Rev. Roum. Sci. Techn.– Électrotechn. et Énerg.
Vol. **69**, *1*, pp. 85–90, Bucarest, 2024

A PROPOSAL OF DIGITAL IDENTITY MANAGEMENT USING BLOCKCHAIN

RALUCA VERONICA BRĂCĂCESCU[1], ŞTEFAN MOCANU[1], ANCA DANIELA IONIŢĂ[1], CARMEN BRĂCĂCESCU[2]

Keywords: Self-sovereign identity; Digital identity management; Blockchain; Verifiable credentials.

Digital identity is the representation of a person in the digital environment. Nowadays, digital identity has become a very important topic when most activities are moved to the online world. To be secured and respect data privacy, this digital identity must be controlled by its owner, not any other third parties. This paper aims to propose a system for digital identity, presenting its architecture, features, and implementation specifications. This system brings advantages that will also be exposed along with real-life use case scenarios, all proving the necessity of transitioning to a modern identity management model like the Self-Sovereign Identity model. The Self-sovereign identity model is based on blockchain and is fundamental for the digital identity system conceived through research.

1. INTRODUCTION

During the past few years, identity management has become one of the most popular concerns of the information technology field, especially in the **post-pandemic** world. More and more services were transitioned to online and are now remaining online. Digitalization represents the top priority for most states and private companies that want to modernize and simplify processes and align with the citizens' or customers' needs.

Any person must be able to prove his/her identity at any time. Over 1 billion people in the world do not have any legal identity card, not even a physical identity document, passport, or driving license. However, those with identity cards cannot use them in the digital environment, so a digital identification document (ID) is needed [1].

Of the existing identity management models, the Self-Sovereign Identity (SSI) model is the newest with a user-oriented approach. It has gained popularity over the past few years, becoming crucial in digital identity today. The SSI model is decentralized and wants to give full control of the digital identity to its owner (the user). SSI introduces selective disclosure of the identity characteristics and uses the zero-knowledge proof protocol (ZKPP) [2]. It is based on blockchain technology, which makes it trustful and secure.

Identity theft is among the most widespread crimes on the Internet, a real threat, leading to significant fraud and financial losses. In 2018, one revealed the Cambridge Analytica and Facebook case, where 87 million users' data were shared without consent and used for political purposes [3]. It is imperative to ensure personal data's protection, security, and confidentiality at the highest level. In centralized identity management systems, there is always a third party involved, an identity provider or a service provider that manages users' identities, such as Google, or Facebook. Because of this, unpleasant situations can occur, and users' data can be in danger [4].

One of the main objectives of the Self-Sovereign Identity model is minimizing the data shared with other entities, sharing just the needed information for a specific situation [5]. For example, if a young person wants to benefit from a discount for being under 25 years old to enter a museum, as it is now, one must present a national ID or passport and hand it to the person in charge of verifying the age. This way, the verifier has access to all data from the document, name, unique identification number, address, and data irrelevant to the given scope and should remain private. Instead, the only thing to be revealed must be the age condition, whether it is satisfied or not, not even the birth date.

This paper aims to present a system developed and implemented with programming tools for digital identity management using Blockchain technology based on the modern SSI model. Section 2 provides related work done in digital identity management, especially regarding SSI, the current context, and trends. It also presents some existing projects along with their purpose and main functionalities. Section 3 describes SSI from a more theoretical point of view and outlines its main pillars. Section 4 introduces the conceived SSI system, with architecture and implementation details. Section 5 is about the proposed solution system functionalities and user cases. Section 6 reveals real-world scenarios for the developed system and situations in which it can be used and have a good impact by simplifying the processes and making them more secure. In section 7, the conclusions of the research will be presented.

2. RELATED WORK

Research conducted by Juniper Research announces that the number of digital identity applications will reach 4.1 billion globally by 2027, increasing from 2.3 billion in 2023. This will be determined by government-backed digital identities replacing physical identity documents as a source of verification for third-party services, such as banking and financial services [6].

There is yet to be a certified, official, widely approved digital ID that can identify people in the online environment. It is also not enough to have a digital ID, an electronic ID, but one controlled and managed by its owner, not by other entities, identity providers or others. There are some countries, like Estonia or Australia, where initiatives were already taken and where a self-sovereign identity for their citizens is being developed [7].

EIDAS (electronic Identification, Authentication, and trust Services) was approved in 2014 by the Council of the European Union and represents a regulation for electronic identification in online services and transactions. It contains standards for digital signatures and digital certificates with the final scope of creating a digital ID usable within all member states. In 2021, the updated version of eIDAS2

[1] National University of Science and Technology "Politehnica" Bucharest, Romania
[2] National Institute for research-Development of Machines and Installations Designed for Agriculture and Food Industry, Bucharest, Romania
E-mails: raluca.bracacescu@stud.acs.upb.ro, stefan.mocanu@upb.ro, anca.ionita@upb.ro, bracacescu@inma.ro

DOI: 10.59277/RRST-EE.2024.69.1.15

appeared, which goes further and approaches the SSI model's principles, giving the owners full control of the identities [8].

Blockchain is a fundamental technology for the SSI model. As SSI wants to provide a decentralized model, Blockchain, a decentralized technology, brings its cryptographic methods and advantages, making it the core for the SSI's variable registry, which manages decentralized identifiers and verifiable credentials. Although blockchain is new, it easily became popular in information technology because of its characteristics. It is a distributed ledger and brings data immutability. All transactions made are stored on the blockchain and cannot be deleted or altered. It has a high level of security and trust. A Goode Intelligence study suggests that by 2025, 20 % of all digital IDs will be based on blockchain technology [9]. Several pilot programs for banking, e-commerce, and government services have already proven that blockchain-based Self-Sovereign Identity implementations can be a solution for removing many third parties involved in data exchange. Self-sovereign identity systems offer user data privacy, are secure, and have a very high development perspective, representing the future of digital identities [10].

There are some initiatives regarding the development of SSI, like uPort, ShoCard, Bitnation, and Sovrin projects.

uPort [11] is a self-sovereign identity platform developed by ConsenSys with the Ethereum blockchain. Its main use case is identity management for decentralized and centralized applications (Dapps) (email or banking). uPort contains three fundamental components: Smart Contracts, a mobile application, and libraries for developers [12].

ShoCard [13] is a digital identity application focused on user identification for travel purposes. It provides a mobile identity storage application that sends signed and encrypted identity data to the Bitcoin blockchain. Users can scan their documents (identity documents, passports, driver's licenses) with the help of the application, which takes the data, encrypts it, and stores it on the mobile phone. They are then encrypted, signed with the user's private key, and published to the blockchain. When registering the user, the application verifies his identity with facial recognition and checks the authenticity of the entered document [12].

Bitnation [14] appeared in 2014 in Amsterdam and is a governance platform based on blockchain. It seeks to provide the concept of world citizenship through a decentralized identity model created with the help of blockchain. The application aims to provide the same services as governments, but voluntarily and borderless. Anyone can become a Bitnation citizen by signing the constitution. More than 1 billion people will be online workers by 2025. These people will offer their services globally and require service providers' jurisdiction and governance.

In addition to these two examples, mentioning the Microsoft initiative related to SSI is also important. In the summer of 2022, at the Identiverse conference, they even offered a demo of their SSI platform, which is still under development and uses the Bitcoin Blockchain [15].

Besides these major projects, there are many research papers about Self-Sovereign Identity, a very interesting one [16] presenting a digital identity with Blockchain, as is the case in this paper. It uses verifiable credentials, decentralized identifiers (concepts presented in detail in the next section), and cryptographic mechanisms to manage them. Still, the user requests the identity from an authority, unlike here, where it is generated automatically only by scanning a physical identity document.

All these related works show a high interest in the field. The system proposed in this article has some similarities in concepts with the projects described above (the use of Blockchain, following SSI principles). This paper focuses on digital identification, creating an online version of physical identification documents, usable in many cases not only in one area but for airports as ShoCard is.

3. BACKGROUND

Digital identity represents an entity (person) in the digital environment and consists of a unique identifier associated with different attributes and characteristics. An identifier is information used to distinguish a person in a system. In the case of a digital ID, the unique identifier is the tax code. Attributes of digital identity are a person's name, surname, date of birth, address, or physical characteristics (eye color, height) [17]. Some of these may change over time; for example, a person may change addresses.

Identity management models have evolved based on three main requirements: security, control, and portability. There are five major identity management models: Isolated Identity Model (Silo), Centralized Identity Model, Federated Identity Model, User-Centric Identity Model (user-centered identity model) and Self-Sovereign Identity model [18].

SSI is still a rather new concept, although it appeared in 2015 and represents the most modern take on digital identities. With the previous identity management models, unlike with SSI, the owners of the digital identities were not in control. There were always third parties involved that managed user's private data that could decide to disclose information without consent. In the SSI model, only users can decide what information will be disclosed, when, and to whom. Selective disclosure is a very important aspect of Self-Sovereign Identity, meaning that the owners can select partial data of the identity to be disclosed, not all the attributes and characteristics [19].

SSI has seven key concepts [20]:

1 Verifiable Credentials (VCs)
2) "The Triangle of Trust "
3) Digital Wallets
4) Digital Agents
5) Decentralized Identifiers (DIDs)
6) Blockchain and verifiable data ledgers
7) Governance frameworks

Verifiable credentials (VCs) are an important component of SSI and are equivalent to physical credentials in the digital world. Some examples of physical credentials are identity cards, driving licenses, **and** bachelor's degree diplomas. These have the big disadvantage that **they cannot be used in the digital environment and,** unfortunately, can be forged, lost, or stolen [21].

Verifiable credentials (VCs) are now a standard developed by the World Wide Web Consortium (W3C) and offer many advantages such as increased security, continuous availability (can be used at any time), selective disclosure of content, and the impossibility of replication [10].

Any credential contains a set of attributes named claims and a subject. The claims in a credential can be of several forms; they can represent characteristics of the subject (age, height), membership or place in an organization (citizenship in a country), or rights (medical benefits, legal rights, library access). There are two methods defined by the VC 1.0 (W3C) data model specification for representing verifiable credentials, and both are based on JavaScript Object Notation (JSON): the JSON-LD representation and the JWT, JSON Web Token representation.

A JWT is a token formed of three strings (subtokens) separated from each other by the dot (.) character. The first subtoken contains meta-information about the type of key used, the second contains the claims and data about the verifiable credential (subject, issuer, expiration date, issue date, attributes), and the third contains the digital signature created with the private key of the issuer [22].

The digital signature of the JWT can be verified with its corresponding public key. This ensures that the real issuer signs the token and it is trustworthy. If the claims of the JWT were to be changed, the digital signature should also be changed. This means the data cannot be altered. Through the system created with decentralized identifiers (DID), a digital signature can be validated with public keys without the involvement of other entities, such as servers or specific providers.

Issuers, holders, and verifiers are the three roles forming "The Triangle of Trust". Verifiable Credentials are exchanged between them. The issuers are the ones who generate the credentials, and each credential has assigned an issuer. Most issuers are organizations, state authorities, financial institutions, universities, and corporations.

Holders request the credentials from issuers. The credentials are then kept in the holder's digital wallets (Digital Wallets). As poof a claim, holders present their credentials to verifiers.

Verifiers are the persons or organizations checking the validity of the credentials. The digital signature of the credentials issuer is analyzed using a DID, a distributed data registry, and a blockchain [20].

Governance frameworks specify the policies and procedures that issuers must follow to issue a verifiable credential. Governance frameworks are how SSI infrastructure and verifiable credentials can scale to work in any trusted community of any size, up to the entire Internet [20]. For clarification, some additional explanations will be given below, especially for the concepts of verifiable credentials and decentralized identifiers, as these are the most important.

All three entities, issuers, holders, and verifiers must have their pair of cryptographic keys and decentralized identifiers. Private keys are kept on their devices, but public keys are distributed across the DID network, so anyone can use the public keys to verify digital signatures.

A DID is obtained starting from the public key or the associated blockchain address. Example DID for Ethereum Blockchain, Rinkeby network, started from public key: did:ethr:rinkeby:0x0314ab2ed700694a0c0b904ac1176cde4 ab993a8b8eaee2246443cdd6e4fa677f7. Behind each DID is a DID document where delegated public keys and other properties are found and information about the key. The document DID is obtained using a blockchain programming method, DID Resolver. The issuer's DID is mentioned inside the verifiable credential, and the verifiers use it to retrieve his public key and verify the digital signature on the verifiable credential.

4. SSI SYSTEM ARCHITECTURE AND IMPLEMENTATION

Further, a proposal for a Self-Sovereign Digital ID solution will be presented, conceived based on the theoretical background presented in the previous chapter, that citizens can use to prove their identity and characteristics to gain access to different services. With this digital ID, users can share partial data from their digital identity, and most importantly, nothing is being disclosed without the user's consent. The process is easy, user-friendly, and consists of generating and scanning QR codes. With the system developed and implemented, identity owners can even transfer the digital ID from one device to another, but with the condition that the digital ID must simultaneously exist on a single device. Trust in the system is ensured by blockchain technology with its defining characteristics, cryptographic keys, and digital signatures. Since sensitive data is managed, a high level of trust in the system must be ensured.

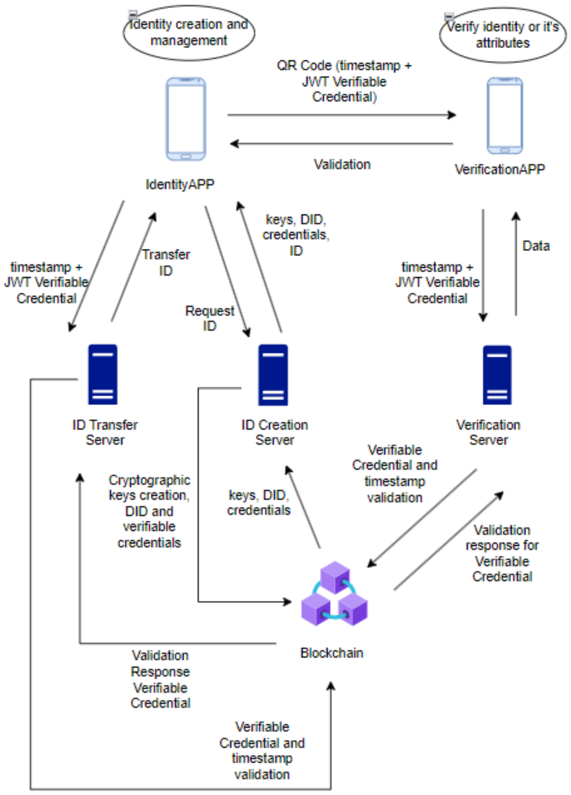
Identity creation and management
Verify identity or it's attributes
QR Code (timestamp + JWT Verifiable Credential)
Validation
IdentityAPP
VerificationAPP
keys, DID, credentials, ID
timestamp + JWT Verifiable Credential
Transfer ID
Request ID
timestamp + JWT Verifiable Credential
Data
ID Transfer Server
ID Creation Server
Verification Server
Verifiable Credential and timestamp validation
Cryptographic keys creation, DID and verifiable credentials
keys, DID, credentials
Validation response for Verifiable Credential
Blockchain
Validation Response Verifiable Credential
Verifiable Credential and timestamp validation

Fig. 1 – Architecture of the proposed digital ID system.

The control over **the user's personal information belongs exclusively to him;** all data is stored on his mobile phone, where the digital identity application is installed, and he is the only one **who** can manage it.

A new modern Self-Sovereign Identity solution is offered with this solution, **which can change digital IDs**.

In Fig. 1, the architecture of the proposed identity management system is presented. This has five main components: Identity app (first mobile application developed, responsible for ID creation, management, and transfer), Blockchain (Ethereum Blockchain), Verification app (second mobile application developed for ID verification), and three servers for ID transfer, ID creation, and ID verification (host the backend part of the two applications processes).

Identity App is a mobile application that creates and manages a user's digital identity. All users' data is automatically collected by scanning the users' physical identity documents; in this case, a Romanian national identification card was used. All retrieved information is stored on the user's device (mobile phone) memory as JWT (JSON Web Token) tokens representing the verifiable credentials. Each identity owner characteristic, like name, date of birth, and tax code, is encoded as a verifiable credential, respectively, a JWT. No user information leaves the device; the user is the only one with full control over everything.

When digital identity creation is initialized, the Identity APP calls the ID Creation Server (in the middle of Fig. 1.) hosted on a cloud platform (Heroku in this case). WebSockets protocol helps establish a communication channel (link) between the server and the mobile app, through which messages are exchanged. The backend part of the application runs on the server in a JavaScript environment. Libraries, packages, and dependencies specific to Ethereum Blockchain in the context of Self-Sovereign digital identities like did-jwt-vc, did-resolver, ethr-did, ethr-did-resolver, were integrated. So, after the physical ID card is scanned, the information is sent to the ID Creation Server, where a unique decentralized identifier (decentralized identifier, DID) and a pair of asymmetric cryptographic keys, private and public, are created and assigned to the user. The decentralized identifier is generated with the DID Create programming method for Ethereum. Blockchain serves as a registry for these decentralized identifiers and their associated DID documents, inside which the public keys of the DID owner and other attributes can be found. The private keys remain on the mobile phone of the digital identity holder. After the DID, the verifiable credentials are generated as a JWT (JSON Web Token) based on the personal information retrieved on the first step, using a programming method that gets the public key and the decentralized identifier of the credential's issuer as parameters. The JWT is composed of three parts: a first part containing metadata about the type of key used, a second part containing VC's claims and credential attributes, and a third part containing the issuer's digital signature issued with the private key. In this case, the issuer will be the same for all users, already exists, and will be specific to the system itself based on the physical document scanned. There is also a Smart Contract deployed in the blockchain that keeps track of the identity documents converted into digital IDs to have a record, making it impossible for a digital identity to appear on multiple devices. Revoked documents are also tracked in this way. If everything is good, the JWTs are created, the DID and the private keys are sent to the Identity APP and stored on the device, and the creation process ends.

When the user wants to use the digital identity, a QR code is generated in the Identity App to verify the fulfillment of certain conditions after completing the creation process. It encapsulates the JWT verifiable credential selected to be shared. A timestamp has been added for security reasons so that each QR code generated becomes unique and valid for 30 seconds, not to be reused. The Verification App will scan it. After scanning the QR code, the dedicated server for identity validation will be called the one on the right end of the figure above Fig. 1. Here, through the blockchain with a specific DID Resolver programming method, the signature part of the verifiable credential will be verified. The claims contained in the credential will be decoded, sending the response back to the Verification App where conditions regarding the user's identity will be validated or not, like an age condition or simply the name will be shown for the verifier, taking into consideration that these are trustful because of the system and its cryptographic methods. Also, on the server, the time stamp is checked to be within the allowed limit, and the credential expiration date is checked not to be exceeded. By calling a method of the previously mentioned Smart Contract, it is validated that the credential has not been revoked.

The digital ID transfer server is required when moving the ID from one device to another. Digital ID cannot exist on multiple devices at the same time. From the Identity App, several QR codes are generated, five in number, which contain user data in the form of verifiable credentials, decentralized identifiers, and private keys. They will be scanned with the new device, and the server will be called to perform checks before the transfer is complete.

To summarize all the tech stack used for the system: for mobile applications, development used Flutter for the servers' backend code JavaScript with specific SSI Ethereum Blockchain libraries and WebSocket for communication between servers and mobile apps.

As is the case with any system, there are some challenges with digital identity management. Two are mentioned in the paper [23]: identity leakage and identity changes. In the system developed, the digital ID has an expiration date to address identity changes that can happen over time. Regarding data privacy, information is stored exclusively on the owner's device. Some logic will indeed happen on the system's backend servers regarding processing the verifiable credentials, but they will not be stored there in any way. Also, in the QR code exchange, the timestamp added to the JWTs makes them unique and valid only for a few seconds to ensure they will not be stolen. In the future, additional security features can be added.

5. FUNCTIONALITY AND USE CASES

The following will present the system's functionalities from a user perspective to understand the technical aspects, the entire concept, and its flow.

First, the user needs to have an identity APP on his mobile device, and after that, he can start creating the digital ID. For this, he must scan his physical identity card for the correct and automatic retrieval of the digital identity data. Since the creation of digital identity takes place exclusively in the online environment, a method for validating a user's identity is required to make sure that the owner of the document presented is the same person creating the digital ID. Thus, the user is asked to take a live selfie, which will be compared with the photo attached to the scanned physical identity card. At this step, the liveness detection technique (LDT) ensures the selfie taken is real, not only an image of the person.

The expiration date of the presented document is also checked to ensure it is not passed, and the register created with the Smart Contract is consulted to signal whether the document has been revoked or used before to create a digital ID. All the information taken from the user is transformed into verifiable credentials. A personal private key and a DID, both automatically generated, will be assigned to the user.

It will be ready for use after finalizing the digital identity creation process. Authentication through facial or fingerprint recognition within the application is mandatory for the user to access its features. This is handled using the mobile phone native authentication.

Identity App allows selective data disclosure; users can choose what information to share. There are several options depending on needs, all based on the data retrieved from the scanned physical identity card. Options include name sharing, date of birth, tax code, or address, but each separately or together if needed. For security reasons, the user must authenticate every time before sharing his data.

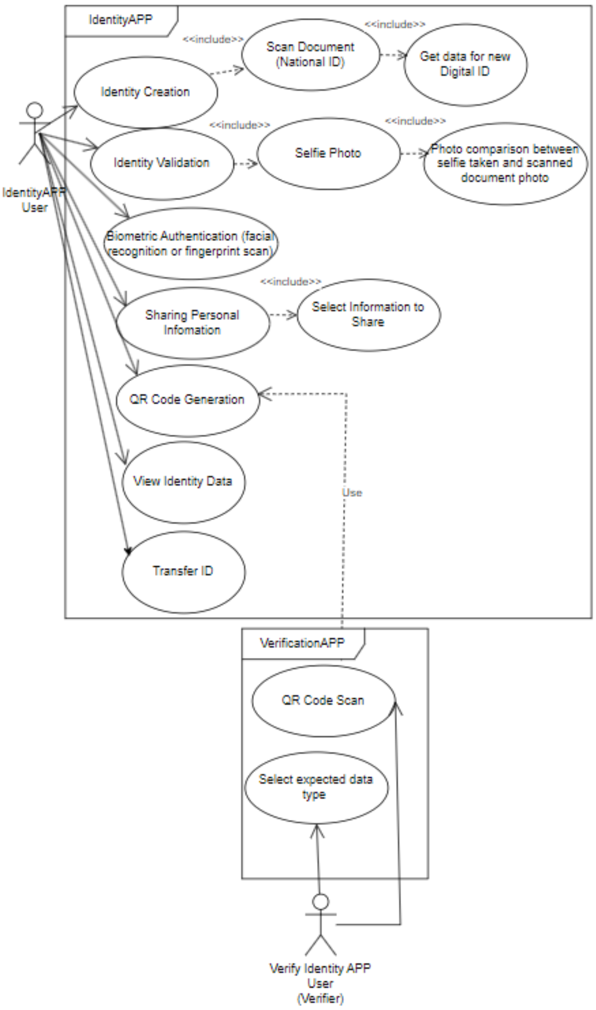
IdentityAPP
<<include>>
Scan Document (National ID)
<<include>>
Get data for new Digital ID
Identity Creation
<<include>>
Selfie Photo
<<include>>
Photo comparison between selfie taken and scanned document photo
Identity Validation
IdentityAPP User
Biometric Authentication (facial recognition or fingerprint scan)
<<include>>
Sharing Personal Infomation
Select Information to Share
QR Code Generation
Use
View Identity Data
Transfer ID
VerificationAPP
QR Code Scan
Select expected data type
Verify Identity APP User (Verifier)

Fig. 2 – User-case diagram of the system.

The user generates a QR code to share his data, which will be scanned with the verification application Verification App. The QR code represents a JWT containing the user's verifiable credentials and a unique timestamp. The timestamp will also be verified because, otherwise, someone can take a snapshot of the QR code and use it outside the application. In the Verification App, the necessary data module or scenario and the conditions to be met must be selected before scanning the QR code. There are predefined scenarios, and the verification step needs to know exactly what is verified and expected.

After selecting the data mode in the Verification App (precondition), the QR code generated by the Identity App will be scanned. Thus, the data will be received as a JWT of verifiable credentials and a timestamp. The QR code has been valid for only 30 seconds since it was issued, which is easily verifiable with the help of the timestamp. Through blockchain, the verifiable credentials will be validated, ensuring that the expiration date is not exceeded or that they have not been revoked. If everything is in order, the data can be retrieved, and the claims about the user can be obtained. Subsequently, the conditions selected through the previous data mode will be checked. At the end, the result will be sent as a message that mentions whether the desired conditions were met or not, or the information about the shared identity holder will be sent.

This is possible if the user wants to transfer his digital identity from one device to another. All the steps for creating a new identity must be completed on the new device: scanning the identity document and taking a selfie photo. As soon as the process is completed, the user will be notified that a digital identity with the same data already exists and will be asked if wants to transfer it. Next, he/she will scan a few QR codes generated by the old phone inside the Identity App. The data will be verified after scanning the codes containing the verifiable credentials, the user's private key, his decentralized identifier, and a time stamp. The new identity, which is the same, just transferred, will be created, and the one on the old phone will be automatically deleted.

6. **REAL-LIFE SCENARIOS**

The result of the research is a self-sovereign digital ID system, with selective disclosure and full control of data given to the owner. Real use cases will be presented further to clarify the developed system's scope and benefits.

A first example of a real scenario in which the system helps identify a person without revealing more information than needed is when taking an exam, whether a national exam, baccalaureate degree, admission to higher form education, or any other exam. With the help of digital identity, the student/candidate can generate a QR code with his name present in the Identity APP, which can then be scanned with the Verification App application. Only the full name of the student/candidate will be disclosed without sharing other information about him, such as address, tax code, and date of birth, as in the case of presenting the physical identity card. Personal data are protected, and the result will be the same; the identity will be established with certainty, thanks to cryptographic means, verifiable credentials, and all the system concepts.

Another real use case scenario is proving an age condition (over 18 years old, under 25, over 65). Age over 18 years old is mandatory from a legal point of view for various activities such as purchasing alcoholic beverages, products containing tobacco, and access to certain locations. Through the implemented system, the age condition over 18 will be certified without disclosure of any other information; not even the name needs to be shared. Also, the Verification App can run on a device connected to a barrier in case of access in certain locations, and the barrier can be raised only after validating the condition. Thus, the entire process will be automated, becoming simpler and, at the same time, safer.

In airports or at border crossings, the system can help simplify the process, offering the same trust. Digital identity can be used, and only the interest data, such as name, first name, date of birth, and ID number, is shared.

Apart from the examples mentioned above, many others can be added; digital identity can serve wherever necessary to distribute and validate information. In situations such as participating in sports competitions, receiving certain parcels, postal packages, and social benefits, in the educational system, online schooling [24], or the healthcare system, including telemedicine, could help track doctor's identities and certifications and patient's medical histories [25]. Blockchain and SSI-related techniques can also become useful in client relationships and water or energy distribution companies [26]. With some modifications and adaptations, digital identity could be used on a large scale and become the only form of identification, even in front of the state authorities.

7. **CONCLUSIONS**

In conclusion, the system represents an original solution for a digital ID using decentralization, verifiable credentials such as JWTs, decentralized identifiers, Ethereum Blockchain, and data sharing with QR codes. Other important contributions are the liveness detection technique added when creating the digital ID and comparing the live photo to the physical scanned document photo, the possibility to transfer a digital ID from one device to another one, and the timestamp added to the JWTs, making them unique in the sharing process.

The model developed can replace physical national ID cards, creating an online form of identification with selective disclosure and high information trust. The system can prove useful in many concrete scenarios, adding value to identity management. Based on how it was built, the system offers trust to the users and the security of their data. It uses tokens and digital signatures integrated with blockchain, so the identity theft risk diminishes. The owner of the digital identity is the only one who can authorize data sharing, and this is the most important aspect; there is no other entity that controls his private information and that has access to it.

Also, based on blockchain technology, the system implements decentralization and ensures no single point of failure. Blockchain nodes have the entire history of transactions made; this way, it cannot be altered, and the source of truth for the digital identities is accurate.

SSI can add major improvements in domains like e-governance, healthcare, banking, and refugee problems, topics of much interest nowadays. Real use case scenarios were presented in the previous chapter.

The system can be improved for future developments, and other documents like driver's licenses and passports can be added. They can be connected to various services, such as e-governance services (health care system, voting system). Some security patterns can be enforced, a superior LDP can be used, and additional features can be developed to ensure the identity of the digital ID owner so no one can forge it.

Received on 30 October 2023

REFERENCES

1. O. White, A. Madgavkar, J. Manyika, D. Mahajan, J. Bughin, M. McCarthy, O. Sperling, *Digital identification: A key to inclusive growth*, McKinsey Global Institute, 2019.
2. F. Wang, P. De Filippi, *Self-sovereign identity in a globalized world: credentials-based identity systems as a driver for economic inclusion*, Front Blockchain, **2** (2020).
3. R. Brescia, *Social change and the associational self: protecting the integrity of identity and democracy in the digital age*, Penn State Law Review, **125,** *3* (2021).
4. Š. Čučko, M. Turkanović, *Decentralized and self-sovereign identity: systematic mapping study*, IEEE Access, **9**, pp. 139009–139027 (2021).
5. G. Laatikainen, T. Kolehmainen, P. Abrahamsson, *Self-sovereign identity ecosystems: benefits and challenges*, Proceedings of the 12th Scandinavian Conference on Information Systems, Article 10, 2021.
6. Juniper Research. Available at: https://www.businesswire.com/news/home/20230226005042/en/Juniper-Research-Active-Digital-Identity-Apps-to-Surpass-4.1-Billion-by-2027-as-Third-party-Platforms-Look-to-Leverage-Civic-Identity-Systems.
7. D. Pöhn, M. Grabatin, W. Hommel, *eID and self-sovereign identity usage: an overview,* Electronics*,* **10** (2021).
8. A. Giannopoulou, *Digital identity infrastructures: a critical approach of self-sovereign identity*, DISO, **2** (2023).
9. Goode Intelligence. Available at: https://www.goodeintelligence.com/press-releases/goode-intelligence-forecasts-that-over-three-billion-digital-identities-will-be-issued-by-2025/
10. J. Keil, *Self-sovereign identity: use cases, level of maturity and adoption*, 2020.
11. uPort. Available at: https://www.uport.me.
12. A. Panait-Drăgnoiu, R. Olimid, A. Stefanescu, *Identity management on blockchain – privacy and security aspects*, Proceedings of the Romanian Academy – Series A: Mathematics, Physics, Technical Sciences, Information Science, **21** (2020).
13. Shocard. Available at: https://shocard.com.
14. Bitnation. Available: https://tse.bitnation.co.
15. J. Uchill, *Microsoft demos SSI open standards at identiverse: 'This is the power of standards'*. Available at: https://www.scmagazine.com/analysis/microsoft-demos-ssi-open-standards-at-identiverse-this-is-the-power-of-standards.
16. Z. Song, Y. Yu, *The digital identity management system model based on blockchain*, International Conference on Blockchain Technology and Information Security (ICBCTIS), 2022, pp. 131–137.
17. U. Der, S. Jähnichen, J. Sürmeli, *Self-sovereign Identity – opportunities and challenges for the digital revolution*, arXiv, 2018.
18. R. Soltani, U. Nguyen, A. An, *A survey of self-sovereign identity ecosystem*, Security and Communication Networks, 2021.
19. F. Schardong, R. Custódio, *Self-sovereign identity: a systematic review, mapping, and taxonomy*, Sensors, **22** (2022).
20. A. Preukschat, D. Reed, *Self-Sovereign Identity: decentralized digital identity and verifiable credentials,* Manning Publications Co, 2021.
21. M. Sroor, N. Hickman, T. Kolehmainen, G. Laatikainen, P. Abrahamsson, *How modeling helps in developing self-sovereign identity governance framework: An experience report*, Procedia Computer Science, **204** (2022).
22. T. Matsuzaki, *Verifiable Credentials: Decentralized Credential Flows*, 2020.
23. Y. Liu, D. He, M.S. Obaidat, N. Kumar, M.K. Khan, K.R. Choo, *Blockchain-based identity management systems: A review*, Journal of Network and Computer Applications, **166** (2020).
24. A. Olteanu, R.N. Pietraru, S.M. Olanescu, M. Moalfa, *Innovations in the educational process in technical universities based on an ontology for interactive teaching system*, Rev. Roum. Sci. Techn. – Électrotechn. et Énerg., **66**, *1*, pp. 53–58 (2021).
25. I.C. Stanica, F. Moldoveanu, M.I. Dascalu, I.V. Nemoianu, G.P. Portelli, *Advantages of telemedicine in neurorehabilitation and quality of life improvement*, Rev. Roum. Sci. Techn. – Électrotechn. et Énerg., **66**, *3*, pp. 195–199 (2021).
26. L. Meng, Q. Zhao, M. Song, Y. Jian, H. Tian, *Authenticated key agreement scheme based on blockchain for AMI communication security*, Rev. Roum. Sci. Techn. – Électrotechn. et Énerg., **68**, *2*, pp. 218–223 (2023).