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.

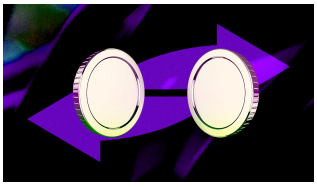
Download Science-Notes as a pdf

DSF Science Notes Editorial Board

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

Academic Insights

Optimising Cross-Chain Swaps: A Game Theoretic Analysis of HTLCs and Packetised Payments



Optimising Cross-Chain Swaps: A Game Theoretic Analysis of HTLCs and Packetised Payments

Academic Insight

- The integration of cross-chain interoperability is crucial for a variety of decentralised finance (DeFi) applications such as decentralised exchanges (DEXs) and decentralised applications (DApps). The technology must be trustless to prevent reliance on centralised intermediaries, Hash Time Locked Contracts (HTLCs) are commonly used for this purpose.
- Atomic swaps present a risk of asset value fluctuation during the exchange, increasing the likelihood of one party abandoning the swap. This can result in opportunity costs for the other party.
- A game theoretic framework can be established to construct a parametrised solution for determining the success rate of cross-chain swaps through HTLCs and Packetised Payments (PPs).
- The current parameters often lead to high failure rates in cross-chain swaps. In the context of PPs, these parameters can theoretically enable malicious actors to gain profits.
- The game theoretic framework is extended to derive optimisation solutions that enhance the success rate of atomic swaps and PPs, focusing on collateralisation and adjustable exchange rates.

Introduction

Atomic Swaps

Direct and automatic peer-to-peer (P2P) exchanges of crypto assets on fundamentally different blockchain networks without the use of centralised intermediaries [DMHM19].

In the Decentralised Finance (DeFi) landscape, interoperability between disparate blockchain networks is paramount for data and value transmission across chains [Mao22]. Cross-chain technology has applications in Decentralised Exchanges (DEXs), cross-platform Decentralised Applications (DApps), tokenised real assets, distributed transaction platforms, etc. The technologies need to enable secure and trustless transactions to prevent reliance on centralised intermediaries. To this end, Hash Time Lock Contracts (HTLCs), a form of atomic swaps, are commonly used to achieve cross-chain asset exchange. HTLCs and all other atomic swaps have inherent risks associated with them: (1) value fluctuation during the exchange, and (2) high incentives for malicious agents [DR23]. An alternative approach is Packetised Payments (PPs) [Rob19], which implement a series of alternating transactions to achieve cross-ledger exchange. This article summarises the recent studies regarding these protocols - unravelling their execution success rate bottlenecks and exploring the proposed solutions [JX21] [AD21].

HTLCs

HTLCs are a type of smart contract that uses elements of cryptocurrency on-chain transactions along with hash-lock and time-lock contracts to reduce counterparty risk in cross-chain asset exchange [JP16]. A hash lock is a hashed or cryptographically scrambled version of the secret (key) generated by the agent initiating the swap and is used by both agents to lock their assets and exchange them. The swap is complete when the initiating agent reveals the preimage of the hashlock to access the received assets, which enables the second agent to access their received assets. Further, if the HTLC contract is not completed within the pre-determined time constraint, both parties automatically receive their initial assets, and the swap fails.

PPs

Packetised Payments start by breaking down transactions into packets. Further, on each step, the participant would match the previous transfer and extend their transfer, hence ensuring equal distribution of counterparty risk. If any participant were to exit the transaction, the other agent would lose a maximum of one packet, which is sized to be economically insignificant.

Game Theoretic Analysis

A game theoretic framework is developed to sequentially analyse events in the two protocols and derive probabilities for the success rate of cross-chain exchanges. The detailed version of the below discussion can be found in [JX21] [AD21].

Game Theoretic Framework for HTLCs

Two agents, Alice (A) and Bob (B), are aiming to trade $token_a$ From $chain_a$ for $token_b$ from $chain_b$ at a defined exchange rate P^*. $token_b$'s price at time t is denoted by P_t. At each step during the exchange, the agents can choose to either stop or continue the exchange. The steps are as follows –

- **Step 1:** (A) decides whether to initiate the swap by writing a swap HTLC on $chain_a$ (cont) or not (stop).
- **Step 2:** (B) decides whether to write an HTLC on $chain_b$ (cont) or not (stop).
- **Step 3:** (A) decides whether to unlock $token_b$ (cont) or not (stop).
- **Step 4:** (B) decides whether to unlock $token_a$ (cont) or not (stop).

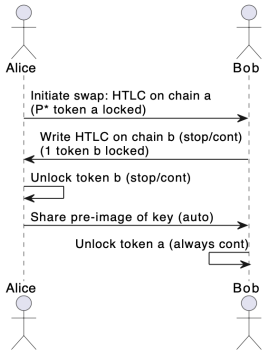


Fig. 1 HTLC game diagram.

viability range for the swap to continue. P_t being higher than a derived maximum or minimum would bring the success probability to zero.

In step 3, A gets to make the sole decision of whether to complete the swap or not, hence can choose to stop if the exchange price drops and execute if it rises. In this instant, A has the optionality akin to an American option, as she can choose to execute or not at any moment up to the expiration time.

It is found that in steps 1 to 3, the greater the range between minimum and maximum viable values of P_t, the higher the probability of the swap succeeding.

Key Findings

1. **Exchange Rate:** The success of the swap depends on a defined range of exchange rates P^*. Deviations from this range significantly impact the success probability. The overall success rate is highly sensitive to the range of values allowed for P^*; therefore, the stability and security of HTLCs can be optimised by maximising this range.
2. **Success premium:** This is the measure of how determined each party is to see the swap succeed. Actors with low success premiums would cause a low success rate for the swap and come off as malicious. A high success premium leads to a high success rate and a greater range of feasible P^*.
3. **Time preference (r):** Time preference describes an agent's impatience level - the desire to access assets now rather than later. larger r results in a narrower viable range of values for P^*. If r is greater than a calculated critical value, the swap is rendered impossible as no P^* remains feasible.
4. **Transaction confirmation time:** Higher confirmation time on either chain shrinks the viable range of P^* as the increased time taken reduces the transaction utility functions for either or both parties. When P^* is chosen to maximise the success rate, a lower confirmation time increases the success rate.
5. **Price trend and volatility:** A High upward trend of the exchange rate increases the success rate as Alice is highly likely to decide in favour of the final optionality she receives. In contrast, higher volatility reduces the success rate.

Transaction Confirmation Time

The time between a network receiving a transaction and the transaction getting processed on the chain by a miner node.

HTLCs experience reoccurring and numerous transaction failures. Hence, it can be stated that existing parameters and success premiums of agents are stacked such that success rates cannot be optimal.

Extending the above game theoretic framework to PPs proves that not only do malicious agents have no incentive to complete transactions, but also that they can enter multiple transactions in parallel to generate large profits.

Optimising Cross-Chain Swaps

This game theoretic analysis is persistent across various trustless cross-chain swap protocols [MB20]. Therefore, solutions derived by extending the methodology can be widely implemented to generate higher success rates of swaps and minimise incentives for malicious actors to stop the exchange.

Swaps with collateral

Alice and Bob move an allowance to a trusted smart contract on $chain_a$ to charge each of them simultaneously the same amount of collateral, Q $token_a$, before the swap. The smart contract can be connected to an oracle that observes the transaction. If any agent decides to stop at any time, the other agent receives both collaterals.

Oracle

A third-party service that connects on-chain smart contracts to the external world.

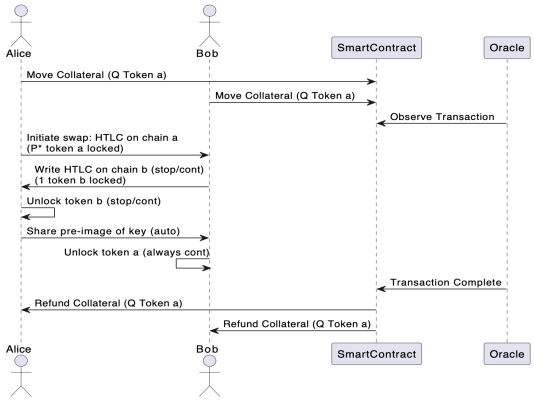


Fig. 2 HTLC with collateral game diagram.

The extension of the game theoretic framework to this system shows that the success rate increases with collateral amount Q. This is because higher Q allows for larger exchange rate P_t movements; consequently, the sensitivity of the success rate towards P^*, volatility, and trend is reduced. The incentives that malicious actors may gain from massive price movements are eliminated by the loss of higher collateral. Therefore, the best strategy for malicious actors is to continue – maximising the success rate of the swap.

Adjustable Exchange Rates

This is an extension to the HTLC game. The agents not only have the freedom to choose to continue or stop, but they can also decide the exact amount of funds to lock in, that is, P^* isn't fixed and can be adjusted as P_t changes on each step.

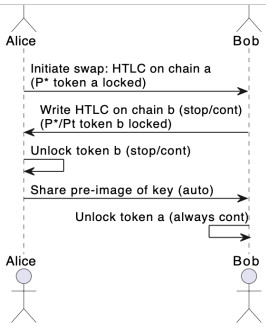


Fig. 3 HTLC with adjustable exchange rate game diagram.

It is found that the absence of a pre-determined exchange rate boosts the success rate and allows for the possibility of success over a wider range of exchange parameters.

Conclusion

The game theoretic approach developed in the referenced papers and discussed above is a rigorous quantitative method to study the viability and sensitivity of various cross-chain technologies. An analysis of HTLCs and PPs reveals execution success rate bottlenecks. The findings are not local to these protocols as other investigations successfully apply similar game theoretic analysis to a variety of protocols. Extending the analysis offers crucial solutions - collateralisation and adjustable exchange rates. These help mitigate counterparty risks by aligning incentives for all parties. The findings, applicable across various trustless cross-chain swap protocols, offer a blueprint for elevating success rates and minimising vulnerabilities, contributing to the advancement of secure and efficient decentralised finance ecosystems.

Aaryan Gulia
January 2024

References

[AD21](1,2) Jiahua Xu Alevtina Dubovitskaya, Damien Ackerer. A game-theoretic analysis of cross-ledger swaps with packetized payments. *Lecture Notes in Computer Science*, 2021. URL: https://link.springer.com/content/pdf/10.1007/978-3-662-63958-0.pdf.

[**DR23]** Tien Tuan Anh Dinh Daniël Reijsbergen, Bretislav Hajek. Crocodai: a stablecoin for cross-chain commerce. 2023. URL: https://doi.org/10.48550/arXiv.2306.09754, arXiv:2306.09754.

[**DMHM19]** Dr David Donald Dr Mahdi H. Miraz. Atomic cross-chain swaps: development, trajectory and potential of non-monetary digital token swap facilities. *SSRN Electronic journal*, 2019. URL: https://www.researchgate.net/publication/330419487_Atomic_Cross-Chain_Swaps_Development_Trajectory_and_Potential_of_Non-Monetary_Digital_Token_Swap_Facilities.

[JX21](1,2) Alevtina Dubovitskaya Jiahua Xu, Damien Ackerer. A game-theoretic analysis of cross-chain atomic swaps with htlcs. *IEEE*, 2021. URL: https://doi.org/10.1109/ICDCS51616.2021.00062.

[**JP16]** Thaddeus Dryja Joseph Poon. The bitcoin lightning network: scalable off-chain instant pay- ments. *Lightning Network*, 2016. URL: https://lightning.network/lightning-network-paper.pdf.

[**Mao22]** Hanyu Mao. A survey on cross-chain technology: challanges, development, and prospect. *IEEE Access*, 2022. URL: https://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=9982450&tag=1.

[**MB20]** Maria Potop-Butucaru Marianna Belotti, Stefano Moretti. Game theoretical analysis of cross-chain swaps. *IEEE*, 2020. URL: https://ieeexplore.ieee.org/document/9355687.

[**Rob19]** D Robinson. Htlcs considered harmful. *Stanford Blockchain Conference (2019)*, 2019. URL: http://diyhpl.us/wiki/transcripts/stanford-blockchain-conference/2019/htlcs-considered-harmful/.

Innovation & Ideation

Blockchain in the Metaverse: A New Digital Era

Decentralised Physical Infrastructure Network (DePIN)

Blockchain in the Metaverse: A New Digital Era

Innovation & Ideation

- The Metaverse integrates VR, AR, and XR with blockchain, enhancing immersive experiences and revolutionising digital transactions and asset management.
- Blockchain serves as both a data repository and an economic system foundation in the Metaverse, linking virtual and real-world economies.
- Blockchain increases the security and decentralisation of digital interactions in the Metaverse, ensuring transparent and trustworthy asset management.
- Key projects like Decentraland, Sandbox, Illuvium, and Axie Infinity demonstrate blockchain's diverse applications in the Metaverse, from virtual real estate and gaming to e-commerce.
- Addressing privacy, potential centralisation, and ensuring secure, reliable blockchain architecture are major challenges for blockchain integration in the Metaverse.
- The continued development of blockchain is crucial for the Metaverse's growth, hinting at a future where digital and physical realities seamlessly merge, offering new possibilities for digital interaction and economic models.

Introduction

The Metaverse, a sophisticated digital evolution, integrates technologies like Virtual Reality (VR), Augmented Reality (AR), and Extended Reality (XR), creating an immersive virtual experience [HTGW+23]. Alongside these technologies, the role of blockchain is crucial. Known for its security and transparent peer-to-peer system, blockchain is essential in redefining digital transactions and asset management within the Metaverse [BAKE22].

Augmented Reality

Augmented Reality (AR) is an interactive experience that combines the real world with computer-generated content.

Virtual Reality

Virtual Reality (VR) is a simulated experience designed to give the user an immersive sensation of being in a virtual world.

Extended Reality

Extended Reality (XR) is a catch-all term used to refer to AR, VR, and Mixed Reality (MR).

Blockchain technology significantly enhances the way digital assets are managed and transactions are executed in the Metaverse, contributing to a more secure and integrated virtual economy [HTGW+23]. This integration is crucial for the integrity of digital interactions in the Metaverse [BAKE22]. It enables safe and transparent handling of digital assets and transactions, making it indispensable for the Metaverse's economic and interactive frameworks. In this environment, where interactions predominantly occur through digital avatars, blockchain ensures these interactions are secure, trustworthy, and verifiable [BRC+22]. These advanced technologies collectively contribute to the Metaverse's potential to revolutionise various sectors, including education, real estate, entertainment, and medicine [LWG+22].

Integrating Blockchain with the Metaverse: Core Concepts and Technologies

The Metaverse, initially conceptualised by Neal Stephenson in his 1992 novel "Snow Crash," represents an advanced blend of the physical, human, and digital worlds within a computer-generated universe [WSZ+22]. This evolving concept is now seen as a potential next evolutionary phase of the internet. In this virtual realm, individuals engage in an alternate existence through digital avatars, a process facilitated by advancements in VR technology.

Digital Avatar

A digital avatar is a visual representation of a user in the virtual world.

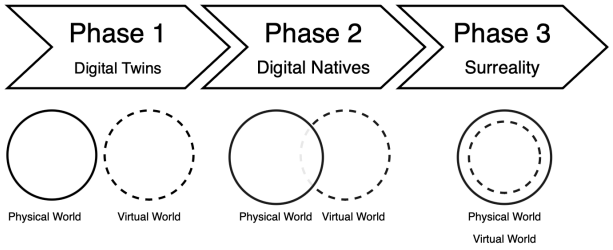


Fig. 4 Development trajectory of the Metaverse.

Central to the Metaverse is the integration of various emerging technologies. It utilises digital twins to replicate the real world, while VR and AR enhance the immersive experience. The Metaverse also incorporates advanced technologies like 5G for ultra-reliable and low-latency communication, supported by wearable sensors and brain-computer interfaces to enhance user interaction [HTGW+23]. This evolution is transitioning from concept to reality, driven by rapid technological advancements and attracting interest from major tech companies such as Meta, Microsoft, Tencent, and NVIDIA. The development trajectory of the Metaverse involves three phases [WSZ+22]:

Digital Twins

A digital twin is a virtual representation of a physical object, system, or process that is updated in real-time using data from sensors and other sources. It uses machine learning, simulation, and reasoning to help decision-making.

Digital Natives

A person born or brought up during the age of digital technology and so familiar with computers and the internet from an early age.

1. Starting with the creation of digital twins that mirror the physical world.
2. Moving towards a stage where digital natives generate unique content and innovations.
3. Culminating in a stage of a self-sustaining, expansive virtual world that transcends the boundaries of physical existence and offers experiences beyond the limitations of reality. This vision of the metaverse suggests a future where virtual and physical realms are seamlessly intertwined, offering limitless possibilities for human interaction and experience.

centralised financial systems with a secure, transparent, and immutable peer-to-peer network [FLY+22]. Blockchain technology emerges as a pivotal advantage in the Metaverse, enabling secure and transparent transactions for digital assets like virtual real estate, avatars, and in-game items, all of which can have significant real-world value [Amb23].

Digital Assets

A digital asset is generally anything that is created and stored digitally, is identifiable and discoverable, and has or provides value.

Blockchain's integration into the Metaverse allows for the management of digital assets through blockchain-based tokens, streamlining trading processes and enabling the purchase of virtual goods and services on decentralised platforms without traditional intermediaries [Amb23]. Furthermore, blockchain intersects with the Metaverse in the realm of digital identity. Users can create verifiable digital identities with blockchain-based systems, enhancing security and granting ownership and control over their digital identities across different Metaverse platforms [Amb23].

This synergy between blockchain and the Metaverse sets the stage for intriguing evolution in digital ownership and commerce. Blockchain's role in securely managing digital assets and crafting unique digital identities is pivotal in enriching virtual experiences in the Metaverse [Amb23]. It opens new avenues for digital ownership and commerce, suggesting a future where virtual and physical realms are seamlessly intertwined, offering limitless possibilities for human interaction and experience.

Blockchain's Role in Enhancing the Metaverse

In the Metaverse, blockchain's role is crucial for maintaining a secure and decentralised digital ecosystem. This technology guarantees the safety and confidentiality of data, a necessity in a complex digital landscape. It also authenticates and manages the ownership of digital assets, fostering trust among users. Essentially, blockchain empowers users by ensuring the Metaverse's security and fostering decentralisation [MSA+22]. Blockchain's integration into the Metaverse significantly improves its functionality. It provides a clear and unchangeable ledger system that facilitates digital transactions without a central overseeing authority. Blockchain enables distinctive functionalities like smart contracts and the use of Non-Fungible Tokens (NFTs) for establishing ownership, as well as cryptocurrency as the currency of the virtual economy [Tec22].

Role of Virtual Currencies

Digital currencies like Bitcoin are crucial in the Metaverse for the smooth execution and integrity of virtual financial transactions. These digital currencies enable transactions for goods and services within this fully digital space, promoting new paths for business and entrepreneurial activities. Their secure nature, using sophisticated encryption methods, safeguards against fraudulent activities and theft. In gaming scenarios, virtual currencies incentivise players through rewards, enhancing the gaming experience [K23].

Enhancing Data within the Metaverse

Distributed Data Storage

Distributed storage is a method of storing data across multiple nodes, typically in a network of interconnected computers. As a result, the data is readily available, scalable, and resilient against failures.

Blockchain's peer-to-peer data-sharing capability effectively meets the Metaverse's extensive data-handling needs. Innovations in blockchain-based models synchronise the real and virtual worlds, safeguarding against data manipulation in cross-chain exchanges. Distributed data storage addresses the limitations of traditional centralised storage, reducing operational costs and enhancing data security [FLY+22].

Developing a Virtual Economic Framework in the Metaverse

A variety of digital assets, including User-Generated Content (UGC), Professional Generated Content (PGC), Artificial Intelligence-Generated Content (AIGC), and Non-Fungible Tokens (NFTs), play a key role in the Metaverse economy. Blockchain technology uniquely authenticates and ensures the ownership of these digital items. The trade and marketplace for these assets are distinguished by blockchain and cryptocurrencies, bypassing traditional intermediaries. Ethereum's smart contracts and DeFi platforms like Uniswap are pioneering new economic models in the Metaverse. Challenges like Miner Extractable Value (MEV) indicate the complex and evolving landscape of this economy [HQT+23]. Blockchain also underpins transactions involving virtual resources like land and goods, linking the Metaverse's virtual economy with real-world financial systems [FLY+22].

Applications in Health Care, Education & Training

The rapid adoption of telehealth, particularly highlighted during the COVID-19 pandemic, has transformed healthcare delivery. In the U.S., services offered by facilities jumped from 43% pre-pandemic to 95% in 2020 [BRC+22]. This surge, particularly in remote areas, as seen in India, showcases the increasing reliance on virtual healthcare solutions. The Metaverse, with technologies such as Epazz Slims and Zimmer Biomet's OptiVu, enhances this trend by providing virtual environments for patient-doctor interactions, promising wider access to healthcare, cost reductions, and lower infection risks [BRC+22]. In this context, blockchain technology can significantly enhance telehealth by providing secure patient data management. Blockchain's inherent security and transparency ensure the confidentiality and integrity of patient records, a critical aspect in the healthcare sector.

In the realm of education, the Metaverse revolutionises traditional methods, shifting from 2D tools to immersive 3D experiences in virtual settings. This shift is crucial in democratising education and addressing challenges like declining educational quality and student engagement [LWG+22] [BRC+22]. Blockchain can add substantial value in this sector, particularly through transparent credentialing systems. By leveraging blockchain, educational institutions can issue verifiable and immutable certificates and credentials, enhancing the trustworthiness and ease of verification of academic qualifications across different platforms. This not only streamlines the credentialing process but also opens up new avenues for lifelong learning and professional development in a secure and authenticated manner.

In both healthcare and education, the integration of blockchain within the Metaverse paves the way for more secure, efficient, and transparent systems. It supports the evolution of these sectors by enabling new functionalities and improving user trust and experience.

Notable Blockchain-based Metaverse Projects

The integration of blockchain into the Metaverse has led to the emergence of several notable projects, each leveraging blockchain as a core technology for their virtual world foundations and services:

Ethereum blockchain, offering users complete control over their creations [Dec24].

- **Sandbox:** Built on the Ethereum blockchain, Sandbox is a decentralised, user-generated Metaverse. Users can create, own, and monetise immersive gaming experiences using SAND, the platform's utility token. It features a voxel gaming environment where users can create and animate 3D objects as NFTs [Gam23].
- **Illuvium:** An open-world fantasy battle game built on the Ethereum blockchain. Players can capture fantasy creatures, known as Illuvials, and use them in battles. Illuvium leverages Immutable X, a layer-2 Ethereum scaling solution, for trading NFTs with zero gas fees [Doc23].
- **Axie Infinity:** A Play-to-Earn Metaverse project where players collect, raise, breed, and battle fantasy creatures called Axies. It features a player-centric economy, allowing players to own, sell, and trade in-game resources, with most transactions processed on the Ethereum-linked sidechain, Ronin [Axi21].

These projects illustrate the diverse applications of blockchain in the Metaverse, from virtual real estate and gaming to e-commerce. They showcase how blockchain technology is being used to create decentralised, user-controlled virtual environments, opening up new possibilities for digital ownership and commerce in the virtual world.

Challenges and Concerns

Integrating blockchain technology into the Metaverse presents several key challenges and concerns that need to be addressed to ensure its successful implementation [FLY+22]:

- **Privacy Concerns:** Addressing privacy issues is essential for integrating blockchain into the Metaverse to ensure that sensitive user data remains protected.
- **Potential Centralisation:** Avoiding centralisation within blockchain networks is essential to preserve the decentralised nature of the Metaverse.
- **Secure and Reliable Architecture:** Establishing a more secure and reliable blockchain architecture is crucial for supporting the Metaverse's complex environment.
- **Resilience Against Attacks:** Enhancing the resilience of blockchain systems against cyber attacks to ensure robust security.
- **Auditing Complexity:** Managing the intricate process of auditing blockchain transactions to maintain transparency and accountability.
- **Balancing Transparency and Data Protection:** Striking a balance between transaction transparency and the protection of sensitive data is vital in the Metaverse.

Conclusion

The integration of blockchain into the Metaverse is a significant step in reshaping how we interact and transact digitally. Looking forward, continued advancements in blockchain are expected to further enhance its role in the Metaverse, particularly in improving transaction security and system efficiency. Key developments like enhanced interoperability and user-friendly interfaces will play a crucial role in expanding the Metaverse. Establishing clear regulations for blockchain use within this space is essential for maintaining security and ethical practices. Moreover, adopting environmentally sustainable blockchain practices will be important for future growth. We anticipate a Metaverse where blockchain is seamlessly integrated, offering new opportunities for digital ownership and economic models. As we progress, the ongoing evolution and thoughtful integration of blockchain technology will be key to unlocking the full potential of the Metaverse.

Tzoulian Pougios
January 2024

References

[Amb23] (1,2,3,4) Diana Ambolis. Blockchain and metaverse: top 10 ways blockchain will boost the use of metaverse. *Blockchain Magazine*, 2023. URL: https://blockchainmagazine.net/blockchain-and-metaverse-top-10-ways-blockchain-will-boost-the-use-of-metaverse/.

[Axi21] AxieInfinity. Axie infinity whitepaper. *AxieInfinity*, 2021. URL: https://whitepaper.axieinfinity.com.

[BRC+22] (1,2,3,4) Gaurang Bansal, Karthik Rajgopal, Vinay Chamola, Zehui Xiong, and Dusit Niyato. Healthcare in metaverse: a survey on current metaverse applications in healthcare. *Ieee Access*, 10:119914–119946, 2022.

[BAKE22] (1,2) Ouns Bouachir, Moayad Aloqaily, Fakhri Karray, and Abdulmotaleb Elsaddik. Ai-based blockchain for the metaverse: approaches and challenges. In *2022 Fourth International Conference on Blockchain Computing and Applications (BCCA)*, 231–236. IEEE, 2022.

[Dec24] Decentraland. Introduction. *decentraland.org*, 2024. URL: https://docs.decentraland.org/player/general/introduction/.

[Doc23] Illuvium.io Docs. Illuvium whitepaper. *Illuvium*, 2023. URL: https://docs.illuvium.io/illuvium-whitepaper/.

[FLY+22] (1,2,3,4) Yuchuan Fu, Changle Li, F Richard Yu, Tom H Luan, Pincan Zhao, and Sha Liu. A survey of blockchain and intelligent networking for the metaverse. *IEEE Internet of Things Journal*, 10(4):3587–3610, 2022.

[Gam23] The Sandbox Game. What is the metaverse? a guide to the future of the web. *Sandbox*, 2023. URL: https://www.sandbox.game/en/blog/what-is-the-metaverse-a-guide-to-the-future-of-the-web/3362/.

[HQT+23] Huang Huawei, Zhang Qinnan, Li Taotao, Yang Qinglin, Yin Zhaokang, Wu Junhao, Zehui Xiong, Zhu Jianming, Jiajing Wu, and Zibin Zheng. Economic systems in the metaverse: basics, state of the art, and challenges. *ACM Computing Surveys*, 56(4):1–33, 2023.

[HTGW+23] (1,2,3) Thien Huynh-The, Thippa Reddy Gadekallu, Weizheng Wang, Gokul Yenduri, Pasika Ranaweera, Quoc-Viet Pham, Daniel Benevides da Costa, and Madhusanka Liyanage. Blockchain for the metaverse: a review. *Future Generation Computer Systems*, 2023.

[K23] Ashwani K. What is the role of virtual currencies in the metaverse? *DevOps School*, 2023. URL: https://www.devopsschool.com/blog/what-is-the-role-of-virtual-currencies-in-the-metaverse/.

[LWG+22] (1,2)

[MSA+22] Md Ariful Islam Mozumder, Muhammad Mohsan Sheeraz, Ali Athar, Satyabrata Aich, and Hee-Cheol Kim. Overview: technology roadmap of the future trend of metaverse based on iot, blockchain, ai technique, and medical domain metaverse activity. In *2022 24th International Conference on Advanced Communication Technology (ICACT)*, 256–261. IEEE, 2022.

[Tec22] TPP Technology. Why blockchain is a key technology for the metaverse? *TppTechnology*, 2022. URL: https://www.tpptechnology.com/en/blog/why-blockchain-is-a-key-technology-for-the-metaverse/.

[WSZ+22](1,2) Yuntao Wang, Zhou Su, Ning Zhang, Rui Xing, Dongxiao Liu, Tom H Luan, and Xuemin Shen. A survey on metaverse: fundamentals, security, and privacy. *IEEE Communications Surveys & Tutorials*, 2022.

Decentralised Physical Infrastructure Network (DePIN)

Innovation & Ideation

Key Insights

- DePINs enhance transparency and user control, shifting management from centralised entities to a community-based model.
- Blockchain and DLT enable secure, innovative applications like Filecoin, which democratises storage and rewards participation.
- The tokenisation model in DePIN incentivises contributions (e.g., GPU power, storage) with tokens, sustaining network operations.
- Zero-Knowledge Proofs (ZKPs) in DePIN ensure secure and private verification processes, enhancing data integrity.
- DePINs require extensive infrastructure, potentially limiting participant access and risking centralisation by powerful entities like mining pools.
- By decentralising storage and other services, DePIN could reduce costs by up to 70%, though user engagement and profitability remain critical for growth.
- Successful expansion of DePIN depends on overcoming scalability, governance, and resource access challenges to achieve broader adoption.

Introduction

Decentralisation stands as a pivotal method for ensuring information transparency. The emergence of blockchain and Decentralised Ledger Technology (DLT) has illuminated the prospects of integrating such innovations into various infrastructures. Bitcoin introduced the concept of decentralisation as a peer-to-peer cash network [Nak08]. Decentralisation has been a main topic of discussion in recent trends [dcooperationeddeveloppementeconomiques19]. This concept has also been explored in the context of transitioning traditional physical networks towards decentralisation [BWL+23].

Numerous infrastructures, such as wireless networks, cloud storage, and computing, can benefit from decentralisation. DePIN, for instance, can be defined as an infrastructure network constructed, maintained, and operated through blockchain protocols within a decentralised and open network [Lep24].

The current solution provides a centralised infrastructure for users, such as AWS, where Amazon oversees controlling and maintaining the cloud services. Conversely, in a decentralised solution, the community and token holders assume responsibility for facilitating and delivering these services. This science note delves into the workings of this technology, its applications, and its implementation strategies. Moreover, we analyse the benefits of Decentralised Physical Infrastructure Networks (DePIN) alongside the concerns surrounding their use within physical infrastructures.

What is DePIN and How it Works

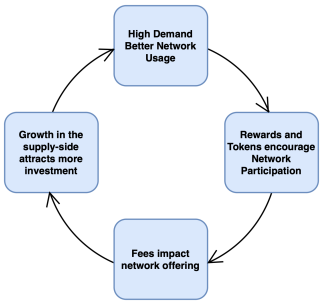


Fig. 5 DePIN Life Cycle.

DePIN has garnered attention in recent developments for bridging decentralisation with the physical realm. Decentralisation has promised values such as enhancing transparency, reducing censorship, improving user control by granting access to the decision-making processes, and diminishing reliance on intermediaries within the network [Sar23].

Functioning as a crypto-economic system, DePIN comprises several components: i) individual autonomous actors, ii) economic policies embedded in software, iii) emergent properties arising from the interactions of those actors according to the rules defined by the software [BWL+23] [Bal22].

At the core of DePIN's operation lies the tokenisation model, which incentivises participants to contribute essential resources to the network. This participation entails offering resources such as GPU power, hotspots, and storage. Users within the network benefit from

Tokenisation

Tokenisation is the process of converting assets or rights into digital tokens that can be recorded and managed. These tokens can represent a

use the provided tokens to access storage offered by network participants [Ide23].

transactions within the network.

Participant verification is essential in a vast network of users utilising their devices to sustain DePIN. Methods like Zero-Knowledge Proof (ZKP) enable the verification of new members while ensuring they possess the requisite equipment without revealing their credential information [Sar23].

Zero-Knowledge Proof

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.

Use Cases

Filecoin stands out as a great example of DePIN utilisation, offering decentralised storage solutions. Miners can engage with the network by allocating their unused storage and earning rewards, effectively transforming cloud storage into an algorithmic market facilitated by peer-to-peer networking.

This system uses cryptographic algorithms to ensure that all files are saved securely. The community behind Filecoin governs the network's authority. They are committed to upholding transparency, decentralisation, and open-source principles throughout the network.

Numerous advantages come from utilising Filecoin services. Being a decentralised network, there are no geographical limitations on user participation, fostering inclusivity. However, users should consider the efficiency of their equipment and electricity costs. Additionally, the transparency and security provided by cryptographic algorithms enhance user trust. Filecoin's commitment to open-source development ensures users have access to the latest software for seamless operation.

Nevertheless, alongside the benefits come certain concerns. Profitability challenges have jeopardised user interest, affecting network participation. The scarcity of users providing necessary equipment and facilities has currently impacted the network's efficacy. Enhanced profitability systems and increased user engagement could mitigate these challenges and drive network growth [Fil24] [Sch24].

Advantages

Ballandies et al. [BWL+23] explore the advantages of employing DePINs across various domains. Firstly, decentralisation offers resilience and reliability to networks. Blockchain's transparency feature fosters trust among users by ensuring transparency while maintaining participant anonymity. Additionally, permissionless blockchain networks enhance scalability and utility within the infrastructure network.

Cost efficiency emerges as another key benefit of DePIN networks. Adopting a decentralised approach akin to AWS may cut cloud storage costs by as much as 70%. Despite challenges in infrastructure development, this approach holds promise, particularly for smaller businesses [Sel24].

Concerns

Decentralised Physical Infrastructure Networks are still in their infancy, with significant room for development and maturation. Despite the numerous benefits, there are downsides to the technology. Concerns about the governance and the actual decentralisation of the network persist. Even though these networks are foundational to decentralisation, they require extensive technological infrastructure, which may not be accessible to all users. For example, you may have a few gigabytes of storage on your laptop, but this will not suffice for a massive network. Mining pools often have the required infrastructure, giving them the potential to dominate network control, which can shift the decentralisation in their favour.

Additionally, these networks often necessitate large-scale resources such as powerful GPUs, which may not be accessible to many users. This limitation can affect the scalability of the network.

Conclusion

Although DePIN technology is on its path to revolutionising the decentralisation of physical infrastructure like sensors, storage, GPUs, and more, there are several concerns that need to be addressed. Proper implementation of these physical infrastructures can help to reduce costs, increase transparency, and enhance overall network resilience. DePINs also offer the potential to take control from centralised players like AWS, challenging them by empowering individuals to participate in the network with their equipment. As the technology develops, addressing these concerns effectively will be crucial to its success and widespread adoption.

Hamed Mousavi
March 2024

References

[BWL+23](1,2,3) Mark C Ballandies, Hongyang Wang, Andrew Chung Chee Law, Joshua C Yang, Christophe Gösken, and Michael Andrew. A taxonomy for blockchain-based decentralized physical infrastructure networks (depin). *arXiv preprint arXiv:2309.16707*, 2023.

[**Bal22]** Mark Christopher Ballandies. *Fundamentals of Cryptoeconomics: On the design, construction, and impact of blockchain-based systems and incentives*. PhD thesis, ETH Zurich, 2022.

[**dcooperationeddeveloppementeconomiques19]** Organisation de coopération et de développement économiques. *Making Decentralisation Work: A Handbook for Policy-Makers*. OECD Publishing, 2019.

[**Fil24]** Filecoin. Depin hub. *Filecoin*, 2024. URL: https://depinhub.io/projects/filecoin.

[**Ide23]** IdeaSoft. Decentralized physical infrastructure (depin) explained. *IdeaSoft*, 2023. URL: https://ideasoft.io/blog/what-are-decentralized-physical-infrastructure-networks-depin/#:~:text=Let%27s%20explore%20how%20DePIN%20works,to%20that%20of%20venture%20capitalists.

[**Lep24]** Mensholong Lepcha. Decentralized physical infrastructure network (depin). *Techopedia*, 2024. URL: https://www.techopedia.com/definition/decentralized-physical-infrastructure-networks-depin#:~:text=Decentralized%20physical%20infrastructure%20networks%20(DePINs)%20are%20blockchain%20protocols%20that%20build,%2C%20data%20collection%2C%20and%20more.

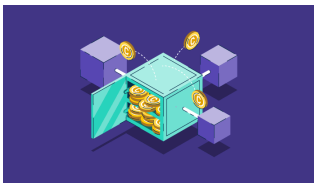
[Sar23](1,2) Dipankar Sarkar. Generalised depin protocol: a framework for decentralized physical infrastructure networks. *arXiv preprint arXiv:2311.00551*, 2023.

[**Sch24]** Louis Schoeman. Filecoin reviewed. *SA Shares*, 2024. URL: https://sashares.co.za/filecoin-review/#gs.83eb6f.

[**Sel24]** Ryan Selkis. Crypto theses 2024. *Messari*, 2024. URL: https://resources.messari.io/pdf/crypto-theses-for-2024.pdf.

Academic Insights

A Comparative Analysis of Different Proof of Stake Consensus Mechanisms



Exploring the World of Maximal Extractable Value (MEV) in Blockchain

A Comparative Analysis of Different Proof of Stake Consensus Mechanisms

Academic insight

Key Insights

- Platt et al.'s paper underscores the high energy consumption of Proof of Work (PoW) systems like Bitcoin and highlights the relative energy efficiency of Proof of Stake (PoS) systems.
- The energy usage of PoS blockchains is significantly influenced by the hardware used by validators, emphasizing the importance of hardware selection in these systems.
- There are notable variations in energy consumption among different PoS systems, influenced by various factors such as system design, implementation, and the number of validator nodes
- Hedera, a permissioned DLT system, showcased the lowest energy consumption per-transaction in the study. This highlights Hedera's superior efficiency and positions it as a sustainable option in the blockchain sector.
- The authors developed a unique model to measure energy consumption on a per transaction basis in PoS blockchains, providing a nuanced understanding of energy usage
- The research advocates for a transition from energy-intensive PoW systems to more efficient PoS systems, suggesting that energy-saving hardware could drastically reduce energy consumption in PoS systems.

Introduction

Platt et al. [PSP+21] in their academic paper, "The Energy Footprint of Blockchain Consensus Mechanisms Beyond Proof-of-Work", delve into the energy implications of different blockchain consensus mechanisms, primarily Proof of Work (PoW) and Proof of Stake (PoS). The authors highlight the extreme energy consumption of PoW systems, exemplified by Bitcoin, which has attracted criticism due to its environmental impact. As an alternative, PoS mechanisms aim to be more energy-efficient. However, the paper underscores that the energy consumption of PoS blockchains also depends greatly on the type of hardware used by validators.

The authors make a comparative analysis of different PoS systems, shedding light on their energy consumption patterns. They argue that the energy efficiency of consensus mechanisms is a vital factor determining their effectiveness and suitability for use in distributed ledger technology (DLT) systems. Their work underscores the need for more focused research and an understanding of the energy implications of these mechanisms in the rapidly evolving world of blockchain technology.

The Energy Intensity of Blockchain Consensus Mechanisms and Bitcoin's Overwhelming Energy Footprint

Proof-of-Work (PoW) systems like Bitcoin are criticised for their high energy requirements, comparable to those of industrialised nations, due to their correlation with market capitalization [SBFK20]. Proof-of-Work (PoW) is a mechanism designed to resist Sybil attacks, and it has been implemented in many of the initial cryptocurrencies [Nak08]. This raises sustainability concerns. Platt et al. [PSP+21] demonstrate that Proof-of-Stake (PoS) systems, which prioritise validators with higher stakes in the native currency, significantly reduce energy consumption. Despite this, Bitcoin's energy use dwarfs that of all analysed PoS systems by at least two orders of magnitude, emphasising the potential of PoS as a more sustainable alternative [IM19].

Variation in Energy Footprint and Consumption Patterns Among PoS Systems

There are marked variations in energy consumption among PoS systems. Factors such as system design, implementation, hardware used, number of validator nodes, and system throughput contribute to this variation. Permissionless systems, in particular, display larger energy footprints, indicating that these factors significantly affect their energy efficiency. Furthermore, the hardware employed by validators substantially influences the energy consumption of PoS blockchains, with the energy usage of a validator node discovered to be independent of system throughput in the permissionless systems analysed. Especially less active permissionless systems demonstrate a higher energy demand per transaction due to lower throughput and a large number of validators [Car21].

Methodology Overview

The authors assumed that the validating nodes would run on comparable server hardware types, regardless of network load. Thus, the overall energy requirement of a protocol was attributed exclusively to the number and the specific hardware configuration of the validator nodes. Three different hardware configurations were considered to cover the potential hardware variation and expected hardware usage: a single-board computer, a rack-mount server for midsize and large enterprises, and a high-performance server. This holistic approach allowed for a nuanced analysis of energy consumption across PoS blockchains.

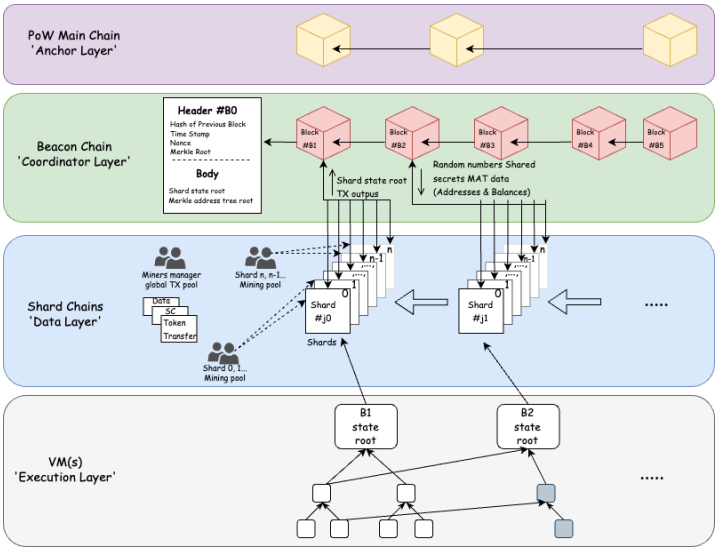


Fig. 6 Ethereum 2.0's Consensus Mechanism.

Examination of PoS DLT Systems

The study [PSP+21] examined several high market capitalization DLT systems employing a PoS consensus algorithm, including Ethereum 2.0 with 183,753 validators, Algorand with 1,126 validators, Cardano with 2,958 validators, Polkadot with 297 validators, Tezos with 399 validators, and Hedera with 21 validators. These systems, despite their shared usage of PoS, vary in numerous aspects, such as minimum thresholds for validation and delegation, the need to lock up stakes, and rewards for validators. These findings provide a comprehensive view of the energy consumption landscape on PoS-based blockchains.

- **Bitcoin:** The energy consumption of Bitcoin, which uses a Proof-of-Work (PoW) consensus mechanism, exceeds the energy consumption of all Proof-of-Stake (PoS)-based systems analysed by at least two orders of magnitude.
- **Ethereum 2.0:** Ethereum 2.0, which is transitioning to a PoS consensus mechanism, is expected to have significantly lower energy consumption than Bitcoin. However, the exact energy consumption varies depending on the throughput of the system.
- **Algorand:** Algorand, a PoS-based permissionless system, has lower energy consumption than Bitcoin and Ethereum 2.0. The energy consumption per transaction is relatively low due to its high throughput and a small number of validators [GHM+17].
- **Cardano:** Cardano, another PoS-based system, also has lower energy consumption than Bitcoin. However, it consumes more energy than Algorand due to its lower throughput and higher number of validators.
- **Polkadot and Tezos:** These PoS-based systems have lower energy consumption than Bitcoin and Ethereum 2.0. However, their energy consumption is higher than that of Algorand and lower than that of Cardano.
- **Hedera:** Hedera, a permissioned system, has the lowest energy consumption per transaction among the systems analysed. This is due to its high throughput and small number of validators. Transactions don't aggregate into blocks. Instead, they disseminate through a "gossip about gossip" protocol, where any new information acquired by a node is propagated exponentially quickly throughout the network [Hed21].

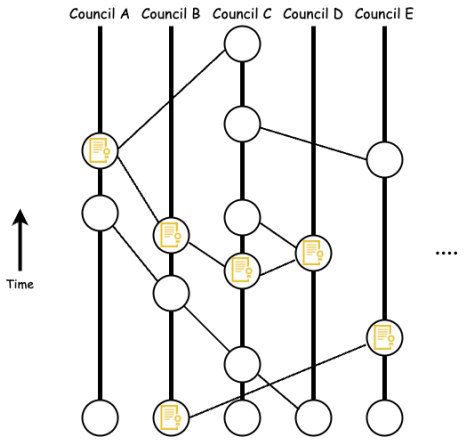


Fig. 7 Hedera's Consensus Mechanism.

The study [PSP+21] conducted an in-depth analysis of various Distributed Ledger Technology (DLT) systems, focusing on their consensus mechanisms, number of validators, throughput, and energy consumption. The findings highlighted the necessity of transitioning from energy-intensive Proof of Work (PoW) systems, such as Bitcoin, to more energy-efficient Proof of Stake (PoS) systems.

Bitcoin's PoW system was found to be at least three orders of magnitude higher in energy consumption than the most energy-consuming PoS system. Most PoS systems were found to consume less energy than the VisaNet payment network.

Significant differences in energy consumption were observed among the PoS systems studied. These differences were ascribed to the number of validators, the throughput of the systems, and the type of hardware utilised by the validators. For instance, Hedera, a permissioned system with 21 validators, showed the least energy consumption per transaction. Conversely, systems with more validators and lower throughput had higher energy demands.

The study identified the assumption that the number of validators is an affine function of throughput as a limitation. Future studies were recommended to consider the network-wide energy consumption beyond validator nodes for a more comprehensive understanding of the energy usage in DLT systems.

Conclusion

Platt et al. [PSP+21] emphasised the urgent need for transitioning from energy-intensive PoW systems to more efficient PoS systems. Their analysis reveals that by opting for energy-saving hardware, PoS systems could drastically lower their energy consumption, potentially outperforming even traditional central payment systems in terms of energy usage. This research injects optimism into the discourse around blockchain technology's role in addressing climate change. Moreover, it serves as an important call to action for blockchain developers and practitioners, urging them to prioritise energy efficiency in their system designs. Utilising benchmarking frameworks to quantify real energy usage could be especially beneficial for permissioned systems that strive for high performance [SRL+21]. In the future, more nuanced models and factors influencing validator count, beyond network throughput, could be considered for a more comprehensive understanding.

Ali Kathia
October 2023

References

| **Car21]** Nic Carter. How much energy does bitcoin actually consume?,,,. *Harvard Business Review*, 2021.

| **GHM+17]** Yossi Gilad, Rotem Hemo, Silvio Micali, Georgios Vlachos, and Nickolai Zeldovich. Algorand: scaling byzantine agreements for cryptocurrencies. In *Proceedings of the 26th symposium on operating systems principles*, 51–68. 2017.

| **Hed21]** Hedera. What is gossip about gossip? *Hedera*, 2021. URL: https://hedera.com/learning/hedera-hashgraph/what-is-gossip-about-gossip.

| **IM19]** Leila Ismail and Huned Materwala. A review of blockchain architecture and consensus protocols: use cases, challenges, and solutions. *Symmetry*, 11(10):1198, 2019.

| **Nak08]** Satoshi Nakamoto. Bitcoin: a peer-to-peer electronic cash system. *Decentralized business review*, pages 21260, 2008.

[PSP+21](1,2,3,4,5,6) Moritz Platt, Johannes Sedlmeir, Daniel Platt, Jiahua Xu, Paolo Tasca, Nikhil Vadgama, and Juan Ignacio Ibañez. The energy footprint of blockchain consensus mechanisms beyond proof-of-work. In *2021 IEEE 21st International Conference on Software Quality, Reliability and Security Companion (QRS-C)*, 1135–1144. IEEE, 2021.

| **SBFK20]** Johannes Sedlmeir, Hans Ulrich Buhl, Gilbert Fridgen, and Robert Keller. The energy consumption of blockchain technology: beyond myth. *Business & Information Systems Engineering*, 62(6):599–608, 2020.

| **SRL+21]** Johannes Sedlmeir, Philipp Ross, André Luckow, Jannik Lockl, Daniel Miehle, and Gilbert Fridgen. The dlps: a new framework for benchmarking blockchains. *AIS*, 2021.

Exploring the World of Maximal Extractable Value (MEV) in Blockchain

Academic insight

Key Insights

- MEV's impact extends beyond transaction ordering profits, influencing network congestion and fee inflation, with miners potentially altering their behaviour to chase these extractable values.
- To reduce the manipulative impact of MEV on transaction order, proposals for including transactions based on objective metrics like gas prices or timestamps are being examined.
- The emergence of specialised roles, including arbitrage traders and bot operators, signifies the development of a sophisticated MEV ecosystem, focusing on the optimisation of transaction placement for maximum returns.
- To enhance the fairness of blockchain networks, new protocols are being developed that aim to level the playing field by minimising the advantages of MEV for miners with greater computational resources.
- To protect end users from predatory MEV strategies, such as sandwich attacks, solutions are being researched that would obscure transaction details from potential attackers.
- To maintain the integrity of consensus mechanisms in the face of MEV, strategies are being considered that could deter miners from deviating from honest practices for short-term gains.

Introduction

Maximal Extractable Value (MEV) also known as Miner Extractable Value (MEV), an increasingly crucial topic in the realm of blockchain research, refers to the monetary advantage a miner can acquire by strategically manipulating transactions in a block they produce. Recent studies have begun to shed light on the complexities of MEV, exposing both its potential threats and opportunities within the blockchain infrastructure. This science note offers an in-depth analysis of recent academic findings, focusing on the operational dynamics of MEV, its implications on the fairness and security of blockchain networks, and the proposed solutions to mitigate its effects.

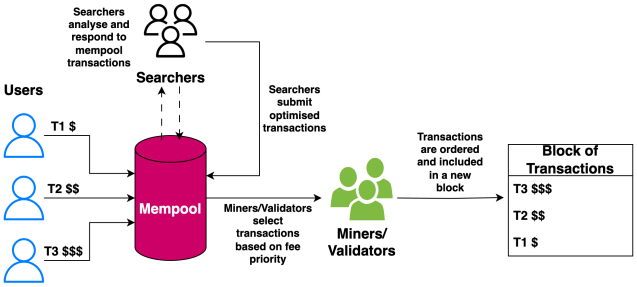


Fig. 8 Transaction Prioritisation in the Context of Miner Extractable Value (MEV).

The concept of Miner/Maximal Extractable Value (MEV) was coined by Daian et al. [DGK+20] to define the maximum profit a miner can secure by strategically adjusting transaction sequences. This practice, prevalent in various financial applications, has evolved into a profitable industry dominated by specialised searchers like arbitrage traders and bot operators. These searchers focus on identifying opportunities and constructing transactions to maximise MEV, often involving the precise placement of transactions.

In blockchains supporting smart contracts, miners or validators prioritize transactions with higher fees for inclusion in blocks, impacting the mempool where unconfirmed transactions wait, often delaying those with lower fees. A common MEV scenario involves miners exploiting arbitrage opportunities on trading platforms, sometimes leading to bidding wars with bots for higher transaction fees [Cha22].

The impact of MEV is significant, particularly on end users who pay transaction fees, and on miners who select transactions based on these fees to maximise profits. While MEV is a relatively new field, it has already seen substantial research focused on understanding, quantifying, and mitigating its effects, especially in terms of common sources of MEV and the security concerns they pose. Common strategies include front running, where transaction fees are exchanged for block space with non-miner MEV extractors, and back running, which involves manipulating transactions for profit from on-chain events [Cha22].

Frontrunning: This involves placing the attacker's transactions ahead of the victim's. For instance, an attacker may offer higher transaction fees to ensure their transaction gets executed first to exploit a rare market opportunity. Block space is sold to non-miner MEV extractors in return for transaction fees through Priority Gas Auctions.

Backrunning: In this scenario, the attacker places their transaction right after the victim's transaction to take advantage of the market change initiated by the victim. For instance, if a transaction on Exchange X significantly increases an asset's price, it opens an arbitrage opportunity. Here, the backrunner could purchase the same asset from another exchange, X′, at a lower cost and then sell it on X, keeping the price difference [YZH+22]. In this scenario, the backrunner's transaction does not harm the user and aids in maintaining price consistency between the two exchanges. In a similar context, backrunning can also be used to capitalise on Oracle updates for liquidation opportunities [QZG+21].

Sandwich Attacks: Sandwich attacks present a more complex MEV extraction method where the attacker places two transactions, one before and one after the victim's regular trade. The goal is to manipulate asset prices in such a way that the attacker benefits from the victim's loss [ZQT+21]. However, executing sandwich attacks can be risky for the attacker as any deviation from the desired transaction order can lead to financial loss. In most cases, these attacks are executed via MEV auction platforms.

Bribery Attacks: Attackers may generate MEV to encourage miners to act in their favour, this is known as a bribery attack. These attacks can range from incentivizing miners to temporarily delaying a transaction by offering higher fees for a conflicting transaction to more complex schemes facilitated by smart contracts [TYME21] [WHF19]. The impact of bribery attacks varies depending on the specific application.

Impact on Blockchain Fairness and Security Risks

Eskandari et al. [EMC20] highlighted a disconcerting aspect of economic inequality that MEV introduces into a system fundamentally designed for decentralisation and equality. Their research showed that miners with more significant computational resources are advantaged, leading to an unequal distribution of wealth and power within the network. This core issue necessitates more rigorous examination and underscores the urgency for remedies that re-establish equilibrium and honour the essential principles of blockchain technology.

Financial Losses

Certain forms of MEV extraction can result in direct financial losses for users. A case in point is the predatory sandwich attacks, which led to profits exceeding $3 million for attackers in November 2022 alone [Eig22]. This substantial gain was, unfortunately, the result of monetary losses suffered by the victims.

Inefficiencies Stemming from Coordination Deficit

The competitive pursuit of MEV by bots can lead to on-chain bidding battles. These contests may contribute to network traffic jams and inflate transaction costs. Some strategies intended to counter MEV can unintentionally trigger other forms of inefficiency. For instance, implementing a first-come-first-served transaction ordering can shift the competitive battleground to off-chain latency, thereby instigating off-chain latency wars among MEV searchers.

Threat to Consensus Stability

Carlsten et al. [CKWN16] demonstrated that when transaction fees surpass block rewards, miners may stray from honest mining practices. They could create forks with high-fee blocks to entice other miners to contribute to their forks. MEV can be seen as an expanded form of transaction fees directed to the miner, and a significant MEV can amplify this issue. Today, lucrative MEV extraction often outweighs block rewards [Fla22].

derived from MEV.

A Catalyst for Centralisation

Vitalik [But21] asserted that MEV could foster centralisation given the notable economies of scale associated with uncovering complex MEV extraction opportunities. A future dominated by centralisation and monopoly is undesirable as it undermines the principles of transparency and decentralisation. There's also a concern that MEV could promote "vertical integration" [HG22] where miners and traders combine to establish exclusive systems. This development could potentially jeopardise the transparency and permissionless nature of the blockchain.

Solutions and Future Directions

MEV Auction Platforms

MEV auction platforms serve to facilitate auctions that allocate block space to users who place bids for their transaction inclusion. They place a high emphasis on transaction privacy and atomicity. Their services are mostly availed by MEV searchers, who carry out their MEV extraction transactions covertly, and regular users who protect their transactions from being exposed to searchers [YZH+22].

With the Ethereum merge, MEV auction platforms bifurcated into pre-merge and post-merge types. Pre-merge platforms like Flashbots and Eden Network use first-price sealed-bid auctions. Post-merge platforms are set to see native support in the form of a Proposer-Builder Separation (PBS) protocol in future Ethereum versions. However, an interim realisation, MEV-Boost, continues to rely on trusted relays. For users exclusively interested in privacy, these platforms offer private channels that can be accessed via RPC endpoints [YZH+22].

Time-Based Transaction Ordering

Time-based ordering properties form a category of solutions aimed at preventing transaction order manipulation in the blockchain ecosystem. The concept, initially proposed by Kelkar et al. [KZGJ20], is built around "receive-order fairness," which is a first-come-first-served approach to transaction ordering. This notion has been further explored and improved upon by systems, which offer enhanced liveness and reduced communication complexity.

In the field of transaction ordering, relative fairness has also been a focus of exploration. Kursawe et al. [Kur20] propose the concept of relative fairness, stipulating that if all honest validators see transaction T before a given time and another transaction T′ after this time, T should be scheduled before T′. Zhang et al. [ZSC+20] offer a similar concept called ordering-linearizability. While there are slight differences in these approaches, they can be integrated into a single property referred to as fair separability.

Baird et al. [Tea20], in their exploration of Hashgraph, introduce a method that assigns each transaction a fair timestamp, derived from the median time that each node reports receiving the transaction first. A potential vulnerability in this method, however, is that a single adversary could manipulate a median-time-based order.

Conclusion

MEV, while a challenging facet of the blockchain universe, offers valuable insights into the intricate dynamics of blockchain systems. Its study reveals critical areas of vulnerability, while also inspiring new strategies for enhancing system fairness and security. As the blockchain landscape continues to grow and evolve, addressing the issue of MEV will remain a pivotal focus in ongoing academic research and technological innovation.

Ali Kathia
December 2023

References

[**But21]** Vitalik Buterin. Proposer/block builder separation-friendly fee market designs. *Ethereum Research*, 2021. URL: https://ethresear.ch/t/proposer-block-builder-separation-friendly-fee-market-designs/9725.

[**CKWN16]** Miles Carlsten, Harry Kalodner, S Matthew Weinberg, and Arvind Narayanan. On the instability of bitcoin without the block reward. In *Proceedings of the 2016 ACM SIGSAC conference on computer and communications security*, 154–167. 2016.

[Cha22] (**1**,**2**) Yash Kamal Chaturvedi. Mev in defi. *Ether World*, 2022. URL: https://etherworld.co/2022/04/05/mev-research-report/.

[DGK+20] (**1**,**2**) Philip Daian, Steven Goldfeder, Tyler Kell, Yunqi Li, Xueyuan Zhao, Iddo Bentov, Lorenz Breidenbach, and Ari Juels. Flash boys 2.0: frontrunning in decentralized exchanges, miner extractable value, and consensus instability. In *2020 IEEE Symposium on Security and Privacy (SP)*, 910–927. IEEE, 2020.

[**Eig22]** EigenPhi. Sandwich overview | eigenphi. *EigenPhi*, 2022. URL: https://eigenphi.io/mev/ethereum/sandwich.

[**EMC20]** Shayan Eskandari, Seyedehmahsa Moosavi, and Jeremy Clark. Sok: transparent dishonesty: front-running attacks on blockchain. In *Financial Cryptography and Data Security: FC 2019 International Workshops, VOTING and WTSC, St. Kitts, St. Kitts and Nevis, February 18–22, 2019, Revised Selected Papers 23*, 170–189. Springer, 2020.

[**Fla22]** Flashbots. Transparency dashboard | flashbots. *Flashbots*, 2022. URL: https://dashboard.flashbots.net/.

[**HG22]** Hasu and Stephane Gosselin. Why run mev-boost? *Flashbots*, 2022. URL: https://writings.flashbots.net/why-run-mevboost/.

[**KZGJ20]** Mahimna Kelkar, Fan Zhang, Steven Goldfeder, and Ari Juels. Order-fairness for byzantine consensus. In *Advances in Cryptology–CRYPTO 2020: 40th Annual International Cryptology Conference, CRYPTO 2020, Santa Barbara, CA, USA, August 17–21, 2020, Proceedings, Part III 40*, 451–480. Springer, 2020.

[**Kur20]** Klaus Kursawe. Wendy, the good little fairness widget: achieving order fairness for blockchains. In *Proceedings of the 2nd ACM Conference on Advances in Financial Technologies*, 25–36. 2020.

336–350. 2021.

[Tea20] Hedera Team. Hedera technical insights: fair timestamping and fair ordering of transactions. *Hedera*, 2020. URL: https://hedera.com/blog/fair-timestamping-and-fair-ordering-of-transactions.

[TYME21] Itay Tsabary, Matan Yechieli, Alex Manuskin, and Ittay Eyal. Mad-htlc: because htlc is crazy-cheap to attack. In *2021 IEEE Symposium on Security and Privacy (SP)*, 1230–1248. IEEE, 2021.

[WHF19] Fredrik Winzer, Benjamin Herd, and Sebastian Faust. Temporary censorship attacks in the presence of rational miners. In *2019 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW)*, 357–366. IEEE, 2019.

[YZH+22](1,2,3) Sen Yang, Fan Zhang, Ken Huang, Xi Chen, Youwei Yang, and Feng Zhu. Sok: mev countermeasures: theory and practice. *arXiv preprint arXiv:2212.05111*, 2022.

[ZSC+20] Yunhao Zhang, Srinath Setty, Qi Chen, Lidong Zhou, and Lorenzo Alvisi. Byzantine ordered consensus without byzantine oligarchy. In *14th USENIX Symposium on Operating Systems Design and Implementation (OSDI 20)*, 633–649. 2020.

[ZQT+21] Liyi Zhou, Kaihua Qin, Christof Ferreira Torres, Duc V Le, and Arthur Gervais. High-frequency trading on decentralized on-chain exchanges. In *2021 IEEE Symposium on Security and Privacy (SP)*, 428–445. IEEE, 2021.

Industry Perspective

Flash Loan Attacks in Decentralised Finance

Net Zero Banking Alliance: A Token-based Model

Flash Loan Attacks in Decentralised Finance

Industry Perspective

Key Insights

- Flash loans, a distinct DeFi feature, offer uncollateralised loans within a single transaction, providing liquidity for various strategies. Flash loan attacks exploit DeFi vulnerabilities, aiming for high profits with minimal risk, resulting in substantial financial losses across multiple DeFi platforms.
- Attackers use methods like oracle and governance manipulation, front running, and liquidity removal to exploit protocol vulnerabilities.
- Notable flash loan attacks involve price oracles, governance manipulation, and liquidity drainage, showcasing the challenges in securing DeFi protocols.
- Defensive strategies, such as transaction monitoring, requiring approval for flash loan usage, and improved oracle designs, aim to mitigate flash loan attacks. However, the evolving nature of attacks continues to challenge their effectiveness.
- Ongoing research in monitoring, analytics, incentive mechanisms, and oracle designs is crucial to achieve stability in DeFi and maximise its potential. Security challenges persist due to the open and interconnected nature of DeFi protocols.

Introduction

Decentralised finance (DeFi) seeks to replicate traditional financial services, such as lending and trading, using blockchain smart contracts. One notable feature is flash loans—uncollateralised loans that must be repaid within the same transaction [aav23]. Flash loans alleviate liquidity constraints for arbitrage and hedging strategies. However, they also equip potential attackers with capital for market manipulation.

In a flash loan attack, the borrower exploits vulnerabilities to extract profits exceeding the small loan fee. For instance, manipulating oracle prices to secure loans larger than what collateral would permit [aav23]. Flash loan attacks have resulted in over $750 million in losses across various DeFi platforms [DeF].

This science note reviews academic literature that analyses flash loan attacks in DeFi. First, we discuss attacker incentives and common methods. Next, we delve into prominent attack cases and their measurable impacts. Finally, we explore emerging defensive techniques and the remaining challenges. This examination highlights the novel risks posed by flash loans and the difficulties in balancing innovation and security in decentralised systems.

Flash loans leverage the atomicity of blockchain transactions — either all state changes succeed, or all are reverted. This ensures loan repayment before changes take effect [aav23]. Collateral is unnecessary since no counterparty risk is involved. Borrowers only need to pay a small fee (e.g., 0.09%) to the lending pool, making loans capital efficient. Lenders benefit from fee revenue, and borrowing demand boosts overall pool liquidity. However, attackers exploit the fact that flash loans provide almost unlimited capital for market manipulation within a single transaction. Successful attacks yield profits far exceeding the fractional loan fee.

Attack Incentives and Methods

Flash lending made its debut in 2018 by the Marble Protocol and quickly found popularity with traders looking to profit off arbitrage opportunities between decentralised exchanges [aon]. The central incentive for flash loan attacks is to gain substantial profits with minimal risk. Attackers extract value from DeFi protocols before changes are reverted due to failed repayment. Importantly, there is essentially no cost to attempting attacks repeatedly as long as the initial loan is repaid [aav].

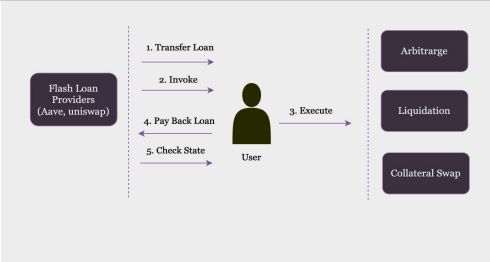


Fig. 9 Typical Flashloan Attack

Typical attack methods include:

- **Arbitrage:** Attackers can use flash loans to execute arbitrage transactions and profit from price differences between different decentralised exchanges (DEXs). Even though this attack may not be malevolent, reputable traders may nonetheless suffer losses as a result of it.
- **Price manipulation:** Attackers can use flash loans to manipulate the price of a cryptocurrency by artificially inflating or deflating its value. This can cause significant losses for traders who have placed orders based on manipulated prices.
- **Removal of liquidity/Smart contract exploits:** Draining pooled reserves through flash borrowing to disable markets or deposit contracts [WWL+21]. Attackers can exploit DeFi smart contract vulnerabilities including re-entrancy issues and integer overflow errors by using flash loans. They might be able to carry out more assaults or steal money from the protocol as a result [Pal].

These techniques combine borrowed capital with issues in incentive design, oracle integrity, and contract logic. Successful attacks across multiple protocols demonstrate how interconnectivity amplifies vulnerabilities [aav23].

Prominent Attack Cases

Recent flash loan assaults have exposed the weaknesses and inherent risks of decentralised finance (DeFi) platforms. Euler Finance experienced a significant breach in March 2023, resulting in 197 million dollars in losses. The hacker was able to influence the platform's borrowing capabilities by exploiting a weakness in Euler's rate computation, notably within the eToken function. Similarly, Cream Finance had a flash loan attack in October 2021, resulting in losses of more than 130 million dollars. The attacker exploited flaws in Cream's yUSDVault in order to double the perceived value of particular tokens. Furthermore, in November 2021, bZx was subjected to a sophisticated hack that included two independent assaults that targeted flaws in the platform's reliance on a single oracle for pricing determination [Pal].

In total, 12 of the top 20 DeFi exploits by profit involved flash loans [DeF], with estimated losses exceeding $750 million. These incidents underscore how flash loans enable complex manipulation that is challenging to anticipate. Attacks are growing in sophistication by combining multiple techniques. These real-world cases emphasise the utmost importance of fortifying security measures, including the implementation of multiple trusted oracles and robust risk management protocols, to fortify DeFi platforms against flash loan attacks and curtail potential financial losses.

Emerging Defensive Techniques

In response to rampant flash loan attacks, several defensive techniques have emerged. One approach involves transaction monitoring and the detection of common attack patterns, such as rapid pumping and dumping of oracles. This allows for pre-emptive action against the attack and transaction reversals.

Another mitigation strategy is to require credit-based approval for flash loan usage in a protocol's smart contracts. While this restricts manipulation using flash loans, it may also compromise the intended flexibility of flash loans. Usage of models like the Recency, Frequency and Monetary model (RFM) which is a marketing technique used to quantify user value based on recency, frequency, and monetary value of purchases. Recency measures how recently a user has made a purchase, Frequency measures how often they purchase, and Monetary measures how much money they spend. Users are segmented into groups based on their RFM scores to identify reliable users.

At the protocol level, leveraging time-weighted average pricing via oracles helps reduce manipulation, as does using the maximum across multiple oracles. However, oracle designs remain a challenge. Additionally, proposals to share liquidity across central and decentralised exchanges can mitigate the impact of liquidity attacks [spr].

Despite these defences, the effectiveness remains elusive as attacks continue to grow more sophisticated. Inherent challenges persist in securing economic protocols atop public blockchains that permit open access [WWL+21].

Conclusion

In summary, flash loans offer both capital efficiency and the potential for manipulation. Numerous DeFi protocols and users have fallen victim to sophisticated attacks, resulting in damages exceeding $750 million to date. Technical and economic solutions are still evolving, but following best practices like third-party auditing, re-entrancy guards and credit-based checks can mitigate the risks of such attacks immensely.

It is important to stay updated with the latest best practices and reports as the DeFi landscape is continuously evolving, by following best practices and being vigilant, we can help to build a safe DeFi landscape for everyone.

Arafath Shariff
December 2023

References

[DeF] (1,2) De.Fi - DeFi Investing & Yield Farming Platform — de.fi. https://de.fi/incidents. [Accessed 30-12-2023].

[**aon]** Flash Loan Attacks: A Case Study | Aon — aon.com. https://www.aon.com/cyber-solutions/aon_cyber_labs/flash-loan-attacks-a-case-study/. [Accessed 30-12-2023].

[aav23](1,2,3,4) Flash Loans — docs.aave.com. 2023. [Accessed 30-12-2023]. URL: https://docs.aave.com/faq/flash-loans.

[**aav]** aavefoundation. Flash Loans: What Are They & How Do They Work? | CoinLedger — coinledger.io. https://coinledger.io/learn/flash-loans. [Accessed 30-12-2023].

[Pal](1,2) Roman Palamarchuk. Flash Loan Attacks: Risks & Prevention - Hacken — hacken.io. https://hacken.io/discover/flash-loan-attacks/. [Accessed 02-01-2024].

[WWL+21](1,2) Dabao Wang, Siwei Wu, Ziling Lin, Lei Wu, Xingliang Yuan, Yajin Zhou, Haoyu Wang, and Kui Ren. Towards a first step to understand flash loan and its applications in defi ecosystem. 2021. URL: https://doi.org/10.1145/3457977.3460301, doi:10.1145/3457977.3460301.

Net Zero Banking Alliance: A Token-based Model

Industry Perspective

Disclaimer: The views and opinions expressed in this article are solely those of the author

Key Insights

- A token-based model marks a significant evolution in sustainable finance, effectively integrating environmental goals with banking operations, particularly in managing financed emissions.
- Tokens quantify CO2 emissions, offering a precise and transparent method to track and manage emissions in banking activities, aligning financial practices with environmental targets.
- This system allows for nuanced emissions management, supporting intertemporal and cross-industry compensation, and enhancing efforts to achieve Net Zero goals.
- Utilising blockchain technology for CO2 tokens adds a layer of security and efficiency, fostering trust in the banking sector's environmental commitments.
- The model shifts focus from traditional metrics to the actual purpose of financing, ensuring a more accurate impact in reducing banking portfolios' carbon footprint.
- Despite its potential, the model's implementation faces challenges such as stakeholder alignment, regulatory compliance, and balancing financial and environmental objectives, underscoring the need for ongoing adaptation in sustainable finance.

Introduction

ESG, an acronym that stands for Environmental, Social, and Governance, represents a paradigm shift in how businesses, financial systems, and investors evaluate the impact of their activities. While the three pillars—environmental, social, and governance—reflect distinct dimensions, our spotlight falls distinctly on the environmental realm, echoing the growing urgency to address climate change and environmental sustainability.

Within the environmental spectrum, the concept of emissions is stratified into three critical scopes, each bearing a unique set of challenges and opportunities.

Scope 1 emissions encompass direct emissions from sources owned or controlled by the bank, which typically include internal combustion engines and on-site energy production. These emissions are directly measurable and quantifiable, forming the foundational layer of a bank's carbon footprint.

Scope 2 emissions, on the other hand, entail indirect emissions associated with the electricity, heating, and cooling consumed by a bank. While not originating directly from the bank, Scope 2 emissions are nevertheless a consequence of the bank's operations, highlighting the necessity to transition towards cleaner, renewable energy sources.

Scope 3 emissions broaden the horizon, encompassing a web of indirect emissions that result from a bank's value chain. This includes emissions linked to the bank's customers, suppliers, and the lifecycle of products and services. Thus, a bank's Scope 3 emissions essentially comprise the Scope 1 and Scope 2 emissions of their customers. Consequently, it is common to refer to these as 'financed emissions' [nat23].

Furthermore, one of the most important metrics in the ESG world is CO2 Equivalent (CO2e) [eur23]. It quantifies emissions in terms of the amount of CO2 that would exert an equivalent warming effect over a specified period. Understanding CO2e is vital for assessing and mitigating environmental impact.

CO2 Equivalent (CO2e)

CO2 equivalent, often abbreviated as CO2e, is a crucial measurement that represents a unified metric encompassing various greenhouse gases' impact on global warming.

In this article, we aim to explore the links between the banking system and its financed emissions. The Net Zero Banking Alliance [une23] stands at the forefront of this exploration. This collaborative coalition of banks and financial institutions is dedicated to mitigating climate change. Its primary goal is to address 'Scope 3' emissions, which constitute the largest portion of a bank's emissions. Banks participating in this initiative commit to reducing their CO2e footprint, particularly by focusing on their Scope 3 emissions. From the customers' perspective, these are equivalent to Scope 1 and Scope 2 emissions, often termed 'financed emissions.' In addition to reducing emissions, these banks support sustainable initiatives. This alliance is crucial in reshaping the financial sector's role in environmental conservation. Its goals include a 55% reduction in financed emissions by 2030 and, by 2050, balancing any remaining financed emissions with activities that remove an equivalent amount of greenhouse gases from the atmosphere, such as afforestation, reforestation, and carbon capture technologies [Uni23] [SA23].

For financial institutions, joining the Net Zero Banking Alliance is pivotal. It goes beyond just meeting regulatory requirements; it establishes credibility, fosters client trust, and attracts eco-conscious investors. Embracing sustainability, banks contribute to environmental protection and enhance their long-term viability and resilience against climate-related risks.

Additionally, being a pioneer in adopting the Net Zero approach proactively can provide a competitive edge in the growing arena of green assets. Contrary to the common misconception of a trade-off between emissions and profits, it is possible to cut this trade-off by highlighting the potential for simultaneous environmental stewardship and financial growth.

and not as effective from an ESG optimisation perspective. In other words, it is not fully efficient in reducing the carbon footprint of current bank portfolios.

Net Zero as-Is mechanics

Current strategies and methodologies in the banking industry involve several key steps to integrate Net Zero principles:

- **Identifying Industry Perimeter:** A bank should identify which industries want to consider its Net-Zero analysis. A bank can have a baseline for each industry analysed. Industry perimeters (e.g., Oil & Gas, Power, Steel, etc.) are identified based on NACE codes [Eur10] related to customers as present in Master Data information. This is one of the most significant pain points. The Net Zero methodology should be linked to the purpose of the financing, not the NACE code of the company. For example, general financing with no clear purpose should no longer be allowed. If a steel company has a loan for installing photovoltaic panels to generate renewable energy for its activities, this loan should not be included in the Net Zero baseline for the Steel industry. This represents a major data quality issue in banks. It's crucial to start an initiative to map the real purpose of historical loans (i.e., stock) to avoid withdrawing credit lines from companies that are paradoxically implementing ESG strategies, as in the steel company example. According to the standard and as-is Net Zero approach, general financing towards steel (typically mapped with steel NACEs) should be avoided due to the carbon intensity emissions of the steel industry. However, financing for renewable energy, mapped with specific NACEs related to the specific purpose of financing and not to the industry, will highlight an ESG benefit derived from this financing. In conclusion, it is crucial to analyse these additional problems related to NACEs.

Consider that banks' Master Data databases typically assign a single NACE to holding companies or heterogeneous groups. For Holding Companies, a generic NACE is inserted. From a climate and net-zero perspective, this generic holding NACE is not useful. Take, for example, a large Oil & Gas group, comprising a holding and various operating companies. The holding company often manages financial activities for the operating companies, leveraging its bargaining power with banks for better interest rates. The funds from banks are, as expected, used not for holding activities but for the operating companies' activities, which relate to the oil & gas industry. For a consistent Net-Zero methodology, it is crucial to consider the real NACE underlying this group, which is the Oil & Gas NACE, not the Holding one.

In the case of heterogeneous Groups, like Amazon, which spans e-commerce, IT and cloud services, gaming, etc., banks usually map in their Master Data the so-called main NACE, often based on a turnover analysis. This main NACE is linked to the department/product/function generating the most turnover. While this is a quick solution for Master Data issues, from a climate and net zero methodology standpoint, if a heterogeneous group has diverse ESG profiles (e.g., e-commerce and servers have different climate anf environmental profiles due to servers' higher water usage compared to e-commerce activities, and e-commerce activities producing more CO2 Scope 1 due to trucks delivering goods), it becomes important to re-classify this group according to its legal entities. This re-classification helps in understanding how many ESG profiles exist and which entity truly needs a net-zero commitment and action plan.

- **Credit features: lifecycle or status:** Credit features, particularly the lifecycle or status of a credit, significantly impact the baselines for financed emissions. Emissions are linked to financed companies, and the characteristics of granted credit play a crucial role in the construction of these baselines. For example, a 30-year credit with 5 years remaining requires the bank to assess its strategic value in the portfolio, impacting whether it's renewed or not. Once such a credit expires, its associated financed emissions are removed from the Net Zero metrics, improving the bank's carbon footprint. This is especially true when credits are at zero residual maturity. Additionally, the credit status, reflecting the borrower's creditworthiness, is a key factor. Credits in good standing that turn non-performing (due to repayment issues) can paradoxically improve Net Zero values. Non-performing credits, often linked to operationally troubled companies, imply reduced emissions. When offloaded by the bank, these credits no longer affect its net-zero metrics. However, including non-performing exposures (NPEs) in baselines without adjustment can lead to inflated baselines and significant apparent reductions in carbon footprints in subsequent years, a form of greenwashing. Therefore, it's best practice to exclude loans with less than a year of residual maturity and to be cautious about including NPEs in baselines to avoid artificially inflated metrics and misleading progress towards Net Zero targets.
- **Common Metrics Towards Various Industries in Net Zero Baseline:** Establishing common metrics for various industries is essential in the Net Zero baseline.
- **Calculating EVIC for Each Customer:** EVIC, or Enterprise Value Including Cash, is calculated as the sum of the ordinary shares' market capitalisation at the fiscal year-end, the market capitalization of preferred shares at the fiscal year-end, and the book values of total debt and minority interests [Man22]. The current calculation methodology involves determining the proportion of a company's EVIC that is attributable to a specific bank.

Enterprise Value Including Cash (EVIC)

Enterprise Value Including Cash (EVIC) is defined as the aggregate of the market capitalization of a company's ordinary and preferred shares at the end of the fiscal year, combined with the book values of its total debt and minority interests, without subtracting any cash or cash equivalents to preclude the occurrence of negative enterprise values.

Net Zero as-is approach		
Bank 1	**Steel company**	
Total assets €500m	EVIC	€1b
	Bank 1 loan to Steel company	€100m
	Bank 2 loan to Steel company	€200m
	Bank 3 loan to Steel company	€400m
	etc.	
	% EVIC attributable to Bank 1	**10%**
	€100m / €1b	

For example, let's consider a steel company with a €1 billion EVIC, financed by several banks. If Bank 1 has extended a loan of €100 million to this company, it means Bank 1 holds 10% of the steel company's EVIC. According to the Net Zero methodology, 10% of the steel company's emissions (Scope 1 and Scope 2) are then attributable to Bank 1's financed emissions (Scope 3), and this 10% contributes to Bank 1's Net Zero emissions baseline.

However, this is another point of contention. For a bank joining the Net Zero Banking Alliance, it's more relevant to consider the proportion of the loan granted to the steel company in relation to the bank's balance sheet, rather than the other way around. This requires a paradigm shift in the calculation approach. The table below illustrates this concept.

Total assets	€500m	EVIC	€1b
		Bank 1 loan to Steel company	€100m
		Bank 2 loan to Steel company	€200m
		Bank 3 loan to Steel company	€400m
		etc.	
% of loan towards steel company out to Bank 1's total assets €200m / €1b	**20%**		

As demonstrated in this example, and comparing the two tables, the accurate ratio to consider should be 20%, not 10%. This 20% represents the portion of the steel company's emissions that should be attributable to Bank 1's Net Zero baseline.

This paradigm shift enables the consideration of the coefficient of transformation of brown assets into green assets, which serves as a proxy for a bank's ability to transition from a high-carbon to a low-carbon economy. Consider the following example:

- A small bank with a balance sheet of €10 million, where its only asset is a €10 million loan to a carbon-emitting company.
- A large bank with a balance sheet of €10 billion that lends €1 billion to the same carbon-emitting company, despite the large bank having 100 times the amount of EVIC (Economically Viable Investment Capital) compared to the small bank.

Which bank is environmentally better? The small bank, with no margin or time to transition from brown assets (the €10 million loan to the carbon-emitting company), finds itself stuck. The loan is already granted and cannot be withdrawn, given its medium to long-term nature. Therefore, its coefficient of transformation of brown assets into green assets is zero, as it cannot invest in green assets. Financially, it isn't viable to sell the entire credit to another institution due to the necessity of accepting a high discount rate, which could lead to financial troubles due to its lack of bargaining power.

In contrast, the large bank has €9 billion available to invest in green assets, as brown assets constitute only 1/10th of its total assets (€1 billion). This significant sum allows the bank to consider divesting from the €1 billion by selling the credit to another financial institution without encountering financial difficulties.

So, paradoxically, from an environmental standpoint (considering a bank's transition capability from a high-carbon to a low-carbon economy), the large bank is more advantageous than the small bank, having both the means and the capital to invest in green assets.

Returning to our data tables, please consider this example:

Net Zero proposed approach			
Banks		**Steel company**	
Bank 1 - Total assets	€1000m	EVIC	€10b
Bank 2 - Total assets	€1000m	Bank 1 loan to Steel company	€1000m
Bank 3 - Total assets	€1000m	Bank 2 loan to Steel company	€1000m
Bank 4 - Total assets	€1000m	Bank 3 loan to Steel company	€1000m
Bank 5 - Total assets	€1000m	Bank 4 loan to Steel company	€1000m
Bank 6 - Total assets	€1000m	Bank 6 loan to Steel company	€1000m
Bank 7 - Total assets	€1000m	Bank 6 loan to Steel company	€1000m
Bank 8 - Total assets	€1000m	Bank 7 loan to Steel company	€1000m
Bank 9 - Total assets	€1000m	Bank 8 loan to Steel company	€1000m
Bank 10 - Total assets	€1000m	Bank 9 loan to Steel company	€1000m
		Bank 10 loan to Steel company	€1000m
% of loan towards steel company out to Bank X's total assets €1000m / €10b	**10%**		

As you can see, no double-counting mechanism is in place.

- **Setting Baseline Years and Targets:** Financial institutions establish baseline perimeter criteria and specific emission reduction targets for high-emission industries, including cement, aviation, automotive, oil & gas, and the power sector. Each perimeter comprises a list of companies operating in one of these industries that meet certain pre-determined criteria, serving as the starting point for evaluating environmental impact. Criteria examples may include the exclusion of non-performing exposures, mid-caps, high-capitalisation companies, and certain low-emitting industries, among others.
- **Monitoring at Company and Portfolio Levels:** Banks meticulously monitor emissions data at both the company and portfolio levels, with detailed expectations for emission reduction. Actual emission values are compared against expected detailed GHG values during the Net Zero time horizon (2030 and 2050), facilitating a comprehensive analysis of the environmental impact [SA22].
- **Plethora of Metrics:** The metrics used within banks and industries, especially in the Oil & Gas sector, are not uniform. For example, Credit Agricole's Net Zero Oil & Gas targets [SA23] include 'Scope 1&2 of all counterparts and Scope 3 of upstream players, based on our on-balance sheet exposure.' In contrast, UniCredit's Net Zero Oil & Gas targets [Uni22a] consider only 'Scope 3, Category 11' [Uni22b]. This example illustrates how targets vary depending on the metrics used. The Net Zero Banking Alliance should ensure a top-down approach that is equal for all market players.
- **Integration of Net Zero in Credit Origination Processes:** It is essential to integrate Net Zero principles into credit origination processes. Each potential counterpart is evaluated from a Net Zero perspective, including determining if the counterpart falls within the baseline perimeter. If it does, the next step is to assess whether the counterpart adheres to the expected reduction plan outlined in Net Zero documents. If the criteria are met, the credit process proceeds; if not, additional documentation and commitments are requested. In some cases, if the criteria are not met, the credit may not be approved, ensuring support only for environmentally responsible businesses.

This meticulous approach should ensure that banks not only adhere to their own sustainability goals but also contribute significantly to the global effort of reducing carbon emissions. By embedding Net Zero principles into their credit evaluation processes, financial institutions play a vital role in promoting environmentally conscious business practices and fostering a greener, more sustainable future.

Net Zero proposed approach

As discussed in the previous section, the current Net Zero approach has several weaknesses, primarily related to the NACE-industry related approach, the plethora of metrics, and the EVIC approach. Additionally, a revised approach should consider the following aspects:

might be overly penalising, particularly for customers with high transition risks, potentially depriving them of the opportunity to set up effective transition plans to reduce their emissions.

2. **Incorporating mechanisms for compensation:** The existing model links the granting of credit to a company's emissions but fails to include mechanisms for compensation:

- Between different companies.
- Within the same bank's portfolio.
- Across various industries that constitute the bank's exposure.

In our view, the challenge lies in **mismatched metrics and the unexploited CO2e potential**. For instance, when companies exceed their emission reduction targets, there remains an unutilised CO2e capacity. This presents an opportunity for financing other businesses, both in general financing and specialised financing domains.

By addressing these issues, the proposed approach aims to create a more balanced and effective strategy for implementing Net Zero principles in the banking sector. This would allow for a more nuanced assessment of companies' emissions and better support the transition towards lower carbon outputs across different industries [San23].

Scenario 1

Values in tons of CO2 equivalents
Scenario 1 - Best Scenario

		Expected emissions evolutions					*Real life emissions evolutions*					*Savings CO2 equivalent/Debit CO2 equivalent*				
Oil & gas portfolio	**Baseline emissions - YEAR X**	**YEAR X+1**	**YEAR X+2**	**YEAR X+3**	**YEAR X+4**	**YEAR X+5**	**YEAR X+1**	**YEAR X+2**	**YEAR X+3**	**YEAR X+4**	**YEAR X+5**	**YEAR X+1**	**YEAR X+2**	**YEAR X+3**	**YEAR X+4**	**YEAR X+5**
Company A	112	95.2	86.8	82.6	80.5	78.4	94.560	86.050	80.026	70.423	64.085	-0.640	-0.750	-2.574	-10.077	-14.315
Company B	195	165.75	151.125	143.813	140.156	136.5	164.670	128.443	106.607	85.286	81.874	-1.080	-22.682	-37.205	-54.870	-54.626
Company C	276	234.6	213.9	203.55	198.375	193.2	231.000	212.520	201.894	171.610	139.004	-3.600	-1.380	-1.656	-26.765	-54.196
Company D	345	293.25	267.375	254.438	247.969	241.5	290.000	234.900	194.967	165.722	134.235	-3.250	-32.475	-59.471	-82.247	-107.265
Company E	2121	1802.85	1643.78	1564.24	1524.47	1484.7	1800.456	1632.670	1387.770	1124.093	910.516	-2.394	-11.105	-176.468	-400.375	-574.184
Company E	3478	2956.3	2695.45	2565.03	2499.81	2434.6	2954.000	2392.740	1985.974	1568.920	1506.163	-2.300	-302.710	-579.051	-930.893	-928.437

This scenario represents the best-case outcome: assuming a target for reducing emissions by 30%, all companies in our example successfully meet this target. Consequently, no CO2 equivalent compensation within the portfolio is necessary.

Subtotals - Savings CO2 equivalent/Debit CO2 equivalent				
YEAR X+1	**YEAR X+2**	**YEAR X+3**	**YEAR X+4**	**YEAR X+5**
-13,264	-371,103	-856,424	-1,505,228	-1,733,023

Total Oil & gas portfolio
-4,479,042

As demonstrated in the data, this portfolio achieves a total savings of 4,479,042 tons of CO2 equivalent. These savings can be transferred from this portfolio to other portfolios that are not generating savings but are accruing CO2 equivalent debits.

Scenario 2

In this scenario, as illustrated in the data below, the portfolio generates a CO2 equivalent debit in years X+1 and X+2. Faced with this situation, the top managers of the Oil & Gas portfolio have a couple of options, according to the proposed model:

- Compensate for the debit by requesting an equivalent amount of CO2 equivalent savings from other portfolios. This approach relies on the inter-portfolio exchange of CO2 credits to balance emissions.
- If they have confidence in the credibility of their customers' transition plans, they can opt to wait for intertemporal compensation within their own Oil & Gas portfolio.

For instance, examining the table provided, it's evident that all companies within the portfolio eventually reach the target reduction of 30%. The previous CO2 debits (related to years X+1 and X+2) are successfully compensated in subsequent years X+3, X+4, and X+5.

Values in tons of CO2 equivalents
Scenario 2 - internal compensation within the portfolio and all companies reach the targets

		Expected emissions evolutions					*Real life emissions evolutions*					*Savings CO2 equivalent/Debit CO2 equivalent*				
Oil & gas portfolio	**Baseline emissions - YEAR X**	**YEAR X+1**	**YEAR X+2**	**YEAR X+3**	**YEAR X+4**	**YEAR X+5**	**YEAR X+1**	**YEAR X+2**	**YEAR X+3**	**YEAR X+4**	**YEAR X+5**	**YEAR X+1**	**YEAR X+2**	**YEAR X+3**	**YEAR X+4**	**YEAR X+5**
Company A	112	95.2	86.8	82.6	80.5	78.4	94.560	86.050	80.026	70.423	64.085	-0.640	-0.750	-2.574	-10.077	-14.315
Company B	195	165.75	151.125	143.813	140.156	136.5	164.670	128.443	106.607	85.286	81.874	-1.080	-22.682	-37.205	-54.870	-54.626
Company C	276	234.6	213.9	203.55	198.375	193.2	246.000	226.320	215.004	182.753	148.030	11.400	12.420	11.454	-15.622	-45.170
Company D	345	293.25	267.375	254.438	247.969	241.5	299.000	285.000	236.550	201.068	162.865	5.750	17.625	-17.888	-46.901	-78.635
Company E	2121	1802.85	1643.78	1564.24	1524.47	1484.7	2010.000	1987.000	1688.950	1368.050	1108.120	207.150	343.225	124.713	-156.419	-376.580
Company E	3478	2956.3	2695.45	2565.03	2499.81	2434.6	2954.000	2392.740	1985.974	1568.920	1506.163	-2.300	-302.710	-579.051	-930.893	-928.437

Subtotals - Savings CO2 equivalent/Debit CO2 equivalent				
YEAR X+1	**YEAR X+2**	**YEAR X+3**	**YEAR X+4**	**YEAR X+5**
220,280	47,127	-500,551	-1,184,080	-1,446,118

Total Oil & gas portfolio
-2,863,342

Scenario 3

In this scenario, as shown in the data below, the portfolio generates a CO2 equivalent debit in years X+1 and X+2. The top managers of the Oil & Gas portfolio, following the proposed model, have several options:

- They can compensate for the debit by requesting an equivalent amount of CO2 equivalent savings from other portfolios, effectively balancing emissions through inter-portfolio exchanges.
- If they trust the credibility of their customers' transition plans, they can opt for intertemporal compensation within their own Oil & Gas portfolio.

However, in contrast to Scenario 2, not all companies within this portfolio achieve the target reduction of 30%. Therefore, according to our model, the previous CO2 debits (related to years X+1 and X+2) are only partially compensated in years X+3, X+4, and X+5.

Additionally, for a company like Company C, which does not meet the target, the top managers face a strategic decision. If Company C is significant for the bank's income statement and balance sheet, they might decide to retain it in the portfolio. Conversely, if Company C is not strategically important from an economic and financial perspective, a run-off strategy may be implemented, or a deeper analysis of the new transition plan could be considered.

This scenario highlights the challenges and strategic decisions involved in managing a portfolio with varying levels of emission reductions and underscores the importance of aligning environmental goals with financial and economic considerations.

		Expected emissions evolutions					Real life emissions evolutions					Savings CO2 equivalent/Debit CO2 equivalent				
Oil & gas portfolio	Baseline emissions - YEAR X	YEAR X+1	YEAR X+2	YEAR X+3	YEAR X+4	YEAR X+5	YEAR X+1	YEAR X+2	YEAR X+3	YEAR X+4	YEAR X+5	YEAR X+1	YEAR X+2	YEAR X+3	YEAR X+4	YEAR X+5
Company A	112	95.2	86.8	82.6	80.5	78.4	94.560	86.050	80.026	70.423	64.085	-0.640	-0.750	-2.574	-10.077	-14.315
Company B	195	165.75	151.125	143.813	140.156	136.5	164.670	128.443	106.607	85.286	81.874	-1.080	-22.682	-37.205	-54.870	-54.626
Company C	276	234.6	213.9	203.55	198.375	193.2	246.000	226.320	215.004	213.456	199.675	11.400	12.420	11.454	15.081	6.475
Company D	345	293.25	267.375	254.438	247.969	241.5	299.000	285.000	236.550	201.068	162.865	5.750	17.625	-17.888	-46.901	-78.635
Company E	2121	1802.85	1643.78	1564.24	1524.47	1484.7	2010.000	1987.000	1688.950	1368.050	1108.120	207.150	343.225	124.713	-156.419	-376.580
Company E	3478	2956.3	2695.45	2565.03	2499.81	2434.6	2954.000	2392.740	1985.974	1568.920	1506.163	-2.300	-302.710	-579.051	-930.893	-928.437

Subtotals - Savings CO2 equivalent/Debit CO2 equivalent				
YEAR X+1	YEAR X+2	YEAR X+3	YEAR X+4	YEAR X+5
220,280	47,127	-500,551	-1,214,782	-1,497,763

Total Oil & gas portfolio
-2,945,689

Scenario 4

In this scenario, none of the companies within our portfolio reach the final target of a 30% reduction in emissions, and all fail to meet the yearly targets from year X+2 onwards.

In such a case, a detailed analysis is required for each company to determine:

- Which companies should be put in run-off due to their inability to meet emission targets?
- Which companies should be retained in the portfolio? This could be because they are strategically important, or they could potentially be financed with green financing, among other reasons.

Moreover, it becomes necessary to compensate for these CO2 debits with emissions savings from another portfolio, such as the power portfolio. This analysis should be conducted annually as soon as the yearly data are available. The focus should be on cherry-picking companies that:

- Are on track to reach the Net Zero pathway.
- Are the most profitable for the bank.
- If they are not on track to reach the Net Zero pathway but are profitable and strategic for the bank's portfolio, they should be financed with green financing to help them align with the Net Zero pathway.

This scenario highlights the need for an ongoing, dynamic approach to portfolio management, balancing environmental targets with financial and strategic considerations. It underscores the importance of adaptive strategies in achieving Net Zero goals while maintaining profitability.

Values in tons of CO2 equivalents
Scenario 4 - no internal compensation within the portfolio and NO company reach the targets

		Expected emissions evolutions					Real life emissions evolutions					Savings CO2 equivalent/Debit CO2 equivalent				
Oil & gas portfolio	Baseline emissions - YEAR X	YEAR X+1	YEAR X+2	YEAR X+3	YEAR X+4	YEAR X+5	YEAR X+1	YEAR X+2	YEAR X+3	YEAR X+4	YEAR X+5	YEAR X+1	YEAR X+2	YEAR X+3	YEAR X+4	YEAR X+5
Company A	112	95.2	86.8	82.6	80.5	78.4	94.560	92.669	86.182	84.458	83.614	-0.640	5.869	3.582	3.958	5.214
Company B	195	165.75	151.125	143.813	140.156	136.5	164.670	161.377	150.080	147.079	145.608	-1.080	10.252	6.268	6.922	9.108
Company C	276	234.6	213.9	203.55	198.375	193.2	246.000	241.080	224.204	219.720	217.523	11.400	27.180	20.654	21.345	24.323
Company D	345	293.25	267.375	254.438	247.969	241.5	299.000	293.020	272.509	267.058	264.388	5.750	25.645	18.071	19.090	22.888
Company E	2121	1802.85	1643.78	1564.24	1524.47	1484.7	2010.000	1969.800	1831.914	1795.276	1777.323	207.150	326.025	267.677	270.807	292.623
Company E	3478	2956.3	2695.45	2565.03	2499.81	2434.6	2954.000	2894.920	2692.276	2638.430	2612.046	-2.300	199.470	127.251	138.618	177.446

Subtotals - Savings CO2 equivalent/Debit CO2 equivalent				
YEAR X+1	YEAR X+2	YEAR X+3	YEAR X+4	YEAR X+5
220,280	594,440	443,502	460,740	531,601

Total Oil & gas portfolio
2,250,563

Tokens for Net Zero Proposed Mechanics

The proposed model for Net Zero banking is founded on several key principles:

1. Compensation of CO2 equivalent within and across portfolios, including intertemporal compensation.
2. Compensation of CO2 equivalent among companies within the same portfolio.
3. The use of tokens and tokenomics as central enablers for the efficient management and allocation of CO2 equivalent units.

Building Blocks of the New Model:

- **Maximising Revenues and Emission Reduction:** This model aims to maximise revenues without exceeding CO2 equivalent targets, effectively eliminating the trade-off between emissions and profits.
- **Introduction of Tokens:** Tokens represent CO2 equivalent units, facilitating efficient and value-driven transactions. These digital tokens are transferable within the bank's organisational structures (e.g., from one portfolio to another) using internal transfer rates.
- **Central Organisational Structure:** A centralised 'CO2 Treasury' manages the CO2 tokens, providing an effective system for reallocating savings from compliant companies to those that are not.

Tokens are digital representations of CO2 equivalent units and possess several characteristics:

- **Fungibility:** Tokens are interchangeable, each having an equivalent value within the system.
- **Divisibility:** Tokens can be divided into smaller units, enhancing liquidity.
- **Intrinsic Value:** Tokens hold real value, making them valuable assets.

Tokenomics governs these tokens, ensuring sustainable supply, stability, and a robust carbon credit ecosystem. The value of these tokens may fluctuate based on various factors and can be transferred with specific penalties or weighting schemes to maximise effectiveness.

Central organisational structure 'CO2 Treasury' can play a crucial role in this model, managing the distribution and movement of CO2 equivalent tokens among portfolios and over time. This centralised system ensures efficient allocation and utilisation, avoiding moral hazards among Relationship Managers.

Utilising blockchain technology can significantly enhance the transparency, security, and efficiency of these transactions. Blockchain provides an immutable ledger that ensures the integrity of token movements, fostering trust among stakeholders. The 'CO2 Treasury' issues these tokens when baselines are established and is the sole official issuer of CO2 tokens within the bank. It is the only organisational structure authorised to move them among bank portfolios. The responsibility for intertemporal movements within the same portfolio lies with the Portfolio Manager.

In summary, the proposed token-based Net Zero banking model represents a significant shift in the industry. By adopting tokens, banks can more effectively navigate the complexities of emissions reductions. This model's key components include maximising revenues, introducing tokens, implementing a central organisational structure, and integrating blockchain technology.

The key findings highlight areas for improvement in As-Is Net Zero mechanics, suggesting a shift in focus to the NACE of loans rather than companies, and assessing loans based on their impact on the bank's balance sheet. Efficient carbon credit management can be achieved through a token-based model that manages CO2 equivalent units effectively, aiding in meeting emissions targets while maximising business opportunities. Furthermore, Blockchain Integration enhances the transparency and security of CO2 token transactions, fostering trust among stakeholders.

Future research on the token-based Net Zero banking model should focus on two key areas: the effectiveness of transferring CO2 equivalent tokens within the banking system, particularly considering penalties and valuation over time, and the impact of this model on banks' business models, risk management, and client relationships. This exploration is crucial for advancing a sustainable and financially viable approach in the banking sector.

Alessio Pezzotta
December 2023

References

[**Eur10]** Europa. List of nace codes. *European Commission*, 2010. URL: https://ec.europa.eu/competition/mergers/cases/index/nace_all.html.

[**eur23]** europa. Glossary:carbon dioxide equivalent. *europa*, 2023. URL: https://ec.europa.eu/eurostat/statistics-explained/index.php?title=Glossary:Carbon_dioxide_equivalent.

[**Man22]** Open Risk Manual. Enterprise value including cash. *openriskmanual*, 2022. URL: https://www.openriskmanual.org/wiki/Enterprise_Value_Including_Cash#:~:text=Definition%20Enterprise%20Value%20Including%20Cash%20(EVIC)%20is%20the,book%20values%20of%20total%20debt%20and%2(

[**nat23]** nationalgrid. What are scope 1, 2 and 3 carbon emissions? *nationalgrid*, 2023. URL: https://www.nationalgrid.com/stories/energy-explained/what-are-scope-1-2-3-carbon-emissions.

[**SA22]** Crédit Agricole S.A. Crédit agricole s.a. details its intermediary targets and action plans to reach carbon neutrality by 2050 on 5 sectors. *Crédit Agricole S.A.*, 2022. URL: https://www.unicreditgroup.eu/en/esg-and-sustainability/net-zero.html.

[SA23](1,2) Crédit Agricole S.A. Crédit agricole s.a. details its intermediary targets and action plans to reach carbon neutrality by 2050 on 5 sectors. *Climate workshop*, 2023. URL: https://www.credit-agricole.com/en/pdfPreview/196180.

[**San23]** Intensa Sanpaolo. Strategy and net-zero. *CLIMATE CHANGE*, 2023. URL: https://group.intesasanpaolo.com/en/editorial-section/a-year-of-sustainability/targets-results-initiatives/climate-change/strategy-and-net-zero.

[**une23]** unepfi. Net-zero banking alliance industry-led, un-convened. *unepfi*, 2023. URL: https://www.unepfi.org/net-zero-banking/.

[**Uni22a]** UniCredit. Overview of key design choices. *Oil&Gas*, 2022. URL: https://www.unicreditgroup.eu/content/dam/unicreditgroup-eu/documents/en/sustainability/NetZero/Oil_and_Gas.pdf.

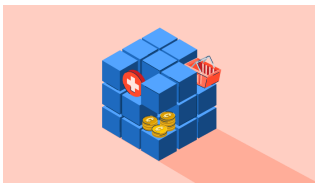
[**Uni22b]** UniCredit. Our path towards net zero. *ESG and Sustainability*, 2022. URL: https://www.unicreditgroup.eu/en/esg-and-sustainability/net-zero.html.

[**Uni23]** UniCredit. Our net zero targets. *UniCredit*, 2023. URL: https://www.unicreditgroup.eu/en/one-unicredit/articles/2023/february/our-net-zero-targets.html.

Innovation & Ideation

The Symbiotic Relationship between Blockchain and Artificial Intelligence

Staking and Reward Mechanisms in Proof of Stake Protocols



The Symbiotic Relationship between Blockchain and Artificial Intelligence

Innovation & Ideation

- Blockchain and AI present a synergistic relationship, where each technology can address the inherent challenges of the other, leading to the creation of a secure, efficient, and intelligent system.
- AI technology can enhance blockchain-based Decentralised Finance (DeFi) operations by providing advanced analytic tools, thus allowing for more sophisticated fund management and yield optimisation.
- An exemplary application of AI in DeFi is SingularityDAO, which uses AI for managing liquidity, predicting market movements, and rebalancing portfolios.
- Challenges such as proving the origin of AI-generated content and computations in blockchain can potentially be addressed with technologies like Zero-Knowledge Machine Learning (ZKML) and blockchain-NFTs for AI models, though these solutions still have limitations and areas for further research and development.

Introduction

Artificial intelligence and blockchain are two progressive technologies with great potential to stimulate the intelligent evolution of various industries. Each possesses inherent strengths but also faces its own unique challenges. AI is gradually transforming industries by introducing advanced capabilities but struggles with issues such as interpretability and effectiveness. It operates based on three key elements: algorithms, computational power, and data [ZSL+21]. On the other hand, blockchain, despite being an advantageous foundation for trustworthy transactions, grapples with hurdles concerning energy consumption, scalability, security, privacy, and efficiency [ZSL+21]. Despite these separate research directions and associated challenges, AI and blockchain exhibit a natural synergy due to shared requirements for data analysis, security, and trust. This intersection between the two technologies can significantly amplify their respective strengths. According to the estimations of Spherical Insights, the Blockchain AI Market, valued at USD 230.10 million in 2021, is projected to grow to USD 980.70 million by 2030 [Ins22]. The merger of these two technologies is an area that still calls for in-depth exploration. Moving forward, we'll examine AI in the context of blockchain, investigating in detail the possible intersections and inherent value these two technologies may possess when coalesced.

The mutual empowerment between blockchain and AI technology

Rohan Pinto, the CTO of 1Kosmos BlockID [Pin18] pointed out that the centralised AI can lead to misuse, including extensive surveillance via facial recognition and computer vision technology. Moreover, developing solutions in a centralised setting necessitates businesses to relinquish privacy and control of their data to third parties. Here, blockchain technology plays a crucial role by potentially addressing several drawbacks associated with AI.

AI algorithms excel at handling vast amounts of data and mimicking cognitive processes akin to the human brain. Utilizing complex neural networks, they recognise patterns, predict outcomes, and make decisions. Conversely, blockchain networks offer a transparent, decentralised, and tamper-resistant transaction layer. Anyone connected to the network can use it, and once data is stored, it becomes unalterable. This allows users to interact with the blockchain in a trust-minimised, permission-less manner.

Blockchain's inherent qualities of decentralisation, immutability, and anonymization can address some of AI's key needs. It can break data silos and facilitate the free flow of algorithms, computational power, and data resources [Sam23]. Additionally, blockchain can ensure the integrity of original data and enhance the audit credibility and traceability of AI's operations. It can document AI's decision-making processes, thereby increasing transparency, explicability, and trust in AI's actions.

Conversely, AI can reciprocate by improving the architecture of blockchain systems, making them more secure, energy-efficient, and effective. In essence, the convergence of AI and blockchain technologies results in an autonomous, credible, and intelligent system, leveraging the benefits of both while mitigating their respective shortcomings.

Enhancing DeFi Operations with AI

Most commonly, research and applications have explored the potential of using blockchain to augment AI []. However, our focus is on exploring how AI can enhance Decentralised Finance. As a core application of blockchain, Decentralised Finance (DeFi) has consistently been a subject of keen interest in both academic and commercial research.

Raheman et al. [RKG+21] designed an infrastructure of AI agents or "Oracles" for portfolio management, liquidity provision, and price prediction in various decentralised financial markets. As shown in Fig. 10, these Oracles will increase investment value and returns by offering liquidity. They serve end business applications, smart contracts, and other agents. A key aspect is the distinction between an "inventory/portfolio" that comprises multiple assets and a "DEX swap pool" or "DEX balancing pool," which is one of several portfolio maintenance strategies. Therefore, a single "inventory/portfolio" may contain multiple "DEX swap pools" or "DEX balancing pools" with various strategies.

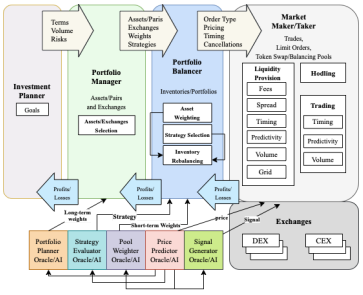


Fig. 10 The business functions (at the top) are served by AI Oracles (at the bottom).

Fig. 11 is the diagram showing how the AI oracles interact with each other and the data sources.

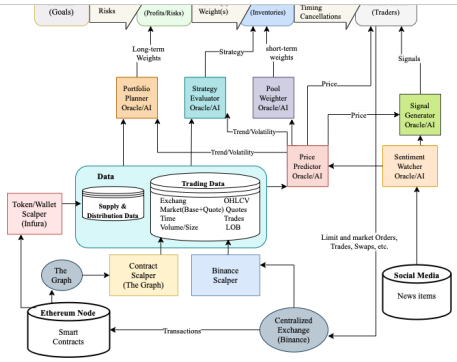


Fig. 11 AI Oracles (in the middle) serving business functions/applications (at the top) relying on data scalping services (at the bottom).

AI oracles are being developed for a comprehensive portfolio management system, utilizing on-chain data and predictive analytics. Key components include:

- A Portfolio Planner Oracle for long-term investment strategies,
- A Strategy Evaluator Oracle for assessing competitive strategies
- A Pool Weighting Oracle for adjusting short-term risks
- A Signal Generator Oracle for real-time trading and liquidity advice
- A Sentiment Watcher Oracle for monitoring social and online media buzz about specific tokens

These components are informed by the Price Predictor, which predicts price trends and volatility using AI and machine learning. Data is sourced from various channels, including centralised exchanges and live Ethereum Nodes. The architecture is currently under construction, with primary components being the Strategy Evaluator, Price Predictor, Portfolio Planner, and Pool Weighter. The research [RKG+21] also indicates that there are opportunities to improve the predictor model's efficiency, such as sharing models across similar markets or using pre-trained models that match expected market conditions. For more details on the architecture and test result, please see here.

In general, DeFi allows users to access financial services without intermediaries. Compared to traditional finance, DeFi allows users to have greater control over their assets and avoid the fees associated with centralised exchanges.

- With the help of AI, DeFi platforms can analyse vast amounts of data to provide personalized investment and minimise risks. Machine Learning Algorithms (MLA) can help identify investment opportunities and optimise smart contracts. These can help users make more informed decisions to increase profits.

Yield aggregator and decentralised exchange (DEX) are specific applications under the DeFi ecosystem.

- Yield Aggregators automatically shift their users' funds between different DeFi protocols to seek out the highest yield. This process is typically based on complex algorithms and strategies, and the goal is to maximize return on investment, taking into account factors such as gas fees and potential risks. AI can significantly improve the efficiency and performance of yield aggregators by helping to analyse market trends and determine the optimal strategies for fund allocation.
- DEXs are decentralised platforms where cryptocurrencies can be traded directly between users. AI can contribute to DEXs in several ways, including optimising liquidity provision, predicting market movements, improving price matching algorithms, and detecting abnormal trading behaviours.

SingularityDAO is a representative application of AI within the decentralised finance (DeFi) ecosystem. It is a decentralised protocol that facilitates user-friendly crypto asset management, employing advanced risk management and analytic tools. This non-custodial system nurtures a new network of Digital Asset Managers, providing automated trading strategies powered by AI-enhanced data analytics. [Sin20].

- In the context of SingularityDAO, AI is applied to manage liquidity and predict market movements. AI algorithms dynamically manage portfolios, execute efficient asset allocation, and provide liquidity to high-quality tokens in decentralised exchanges (DEXs). This essentially optimises the performance of the token sets (or DynaSets) within complex markets.
- Yield aggregators in DeFi automatically move their users' funds between different liquidity pools to maximize returns. SingularityDAO applies AI to this concept through their DynaSets, which are actively managed portfolios (or baskets) of utility tokens from early-stage AI projects. AI models help in the management and rebalancing of these DynaSets, optimising for the best possible returns.

SingularityDAO is not solely a DEX, a liquidity pool, or a yield aggregator in the traditional sense, it leverages AI to bring sophisticated fund management and yield optimisation techniques to these areas within the DeFi ecosystem.

Challenges and Solutions

With AI technology becoming increasingly sophisticated, the line between AI-generated content and human-created content is blurring. As such, there is a growing need to ascertain the origin of content—whether it was generated by applying a specific AI model to a particular input. Zero-knowledge cryptography could provide a solution, offering a method to validate the outputs from these models without revealing any sensitive information about the input or the model itself—a process often referred to as ZKML (Zero-Knowledge Machine Learning). This capability could be extremely useful in sensitive fields like healthcare, where the confidentiality of patient data is paramount. However, it's important to note that ZKML currently focuses on creating zero-knowledge proofs for the inference (or output) of machine learning models, not the training phase, which is a highly computationally demanding task [dcbuilderethtWT23].

Battah et al. [BMY+22] proposed a solution using blockchain and NFTs to address the limitations of existing methods in managing AI model ownership, trading, and access by providing traceability, transparency, auditability, security, and trustful features. It leverages blockchain technology to create a decentralised and transparent system where ownership rights and exchanges of AI models can be managed in a trustworthy manner. By using NFTs linked to AI models, smart contracts are employed to enforce ownership, ease of access, and exchange policies. This ensures that the ownership of AI models is

assets and provides provenance of data, overcoming trust concerns. Overall, the solution aims to provide a secure and reliable framework for managing AI model ownership, trading, and access. This system keeps track of all assets and provides provenance of data, which could potentially address the trust concerns that can arise with AIGC NFTs.

While blockchain technology does not natively recognise or comprehend real-world events, it could be advantageous if it were cognizant of such incidents. This understanding could enable the transfer of value in accordance with real-world situations. Oracles provide a solution to this by serving as intermediaries that fetch and verify real-world data for blockchains. However, they may not suffice in all cases because some real-world data requires computation before it's sent to the blockchain. For instance, a yield aggregator aiming to transfer deposits between different pools to maximize yield in a trust-minimised way would need to compute the current yields and risks of all available pools. This forms an optimisation problem that machine learning is well-equipped to tackle. Nevertheless, executing machine learning computations on the blockchain is costly. This presents an opportunity for ZKML, which would allow machine learning computations to be conducted off-chain but verified on-chain in a zero-knowledge manner, which could potentially reduce costs and increase efficiency [Sam23].

Conclusion

The symbiotic relationship between blockchain and artificial intelligence can pave the way for transformative developments in various industries. The strengths of these technologies address each other's challenges, resulting in a more secure, efficient, and intelligent system. Decentralised finance (DeFi), a prominent application of blockchain, has particularly benefited from this convergence, with AI enhancing analytic capabilities and optimising yields. Yet, challenges remain, such as proving the origins of AI-generated content and computations in the blockchain environment. Emerging solutions like Zero-Knowledge Machine Learning (ZKML) and blockchain-backed NFTs for AI models offer promising possibilities but require further exploration. As research and development continue, we can anticipate a future where these powerful technologies seamlessly intertwine, driving innovative solutions across a multitude of sectors.

Ruoyi Zhao
October 2023

References

[BMY+22] Ammar Battah, Mohammad Madine, Ibrar Yaqoob, Khaled Salah, Haya R. Hasan, and Raja Jayaraman. Blockchain and nfts for trusted ownership, trading, and access of ai models. *IEEE Access*, 10():112230–112249, 2022. doi:10.1109/ACCESS.2022.3215660.

[dcbuilderethtWT23] dcbuilder.eth and the Worldcoin Team. An introduction to zero-knowledge machine learning (zkml). 2 2023. URL: https://worldcoin.org/blog/engineering/intro-to-zkml.

[Ins22] Spherical Insights. Blockchain ai market: overview. 8 2022. Accessed: 2023-06-07. URL: https://www.sphericalinsights.com/reports/blockchain-ai-market.

[Pin18] Rohan Pinto. Next steps in the integration of artificial intelligence and the blockchain. 10 2018. Accessed: 2023-06-07. URL: https://www.forbes.com/sites/forbestechcouncil/2018/10/09/next-steps-in-the-integration-of-artificial-intelligence-and-the-blockchain/.

[RKG+21] (1,2) Ali Raheman, Anton Kolonin, Ben Goertzel, Gergely Hegyközi, and Ikram Ansari. Architecture of automated crypto-finance agent. In *2021 International Symposium on Knowledge, Ontology, and Theory (KNOTH)*, volume, 10–14. 2021. doi:10.1109/KNOTH54462.2021.9686345.

[Sam23] (1,2) Kyle Samani. The convergence of crypto and ai: four key intersections. 6 2023. URL: https://multicoin.capital/2023/06/02/the-convergence-of-crypto-and-ai-four-key-intersections/.

[Sin20] SingularityDAO. Singularitydao lightpaper. 11 2020. URL: https://ouroboros.mobi/wp-content/uploads/2021/10/SingularityDAO-Whitepaper.pdf.

[ZSL+21] (1,2) Zhonghua Zhang, Xifei Song, Lei Liu, Jie Yin, Yu Wang, and Dapeng Lan. Recent advances in blockchain and artificial intelligence integration: feasibility analysis, research issues, applications, challenges, and future work. *Security and Communication Networks*, 2021:1–15, 2021.

Staking and Reward Mechanisms in Proof of Stake Protocols

Innovation & Ideation

Key Insights

- There are various applications of PoS-based Systems evolving using diverse reward mechanisms.
- Reward mechanism is a critical aspect, affecting both incentive structures and system decentralisation.
- There is a trade-off: the more open the staking process is, the more inequality the reward distribution tends to be.
- The way how PoS is implemented greatly matters in its equality and decentralisation.
- We need to critically think about various PoS protocols. Not only know the high return rate, but also realise the centralisation and risks in different systems.

Introduction

Blockchain's trustless foundation removes the necessity for inter-party trust, with its security and decentralisation hinging on a fair consensus mechanism while Proof-of-Work (PoW) and Proof-of-Stake (PoS) are currently the two most used consensus protocols. Proof-of-Work (PoW) involves computating power competition and thus is criticised for its environmental footprint and potential inequities in mining. Conversely, Proof-of-Stake (PoS) operates on asset collateralisation i.e., tokens and is getting popular due to its energy efficiency but faces risks of wealth concentration. This science note summarises Dr. Sheng-Nan Li's talk, which delves into the nuances and challenges of PoS protocols, especially focusing on staking and reward mechanisms [Li23].

Proof-of-Work (PoW)

Proof-of-Work (PoW) is a consensus algorithm where participants, termed miners, solve complex computational problems to validate and record transactions. This mechanism, while secure, is often associated with significant energy consumption due to the required computational power.

Proof-of-Stake (PoS)

demonstrate ownership of a certain amount of cryptocurrency to validate and create new blocks. Unlike PoW, PoS offers energy efficiency by not relying on extensive computational tasks and instead emphasises asset collateralisation for network security.

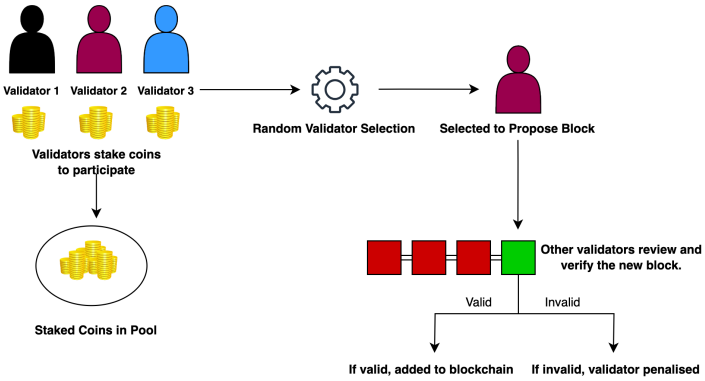


Fig. 12 Proof-of-Stake (PoS) Consensus Mechanism.

Overview of PoS Reward Mechanisms

To discuss the properties of staking and reward distribution in PoS, Ethereum 2.0, Cardano, and Polkadot are selected as examples.

Ethereum 2.0

Ethereum 2.0 [ethereumorg23], launched on September 15, 2022, signifies a major shift in the blockchain realm by adopting the Proof of Stake consensus protocol, specifically the Casper-FFG and LMD-GHOST versions. Central to this new protocol are validators as the main actors, including attesting to blocks and proposing new ones. The attestation process involves a minimum of 128 validators who propose attestations or votes as the attesting committee, from which 16 are chosen as Aggregators. Additionally, one validator is designated as the block proposer to propose one block per slot. The reward with a sum_weight of 64 is structured based on various criteria as:

- timely vote for the correct source checkpoint (weight=14)
- timely vote for the correct source checkpoint (26)
- timely vote for the correct head block (14)
- participated in a sync committee: (2)
- proposed a block in the correct slot: (8) (~ 7/8 attesting reward)

Additionally, a key concept of the consensus and staking aspect is the validator effective balance, which is capped at 32 ETH and triggers ejection when it reaches 16 ETH. It takes 12 seconds for a slot and around 6.5 minutes for an Epoch (32 slots). Reward payout happens after two epochs following the finalisation of a block. For the reward distribution, we have:

$$\text{base\_reward} = \frac{\text{Base\_Reward\_Factor (64)}}{\text{Base\_Reward\_Per\_Epoch}(4) \times \sqrt{\sum \text{active\_balance}}} \times \text{effective\_balance}$$

On the other hand, penalties are in place for cases such as failing to vote timely on the correct head, source, or target. However, there is no penalty for failing to propose a block. The more severe penalty, known as slashing, applies to proposers who propose two different blocks for the same slot and to attesters who engage in 'surround voting' or 'double voting.' This results in a 36-day removal and the burning of a fraction of the staked ether.

Cardano

Cardano, with its Shelley update [car23] introduced on July 29, 2020, employs the Ouroboros Praos consensus protocol (PoS). Central to its system are stake pools consisting of stake pool operators (SPOs), who act as slot leaders responsible for producing blocks. Additionally, there are delegators who can allocate their stakes to these pools. Cardano's system divides time into epochs, with each epoch containing 432,000 slots (1 second) that equate to five days. Rewards are dispensed at the end of each epoch. Cardano introduces a unique staking system with its "Pledging" or self-staking mechanism, allowing stake pool operators to commit their own ADA cryptocurrency, influencing the rewards they can potentially earn. To ensure the network remains decentralised and no single pool gains excessive control, Cardano has implemented a "Saturation Parameter." This parameter sets an optimal size for each pool, beyond which rewards begin to diminish, encouraging a balanced distribution of stakes across various pools. Additionally, the total rewards, sourced from a maximum supply, are influenced by factors like the pool's performance, and they are distributed proportionally based on produced blocks and the pool's total active stake. After deducting declared fees for pool operation, the remaining rewards are shared proportionally among all delegators, including the pool operator.

Polkadot

Launched in May 2020, Polkadot operates using a Nominated Proof of Stake (NPoS) consensus mechanism [Das23]. In this system, nominators can select up to 16 validator candidates, with the active validator set capped at 297. These validators, once elected, are responsible for producing blocks in the relay chain and also accept proofs from collators, who collect transaction data and proofs from the parachains. Time is organised into eras, each lasting 24 hours, during which validators produce blocks. Reward payout happens at the end of every era, with the total rewards following an inflationary model, estimated at approximately 10% yearly by total stake. Validators earn era points for their contributions, which influence their rewards but are separate from their stakes. Notably, the rewards are generally equal among all validators but can vary based on the era points they've accumulated. Validators can also claim a commission fee, while nominators share the

including penalties of a fixed percentage of the stake of validator slot ranging from 0.01% to 100% and kicking out range from removing from the list of candidates in the next election to removing from all the nominators' lists of trusted candidates, depending on the severity of the violation.

Overall, PoS protocols of Ethereum 2.0, Cardano, and Polkadot differ in the terminologies, the main actors and their roles, the incentive and reward distribution, and other technical details. This leads to the next question whether the rewards are fairly distributed to the validators in real PoS-Platforms.

Coin	Launch	Roles	Reward period	Slashing	Key Notes
Ethereum 2.0 (PoS)	Sep-22	Proposer/ Attesting committee	Epoch (~6.5mins)	YES	capped at 32 ETH
Cardano (PoS)	Jul-20	Pool operator/ delegator	Epoch (5 days)	NO	Pledge factor/ saturation
Polkadot (NPoS)	May-20	Validator/ Nominator/ Collator	Era (24 hours)	YES	Era points/ equally distribute

Decentralisation of Reward Distribution

To evaluate the decentralisation of reward distribution, particularly the distribution of wealth among participants, two primary metrics are employed:

Gini Index

The Gini Index [Has23] is the most frequently used inequality index of income or wealth distribution among a nation's population. It can theoretically range from 0 (complete equality) to 1 (complete inequality, where one participant possesses everything while others have nothing). In PoW-based systems, the Gini Index measures the inequality of mining revenue distribution among miners. The Gini Index is applied to the stakes and rewards of validators as:

$$G = \frac{\sum_{i=1}^{N} \sum_{j=1}^{N} |x_i - x_j|}{2n \sum_{i=1}^{N} x_i}$$

$$\text{where } x_i \text{ is the stake or reward of a validator } i, \text{ and there are } N \text{ validators.}$$

Nakamoto Coefficient

The Nakamoto Coefficient [Boa23] quantifies decentralisation by specifying the number of participants needed to compromise the system. In this setting, it is based on the stakes of validators. It specifies the minimum share of participants required to hold more than 50% of the staking power. A higher Nakamoto Coefficient indicates better decentralisation of the protocol. It's expressed as:

$$N_c = \frac{1}{n} \min \left(k \in [1, 2, \ldots, K] : S^{-1} \sum_{i=1}^{k} s_i > 0.5 \right)$$

$$\text{where } s_i \text{ is the stake of validator } i \text{ and there are } N \text{ validators.}$$

Diving deeper into the landscape, Polkadot and Cardano present contrasting approaches. Despite its limited set of validators, Polkadot has seen substantial growth in stake pools. On the other hand, with an unlimited validator set, Cardano recently noted that only around 40% of its pools receive rewards in each epoch. When analysing the distribution patterns, Polkadot emerges as a leading player in both stake and reward distribution. Its design, which emphasises equal reward distribution, has resulted in the lowest Gini Index and the most substantial Nakamoto Coefficient. In contrast, Cardano, despite its open validator set, exhibits a relatively high level of inequality.

In essence, how PoS is implemented plays a crucial role in determining both its equality and decentralisation [HTC+21].

General Framework of PoS Modeling

To clarify components that characterise the staking and reward of PoS protocols and develop an evaluation framework for better protocol design, an extensible framework of modelling (D)PoSs is introduced by Dr. Li. The framework process is split into three parts:

1. Planning the total reward before the reward period;
2. Designing the staking behaviours and the reward distribution during the reward period;
3. Measurement after prolonged operation.

Use-case: Staking Model in Hedera

Hedera Hashgraph, with its unique consensus mechanism known as the hashgraph consensus algorithm, offers an interesting case study for staking models. The hashgraph consensus algorithm operates using a Directed Acyclic Graph (DAG). The hashgraph methodology facilitates transaction processing at speeds vastly superior to conventional proof-of-work blockchains.

A negative value of its **Degree Assortativity** for weekly transaction networks suggests a disassortative nature, indicating that a significant portion of the participants likely transact through a select few dominant intermediaries. When examining wealth distribution within the network, it is observed that early users, those who joined during the initial month or year, tend to hold a substantial amount of tokens. However, a shift towards a more equitable distribution is evident post mid-2022.

The dynamics of account growth, the rate of Daily Active Accounts (DAA), and the volume of daily transaction fees are used in empirical data analytics.

Firstly, the growth of daily transaction fees is fitted and forecasted by the log-log function for better planning of the future total reward. Assuming the reward solely comes from transaction fees without inflation or self-finance, the yearly total reward can be scheduled in different trends such as increasing, decreasing, and constant trends.

Secondly, regarding the modelling of staking behaviours such as staking selection, stakers base their decisions on the time-weighted values of a validator's performance. This is used when they select a node to determine the percentage of each staker's balance. This encompasses factors like historical participation levels and reward rates. As for saturation, the

staker preference, two memory functions which assign weight to the node's participation level and reward rate in each reward period, that is the probability that delegators select validators based on their participation and reward rate, are combined to produce a score for each node.

Thirdly, the daily total reward is distributed among nodes and stakers. Each node's daily reward is determined by its latest participation level relative to a specified threshold and the proportion of stakes received by the node. Similarly, each staker's daily reward depends on the participation level of their selected node and their share of the stake in that node's total received stakes.

Finally, the evaluation of decentralisation using the Gini Index suggests rewards are more equitably distributed among validators (nodes) than stakers. Moreover, the Nakamoto Coefficient indicates that a voting-weighted system is more decentralised than the "one stake one vote" approach.

Conclusion

Modelling (D)PoS offers insights into the long-term implications of protocol adjustments and enhances our understanding of the behavioural tendencies of validators or stakers. It also highlights their influence on system decentralisation. As we delve deeper into various PoS protocols, it's crucial to recognise not just the attractive return rates but also the centralisation and potential risks inherent in different systems.

Jinlu Liu
December 2023

References

[**Boa23]** Cryptoken Board. Nakamoto coefficient — how decentralized is your blockchain. *medium*, 2023. URL: https://medium.com/@cryptoken_board/nakamoto-coefficient-how-decentralized-is-your-blockchain-04842c03ed48#:~:text=On%20a%20typical%20Proof%20of,all%20stake%20on%20the%20network.

[**car23]** cardano. Cardano roadmap - shelley. *Cardano*, 2023. URL: https://roadmap.cardano.org/en/shelley/.

[**Das23]** Lipsa Das. What is nominated proof of stake (npos)? *Ledger Academy*, 2023. URL: https://www.ledger.com/academy/topics/blockchain/what-is-nominated-proof-of-stake-npos#:~:text=NPoS%20allows%20nominators%20to%20choose,choose%20up%20to%2016%20validators.

[**ethereumorg23]** ethereum.org. Proof-of-stake (pos). *ethereum.org*, 2023. URL: https://ethereum.org/en/developers/docs/consensus-mechanisms/pos/.

[**Has23]** Joe Hasell. Measuring inequality: what is the gini coefficient? *ourworldindata*, 2023. URL: https://ourworldindata.org/what-is-the-gini-coefficient.

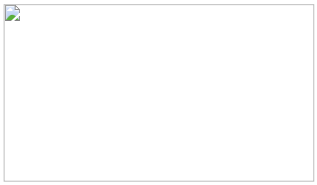
[**HTC+21]** Yuming Huang, Jing Tang, Qianhao Cong, Andrew Lim, and Jianliang Xu. Do the rich get richer? fairness analysis for blockchain incentives. In *Proceedings of the 2021 International Conference on Management of Data*, 790–803. 2021.

[**Li23]** Shengnan Li. Effects of consensus and incentives on the functioning of blockchains. *University of Zurich*, 2023.

Academic Insights

The Detection of Scams on the Ethereum Blockchain

Opportunities and Risks for Traditional Insurance Companies and Banks with DeFi Business Models



The Detection of Scams on the Ethereum Blockchain

Academic Insight

Key Insights

- Ethereum harbours an array of scams, spanning phishing, Ponzi schemes, and pump-and-dumps.
- Identifying and countering these scams pose intricate challenges, encompassing systematic analysis, accurate feature extraction, and prompt detection.
- Novel strategies emerge: trans2vec leveraging transaction to tackle phishing, SADPonzi deciphering bytecode for Ponzi schemes, and LightGBM incorporating N-gram features to foresee early-stage honeypots.
- Predicting rug pulls involves assessing the pool state, token distribution of users, and forecasting the coin being pumped relies on sophisticated market movement information.

Introduction

Ethereum is famous as the largest blockchain platform that supports smart contracts, which has become increasingly prosperous and has attracted investors from all over the world. However, due to its anonymity, Ethereum has become a hotbed for various kinds of fraudulent activities, such as phishing scams, Ponzi schemes, honeypot schemes, rug pull scams, pump-and-dump schemes, and so on, which pose a serious threat to trading security on Ethereum. From Chainalysis 2022 Crypto Crime Report [Tea22], scams have been the largest form of cryptocurrency-based crime since

surrounding scam detection on Ethereum and summarise detection techniques of five kinds of common scams.

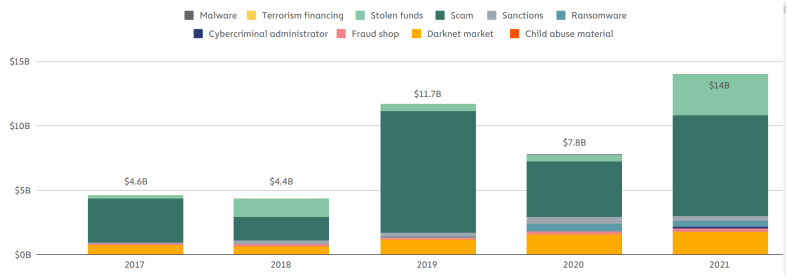


Fig. 13 Total cryptocurrency value received by illicit address from 2017 to 2021.

Challenges in Scam Detection on Ethereum

There are three main challenges to be addressed in scam detection on Ethereum :

- **How to systematically analyse scams:** Different types of scams may employ different methods and strategies, targeting different victims. Therefore, researchers need to collect and analyse a large amount of fraud case data to gain a deeper understanding of the characteristics and patterns of fraudulent behaviour.
- **How to extract effective features:** The performance of scam detection is closely related to the choice of extracted features. Since fraudulent behaviour may exhibit subtle differences from normal behaviour, it is necessary to select discriminative features to distinguish between the two.
- **How to timely detect scams:** Detecting scams timely is crucial to minimise losses and prevent more ordinary investors from falling victim to fraud. When scams are identified or predicted early, authorities and exchanges can take appropriate actions to freeze suspicious accounts and block fraudulent transactions.

Phishing Scam Detection

Phishing Scam

Phishing scam is a common kind of scam where phishers attempt to obtain sensitive information and money from accounts by disguising as a trustworthy entity.

Wu et al. [WYL+22] conducted the first investigation on phishing identification on Ethereum. Transaction information is very critical but cannot be captured by general random walk-based network embedding methods. Therefore, they proposed a novel network embedding algorithm called trans2vec to extract the features for subsequent phishing identification by taking the transaction amount and timestamp into consideration. They also assumed that a larger amount of value of the transaction implies a closer relationship between accounts and the later the transaction is, the greater the impact on the current relationship of the accounts.

New means of Non-Fungible Tokens (NFTs) phishing scams have emerged in the Ethereum ecosystem with the popularity of NFTs. Previous research lacks a systematic review and retrospective analysis of NFT phishing scams. Yang et al. [YLW23] collected 469 NFT phishing accounts and transactions and systematically summarised different patterns of NFT phishing scams, measuring the economic impacts and preferences of scammers. Interestingly, NFT phishers chose to transfer 57.5% of NFTs to their accomplices for further operations, accompanied by signs of gang theft. Detecting NFT phishing gangs and exploring withdrawal methods could be a potential research direction in the future.

Ponzi Scheme Detection

Ponzi Scheme

The Ponzi scheme is an investment fraud in which so-called returns are paid to existing investors through funds provided by new investors.

Existing methods to identify Ponzi smart contracts can be classified into two categories: transaction behaviour-based detection [JLTGG19] and opcodes-based detection [CZC+18]. The former requires a considerable number of transactions to learn the behaviours, and the latter lacks interpretability. Chen et al. [CLS+21] proposed SADPonzi, a semantic-aware detection approach, which utilises the symbolic execution technique to extract semantic information from contract bytecode and match it with four semantic patterns of Ponzi contracts, ultimately identifying Ponzi contracts. Experimental results indicate that SADPonzi outperforms all the existing techniques in terms of accuracy and robustness. However, the symbolic execution technique has a limitation in handling evasion methods which can lead to serious path explosion.

Honeypot Scheme Detection

Honeypot Scam

Honeypot Scheme is a smart contract intentionally designed with a flaw to attract victim attackers, who attempt to exploit it by sending funds. However, the contracts fail to operate as expected, resulting in the loss of the investment.

To detect honeypot contracts early in their creation, Chen et al. [CGC+20] put forward a machine learning model for honeypot contracts detection based on N-gram features and LightGBM. They construct a series of N-Gram-based features and use a feature selection method to drop out those useless features. The model performs well in different imbalances of the data set. In the future, it is a potential way to combine the behaviour of contracts' creators and features of contracts to get a more accurate classification model for detecting honeypot contracts.

Rug Pull Scam Detection

Rug Pull Scam

Rug Pull Scam is a scam where developers abandon a project and take their investors' money when enough investors rush into the project and exchange it for worthless tokens.

Xia et al. [XWG+21] are the first ones to propose an accurate approach for flagging rug pull scams and the scam tokens on Uniswap based on a guilt-by-association heuristic and a machine-learning powered technique. The guilt-by-association heuristic technique helps to identify and expand obvious scam tokens and scammers. Machine learning-

of collusion addresses can be seen in [Fig. 14].

However, the method proposed by Xia et al. [XWG+21] is only effective for detecting scams accurately after they have been executed. Mazorra et al. [MAD22] designed an accurate automated rug pull detection to predict future rug pulls and scams using relevant features of the pool's state and the token distribution among the users. They use the Herfindahl–Hirschman Index and clustering transaction coefficient as heuristics to measure the distribution of the token among the investors. Additionally, they feed these features to train XGBoost and FT-Transformer models, respectively, and predict tokens before the malicious manoeuvre.

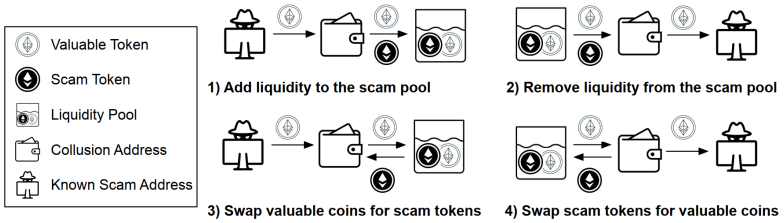


Fig. 14 Four kinds of collusion addresses categorized based on their Uniswap transaction behaviours.

Pump-and-Dump Scheme Detection

Pump-and-Dump Scheme

Pump-and-Dump Scheme is a form of price manipulation that involves artificially inflating an asset's price before selling the cheaply purchased asset at a higher price. Once the assets are dumped, the price falls and investors lose money.

Telegram, with its relative anonymity, has fostered the organisation of pump-and-dump activities by many people in channels. Xu et al. [XL19] analysed features of pumped coins and market movements of coins before, during, and after pump and dump. They also built a predictive random forest model and a generalised linear model able to predict the coin being pumped before the actual pump event by Telegram channels using the information of market movements. In addition, they proposed a simple but effective trading strategy that can be used in combination with the prediction models, leading to fewer people falling victim to market manipulation and more people trading strategically. Different from the work in [XL19], La et al. [LMMSS23] built a machine learning model able to detect pump-and-dump schemes using the information of rush orders within 25 seconds from the moment it starts, instead of predicting it before it happens.

Conclusion

The popularity of Ethereum has attracted a surge of fraudulent activities, posing serious risks to users. Detecting and preventing scams on Ethereum presents several challenges, ongoing research and innovative approaches are making significant progress in scam detection. Scam detection on Ethereum remains a worthwhile and pressing challenge in the field. Through ongoing exploration and innovation, we can collectively strive to build a more secure and trustworthy cryptocurrency trading ecosystem.

Qishuang Fu
August 2023

References

[**CGC+20]** Weili Chen, Xiongfeng Guo, Zhiguang Chen, Zibin Zheng, Yutong Lu, and Yin Li. Honeypot contract risk warning on ethereum smart contracts. In *IEEE International Conference on Joint Cloud Computing*, volume, 1–8. Oxford, UK, Aug. 2020. IEEE.

[**CZC+18]** Weili Chen, Zibin Zheng, Jiahui Cui, Edith Ngai, Peilin Zheng, and Yuren Zhou. Detecting ponzi schemes on ethereum: towards healthier blockchain technology. In *Proceedings of the ACM Web Conference*, volume, 1409–1418. Lyon, France, April 2018. ACM.

[**CLS+21]** Weimin Chen, Xinran Li, Yuting Sui, Ningyu He, Haoyu Wang, Lei Wu, and Xiapu Luo. Sadponzi: detecting and characterizing ponzi schemes in ethereum smart contracts. In *Proceedings of the ACM on Measurement and Analysis of Computing Systems*, volume 5. New York, NY, USA, June 2021. ACM.

[**JLTGG19]** Eunjin Jung, Marion Le Tilly, Ashish Gehani, and Yunjie Ge. Data mining-based ethereum fraud detection. In *IEEE International Conference on Blockchain*, volume, 266–273. Atlanta, USA, July 2019. IEEE.

[**LMMSS23]** Massimo La Morgia, Alessandro Mei, Francesco Sassi, and Julinda Stefa. The doge of wall street: analysis and detection of pump and dump cryptocurrency manipulations. *ACM Transactions on Internet Technology*, Feb. 2023.

[**MAD22]** Bruno Mazorra, Victor Adan, and Vanesa Daza. Do not rug on me: leveraging machine learning techniques for automated scam detection. *Mathematics*, 10(6):949, Mar. 2022.

[**Tea22]** Chainalysis Team. The 2022 crypto crime report. Feb. 2022. URL: go.chainalysis.com/2021-crypto-crime-report.

[**WYL+22]** Jiajing Wu, Qi Yuan, Dan Lin, Wei You, Weili Chen, Chuan Chen, and Zibin Zheng. Who are the phishers? phishing scam detection on ethereum via network embedding. *IEEE Transactions on Systems, Man, and Cybernetics: Systems*, 52(2):1156–1166, Feb. 2022.

[XWG+21](1,2) Pengcheng Xia, Haoyu Wang, Bingyu Gao, Weihang Su, Zhou Yu, Xiapu Luo, Chao Zhang, Xusheng Xiao, and Guoai Xu. Trade or trick? detecting and characterizing scam tokens on uniswap decentralized exchange. In *Proceedings of the ACM on Measurement and Analysis of Computing Systems*, volume 5, 1–26. New York, NY, USA, December 2021. ACM.

[XL19](1,2) Jiahua Xu and Benjamin Livshits. The anatomy of a cryptocurrency Pump-and-Dump scheme. In *Proceedings of the 28th USENIX Conference on Security Symposium*, 1609–1625. Santa Clara, CA, Aug. 2019. USENIX Association.

Opportunities and Risks for Traditional Insurance Companies and Banks with DeFi Business Models

Industry Perspective

Disclaimer: The views and opinions expressed in this article are solely those of the author

Key Insights

- Legacy banks and financial institutions face internal and external challenges in integrating cryptocurrencies into their existing business framework for generating new revenue streams.
- The internal perspective involves leveraging distributed ledger technology for enhanced management, while the external perspective centres on handling crypto customers with an emphasis on regulatory compliance and environmental sustainability
- Legacy banks often miss out on business opportunities due to constraints related to regulation, organisation, processes, delivery, and employee biases.
- Offering tailored financial products, such as crypto mining equipment insurance and crypto hedging insurance, can enhance profitability and help diversify the revenue streams of Legacy Banks and financial institutions.
- Talent acquisition and skill development are crucial to improve crypto risk management within legacy banks.

Introduction

The decentralised finance (DeFi) ecosystem, with its innovative models and frameworks, has introduced disruptive business models that challenge the traditional financial landscape. This article aims to analyse this challenge in detail, exploring how traditional players in finance can leverage the hidden and visible value within DeFi business models. To enhance your understanding of this topic and to provide you with a better understanding of this article, I recommend reviewing the following articles "*Short Survey on Business Models of Decentralized Finance*" by Jiahua Xu and Teng Andrea Xu and "*DeFi vs TradFi: Valuation Using Multiples and Discounted Cash Flow*" by Teng Andrea Xu, Jiahua Xu, Kristof Lommers.

Business Ideas

Let's begin with a foundational overview, drawing insights from the aforementioned articles.

Within the context of Decentralised Finance (DeFi) Business Models among the prominent DeFi business models are Protocols for Loanable Funds (PLFs), Decentralised Exchanges (DEXs), and Yield Aggregators. This section will delve into these DeFi models and discuss their potential adoption by traditional insurance companies and banks. Any additional details not covered in this article can be further explored in the aforementioned articles.

a) Protocols for Loanable Funds (PLFs):

PLFs have revolutionised lending and borrowing within the financial sector. These protocols facilitate access to loans and cryptocurrency lending without intermediaries. Revenues are generated through interest rates, shared between the protocols and lenders.

b) Decentralised Exchanges (DEXs):

DEXs enable peer-to-peer cryptocurrency trading, eliminating the need for intermediaries. These platforms earn revenue by charging trading fees, contributing to the protocol's treasury.

c) Yield Aggregators:

Yield Aggregators merge strategies to optimise investor returns. Investors deposit funds into "Vaults," implementing diverse strategies for profitability. Yield Aggregators levy commission fees on strategy profits.

Resolving the Paradox

The question arises: Is it paradoxical for traditional insurance companies and banks, champions of centralised finance, to embrace DeFi models to extract additional value while upholding their established positions? However, as the financial landscape evolves, exploring innovative opportunities becomes essential to maintain profitability and stay ahead in the highly competitive and regulated financial sector. To be noted that profits in the financial industry are significantly influenced by Central Bank decisions, particularly interest rate fluctuations. **By adopting decentralised finance business models, though seemingly paradoxical at first glance, financial institutions can stabilise revenues and partially free themselves from Central Bank decisions.** With this context in mind, let's explore potential business opportunities and risks for traditional banks and insurance companies in adopting each DeFi business model.

a) PLFs:

- **Business Opportunities for Traditional Banks**:
  1. Penetrating a New Market: Through PLFs, banks can tap into the burgeoning cryptocurrency lending market, attracting a fresh customer base. The emphasis, in reality, must be on cross-selling and upselling commercial opportunities, rather than immediate profits.
  2. Diversified Revenues: PLFs provide an additional revenue stream, complementing traditional lending practices.
  3. Technological Innovation: Legacy IT systems in banks are challenging to overhaul. PLFs, with their innovative technology, could serve as pilot systems, gradually expanding across the organisation.
- **Risks for Traditional Banks**:
  1. Regulatory Uncertainty: DeFi lacks comprehensive regulations, exposing banks to potential legal and regulatory complexities.
  2. Smart Contract Vulnerabilities: Relying on smart contracts exposes banks to cybersecurity risks and financial losses.
- **Business Opportunities for Insurance Companies**:
  1. Smart Contract Insurance: Insurance firms can offer coverage against smart contract vulnerabilities in PLFs, safeguarding users and generating premiums.

- **Risks for Insurance Companies**:
    1. Limited Historical Data: Insufficient data on DeFi transactions could hinder accurate risk assessment and policy pricing.
    2. Market Volatility: Cryptocurrency's volatile nature could pose challenges in pricing insurance products, necessitating reinsurance policies. In the article "DeFi vs TradFi: Valuation Using Multiples and Discounted Cash Flow" we can learn how to value digital assets. Furthermore, it is paramount to note that, so far, this value is extremely volatile, and traditional players need to surf on this volatility, need to learn how to govern this volatility.
- **Risk Management Practices**:
    1. Tech Collaboration: Insurers can partner with tech experts to bolster smart contract security and mitigate risks.
    2. Robust Risk Models: Creating advanced risk models for DeFi-related insurance products can enhance underwriting precision.

b) DEXs:

- **Business Opportunities for Traditional Banks**:
    1. Liquidity Provision: Banks can serve as liquidity providers on DEX platforms, earning fees and interest on deposited assets.
    2. Market Expansion: DEX partnerships enable banks to broaden their market reach beyond conventional borders.
- **Emerging Risks for Traditional Banks**:
    1. Counterparty Risks: Engaging with anonymous DEX users exposes banks to counterparty risks and potential fraud, although modern risk management practices mitigate these concerns.
    2. Reputation Risks: Involvement in unregulated DEX spaces could tarnish a bank's reputation if associated with illicit activities.
- **Business Opportunities for Insurance Companies**:
    1. Secure Custody Solutions: Insurance firms can offer secure custody solutions for DEX users, reducing asset loss risk.
    2. Smart Contract Risk Coverage: Insurance products can be designed to cover smart contract vulnerabilities on DEXs.
- **Risks for Insurance Companies**:
    1. DEX Risk Understanding: Insurance firms might lack comprehensive knowledge of DEX-specific risks, impacting policy underwriting.
    2. Pricing Data Limitation: The absence of pricing data for DEX-related risks could hinder accurate insurance product pricing.
- **Risk Management Practices**:
    1. Security Audits: Insurers can conduct security audits of DEX platforms to ensure adherence to high-security standards.
    2. Blockchain Expert Collaboration: Collaboration with blockchain experts aids insurers in comprehending and assessing DEX-related risks.

c) Yield Aggregators:

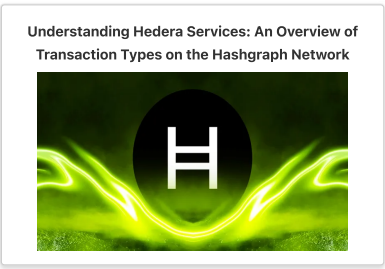
- **Business Opportunities for Traditional Banks**:
    1. Investment Ventures: Banks can partner with Yield Aggregators to offer innovative investment opportunities to clients, potentially yielding higher returns.
    2. Fee-Based Income: Banks can receive fees for directing client funds toward specific Yield Aggregator strategies, reducing reliance on central bank interest rate changes.
- **Risks for Traditional Banks**:
    1. Investment Volatility: Involvement with Yield Aggregators exposes banks to market volatility and possible investment losses.
    2. Reputation Risks: Poor strategy performance may harm a bank's reputation.
- **Business Opportunities for Insurance Companies**:
    1. Tailored Investments: Insurance firms can craft investment products incorporating Yield Aggregator strategies.
    2. Risk Mitigation Services: Insurance companies can provide risk mitigation services to Yield Aggregator users, reducing potential losses.
- **Risks for Insurance Companies**:
    1. Complex Risk Evaluation: Grasping and evaluating diverse Yield Aggregator strategies might pose challenges for insurers.
    2. Strategy Performance Uncertainty: Insurers face uncertainty in predicting the performance of selected Yield Aggregator strategies.
- **Risk Management Practices**:
    1. Diversification: Encouraging investors to diversify across different Yield Aggregators can mitigate risks tied to individual strategies.
    2. Transparent Reporting: Insurers can demand transparent reporting from Yield Aggregators, ensuring clients comprehend their investments.

Conclusion

Although the adoption of DeFi business models by traditional insurance companies and banks may seem paradoxical, exploring these opportunities is essential to thrive in a competitive financial landscape. Understanding unique business opportunities and potential risks associated with each DeFi model is crucial for informed decision-making. By implementing robust risk management practices and collaborating with blockchain experts, traditional financial institutions can harness DeFi's potential while mitigating inherent risks. This shift is strategic, enabling institutions to capitalise on emerging opportunities and ensure long-term sustainability within the financial industry mitigating existing and emerging risks.

Alessio Pezzotta
September 2023

References



Understanding Hedera Services: An Overview of Transaction Types on the Hashgraph Network

Industry Perspective

Key Insights

- Hedera's unique protocol and algorithm ensure a fast, secure, and fair platform for real-time applications and services.
- Hedera's native cryptocurrency, HBAR, bolsters network security and powers transactions at low, stable fees.
- Hedera's USD-fixed transaction fees, tailored for network operations, counteract HBAR price fluctuations to provide a stable and predictable cost framework for users.
- The Hedera Consensus Service streamlines consensus processes, fostering trust and decentralisation for various applications.
- The Hedera Token Service streamlines tokenisation, supporting secure asset conversion, and promoting interoperability.

Introduction

Hedera is a distributed ledger technology designed to offer a secure, fair, and fast platform for a new generation of real-time applications and services [HH23]. In the Hedera network, a user initiates a transaction, which is then quickly disseminated among nodes through an efficient "gossip" protocol. Nodes gossip messages to each other about transactions randomly. Consensus on transactions is achieved independently by nodes using a virtual voting algorithm, which calculates a consensus timestamp based on the median timestamp when the majority of nodes received the transaction. This mechanism ensures transaction fairness and security, as no single node can significantly manipulate the order, thereby providing resilience against malicious activities.

Gossip about gossip

The "Gossip about Gossip" protocol is a fundamental part of the consensus algorithm, which disseminates transactions across network nodes through random information exchange, similar to social gossip. Beyond transaction data, this protocol also conveys the timeline and pathway of data propagation, enabling an efficient consensus on transaction order without a laborious proof-of-work process.

The transaction recording process using Hedera and its benefits can be seen in Fig. 15.

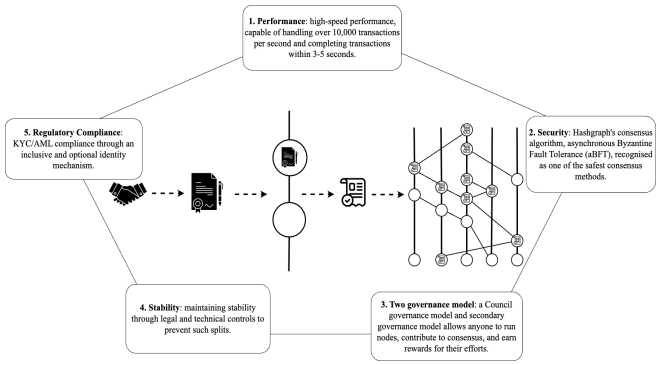


Fig. 15 Hedera Transaction Recording Process & Its Key Benefits.

Since Hedera launched in August 2018, it has offered unique transactional capabilities through its native HBAR cryptocurrency, used both for network security and as fuel for network services. As a proof-of-stake network, HBARs help safeguard the network by representing voting power; thus, wider distribution of HBARs prevents potential attacks by making it prohibitively expensive for a malicious entity to control one-third of the coins. In addition, HBARs serve as fuel for network services, compensating nodes for computing resources and ensuring low stable transaction fees. For example, a cryptocurrency transfer currently costs $0.0001 (paid in HBARs) [BGT19].

Hedera Cryptocurrency Service

Hedera provides two distinct services related to digital assets: the Hedera Cryptocurrency Service and Token Service. The Cryptocurrency Service pertains specifically to the use of HBAR for transactions and fees on the network, while the Token Service provides a platform for users to create and manage their own custom tokens. Hedera's cryptocurrency is engineered for speed, resulting in minimal network fees and enabling feasible micro-transactions. When Hedera is fully operational, every user will have the capability to manage a network node and receive cryptocurrency payments for this contribution. To create an account, all that is needed is to generate a key pair; there is no need for a linked name or address. However, users are given the flexibility to link hashes of identity credentials from any selected third-party certificate or

Compliance section [BHM20].

Fees Associated with Hedera Transactions

Hedera's network fees are designed for specific network operations. The fees are payable in HBAR but are also fixed in USD for stability.

> **Note**
>
> **HBAR Denominations and Abbreviations**
>
> Hedera denominates HBAR into various units:
>
> ```
> 1 gigabar (Gℏ) = 1 billion HBAR
> 1 megabar (Mℏ) = 1 million HBAR
> 1 kilobar (Kℏ) = 1,000 HBAR
> 1 hbar (ℏ) = 1 HBAR
> 1 millibar (mℏ) = 0.001 HBAR
> 1 microbar (μℏ) = 0.000001 HBAR
> 1 tinybar (tℏ) = 0.00000001 HBAR.
> ```

Fee structures for various operations are as follows:

- Cryptocurrency Service: The cost for creating a crypto account is $0.05, for auto renewing an account is $0.00022, and for transferring cryptocurrency is $0.0001, amongst others.
- Consensus Service: Fees for creating a topic on the Consensus Service is $0.01, for updating a topic is $0.00022, and for submitting a message is $0.0001, etc.
- Token Service: The cost to create a token is $1.00, to update a token is $0.001, and to associate a token with an account is $0.05, amongst others.
- File Service: The fee for creating a file is $0.05, updating a file is $0.05, and deleting a file is $0.007, etc.
- Smart Contract Service: Fees for creating a contract are $1.0, for updating a contract are $0.026, and for making a contract call are $0.05, etc.

Exact service fees will be visible once finalised through the pricing calculator.

Hedera Consensus Service

The Hedera Consensus Service (HCS) is an essential component of the Hedera network that provides a decentralised, secure, and verifiable log of events. It facilitates agreement on transaction order and timing across diverse applications, ranging from supply chains to multiplayer gaming. More than just a transactional ledger, HCS revolutionises the blockchain ecosystem by offering swift, fair, and decentralised consensus. Utilising the hashgraph consensus algorithm, HCS expedites transaction settlements, fostering transparency with a timestamped process. It not only bolsters efficiency and the trust model of private networks but also significantly reduces operational costs. Moreover, it promotes a collaborative environment for interconnected applications, paving the way for the next wave of decentralised applications[BGT19].

HCS Architecture and Configuration

HCS is made accessible through various SDKs and the Hedera API (HAPI). It processes byte string messages from client applications tied to unique topics. These messages, carrying transactional details, are processed against a fee in HBARs, Hedera's native currency. Upon successful processing, the Hedera ledger returns a record with consensus details, timestamps, sequence numbers, and running hashes reflecting previous messages. To configure this service, organisations set up mirror nodes, program applications, and define unique keys and topics for transactions to configure HCS. After verification and confirmation of the transaction fee payment, the transaction information is disseminated across the network to establish a consensus timestamp. Mirror nodes receive this information, facilitating the creation of state proofs and further transaction processing. This configuration ensures robust record distribution and real-time auditing, fostering transparency and immediate validation of transaction order and accuracy.

Hedera Token Service

The Hedera Token Service (HTS) enables native token creation on the Hedera platform, storing information on the public Hedera ledger and offering pseudonymous privacy. This model is governed by the Hedera Governing Council and allows for limited customisation [HH20]. HTS makes token deployment straightforward and cost-effective, without the need for additional infrastructure. It can support high throughput applications with thousands of transactions per second, achieving transaction finality in 3-5 seconds. The interoperability of tokens across the Hedera ecosystem and decentralised trust model ensures transparent, verifiable transactions.

Applications of Hedera's Tokenisation Model

Hedera's tokenisation model can support various token use cases [HH20]. In financial services, it can facilitate efficient trading and settlement of assets like bonds, stocks, or commodities. Tokens can also track physical goods in supply chains, enable fractional ownership in real estate, represent unique art pieces as Non-fungible tokens, and form the backbone of Decentralised Finance. Other applications include tokenising in-game assets, loyalty rewards, and personal identities for enhanced security and user privacy.

Hedera Smart Contract Service

Hedera's Smart Contract Service revolutionises the world of blockchain programming by introducing exceptional features that enhance performance, reduce costs, ensure security and fairness, and promote interoperability with Ethereum. The service allows the development of smart contracts using Solidity, a common language in Ethereum, simplifying the transition for developers familiar with Ethereum's ecosystem [Cla22]. The Besu EVM, tailored for the Hedera network and hashgraph consensus, enables high-speed transactions, predictable low fees, a negative carbon footprint, and exceptional performance with 15 million gas per second [Hed]. By leveraging the hashgraph consensus algorithm, the service offers rapid transaction finality and optimises contract execution, surpassing the capabilities of traditional block-based systems. It is designed to maintain low and predictable costs, significantly benefiting developers compared to Ethereum's fluctuating

contracts to Hedera, showcasing its adaptability and convenience for developers.

See also

The full documentation for the Smart Contract Service and a "Deploy Your First Smart Contract" tutorial here. Additionally, a JavaScript code snippet is provided below for creating a very first smart contract transaction on Hedera.

```
{
....
//Create the transaction

const transaction = new ContractCreateTransaction()

    .setGas(100_000_000)
    .setBytecodeFileId(bytecodeFileId)
    .setAdminKey(adminKey);

//Modify the default max transaction fee (default: 1 hbar)

const modifyTransactionFee = transaction.setMaxTransactionFee(new Hbar(16));

//Sign the transaction with the client operator key and submit it to a Hedera network

const txResponse = await modifyTransactionFee.execute(client);

//Get the receipt of the transaction

const receipt = await txResponse.getReceipt(client);

//Get the new contract ID

const newContractId = receipt.contractId;

console.log("The new contract ID is " + newContractId);
....
}
```

Hedera File Service

Hedera's File Service provides a resilient, secure, and efficient system for data storage in a decentralised environment. It functions like a transaction graph, processing data in parallel and storing files across all network nodes in Merkle Trees and Merkle Directed Acyclic Graphs, ensuring tamper-proof, regionally accessible, and 100% available data. A unique feature is the provision of proof-of-deletion, allowing businesses to comply with General Data Protection Regulations (GDPR) requirements. Files in the system have a set expiration date and are deleted automatically, while the storage service costs are based on the file size and the desired storage duration. Furthermore, Hedera offers controlled mutability via WACL (WriteAccess Control) keys, providing flexible data management and ensuring consensus for any changes. Transactions on Hedera are limited to 4KB, ensuring efficiency, although larger files can be accommodated through the appending of additional data. The service supports various transactions including creating, appending, deleting, and updating files, offering comprehensive and flexible options for developers and users. In essence, Hedera's File Service is a robust, secure, and efficient solution for decentralised data storage, embodying the low-cost and high-performance advantages of the platform [Won19].

Merkle Directed Acyclic Graph

Merkle DAG is a unique form of DAG where each node is identified by a cryptographic hash, composed of the node's content and the identifiers of its children nodes. They are self-verifying structures, immutable by nature, and constructed from the leaves up, meaning children nodes are added before their parents, with each node essentially serving as the root of its own sub-Merkle DAG.

The architecture of Hedera's core services can be seen in Fig. 16.

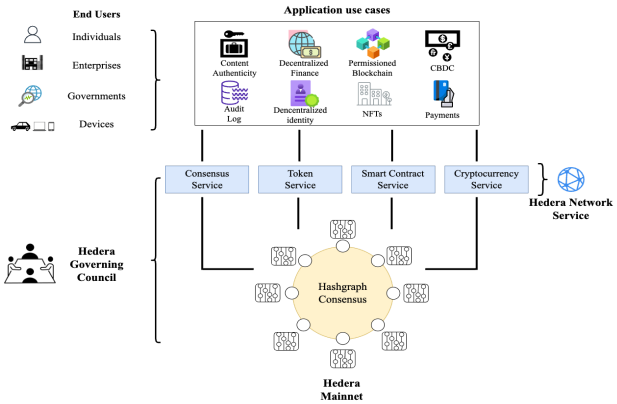


Fig. 16 Architecture of Hedera's core service

Conclusion

Hedera has emerged as a pioneer in the realm of blockchain and Distributed Ledger Technology (DLT), leveraging unique transactional capabilities. It has significantly transformed the DLT landscape through its core services such as the Hedera Cryptocurrency Service, Hedera Consensus Service, Hedera Token Service, Smart Contract Service, and File Service, altering the handling of consensus and tokenisation. The advanced transactional capabilities of Hedera, coupled with its suite of innovative services, position it as a substantial disruptor in the blockchain and DLT arena. Its commitment to cost-effectiveness, high performance, secure operations, and transparency has the potential to redefine how businesses and individuals interact with distributed ledger technology, thus paving the way for the next wave of decentralised applications.

Ruoyi Zhao

References

[Hed] What is hedera hashgraph. URL: https://hedera.com/learning/hedera-hashgraph/what-is-hedera-hashgraph.

[BGT19](1,2) Leemon Baird, Bryan Gross, and Donald Thibeau. Hedera consensus service. Technical Report, Hedera Hashgraph, 2019. Technical Whitepaper. URL: https://hedera.com/hh-consensus-service-whitepaper.pdf.

[BHM20] Leemon Baird, Mance Harmon, and Paul Madsen. Hedera: a public hashgraph network & governing council. Technical Report, Hedera, August 2020. URL: https://hedera.com/hh_whitepaper_v2.1-20200815.pdf.

[Cla22] Kadeem Clarke. Smart contracts, done smarter: hedera ecosystem overview. 3 2022. URL: https://medium.com/momentum6/smart-contracts-done-smarter-hedera-ecosystem-overview-93c79d69e855.

[HH20](1,2) LLC Hedera Hashgraph. Tokenization on hedera. Technical Report, Hedera Hashgraph, LLC, 2020. Technical Whitepaper. URL: https://hedera.com/hh_tokenization-whitepaper_v2_20210101.pdf.

[HH23] LLC Hedera Hashgraph. Understanding decentralization of hedera hashgraph. Technical Report, Hedera Hashgraph, LLC, 3 2023. Technical Report, Version 1. URL: https://files.hedera.com/hh-decentralization-of-consensus.pdf.

[Won19] Evelyn Wong. Hedera hashgraph services — part 2: file storage service. 3 2019. URL: https://medium.com/hashingsystems/hedera-hashgraph-services-part-2-file-storage-service-f37f4323b667.

Crypto and Digital Assets Risk Management: Navigating Opportunities and Challenges

Industry Perspective

Disclaimer: The views and opinions expressed in this article are solely those of the author

> **Key Insights**
>
> - Cryptocurrencies and digital assets offer legacy banks opportunities for diversification and portfolio expansion beyond traditional financial instruments, leading to potential risk-adjusted returns and exposure to new markets.
> - Banks need to consider the inter-relationships between arising risks deriving from crypto-currencies and traditional risks such as interest rate risk, currency risk, and liquidity risks when managing their exposure to these assets.
> - Interest rate fluctuations can impact the valuation and attractiveness of cryptocurrencies, influencing banks' investment strategies and portfolio allocation.
> - Banks have opportunities to hedge against volatility in customer digital asset portfolios and their own exposure to price volatility through emerging cryptocurrency derivatives and hedging instruments.
> - Banks, especially in the European Union, need to consider climate and environmental risks associated with financing crypto customers, given the energy-intensive nature of cryptocurrency assets.
> - Effective risk management practices, proactive monitoring, robust internal controls, and compliance with regulations are crucial for banks to navigate the opportunities and challenges presented by cryptocurrencies and digital assets.

Introduction

Cryptocurrencies and digital assets have emerged as disruptive forces in the financial industry, presenting both opportunities and risks for banks [NBMG16, Pan23]. As technology advances and the digital economy expands, it is crucial for banks (to be more specific: legacy and traditional banks) to understand and effectively manage the risks associated with these assets. These risks are generated and linked from the following drivers:

- the volatile nature and intrinsic features of digital assets and cryptos
- customers that trade and hold these specific assets
- as-is organisational frameworks related to risk management and best practices that did not consider cryptocurrencies and digital assets

The objective of this article is twofold: on one hand to provide a review of the main financial and non-financial risks arising from the management of non-standard products for traditional banks; on the other hand, to identify the key value drivers within risk management to uncover new best practices and new business opportunities.

To achieve these two objectives, the pros and cons of each risk will be emphasised.

At the conclusion of the article, the risks that can raise greater concern and those that can be harnessed as catalysts to amplify innovation, both technologically and financially, will become clear.

Managing Risks

Let us begin with an examination of the various pros related to holding and trading cryptocurrencies for legacy Banks:

1. **Diversification and Portfolio Expansion**: Cryptocurrencies and digital assets offer banks the potential for diversifying their portfolios beyond traditional financial instruments. This can enhance risk-adjusted returns and provide exposure to new markets and investment opportunities.
2. **Client Demand and Engagement**:
   Banks that offer cryptocurrency services can attract and retain more clients seeking exposure to digital assets. Meeting this demand can lead to increased customer engagement and revenue generation (i.e., new revenue streams). Let's look for example at Revolut Ltd. case [Ltd21]. As widely acknowledged, Revolut stands as one of the most accomplished digital banks, providing customers with an array of services encompassing crypto services, traditional banking features, and various other financial offerings. The Financial Statements of Revolut Ltd. communicate that the company succeeded in drawing a substantial customer base by utilising a comprehensive financial package, with its cryptocurrency services taking the spotlight. Moreover, Revolut's strong suit lies in its ability to enable many individuals to manage cryptocurrencies without encountering technicalities or complexities associated

and Revolut users, as depicted in the table below. Revolut's growth rate is remarkable, encompassing both its customer base and revenues. **This underscores the hidden value that legacy banks can uncover and harness by integrating cryptocurrency and digital asset services into their existing offerings.**

Revolut Ltd main financials	2021	2020	2019
Total Retail Customers (#)	16,42 million	11,27 million	10.00 million
Total Revenues (000)	636,205	219,931	166,026

3. **Innovation and Competitive Advantage** [NBMG16]:
   Embracing cryptocurrencies allows banks to position themselves as innovators in the financial industry. It demonstrates adaptability and can help differentiate them from competitors enabling the creation of a different, cutting-edge competitive advantage, something that is rare in the financial industry, and hard to copy. It is very important to highlight that, within the legacy banks market, the first mover advantage is paramount – guaranteeing the capture of extra profits that later movers cannot exploit.

At this stage, it becomes crucial to emphasise the interrelations between cryptocurrencies and traditional risks. Below, you will discover the key insights pertaining to this subject.

1. **Interest Rate Risk** [DugganWaynePowellFarran23, Tan23]: Banks need to consider the potential impact of interest rate fluctuations on the valuation of cryptocurrencies, especially if they hold these assets on their balance sheets. It's important to recognise that the relationship between interest rates and cryptocurrencies is complex and influenced by numerous factors, including absolute value of interests, market sentiment, regulatory developments, and technological advancements [DugganWaynePowellFarran23, Pec23, Tan23]. Banks need to carefully assess and monitor these dynamics to effectively manage the interest rate risk associated with cryptocurrencies.
   Let's look at the **Interest Rate Increase** scenario:

   If interest rates rise, they can have several implications for cryptocurrencies held by banks:

   - **Valuation Impact**: cryptocurrencies, like other investment assets, may experience a decline in value when interest rates increase. This valuation impact can affect the overall profitability of the bank's investment portfolio.
   - **Opportunity Cost**: Rising interest rates can make traditional fixed-income investments more attractive, potentially diverting investment capital away from cryptocurrencies. This could lead to a reduced allocation to cryptocurrencies within the bank's portfolio.

   Conversely, if **interest rates decrease**, they can also affect cryptocurrencies in the following ways:

   - **Valuation Impact**: cryptocurrencies may experience increased demand when interest rates decline, leading to potential price appreciation. However, it is important to note that cryptocurrencies are influenced by various other factors, and interest rates alone may not be the sole driver of their valuation.
   - **Investment Attractiveness**: lower interest rates can make cryptocurrencies relatively more attractive compared to traditional fixed-income investments that provide lower yields. Banks may consider increasing their exposure to cryptocurrencies as part of their investment strategy during periods of low-interest rates.

   Moreover, it's worth noting that interest rate risk related to cryptocurrencies primarily arises when they are held as investment assets on a bank's balance sheet. If cryptocurrencies are held for other purposes, such as providing custody [20223]or trading services, the interest rate risk may be less relevant. As with any investment asset, banks should have appropriate risk management policies and frameworks in place to assess and monitor interest rate risk associated with cryptocurrencies. This may involve stress testing, scenario analysis, and regular reviews to ensure the bank's exposure to interest rate fluctuations aligns with its risk appetite and strategic objectives.

2. **Currency Risk**: Cryptocurrencies are not tied to any specific fiat currency, so it is possible to infer that no idiosyncratic currency risk is in place.
3. **Hedging Risks** [Tan23]: here, hedging risks have two financial legs:
   - The first one is related to the protection against volatility related to customer digital assets portfolios (that can be seen as a commercial opportunity for legacy banks)
   - The second one is related to the protection of the legacy bank itself against volatility. Please note that cryptocurrency derivatives (or more in general, digital assets derivatives) and hedging instruments are emerging, providing opportunities, and related risks, for banks to hedge their exposure to price volatility and mitigate associated risks.
4. **Liquidity Risks** [Tan23]: cryptocurrency markets can experience liquidity challenges, especially during periods of market stress. Banks should carefully assess liquidity ratios and availability (to be more specific also in the interbank and monetary market) when holding and trading these assets.
5. **Climate & Environmental Risks**: banks, especially in the European Union, have targets (such as Net Zero Banking Alliance) on their greenhouse gas (GHG) emissions and financed emissions (GHG emissions produced by banks' customers). This topic is very relevant because financing crypto customers could result in increasing GHG financed emissions. Since some cryptocurrency assets/digital assets are very energy-intensive assets (e.g., due to mining), the main challenge is how to make a fruitful cherry-picking of digital and crypto assets that at the same time:
   - rely on the most efficient technology (hence, they emit less with respect to the market)
   - guarantee the most profitable income for legacy banks and customers, given the GHG emissions target
6. **Reputational Risks**: Reputational risks can emerge while managing cryptocurrencies and crypto customers, stemming from regulatory scrutiny as well as media and public perception surrounding these assets.
7. **ICT Risks** [Ser23, Tan23]: Information and Communication Technology (ICT) risks refer to the potential risks associated with the use of technology, information systems, and infrastructure within an organisation. In the context of cryptocurrencies and digital assets, ICT risk could be the paramount one, and can manifest in the following ways:
   - **Security of Digital Wallets and Exchanges**:
     - Unauthorised Access: Cryptocurrency wallets (provided by legacy banks) can be vulnerable to unauthorised access, leading to (personal) data theft or loss of digital assets. Risks include hacking attempts, phishing attacks, or malware targeting the storage or transfer mechanisms of cryptocurrencies.
     - Infrastructure Vulnerabilities: Weaknesses in ICT infrastructure, such as servers, networks, or software, can expose digital wallets to potential security breaches. Vulnerabilities in infrastructure may arise due to outdated systems, inadequate security measures, or insufficient monitoring and patching practices.
   - **Data Integrity and Availability**: No specific issues coming from these topics.
8. **Cyber Risks** [Ser23, Tan23]: Cyber risks refer to the potential risks arising from malicious activities. In the context of cryptocurrencies and digital assets, cyber risks can include, inter alia:

fake websites, or social engineering techniques.
    - **Malware and Ransomware Attacks**: Malicious software can be used to target digital wallets, exchanges, or users, aiming to gain unauthorised access, steal funds, or encrypt data for ransom. Ransomware attacks can disrupt operations and cause financial losses if not adequately mitigated.
    - **Insider Threats**: Internal personnel with access to sensitive information or systems can intentionally or unintentionally misuse or compromise digital assets.
9. **Operational Risks**: There are no specific or innovative aspects in terms of Operational Risks. All Operational Risks are interconnected and integrated within the Cyber Risk realm. Therefore, there's no necessity to extensively explore this topic.

As evident from the text above, ICT Risks and Cyber Risks pose the most significant threats that legacy banks must face, and these could even lead to potential reputational risks in the event of their occurrence. These two areas require the most substantial efforts in terms of financial IT investment, skilled human resources, and new organisation framework by the legacy banks. They must undertake considerable technological advancements to enter the realm of the cryptocurrency business.

	Summary of Risks for Traditional Banks in Managing Cryptocurrencies	Emerging issues for traditional banks?	Are these risks levers for new business opportunities?	Is this risk a driver for an innovative, hard-to-replicate, and rare competitive advantage?	Is this Risk a driver for technology leapfrogging for Legacy Banks?
1	**Interest Rate Risk**	NO	YES	NO	NO
2	**Currency Risk**	NO	YES	NO	NO
3	**Hedging Risks**	YES	YES	YES	NO
4	**Liquidity Risks**	NO	YES	NO	NO
5	**Climate & Environmental Risks**	YES	YES	NO	NO
6	**Reputational Risks**	YES	NO	NO	NO
7	**ICT Risks**	YES	NO	YES	YES
8	**Cyber Risks**	YES	NO	YES	YES
9	**Operational Risks**	NO	NO	NO	NO

Main results

The objective of this article, as previously mentioned, was two-fold: firstly, to provide an overview of the main financial and non-financial risks arising from managing non-standard products for traditional banks, such as cryptocurrencies and digital assets. Secondly, to pinpoint the key value drivers within risk management to uncover novel best practices and innovative business opportunities. The primary advantage of the guidelines outlined in the main section of this article is the following: to manage cryptocurrencies and digital assets, banks must introduce an additional variable, in other words, an additional complexity layer, into their organisational framework, and to be more specific within their risk management models. This complexity translates into both a negative aspect, which can be represented as increased costs to manage this new layer of complexity, and a positive aspect: skilful management of this complexity could transform legacy institutions into innovative ones, securing additional profits and competitive advantages that are rare and hard to replicate within the financial industry [20223, DugganWaynePowellFarran23, NBMG16, Tan23].

Furthermore, the legacy bank that first adopts this new analytical variable into its risk management model (and therefore, also into its business approach) can enjoy the benefits of being a first mover.

Eventually, the following key takeaways emerge: 1. Banks can benefit from engaging with cryptocurrencies through diversification, attracting clients, and fostering innovation (let's look for example at the Revolut case, highlighted in this article). 2. Effective, proactive, and reactive risk management practices are crucial to mitigate traditional risks (e.g., interest rate risk) in the context of cryptocurrencies. 3. Liquidity risks in cryptocurrency markets require careful consideration and contingency planning. 4. Proactive monitoring, robust internal controls, and compliance with regulations are essential for banks to manage risks effectively.

Conclusion

Cryptocurrencies and digital assets represent a significant paradigm shift in the financial industry.

It's important for a legacy bank to:

- gain a rare and hard-to-replicate competitive advantage, leveraging also on first-mover advantage. The ultimate objective is to secure additional profits compared to the current state.
- tailor risk management practices specific to your organisation, regulatory requirements, and commercial opportunities. Banks that recognise and embrace these changes can harness new opportunities while managing the associated risks. By adopting a proactive and reactive approach to risk management, banks can position themselves at the forefront of innovation, enhance customer relationships, and drive sustainable growth in the digital era.

Alessio Pezzotta
September 2023

References

[20223](1,2) Custodial vs non-custodial wallets. Feb. 2023. URL: https://crypto.com/university/custodial-vs-non-custodial-wallets.

[DugganWaynePowellFarran23](1,2,3)

[Ltd21](1,2) Revolut Ltd. Annual report and financial statements. Dec. 2021. URL: https://assets.revolut.com/pdf/Revolut_Ltd_YE_2021_Annual%20Report.pdf.

[NBMG16](1,2,3) Arvind Narayanan, Joseph Bonneau, Edward Felten, Andrew Miller, and Steven Goldfeder. *Bitcoin and Cryptocurrency Technologies: A Comprehensive Introduction*. Princeton University Press, 2016.

[Pan23] Fabio Panetta. Paradise lost? how crypto failed to deliver on its promises and what to do about it. Jun. 2023. URL: https://www.ecb.europa.eu/press/key/date/2023/html/ecb.sp230623_1~80751450e6.en.html.

[Pec23] Marcel Pechman. How do the fed's interest rates impact the crypto market? Mar. 2023. URL: https://cointelegraph.com/news/how-do-the-fed-s-interest-rates-impact-the-crypto-market.

[Ser23](1,2) Andrey Sergeenkov. How to manage risk when trading cryptocurrency. May 2023. URL: https://www.coindesk.com/learn/how-to-manage-risk-when-trading-cryptocurrency/.

[Tan23](1,2,3,4,5,6,7) Lynette Tan. Managing crypto investment risks. Jun. 2023. URL: https://www.dbs.com.sg/personal/articles/nav/investing/crypto-risk.

Innovation & Ideation

Soulbound Tokens (SBTs)

Understanding Zero Knowledge Proofs

Soulbound Tokens (SBTs)

Innovation & Ideation

Key Insights

- 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 are 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.

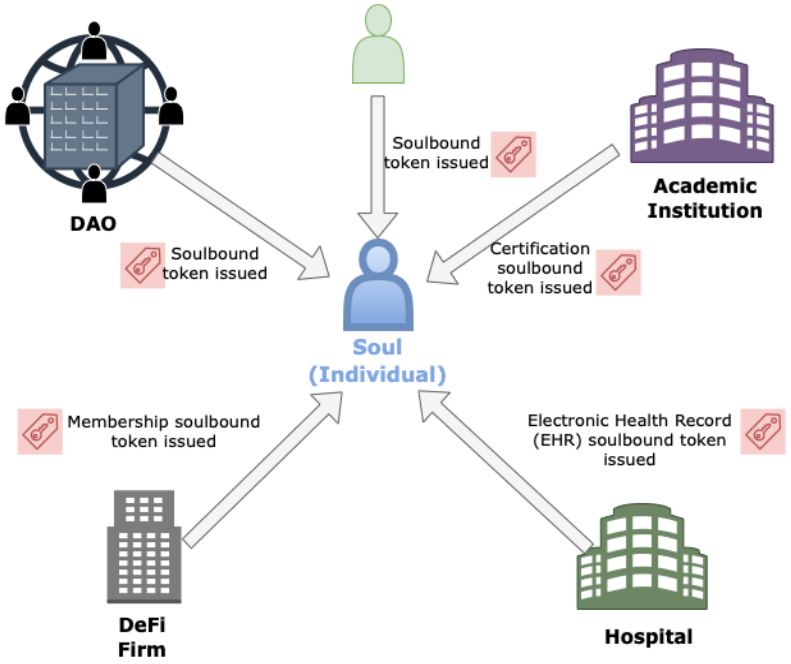


Fig. 17 Soulbound Token Issuance in DeSoc.

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.

Economic growth is primarily driven by networks yielding increasing returns, but the current private property paradigm of DeFi can limit such 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.

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

A collusion attack in blockchain refers to a scenario where a group of participants in a 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, incentivising users of the old platform to migrate their assets.

Functionality of SBTs

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 example, an individual could possess an array of 'Souls', each symbolizing different facets of their identity, such as their professional credentials, and medical histories, among other elements [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].

Preventing Sybil Attacks in DAOs

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 digitisation 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

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 profiles.

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 marginalised social groups who are more likely to experience disfavour [ShrishtiEth22]. 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 worth contemplating.

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
July 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.

[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 forms of ZKP, like zk-SNARKs and zk-STARKs, have evolved to provide shorter proofs, lower computational requirements, and eliminate the need for a trusted setup.
- ZKPs are revolutionising a range of blockchain applications, from Digital Identity and Traffic Management Systems to Mobile Health, ridesharing, and real estate transactions, by ensuring privacy-centric 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 decentralised 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 reconciling 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].

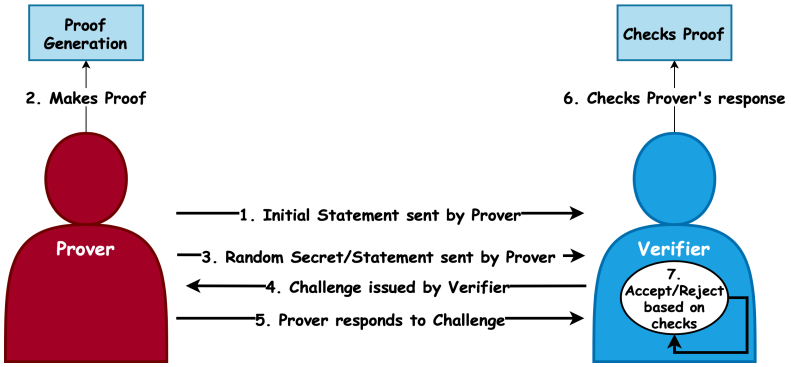


Fig. 18 Zero-Knowledge Proof Protocol Flow.

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 groundbreaking paper. 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.

Zero-Knowledge Proof

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.

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.

ZK-SNARKs (Zero-Knowledge Succinct Non-Interactive Argument of Knowledge)

These are compact, quick to verify cryptographic proofs that allow one party to prove they know specific information without revealing that information. The downside is they require a "trusted setup," where a secret parameter must be generated and then destroyed.

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].

ZK-STARKs (Zero-Knowledge Scalable Transparent Arguments of Knowledge)

These are similar to ZK-SNARKs, but they don't require a trusted setup, making them more secure. They also remain efficient even as the

attacks. However, they generate larger proof sizes compared to ZK-SNARKs.

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 behaviour 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.

To mitigate these risks, Non-Interactive Zero-Knowledge Proof can be used as part of a lightweight authentication scheme. 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].

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
August 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] 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] 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] Wanxin Li, Hao Guo, Mark Nejad, and Chien-Chung Shen. Privacy-preserving traffic management: a blockchain and zero-knowledge proof inspired approach. *IEEE access*, 8:181733–181743, 2020.

[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.

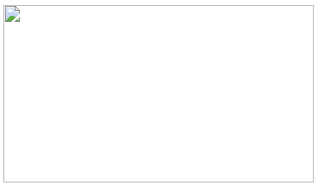
[MGGR13] Ian Miers, Christina Garman, Matthew Green, and Aviel D Rubin. Zerocoin: anonymous distributed e-cash from bitcoin. In *2013 IEEE Symposium on Security and Privacy*, 397–411. IEEE, 2013.

[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.

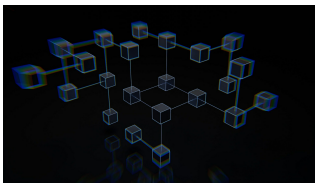
[YL20] Xiaohui Yang and Wenjie Li. A zero-knowledge-proof-based digital identity management scheme in blockchain. *Computers & Security*, 99:102050, 2020.

Academic Insights

Governance In DeFi



Blockchain Bridge Security



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, decentralised exchanges and yield aggregators. This research work employed case studies to comprehend the governance mechanisms of these protocols.

Similarly, the result by Jensen et al. [JvWR21] demonstrates centrality in voting power with the protocols' top 5, top 100, and top 1000 wallet addresses controlling the 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. 19]. 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.

Decentralised Exchanges

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

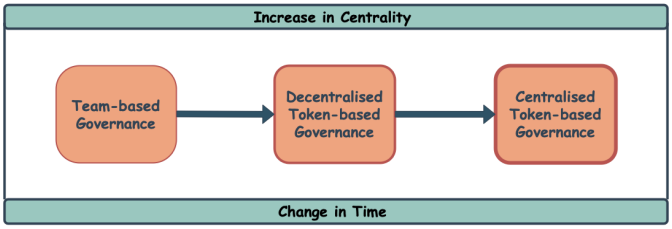


Fig. 19 The Tendency for Centralisation in DeFi Governance.

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 weighted 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 favour, typically by coordinating their votes to create a supermajority.

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 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 bond voting and an AI-enabled parameter-selection solution

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.

[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.

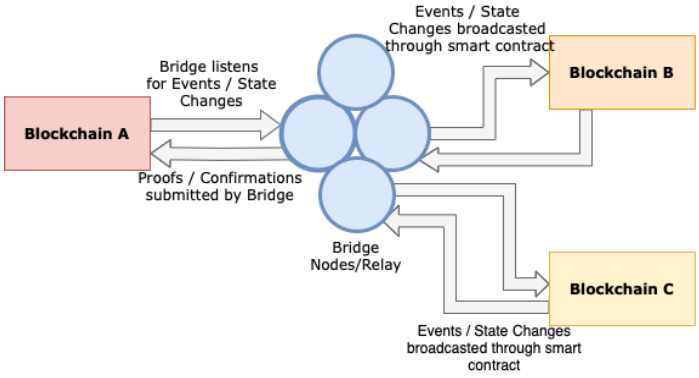


Fig. 20 Communication through a Blockchain Bridge.

Interoperability and Security Challenges

Zero-Knowledge Proofs

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].

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.

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.

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.

Pillai et al. [PBHouM22] 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, 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.

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.

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.

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, and then proceeds with the asset transfer through a cross-blockchain interaction process.

Maintaining Sovereignty of blockchains

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

[**Bro22]** Ryan Browne. Hackers have stolen $1.4 billion this year using crypto bridges. here’s why it’s happening, cnbc. *CNBC*, 2022. URL: https://www.cnbc.com/2022/08/10/hackers-have-stolen-1point4-billion-this-year-using-crypto-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.

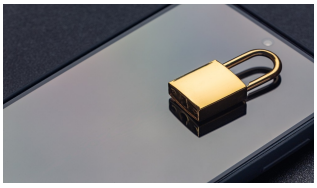
[**XZC+22]** Tiancheng Xie, Jiaheng Zhang, Zerui Cheng, Fan Zhang, Yupeng Zhang, Yongzheng Jia, Dan Boneh, and Dawn Song. Zkbridge: trustless cross-chain bridges made practical. *arXiv preprint arXiv:2210.00264*, 2022.

[**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.

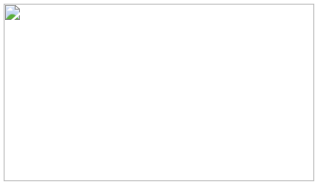
[**ZLZ20]** Jianbiao Zhang, Yanhui Liu, and Zhaoqian Zhang. Research on cross-chain technology architecture system based on blockchain. In *Communications, Signal Processing, and Systems: Proceedings of the 8th International Conference on Communications, Signal Processing, and Systems 8th*, 2609–2617.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

Industry Perspective

Mobile Theft Prevention using Blockchain



Financial Institutions and Crypto Customers



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 decentralised solution to prevent mobile theft.
- The proposed model of using blockchain for mobile theft prevention offers several potential advantages over existing methods, including decentralised and tamper-proof tracking, automation of processes, 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 meagre 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 decentralised 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 unauthorised 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 organisations 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 organisations 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 organisations protect their mobile devices and personal information by providing a decentralised 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.

- **Decentralised and tamper-proof:** Blockchain technology enables a decentralised 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 helps to maintain the privacy of the users.
- **Automation of processes:** Smart contracts can be programmed to automatically disable the device once the signal is sent, reducing human error and increasing 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 decentralised 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.

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 acts 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.

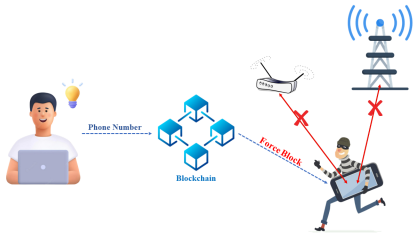


Fig. 21 Working Mechanism of Mobile Theft Prevention Using Blockchain

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 authorised 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 exist 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 exist 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, and 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.

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]** 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/.

Financial Institutions and Crypto Customers

Industry Perspective

Disclaimer: The views and opinions expressed in this article are solely those of the author

Key Insights

- Legacy banks and financial institutions face internal and external challenges in integrating cryptocurrencies into their existing business framework for generating new revenue streams.
- The internal perspective involves leveraging distributed ledger technology for overall better management.
- The external perspective focuses on managing crypto customers, including regulatory compliance and environmental sustainability.
- Legacy banks often miss out on business opportunities due to constraints related to regulation, organisation, processes, delivery, and employee biases.
- Innovative central organisational structures should establish clear provisions, monitor key performance indicators, and develop product management strategies.
- Offering tailored financial products, such as crypto mining equipment insurance and crypto hedging insurance, can enhance profitability and help diversify revenue streams.
- Talent acquisition and skill development are crucial to improve crypto risk management within legacy banks.
- Additional expertise is required in advanced programming languages, an end-to-end vision of innovation, and product design.
- By addressing these challenges, legacy financial institutions can embrace the potential of cryptocurrencies and stay ahead in the evolving financial landscape.

A Background Story

Some months ago, a friend of mine working in the sales department of a major European bank told me about a chaotic experience he had with a potential client. The client was a cryptocurrency miner who had invested in a warehouse in Switzerland and filled it with state-of-the-art computers for mining. The business was thriving, and with the cryptocurrency boom, it was yielding good profits. However, some weather events, like a hailstorm, had caused heavy damage to his equipment.

The miner contacted my friend to inquire about insurance protection against such weather events. My friend saw the opportunity and approached the relevant departments in his bank, including bank insurance and product design. That's where the story ended. My friend spent countless meetings and days explaining the basics to our colleagues: what a miner

prospective customer. Preventing these missed business opportunities from happening again in legacy banks is the subject of this science note.

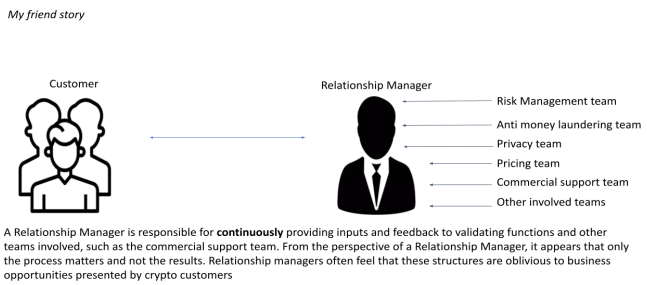


Fig. 22 Functions of the Relationship Manager.

Introduction

Cryptocurrencies present unique challenges for legacy financial institutions from both internal and external viewpoints. Internally, these institutions must explore how to integrate cryptocurrencies and distributed ledger technologies into their existing systems, leveraging the technology to embrace a new era of financial management. This internal perspective significantly impacts processes and IT infrastructure and also has implications for costs and IT investments, from a financial statement standpoint.

Externally, the presence of institutional and retail cryptocurrency customers (e.g., cryptocurrency platforms or cryptocurrency holders) creates a conundrum. This demands meticulous attention to regulatory compliance, risk management, and product offerings within the existing framework, which aims to discover innovative revenue streams beyond traditional avenues. Indeed, from a financial statement perspective, this external view could have a significant impact on revenues, allowing a diversification strategy.

> **Internal Perspective**
>
> Legacy banks face the challenge of integrating cryptocurrencies into their traditional banking systems, which involves exploring ways to leverage blockchain technology, decentralisation, and secure transactions. By effectively integrating these digital assets, legacy banks can tap into the potential of cryptocurrencies and offer innovative financial services to their customers.

Managing Crypto Customers

Legacy banks encounter a unique set of challenges when engaging with crypto customers [Ban23a, Ban23b]. Relationship managers and salespeople must navigate the complexities of regulatory compliance, such as Anti-Money Laundering (AML) and Know Your Customer (KYC) regulations, to ensure adherence while facilitating a seamless customer experience. Additionally, concerns related to environmental sustainability and energy consumption associated with cryptocurrencies need to be addressed, providing clarity on the bank's stance regarding these issues.

Legacy banks often miss out on business opportunities due to the interplay of regulatory, organisational, process, delivery, and employee bias constraints. To overcome these constraints and expand their business opportunities, legacy banks must adopt a proactive and reactive approach by focusing on setting up new central organisational structures within their general management organisation. These new structures have responsibilities to provide clear provisions (both from credit risk and reputation risk management), Key Performance Indicators (KPIs), and product management strategies exclusively dedicated to managing cryptocurrencies and serving crypto customers.

By proactively tackling both internal and external challenges, legacy financial institutions can begin to adeptly navigate the rapidly shifting landscape of cryptocurrency. In this article, we delve into a variety of innovative strategies and approaches that could be harnessed to tap into the vast potential of cryptocurrencies. A profound paradigm shift, altering how legacy banks engage with and manage cryptocurrencies, is indeed a pressing necessity in today's digital era.

Assessing Regulatory and Compliance Considerations

Engaging with crypto customers entails navigating through stringent regulatory obligations, such as AML and KYC regulations. Relationship managers and salespersons must ensure effective compliance with these regulations while also addressing concerns regarding environmental sustainability, given the energy-intensive nature of certain cryptocurrencies.

Given that these professionals receive no support from other organisational structures within their banking or financial institutions, the burden of responsibility rests squarely on their shoulders. The breadth of their tasks is considerable, presenting a complex landscape that must be navigated independently.

To illustrate this from an operational standpoint, these individuals must personally interpret and apply relevant legal constraints due to a lack of cryptocurrency regulatory knowledge amongst legal professionals in traditional banks. Beyond this, they must design and implement a profitable pricing strategy that gains management approval, a task often involving numerous meetings, complex analyses, and financial simulations.

Moreover, they must fulfil climate, anti-money laundering, and privacy assessments, which are lengthy, complex, and mandatory in the credit process [Uni18a]. All these activities are required to be performed simultaneously and swiftly to maintain a positive commercial relationship with customers and analyze competitors' actions. A chaotic, complex, and overwhelming task without help!

A more constructive approach has been lacking mainly due to the two major reasons:

- Unclear regulation about cryptos.

On the latter, the EU has been working on regulating cryptocurrencies to address potential risks and ensure consumer protection. While there is no specific comprehensive regulation for crypto management in banks, the following regulations may be relevant:

- MiCAR (Market in Crypto-Assets Regulation) [Com20].
- Anti-Money Laundering Directive (AMLD) [Uni15].
- Markets in Financial Instruments Directive (MiFID II) [Uni14].
- EU General Data Protection Regulation (2016/679, "GDPR") [Uni18b].

From the perspective of a middle-aged EU bank employee, these regulations fail to provide a clear and straightforward framework. Instead, they offer only basic principles and contribute to the overwhelming amount of documentation that banks must manage within the European Union. Essentially, this situation becomes a burden, leading to additional costs without generating any significant increase in revenue. We will explore some potential solutions to these problems next.

Expanding Business Opportunities

Relationship managers and salespersons of legacy banks usually miss out on significant business opportunities due to the interplay of regulatory, organisational, process, delivery, and employee bias constraints. To overcome these limitations, again, a paradigm shift is needed. Instead of treating crypto customers as a challenging prospect, the entire organisation should embrace a proactive and reactive approach, which means setting up enabling factors for allowing the onboarding of crypto customers. These enabling factors entail creating central organisational structures within the bank that specialise in crypto management, encompassing risk management, AML, privacy, and product creation and offerings.

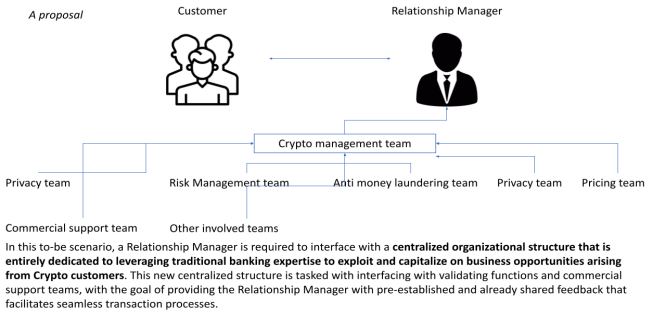


Fig. 23 Alternative Scenario with Relationship Manager.

Establishing Centralised Organisational Structures

Central organisational structures dedicated to managing cryptocurrencies need to be set up from scratch because they can provide the necessary focus and guidance, encompassing both business and technical perspectives. These entities should establish clear provisions, mapping opportunities and risks, and set up and monitor KPIs and product management strategies.

By assigning specific responsibilities and structured activities, legacy banks can effectively identify and serve the right crypto customers, while ensuring compliance and risk mitigation and disregarding crypto customers that do not respect the bank provisions (e. g. crypto customers that do not have data privacy IT servers within a certain list of countries, or crypto customers that have some previous criminal records in terms of money laundering). Furthermore, offering tailored financial products, such as financing and insurance solutions, can enhance the profitability of the legacy institution. These bespoke products can be imagined only by employees who are engaged and motivated in the crypto world. Here are some examples of innovative crypto products that legacy banks could sell to crypto customers:

1. Crypto Mining Equipment Insurance: Develop insurance policies specifically designed to cover the risks associated with crypto mining equipment, such as physical risks (e.g., flood, hailstorm, theft, damage, or breakdown. This type of coverage would provide financial protection for miners who invest heavily in hardware
2. Crypto Hedging Insurance: Develop insurance policies specifically designed to cover the risks of extreme price volatility. This type of coverage would provide financial protection for crypto holders against price volatility
3. Operative Risks Insurance: Offer insurance policies that cover losses resulting from smart contract vulnerabilities, coding errors, and fraudulent or failed transactions. This coverage could offer reimbursement for lost funds due to transaction errors, technical glitches, or fraudulent activities.

Talent Acquisition and Skill Development

Overcoming biases and improving crypto risk management within legacy banks may require attracting talent from outside the financial industry. Re-skilling and up-skilling existing employees may not be sufficient; therefore, individuals with fresh perspectives and expertise, especially those from product design and development will be required. This transformation process should focus on developing a workforce with the necessary skills to navigate the complexities of cryptocurrencies and related financial services.

In the general context, and simplifying it to the utmost, within legacy banks there are now individuals who possess extensive expertise in accounting, credit risk and loan origination, as well as classical IT knowledge related to applications managing transactions and data. The skills that are lacking to integrate an active and proactive understanding of cryptocurrencies pertain to:

1. Advanced and cutting-edge programming languages
2. An eclectic and end-to-end vision of innovation (currently, innovation departments in legacy banks only focus on processes and costs rather than revenues and products)
3. Proficiency in designing new products that are completely different from the traditional ones.

Legacy financial institutions must proactively address the challenges associated with managing crypto customers. By navigating regulatory considerations, expanding business opportunities, establishing central organisations, and attracting specialised talent, these institutions can unlock the potential of cryptocurrencies within their existing frameworks. Embracing this transformation will not only help overcome the constraints imposed by regulation and biases but will also position the institutions at the forefront of the evolving financial landscape.

Alessio Pezzotta
June 2023

References

[**Ban23a]** European Central Bank. Crypto-assets: a new standard for banks. *European Central Bank*, 2023. URL: https://www.bankingsupervision.europa.eu/press/publications/newsletter/2023/html/ssm.nl230215_1.en.html.

[**Ban23b]** European Central Bank. Take-aways from the horizontal assessment of the survey on digital transformation and the use of fintech. *European Central Bank*, 2023. URL: https://www.bankingsupervision.europa.eu/ecb/pub/pdf/Takeaways_horizontal_assessment~de65261ad0.en.pdf.

[**Com20]** European Commission. Regulation of the european parliament and of the council. *European Commission*, 2020. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52020PC0593.

[**Uni14]** European Union. Markets in financial instruments regulation (mifir). *European Union*, 2014. URL: https://eur-lex.europa.eu/EN/legal-content/summary/markets-in-financial-instruments-regulation-mifir.html.

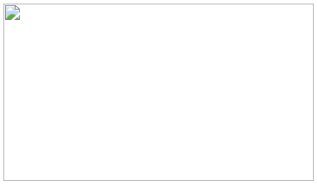
[**Uni15]** European Union. Anti-money laundering directive. *European Union*, 2015. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:32015L0849.

[**Uni18a]** European Union. Directive of the european parliament. *European Union*, 2018. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF.

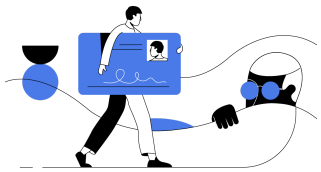
[**Uni18b]** European Union. General data protection regulation. *European Union*, 2018. URL: https://gdpr-info.eu.

Innovation & Ideation

Sharding: A Panacea for Blockchain Scalability Challenges



Self-Sovereign Identity: Technical Foundations and Applications



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)

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 decentralisation.

> **Note**
>
> **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 are 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 the 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 generalisability 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.

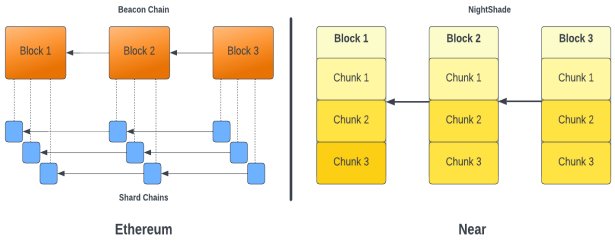


Fig. 24 Sharding in Ethereum vs Near Blockchain

Sharding in Ethereum

In Ethereum, data is distributed among several “shard chains” ([Fig. 24]). 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 synchronisation and ensuring a common ledger. The shards receive sets of transactions from the mempool. Under the Ethereum 2.0 proposal, these TXs are split based on their transaction types: Token transfers and Smart contract interactions. Validators then use an EVM to process shards’ data into a block and update the Merkle tree’s state on the beacon chain [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. 24]. 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.

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

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. 25], 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 proof of the latest execution message.

VRF

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

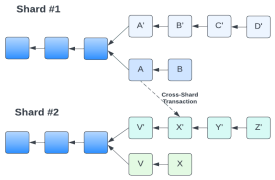


Fig. 25 Cross-Shard Communication

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 of outgoing messages to be sent to other shards, and each message within a specific queue is assigned a unique sequence number.

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 minimising centralisation 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](1,2) Hedera. Hedera hashgraph whitepaper. *Hedera*, 2020. URL: https://hedera.com/hh_whitepaper_v2.1-20200815.pdf.

[**HPZ+22]** Huawei Huang, Xiaowen Peng, Jianzhou Zhan, Shenyang Zhang, Yue Lin, Zibin Zheng, and Song Guo. Brokerchain: a cross-shard blockchain protocol for account/balance-based state sharding. In *IEEE INFOCOM 2022-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]**

[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.

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. 26]. 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.

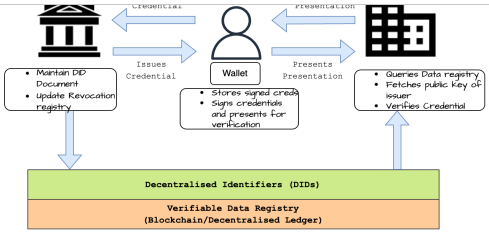


Fig. 26 SSI entities and their relations

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

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

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.