

Using blockchain technology for ID management: a case study for Albania

Elva Leka¹, Luis Lamani², Enkeleda Hoxha³

Polytechnic University of Tirana, Tirane, Albania^{1,2}

Albanian University, Tirane, Albania³

elva.leka@fgjm.edu.al, luis.lamani@fgjm.edu.al, leda_h@hotmail.it

Abstract - In this paper we have presented a framework, which proposes to adopt blockchain technology for ID card management in Albania, to increase the security and privacy of personal data. The way how the actual ID cards in Albanian tend to offer security is by using a microprocessor, encrypting the data in the card. However, the centralized data management systems have single points of failure that leave the system vulnerable to attack and operational risks such as: (1) inside hacking, where unauthorized changes of personal information may happen from the inside system; (2) fake digital identities creation or (3) sale of personal identity's data to third interested parties. An answer to address the above-mentioned drawbacks is a decentralized identity management system, which calls for a user-centered strategy and returns complete identification control to the individual. Blockchain technology has the potential to revolutionize modern civilizations and their applications. Administrative processes, security, privacy, integrity and confidentiality are some actions that could have an impact. Furthermore, we present an analysis of previous work on blockchain-based identity management and provide a proposal use case applicable in Albania compared to actual implementation.

KEYWORDS: BLOCKCHAIN TECHNOLOGY, SECURITY, PUBLIC ADMINISTRATION, ID MANAGEMENT

I. INTRODUCTION

A blockchain ID card is a chip which is used to store personal information about the citizen that owns that card, such as: full name, gender, national identification number, fingerprints cryptographic keys, and certificates [1]. In the world we live today with a technologically advanced society, digital identification is gaining great importance. Therefore, it is necessary to create a digital identity system to be positive and sustainable for the long term, and furthermore to be developed as user-centered solutions that enhance user safety, benefit and control [2]. Managing individual identities inside a system, such as a business, network, or even a nation, is referred to as identity management. Our reliance is on identity information management, which aims to manage and secure our personal information while additionally providing related services [3]. Centralized databases are vulnerable regarding identity theft and data breaches. As a result, some nations have looked at and implemented blockchain applications for digital identification. The authentication of many types of identity documents, particularly those used for international transactions, and the prevention of data loss are two issues that blockchain is considered to solve. The possibility of blockchain for self-sovereign identity is also intriguing to stakeholders [4].

A national identity card, which is provided by the government in most countries, is the main system used for both identity verification and at least one functional authentication purpose. Estonia and Finland have also received recognition for their contributions to the advancement of e-government technologies in Europe, among other nations. The Estonian e-Residency system has now developed a new digital nation for world citizens. To safely identify themselves and access e-services, anyone can offer digital signatures using their ID card, Mobile-ID, or Smart-ID. The technology can be used for document signing, banking, payment services, and company registration [5]. Incorporating banking, payment processing, document signing, and company registration are all possible uses for the system.

Creating complete identity management systems that link people's identities throughout their lives—from birth certificates, civil registration records, driver's licenses, and marriage certificates to voter registration and national identity cards—represents a new opportunity for governments [6]. Governments in developing nations are simultaneously expected to carry out many of the same tasks that governments in developed nations can do, including "ensuring universal access to health care and education and administering a wide variety of transfer programs" [7]. The approach, however, has raised security issues because it controls the identification that gives a person their uniqueness. Numerous instances of misuse, duplication, or leakage of highly sensitive personal information, as well as hacking of financial assets, are common. The nation that is harmed suffers economic costs as a result of these security incidents. As a result, managing one's identity becomes a crucial issue for those working in the private sector and higher education also.

Our focus in this paper will be on ID card management. There have been numerous attempts to identify efficient strategies for safeguarding data related to national identification, such as the centralized server that Albania employed while creating its national identity management system. But these methods continue to focus on centralized data management systems with single points of failure, which leaves the system open to attack, because it is possible for an enemy to accomplish its nefarious goals of stealing, abusing, or manipulating the data at the centralized server.

Blockchain technology eliminates the shortcomings associated with centralized data management systems by providing decentralized transactions and safe data management [8]. When Satoshi first proposed the concept in 2008, it was to manage the data for the Bitcoin cryptocurrency. A blockchain is a method for verifying, clearing, settling, tracking, and recording the ownership of assets as they are traded, as not a form of money [9]. This paper uses the identity management system for Albania as a case study to offer a proposal for a protected national identity management system based on blockchain technology. The model addresses user identity disclosure, authentication, and verification. The establishment of a virtual user's true identity on the Blockchain and linking the user's entity information to the metamask address are further ways to thwart Sybil's attacks. Additionally, a handshake protocol paradigm for identity disclosure is proposed, giving users the freedom to decide which identification attribute to disclose to other blockchain users. The creation of a web page prototype for the suggested system is the last phase. The prototype included models that are crucial elements of the recommended national identity management system.

In this article, the sections are divided as follows. In section II we will talk about the general background of blockchain technology and related work that has been implemented in connection with ID management. Then, in section III the current management system in Albania is reflected. The proposed architecture and the implementation are presented in section IV, and the last section V shows the conclusions and future works.

II. BACKGROUND AND RELATED WORK

2.1 Background

Understanding this technology's basic concepts as well as the issues it brings up is essential. Blockchains are collections of information known as blocks, which are linked to one another using various cryptographic techniques. The hash code, confirmation time, and other details identify each block. On the blockchain, there is a digital record of everything we do identifiable, verifiable, storable, and exchangeable signatures are present on every node of the blockchain, enabling a chain of custody to be established from the original owner back to the node [10].

It is important to select a suitable blockchain platform according to the requirements and technical features of a specific implementation. The most popular known blockchain platforms are:

Ethereum, Hyperledger Fabric, Hyperledger Sawtooth, R3 Corda, Stella, etc. [11]. For our implementation, we have chosen the Ethereum platform. Ethereum [12] was developed to expand beyond the scope of a transactional cryptocurrency and utilise blockchain technology to introduce a decentralized framework to the internet. Ethereum is an open platform, and we may use it to easily start a decentralized application and set its own rules for ownership, transactions, and state transactions [13]. Most of the smart contracts are created by using Ethereum. A smart contract is a digital contract, which represents self-executing programs with specific terms and conditions and it would be executed and added to the blockchain network once the conditions are met [14]. A smart contract is designed to remove the requirements for a controller and create a system of mutual trust between participants.

2.2 Related Work

According to our study, several blockchain-based identity systems have been proposed and implemented in different countries.

In their paper [15] authors have introduced a new method of blockchain formation for reliable storage of the personal data of ID-card holders. In order to use the blockchain network for more than only storing ID information and to enable the ability of access control of data as well as boost security, they suggest a novel blockchain structure dubbed "Blockchain Tree". The authors believe that the solution they propose is more secure and furthermore the methodology for building a storage system, access control, and document verification can be used not only for ID-cards but also for other documents, such as driver's licenses, education documents, personal medical information, social security cards, etc.

Authors in [16] have proposed a model for a smart card management system using blockchain technology in Bangladesh. They believe that their proposed model will help the government to secure citizens' private information and bring transparency to their information management.

Estonia is one of the first countries that has implemented the Digital ID, which is powered by the Republic of Estonia. E-Residency is a new brand of digital nation for residents around the world. In contrast to many other nations, every Estonian possesses a state-issued digital identity without any physical touch, regardless of where they live [8]. Every user can securely identify themselves and access services by providing digital signatures with their ID card. The system is accessible to residents for document signing, banking, and payment services [9]. For document signing and document verification, the cards use 2048-bit RSA encryption. The Estonian legal system fully supports the use of this technology for digital signatures on legal documents. The advent of e-Residency is a significant shift, making the recent news that the Estonian government is now collaborating with Bitnation to provide e-Residents with a public notary service based on blockchain technology [17]. The way how identity information is managed and authenticated could be completely altered by using blockchain in e-Residency.

On the other hand, South Korea uses digital driver's licenses. This is the first digital identification card authorized in South Korea and was approved by the Ministry of Science and ICT in September 2019 [18]. The PASS application uses decentralized identity (DID). A brand-new class of distinct identifiers called a decentralized identifier (DID) is used to verify digital identities that are entirely under the control of the identity's owner. Cryptographic keys can be used by a DID owner to prove ownership of the DID. To confirm the validity of the issuing authority's signature on a credential, one can also use the public key of the Document DID. There are many advantages to using DID technology, but two stand out the most. For starters, because credentials can be verified, it should make it much harder to fake a driver's license. The second important advantage is that an individual can choose how much data to make available to a third party. For example, a driver's license indicates a person's age and using DID, you can prove that you are over 21 without giving your date of birth or even your name [19].

Another proposed digital identity solution is called *ShoCard* [20,21], which integrates blockchain information with facial

recognition technologies. ShoCard employs data hashing, out-of-band communication, data matching, and two-factor authentication to safeguard and validate identification. It also uses robust multi-key public/private key encryption. The key topics covered are airline user identification, secure enterprise identity verification, banking institutions, and access to the website and application. It offers a mobile application that lets users save identities and add hashed, signed IDs to the Bitcoin blockchain. Once the user scans their document, the application scans each Machine-Readable Zone (MRZ) and keeps an encoded version on the device. Each field is then broadcast on the blockchain, hashed in a single direction, and signed using the user's private key [20]. The recipient's public key is used to encrypt the local copy of the data before it is transferred via the QR code to any third party for exposure.

uPort [22] is an identity registration method on the Ethereum blockchain. It allows users to authenticate themselves and communicate information with other users clearly and transparently. uPort uses the same cryptography as Ethereum, but for a different reason. The public key is visible to everyone and is used to complete transactions and the private key is more like a secret phrase that only the user knows. The infrastructure required for off-chain data transfer and identity verification is provided by the uPort registry, which is a unique smart contract used by all uPort identities. In essence, it enables identities to assert their identities [22]. In 2017, uPort partnered with the Swiss city of Zug to use its identity management system for municipal services. In November, the Zug government offices organized the first official citizen's identity registration in front of a live audience. Citizens access the service through QR codes and only need to prove their identity once with official documentation [23].

Sovrin [24]: A non-profit corporation called the Sovrin Foundation supervises the Governance Framework that controls the Sovrin Network, a free service that permits self-sovereign identity on the Internet. Users are free to secure, store, and choose the identifying credentials they desire to use, such as a driver's license or employment card, thanks to the decentralized nature of the Sovrin network, which does not rely on separate databases that regulate access to those credentials. In a private setting, the holder of self-sovereign identity can display their credentials that can be independently verified. Information regarding your age, gender, education, and employment are some examples is the data that contains the credentials. The Hyperledger Indy Project and open standards form the sole foundation of the Sovrin protocol. All Sovrin IDs and public keys are aliases by design. Pairwise alias identities, in which each relationship has a unique distributed identifier, provide the solution (DID). Any individual, team, or IoT device that checks the identity owner's credentials can be sure that the proof or information being supplied is accurate and timely when using the Sovrin Network. Additionally, companies can avoid the legal responsibilities that come with maintaining vast amounts of potentially stolen or ill-used client data [25].

III. ACTUALL ID-MANAGEMENT SYSTEM IN ALBANIA

In this section, we will first present the current system which is used for id-management in Albania and the role of AKSHI which is the National Agency of the Information Society. Albania's present structure The European Agenda 2020 and the Regional Strategy SEE-2020 collaborated to create the Intersectoral Strategy "Digital Agenda of Albania 2015-2020," which aims to improve the digital agenda in a coordinated and efficient manner to improve living conditions for citizens and deliver high-quality services [26].

3.1 Albanian ID Card

Identification cards for Albanian Citizens are produced by the concessionary company Aleat Sh.p.k. ID Documents incorporate biometric and electronic elements and use dual-embedded chips which makes it possible to read citizens' biometric data and identify them. To be able to use the ID card it is needed a card reader called MSO and its drivers, which allow the PC to communicate the IDC microchip and read its data. Security elements are embedded within

Albanian ID Cards: Fingerprint authentication which identifies the owner of ID and electronic certificates allowing the IDC to be used for electronic purposes such as Electronic Signature of eDocuments.

In case an ID document is lost or stolen, the IDC holder can report it or go to the Company service point to revoke its certificates, by making this ID invalid to be used by unauthorized persons or for illegal purposes.

3.2 E-Albania

Albania state has developed a web-based portal, called E-Albania, which is a multifunctional system and serves to provide electronic public services to citizens and businesses 24 hours, 7 days a week. It started functioning as a project invested by European Union in 2009 and now offers more than 600 services, which are offered through various online systems and more than 240 institutions are connected with an e-government portal, increasing interaction between government, society, citizens and business [27].

The Government Interaction Platform, the fundamental architecture that facilitates interaction with the electronic systems of public entities, is linked to the e-Albania government webpage. The mission of e-Albania is to be the main channel for receiving online public administration services for citizens, businesses and public administration employees themselves [28].

The information presented on the platform is updated by the institutions when needed. It is linked to the Government Interaction Platform (Government Gateway), which enables real-time data transmission between 48 systems. The interoperability system is an Enterprise Service Bus solution with a service-oriented design that serves as a versatile central system. The National Register of Civil Status for persons and the National Commercial Register for enterprises serve as electronic databases for the electronic verification of the information users enter throughout the registration procedure. Using NID for citizens and NUIS for businesses, the authentication and identification procedure is based on the "Single-Sign-On" technique to produce a unique identity for each user. More than 50 million transactions are generated per year. Furthermore, 30 different types of documents can be downloaded from the portal equipped with a digital stamp, thus reducing paper use and saving time and money [29].

Other very important benefits that the connection of E-Albania with the Government Interoperability Platform offers are: (1) offering certificates and health cards; (2) facilitation of the flow of electronic information which is necessary to provide public services; (3) exchange of data between systems in state institutions; (4) increasing transparency; (5) offering possibility to analyze large volume of data, frequency of visits, number of transactions performed per visit.

The distinctive, multipurpose government portal e-Albania is developed and managed by the National Agency of the Information Society (AKSHI). AKSHI processes personal data while upholding and preserving fundamental liberties and rights of the individual, including the right to maintain one's privacy [30].

The fundamental architecture that enables interoperability is called Government Gateway. It allows for the integration of all internal government electronic systems. An integration system is required for all internal government electronic information systems to communicate with GG Core. This system will enable communication between internal backend systems and the GG core. Department Integration Server is one of the top options for this integration system (DIS).

The primary government portal, e-Albania can disclose the functionality of these internal systems, facilitating and streamlining citizen service. Messages sent and received between internal systems and between the main portal and internal systems are stored and tracked by an interoperability architecture.

3.3 Cyber Attacks on Albania

The On 15th of July 2022 the e-Albania portal, was unavailable during a cyberattack, which made the system vulnerable, because the attackers accessed sensitive data stored in state computers. The portal was hacked again 2 months later, by penalizing all the

services this system offers, by risking all sensitive data, security, confidentiality and integrity. The actors that initiated those attacks have named themselves as "HomeLand Justice" [31]. "HomeLand Justice" has done a series of attacks for approximately one year before launching cyber-attack, such as: (1) they periodically accessed and exfiltrate e-mail content; (2) included a ransomware-style file encryptor and disk wiping malware; (3) network reconnaissance, and credential harvesting from Albanian networks (May and June 2022); (4) deployed a version of ZeroClear destructive malware; (5) On September, actors launched another wave of cyber-attacks against the Government of Albania, using similar TTPs and malware as the cyber-attacks in July.

HomeLand Justice infiltrates the infrastructure of the Albanian Government using DDoS and Ransomware attacks. Due to this, neither residents nor administrative staff could access any administrative services or other types of services. The technique, which involves using malware to freeze data and then leak stolen papers, is frequently used by Iranian hackers.

The Government Gateway Platform is the platform at the center of every state record and the primary system of the Albanian government institutions. It is based on Microsoft products like SQL Server and BizTalk Servers [32]. It makes use of data storage as the database server. A Single Point of Failure (SPOF) is a risk that could arise from a flaw in the circuit of the system's design, implementation, or configuration. SPOF stands for a flaw or failure that has the potential to render an entire system inoperable. And the HomeLand Justice team utilized this exact tactic to access these databases.

IV. BLOCKCHAIN-BASED PROPOSED SOLUTION

In this section, we present the proposed architecture of the application and the implementation part.

4.1 Proposed application architecture

This work proposes a new paradigm for restricted data sharing utilizing Ethereum smart contracts. The decentralized file system, InterPlanetary File System (IPFS), and permission document sharing are the main components of our approach. Each participant has a public and private key, as well as a distinct account address that serves as their network identification. Users, documents, and requesting access data from the institution are the three main components of the above-mentioned approach. As can be seen in Figure 1, a hash code is provided to the user who then sends the data to the blockchain network via the smart contract. When a user enters the information for a document and uploads a picture of it, the information is transmitted to IPFS for storage, and the user receives an IPFS hash that is then sent to the blockchain network via a smart contract. When a user's data is requested by an institution, smart contract is called and the user is informed of the request. The user can then choose to accept or reject the request.

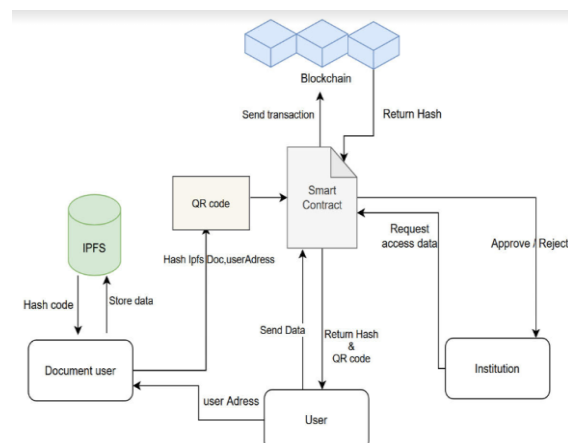


Figure 1. Workflow diagram

Furthermore, Figure 2 presents the level of architecture. The system has some important layers such as: Back-end level, middle

tier (Alchemy, Metamask), IPFS, and Ethereum Platform. To engage in nodes and complete transactions, we have chosen to use the Ethereum blockchain platform, which is a public blockchain. The package list runtime of the localhost URL, or the local server, is entered at the beginning of the prototype flow. After the user selects the package, it will be downloaded and encoded. We prepared to send transactions using our Ethereum address. Then, using Metamask, we sign the transaction on the blockchain. After that, we will combine the data, value, target address, gas price, and gas to create a transaction hash. When we attempt to test the package via a Chrome extension, the same process takes place. We merely need to call the hashing and validations API in the Chrome extension to obtain the outcome.

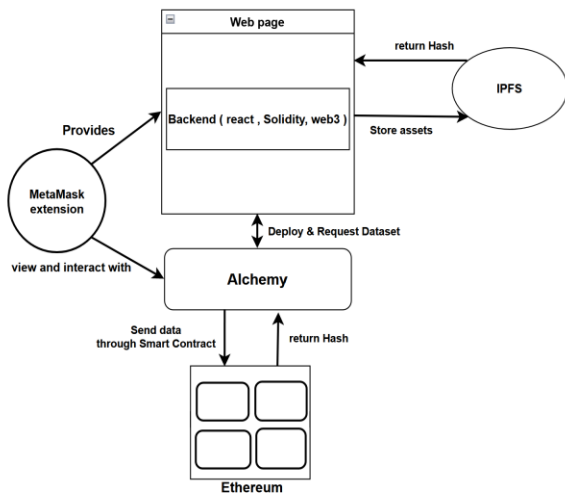


Figure 2. Levels of Architecture

4.2 Implementation

This section presents the main implementation details that have been chosen to connect to the blockchain and then verify on the blockchain network. For the configuration part and to prepare the appropriate development environment we have chosen the following technologies:

- *Ethereum*, as the platform for blockchain network development
- *Solidity*, as the language to deploy smart contracts
- *Metamask*, for the account creation
- *Alchemy*, form building an app to connect the blockchain API to Ethereum
- "*Hardhat*" package/module that will serve to compile the smart contract and run Solidity on a local development network.

After the contract is set up on the blockchain, its specific address is provided to us. We also receive the Binary Application Contract Interface (ABI), which is the standard method for interacting with contracts in the Ethereum ecosystem, both from outside the blockchain and for contract-to-contract communication, along with the contract address.

4.3 Proposed application architecture

This section presents the pseudocodes of the functions we have implemented into our smart contract. The first algorithm looks in the details for a registered person and grants approval after ensuring that no registered person exists in the system with such details. The associated hash is then sent to the user whose registration it is.

```

Algorithm 1: Add User and submission through Smart Contracts
1  Input: MetaMask Address,
2  Full Name,
3  Document Number,
4  Email Id,
5  Mobile Id
6  ContractState is Verify
7  UserData is Ready to Submit
8  If the User is registered = true
9      ContractState changes to Wait for Approvals
10     UserState is Submit for Approval
11     Return: Hash of transaction
12 End
13 Else
14     Reverse ContractState and Show an error
15 End
    
```

This second algorithm, which displays information about a registered user who uploads document data via IPFS, is next presented. *ApprovalStatus* changes to 2, if it is approved, or 3 if it is Rejected. After the submission, this data is sent to the blockchain through a smart contract.

```

Algorithm 2: Add Document User and submission through Smart Contract
1  Input: MetaMask Address,
2  Document Number,
3  Full Name,
4  Date of Birth,
5  Document Address,
6  Document IPFS Hash
7  ContractState is Verify
8  UserData is Ready to Submit
9  If DocumentHash {UserAddress} = IPFS hash of Document Then
10     ContractState changes to Signature provided
11     UserState is Submit for Approval
12     ApprovalStatus changes to 2 {Approved}
13     Create a Validation message for successful submitted
14 End
15 Else
16     ContractState changes to Signature Denied
17     Change UserState to Not Provided
18     Approval Status change to 3 {Rejected}
19     Create message error
20 End
21 Else
22     Reverse ContractState and Show an error
23 End
    
```

After an institution has made a data request, the final algorithm indicates the user's approval of the data that have been confirmed.

```

Algorithm 3: Request Access for User Document
1  Input: MetaMask Address of User,
2  Contract State Signature Provided
3  Name Administration is Provided
4  If Document No is checked Then
5      Change Document No = 1 {requested}
6  If Document FullName is checked Then
7      Change Document FullName = 1 {requested}
8  If the Document Date of Birth is checked Then
9      Change Document DateBirth = 1 {requested}
10 If the Document IPFS Hash is = IPFS hash Then
11     Change Document IPFS Hash = 1 {requested}
12 If message Transaction = successful
13     Return: Hash transaction
14 End
15 Else
16     Reverse ContractState and Show an error
17 End
    
```

V. INTERFACES

In this part we present two interfaces for the prototype we have developed, one of which is used for the user menu and the other for the administration menu. First, we need to get the private key that we got when setting up the account through Metamask. With the private key, we can access the account where we are authorized to sign the transaction. Next, we need Alchemy to connect to the Goerli test network. Using React modules: web3 and eth_accounts, specifying parameter values.

Figure 3 presents the Web page of our application, including the main functions of (1) *User Menu* which are: 'Create user', 'Add Document' and 'View & Approve Access'; and *Administration Menu* functions, which are: 'Request access', 'View Access Status'.

Meanwhile, Fig. 4 presents the transaction of a 'User creation' and Fig. 5 presents an access request to the user document.

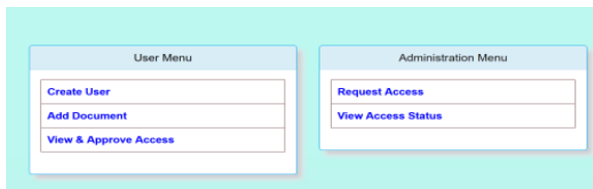


Figure 3. Web Page

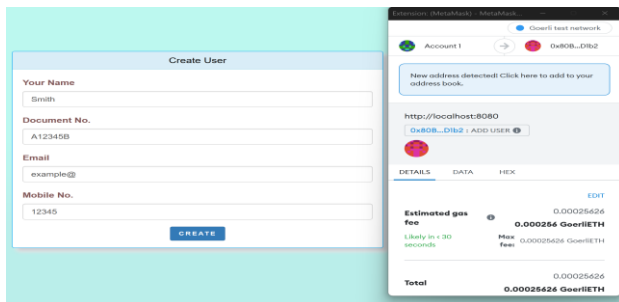


Figure 4. 'Create User' Transaction and Smart Contract Interaction

Add Document

Document No.

Name as per Document

Date of Birth as per Document

Address as Document

Attach Document

 No file selected.

Figure 5. Request access to the user's document

Security side: Data structures created by blockchain technology include built-in security features. It is founded on cryptographic, decentralized, and consensus concepts that guarantee the integrity of transactions. The consensus process ensures that each new block added to the Blockchain is the sole version of the truth recognized by all Blockchain nodes. A consensus protocol's goal is to let participants agree on the contents of a blockchain at a certain time (including new blocks). We used the proof-of-stake (PoS) consensus mechanism of the Goerli testnet, a platform for Web3 developers to test blockchain applications before releasing them on the Ethereum mainnet.

VI. CONCLUSION

In many ways, blockchain creates its utility and can be used to close loopholes in a variety of applications. Blockchain is even more advantageous when integrating with the public sector because both sectors have many common values, such as transparency. However, it is important to recognize that blockchain is not suitable for all applications. As a result, defining the requirement and the relationship between the desired use case and the technology is a prerequisite. Furthermore, blockchain may not be the best option when it comes to connecting to legacy systems or moving existing architecture from traditional systems to blockchain-based systems. When it comes to new use cases, blockchain shines. Development, prototyping, and trial-and-error use case experimentation will pave the way for blockchain to mature, just as traditional technology took time to stabilize the current market. This study proposes a

blockchain-based national identity management system. The study was guided by the many security ideas of blockchain technology, such as decentralization, proof-of-work, and anonymity, to name a few. These notions gave developers a solution to the problems posed by a centralized data management system. As a result, solutions proposed for secure identity creation and modification, identity authentication model, and identity discovery. Attack prevention also can be achieved by associating a single virtual identity with a physical identity, which prevents users from creating multiple identities on the system.

Despite the efforts made in this paper to meet the stated objectives, more work is required in the areas of identity reputation and third-party access and permission to user information. The handshake working methodology for identity discovery was inadequate and poorly executed. As a result, future research will focus on how to create a comprehensive and flexible handshake protocol that allows users to choose which attributes to reveal to others. The identity management system must have a reputation subsystem that reflects user behaviour in the real world and shows how often users communicate (transact).

Furthermore, as future work, we should also consider some challenges of adapting blockchain in ID management. We can mention here: (1) *data modification*, since it is very difficult to modify or delete it, (2) human errors, because the immutability feature of blockchain requires that information added to the database to be correct; (3) *power consumption*, due to the use of PoW consensus algorithm.

REFERENCES

- [1] Jacobs, B., Poll, E. Biometrics and Smart Cards in Identity Management. *In book: Innovating Government*, January 2011, pp. 419-438, DOI: 10.1007/978-90-6704-731-9_23.
- [2] World Economic Forum, Committed to Improving the State of the World. I Insight Report – Identity in a Digital World. A New Chapter in the Social Contract. 2018. Available at: https://www3.weforum.org/docs/WEF_INSIGHT_REPORT_Digital%20Identity.pdf.
- [3] El Haddouti, S., El Kettani, M. D.E.-C. Analysis of Identity Management Systems Using Blockchain technology. *Proc. of the International Conference on Advanced Technologies and Networking (CommNet)*, April 2019, pp. 1-7, published by IEEE, Online ISBN: 978-1-5386-8317-0, Print ISBN: 978-1-5386-8318-7, DOI: 10.1109/COMMNET.2019.8742375
- [4] Lopez, A. M. *Self-Sovereign Identity – The Future of Identity: Self-Sovereignty, Digital Wallets and Blockchain*. September 2020, DOI: 10.18235/002635, Available at: <https://publications.iadb.org/en/self-sovereign-identity-future-identity-self-sovereignty-digital-wallets-and-blockchain>.
- [5] Martinson, P. *Estonia the Digital Republic Secured by Blockchain*. 2019, Available at: <https://www.pwc.com/gx/en/services/legal/tech/assets/estonia-the-digital-republic-secured-by-blockchain.pdf>, Visited on September 2022.
- [6] Gelb, A., Clark, J. *Identification for Development: The Biometrics Revolution*. Center for Global Development, CDG, Washington, 2013, Available at: https://www.cgdev.org/sites/default/files/1426862_file_Biometric_ID_for_Development.pdf.
- [7] Tan, E., Mahula, S., Crompyoets, J. Blockchain Governance in the Public Sector: A Conceptual Framework for Public Management. *Government Information Quarterly*, Vol. 39, Issue 1, January 2022, pp. 101625 ISSN: 0740-640X, DOI: 10.1016/j.giq.2021.101625, Published by Elsevier.
- [8] *The Digital Society, Estonian e-Residency*. Available at: <https://e-estonia.com/eresidents/about/>, Latest access: October 2022
- [9] Sullivan, C., Burger, E. E-residency and Blockchain. *Computer Law & Security Review: The International Journal of Technology and Practice*, 2017. Published by Elsevier Ltd, ScienceDirect, Volume 33, Issue 4, pp.470-481, 2017, DOI: 10.1016/j.clsr.2017.03.016.
- [10] Miah, M. S. U., Hossain, M. S., Rupai, A. A. A. *Introduction to Blockchain – Blockchain for Data Analytics*. January 2019, Published by Cambridge Scholars Publishing, UK, ISBN (10): 1-5275-4429-X, ISBN (13): 978-1-5275-4429-1

- [11] Mohammed, A. H., Abdulateef, A. A., Abdulateef, I. A. Hyperledger, Ethereum and Blockchain Technology: A Short Overview. In *2021 3rd International Congress on Human-Computer Interaction, Optimization and Robotic Applications (HORA)*, June 2021, DOI: 10.1109/HORA52670.2021.9461294.
- [12] Sajana, P., Sindhu, M., Sethumudhavan, M. On Blockchain Applications: Hyperledger Fabric and Ethereum. *International Journal of Pure and Applied Mathematics*, Vol. 118, No. 18, 2018, pp. 2965-2970, ISSN online: 1314-3395, ISSN print: 1311-8080
- [13] Gopal, N., Biju, J. M., Prakash, V. V. Different Blockchain Platforms and Algorithms. In *International Research Journal of Engineering and Technology (IRJET)*, Vol. 6, No. 3, pp. 4853-4858, March 2019, e-ISSN: 2395-0056, p-ISSN: 2395-0072.
- [14] Zhou, H., Fard, A. M., Makanju, A. The State of Ethereum Smart Contracts Security: Vulnerabilities, Countermeasures, and Tool Support. *Journal of Cybersecurity and Privacy*, 2022, 2, pp. 358-378, DOI: 10.3390/jcp2020019.
- [15] Kushch, S., Baryshev, Y., Ranise, S. Blockchain Tree as a Solution for Distributed Storage of Personal ID Data and Document Access Control. *Sensor* 2022, Vol. 13, No.2, pp. 3621, Published by MDPI, DOI: 10.3390/s20133621.
- [16] Shome, A., Biswas, M., Datta, P., Bhowmik, A. A secured Smart National Identity Card Management Design Using Blockchain. In *2nd International Conference on Advanced Information and Communication Technology*, UIU, Dhaka, Bangladesh, November 2020, DOI: 20.1109/ICAICT51780.2020.9333487.
- [17] Tammpuu, P., Masso, A. Transnational Digital Identity as an Instrument for Global Digitalization Residency. *Information System Frontiers*, 2019, Vol. 21, No. 2, DOI: 10.1007/s10796-019-09908-y.
- [18] Mapperson, J. One Million South Koreans Now Have Blockchain Drivers Licences. August 2020. Available at: <https://cointelegraph.com/news/one-million-south-koreans-now-have-blockchain-drivers-licenses>.
- [19] Wang, H. Yang, D. Research and Development of Blockchain Recordkeeping at the National Archives at Korea. *Computers*, 2021, 10, 19, DOI: 10.3390/computers10080090.
- [20] ShoCard Inc. *ShoCard: Travel Identity for the Future – White Paper*. SITA. Available at: https://canada-ca.github.io/PCTF-CCP/docs/RelatedPolicies/SITA_Identity_2016.pdf, Accessed on: October 2022.
- [21] ShoCard Inc. Available: <https://shocard.com/>, Accessed on: October 2022.
- [22] Braendgaard, P. What is a uPort identity?. February 2017, Available at: <https://medium.com/uport/what-is-a-uport-identity-b790b065809c>, Latest accessed October 2022.
- [23] Young, A., and Verhulst, S. *Self Sovereign Identity for Government Services in Zug, Switzerland*. October 2018, Available at: <https://blockchan.ge/blockchange-government-services.pdf>.
- [24] Sovrin Foundation. Sovrin: A Protocol and Token for Self-Sovereign Identity and Decentralized Trust. A White Paper from the Sovrin Foundation Version 1.0. January 2018. Available at: <https://sovrin.org/wp-content/uploads/Sovrin-Protocol-and-Token-White-Paper.pdf>, latest access: October 2022.
- [25] Windley, Ph. J. Sovrin: An Identity Metasystem for Self-Sovereign Identity. *Frontiers in Blockchain*, Vol. 4, July 2021, DOI: 10.3389/fbloc.2021.626726.
- [26] AKSHI. Axfenda Digjitale e Shqiperise 2022-2026. Available at: <https://akshi.gov.al/wp-content/uploads/2022/06/vendim-2022-06-01-370-Agjenda-Digjitale-e-Shqiperise-22-26-dhe-plani-i-veprimit.pdf>, Latest access: October 2022.
- [27] E-Albania Portal. Available at: <https://e-albania.al/>, Latest access: October 2022.
- [28] Elezaj, O., Tole, Dh., Baci, N. Big Data in e-Government Environments: Albania as a Case Study. *Academic Journal of Interdisciplinary Studies*, Vol. 7, No.2, pp. 117-124, July 2018, Online ISSN: 2281-4612, Print ISSN: 2281-3993, DOI: 10.2478/ajis-2018-0052.
- [29] Prifti, V. Information Data Management in Big Data. Case study: E-Albania Government Portal. *International Scientific Journal "Industry 4.0"*, 2022, Vol. 7, No. 3, pp. 87-89, Online ISSN: 2524-997X, Print ISSN: 2534-8582.
- [30] Salliu, F. What is the Stage of Development of Albania in the Information Society?. *European Journal of Interdisciplinary Studies*. May-August 2015, Vol. 1, No. 2, Online ISSN: 2411-4138, Print ISSN: 2411-958X, pp.141-153.
- [31] Department of Justice Federal Bureau of Investigation and Cybersecurity & Infrastructure Agency, "Iranian State Actors Conduct Cyber Operations Against the Government of Albania", Joint Cybersecurity Advisory, September 2022, Available at: <https://www.ic3.gov/Media/News/2022/220921.pdf>, Accessed on October 2022.
- [32] ikubINFO Software Engineering, "Government Gateway Platform", Available at: <https://ikubinfo.al/government-gateway/>, Accessed on October 2022.