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 [2], 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 [4], [3]. 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 [4], [3].
- **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 [2], [5].

- **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 [4], [2].

- **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 [4], [2].

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 [3], [2].

- **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 [3].

- **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 [3], [5].

- **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 [4], [5].

- **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 [2], [5].

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 [4].
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 [3].
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 [3] ,[5].

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 [5], [1].
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 [4], [1].
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 [1].

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 [4] ,[5].

2.2.2 Types of Consensus Mechanisms

In the previous section we discussed an example of how blockchain uses a consensus mechanism called PoW [2], [6]. 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 [2], [6]. 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 [6]. 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.

2.3 Types and Advantages of Blockchains

2.4 Comparative of Bitcoin and Ethereum

2.4.1 Bitcoin

2.4.2 Ethereum

Chapter 3

Identity

Chapter 4

SSI

Chapter 5

Cryptography

Chapter 6

Cybersecurity

Chapter 7

Framework

Chapter 8

Integration

Chapter 9

Conclusions

Proof of Take (PoT)

Bibliography

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

[2] 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.

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

[4] 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.

[5] 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.

[6] 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.