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

Dopo aver spiegato nel Capitolo [1] gli obiettivi ed il lavoro prodotto per raggiungerli, il resto della tesi è definito nel seguente modo:

- Nella prima parte del Capitolo [2] si introduce il problema della Network Security Automation e si descrive il framework di Verefoo, ponendo particolare attenzione sul suo funzionamento ad alto e basso livello. Nella seconda parte sono descritte le definizioni delle Proprietà di sicurezza da passare come input al framework, con una spiegazione dettagliata di come queste intervengono nella definizione della topologia finale che verrà fornita come output dal framewrok.
  Infine verranno introdotti i grafi che verefoo richiede ed utilizza nella computazione dei vari *NSF*.

- Il Capitolo [3] definisce l'architettura di docker, specificando la differenza tra usare docker per la virtualizzazione e delle semplici macchine virtuali. Successivamente viene fatto un approfondimento sul docker-compose, un tool in grado di poter istanziare più container velocemente tramite script. Nella parte finale viene spiegato come effettuare il networking sui container instanziati, come definirlo tramite docker-compose e come testare le comunicazioni in modo efficiente.

- Il Capitolo [4] descrive gli obiettivi posti all'inizio di questo lavoro di tesi. Più specificatamente, per ogni obiettivo presente verranno specificate le modalità e le scelte effettuate per portarlo a termine con una descrizione accurata dei vari passi che sono stati svolti prima della soluzione definitiva. Inoltre viene descritto in maniera più profonda rispetto a questo indice la descrizione dei futuri capitoli.

- Il Capitolo [5] descrive i lavori svolti nella prima delle due demo di cui questa tesi tratterà. Inizialmente viene descritto tramite pezzi di codice lo sviluppo

dell'installer prodotto affinchè un qualsiasi utente possa utilizzare la demo in maniera pratica ed agile. Nei paragrafi successivi vengono evidenziati i punti critici incontrati, elencando le modifiche apportate affinchè essa possa funzionare correttamente. Nell'ultimo paragrafo infine verranno specificati ulteriori upgrade che si possono inserire nella demo per mettere in mostra in maniera ancora più evidente il lavoro svolto da Verefoo.

- Il Capitolo [6] descrive i lavori svolti ed implementati su Verefoo. In questo capitolo viene descritto il processo di merge fra le versioni precedentemente esistenti di Verefoo. Successivamente verrà quindi spiegato, anche tramite frammenti di codice, gli step che il framework eseguirà per produrre in output una rete che soddisfi contemporaneamente tutti i requisiti di sicurezza passati come input. Infine si evidenziano anche le difficoltà che sono emerse lavorando al framework, e verranno proposte alcune soluzioni per poter evitare simili problematiche in futuro.
- Il Capitolo [7] descrive lo sviluppo della seconda Demo. In un primo momento viene mostrata la topologia di rete scelta da virtualizzare, con la finalità di indicare le nuove funzionalità di verefoo sviluppate al completamento del secondo obiettivo della tesi. Successivamente vengono descritti tutti i passi svolti per implementare la demo, con un commento per il codice che è stato utilizzato. Infine si evidenziano anche i limiti della demo prodotta con alcuni futuri aggiornamenti possibili.
- Il Capitolo [8] elenca i lavori futuri da svolgere all'interno del framework, la necessità di poter implementare soluzioni alternative a quella proposta in questo documento, e i limiti che devono essere superati affinchè il framework possa essere utile in un ambiente reale e non solo di testing virtualizzato. Infine vengono descritte le conclusioni del lavoro, con un riassunto generale di tutto ciò che è stato prodotto.

Chapter 2

Introduzione generale

2.1 Principi generali

Il problema della determinazione della pressione barometrica dell'atmosfera di Giove non ha ricevuto finora una soluzione soddisfacente, per l'elementare motivo che il pianeta suddetto si trova ad una distanza tale che i mezzi attuali non consentono di eseguire una misura diretta. La Application Programming Interface (API) è un componente essenziale per lo sviluppo del software. Greatest Common Divisor Conoscendo però con grande precisione le orbite dei satelliti principali di Giove, e segnatamente le orbite dei satelliti medicei, è possibile eseguire delle misure indirette, che fanno ricorso alla nota formula Galilei [1612]:

$$\Phi = K \frac{\Xi^2 + \Psi_{\max}}{1 + \mathrm{j}\,\Omega} \ . \tag{2.1}$$

In (2.1) le varie grandezze hanno i seguenti significati:

1. Φ angolo di rivoluzione del satellite in radianti se $K = 1$, in gradi se $K = 180/\pi$;
2. Ξ eccentricità dell'orbita del satellite; questa è una grandezza priva di dimensioni;
3. $\Psi_{\max}$ rapporto fra il semiasse maggiore ed il semiasse minore dell'orbita del satellite, nelle condizioni di massima eccentricità;
4. Ω velocità istantanea di rotazione;

Le grandezze in gioco sono evidenziate nella Figura 2.1.

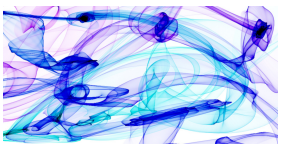

Figure 2.1. Come includere una figura, salvata nella cartella immagini.

Chapter 3

Il barometro

3.1 Generalità

In questa sezione proviamo a modificare l'INTERLINEA.

Il barometro, come dice il nome, serve per misurare la pesantezza; più precisamente la pesantezza dell'aria riferita all'unità di superficie.

Studiando il fenomeno fisico si può concludere che in un dato punto grava il peso della colonna d'aria che lo sovrasta, e che tale colonna è tanto più grave quanto maggiore è la superficie della sua base; il rapporto fra il peso e la base della colonna si chiama pressione e si misura in once toscane al cubito quadrato, Torricelli [1606]; nel Ducato di Savoia la misura in once al piede quadrato è quasi uguale, perché colà usano un piede molto grande, che è simile al nostro cubito.

3.1.1 Forma del barometro

Il barometro consta di un tubo di vetro chiuso ad una estremità e ripieno di mercurio, capovolto su di un vaso anch'esso ripieno di mercurio; mediante un'asta graduata si può misurare la distanza fra il menisco del mercurio dentro il tubo e la superficie del mercurio dentro il vaso; tale distanza è normalmente di 10 pollici

toscani, Torricelli [1606], Torricelli and Vasari [1607], ma la misura può variare se si usano dei pollici diversi; è noto infatti che gl'huomini sogliono avere mani di diverse grandezze, talché anche li pollici non sono egualmente lunghi.

3.2 Del mercurio

Il mercurio è un a sostanza che si presenta come un liquido, ma ha il colore del metallo. Esso è pesantissimo, tanto che un bicchiere, che se fosse pieno d'acqua, sarebbe assai leggiero, quando invece fosse ripieno di mercurio, sarebbe tanto pesante che con entrambe le mani esso necessiterebbe di essere levato in suso.

Il Monte Amiata, che è locato nel territorio del Ducato[26] del nostro Eccellentissimo et Illustrissimo Signore Granduca di Toscana[27], è uno dei luoghi della terra dove può rinvenirsi in gran copia un sale rosso, che nomasi *cinabro*, dal quale con artifizi alchemici, si estrae il mercurio nella forma e nella consistenza che occorre per la costruzione del barometro terrestre[*].

La densità del mercurio è molto alta e varia con la temperatura come può desumersi dalla tabella 3.1.

Colonna 1	Colonna 2	Colonna 3	Colonna 4
	10	100	13,8
2	20		13,6
	30	300	13,5
4	40		13,3

Table 3.1. Descrizione completa: didascalia della tabella.

Observation 1 This is the English version of *Osservazione*.

Per nostra fortuna, questo grande freddo, che necessita per la confetione de li sorbetti, molto raramente, se non mai, viene a formarsi nelle terre del Granduca Eccellentissimo, sicché non vi ha tema che il barometro di mercurio possa essere ruinato dal grande gelo e non indichi la pressione giusta, come invece deve sempre fare uno strumento di misura, quale è quello che è descritto costì J.T. [1964].

[26] Naturalmente stiamo parlando del Granducato di Toscana.

[27] Cosimo IV de' Medici.

[*] Nota senza numero...
...e che va a capo.

Temperatura °C	Densità t/m^3
0	13.8
10	13.6
50	13.5
100	13.3

Table 3.2. Densità del mercurio. Si può fare molto meglio usando il pacchetto booktabs.

Chapter 4

Primo capitolo della seconda parte

4.1 How to

Il testo di questo capitolo di trova in un file .tex separato!, nella cartella Part_II

Lorem ipsum dolor sit amet, consectetuer adipiscing elit. Ut purus elit, vestibulum ut, placerat ac, adipiscing vitae, felis. Curabitur dictum gravida mauris. Nam arcu libero, nonummy eget, consectetuer id, vulputate a, magna. Donec vehicula augue eu neque. Pellentesque habitant morbi tristique senectus et netus et malesuada fames ac turpis egestas. Mauris ut leo. Cras viverra metus rhoncus sem. Nulla et lectus vestibulum urna fringilla ultrices. Phasellus eu tellus sit amet tortor gravida placerat. Integer sapien est, iaculis in, pretium quis, viverra ac, nunc. Praesent eget sem vel leo ultrices bibendum. Aenean faucibus. Morbi dolor nulla, malesuada eu, pulvinar at, mollis ac, nulla. Curabitur auctor semper nulla. Donec varius orci eget risus. Duis nibh mi, congue eu, accumsan eleifend, sagittis quis, diam. Duis eget orci sit amet orci dignissim rutrum.

Bibliography

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

Duane J.T. Learning curve approach to reliability monitoring. *IEEE Transactions on Aerospace*, 2:563–566, 1964.

E. Torricelli. *La pressione barometrica*. Il Porcellino, 1606.

E. Torricelli and A. Vasari. Delle misure. *Atti Nuovo Cimento*, III(2):27–31, 1607.