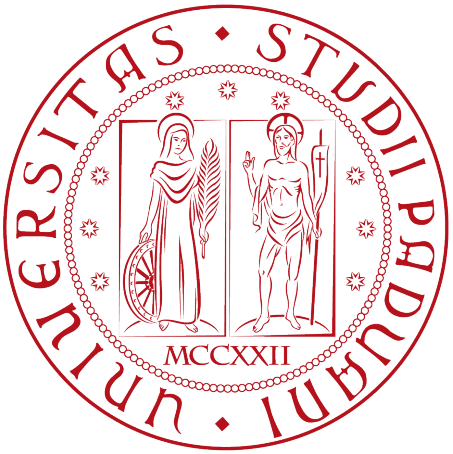
University of Padua

Department of Mathematics "Tullio Levi-Civita"

Bachelor's Degree in Computer Science



Owning your data through Self-Sovereign Identity: agents implementation for Verifiable Credentials interaction

Bachelor thesis

Supervisor
Prof. Alessandro Brighente

Co-Supervisors
Prof. Mauro Conti
Dott. Mattia Zago

Graduating
Matteo Casonato

Academic Year 2021-2022

Abstract

Nowadays, most of our data is owned by private companies, and everyone knows everything about us because privacy online is not well preserved. Imagining a world different from this is difficult, but things can change thanks to Self-Sovereign Identity (SSI).
SSI's approach aims to bring credentials back to the actual owners, the people. This is possible through cryptography and secure authentication layers (e.g., OAuth, OpenID-Connect).
The developed product embraces this philosophy and offers a solution where the users are the holders, issuers, or verifiers of VCs (Verifiable Credentials). Specifically, will be developed software agents who create, issue, verify, modify or even revoke the credentials, leveraging an SSI Kit.

This paper describes in detail Matteo Casonato's (approx.) three hundred hours of internship at the company Athesys S.r.l. (actually, working for its sub-startup Monokee). The goal was to merge SSI off-chain (i.e., outside the blockchain) operations with on-chain smart contracts.
In particular, the job has been divided into three macro stages:

1. Deep dive into the SSI technology, studying all of its primitives and problem analyzation;

2. Development of a Software Development Kit (SDK), which enabled us to dialog with an SSI Kit (off-chain logic); in the meantime, my friend and co-worker Matteo Midena developed the smart contracts (on-chain logic);

3. Merge off-chain and on-chain solutions in a proof of concept web application.

"If you always do what you've always done,
you'll always get what you've always got."

— Henry Ford

Acknowledgments

First of all, I would like to thank the people who helped me during the writing of this paper: my supervisor Dott. Alessandro Brighente and my co-supervisors Prof. Mauro Conti and Dott. Mattia Zago.

Also, I want to thank my parents, who have always supported me, and never stopped me from doing anything I truly wanted.

Finally, I thank my friends, who have eased these sometimes intense but very satisfying years.

Padova, September 2022 Matteo Casonato

Contents

List of Figures

List of Tables

Chapter 1

Introduction

This chapter will introduce the problem: what we are analyzing, why this problem exists, how it is defined, and how it can be resolved. Also will be introduced the company, the internship, and the work methodology.

1.1 The problem

As stated in the abstract, the main problem is preserving the ownership of people's data. In order to achieve this objective, we will pass through problems like interoperability, privacy safeguarding, law compliance, security, and others.

Assuming we can create a system where people hold their credentials (called Verifiable Credentials, or VCs):

1. How can these credentials be shown to and verified in the same manner by different actors?
2. Can we demonstrate something without revealing it, preserving our privacy this way?
3. Is it possible to save on blockchain people's data, or are we going against specific privacy laws?
4. Are credentials susceptible to attacks from hackers trying to steal our data?

Thanks to Self-Sovereign Identity, we can give a positive answer to all of these questions, but as is often the case, we have to deal with compromises.

Worldwide scenario The current situation is clear. Every time we interact with a new website, we may want to interact with it, and to do so, we have to register to create a profile. In this phase, we have to give our data to the company, and they will be stored in their databases.

Problem identification Let us now try to answer the previous questions to check how the present context is managed:

1. **Interoperability** | We could have two cases. In the first one, we use a technology that enables us to use our existing account on multiple websites, which integrates this solution, for example, "Sign-Up with Google". Here our data is owned by Google, which shares them (if we grant permission) with third parties, and no

one prohibits third parties from keeping our shared data saved. In the second case, we must register each time if the third party does not integrate other "Sign-Up with *" solutions. In both cases, third parties can collect our data (in the first case, Google explicitly knows our interests, but there is a minimum degree of interoperability). Also, in most cases, companies will let us create multiple accounts without verifying our data (one exception to this is the use of KYC).

2. **Privacy** | In some cases, we must show our data with complete transparency: for example, the police stop us on the street and ask for our details. Nevertheless, let us suppose we want to demonstrate something without revealing the details. For example, someone has graduated and wants to demonstrate it without revealing his final grade. We can do this thanks to a cryptography method called *Zero-Knowledge Proof*. However, this has not yet been implemented in most current systems.

3. **Law compliance** | If we consider saving users' data in blockchains, this problem does not exist as we examine centralized systems which do not use them. By the way, of course, there are privacy laws companies must follow (like GDPR).

4. **Security** | Our information is stored in databases. With a data breach, considering a centralized system, a malicious actor can access all users' data at once. Sadly, this happens often. So often that someone has made a website where anyone can check if his data has been stolen online at least once (Have I Been Pwned?).

Problem statement With the above considerations, it is clear that the existing systems work but could be significantly improved. In fact, interoperability enhancement would mean privacy and security penalization. Compromises exist, but if the system is well designed, they can be significantly reduced or at least moved to less dangerous areas. Here, the need for a more secure way to store user data arises. A way that intersects the analyzed points, bringing new power to people and reducing that of companies. This is the Self-Sovereign Identity's principle, which the developed solution will leverage.

Approaches SSI's concept is pretty simple, as opposed to its (in development) implementation. Everyone has different relationships or unique sets of identifying information. This information could include birth date, citizenship, university degrees, or business licenses. In the physical world, these are represented as cards and certificates that the identity holder holds in their wallet or a safe place like a safety deposit box. They are presented when the person needs to prove their identity or something about it.
Self-sovereign identity (SSI) brings the same freedom and personal autonomy to the internet in a safe and trustworthy identity management system. SSI means the individual (or organization) manages the elements that make up their identity, and he digitally controls access to those credentials, called Verifiable Credentials (or VCs). They are digital representations of information that can be verified by a third party.

This is achievable by involving three participants:

1. **Holder** | The holder is an individual in the scenario, although it can also be an organization/company. The holder is the entity that holds the credential.

2. **Issuer** | The issuer is the institution, be it a company, certifier body, or governmental organization, that has been awarded a level of trust to provide information (i.e., a public body that issued a passport)

3. **Verifier** | The verifier is the individual, organization, company, or government with whom the holder must prove information's legitimacy and trustworthiness.

The Verifiable Data Registry grants the trust: here are stored schemas and identifiers (linked to the credentials) that the verifiers use to check data validity without the issuer's intervention.

To make a preliminary check of this solution's viability, let us try to answer the previous four questions, considering the new scenario:

1. **Interoperability** |

2. **Privacy** |

3. **Law compliance** |

4. **Security** |

Check delle 4 domande –> sono ok –> 10 principi

1.2 Basic use cases

1.3 Company, internship, work methodology

Chapter 2

State of the art and technology background

2.1 Problem's preliminary analysis

2.2 Technology concepts

2.3 State of the art

Chapter 3

Solution

3.1 Solution proposal

3.2 Solution development

3.2.1 Technologies and Tools

3.2.2 SSI Kit SDK development

3.2.3 Smart Contract integrations - Web App Proof of Concept

3.3 Discussion

3.3.1 Achievements

3.3.2 Acquired knowledge

3.3.3 Future developments

3.3.4 Personal evaluation

Conclusion

Bibliography

Bibliographical references

James P. Womack, Daniel T. Jones. *Lean Thinking, Second Editon*. Simon & Schuster, Inc., 2010.

Websites consulted

Manifesto Agile. URL: http://agilemanifesto.org/iso/it/.