

Li, T. et al. (2023) Metaopera: A cross-metaverse interoperability protocol, arXiv.org. Available at: https://arxiv.org/abs/2302.01600 (Accessed: 18 May 2023).

Pillai, B. et al. (2022) 'Cross-blockchain technology: Integration Framework and security assumptions', IEEE Access, 10, pp. 41239–41259. doi:10.1109/access.2022.3167172.

P. Frauenthaler, M. Sigwart, C. Spanring and S. Schulte, "Leveraging blockchain relays for cross-chain token transfers", Gas, vol. 300, pp. 6, Mar. 2020.

P. Sztorc, Drivechain—The Simple Two Way PEG, Jun. 2019, [online] Available: http://www.truthcoin.info/blog/drivechain/.

Ryan Browne, M.S. (2022) Hackers have stolen $1.4 billion this year using crypto bridges. here's why it's happening, CNBC. Available at: https://www.cnbc.com/2022/08/10/hackers-have-stolen-1point4-billion-this-year-using-crypto-bridges.html (Accessed: 22 May 2023).

Sam Kessler and Sage D. Young (2022) Ronin attack shows cross-chain crypto is a 'bridge' too far, CoinDesk Latest Headlines RSS. Available at: https://www.coindesk.com/layer2/2022/04/05/ronin-attack-shows-cross-chain-crypto-is-a-bridge-too-far/ (Accessed: 22 May 2023).

T. Hardjono, A. Lipton and A. Pentland, "Toward an interoperability architecture for blockchain autonomous systems", IEEE Trans. Eng. Manag., vol. 67, no. 4, pp. 1298-1309, Nov. 2020.

Wang, X. et al. (2022) TrustBoost: Boosting Trust among interoperable blockchains, arXiv.org. Available at: https://arxiv.org/abs/2210.11571 (Accessed: 18 May 2023).

Xie, T. et al. (2022) 'ZkBridge', Proceedings of the 2022 ACM SIGSAC Conference on Computer and Communications Security [Preprint]. doi:10.1145/3548606.3560652.

Zamyatin, A. et al. (2019) 'Xclaim: Trustless, interoperable, cryptocurrency-backed assets', 2019 IEEE Symposium on Security and Privacy (SP) [Preprint]. doi:10.1109/sp.2019.00085.

Mobile Theft Prevention using Blockchain

Industry Perspective

- Mobile theft is a major concern for smartphone users worldwide, with an estimated 70 million smartphones lost each year.
- Blockchain technology has the potential to provide a secure and decentralized solution to prevent mobile theft.
- The proposed model of using blockchain for mobile theft prevention offers several potential advantages over existing methods, including decentralized and tamper-proof tracking, automation of process, cross-border usage, and cost reduction.
- The smart contract enables the registration of new mobile devices and maps them to their respective phone numbers. It provides a secure and tamper-proof solution for tracking the status of mobile devices on the blockchain.
- The implementation of blockchain-based mobile theft prevention solutions provides an added layer of security that can greatly benefit mobile phone users, manufacturers, and society at large.

Introduction

Mobile theft is a major concern for smartphone users worldwide. With the increasing reliance on mobile devices for personal and professional use, the theft or loss of a smartphone can result in a significant loss of data and privacy. Studies indicate that a staggering number of smartphones, estimated at 70 million, are lost each year, with a meager 7% recovered [Hom16]. Further, company-issued smartphones are not immune to these occurrences, as research has shown that 4.3% of them are lost or stolen annually. Workplace and conference environments are the leading hotspots for smartphone theft, with 52% and 24% of devices stolen, respectively. Moreover, these numbers appear to be increasing, with recent studies indicating a rise of 39.2% between 2019 and 2021 [Hen22]. Given these alarming statistics, there is a growing need for effective mobile theft prevention measures. Blockchain technology has the potential to provide a secure and decentralized solution to prevent mobile theft. By leveraging the immutable and distributed nature of blockchain, it is possible to create a tamper-proof system that can prevent unauthorized access to mobile devices. In this article, we will explore the potential of blockchain technology for mobile theft prevention, its advantages and limitations, and the future prospects of this emerging field.

The proposed technology of using blockchain for mobile theft prevention is still in the development stage and has not yet been widely adopted on a national or international level. However, there are several companies and organizations that are exploring the use of blockchain for mobile security and anti-theft solutions. Internationally, companies such as Samsung and Huawei are researching the use of blockchain for mobile security, with Samsung filing several patents for blockchain-based mobile security solutions [For22, Hua18].

There is currently no known widespread adoption of blockchain for mobile theft prevention. However, governments all over the world have been exploring the use of blockchain for various applications, including supply chain management and digital identity. This indicates that there is an interest in the technology and a potential for the proposed model to be adopted globally.

Rationale Behind Mobile Theft Prevention using Blockchain

Mobile theft has become a growing concern for individuals and organizations around the world. In addition to the financial loss associated with the theft, there is also a significant risk of personal data being compromised. The use of blockchain technology for mobile theft prevention offers a secure and efficient solution for preventing mobile theft [Gob18]. This technology can help individuals and organizations protect their mobile devices and personal information by providing a decentralized and tamper-proof way to track and block stolen mobile devices. By using private blockchains, the proposed model can be implemented in a way that ensures security and privacy, while also reducing the risk of fraud or malicious activity.

- **Decentralized and tamper-proof:** Blockchain technology enables a decentralized and tamper-proof system for tracking and disabling stolen mobile devices. This ensures that the information stored on the blockchain is accurate and cannot be tampered with, making it a reliable source for tracking stolen devices [Chi23].

companies and their nodes [IR21]. This helps to ensure the security of the network and the data stored in it, and also helps to maintain the privacy of the users.

- **Automation of process:** Smart contracts can be programmed to automatically disable the device once the signal is sent, reducing human error and increasing the efficiency [DD21].
- **Cross-border usage:** The proposed model can be used in cross-border cases, making it more efficient and effective than existing methods [Ram21].
- **Cost reduction:** By reducing the number of mobile thefts, the proposed model can also have a positive economic impact. This can include reducing the costs associated with mobile theft for consumers, mobile carriers, and insurance companies [Ali20].

Alternative Technologies Available under Development

- **IMEI blocking:** One of the most common methods for preventing mobile theft is to block the IMEI (International Mobile Equipment Identity) number of a stolen device. This can be done by reporting the theft to the mobile carrier, who will then blacklist the IMEI number and prevent the device from connecting to the network [Hic22].
- **SIM card blocking:** Similar to IMEI blocking, SIM card blocking involves disabling the SIM card of a stolen device. This can be done by reporting the theft to the mobile carrier, who will then deactivate the SIM card and prevent the device from connecting to the network [Tre15].
- **Remote wipe:** Some mobile devices include a remote wipe feature, which allows the device owner to remotely delete all of the data on their device if it is lost or stolen [AIT23].
- **Mobile tracking apps:** There are a variety of mobile tracking apps available that allow device owners to track the location of their device and remotely lock or wipe it if it is lost or stolen [Mar23].

In comparison, the model of using blockchain for mobile theft prevention offers several potential advantages over these existing methods. A decentralized and tamper-proof system for tracking and disabling stolen devices, and the smart contract can be programmed to automatically disable the device once the signal is sent, reducing human error and increasing the efficiency. Additionally, the proposed model can potentially work in cross-border cases, which is not possible with IMEI and SIM card blocking, and also can be integrated with other theft prevention methods.

Methodology

The smart contract enables the registration of new mobile devices and maps them to their respective phone numbers. This allows users to update the status of their mobile devices on the blockchain, indicating whether they are lost or stolen. The smart contract also allows for changes to be made to the registered mobile devices' information, such as their International Mobile Equipment Identity (IMEI) number, and to update the corresponding phone number. In this way, the smart contract provides a secure and tamper-proof solution for tracking the status of mobile devices on the blockchain.

The mobile application is designed to constantly monitor the state of the mobile device by making API calls to the blockchain. If the blockchain indicates that the device has been reported stolen, the application takes action by disabling the device's Wi-Fi and network connections and forcing it into airplane mode. By doing so, the application prevents the thief from using any of the phone's features, rendering it useless until it can be recovered by the rightful owner.

When a mobile phone is marked as stolen on the blockchain through the smart contract and later found, the owner can connect it to a computer via USB and use USB mode to provide data to the phone. This allows the owner to activate the phone again by providing the data through the USB based hotspot.

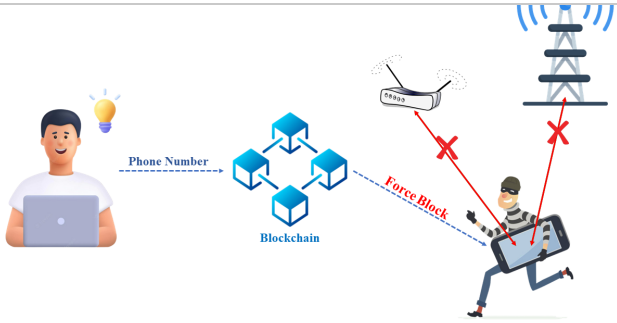


Fig. 3 Working Mechanism of Mobile Theft Prevention using Blockchain

The smart contract is written in both Solidity and JavaScript programming languages that can be deployed on a blockchain network. It is designed to prevent mobile theft by using a mapping function to keep track of mobile devices using their IMEI numbers and phone numbers.

The smart contract consists of six functions that can be called by authorized users.

- `addIMEI()` allows users to add their mobile devices to the blockchain by passing in their IMEI and phone numbers. The function first checks if the IMEI and phone numbers already exist on the blockchain, and if not, it adds the device to the mapping function.
- `activateLost()` is used to activate the lost mode of a mobile device. The function checks if the IMEI number of the device exists on the blockchain and if it does, it sets the value of `isIMEIlost` to true, indicating that the device is lost.
- `deactivateLost()` is used to deactivate the lost mode of a mobile device. The function checks if the IMEI number of the device exists on the blockchain and if it does, it sets the value of `isIMEIlost` to false, indicating that the device is no longer lost.
- `changeIMEI()` allows users to change the IMEI number of their device. The function checks if the old IMEI and phone number exists on the blockchain and if it does, it replaces the old IMEI with the new one.
- `changePhoneNumber()` allows users to change the phone number associated with their device. The function checks if the old IMEI and phone number exists on the blockchain and if it does, it replaces the old phone number with the new one.
- `checkIMEI()` is a view function that allows anyone to check if a particular device is lost by passing in the IMEI number of the device. The function returns true if the device is lost, and false if it is not.

Impact on Users and Mobile Manufacturers

As the world continues to advance technologically, mobile phone theft has become a common issue that affects many people. However, with the implementation of a blockchain-based mobile theft prevention solution, it is possible to mitigate this problem.

For users, this solution provides an added layer of security, ensuring that their mobile devices cannot be easily used if they are lost or stolen. With the mobile application continuously reading the state of the mobile through API calls to the blockchain, it is possible to detect if the mobile is stolen, and take appropriate actions to disable the mobile network, Wi-Fi, and force activate airplane mode, preventing the thief from using any of the phone's functionalities.

For mobile manufacturers, implementing blockchain-based mobile theft prevention solutions will increase customer satisfaction and retention as users are likely to be attracted by the added security feature. This, in turn, will lead to an increase in sales and profits.

Economic and Social Benefits

increase in the amount of money available for investment in other areas of the economy. Additionally, it can also help to reduce insurance premiums for mobile phone owners, leading to savings for consumers.

On a social level, it can help to reduce the fear of being robbed or mugged and reduce the potential for violent confrontations between victims and thieves. This can lead to an overall improvement in public safety and security.

Future Possibilities and Extensions

The implementation of this blockchain-based mobile theft prevention solution has future possibilities and extensions. It can be extended to other mobile devices like laptops, tablets, and smartwatches, further increasing the level of security for users. Additionally, it can be integrated with existing law enforcement agencies to enhance the tracking of lost or stolen mobile devices. This will make it easier for law enforcement to recover stolen mobile devices and increase the likelihood of criminals being brought to justice.

In conclusion, the implementation of blockchain-based mobile theft prevention solutions provides an added layer of security that can greatly benefit mobile phone users, manufacturers, and society at large. The potential for future extensions and possibilities only adds to its value, making it an ideal solution for improving the safety and security of mobile devices.

Yathin Prakash Kethepalli
April 2023

References

[Ali20] Ahmed Ali. Blockchain technology and business use-cases for cost reduction. pages, 12 2020.

[AIT23] Asha Iyengar, Jeff Borsecnik and Team. Perform a remote wipe on a mobile phone. *Microsoft*, 2023. URL: https://learn.microsoft.com/en-us/exchange/clients/exchange-activesync/remote-wipe?view=exchserver-2019.

[Chi23] Chirag. Blockchain: the technology revolutionizing mobile app security. *Appinventive*, 2023. URL: https://appinventiv.com/blog/blockchain-technology-revolutionizing-mobile-app-security/.

[DD21] Utpal Biswas Debashis Das, Sourav Banerjee. A secure vehicle theft detection framework using blockchain and smart contract. *Springer*, 2021. URL: https://doi.org/10.1007/s12083-020-01022-0.

[For22] Savannah Fortis. Samsung uses blockchain-based security for devices in its network. *Cointelegraph*, 2022. URL: https://cointelegraph.com/news/web3-protection-platform-introduces-improved-detection-mechanics-in-latest-update.

[Gob18] Andreas Göbel. Using blockchain to prevent mobile phone theft. *Camelot*, 2018. URL: https://blog.camelot-group.com/2018/12/using-blockchain-to-prevent-mobile-phone-theft/.

[Hen22] Beatriz Henriquez. Mobile theft and loss report - 2020/2021 edition. *PREY Project*, 2022. URL: https://preyproject.com/blog/mobile-theft-and-loss-report-2020-2021-edition.

[Hic22] Jacob Hicks. How to block a stolen iphone with an imei number. *DeviceTests*, 2022. URL: https://devicetests.com/how-to-block-a-stolen-iphone-with-an-imei-number.

[Hom16] Elaine J. Hom. Mobile device security: startling statistics on data loss and data breaches. *ChannelProNetwork*, 2016. URL: https://www.channelpronetwork.com/article/mobile-device-security-startling-statistics-data-loss-and-data-breaches.

[Hua18] Huawei. Huawei blockchain whitepaper. *Huawei*, 2018. URL: https://www.huaweicloud.com/content/dam/cloudbu-site/archive/hk/en-us/about/analyst-reports/images/4-201804-Huawei%20Blockchain%20Whitepaper-en.pdf.

[Ire21] Gwyneth Iredale. The rise of private blockchain technologies. *101 Blockchains*, 2021. URL: https://101blockchains.com/private-blockchain/.

[Mar23]

[Ram21] Murali Ramakrishnan. How blockchain works in cross-border payments. *Springer*, 2021. URL: https://blogs.oracle.com/financialservices/post/how-blockchain-works-in-cross-border-payments-.

[Tre15] Mobile ICT Trends. Erasing your device, blocking your sim card: how to be prepared when your phone gets stolen. *econocom*, 2015. URL: https://blog.econocom.com/en/blog/what-to-do-if-your-mobile-device-gets-stolen-how-do-you-block-your-sim-card-heres-how-to-be-prepared-for-the-loss-or-theft-of-your-mobile/.

Self-Sovereign Identity: Technical Foundations and Applications

Innovation & Ideation

Key Insights

- SSI systems leverage Decentralised Identifiers (DIDs) and Verifiable Credentials (VCs) to enable secure and trustworthy data sharing between issuers, holders, and verifiers, without relying on a centralised authority.
- Privacy-preserving techniques, such as zero-knowledge proofs and selective disclosure, allow SSI users to maintain control over their digital identities and securely share credentials without exposing unnecessary information.
- The implementation of SSI in various industries, including healthcare, land registration, and e-voting, demonstrates the potential for SSI to revolutionise identity management and enhance security, privacy, and trust in these systems.
- While blockchain is not mandatory for SSI systems, its use as a decentralised data registry ensures secure, tamper-evident, and verifiable storage of credentials, contributing to the trustworthiness and reliability of identity management processes.

Introduction

According to World Bank estimates, nearly 850 million people lack an official identity [JC23], and the proliferation of digital devices has made it increasingly essential to possess a verifiable digital identity. This has led to a rise in digital transactions and the need for a secure and reliable identity management system. SSI is emerging as a decentralised alternative to traditional centralised identity management systems, in which identities are cryptographically verifiable. It allows individuals to control their digital identities and share them with trusted parties. Each entity in the SSI system is identified by a unique DID (Decentralised Identifier) as shown below, which can be resolved to reveal information such as the entity's public key and other metadata.

DID breakdown

See also

Find out more about some of the most commonly used DID methods:

- DID:INDY
- DID:UPORT
- DID:SOV

While centralised identities and federated identities offer convenience, control remains with the identity provider [LB15]. User-centric identities such as OpenID [RR06] and OAuth [FKustersS16] improve portability but do not give complete control to the users. SSI is designed to give users full control over their digital identities, and involves guiding principles

Knowledge Proofs, among others.

The three main parties involved in SSI systems are the issuer, holder and verifier, as shown in [Fig. 4]. The issuer issues a cryptographically signed credential to the holder, and the verifier is the entity that confirms the credential's authenticity using a decentralised data registry such as a Blockchain. Holders store their credentials in secure digital wallets and can share them with other parties as needed. The holder can also create a presentation and share it with the verifier on request.

SSI

Self-Sovereign Identity (SSI) is a decentralised digital identity management system which leverages blockchain technology as a data registry, allowing individuals to create, control, and share their identities securely.

Verifiable Credential

A verifiable credential is a digital artefact that provides tamper-evident, cryptographically verifiable proof of an individual's personal information or attributes.

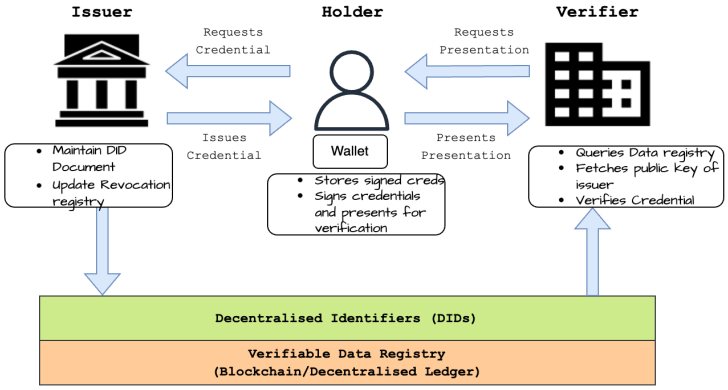


Fig. 4 SSI entities and their relations

See also

This is a verifiable credential issued using the javascript didkit-wasm library.
Click here for full credential


```
{
....
 "id":"urn:uuid:7041d211-72c9-49fe-b6d1-d8b6b94abfe3",
      "type":[
         "VerifiableCredential",
         "BasicProfile"
      ],
      "credentialSubject":{
         "id":"did:pkh:tz:tz1N699qJqMVbMDan2r6R3QYFw42J5ydReh6",
         "alias":"TU Munich",
         "website":"Germany",
         "description":"My name",
         "logo":"Helene-Mayer-Ring 7B"
      },
      "issuer":"did:pkh:tz:tz1QRuc9BkvsBfeSGr6kJ5GCzBsrDjMedvA7",
      "issuanceDate":"2023-01-13T12:24:52.630Z",
....
}
```

- SSI solutions are designed to be blockchain-agnostic and adhere to W3C's specifications.
- The identity wallets (e.g., uPort, Trinsic, Connect.Me) are different from the digital wallets (e.g., Coinbase, Ledger, Trezor) that store cryptocurrencies in the sense that they store and manage DIDs and VCs instead of cryptocurrencies.
- To protect privacy, SSI solutions (e.g. - Hyperledger Indy and Aries) are increasingly using Zero-Knowledge Proofs (ZKPs) to prove the authenticity of credentials without revealing the actual data.
- To facilitate secure communication between different SSI components (issuer-holder-verifier), DIDComm and CHAPI protocols have been developed and are heavily used.

Applications for SSI

SSI in healthcare

Zero-Knowledge Proofs

A zero-knowledge proof (ZKP) is a cryptographic technique that enables one party, the prover, to convince another party, the verifier, of the validity of a statement or the possession of a secret without revealing any additional information about the underlying secret or data.

Recent studies have demonstrated the feasibility of using zero-knowledge proofs to disclose information selectively, such as proof of vaccination status, without revealing users' identities. These studies have employed interoperable open-source tools to implement these systems globally at a minimal cost. Schlatt et al. [SSFU22] illustrates how a customer can leverage a Zero-knowledge Proof concept called 'blinded link secret' to disclose information selectively. Similarly, Barros et al. [dVBSFCustodio22] implemented a prototype of an application for presenting proof of vaccination without revealing users' identities. Furthermore, it uses interoperable open-source tools across countries to implement this system globally at a minimal cost for each country's government. The NHS Digital Staff Passport solution [LC22] employs the Sovrin Network as a public key infrastructure (PKI) to manage verifiable credentials for staff onboarding. Hospitals register on the network and use their private keys to sign credentials, while staff members utilise Evernym's Connect.Me SSI digital wallet app to store and share credentials.

SSI in land registration

Shuaib et al. [SHU+22] suggest that a blockchain-based land registry system can be combined with a self-sovereign identity (SSI) solution to provide a secure and efficient identity management system for landowners. Three existing SSI solutions, Everest, Evernym, and uPort [Ame22], were evaluated based on SSI principles [All16] to determine their compliance and effectiveness in addressing identity problems in land registry systems. The Everest platform was found to be the most compliant with the SSI principles, whereas Evernym and uPort had some limitations in terms of interoperability and user control.

SSI in e-voting

Estonia is one of the few countries in the world that have managed to make e-voting a reality [SS22]. Sertkaya et al. [SRR22] proposed an EIV-AC scheme that integrates the Estonian Internet voting (EIV) scheme with anonymous credentials (AC) based on self-sovereign identity (SSI). The use of SSI-based anonymous credentials enables voters to prove their eligibility to vote without revealing their identity. The zero-knowledge proof of identity is used to prove that the voter has the right to vote without revealing any additional information. The EIV-AC scheme enhances the security and privacy of the EIV scheme, making it more compliant with privacy-enhancing and data minimisation regulations.

SSI in finance and identity management

Innovative proposals surrounding digital identity management systems, such as Kiva's architecture, suggest the development of an insurance marketplace for consequential damages related to identity claims. This marketplace could offer a market mechanism for evaluating the accuracy, trustworthiness, and usefulness of various identity claims, subsequently allowing lenders to confidently underwrite loans, even to individuals lacking formal credit history.

subsequent lenders.

Ferdous et al. [FIP23] introduce a *SSI4Web* framework and demonstrate how an SSI-based framework can be designed for web services and offer a secure and passwordless user authentication mechanism, which eliminates the need for users to remember passwords and reduces the risk of password breaches.

Can SSI work without Blockchain?

Blockchain is one of many options when implementing a Self-sovereign Identity system. Alternatives like IPFS, Public-key cryptography and even traditional Certificate Authorities can be used to implement SSI. However, the main advantage of using Blockchain is that it provides a decentralised and immutable ledger that can be used to store and verify credentials.

Conclusion

Self-sovereign identity can potentially revolutionise various industries, including healthcare, voting systems and many more. However, as research and development in SSI progress, it will be crucial to address interoperability, scalability, and usability challenges to realise SSI's potential in a global context fully.

Parshant Singh
April 2023

References

[All16] Christopher Allen. The path to self-sovereign identity. *Life With Alacrity*, 2016. URL: http://www.lifewithalacrity.com/2016/04/the-path-to-self-soverereign-identity.html.

[Ame22] New America. Three self-sovereign identity platforms to watch. *New America*, 2022. URL: https://www.newamerica.org/future-land-housing/reports/nail-finds-hammer/three-self-sovereign-identity-platforms-to-watch/.

[BCHR+19] Jorge Bernal Bernabe, Jose Luis Canovas, Jose L Hernandez-Ramos, Rafael Torres Moreno, and Antonio Skarmeta. Privacy-preserving solutions for blockchain: review and challenges. *IEEE Access*, 7:164908–164940, 2019.

[dVBSFCustodio22] Mauricio de Vasconcelos Barros, Frederico Schardong, and Ricardo Felipe Custódio. Leveraging self-sovereign identity, blockchain, and zero-knowledge proof to build a privacy-preserving vaccination pass. *Blockchain, and Zero-Knowledge Proof to Build a Privacy-Preserving Vaccination Pass*, 2022.

[FIP23] Md Sadek Ferdous, Andrei Ionita, and Wolfgang Prinz. Ssi4web: a self-sovereign identity (ssi) framework for the web. In *Blockchain and Applications, 4th International Congress*, 366–379. Springer, 2023.

[FKustersS16] Daniel Fett, Ralf Küsters, and Guido Schmitz. A comprehensive formal security analysis of oauth 2.0. In *Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security*, 1204–1215. 2016.

[JC23] CLAIRE CASHER JULIA CLARK, ANNA DIOFASI. 850 million people globally don't have id—why this matters and what we can do about it. *World Bank*, 2023. URL: https://blogs.worldbank.org/digital-development/850-million-people-globally-dont-have-id-why-matters-and-what-we-can-do-about.

[LC22] Mary Lacity and Erran Carmel. Implementing self-sovereign identity (ssi) for a digital staff passport at uk nhs. *University of Arkansas*, 2022.

[LB15] Maryline Laurent and Samia Bouzefrane. *Digital identity management*. Elsevier, 2015.

[RR06] David Recordon and Drummond Reed. Openid 2.0: a platform for user-centric identity management. In *Proceedings of the second ACM workshop on Digital identity management*, 11–16. 2006.

[SSFU22] Vincent Schlatt, Johannes Sedlmeir, Simon Feulner, and Nils Urbach. Designing a framework for digital kyc processes built on blockchain-based self-sovereign identity. *Information & Management*, 59(7):103553, 2022.

[SRR22] Isa Sertkaya, Peter Roenne, and Peter YA Ryan. Estonian internet voting with anonymous credentials. *Turkish Journal of Electrical Engineering and Computer Sciences*, 30(2):420–435, 2022.

[SHU+22] Mohammed Shuaib, Noor Hafizah Hassan, Sahnius Usman, Shadab Alam, Surbhi Bhatia, Arwa Mashat, Adarsh Kumar, and Manoj Kumar. Self-sovereign identity solution for blockchain-based land registry system: a comparison. *Mobile Information Systems*, 2022:1–17, 2022.

Sharding: A Panacea for Blockchain Scalability Challenges?

Innovation & Ideation

Key Insights

- Sharding is a promising scaling technique for blockchains, dividing the network into smaller partitions called shards to process transactions in parallel, thus increasing throughput.
- Sharding approaches in blockchain systems vary, with solutions like Ethereum 2.0 using multiple shard chains coordinated by a beacon chain, and others, such as Near Protocol's Nightshade, opting for processing data chunks in a single blockchain with different validator sets.
- Sharding implementation faces challenges in security, cross-shard communication, and data availability. These require solutions like random validator assignment, transaction receipts, and erasure coding.
- While sharding offers potential scalability improvements, layer 2 solutions like ZK-Rollups and Optimistic Rollups remain the preferred short-term scaling methods until sharding proves its ability to handle high transaction volumes.

As the adoption of blockchain technology increases, scalability remains the central challenge and a major obstacle for blockchain to be adopted by mainstream industries. Bitcoin can only process 7 transactions per second (TPS), while the Ethereum blockchain can only process 15 TPS. Although after the Merge of Ethereum 1.0 into Ethereum 2.0, the TPS of Ethereum 2.0 is expected to reach 100,000 TPS, gas fees remain a major issue. Ethereum has been relying on ZK-rollups to scale the network, but rollups are only a short-term solution because of interoperability issues with other blockchains since they are mainly Ethereum-focussed. Therefore, the blockchain community is actively looking for a solution to the scalability problem.

What is Sharding?

Sharding, originally a database design principle, is now being considered a promising solution to overcome the scalability challenges of blockchain systems. This scaling technique divides the blockchain network into smaller partitions called shards, each responsible for processing a subset of transactions. This allows the blockchain to process more transactions in parallel, thereby increasing the throughput of the system.

There are 2 common techniques blockchains implement to improve throughput:

- Delegate all the computation to a small set of powerful nodes; (e.g., Algorand, Solana)
- Each node in the network only does a subset of the total work (Sharding). Ethereum, Near, Hedera use this technique.

ZK-Rollups

ZK-Rollups in Ethereum are a Layer 2 scaling solution that uses zero-knowledge proofs to bundle multiple transactions into a single proof on the main chain. This reduces on-chain data storage and gas costs while maintaining security. As a result, ZK-Rollups enable higher throughput, lower fees, and faster confirmations for Ethereum transactions while preserving privacy and decentralization.

Sharding in Blockchains vs Traditional Databases

The sharding techniques used in traditional databases cannot be directly applied to blockchains because of the following reasons:

- Blockchains rely on Byzantine Fault Tolerance (BFT) consensus protocols which have been shown to be a scalability bottleneck.
- Distributed databases depend on highly available transaction coordinators for atomicity and isolation assurance; however, blockchain coordinators could exhibit malicious behaviour.
- In a distributed database, any node can belong to any shard, but a blockchain must assign nodes to shards in a secure manner to ensure that no shard can be compromised by the attacker.

Different Sharding Approaches

Huang et al. [HPZ+22] proposed a new cross-shard blockchain protocol called BrokerChain that aims to address the issue of hot shards and reduce the number of cross-shard transactions. They showed this protocol outperforms other state-of-the-art sharding methods in terms of transaction throughput, confirmation latency and queue size of transaction pool. Tennakoon et al. [TG22] propose a blockchain sharding protocol with dynamic sharding where smart contract invocations stored in blocks reconfigure the sharding. This protocol is effective because it improves the efficiency of the blockchain, preventing resource wasting by closing the shards that are not processing as many transactions or are idle. There have been a few proposed sharded blockchains such as Elastico [LNZ+16], OmniLedger [KKJG+18] and RapidChain [ZMR18]. Nonetheless, such systems are predominantly constrained to cryptocurrency use cases in open (or permissionless) environments. Due to their reliance on the unspent transaction output (UTXO) model—a simplistic data structure—these methods lack generalizability for applications beyond Bitcoin [DDL+19]. So we will focus on more general-purpose blockchains such as Ethereum and Near Blockchain.

Hot Shards

Hot shards are shards that are experiencing a high volume of transactions, which can negatively impact the performance and security of the blockchain system.

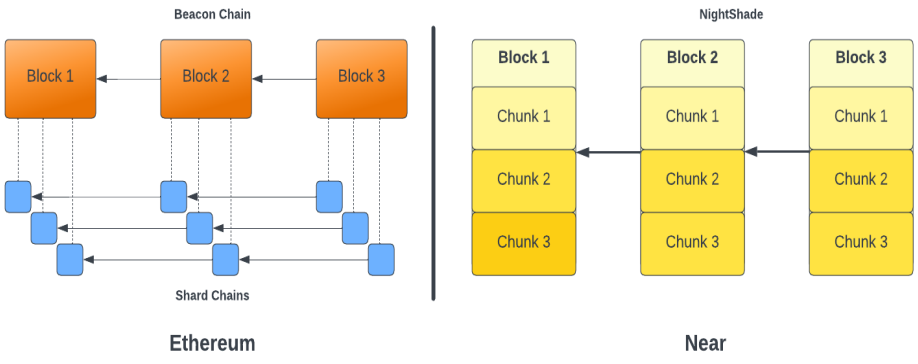


Fig. 5 Sharding in Ethereum vs Near Blockchain

Sharding in Ethereum

In Ethereum, data is distributed among several "shard chains" ([Fig. 5]). Each of these shard chains submits a record of transactions to the "beacon chain" or "coordinating layer", which coordinates and manages the shards by maintaining synchronization and ensuring a common ledger. The shards receive sets of transactions from the mempool. Under the

[KTTI22].

Sharding in Near Blockchain

Near's sharding technique is called "Nightshade" [Nea20a]. Although the full implementation is still in progress, the idea is that instead of having multiple subchains with a single beacon chain, the data is divided into smaller partitions called chunks. Each chunk is processed by a different set of validators. The validators are randomly assigned to chunks, and the assignment is done in a way that the same validator is not assigned to multiple chunks, as shown in [Fig. 5]. At present, the Near blockchain has 4 shards, and the eventual plan is to have 100 shards {cite}`near roadmap.

Sharding Challenges

The main issue with sharding is that it is extremely complicated to implement, as it opens up possibilities of new attack vectors and security challenges. The following are some of the challenges that need to be addressed before sharding can be implemented in a blockchain system.

Security

In a 10-shard system, each shard's security is reduced by a factor of 10 due to separate validator sets. Upon hard-forking a non-sharded chain with X validators into a sharded chain, each shard has X/10 validators. Consequently, compromising one shard necessitates corrupting only 5.1% (51% / 10) of the total validators. This is a significant reduction in security. To overcome this challenge, Ethereum uses a beacon chain to randomly assign validators to shards. Blockchains like Near and Algorand use Verifiable Random Functions (VRFs) to assign validators to shards. This ensures that the validators are randomly assigned to shards and the same validator is not assigned to multiple shards.

Hafid et al. [HHS22] propose a Probabilistic Generating Function Analysis (PGFA) approach as an effective and tractable method to analyze the security of sharding-based blockchain protocols. They conclude that an increase in the number of Sybil IDs (unique nodes), network size, and ID Selection Pool (random pool from which nodes are randomly selected to be assigned to shards) size results in a higher failure probability, compromises network security and can lead to shard takeover attacks.

Cross-Shard Communication

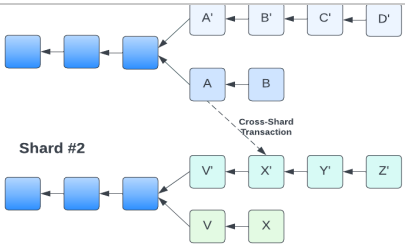
VRF

Verifiable Random Functions (VRFs) are cryptographic primitive that allows a user to generate a random number that can be verified by anyone.

As the network gets divided into multiple shards, it is important to ensure that the shards can communicate with each other to maintain consistency and interoperability. As seen in [Fig. 6], this can be problematic if there is forking within the shards and the block issuing the transaction is not included in the canonical chain. Both Near and Ethereum overcome this challenge by exchanging receipts between the shards. The receipts are used to prove that a transaction has been executed on a shard [Nea20b] and the corresponding transaction can be executed on the other shard. In Hedera Hashgraph, which uses a gossip protocol to exchange information between shards, each shard maintains a queue of outgoing messages for other shards. Messages are sent from one shard to another through nodes randomly contacting each other, along with proof of consensus. The process continues until the receiving shard confirms message processing with an updated sequence number in its shared state [Hed20]. Instead of receipts, Hedera uses sequence numbers which are maintained by a shard for each other shard as a proof of latest execution message.

Sequence Numbers

In the context of Hedera's multi-shard system, sequence numbers are 64-bit identifiers assigned to inter-shard messages to keep track of their order. When a transaction involves resources from different shards, it triggers inter-shard messages. Each shard maintains a queue



queue is assigned a unique sequence number.

Fig. 6 Cross-Shard Communication

Data Availability

The data availability problem relates to the difficulty of ensuring that all necessary data for verifying a block's validity is accessible to all participants in the network. For instance, a light client cannot access complete block data and thus cannot verify the validity of data. To overcome this problem, erasure coding is used. If the light client can retrieve a sufficient number of chunks of data, it can reconstruct the original data and verify the block's validity. Ethereum and Near are currently using this approach.

Erasure Codes

Erasure codes allow a piece of data M chunks long to be expanded into a piece of data N chunks ("chunks" can be of arbitrary size), such that any M of the N chunks can be used to recover the original data.

Sharding in Hedera

As per Hedera network's whitepaper [Hed20], it starts as a single shard composed of nodes managed by Governing Council Members. As the council grows, the network will transition to a multi-shard system to enhance performance, enable parallel consensus, and maintain asynchronous Byzantine fault tolerance. Nodes will be randomly assigned to shards by a master shard, balancing hbar distribution and minimizing centralization risks. Shards will trust and collaborate, allowing seamless cross-shard transactions. Nodes will communicate via push messages, maintaining queues for inter-shard messaging. Transactions involving multiple shards will be consistently recorded in each shard's state, ensuring ledger-wide coherence and integrity. The master shard will be responsible for maintaining the overall state of the network, including the hbar supply and the hbar distribution across shards.

Conclusion

Sharding is the most promising solution to overcome the scalability challenges of blockchain systems. However, although Ethereum and Near have made significant progress in implementing sharding, it is still not time-tested and it remains to be seen whether these blockchains will be able to bear a load of transactions volume when scenarios such as DeFi boom or NFT craze happen again. Until then, layer 2 solutions such as ZK-Rollups and Optimistic Rollups will continue to be the preferred scaling solutions for blockchain systems.

Parshant Singh
May 2023

References

[DDL+19] Hung Dang, Tien Tuan Anh Dinh, Dumitrel Loghin, Ee-Chien Chang, Qian Lin, and Beng Chin Ooi. Towards scaling blockchain systems via sharding. In *Proceedings of the 2019 international conference on management of data*, 123–140. 2019.

[HHS22] Abdelatif Hafid, Abdelhakim Senhaji Hafid, and Mustapha Samih. A tractable probabilistic approach to analyze sybil attacks in sharding-based blockchain protocols. *IEEE Transactions on Emerging Topics in Computing*, 2022.

[Hed20] Hedera. Hedera hashgraph whitepaper. *Hedera*, 2020. URL: https://hedera.com/hh_whitepaper_v2.1-20200815.pdf.

IEEE Conference on Computer Communications, 1968–1977. IEEE, 2022.

[KKJG+18] Eleftherios Kokoris-Kogias, Philipp Jovanovic, Linus Gasser, Nicolas Gailly, Ewa Syta, and Bryan Ford. Omniledger: a secure, scale-out, decentralized ledger via sharding. In *2018 IEEE Symposium on Security and Privacy (SP)*, 583–598. IEEE, 2018.

[KTTI22] Alexander Kudzin, Kentaroh Toyoda, Satoshi Takayama, and Atsushi Ishigame. Scaling ethereum 2.0 s cross-shard transactions with refined data structures. *Cryptography*, 6(4):57, 2022.

[LNZ+16] Loi Luu, Viswesh Narayanan, Chaodong Zheng, Kunal Baweja, Seth Gilbert, and Prateek Saxena. A secure sharding protocol for open blockchains. In *Proceedings of the 2016 ACM SIGSAC conference on computer and communications security*, 17–30. 2016.

[Nea20a] Near. Near nightshade whitepaper. *Near*, 2020. URL: https://near.org/papers/nightshade/.

[Nea20b] Near. Near runtime spec. *Near*, 2020. URL: https://nomicon.io/RuntimeSpec/Receipts.

[TG22] Deepal Tennakoon and Vincent Gramoli. Dynamic blockchain sharding. In *5th International Symposium on Foundations and Applications of Blockchain 2022 (FAB 2022)*. Schloss Dagstuhl-Leibniz-Zentrum für Informatik, 2022.

[ZMR18] Mahdi Zamani, Mahnush Movahedi, and Mariana Raykova. Rapidchain: scaling blockchain via full sharding. In *Proceedings of the 2018 ACM SIGSAC conference on computer and communications security*, 931–948. 2018.