Self-Sovereign Identity in University Context

Araceli Queiruga-Dios, Juan José Bullón Pérez
Universidad de Salamanca
Salamanca, Spain
queirugadios, perbu@usal.es

Luis Hernández Encinas
Spanish National Research Council (CSIC)
Madrid, Spain
luis@iec.csic.es

***Abstract*—A user-centred identifier enables verifiable and decentralized digital identity, and lead users to control and to generate their own identifiers using systems they trust. This is how Self-Sovereign Identity works. This paper presents the case of universities, where several different agents need their own identifier and shows a digital identity mathematical model for the academic context. Moreover, the Alastria model for the same context is detailed for a specific case of students' mobility.**

I. Introduction

A digital identity is considered as a digital reference to a person [1]. It is the means for individuals to prove electronically that they are who they say they are and it make possible to distinguish different people or entities from one another. In the case of Self-sovereign identity (SSI) users own and manage their digital identity without a service provider, and which cannot be taken away from them. Essential characteristics of SSI are security of personal data, controllability and the "right to be forgotten", and portability that gives user the option to access it wherever they want, from all places and at every time [2]–[4].

The Regulation (EU) No 910/2014 of the European Parliament and of the Council of July 23, 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC (OJ L 257, 28.8.2014, pp. 73-114), defines the Decentralized Identifier (DID) of the SSI, as a new way of identify digital identity. The DID is under the control of the user, and it does not depend on any centralized registry, identity provider, or certificate authority. A DID document is a digital document that describes how to use that specific DID. Moreover, the DID document may contain at least proof purposes and verification methods (provide mechanisms for proving things such as authentication), and service endpoints (enable trusted interactions with the DID controller).

User-centred identity avoid external control and make users their own identity providers, and thus, there is no need of a external provider or trusted third party. Institutions, companies or social networks do no longer need to trust each other, they just need to trust the user [5]. It is more and more common to find users that don't want to reveal their private information when they access to network services. When doing this, an individual must be authorized to enter the network services after identity and corresponding keys identification, which are generated and managed by the network operator. However, this procedure makes users lose the control of their data. SSI provides users the control of their personal data and identifying information, and avoid access to their sensitive data by third persons [6].

Sometimes an individual changes his residence, he get a new certificate or attestation, or get the driven license for the first time, or changes the service provider. In the past, these issues usually indicated that the person must start again with the process of creating new identities. One of the advantages of SSI is that users can maintain their digital identities, which do not depend on their residence, their national eID infrastructure or their service providers [7].

Besides control the secure storage, access and control of personal information, with this identity system, users can add or delete their personally identifying information. This feature adds new functionalities to this systems and improve other traditional identity management schemes [6].

A secure identity management model is possible with the use of Distributed Ledger Technology (DLT). Blockchain distributed ledger technology has proven to allow trusted and auditable computing using a decentralized network of peers not controlled by anyone, which does not need that third entity that has to be trusted in current systems. Operations and transactions carried out on the blockchain platform are known as a ledger [8]–[10].

Blockchain technology includes hash functions, digital signatures, elliptic curves, and Merkle trees to ensure information integrity, verification and authentication [11].

Universities provide training in the form of short or long courses, degrees, Ph.D. courses, etc. that may range from a few hours to months or years, to "students" from diverse interests and backgrounds. Students could be young people arriving to higher education, or teachers from different educational levels, or employees or pensioners, or individuals that want to receive any kind of training. The emergence of technologies as mobile devices and smart phones increase the possibilities to access to studies from all over the world. Although the existing university services and processes are highly centralized relying mainly in the rector and vice-rectors, and the administrative statements, all people involved in university context need a digital identity [12].

This paper is organized as follows: Section II details the digital identity model for the university context. Section III is centred in Alastria model adapted to the higher education environment. Finally, some conclusions from this study are included.

II. European Self-Sovereign Identity Framework

The Electronic Identification and Trust Services (eIDAS) Regulation creates a new system for secure electronic interactions across the EU between businesses, citizens and public authorities. It aims to improve trust in EU-wide electronic transactions and to increase the effectiveness of public and private online services and e-commerce. It applies to electronic identification (eID) schemes notified to the European Commission by EU countries. It removes existing barriers to the use of eID in the EU. For instance, it would now be straightforward for a Portuguese firm to tender for a public service contract in Sweden, while EU funding grants can be managed wholly online.

In 2018, 27 EU Member States, Norway, and Liechtenstein signed a declaration creating the European Blockchain Partnership (EBP). This group assists the European Commission with the establishment of a European Blockchain Services Infrastructure (EBSI) that will support the delivery of cross-border digital public services, with the highest standards of security and privacy. The EBSI is designed as a market-friendly ecosystem based on open standards and a transparent governance model and is the first blockchain infrastructure in the entire EU to provide a secure system for governmental entities, which are able to act as intermediaries for many digital transactions.

In this way, EBSI supports the creation of cross-border services that help citizens and companies to manage identity, educational credentials and registration documents. To this end, since 2020, EBSI has been implementing a network of distributed nodes across Europe, supporting applications focused on seven selected use cases. These selected use cases are detailed in Table I. Moreover, there are currently four use cases: Self-Sovereign Identity, Diploma, Document Traceability and Trust Data Sharing.

The European Self-Sovereign Identity Framework (ESSIF) arose to achieve trusted identification and authentication in a decentralized network and to allow citizens to use their own digital identity without a centralised authority. This trusted authority is not needed anymore.

In Europe, the SSI framework makes possible digital interactions between citizens and official public entities, and between different public entities and/or private parties. ESSIF is aligned with the General Data Protection Regulation (GDPR) and the electronic IDentification, Authentication and trust Services (eIDAS). This legal frameworks provide citizens' secure European digital identity. Moreover, this framework is based in the EBSI.

Therefore and to avoid digital fraud, governments need technology capable of verifying the authenticity of the information they handle, with the goal of sever society. This has become a challenge that is essential to address. To build the European regulatory framework in the process of moving from paper to a digital environment, personal information must be shared in a trusted way.

The main objective of the EBSI-based European ESSIF is to identify natural persons and legal entities. The identification can be done with many types of documents such as attestations, diplomas, permissions (driving license, etc.), or other different relationships between entities. To makes this possible the following aspects must be considered:

1) To define the technological components and architecture of the ESSIF
2) To establish the ESSIF's trust and governance frameworks
3) To integrate the EU regulations
4) To define the core services and minimal functionalities for a full capability
5) To design the different process's paths

Fig. 1 shows the scheme of the ESSIF adapted to the university context, where the student is the natural person that has his own legal presentation. He creates his Decentralized Identifier (DID) and links it to the EBSI ledger. After this, he is able to collect and share data securely. The legal entity (university) has a legal presentation to other parties and delivers services. It can verify data to facilitate digital interactions with other parties. The legal entity, which is uniquely identifiable, is responsible for creating and securing DID and its associated keys. Moreover, the DID is registered on the EBSI Ledger. In this case, the student can obtain a verifiable ID or an attestation in order to identify and authenticate himself when requested by the university staff and faculty. Thus, at this point the student stores his verifiable ID in his user wallet.

The student can request verifiable attestation from his university. In fact, a student with a lot of verifiable credentials (VC) can provide a broader range of trustworthy data. Student's wallet is made of all his VC. On the other hand, the student authenticates to the university presenting the required VC.

III. Digital identity model for university context

The term identification comes from the underlying assumptions on centuries of experience in a paper-based world. The procedures and models of paper-based identifications fails when they wanted to move to a digital networked identities. An identification document such as a passport or a identity card include personal data like name, date and place of birth, etc. These systems link attributes that authenticate individuals as citizens with others that authenticate individuals identity (for instance, the name). Moreover, an off-line identification is possible through a biometric method (the photograph and fingerprint) [13].

On the other hand, a person and any entity can have several identifiers. A serial number, a certificate, a car number plate, the number of a building in a street, or a property registry number are some examples of identifiers. These identifiers are characterised by attributes, which include date of birthday, eye color, genetic pattern, address, location, country, passport or social security numbers, etc., and each attribute has its specific values. With the identifier and the corresponding attributes and attribute values, the entity's identification is established. When someone proofs that association, then the authentication is done. This is the case of the association of a person with her

TABLE I. SELECTED USE CASES IMPLEMENTED BY EBSI

European Self-Sovereign Identity	Implementing a Self-Sovereign Identity model in Europe, allowing users to create and control their own identity across borders
Diploma Management	Citizens gain digital control of their educational credentials, significantly reducing verification costs and improving trust in documents' authenticity
Document Traceability	Storing immutable reference data of documents or other digital artefacts that can be used at a later stage as proof of their authenticity/integrity and can be linked together to build a trusted, time-stamped audit trail
Trust Data Sharing	Securely share data (such as IOSS VAT identification numbers and import one-stop-shop) among customs and tax authorities in the EU
SME Financing	Opening new sources of (co)-finance political efforts in the area of sustainable economy, innovation and SMEs modernization via an EU-wide platform for debt financing
European Social Security Pass (ESSP)	Prevention of fraud or error by ensuring easier communication and data exchange between European countries and the EU Institutions
Asylum Process Management	Facilitation of the management of cross-border and cross-authority processes in dealing with asylum applicants

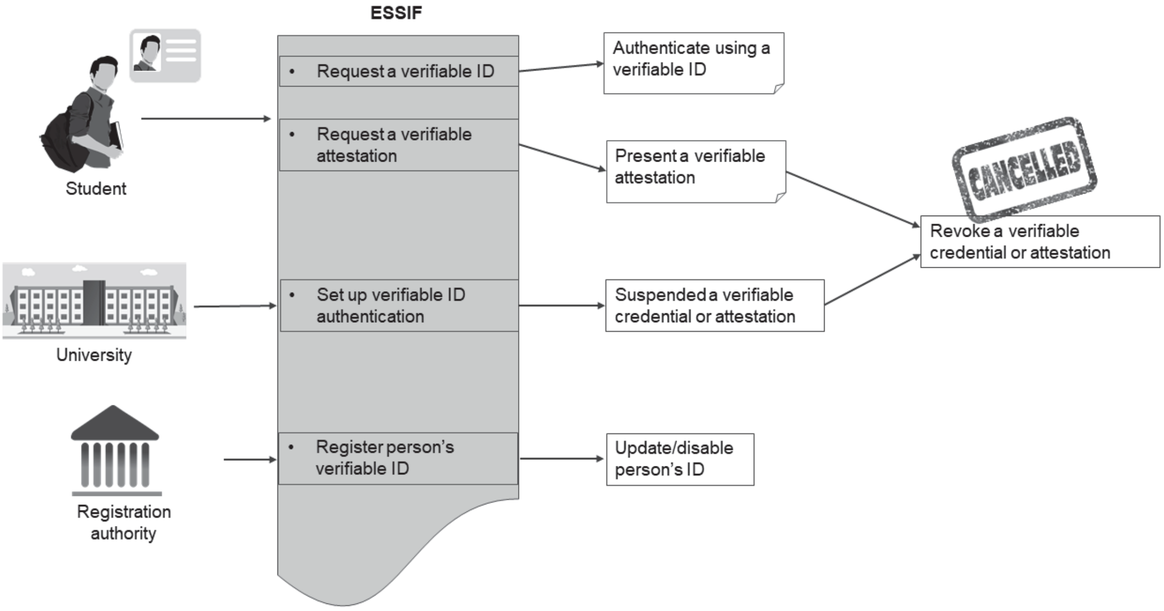
ESSIF
Student
University
Registration authority
• Request a verifiable ID
• Request a verifiable attestation
• Set up verifiable ID authentication
• Register person's verifiable ID
Authenticate using a verifiable ID
Present a verifiable attestation
Suspended a verifiable credential or attestation
Update/disable person's ID
Revoke a verifiable credential or attestation
CANCELLED

Fig. 1. Scheme of the European Self-Sovereign Identity Framework adapted to the university context

bank account, a student with her educational registry number, or the association of the car with its license plate. In the case of money, its presence is its authentication. When an attribute is not linked to an identifier, then it is an anonymous identity [13], [14].

In general, privacy is one characteristic of identification, so privacy protection must be integrated into a identity management system [14].

Based on the digital identity mathematical model defined by Ferdous, Norman, and Poet [15], E denotes the digital entity, which corresponds to a specific student, an academic or an administrative staff in the university context. A set of contexts, $\mathcal{C}$, and subsets of contexts could be considered, inside and outside university. University context could be considered as container of diverse sub-contexts such as email communication, academic record, payment management, etc. Thus, as an example, $email$ and $acad$ are considered, i.e.,

$$\mathcal{C} = \{email, acad\}.$$

Three entities (students) are considered for this case: S_1 (Alice), S_2 (Bob) and S_3 (Carmen), within contexts $email = \{Alice, Bob\}$ and $acad = \{Alice, Carmen\}$.

On the other hand, each attribute has a name an a value. Considering the attributes, A_c, and their values, AV_c, for a given context, $acad$, then:

$$A_{acad} = \{name, degree, course, faculty, subject, mark\}.$$
$$AV_{acad} = \{Alice, Carmen, mechanical, electrical,$$
$$2nd, 1st, engineering\ school,$$
$$chemistry, physics, 6.5, 8\}$$

For a given context, c, a partial function, f_c can be defined in such a way that it establishes the following correspondence: $f_c\colon A_c \times E_c \to AV_c$. Thus f_c associates an attribute value to each attribute and an entity. In the case of academic context, this would be:

$$f_{acad}(name, S_1) = Alice$$
$$f_{acad}(degree, S_3) = electrical$$
$$f_{acad}(faculty, S_3) = engineering\ school$$

f is defined as partial function because not all attributes and entities returns an attribute value in context $acad$.

In the same way, another function can be defined to return, for an attribute, all its possible values for a given context: $g_c\colon A_c \to \mathcal{P}(AV_c)$, i.e.,

$$g_c(a) = \{f_c(a,e) | e \in E_c \text{ and } f_c(a,e) \text{ is defined}\},$$

where $a \in A_c$.

For the case of the academic context this would be,

$$g_{acad}(subject) = \{chemistry, physics\}.$$

Another function, h_c is defined to associate the attribute and its value the corresponding set of entities in context c, i.e., $h_c\colon A_c \times AV_c \to \mathcal{P}(E_c)$. Thus, for $a \in A_c$ and $v \in AV_c$

$$h_c(a,v) = \{e \in E_c | f_c(a,e) = v\}.$$

For the example, this is

$$h_{acad}(faculty, engineering\ school) = \{S_1, S_3\}.$$

Function $ID\colon \mathcal{C} \to A_c$ is defined to get the identifier for all $c \in \mathcal{C}$. So, $f_c(i,e)$ is defined $\forall e \in E_c$, and $f_c(i,e_1) \neq f_c(i,e_2)$ $\forall e_1, e_2 \in E_c$, being $i = ID(c)$.

An attribute value is not unique. Several values could belong to different entities. This is the case, for example, of the name, faculty, degree, etc., which could be the same for several students. In this case, this is defined as a set of partial identifiers, and given by PI_c. It verifies that $PI_c \subseteq A_c$ and $pi \in PI_c \Leftrightarrow f_c(pi,e)$ is defined for some $e \in E_c$. When the attribute does not have a value for any entity it is called null identifier, and it verifies that $NI_c \subseteq A_c$ and $ni \in NI_c \Leftrightarrow f_c(ni,e)$ is undefined $\forall e \in E_c$.

These sets verifies that $A_c = \{ID(c)\} \cup PI_c \cup NI_c$ and they are disjoint sets. In the example of the university context, there is no null identifier because all of them are partial ones, e.g., $ID(acad) = name$, $ID(acad) = degree$, etc.

A new injective function, $p_c\colon AV_c \to E_c$ is defined to map a value of an identifier to its respective entity, for a context, c. In this case, $p(v) = e$, where $v \in AV_c$ is the corresponding value for $ID(c) \in A_c$ and $e \in E_c$, i.e., $f_c(ID(c),e) = v$. For the context in the example:

$$p_{acad}(Alice) = S_1.$$
$$p_{acad}(Carmen) = S_3.$$

For the authentication process, an attribute associated to an identifier is called credential. Secure credentials are secure tokens such as a password, a certificate, voice recognition, retina scan, etc. A binary function that checks entity's identifiers and credentials is defined as follows:

$$IC_c\colon (ID(c) \times AV_c) \times (cred_c \times AV_c) \to \{0,1\},$$

which returns 1 (true) if the identifier and credential matches, and 0 (false) in other cases. In this case, $cred_c$ is the attribute corresponding to the credential for an entity in context c.

The authentication of an individual (entity) in a context $c \in \mathcal{C}$, considering its identifier and all possible attribute's values, is represented by a binary function, $AId\colon E_c \times \mathcal{C} \times \mathcal{P}AV_c \times \mathcal{P}(cred_c) \times A_c \to \mathbb{B}$, with input parameters $e \in E_c$, $i = ID(c)$, $v_j \in \mathcal{P}(i)$, $v_k \in \mathcal{P}(cred_c)$ and $cred_c$. When $e = p_c(v_j)$ and $IC((i,v_j),(cred_c,v_k)) = 1$ then the function AId returns 1 (true), and 0 (false) otherwise.

To summarize, a digital identity model for a given context, $c \in \mathcal{C}$, is made of the following components that were detailed above:

1) The set of entities, E_c.
2) The set of attributes, A_c and their values, AV_c.
3) A function, $ID\colon \mathcal{C} \to A_c$, that maps a context to its identifier.
4) The credential, $cred_c \in A_c$, of each entity.
5) A function, $f_c\colon A_c \times E_c \to AV_c$, that allows to get, for an entity, the value of an attribute.
6) A binary function, $IC_c\colon (ID(c) \times AV_c) \times (cred_c \times AV_c) \to \{0,1\}$, that check the correspondence between an identifier and a credential with their values.

IV. Self-Sovereign Identity model

A Decentralized Identifier (DID) is a unique identifier that enables verifiable and decentralized digital identity, and enable users to control and to generate their own identifiers using systems they trust. Thus, DID allows data sovereignty and it is the central part of self-sovereign identity [16]. Moreover, the unique identifier is defined at a global level, it is cryptographically verifiable, and can work on any blockchain. A DID is linked to a DID document, which contains the owner public key [17]. Fig. 2 shows an example of a DID system that will be detailed throughout this section [18].

Several initiatives have been addressed to provide a decentralized identity model, such as ID2020 [19], Uport [20], Sovrin Foundation [21], or bonifii [22] that allows to develop SSI-based projects [23].

The Red Alastria Consortium (hereinafter, ALASTRIA) is a Spanish non-profit association whose main objective is to create a community made up of all kinds of public and private organizations, as well as individual experts, to promote the implementation, standardization, protection and

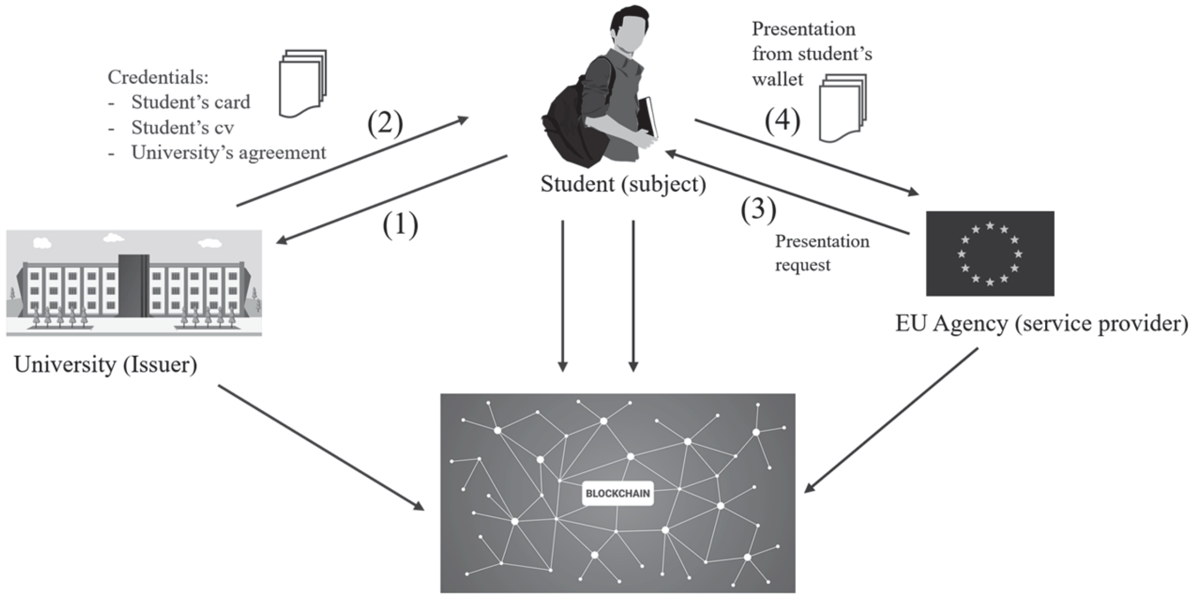

Fig. 2. (1) The student asks for credentials to her university; (2) the university provides her with the required credentials; (3) the EU agency request for proofs of those credentials; and (4) the student proofs her credentials

use of technologies such as Distributed Ledger Technologies (DLT), promoting knowledge and use by Spanish society of this technology, promoting its use among administrations, companies and other social agents.

ALASTRIA has developed the infrastructure called Red T (the "Network" or the Alastria Partner Network) so that its partners and associated entities can carry out concept/product/activity tests on it.

The "T Network" is a public network, according to the ITU classification accessible to any user with a computer and a Internet connection. The Regular Nodes that participate in it must be accepted by the Permitting Nodes, but the default transactions are public. That means that the Critical Nodes participate in the maintenance and security of the Network and that all transactions, unless they decide to use Private Transaction features, they are visible to the various Nodes.

In the T Network there are basically three types of nodes, defined according to their function in the network (detailed in Table II).

The software required for all the nodes, their installation and connection to the T Network of Alastria's partners is described in the GitHub tools that have been created in the ALASTRIA public software repository.

The proposal for digital identity in Blockchain aims to provide an infrastructure and development framework, to carry out sovereign digital identity projects, with full legal validity in the euro zone, following these premises:

- Enable a framework for make use of SSI using Blockchain, with SSI eIDAS Legal Report, also called "eIDAS Bridge"
- Follow the guidelines of the e-Identity Workshop Report, of the EU Blockchain Observatory and Forum
- Compliance with eIDAS Regulation, according to Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC
- Make the Digital Identity in Blockchain and the GRPD two complementary tools, following the recommendations described in EU Blockchain Observatory and Forum

Self-sovereign identity enables users full control over their data, and they have the power to decide who can access it and on what terms. The SSI model developed by Alastria [24] includes a credential issuer (Issuer), which sends the credential to an entity or person (Holder), who could use it for a given service (Verifier). The Verifier should check the authenticity of credentials. An intermediary (verifiable data registry) would be in charge of supporting the verification of these credentials, revocations, public keys, etc. [8].

In what follows the Alastria model for the university context will be detailed. This model distinguish 3 entities [24]:

- Issuer is enable to create an Identity and provide data to users (DID documents).
- Service provider or verifier asks for user's credentials.
- Subject is the final user, in this case a student who wants to apply for an Erasmus grant. Subjects are owners of their identities.

When a Issuer creates a credential, the subject can accept or deny it. Furthermore, users may register to various credential

TABLE II. TYPES OF NODES IN T
NETWORK

Validator (block-maker)	The validator nodes execute the consensus algorithm, which in the case of this Red T is the IBFT
Permissioner (Bootnode)	They are nodes whose physical addresses ("enodes") are perfectly known throughout the network. The network nodes only know the bootnodes they have in their permission file. Through a bootnode, nodes on the network cannot learn about other nodes
Regular (general)	A node that participates by replicating the blockchain, accepting the blocks generated by the validators and executing the transactions included in them. You are also allowed to inject transactions into the network, from sources outside the blockchain

providers [25].

Fig. 2 represents the example related to the university context, where there is no flow between the Issuer and the service provider [18].

An example of these data flow is a student claiming to attend to Universidad de Salamanca (1) and the university issuing attest this claim (2). This is mandatory to travel with a Erasmus grant to another EU university, so, the EU agency will ask the student about this requirement (3) and the student in this example sends this information to the EU agency (4). The agency does not communicate with the university [18].

V. CONCLUSION

University context has been widely studied from different security perspectives. Students, faculty, administrative staff, an some other agents are part of this educational area. The use of a self-sovereign identity enable individuals full control over their data, and the possibility of deciding who can access it and on what conditions.

The digital identity mathematical model included in this paper establishes a relation between contexts, entities, attributes and its values. The identifier was defined as a function that maps a context, such as the university one, to its identifier.

Finally, from the different proposals of decentralized identity, this paper propose the use of Alastria model for the university context.

ACKNOWLEDGMENT

This work was partially supported by Fundación Samuel Solórzano under grant no. FS/26-2020, and by the Spanish State Research Agency (AEI) of the Ministry of Science and Innovation (MICINN), project P2QProMeTe (PID2020-112586RB-I00/AEI/ 10.13039/501100011033), co-funded by the European Regional Development Fund (ERDF, EU).

REFERENCES

[1] J. Sedlmeir, R. Smethurst, A. Rieger, and G. Fridgen, "Digital identities and verifiable credentials," *Business & Information Systems Engineering*, vol. 63, no. 5, pp. 603–613, 2021.

[2] A. Mühle, A. Grüner, T. Gayvoronskaya, and C. Meinel, "A survey on essential components of a self-sovereign identity," *Computer Science Review*, vol. 30, pp. 80–86, 2018.

[3] A. Tobin and D. Reed, "The inevitable rise of self-sovereign identity," *The Sovrin Foundation*, vol. 29, no. 2016, 2016.

[4] Š. Čučko and M. Turkanović, "Decentralized and self-sovereign identity: Systematic mapping study," *IEEE Access*, vol. 9, pp. 139 009–139 027, 2021.

[5] Q. Stokkink and J. Pouwelse, "Deployment of a blockchain-based self-sovereign identity," in *2018 IEEE international conference on Internet of Things (iThings) and IEEE green computing and communications (GreenCom) and IEEE cyber, physical and social computing (CPSCom) and IEEE smart data (SmartData)*. IEEE, 2018, pp. 1336–1342.

[6] J. Xu, K. Xue, H. Tian, J. Hong, D. S. Wei, and P. Hong, "An identity management and authentication scheme based on redactable blockchain for mobile networks," *IEEE Transactions on Vehicular Technology*, vol. 69, no. 6, pp. 6688–6698, 2020.

[7] U. Der, S. Jähnichen, and J. Sürmeli, "Self-sovereign identity – opportunities and challenges for the digital revolution," *arXiv preprint arXiv:1712.01767*, 2017.

[8] R. García Álvarez, "Análisis de smart contracts en ethereum e identidad soberana," Ph.D. dissertation, ETSI_Informatica, 2020.

[9] S. Nakamoto, "Bitcoin: A peer-to-peer electronic cash system," 2008.

[10] G. Zyskind, O. Nathan *et al.*, "Decentralizing privacy: Using blockchain to protect personal data," in *2015 IEEE Security and Privacy Workshops*. IEEE, 2015, pp. 180–184.

[11] V. Gayoso Martínez, L. Hernández-Álvarez, and L. Hernández Encinas, "Analysis of the cryptographic tools for blockchain and bitcoin," *Mathematics*, vol. 8, no. 1, p. 131, 2020.

[12] S. K. Gebresilassie, J. Rafferty, P. Morrow, L. L. Chen, M. Abu-Tair, and Z. Cui, "Distributed, secure, self-sovereign identity for iot devices," in *2020 IEEE 6th World Forum on Internet of Things (WF-IoT)*. IEEE, 2020, pp. 1–6.

[13] J. Camp, "Digital identity," *IEEE Technology and society Magazine*, vol. 23, no. 3, pp. 34–41, 2004.

[14] U. Glässer and M. Vajihollahi, "Identity management architecture," in *Security Informatics*. Springer, 2010, pp. 97–116.

[15] M. S. Ferdous, G. Norman, and R. Poet, "Mathematical modelling of identity, identity management and other related topics," in *Proceedings of the 7th International Conference on Security of Information and Networks*, 2014, pp. 9–16.

[16] M.-H. Rhie, K.-H. Kim, D. Hwang, and K.-H. Kim, "Vulnerability analysis of did document's updating process in the decentralized identifier systems," in *2021 International Conference on Information Networking (ICOIN)*. IEEE, 2021, pp. 517–520.

[17] D. Reed, M. Sporny, D. Longley, C. Allen, R. Grant, and M. Sabadello, "Decentralized identifiers (DIDs) v1. 0 core data model and syntaxes," *W3C First Public Working Draft, https://www.w3.org/TR/did-core/*, 2019.

[18] Q. Stokkink, G. Ishmaev, D. Epema, and J. Pouwelse, "A truly self-sovereign identity system," in *2021 IEEE 46th Conference on Local Computer Networks (LCN)*. IEEE, 2021, pp. 1–8.

[19] "Digital id, ID2020," *https://id2020.org/*, 2020.

[20] "Uport," *https://www.uport.me/*, 2020.

[21] "Sovrin foundation," *https://sovrin.org/*, 2020.

[22] "bonifii," *https://bonifii.com/*, 2020.

[23] O. Avellaneda, A. Bachmann, A. Barbir, J. Brenan, P. Dingle, K. H. Duffy, E. Maler, D. Reed, and M. Sporny, "Decentralized identity: Where did it come from and where is it going?" *IEEE Communications Standards Magazine*, vol. 3, no. 4, pp. 10–13, 2019.

[24] "Alastria," *https://alastria.io/en/*, 2020.

[25] M. Kubach, C. H. Schunck, R. Sellung, and H. Roßnagel, "Self-sovereign and decentralized identity as the future of identity management?" *Open Identity Summit 2020*, 2020.