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 fast-paced landscape of digital evolution, the concept of identity undergoes a paradigm shift from centralized control to self-sovereignty.

This thesis, which was carried out at Links Foundation, delves into the exciting and transformative landscape of Self-Sovereign Identity (SSI) within the realm of decentralized identity management.

By utilizing blockchain technology and the powerful MetaMask tool, a standalone SSI framework has been developed to seamless integrate with Links Foundation's Data Cellar project, showcasing practical and real-world applications. With a focus on cryptographic and cybersecurity aspects, this research ultimately culminates in a decentralized application (DApp) that boasts a combination of sophisticated frontend design (based on React and JavaScript) and a robust backend system (built with NestJs) for ensuring secure and user-centric authentication processes.

This valuable work contributes to the ongoing discussion on the potential of decentralized identity, aligning perfectly with Links Foundation's dedicated efforts towards digital innovation.

Acknowledgements

Contents

List of Tables

List of Figures

Listings

Chapter 1

Introduction

In a world of constantly advancing technology, the very definition of identity has undergone a profound evolution, shifting from the traditional physical realm to the digital world. As a result, managing our identities now requires a reconsideration, leading to the exploration of Self-Sovereign Identity (SSI).

Through the use of blockchain technology, this thesis delves into the world of decentralized identity, offering a new perspective on how we view, safeguard, and maintain control over our digital identities.

1.1 Objectives

Through this project, set within the dynamic ecosystem of Links Foundation, our goal is to deeply investigate the concept of Self-Sovereign Identity (SSI). Our main objectives are twofold: first, to design an independent SSI framework for decentralized identity management using MetaMask and the Ethereum blockchain, and second, to seamlessly incorporate this framework into the advanced Data Cellar project at Links Foundation.

This journey is a deep exploration into the complexities of blockchain technology, tracing the origins of identity from its non-digital beginnings to its modern iteration. By delving into the cryptographic foundations of SSI, this study sheds light on the strong security and privacy measures in place, while also tackling the prevalent cybersecurity obstacles within the SSI realm. With practicality in mind, this research culminates in the creation of a robust and all-encompassing SSI framework, utilizing ground-breaking components such as MetaMask and a customized Ethereum smart contract to revolutionize decentralized identity management. The

successful integration into Data Cellar is a testament to the adaptability and real-world significance of this newly developed framework.

At the end of this journey, lies the accomplishment of a decentralized application (DApp), a significant feat that not only showcases a sleek and intuitive interface crafted with React and JS for the frontend and NestJs for the backend, but also effortlessly integrates the SSI framework. This remarkable milestone not only tackles longstanding hurdles but also opens a gateway to a future where individuals have greater command 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

Background

Chapter 3

Identity

Chapter 4

SSI

Chapter 5

Cryptography

Chapter 6

Cybersecurity

Chapter 7

Framework

Chapter 8

Integration

Chapter 9

Conclusions

citazionepernonavereerroreGalilei [1612]

Bibliography

G. Galilei. *Nuovi studii sugli astri medicei.* Manuzio, 1612.