Kalpa Publications in Computing

Volume 14, 2023, Pages 118–120

Proceedings of V XoveTIC Conference. XoveTIC 2022

Testing and Analysis of Self-Sovereign Decentralized Digital Identity Technology

Pablo Santos-Cabaleiro[1*], Martiño Rivera-Dourado[123†], and José M. Vázquez-Naya[123 ‡]

[1] Facultade de Informática, Universidade da Coruña Elviña, 15071 A Coruña, Spain
[2] Grupo RNASA-IMEDIR, Departamento de Ciencias de la Computación y Tecnologías de la Información, Facultade de Informática, Universidade da Coruña Elviña, 15071 A Coruña, Spain
[3] Centro de Investigación CITIC, Universidade da Coruña Elviña, 15071 A Coruña, Spain

Abstract

The emergence of the Internet has generated new functionalities in our daily lives: data sharing, people communication or even the creation of a new "digital life" within the virtual world. Nowadays, each user visits many websites and web applications, in which the owner companies stores certain information from the user to be able to use the services offered. As a result, the user's digital identity is scattered in many websites databases. During the last few years, some solutions have been developed, proposing a new digital identity solution that is known as Self-Sovereign Identity. This solution allows the decentralization of the user personal data and the self-sovereign identity management using blockchain technology. This paper shows a proof of concept of a simplified self-sovereign identity system that allows the user to manage their personal data with different external and compatible web services.

1 Introduction

The rapid expansion of the Internet made people to create a new type of identity within the Internet. As they browse and exchange information on the Internet, the users forge what is called their digital identity. According to the model proposed by F.Georges [1], the digital identity is made up of three types of "sub-identities": "Declared Identity", "Acted Identity" and "Calculated or inferred Identity". Each term refers to the set of data on the Internet "that the user expressly reveals", "the acting data on the web" and "the calculated or inferred data" respectively [2]. The number of these digital identities has increased exponentially in recent years. The report published by DataReportal [3] states that the number of Internet users is approximately 4.95 billion, which represents 62.5% of the current world population.

[*] Developed the application

[†] Contributed to the development and revision of the project

[‡] Contributed to the development and revision of the project

A. Leitao and L. Ramos (eds.), XoveTIC2022 (Kalpa Publications in Computing, vol. 14), pp. 118–120

Currently, the user's digital identity does not belong exclusively to the user. The different websites and applications which the user visits store a large amount of information about the user digital identity in their internal databases. This fact means that all these companies that are behind each website have the responsibility to protect and guarantee the user's personal data security and privacy. In a hypothetical case where these websites owners were attacked and the user's data was stolen or leaked, the user's privacy would be violated without the user being able to avoid it.

In recent years, a new digital identity model to try to solve this problem has been developed, proposing a new digital identity management system: Self-Sovereign Identity (SSI). It consists of encrypted and digitally signed verified credentials with Decentralized Identifiers (DIDs) that represent bits of personal and identifying information in which the individual chooses which credentials to share and with whom [4]. This new digital identity system is a persistent, portable and interoperable solution that belongs only to the user, rather than to a third party such as a bank or government. Self-Sovereign Identity uses blockchain technology for data sharing. This technology uses a data structure made up of interconnected blocks through hash functions in which information is stored [5] with a lot of characteristics such as decentralization and data integrity, high availability, security and scalability [6].

This paper shows a proof of concept of an SSI management system. This proof of concept consists in a decentralized and self-manageable digital identity simplified prototype, in which the user can register, manage and share their personal data with other third-party compatible web systems that request it through consent and access requests.

2 Methodology

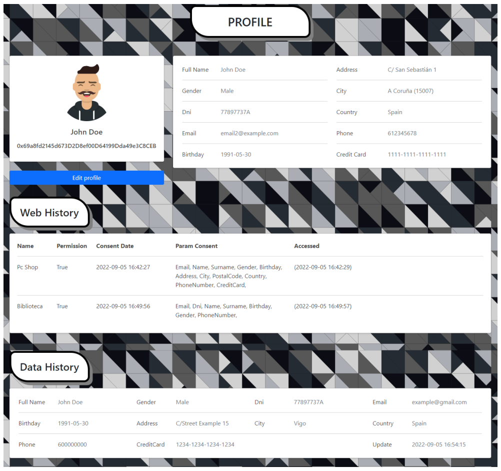
First, a research process has been done on blockchain technology, digital identity and decentralized digital identity in which its characteristics, elements and operation have been analyzed. Subsequently a high-level simplified proof of concept was implemented. For this proof of concept development, it has been chosen an agile methodology based on incremental and iterative development, starting with the implementation of basic structural concepts and functionalities and adding new improvements and functionalities in each interaction implemented.

3 Development

For this purpose, two main systems have been implemented: User Digital Identity Management System (UDIMS), the system in which the user can store his data in the blockchain and manage the data sharing with other web services; and External User Registration System (EURS), an external system available on the Internet, compatible with UDIMS that allows adding personal data of different users and managing access requests to it. To store this information, the user should connect the blockchain and provide his personal data to UDIMS. This system receives this data and stores it in a smart contract deployed in the user's blockchain. Therefore, when the user registers in one EURS, this system creates a request to consult user personal data from the blockchain. If the user approves it, the consent will be registered in the smart contract and the EURS will be able to access the data it has previously requested. EURS systems do not store the users personal data in their databases, instead of, they make data request to the blockchain when they need it.

4 Results

In this proof of concept, we use Ganache blockchain to deploy the smart contract and store the user personal data in it thought UDIMS. In order to provide a complete proof of concept of this system, two duplicated EURS that request different data from the user were implemented: *"Pc Shop"* and *"Library"*. After the user has registered his personal data, he signs up in each EURS providing the parameters to connect to the blockchain. Then, each EURS requests the necessary consent to access to the different attributes of user's personal data. When user accepts it, this consent is recorded in the blockchain and EURS can subsequently access the different requested personal data. In EURS profile view, the user can view the personal data he has approved in each case. At the same time, the user can check the EURS corresponding consents and access in his UDIMS's profile view (see figure 1).



John Doe

0x69a8fd2145d673D2D8ef00D64199Dda49e3C8CEB

Full Name	John Doe	Address	C/ San Sebastián 1
Gender	Male	City	A Coruña (15007)
Dni	77897737A	Country	Spain
Email	email2@example.com	Phone	612345678
Birthday	1991-05-30	Credit Card	1111-1111-1111-1111

Name	Permission	Consent Date	Param Consent	Accessed
Pc Shop	True	2022-09-05 16:42:27	Email, Name, Surname, Gender, Birthday, Address, City, PostalCode, Country, PhoneNumber, CreditCard,	(2022-09-05 16:42:29)
Biblioteca	True	2022-09-05 16:49:56	Email, Dni, Name, Surname, Birthday, Gender, PhoneNumber,	(2022-09-05 16:49:57)

Full Name	John Doe	Gender	Male	Dni	77897737A	Email	example@gmail.com
Birthday	1991-05-30	Address	C/Street Example 15	City	Vigo	Country	Spain
Phone	600000000	CreditCard	1234-1234-1234-1234			Update	2022-09-05 16:54:15

Figure 1: Profile view in UDIMS

Additionally, if the user updates any value of his personal data in UDIMS, his profile data in each EURS in which he had registered will be automatically updated too.The user can also check the update history of his personal data in the UDIMS profile view. All these functionalities made the developed system the complete SSI proof of concept.

References

[1] Fanny Georges. Représentation de soi et identité numérique. une approche sémiotique et quantitative de l'emprise culturelle du web 2.0. https://www.cairn.info/revue-reseaux-2009-2-page-165.htm, 2009.

[2] Fundacion Telefónica. *Identidad digital: el nuevo usuario en el mundo digital.* Ariel S.A, 2013.

[3] Simeon Kemp. Digital 2022: Global overview report. https://datareportal.com/reports/digital-2022-global-overview-report, 2022.

[4] Identity Management Institute. Self sovereign identity. https://identitymanagementinstitute.org/self-sovereign-identity, 2021.

[5] Adam Hayes. Blockchain, explained. https://www.investopedia.com/terms/b/blockchain.asp, 2022.

[6] Imran Bashir. *Mastering Blockchain.* Packt Publishing, 3 edition, 2020.