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.

Introduction

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

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

top 5 wallet addresses accounting for 42.1% and 12.05%, respectively.

yield opportunities for cryptocurrency assets, and provide users with a way to optimize their returns on investment.

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.

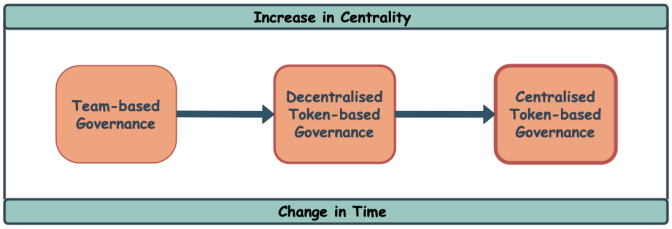

Fig. 1 The Tendency for Centralisation in DeFi Governance.

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 to sybil attacks. The bond voting mechanism issues 'voting bonds' to voters, which essentially requires a commitment to stake an amount of 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 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.

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]**

[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.

[S+] K Stroponiati and others. Decentralized governance in defi: examples and pitfalls. squarespace. retrieved december 30, 2022.

[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 that leverages zk-SNARK technology has been proposed. This provides a secure, trustless cross-chain bridge, marking the first implementation of Zero-Knowledge Proofs (ZKP) in a decentralised trustless bridge system.
- To facilitate secure cross-chain interoperability, a Hash time-lock scheme that does not rely on external trust ensuring transaction security is introduced.
- To mitigate token transfer risks, a series of protocols called TrustBoost using smart contracts to achieve a consensus on top of consensus mechanism is proposed.
- In a bid to boost interoperability, a groundbreaking framework has been proposed that not only mitigates security risks inherent in cross-blockchain technology but also simplifies the process of identifying key assumptions and characteristics.

Introduction

Blockchain technology has been lauded for its potential to disrupt various industries, given its unique properties such as decentralisation, 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 summarise the recent research findings.

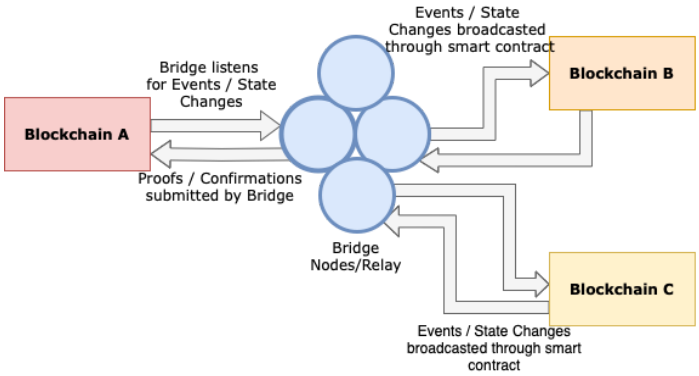

Fig. 2 Communication through a Blockchain Bridge.

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 the Ronin bridge, making it the largest attack in the history of DeFi [KY22]. According to blockchain analytics firm Chainalysis, until August 2022 recurring attacks against bridges have cost users around 1.4 billion USD [Bro22]. In 2022 attacks on bridges accounted for 69% of total funds stolen [Cha22].

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 necessitates the development of novel security models and protocols to protect against potential attack vectors arising from cross-chain communication and is particularly true for blockchain bridges that need to uphold the integrity and security of transactions across disparate networks. Most existing solutions rely on the trust assumptions of committees, which lowers security significantly.

Xie et al. [XZC+22] 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. zkBridge uses the zk-SNARK protocol to achieve both reasonable proof generation times and on-chain verification costs. 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 decentralised trustless bridge.

risks, enhancing the decision-making process, and minimising design mistakes and performance issues. It recognises 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. [KRDO17] on proof-of-stake blockchain protocols is of significant relevance. They outlined a novel cryptographic mechanism that provides transactional security while ensuring transparency.

To mitigate the reliance on external trust assumptions, Li et al. [LYY+23] in their paper proposed a Hash time-lock scheme that utilises 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.

Sidechain

A 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 about data structures and representations, at which point it can be used to implement multiple, interoperable versions of a programme.

Li et al. [LYY+23], identified a high-security and highly scalable option as the 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 [F+20]. 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 [Szt15].

Ding et al. [DDJ+18], 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. [HLP19], 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. [ZHL+19] discussed the scalability-security trade-off in their study on interoperable assets. There is a need for a balance that allows for scalability without jeopardising 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. [ZLZ20] 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, require the weaker blockchain to give up sovereignty. Wang et al. [WSK+22] 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

References

bridges.html.

[Cha22] ChainAnalysis. Cross-chain bridge hacks emerge as top security risk, chainalysis. *ChainAnalysis*, 2022. URL: https://blog.chainalysis.com/reports/cross-chain-bridge-hacks-2022/.

[DDJ+18] Donghui Ding, Tiantian Duan, Linpeng Jia, Kang Li, Zhongcheng Li, and Yi Sun. Interchain: a framework to support blockchain interoperability. *Second Asia-Pacific Work. Netw*, 2018.

[F+20] P Frauenthaler and others. Leveraging blockchain relays for cross-chain token transfers. 2020. *URL: https://www. dsg. tuwien. ac. at/projects/tast/pub/tast-white-paper-8. pdf. White Paper, Technische Universität Wien. Version*, 2020.

[HLP19] Thomas Hardjono, Alexander Lipton, and Alex Pentland. Toward an interoperability architecture for blockchain autonomous systems. *IEEE Transactions on Engineering Management*, 67(4):1298–1309, 2019.

[KY22] Sam Kessler and Sage D. Young. Ronin attack shows cross-chain crypto is a bridge too far, coindesk latest headlines. *CoinDesk*, 2022. URL: https://www.coindesk.com/layer2/2022/04/05/ronin-attack-shows-cross-chain-crypto-is-a-bridge-too-far/.

[KRDO17] Aggelos Kiayias, Alexander Russell, Bernardo David, and Roman Oliynykov. Ouroboros: a provably secure proof-of-stake blockchain protocol. In *Advances in Cryptology–CRYPTO 2017: 37th Annual International Cryptology Conference, Santa Barbara, CA, USA, August 20–24, 2017, Proceedings, Part I*, 357–388. Springer, 2017.

[LYY+23](1,2) Taotao Li, Changlin Yang, Qinglin Yang, Siqi Zhou, Huawei Huang, and Zibin Zheng. Metaopera: a cross-metaverse interoperability protocol. *arXiv preprint arXiv:2302.01600*, 2023.

[PBHouM22] Babu Pillai, Kamanashis Biswas, Zhé Hóu, and Vallipuram Muthukkumarasamy. Cross-blockchain technology: integration framework and security assumptions. *IEEE Access*, 10:41239–41259, 2022.

[Szt15] Paul Sztorc. Drivechain-the simple two way peg. 2015.

[WSK+22] Xuechao Wang, Peiyao Sheng, Sreeram Kannan, Kartik Nayak, and Pramod Viswanath. Trustboost: boosting trust among interoperable blockchains. *arXiv preprint arXiv:2210.11571*, 2022.

[XZC+22] Tiancheng Xie, Jiaheng Zhang, Zerui Cheng, Fan Zhang, Yupeng Zhang, Yongzheng Jia, Dan Boneh, and Dawn Song. Zkbridge: trustless cross-chain bridges made practical. *arXiv preprint arXiv:2210.00264*, 2022.

[ZHL+19] Alexei Zamyatin, Dominik Harz, Joshua Lind, Panayiotis Panayiotou, Arthur Gervais, and William Knottenbelt. Xclaim: trustless, interoperable, cryptocurrency-backed assets. In *2019 IEEE Symposium on Security and Privacy (SP)*, 193–210. IEEE, 2019.

[ZLZ20] Jianbiao Zhang, Yanhui Liu, and Zhaoqian Zhang. Research on cross-chain technology architecture system based on blockchain. In *Communications, Signal Processing, and Systems: Proceedings of the 8th International Conference on Communications, Signal Processing, and Systems 8th*, 2609–2617. Springer, 2020.

Mobile Theft Prevention using Blockchain

Industry Perspective

> **Key Insights**
>
> - 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].

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].
- **Secure and private:** The proposed model uses a private blockchain network that connects the mobile manufacturing companies and their nodes [Ire21]. 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.

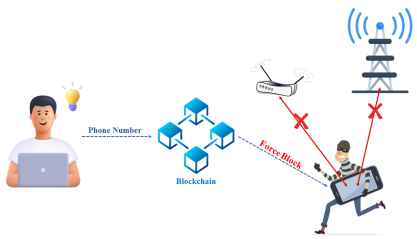

Fig. 3 Working Mechanism of Mobile Theft Prevention using Blockchain

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.

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

The implementation of blockchain-based mobile theft prevention solutions will lead to a reduction in mobile phone theft and related crimes. This will result in a decrease in the costs of replacing stolen or lost mobile phones, and a corresponding 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.

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

[Mar23] Karen Marcus. The 8 best phone tracker apps of 2023. *Lifewire*, 2023. URL: https://learn.microsoft.com/en-us/exchange/clients/exchange-activesync/remote-wipe?view=exchserver-2019.

[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 around security, controllability, and portability. In addition to providing total control, Bernabe et al. [BCHR+19] presented a classification of techniques for maintaining privacy in SSI, which included Secure Multiparty Computation and Zero-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.

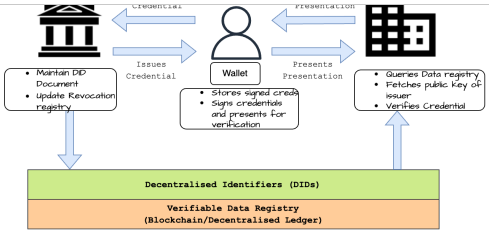

Fig. 4 SSI entities and their relations

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",
....
}
```


Nitty Gritty of SSI

- 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

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.

SSI in healthcare

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

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. Furthermore, by leveraging blockchain technology in a semi-decentralised identity management system, banks and microfinance lenders could underwrite the risk associated with issuing identity credentials, facilitating de-risking for 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.

[**SS22]** Cyber Security and Society. Estonia leads world in making digital voting a reality. *Cyber Security and Society*, 2022. URL: https://www.ft.com/content/b4425338-6207-49a0-bbfb-6ae5460fc1c1.

[**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.

Soulbound Tokens (SBTs)

Innovation & Ideation

- Decentralised Society (DeSoc) serves as an innovative solution that encourages a trust-based, cooperative, bottom-up strategy in constructing resilient networks, thereby enhancing the potential of Web3.
- Soulbound tokens (SBTs), as non-transferable assets, improve the provenance and reputation in the Decentralised Society (DeSoc) and provide a versatile representation of digital identities.
- SBTs have the potential to redefine digital identity verification due to their non-transferable nature, allowing them to authenticate factual records, establish digital inheritance plans, and prevent Sybil attacks in Decentralised Autonomous Organisations.
- SBTs offer functional solutions in various sectors such as finance, real estate, and healthcare, promoting transparency, security, and innovation across these industries.
- Despite the significant advancements that SBTs bring to digital identity systems, they also face obstacles concerning privacy, security, and interoperability.

Introduction

Web3 has largely been anonymous for its users, due to its founding principles, which are deeply rooted in privacy and decentralisation. However, the lack of ability to confirm individual identities, their properties, and affiliations has posed a challenge for blockchain adoption in some industries. Soulbound tokens (SBTs) are set to bridge this identity gap inherent in Web3, facilitating the formation of trusted relationships. Soulbound tokens can be issued by any entity, be it DAOs, academic institutions, DeFi firms, or employers, to denote membership, authentication or certification, or event participation. Moreover, soulbound tokens can utilise these links between individuals and various entities to provide a more comprehensive picture of distinct user identities and their roots. The reputation of the issuing entity is transferred via SBTs to the wallets or individuals who hold them. The more prestigious the issuing body, the higher the standing of the individual in possession of a soulbound token.

As an individual's connections with different entities grow, so does their unique identity and reputation. Soulbound tokens capitalise on this network of connections to construct verifiable identities for souls. NFTs will serve as proof of ownership, and SBTs as proof of character [CG22].

Web3

Web3, short for Web 3.0, is the third generation of internet services for websites and applications that incorporate blockchain-based and decentralised processes. It emphasises a user-centric online experience where data ownership and control is returned to the individual, as opposed to being centralised in large tech companies.

DAOs

A Decentralised Autonomous Organization (DAO) is a blockchain-based system governed by rules encoded as computer programmes known as smart contracts, with decision-making authority distributed among its members.

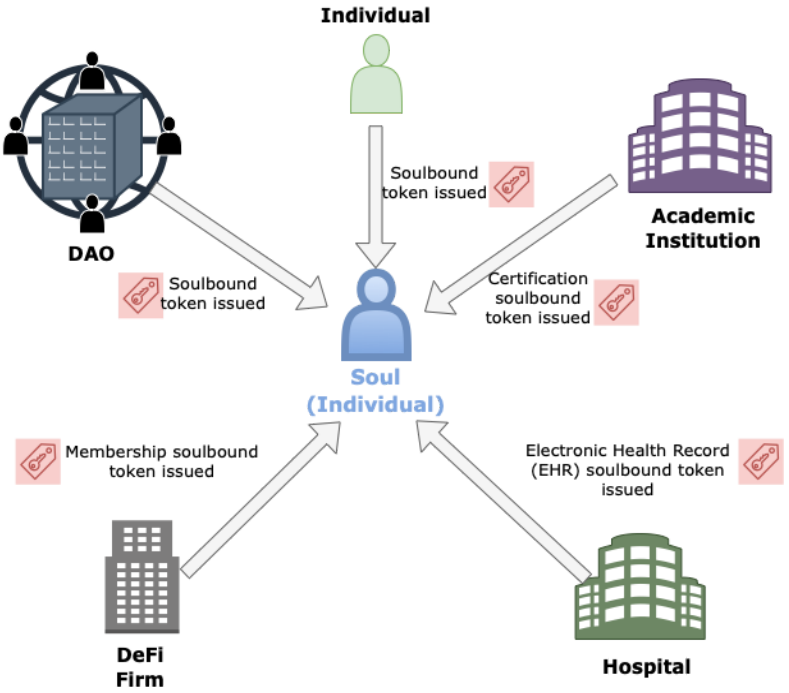

Fig. 5 Soulbound Token Issuance in DeSoc.

Moving towards a Decentralised Society (DeSoc)

Web3 aims to revolutionise society beyond just financial systems, but its current lack of mechanisms to represent human identities and relationships in virtual worlds leads to issues like Sybil attacks, collusion, and an inclination towards hyper-financialization [WOB22]. To counter this, Weyl et al. [WOB22] proposed the concept of a Decentralised Society (DeSoc), an approach fostering complex and diverse relationships across digital and physical realities. It is built on trust and cooperation while also correcting for biases and tendencies to overcoordinate.

Sybil Attack

A Sybil attack is a type of security threat in decentralised networks where a single entity creates multiple fake identities (Sybils) to gain undue influence or control. These attacks can disrupt the functioning of the network by undermining consensus mechanisms.

Collusion Attack

growth. DeSoc recommends treating networks as partially and collectively shared goods, applying governance mechanisms that balance trust and cooperation, while checking for collusion and capture. This model supports a bottom-up approach in building, participating in, and governing networks. Consequently, it creates structures resilient to Sybil and vampire attacks and collusion, and promotes plural networks that provide widespread benefits, agreed upon by diverse members.

The strength of DeSoc lies in fostering broader cooperation by encouraging the creation and intersection of nested networks across the physical and digital realms. Building on trust, it allows for the establishment of resilient plural network goods. This approach enables Web3 to resist short-term financialization and cultivate a future with increasing returns across diverse social connections.

> Note
>
> **Differences between soulbound tokens (SBTs) and regular non-fungible tokens (NFTs)**
>
> - Soulbound Tokens (SBTs) are unique in that they are non-transferable and exhibit public transparency.
> - Regular Non-Fungible Tokens (NFTs), on the other hand, are unique, non-interchangeable tokens that can represent digital assets, such as digital art.
> - Both SBTs and NFTs can serve as a means to authenticate and identify products or records.
> - SBTs stand out in their ability to serve as a form of permission, authorisation, and access to legal documents, binding the token to a specific identity.
> - Conversely, NFTs can be utilised as tickets granting access to exclusive events, without requiring identity verification, as they can be freely transferred between parties.

network conspire together to manipulate the system for their own advantage. This can happen in proof-of-stake or proof-of-work blockchain systems where enough nodes, typically over 50%, are controlled by a colluding group. This allows them to control the validation of transactions, potentially allowing them to double-spend, block transactions, or manipulate the blockchain in other ways. This is often referred to as a 51% attack.

Hyper-financialization

Hyper-financialization refers to the dominance of financial markets, institutions, and elites in the economy.

Vampire Attack

In the context of decentralised finance (DeFi) and blockchain, a vampire attack is a strategy where a new protocol aims to drain liquidity and users from an existing one. This is often done by offering higher rewards or better incentives on the new platform, incentivizing users of the old platform to migrate their assets.

Functionality

A distinct and pivotal characteristic of Soulbound tokens (SBTs) is their inherent non-transferability. Unlike existing NFTs and token standards like the fungible ERC-20 or non-fungible ERC-721, which are built to hold market value and can be sold or transferred between wallets, SBTs are uniquely tied to Souls and therefore are not designed for selling or transferring [Tak23].

SBTs are issued and held within unique accounts known as Souls, which serve as a vessel for these tokens and play a crucial role in establishing provenance and reputation. Souls can denote various entities, ranging from individuals to organisations, companies, and more. It's noteworthy that in a decentralised society (DeSoc), Souls are not required to have a direct human equivalence, meaning a single person can be associated with multiple Souls. Unlike regular NFTs, soulbound tokens (SBTs) are a concept of non-transferable assets [Tit22]. Once issued, they belong to a specific identity [Hil22].

This flexibility can manifest in a multitude of ways. For instance, an individual might have a variety of Souls representing different aspects of their identity - their credentials, medical records, and so on [Tak23].

Potential applications of SBTs

Soulbound Tokens (SBTs) are a revolutionary concept in the realm of blockchain technology, enabling the creation of verifiable, non-transferable digital records tied to an individual's identity or "soul". With their immutable and decentralised characteristics, these tokens offer several potential applications that span numerous industries and societal structures. From authenticating factual records, devising digital inheritance plans, and facilitating alternative credit systems to preventing Sybil attacks in Decentralised Autonomous Organisations (DAOs), enhancing trust in online property rentals, and securing the management of healthcare records, SBTs are primed to reshape the digital world. The following sections detail some of the most promising applications of Soulbound Tokens in diverse fields.

Verifying Authenticity of Factual Records

Soulbound Tokens can be used to confirm the authenticity of supposed factual records, such as photos and videos. As deep fake technology continues to advance, it's becoming increasingly difficult for both humans and algorithms to determine the truth through direct examination. While blockchain inclusion enables us to trace the time a particular work was made, SBTs would enable us to trace the social provenance, giving us rich social context to the Soul that issued the work, their constellation of memberships, aliations, credentials and their social distance to the subject [WOB22].

Digital Inheritance Planning

Soulbound Tokens (SBTs) can be employed as a mechanism to confirm a user's existence. Considering SBT use cases, a digital inheritance plan could be created where the testator generates SBTs for executors, guardians, and beneficiaries, transferring these tokens to their respective wallets. This process not only verifies the existence of all involved parties but also bolsters the security of the testator's digital assets [GCOGI23].

Alternative Credit Systems

An ecosystem of Soulbound Tokens (SBTs) could provide an alternative to traditional credit systems, using education credentials, work history, and rental contracts to build a credit history. Non-transferable SBTs representing loans could be used as non-seizable reputation-based collateral. The system would prevent loan evasion and promote transparency in lending markets, reducing reliance on centralised credit-scoring. Ultimately, this could enhance lending algorithms and facilitate lending within social networks [WOB22].

Soulbound Tokens (SBTs) can also be used to prevent Sybil attacks in Decentralised Autonomous Organisations (DAOs) by differentiating between unique users and potential bots based on their SBTs. More reputable SBT holders can be given more voting power. Specific "proof-of-personhood" SBTs can be issued to assist other DAOs in Sybil resistance. Additionally, vote weight can be adjusted based on correlations among SBTs held by voting participants [WOB22].

Enhancing Trust in Online Property Rental

The economic growth potential of the real estate sector is significant, encompassing diverse industries from retail to housing services. The digitization of real estate, however, has invited several challenges, notably in the form of scams targeting landlords and tenants. To address this issue, a blockchain-based property rental platform is proposed. This platform will utilise Soulbound Tokens (SBTs) to verify the credibility and reputation of users, providing security against online rental fraud. A non-transferable, non-fungible token is provided to the new user that records their reputation across their time on the website. Property listings will be structured as smart contracts on the platform, ensuring secure and immutable transaction terms between landlords and tenants. This could drastically reduce fraud, enhance trust, and potentially transform the online rental industry [SKSK23].

Decentralised Dispute Resolution

Decentralised dispute resolution platforms could use soulbound tokens, tied to an arbitrator's real identity, as a mechanism to enhance system integrity. These tokens, earned through completing tasks, safeguard against system manipulation such as whitewashing or Sybil attacks. Additionally, the tokens represent an arbitrator's decision-making accuracy, not their financial capacity. Arbitrators may need to provide credentials like licences or certificates, along with proof of identity. This data would be presented to a decentralised committee, which upon verification, associates a long-term secret key with the arbitrator's identity and the soulbound token, ensuring transparency and confidentiality [UY22].

Recording Employment History and Professional Qualifications

Soulbound Tokens (SBTs) can be utilised to record employment history and professional qualifications. Employers can distribute these tokens to reflect an employee's work experience, project involvement, accomplishments, and other pertinent details. When seeking new employment opportunities or during job interviews, employees can present these SBTs. Thus, SBTs function as tangible evidence of professional skills and achievements [Tak23].

Authenticating Academic Credentials

Linking Soulbound Tokens (SBTs) to detailed resumes, university degrees, certificates, and transcripts could be another practical use of this technology. Considering that such credentials are non-transferable in the traditional Web2 world, employers and educational institutions could utilise SBTs to authenticate the details provided by an applicant in their resume. Moreover, for reference verification, the addresses of the references could be incorporated into the SBT, facilitating on-chain attestations, and thus further streamlining the verification process [GCOGI23].

Secure Management of Healthcare Records

In a patient-centric soulbound NFT framework for electronic health records (EHRs) to prevent the unauthorised trading of important medical documents, Soulbound Tokens (SBTs) can be employed. These tokens can't be bought or transferred; once assigned, they remain tethered to your private wallet and identity. As such, they're ideal for digitising non-transferable aspects like qualifications, reputation, and healthcare records. The ownership of the token bestows the right to control access to the information it contains, including the ability to revoke that access when required. Instead of being stored in a centralised database, personal information is managed in a blockchain-enabled format, providing enhanced access and control to the token's owner [TT23]. The ability to manage personal information in a blockchain-enabled form rather than having it stored in a central database makes SBTs an option for people who want the most access to their information [Mor23].

Challenges and concerns

Soulbound Tokens (SBTs), as an emerging concept, come with several challenges. Some of the notable concerns include [Lea22]:

- **Privacy:** As SBTs are linked to a specific individual, they could potentially be used for tracking and monitoring that individual's online activities. Technological advancements like zero-knowledge proofs on the blockchain could help address these privacy concerns by providing improved anonymity.
- **Security:** If a user's non-custodial wallet is compromised, malicious entities could misuse the SBTs, particularly those providing exclusive access or governance rights. This could harm the user and the communities they're associated with. This issue can be mitigated by storing assets in secure custodial wallets or vaults.
- **Interoperability:** Like many NFTs, SBTs are often minted on specific blockchains, which can restrict their versatility and applicability beyond their native chain. This limitation can be partially addressed by integrating EVM-compatible chains into prevalent Web3 applications and ensuring most users stay within a single blockchain ecosystem.
- **Non-transferability:** The non-transferable nature of SBTs, while offering numerous benefits, can also pose challenges. If a token is unwillingly assigned to someone, it may lead to issues. This can be resolved by developing more robust permissioned interfaces on top of the blockchain, allowing users to enjoy the benefits of SBTs while also having the option to conceal or remove SBTs from their profile.

To ensure wider adoption and success, these issues associated with SBTs need to be ironed out. Although souls can choose to hide what SBTs reveal, in a way, they could also foster discrimination by revealing too many details in specific situations or contexts. This is particularly true for marginalized social groups who are more likely to experience disfavor [ShrishtiEth22](HackerNoon, CBDCs and soulbound token explained 2022). With the right solutions, non-transferable NFTs like SBTs have the potential to contribute to a more equitable and privacy-focused digital society.

Conclusion

In the quest to build a decentralised society, or DeSoc, Soulbound tokens (SBTs) serve as fundamental components. By creating a solid digital identity and provenance, they play an instrumental role in the growth of this new societal structure. The idea of a decentralised society might seem theoretical or abstract, yet it has numerous practical implications that are

Soulbound tokens, in their diverse and wide-ranging applications, span the spectrum from web3 and DeFi to facets of everyday life. They are a rapidly emerging trend, destined not only to significantly influence the Web3 ecosystem but also to elevate the perception of NFTs. Rather than being seen merely as a means of owning artwork or symbols of prestige, NFTs can function as pivotal tools in the creation and confirmation of digital identities and connections in a decentralised world.

Ali Kathia
May 2023

References

[CG22] Tomer Jordi Chaffer and Justin Goldston. On the existential basis of self-sovereign identity and soulbound tokens: an examination of the "self" in the age of web3. *Journal of Strategic Innovation and Sustainability Vol*, 17(3):1, 2022.

[GCOGI23](1,2) Justin Goldston, Tomer Jordi Chaffer, Justyna Osowska, and Charles von Goins II. Digital inheritance in web3: a case study of soulbound tokens and the social recovery pallet within the polkadot and kusama ecosystems. *arXiv preprint arXiv:2301.11074*, 2023.

[Hil22] Felix Hildebrandt. The future of soulbound tokens and their blockchain accounts. In *Konferenzband zum Scientific Track der Blockchain Autumn School 2022*, number 2, 18–24. Hochschule Mittweida, 2022.

[Lea22] Juan Leal. What are soulbound tokens? *thirdweb*, 2022. URL: https://blog.thirdweb.com/soulbound-tokens/#:~:text=Limitations%20of%20soulbound%20tokens%2C%20or%20non%2Dtransferable%20NFTs&text=Currently%2C%20soulbound%20tokens%20lack%20the,monitor%20that%20person%27s%20online%

[Mor23] Kirsty Moreland. What is a soulbound token? *Ledger Academy*, 2023. URL: https://www.ledger.com/academy/topics/blockchain/what-is-a-soulbound-token.

[SKSK23] Sanskar Sharma, Aryan Kumar, Nidhi Sengar, and Ajay Kumar Kaushik. Implementation of property rental website using blockchain with soulbound tokens for reputation and review system. *ceur-ws.org*, 2023.

[ShrishtiEth22] Shrishti.Eth. Cbdcs and soulbound token explained. *HackerNoon*, 2022. URL: https://hackernoon.com/cbdcs-and-soulbound-token-explained.

[Tak23](1,2,3) Akash Takyar. What are soulbound tokens, and how do they work? *LeewayHertz*, 2023. URL: https://www.leewayhertz.com/soulbound-tokens/.

[TT23] Namrta Tanwar and Jawahar Thakur. Patient-centric soulbound nft framework for electronic health record (ehr). *Journal of Engineering and Applied Science*, 70(1):33, 2023.

[Tit22] Olusegun Joel Titus. Decentralized society's next stage: the soulbound token. *HackerNoon*, 2022. URL: https://hackernoon.com/cbdcs-and-soulbound-token-explained.

[UY22] Ece Su Ustun and Melek Yuce. Smart legal contracts & smarter dispute resolution. In *2022 IEEE 24th Conference on Business Informatics (CBI)*, volume 2, 111–117. IEEE, 2022.

[WOB22](1,2,3,4,5) E Glen Weyl, Puja Ohlhaver, and Vitalik Buterin. Decentralized society: finding web3's soul. *Available at SSRN 4105763*, 2022.

Understanding Zero-Knowledge Proofs and Their Innovative Role in Blockchain

Innovation & Ideation

Key Insights

- Zero-Knowledge Proofs (ZKPs), a cryptographic method, enhances privacy and security in blockchain transactions without sacrificing transparency.
- Advanced ZKP forms, such as zk-SNARKs and zk-STARKs, have evolved to offer shorter proofs, reduced computational requirements, and avoid the need for a 'trusted setup'.
- ZKPs are transforming various blockchain applications, including Digital Identity Management Systems, Traffic Management Systems, Mobile Health Systems, ridesharing, and real estate transactions, by providing privacy-preserving verification.
- Despite their benefits, ZKPs present challenges, including non-deterministic truthfulness, potential undisclosed secrets, and integrity risks. They also require considerable computational resources and lack user-friendliness for developers.
- Despite these challenges, ZKPs play a crucial role in the ongoing evolution of blockchain technologies, promising a future for more private, secure, and decentralized systems.

Introduction

Blockchain technology, while acclaimed for its decentralisation and transparency, often wrestles with the need for confidentiality and privacy. This is where Zero-Knowledge Proofs come into play. They are a groundbreaking solution that reconciles the dichotomy between transparency and privacy on blockchain platforms. In the context of blockchain transactions, ZKPs can verify the validity of transactions without disclosing any of the transaction details, thereby maintaining privacy while still ensuring security [KMS+16]. With the use of ZKPs in the blockchain, it is possible to maintain the immutability and transparency of the blockchain while ensuring the confidentiality of the information [MGGR13].

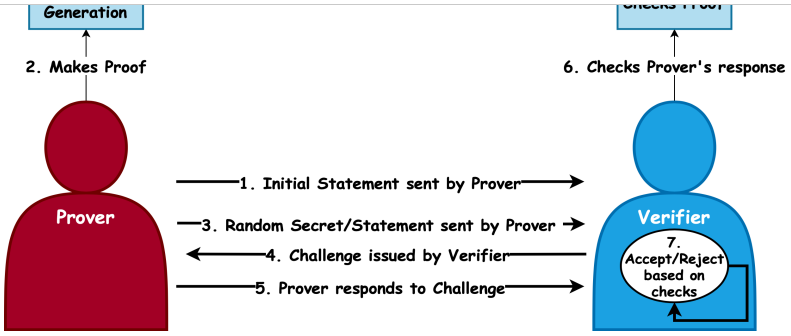

Fig. 6 Zero-Knowledge Proof Protocol Flow.

Deep Dive: What Are Zero-Knowledge Proofs?

The theoretical concept of Zero-Knowledge Proofs was initially introduced by Goldwasser et al. [GMR19] in their 1985 ground-breaking paper. A ZKP is a cryptographic method that enables one party (the prover) to prove to another party (the verifier) that they possess a specific piece of information, without disclosing the information itself, apart from asserting its truth. Their introduction revolutionised the world of cryptography, and they are now an integral part of many privacy-enhancing technologies. As an innovative concept, ZKPs have the potential to significantly enhance confidentiality in blockchain technology, with broad applications ranging from digital identity verification to decentralised finance (DeFi) and private voting systems.

A study by Kosba et al. [KMS+16] illustrated the effective implementation of ZKPs in blockchain technology, using the Zerocash protocol. This innovative protocol allows blockchain users to conduct transactions without disclosing the sender, receiver, or transaction value, thereby ensuring optimal confidentiality.

The development and refinement of ZKPs have led to advanced cryptographic protocols like zk-SNARKs and zk-STARKs. Ben-Sasson et al. [BSCTV14] introduced zk-SNARKs, an upgraded version of ZKPs, which offer shorter proofs and reduced computational requirements. To overcome the limitations of zk-SNARKs, particularly the 'trusted setup' condition, zk-STARKs were proposed, which offer similar benefits without the need for a trusted setup.

The Innovative Role of ZKPs in Blockchain

The introduction of ZKPs in blockchain technologies has enabled a new layer of confidentiality. Specifically, they can validate the truth of a transaction without revealing details about the transaction itself, which opens up new avenues for privacy-preserving applications on blockchain platforms [KMS+16].

Digital Identity Management Systems

Traditional centralised Digital Identity Management Systems (DIMS) are vulnerable to various threats, such as fragmented identity, single point of failure, internal attacks, and privacy leaks. However, the introduction of blockchain technology can mitigate these issues by eliminating the need for a centralised third party. Yet, the inherent transparency of the blockchain also poses privacy challenges due to its open nature.

To address these issues, smart contracts and zero-knowledge proof (ZKP) algorithms can be used to refine the current identity claim model on the blockchain. This enhances the unlinkability of identities and prevents the exposure of attribute ownership, thereby improving user privacy.

The solution also introduces a challenge-response protocol that allows users to selectively reveal attribute ownership to service providers. Notably, during user access to services, authentication is carried out via zero-knowledge proof rather than Identity Providers (IdPs). This means the authentication details are only visible to the service provider, which further safeguards user behavior privacy [YL20].

Traffic Management Systems

Modern traffic systems use a wealth of vehicular data for real-time decision-making, but integrating real-time data from connected vehicles poses data security and privacy challenges. While blockchain has offered innovative solutions, its transparency can compromise privacy.

The non-interactive zero-knowledge range proof (ZKRP) protocol can be used to address privacy concerns in traffic management systems, where sensitive data is often exposed due to blockchain's transparency. This protocol verifies the correctness of a piece of information without revealing any extra details beyond the verification itself. It is a critical component of the proposed decentralised, location-aware architecture designed for maintaining data integrity and privacy in blockchain-based traffic management systems. By leveraging the capabilities of the Hyperledger Fabric platform and the Hyperledger Ursa cryptographic library, this innovative approach has demonstrated its effectiveness and feasibility for real-time traffic management, all while fulfilling necessary data privacy requirements [LGNS20].

Privacy in Mobile Health Systems

The surge of compact mobile devices with wireless connectivity and integrated biosensors has transformed healthcare systems. These wearable devices, part of mobile health (mHealth), regularly collect health data, enabling remote patient monitoring and healthcare services. However, mHealth introduces substantial privacy risks, primarily due to its smartphone-based management system. Specifically, the communication between the monitoring devices and the smartphone, typically via Bluetooth, presents security challenges. Devices are usually paired with a smartphone but aren't necessarily linked exclusively to a specific mHealth app, leaving room for potential data breaches or illegitimate data injection.

This protocol is specifically designed to operate efficiently even on mHealth devices that have limited resources. By implementing this approach, we can ensure that only authorised devices have the ability to interact with the official mHealth application, which significantly strengthens the security and privacy protections of mHealth systems [TDNHDS20].

Identity Verification for Safe Ridesharing

Ridesharing offers several advantages, like reducing traffic congestion and environmental impact. However, the safety and privacy of both riders and drivers is a crucial concern, highlighting the need for a system that can verify identities while preserving privacy among untrusted parties.

In response to this need, a novel system is proposed, integrating zero-knowledge proof (ZKP) and blockchain technology for use in ridesharing applications. This system employs a permissioned blockchain network to verify a driver's identity using ZKP, while also acting as a secure ledger to record ride logs and ZKP records. A protocol is developed to allow user verification without the need to share any private information. The system has been prototyped on the Hyperledger Fabric platform, utilising the Hyperledger Ursa cryptography library, ensuring the secure and private verification of identities in ridesharing applications [LMGN20].

Real Estate Contracts

Given the high stakes involved in real estate contracts, the prevention of forgery and duplication is crucial, especially in the online space. Blockchain technology is emerging as a solution, improving the reliability of such contracts. However, as online real estate transactions using blockchain increase, scalability becomes an issue.

This is where the zero-knowledge proof algorithm comes into play. A novel Ethereum-based online real estate contract system that leverages this algorithm to enhance scalability. The system effectively manages contracts online and detects potential contract forgery via the blockchain. Importantly, the use of the zero-knowledge proof algorithm allows for scalability while preserving security and privacy. This enables the system to prevent fraudulent activities throughout the entire contract process, from initiation to termination. The incorporation of this algorithm thus strengthens the overall reliability and security of real estate transactions conducted online [JA21].

Challenges and Limitations

Zero-knowledge proof, despite its innovative approach, grapples with some limitations and vulnerabilities. Its non-deterministic characteristic means that there isn't an absolute guarantee that the generated values are truthful, but rather, they carry a high probability of being accurate. The technology's verification process, while preserving confidentiality, can also result in the underlying secret remaining undisclosed perpetually. Furthermore, if an untrustworthy party is involved in the process, there's a risk of integrity compromise, as they could manipulate the interactions to yield misleading outcomes [Faw23].

Requires a large amount of computation

Zero-knowledge Proof (ZKP) protocols, comprising intricate algorithms, necessitate an extensive amount of computational resources for their operation and execution. This considerable demand on processing power may pose challenges for common computers involved in the verification process [Bho22].

Not developer friendly

ZKP doesn't offer a user-friendly experience, particularly for developers. For instance, Zk Rollup, a Layer 2 solution that employs ZKP to enhance the scalability of Blockchain, is presently restricted to basic payment applications. The technology is yet to support aggregation, posing significant limitations for its users [Bho22].

Conclusion

As blockchain technologies continue to evolve, the role of Zero-Knowledge Proofs in shaping the future of blockchain applications is undeniably significant. By enabling verification without compromising confidentiality, ZKPs open the door to a vast array of innovative applications in various industries. From digital identity and cybersecurity to decentralised finance and voting systems, the potential for ZKPs to promote a more private, secure, and decentralised future is promising.

Ali Kathia
June 2023

References

[**BSCTV14]** Eli Ben-Sasson, Alessandro Chiesa, Eran Tromer, and Madars Virza. Succinct non-interactive zero knowledge for a von neumann architecture. In *23rd $|$USENIX$|$ Security Symposium ($|$USENIX$|$ Security 14)*, 781–796. 2014.

[Bho22] (**1**,**2**) BhoNetwork. What is zero-knowledge proof (zkp)? details about zkp. *BHO NETWORK*, 2022. URL: https://bho.network/en/what-is-zero-knowledge-proof#h3-21.

[**Faw23]** John Fawole. Zero-knowledge proof – how it works. *hacken.io*, 2023. URL: https://hacken.io/discover/zero-knowledge-proof/#Advantages_and_Disadvantages_of_Zero-Knowledge_Proof.

[**GMR19]** Shafi Goldwasser, Silvio Micali, and Chales Rackoff. The knowledge complexity of interactive proof-systems. In *Providing Sound Foundations for Cryptography: On the Work of Shafi Goldwasser and Silvio Micali*, pages 203–225. 2019.

[**JA21]** SoonHyeong Jeong and Byeongtae Ahn. Implementation of real estate contract system using zero knowledge proof algorithm based blockchain. *The Journal of Supercomputing*, 77(10):11881–11893, 2021.

[KMS+16] (**1**,**2**,**3**) Ahmed Kosba, Andrew Miller, Elaine Shi, Zikai Wen, and Charalampos Papamanthou. Hawk: the blockchain model of cryptography and privacy-preserving smart contracts. In *2016 IEEE symposium on security and privacy (SP)*, 839–858. IEEE, 2016.

[**LGNS20]**

[LMGN20] Wanxin Li, Collin Meese, Hao Guo, and Mark Nejad. Blockchain-enabled identity verification for safe ridesharing leveraging zero-knowledge proof. In *2020 3rd International Conference on Hot Information-Centric Networking (HotICN)*, 18–24. IEEE, 2020.

[MGGR13] Ian Miers, Christina Garman, Matthew Green, and Aviel D Rubin. Zerocoin: anonymous distributed e-cash from bitcoin. In *2013 IEEE Symposium on Security and Privacy*, 397–411. IEEE, 2013.

[TDNHDS20] Antonio Emerson Barros Tomaz, Jose Claudio Do Nascimento, Abdelhakim Senhaji Hafid, and Jose Neuman De Souza. Preserving privacy in mobile health systems using non-interactive zero-knowledge proof and blockchain. *IEEE access*, 8:204441–204458, 2020.

[YL20] Xiaohui Yang and Wenjie Li. A zero-knowledge-proof-based digital identity management scheme in blockchain. *Computers & Security*, 99:102050, 2020.