POLITECNICO DI TORINO

Master's Degree in Computer Engineering
Cybersecurity Focus

Architecting a Decentralized Framework for Self-Sovereign Identity Management

Supervisor
Prof. Danilo Bazzanella
Company Supervisors
Dr. Alfredo Favenza
Dr. Silvio Meneguzzo

Candidate
Luca Rota

Accademic Year 2023/2024

Summary

In the evolving world the concept of identity is going through a significant change. The concept of identity undergoes a paradigm shift from centralized control to self-sovereignty.

This thesis, conducted at Links Foundation explores the realm of Self Sovereign Identity (SSI) in identity management. By leveraging technology and the powerful MetaMask tool we have developed a SSI framework that seamlessly integrates with Links Foundations Data Cellar project. This framework showcases real world applications. The thesis focuses on cybersecurity aspects and culminates in a decentralized application (DApp). The DApp combines frontend design using React and JavaScript with a backend system built with NestJs to ensure secure and user centric authentication processes.

This valuable work contributes to the discussion about the potential of identity aligning perfectly with Links Foundations commitment, to digital innovation.

Acknowledgements

Contents

List of Tables

List of Figures

Listings

Chapter 1

Introduction

In a world of constantly advancing technology, the concept of identity has experienced a significant transformation. It has shifted from being tied to our existence to encompassing the digital realm as well. Consequently the management of our identities now necessitates a reevaluation prompting us to explore the notion of SSI. This thesis delves into the realm of identity using technology providing fresh insights, into how we perceive, protect and retain authority, over our digital identities.

1.1 Objectives

This project delves into the ever-evolving ecosystem of Links Foundation to thoroughly explore the concept of SSI. Our ambitious objectives consist of developing an autonomous SSI framework for managing decentralized identities through the use of MetaMask and the Ethereum blockchain. Furthermore, we strive to seamlessly incorporate this cutting-edge framework into the advanced Data Cellar project at Links Foundation.

This exploration takes us into the intricacies of technology tracing the origins of identity from its non digital beginnings to its current form. By studying the foundations of SSI we gain insights, into the security and privacy measures in place as well as addressing the prevalent cybersecurity challenges within the SSI domain.

With a focus on practicality this research culminates in developing a SSI framework that incorporates groundbreaking elements like MetaMask and a customized Ethereum smart contract. This framework has the potential to revolutionize identity management as evidenced by its integration into Data Cellar.

As we reach the end of this journey we celebrate achieving an accomplishment – creating a DApp. This achievement not showcases an user friendly interface built with React and JS for frontend development and NestJs for backend development but also seamlessly integrates our SSI framework. This milestone not overcomes standing obstacles but also paves the way, for a future where individuals have greater control over their digital identities.

1.2 Outline

After a brief introduction and description of the goals of the thesis presented in Chapter [1], the remaining parts of the paper are structured as follows:

- TODO

Chapter 2

The Blockchain Technology

In the current landscape, blockchain technology has attracted increasing global interest due to its promising applications and potential transformative impacts on various sectors. Founded in 2008 by Satoshi Nakamoto as the mainstay of the Bitcoin system [5], blockchain has evolved from a simple ledger of financial transactions to a fundamental technology that revolutionizes the way information is recorded, shared and managed within decentralized networks.

2.1 What is the Blockchain

The blockchain is a core technology that drives many decentralized systems offering transparency, trust and safety without having to have a central authority. It is basically a distributed ledger that operates through the peer-to-peer [7], [6]. This section talks of the key components and architecture in blockchain, revealing its fundamental features and operating principles.

2.1.1 Core Elements of Blockchain

The blockchain comprises several key elements essential to its functionality:

- **Blocks**: A block is a basic unit comprising of transactional data. Every block is securely connected to the previous one; this connection creates a chain of blocks. The transactions within a block are cryptographically secured; hence, immutability and integrity [7], [6].
- **Transactions**: Transactions are diverse interactions in the blockchain network. These interactions are not limited to the financial transfers only; any

piece of valuable information can be considered as a transaction and diffused within the network [5], [9].

- **Decentralization**: Unlike centralized systems that depend on a single controlling authority, the blockchain is decentralized. It includes a web of interdependent nodes, each replicating the distributed registry. Resilience, transparency and no single points of failure are guaranteed by decentralization [7], [5].

- **Consensus Mechanism**: For verification and agreement of the state of a ledger, blockchain uses consensus mechanisms. The most common mechanism, Proof of Work (PoW), requires miners to solve the complicated cryptographic puzzles in order to add new blocks on the chain. Consensus mechanisms ensure consensus among network participants to prevent attacks by malicious actors [7], [5].

2.1.2 Blockchain Architecture

The structure of the system is carefully crafted to uphold its principles of decentralization, immutability and transparency;

- **Distributed Ledger Technology (DLT)**: At the core of blockchain lies DLT, where all participants, in the network have access to a ledger of transactions. This shared ledger eliminates redundancy. Ensures that everyone has a trusted source of information across the network [6], [5].

- **Immutable Records**: One key feature of blockchain is its records immutability. Once a transaction is recorded on the ledger it cannot be. Tampered with. Any attempt to change a transaction requires adding an one preserving the integrity of data [6].

- **Smart Contracts**: Smart contracts are self executing contracts with predefined rules embedded within the blockchain. These contracts. Enforce agreements between parties speeding up transaction processing and reducing reliance on intermediaries [6], [9].

- **Security Measures**: Cryptography plays a role in ensuring security by protecting transactions from tampering and fraud. Private key pairs authenticate. Enable secure digital identity management. Additionally cryptographic hashing guarantees data integrity and confidentiality [7], [9].

- **Peer-to-Peer Network**: The blockchain functions using a network architecture where participants can directly communicate and interact. This decentralized structure promotes trust and resilience since transactions are verified and validated through consensus, among distributed nodes [5], [9].

2.2 How the Blockchain works

The function of a blockchain system encompasses a complex chain of procedures that safeguard the integrity, transparency, and security of transactions. In this section, we delve into the fundamental mechanisms of blockchain.

2.2.1 Transaction process

Recording transactions

1. **Starting a Transaction:** In a network, users initiate transactions through their wallets. Each wallet has a pair of keys. A key, for starting transactions and a private key for authentication [7].
2. **Creating Blocks:** As transactions take place they are grouped together into blocks of data. These blocks act as containers for recording details like asset movement participants involved and timestamps [6].
3. **Hashing:** Every block contains information and refers to the hash of the previous block. Secure hash functions like SHA 256 play a role in ensuring the integrity and immutability of transactions. Hashing allows each block to have a fingerprint making identification and verification simple [6] ,[9].

Consensus Mechanism

4. **Verification Process:** When a transaction is initiated the information is sent to a network of distributed peer, to peer nodes. These nodes work together to confirm the validity of transactions using consensus mechanisms [9], [4].
5. **Formation of New Blocks:** Valid transactions are added to a Memory Pool (MemPool) where they wait to be included in a block. Miners, who are responsible for creating blocks solve cryptographic puzzles in order to mine blocks. This process, known as PoW requires resources and time [7], [4].
6. **Consensus Algorithm:** In order to add a block to the blockchain nodes must agree on its validity through consensus algorithms. The miner who

successfully creates a block is rewarded. Consensus algorithms ensure that all nodes are synchronized and in agreement, about the state of the blockchain [4].

7. **Blockchain Integrity:** The interconnected nature of blocks ensures the immutability and integrity of the blockchain. Each block references the hash value of its predecessor making it practically impossible to tamper with transactions without altering blocks [7] ,[9].

2.2.2 Blockchain Benefits

Due to the execution process described above and its architecture, blockchain is able to offer many benefits in different areas:

- **Greater Trust:** Blockchain helps establish trust across the network through utilizing the decentralized ledger, making sure that data is consistent and timely plus, it doesn't require intermediaries [7].
- **Enhanced Security:** Blockchain's security features are designed to thwart tampering as well as cybercrime. The blockchain structures transactions as read-only data which is difficult to change and ensures that the data is protected even when it is in transit. Moreover, cryptography is used as a mechanism of verification and the cryptographic infrastructure is used to store and transmit secrets [6].
- **Time Savings:** The utilization of blockchain technology decreases greatly the processing time for transactions since they get completed within a quarter of an hour due to the removal of the centralized authority that confirms [6].
- **Cost Savings:** The blockchain adjusts transaction procedure and lowers operational costs by the removal of intermediaries, as tasks are automated and there is lower duplication of activities through the usage of shared ledger [7], [9].
- **Efficiency Improvements:** The distributed architecture of blockchain increases system resilience, decreases processing costs, and removes the need for centralized network control by distributing network operations thinly, facilitating faster settlements, and solving identity management issues [9].
- **Transparency Enhancement:** A blockchain keeps a permanent record of transactions through which it delivers transparency, accountability and trust to the network users via its chronological and transparent nature [9].

2.3 Blockchain Classification

2.3.1 Types of Blockchains

The blockchain technology comes in various forms, each with unique characteristics that adapt to specific needs and application contexts Beyond the well-known public and private blockchains, it's essential to recognize two other significant variants: hybrid chains and consortium chains.

- **Public Blockchain (Permissionless):** A public blockchain is open to everybody who wants to interact and contribute to the consensus protocol, e.g., Bitcoin. This model provides a high degree of transparency though, it is susceptible to 51% attacks. Its open nature fosters a distrustful environment, as no one individual or entity is solely relied on for transaction validation [7], [6].

- **Private Blockchain (Permissioned):** In contrast to public blockchains, private or permissioned (access is restricted to authorized entities) blockchains allow only a limited set of entities to access the network. This method is popular among situations that demand more of such features such as security as well as control where it gets applied in applications like financial transactions that also handle sensitive data. An access to the network is controlled by a single entity or by particular criteria [7],[9].

- **Hybrid Blockchain:** Hybrid blockchains, on the other hand, are described by the property of switching between different modes having different types of operating systems, for example, public and private blockchains that suit specific needs. This approach provides a greater degree of flexibility and customization compared to conventional blockchain configurations; thereby, the actors have the option to decide the degree of decentralization and control that is suitable for them [7].

- **Consortium Blockchain:** A consortium blockchain is governed by more than one organization or entity working together to ensure the distributed ledger. On the other hand, blockchains that are public or private, consortium blockchains are the only ones that give power to a chosen group of nodes to validate and record transactions. This model is suitable where several subjects need to work with data and processes together but they do not want or they cannot fully trust a unique central entity [6], [5].

2.3.2 Types of Consensus Mechanisms

Blockchains also differ based on the type of consensus mechanism used. In the previous section we discussed an example of how blockchain uses a consensus mechanism called PoW [5], [10]. However there are several types of consensus mechanisms that can be used in a blockchain network.

In general, the two main types of consensus mechanisms are: PoW and Proof of Stake (PoS). With PoW miners solve puzzles to add new blocks, which requires significant computational resources and time [5], [10]. This is elaborated further in Section 2.4.1. On the hand PoS assigns the right to create blocks based on participants cryptocurrency holdings providing benefits such, as energy efficiency and scalability advantages [10]. Further information, about PoS can be found in Section 2.4.2.

There are also other consensus mechanisms beyond PoW and PoS; refer to the table for further details.

2.4 Bitcoin versus Ethereum

2.4.1 Bitcoin

Overview

Bitcoin, launched in 2008 by Satoshi Nakamoto, is a decentralized digital currency that is also accompanied by the great invention, the blockchain. It functions as a peer-to-peer decentralized electronic payment system; it introduces a new way of executing business transactions and the security of data [8]. Bitcoin is an open-source and permissionless blockchain, allowing for involvement of anyone with the required hardware.

Transaction mechanism

When a user sends bitcoins, sender hashed addresses, recipient hashed addresses, transaction amount and fee. Digital signatures prove property rights and the transaction is floated to the network, being submitted to the mempool for confirmation [1]. The mining being the process of validating transactions and so the miners pick transactions from the MemPool in order to create new blocks by solving complex mathematical puzzles called PoW [8]. The winner of the puzzle then broadcasts their newly found block to the network. After a verification done by other network nodes, the block is added to the blockchain, thus finalizing the transaction.

Proof of Work

Bitcoin uses the PoW consensus algorithm to maintain agreement among network participants about the validity of transactions. The PoW was first specified in the Hashcash paper [8]. It requires the miners to search solutions of cryptographic puzzles consuming computational power. Through the cost of computation, the miners establish their commitment to the security of the network as changing the blockchain will require enormous computational resources, hence, making fraudulent endeavors expensive.

Bitcoin Cryptography

Bitcoin use the Secure Hash Algorithm 2 (SHA-2) for cryptographic hashing, which ensures irreversible and collision resistive attributes. This guarantees the data integrity of the blockchain, which makes it impractical to tamper with transactions that are already in the database. Moreover, the Merkle Trees that Bitcoin natively uses for block data encoding take security to the next level [8].

Unspent Transaction Output

Bitcoin transactions are registered in the blockchain as Unspent Transaction Output (UTXO)s, which meaning constant fractions of bitcoins that are linked to certain owner. This UTXO is pervasively distributed over the blockchain and represents ownership. It is subsequently used in other transactions too. Bitcoin balances are not stored in user accounts but rather tracked through the UTXOs associated with their addresses [1].

Advantages and Limitations

Bitcoin is decentralized and provides encryption security that can be used to resist censorship, to ensure accessibility particularly on a global scale and to preserve integrity of the data. Nevertheless, Bitcoin has such limitations as scalability problem, transaction throughput rate without the corresponding increase in the number of transactions and undulatory acceptance and valuation. Furthermore, there are additional security concerns, such as the "51% attack" and human error, which continue to plague the Bitcoin ecosystem [8].

2.4.2 Ethereum

Overview

Ethereum, designed by Vitalik Buterin, is the introduction of Smart Contracts to the crypto-sphere, which is a novelty in the blockchain space, and, obviously, it has been a highly valuable addition. The September 2022 saw the newly born Ethereum 2.0 replace Ethereum 1.0 by incorporating the Beacon Chain and the shift from PoW to PoS consensus mechanism [3]. This change shall constitute one of the really important milestones reached by Ethereum, the blockchain providing scalability, sustainability, as well as security.

Beacon Chain Impact

The introduction of the Beacon Chain revolutionized Ethereum's operating model [3]. It replaced the original execution layer (Mainnet) and introduced a new consensus layer, the PoS which was a major improvement in terms of power consumption and the amount of energy consumed reduced from 99.95%. Validators, staking their ETH, assumed the responsibility of block production and transaction validation, moving away from energy-intensive mining. This transition helped create a sustainable network architecture as well as secure the information connections.

Transaction Mechanism

In Ethereum 2.0, validators play a pivotal role by depositing 32 ETH and operating three essential software components: a execution client, a client for consensus, and a client for validation as well. Here we have the validators appointed randomly for being picked on 12 second timeslots which then make up epochs composed of 32 slots. They formulate and verify blocks and this way they add to the Ethereum System. This process regulates all the transactions on the blockchain. Transactions include processing stages of creating, verifying, and block proposal irrespective of the fact that the transactions are created, verified, combined into execution payloads, and broadcasted across the network so as to make self-enforcement and fault-tolerance in proper working order. Finality being one of the main features of transaction irreversibility, is sealed by using checkpoints that initiate even the smallest epochs. As requisite effort to checkpoints pairs, validators vote in a supermajority to revert them, consequently, block reversal is discouraged and the entire Ethereum network is protected from brainwashing attacks [2].

Proof of Stake

The Ethereum 2.0 version puts the PoS consensus mechanism at the core of the protocol with validators given the chance to make the most of their investment through staking [2]. Validator's deposit their own ETH as bond to release validator software which helps in the job of validating the transactions and generating new blocks proposals. In contrast to proof-of-work, the PoS is doing well in maintaining both the security and the decentralization of validators that attempt to undermine the network due to its feature of penalization.

Ethereum Cryptography

Ethereum 2.0 still relies heavily on the standards of crypto- security for safety, keeping the Keccak-256 algorithm implemented by Ethereum 1.0. These algorithmic primitives give Ethereum strong security by making sure the data integrity, confidentiality, and authenticity [8].

Advantages and Limitations

Ethereum 2.0 is an upgraded version of the original network as well as other blockchain platforms which provide these advancements. Transitioning from PoW to PoS does substantial energy reduction and making Ethereum more sustainable is one of them. Also, PoS model makes the network more secure, decentralized and scalable in order that a flourishing ecosystem of decentralized applications may thrive in it [2]. But after considering the fact that it is the second generation of Ethereum blockchain, it has certain limitations. The processing time still may be a bottleneck as Ethereum is not able to process transactions in the same rate as traditional procedures such as Visa [8]. Besides, the market fluctuation and rumors become the main problems for the stability and the reputation of the Ethereum that calls for continual technological development and management.

Chapter 3

Identity

Chapter 4

SSI

Chapter 5

Cryptography

Chapter 6

Cybersecurity

Chapter 7

Framework

Chapter 8

Integration

Chapter 9

Conclusions

Bibliography

[1] Bitcoin.com. *How Bitcoin Transactions Work*. URL: https://www.bitcoin.com/get-started/how-bitcoin-transactions-work/ (visited on 02/14/2024).

[2] Ethereum Foundation. *Proof of Stake (PoS)*. URL: https://ethereum.org/en/developers/docs/consensus-mechanisms/pos (visited on 02/14/2024).

[3] Ethereum Foundation. *The Merge*. URL: https://ethereum.org/en/roadmap/merge (visited on 02/14/2024).

[4] GeeksforGeeks. *How does the Blockchain Work?* URL: https://www.geeksforgeeks.org/how-does-the-blockchain-work/ (visited on 02/08/2024).

[5] Varun Chandra Gupta et al. "An Intrinsic Review on Securitization using Blockchain". In: *2021 International Conference on Computational Performance Evaluation (ComPE)*. 2021, pp. 971–976. DOI: 10.1109/ComPE53109.2021.9752154.

[6] IBM. *Blockchain Technology*. URL: https://www.ibm.com/topics/blockchain (visited on 02/06/2024).

[7] Rajesh Kumar Kaushal et al. "Immutable Smart Contracts on Blockchain Technology: Its Benefits and Barriers". In: *2021 9th International Conference on Reliability, Infocom Technologies and Optimization (Trends and Future Directions) (ICRITO)*. 2021, pp. 1–5. DOI: 10.1109/ICRITO51393.2021.9596538.

[8] Bharti Pralhad Rankhambe and Harmeet Kaur Khanuja. "A Comparative Analysis of Blockchain Platforms – Bitcoin and Ethereum". In: *2019 5th International Conference On Computing, Communication, Control And Automation (ICCUBEA)*. 2019, pp. 1–7. DOI: 10.1109/ICCUBEA47591.2019.9129332.

[9] Sheetal Sinha, Kumkum, and Ruchika Bathla. "Implementation of Blockchain in Financial Sector to Improve Scalability". In: *2019 4th International Conference on Information Systems and Computer Networks (ISCON)*. 2019, pp. 144–148. DOI: 10.1109/ISCON47742.2019.9036241.

[10] Xuesen Zhang et al. "Research on blockchain consensus algorithm for large-scale high-concurrency power transactions". In: *2022 9th International Forum on Electrical Engineering and Automation (IFEEA)*. 2022, pp. 1221–1225. DOI: 10.1109/IFEEA57288.2022.10037907.