2021 11th IFIP International Conference on New Technologies, Mobility and Security (NTMS) | 978-1-6654-4399-9/20/$31.00 ©2021 IEEE | DOI: 10.1109/NTMS49979.2021.9432656

An Innovative and Decentralized Identity Framework Based on Blockchain Technology

Daniel Maldonado-Ruiz*, Jenny Torres*, Nour El Madhoun†, Mohamad Badra‡
*Departamento de Informática y Ciencias de la Computación, Facultad de Ingeniería en Sistemas Informáticos y Computación, Escuela Politécnica Nacional, Ecuador
†Security and System Laboratory, EPITA, 14-16 Rue Voltaire 94270 Le Kremlin-Bicêtre, France
‡College of Technological Innovation, Zayed University, P.O. Box 19282 Dubai, U.A.E
Email: {daniel.maldonado02, jenny.torres}@epn.edu.ec; nour.el-madhoun@epita.fr; mohamad.badra@zu.ac.ae

***Abstract*—Network users usually need a third party validation to prove that they are who they claim to be. Authentication systems mostly assume the existence of a Trusted Third Party (TTP) in the form of a Certificate Authority (CA) or as an authentication server. However, relying on a TTP implies that users do not directly manage their identities, but delegate this role to a third party. This intrinsic issue can generate trust concerns (e.g., identity theft), as well as privacy concerns towards the third party. The main objective of this research is to present an autonomous and independent solution where users can store their self created credentials without depending on TTPs. To this aim, the use of an TTP autonomous and independent network is needed, where users can manage and assess their identities themselves. In this paper, we propose the framework called Three Blockchains Identity Management with Elliptic Curve Cryptography (3BI-ECC). With our proposed framework, the users' identities are self-generated and validated by their owners. Moreover, it allows the users to customize the information they want to share with third parties.**

***Index Terms*—blockchain, certificate, ECC, identities, self-generated identity, cybersecurity.**

I. Introduction

Identity management is a crucial part of the Access Control process of networking applications. Nowadays, it is a real challenge for networks administrators to maintain an authentication procedure that allows the validation of an identity as in the real world, with specific documents or biometric features. In the context of networks such as the Internet where real identity validation does not exist or barely used, the attacker can easily impersonate users.

Many centralized systems are able to provide online identities and key management for users, always requiring multiple personal information from the user to maintain his identity and keep users' online tracking. Those systems are totally or partially decentralized, and the trust is not provided by the network itself but by other entities acting as a pseudo-decentralized Public Key Infrastructures (PKI), where the users cannot manage their identities by themselves.

978-1-6654-4399-9/21/31.00© 2021 $IEEE$

In the context of PKI, there is a need for Certificate Authorities (CA) to manage the identities. Trusting CAs can be an issue because they are sensitive to hijacking and, as a result, certificates generated and mainted by hijacked CAs cannot be trusted. Identity turned then into the weakest link between all the transactions on the network, since the attacker can pretend to be any user given that he can generate certificates validated by the hijacked CA.

Given this background, this research extends our ideas proposed on [1]: an architectural framework where, with blockchain as an interactive and independent storage system and ECC as a crypto-system, users will be able to create and manage their own identities without any TTP. The proposal presents a distributed and decentralized system that doesn't depend on any external entity. The validation of the network will be internal and immutable, making it a standalone network where users could store their self-created identities. Identities that are created by a mathematical calculation based on ECC over the uniqueness of the user. Uniqueness that will be intrinsic to the user in the validation of their identity.

The main contribution of this paper is to complement the design of an innovative architectural framework that, as was presented in [1], establishes a means by which the user can create and manage his identity by himself/herself. This paper includes the main designs of the architectural framework to be implemented and evaluated. The identity of the user will be strengthened in such a way that it will make it really hard for someone on the Internet to make it vulnerable or impersonate others. As for the user, he/she does not need any external authority to prove his/her identity to others. We note that there are scenarios where users wish to be fully known online or want to preserve their identities from other users to protect their privacy. Consequently, users should be able to decide how to manage their own identities, and to validate and store their self-generated key pairs, certificates and, ultimately, identities.

This paper is organized as follows. Section II presents

the relevant related works for managing identities without using centralized authorities. Section III describes the characteristics of our proposed 3BI-ECC framework, including the architectural prototype. In Section IV, we present our security analysis of the proposed framework and finally in Section V, we conclude the paper.

II. Related Work

Since its appearance with Bitcoin [2], Blockchain has changed the understanding of how information can be managed. The works of [3] shows the applications in which blockchain became a cornerstone, creating new ways for new systems needed to be developed and implemented [4]. Over the past few years, several implementations based on blockchain 2.0 and 3.0 have been achieved based on advantages of blockchain characteristics [5]. One of the main deployment of blockchain was in the context of Internet of Things (IoT) [6] [7], where the ledger is used to store, not only identities of the devices, but also other features that are used to analyze the behaviour of 'things'. In that case, blockchain is considered a strong ally for Big Data [8] [9] [10], where the blockchain can store a lot of information, either raw or through smart contracts, making the analysis of the data more easier and trustworthy. Some of the most recent applications of blockchain are dwvwloped in the context of implementing DNS and PKI systems [11] [12] [13] [14], where the data can be stored and accessed in a easy way. Blockchain was also used to implement and control e-voting systems [15] [16] [17], where the ledger offers a solution to eliminate electoral frauds and to provide all the auditory measurements that a voting system may need. However, this field has some security and trust issues in its implementation, especially in developing countries [18].

There are several examples of frameworks to generate identities and store them dynamically. Most of them focus on Vehicular Ad-Hoc Networks (VANET), the Internet of Vehicles (IoV) paradigm, and in general on the Internet of Things (IoT) paradigm.

Traditional scenarios on autonomous vehicle registration are Vehicle-to-Vehicle (V2V) and Vehicle-to-Infrastructure (V2I). In both cases, privacy-preserving and key interchange realms are mandatory for communication. Examples of this include specific developments like [19], or systems that involve a third trusted party ID-based cryptography with RSA [20], or a multi-certificate Public Key Infrastructure (PKI) [21]. All of these developments allow a certain portability and anonymity. On the other hand, RIDRA [22], a VANET's authentication framework, uses randomized pseudonyms for vehicle registration, to keep pseudo-anonymity. These pseudonyms are known by a Central Authority that validates every entity of the V2V network, where privacy preservation and non-repudiation for every vehicle are ensured. A similar approach is developed by ACPN networks [23], but with pseudonyms generated directly by the Central Authority. Also, by exploring the 'six degrees of separation' concept, Caballero [24] proposes an alternative approach by creating a self-managed VANET without any central authority, to detect and warn about abnormal traffic conditions through the cooperation among the involved users.

Within the IoT field, the main uses of the mentioned frameworks are in Wireless Sensors Networks (WSN) for use on both domestic and industrial IoT systems [25]. These systems, however, are vulnerable to attacks if they don't have an appropriate registration system. To deal with this problem, Antilizer [26] proposes a framework to isolate the compromised part of the network without limiting its information access. To manage decentralization, [27] proposes a framework where information is stored on different storage schemes, mainly on Peer-to-Peer networks. These schemes are dynamically defined by the network itself, with the necessary information stored in a self-management framework. These frameworks, however, can also work in a centralized way, focusing on reducing battery consumption on registration and communications. Examples like [28] work with standard cryptographic techniques and optimization algorithms to keep self-certification without having an excessive energy consumption in all registered devices.

The aforementioned paradigms of framework applications for device management are approximations of identity, in the form of smart contracts or classic certificates. These approximations, however, cannot manage and store people's credentials, because people's information are more complex than any device information. Despite all the possible similarities with people's identity management systems, the reviewed frameworks cannot be used to maintain users' identities, or generate them. Moreover, most decentralized frameworks depend on third-party entities, which is a limitation for the self-generation of identities.

Another important use of blockchain, is with PKIs. In existing literature, there are current implementations of blockchain with PKI as a trust network [29] or as Certificate Authorities Storage facility [30] or some kind of hybrid solution between CA's and PGP's Web of Trust (WoT) with all the features of the blockchain smart contracts [13] [31] [32] [33]. All these solutions, however, consider blockchain as a static ledger: an organized collection of data or accounts used for search and storage (with the obvious security features). This research takes the next step, by using blockchain not only as a ledger but as an integral part of the security; not only to store customized certificates but to generate them and avoid any third party at the same time.

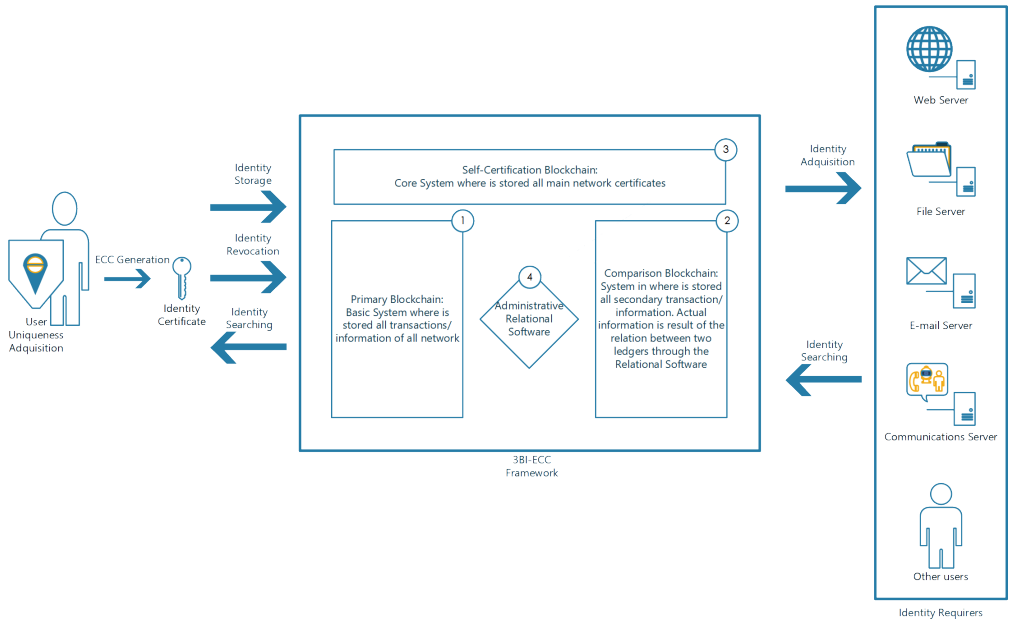

Fig. 1. 3BI-ECC Framework Diagram [1]

III. 3BI-ECC Framework Description

3BI-ECC is a system where, with three related blockchains, in tandem, and the ECC as a cryptographical tool set, users' identities are all self-generated and self-validated. This means that the identities will be validated by their owner, with the information belonging to the user who is willing to share it, without the intervention of any TTP.

Fig. 1 explains the main structure of 3BI-ECC framework, where the main interactions of all the parties in the system are shown, focusing on the features of the blockchain tandem. Every blockchain has its own function to improve the security of searching and storage of identities in the system. Fig. 1 illustrates the main features of every individual blockchain along with their main functions. We explain each of those main functions in the following Sections.

As an implementation scenario, we select the network architecture of Escuela Politécnica Nacional (EPN), because we have all the elements to prove all identity concepts and scenarios. Currently, the EPN network depends on different and external entities to manage their e-mails and their document manager. None of theses systems counts with an Identity validation. If any user requires to digitally sign any document, he/she must go to the national central certifying entity, Banco Central del Ecuador (BCE) to acquire a certificate. EPN's network is the best first scenario to design our proposal.

Fig. 2 describes the main architecture that provides a key pair creation and storage for EPN's students, professors, and workers, including the three blockchains as a unique Certificate Management System. The reason for the use of an EPN network as a test is to probe the capacity of the design, where the prototype needs to be developed in a case where identity is well known. EPN network system has two main applications that depend on the user's identity: E-Mail Server and Document Storage Server. The communication between these two systems and users are through the Certificate Manager:

- Self-Certification Blockchain: Core blockchain ((3) on Figs. 1 and 2) and main contribution of this research. This structure will generate all the certification systems for the other two blockchains, as it is explained in section III-A1.
- Primary Blockchain: Main storage system ((1) on Figs. 1 and 2), also known as Full Blockchain, where all identities will be stored when they are created. It is used as the main repository of the network.
- Comparison Blockchain: Secondary storage system ((2) on Figs. 1 and 2), also known as Revoked blockchain, where all revoked identities will be stored by the relational software. Users will never interact with this blockchain.
- Administrative Relational Software: Middleware software used in the searching and revocation steps to minimize the interaction with the primary blockchain and secure all the revocations of certificates ((4) on Figs. 1 and 2). It will be the front-end in the interaction between the network and users.

The main idea of this architecture is to validate each self-generated user certificate by the core blockchain,

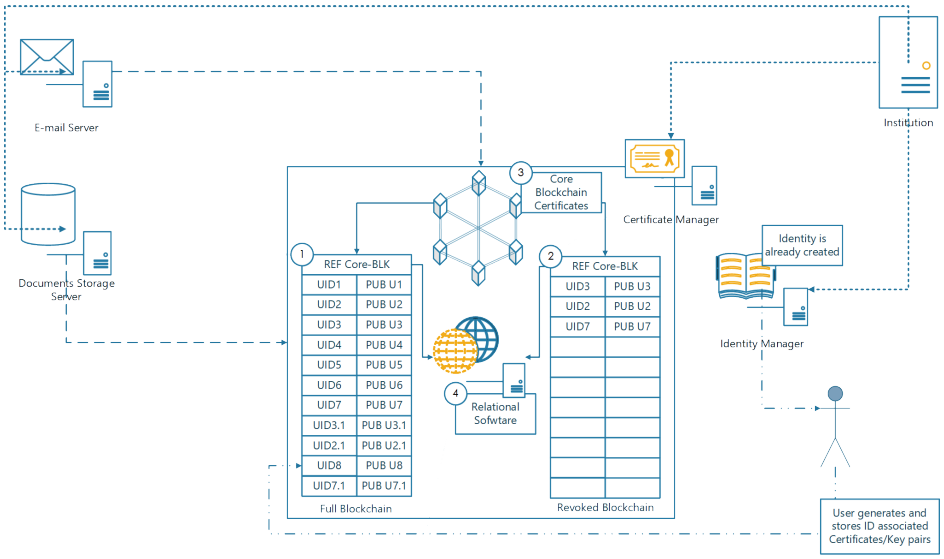

Fig. 2. Basic structure of proposed architecture

because the core will generate and store a set of certificates to be used as a PKI for the other services in the institution. EPN creates the identities for every person (through the Identity Manager) in the system, based on National Identity Service's information. The user needs to validate his own identity through his institutional e-mail provided by the EPN's Identity Manager.

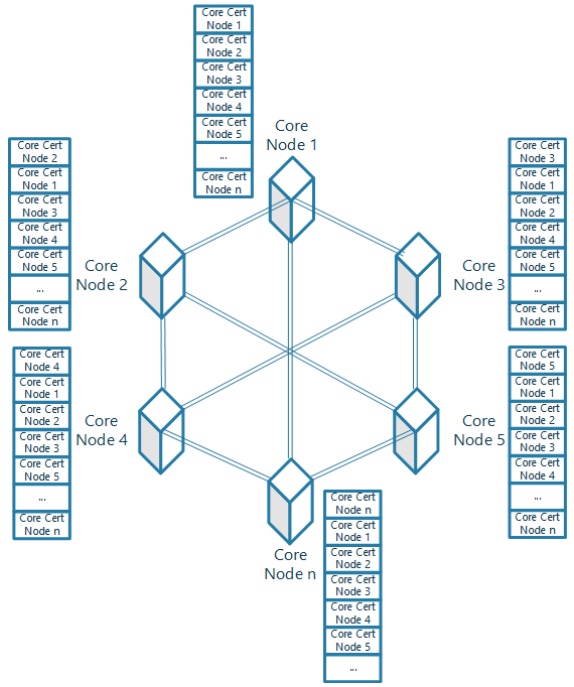

Fig. 3. Core Blockchain with every ledger copy.

A. Framework Initialization

1) Blockchain Initialization: Any identity system needs a kind of prime external validation. The idea of creating 3BI-ECC is that *we don't need this external validation*. To validate all the network by itself, a prime blockchain is used as a cornerstone. When the network is initialized, some random nodes are chosen to contain the core blockchain. Every node generates a key pair with random information and stores the self-signed public key in the form of a 'super' certificate from this core ledger. These public keys are stronger than the others used in the whole system. These certificates will become the ones that validate the other two blockchains as their primary records. Fig. 3 shows how this core blockchain is created in these selected nodes and the copy of the core ledger in every node. The purpose of this core blockchain is to generate an independent network where all the identities are validated internally.

Every blockchain has in its first block one of the 'super' certificates, stored on the Core Blockchain, which allows the validation of all the other stored keys and certificates in every ledger. To avoid any possible violation of Core blockchain, this first block will contain:

- The 'super' certificate that will sign all the user's keys.
- A hash of the block in the core blockchain where the certificate is stored.
- A hash of all core blockchain.

From time to time, it will be validated by the hashes that are correspondent with the original information, verifying that the network remains unchanged.

2) Identity Generation and Storage: To show how our framework can support decentralized identities, it is

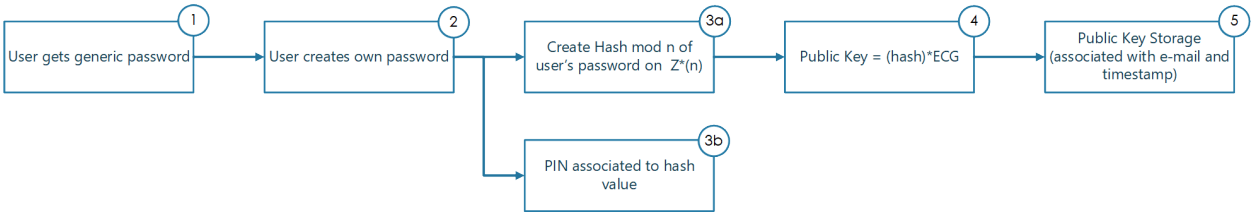

Fig. 4. Key pair creation and storage process.

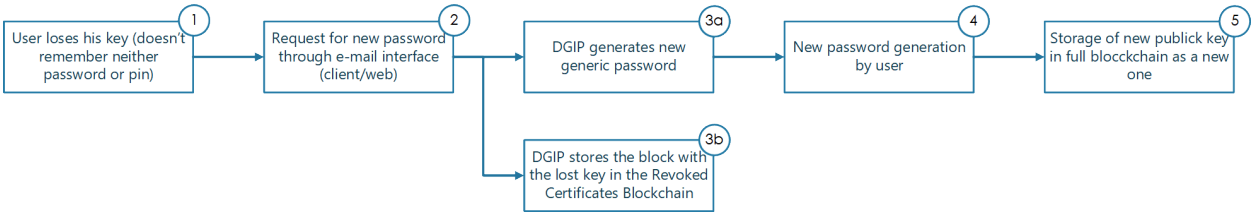

Fig. 5. Recovering password process

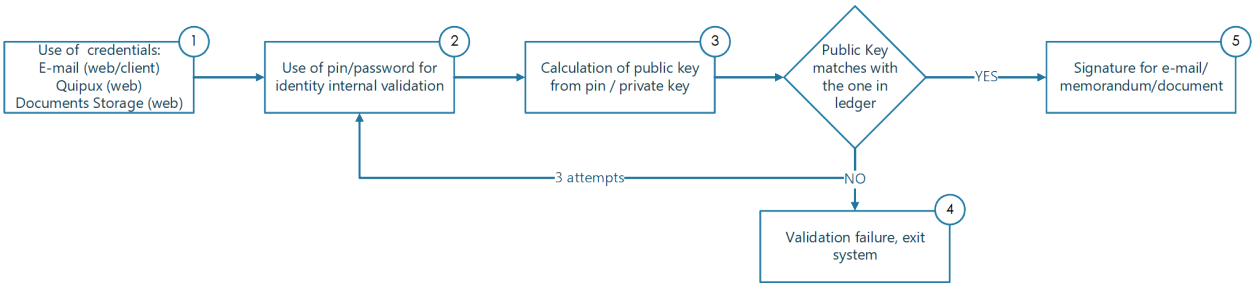

Fig. 6. Basic use of credentials in the communications system.

important to understand the features of each user that is to be represented in his identity. Each identity can have many features to represent an actual person, but one must define which ones are mandatory to define the said identity, and how they can be protected. Every identity must be validated by its owner, but that doesn't mean that a person shares all his real or complete information. The main idea of this research is to maintain self-generated and self-validated identities, where these identities show the amount of information the users need, or want, to share. The validation must come from both the user and the independent network. For this purpose, we aim to, not only develop a theoretical framework for this problem, but also to define a future artifact that stores self-generated identities so that people don't need a centralized authority to validate it.

To solve the self-generated identities problem, it is important to understand the security and the technical basis that will support the framework. Blockchain and its improvements, and ECC, are technologies that have been chosen to be the basis of this research. Both technologies are widely used, but together, they could improve the meaning of validation and the storage of information. Specially ECC, because its mathematical basis allows it to be understood not only in two dimensions but in n-dimensions if these curves maintain its abelian group features [34]. Nowadays, ECC is used by a lot of systems because its calculations and storage don't consume a lot of computational or memory and network resources.

Blockchain, on the other side, must be improved by modifying its inner features to support the storage and management of the main features of self-generated identities across the network. Modifications must not only come from main storage and decentralization, but from validation of the storage of information, which in classical blockchain design is called proof of work (POW). The blockchain system that will be implemented in this research will not store financial transactions but personal identity information in the form of a specific certificate, and that's why the POW must be different and, in some transactions, interactive.

B. Framework Functions

As it was shown in [1], these are three main functions of our framework:

1) Identity Storage: Through e-mail, users can create their own key pairs. E-mail's password becomes an

enabler, that, with ECC, is the seed of the key pair. For this research, e-mail is chosen because all the accounts are unique in the system and the credentials are used for all institutional services. Fig. 4 describes how users create key pairs from custom passwords of their e-mail account:

- When Direccion de Gestion de Información y Procesos (DGIP) creates a new account, a generic password is assigned for that account (1).
- When a user receives his credentials, he needs to change the generic password to one of his own (2).
- Using a hash function on this new password allows to obtain the private key for the user (3a) and allows the association with a 4 characters PIN (3b).
- The PIN is created to simplify the use of the key pair's system and will never be part of the private key or related with its calculation. With ECC, the public key is created from the private key (4) and stored in the decentralized blockchain created just for the public keys as customized certificates (5).

2) Identity Revocation: The public key is stored with the e-mail of the creator, creating a bond between key and e-mail as the main identity of the user. But passwords can be lost. Fig. 5 shows the procedure for recovering a lost password. It is similar to the way when creating a key pair for the first time: when the user's password is lost or compromised (1), he needs to ask for a new one from the Identity Management System (DGIP) through some defined interface (2), when the process shown in III-B1 starts over, including the storage of the new public key (3a) (4) (5). To differentiate revoked keys from the valid ones, the Revoked blockchain will store all the revoked keys, no matter the cause of revocation (3b). None of these blockchains are open for consultation by users at any point. Only the middleware system that compares both blockchains to determine which certificate is valid (the one that is only stored in the Full Blockchain). Passwords and/or PINs are the way to validate the relationship of keys because the password's hash is the private part of the pair.

3) Identity Searching: Fig. 6 shows how to use this system as follows:

- The idea is that a key pair can be used to sign or cipher emails, memorandums, stored documents or any other systems related to the institution (1).
- For any of these uses, a password or PIN must be used to validate identity. The PIN will be used on non-critical systems like the consultation of class schedules and the distribution of classrooms. Passwords will be used in critical systems like e-mail or modification of personal information (inscriptions, payment information, grades) (2).
- The system automatically uses the public or the private key depending on the action requested by the user (3).
- In all cases, the hash must be calculated from a password and the public key must be calculated from this hash in order to validate the stored data in the blockchains and showed by the middleware. If the password/PIN generates a key that matches the stored one, the action is performed (5).
- The user will have three attempts to validate his credentials after which the system closes and informs DGIP of an alleged identity theft (4).

IV. Analysis

A. Security Analysis

The parameters considered when analysing the security of the proposed framework are: identity privacy, node identification, attacks and key agreement.

1) Identity Privacy: Another main purpose of this research is to achieve a way to keep all the users identities secure from any internal or external malicious party. As mentioned in Section III, only the public part of the key pair will be stored in any user blockchain, and when a user needs a key to perform some action, the search will be made by the middleware software, so any user will interact with the blockchains at any time. When users need to sign a document, the system will calculate the on-the-fly private key, without storing it. So only the owner can generate it. That means that the uniqueness of the user is used to create the key, which maintains the privacy of all the system.

2) Node Identification: Every node in the network needs to have the same features to store the two main blockchains. There is no difference between the nodes that store the data blockchains and the ones that store the three blockchains. Every node, however, will have an internal identification to establish internal communications between nodes. This identification will only exist for inter-node communications. Users will communicate with the blockchain through an unified network name. For the users, the store-searching identities network will be used as one entity, making the framework mechanisms more transparent.

3) Attacks: The blockchain decentralization and its inner features is one of the most important methods to avoid attacks over the proposed framework. Every node will, at all times, have both ledgers to avoid any tampering attack. When a unique point of failure exists, it is easier to impersonate that server and fill the network with fraudulent certificates. 3BI-ECC, having its own Proof of Work, prevents any third party from creating a new branch and impersonating the three blockchains.

On the other hand, users cannot have access to modify their own certificates (the stored public key) or to use their private key without the system (the keys are calculated on-the-fly, that's why the private key will not

be stored in any part of the system). And even if a user password is stolen, the attacker will only have access to the stolen identity, the system cannot be modified by a user.

4) Type of Certificates: One of the achievements of this proposal is to avoid relying on any TTP (or even on the storage ledgers) to validate the identity of any user. That is why using X.509-kind of certificates doesn't create any additional value on the present proposal. To solve this, it is intended to create a new type of certificate that can manage an actual identity and not only the chain of CAs that could validate a specific identity. To create this new type of certificates, it is important to define the specific features to make the identity unique in the network. That doesn't mean that users need to give a lot of information about themselves, but the minimum amount of data that can make this uniqueness possible.

For the first example of this proposal, EPN network, the minimum amount of information needed is the name of the user and his email. This information will be stored in the new certificate as fields that would be filled by the identity creator and be associated with the public key that is generated as described in Section III. Every time a user generates a new certificate, the identity information will be cloned from the invalid certificate and associated with the new public key. To modify the non-critical information in the certificate, the system will consider that as a new certificate creation, following the explained steps.

B. Efficiency analysis

With our new framework and architecture, our proposed solution can ensure the following features that are related to the identities in the networks: Decentralization of identity management, self-validation of users and the improvements of blockchain as a concept. The most important achievement is to allow users in the network to use their uniqueness to generate their own personal credentials. Uniqueness could be represented as an e-mail, some specific information or some biometrical features. It means that in any point of communication, users need a third party for the creation of their identity. In this solution, we use a pseudo created identity (an institutional e-mail) because the main objective is to prove that the network architecture works with an identity and a unique feature of each identity. That is why the systems use the password as a seed for the key pair, where some calculations are hidden from the user. The purpose is not to only provide the self-validation, but also the decentralization of every identity in the network. Systems where users can store certificates, smart contracts or key pairs are not enough for fully decentralized communications. It is necessary to allow users to define themselves in the network, with their own features, to avoid impersonations over the network. Using users' uniqueness allows avoiding problems like the ones reported in PGP's WoT [35], where any user can use any name without restriction.

V. Conclusion

Despite the existence of several frameworks and pseudo frameworks for Identity Management that allow ad-hoc and permanent communications, none of them has been implemented to be fully independent and to generate and maintain on-line user identities. Most of these frameworks cannot handle people's certificates, even when a lot of devices are using some forms of X.509 certificates. The differences between a person and, for example, a laundry machine are critical in these frameworks. Also, despite the evolution in security and privacy, identity is still the weakest link between on-line services and users. That is because most of the systems' security relies on the user's capabilities to protect his own identity (tokens, passwords, etc.). Social engineering attacks and ransomware viruses are proof that it is still difficult to secure a user effectively. That is why part of the security of this research is with the user's uniqueness, but not with the user intervention. Improving blockchain mechanisms, in both public and private distributions, is part of the evolution of independent decentralized technologies and of the way Internet is understood nowadays. In this paper, we described a solution to enhance the networking applications by considering Blockchain-based identity management for Authentication and Access Control processes, while managing the lifecycle of these identities.

References

[1] D. Maldonado-Ruiz, J. Torres, and N. El Madhoun, "3BI-ECC: a Decentralized Identity Framework Based on Blockchain Technology and Elliptic Curve Cryptography," *2020 2nd Conference on Blockchain Research & Applications for Innovative Networks and Services (BRAINS)*, pp. 45–46, sep 2020.

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

[3] D. Di Francesco Maesa and P. Mori, "Blockchain 3.0 applications survey," *Journal of Parallel and Distributed Computing*, vol. 138, pp. 99–114, apr 2020.

[4] N. El Madhoun, J. Hatin, and E. Bertin, "A decision tree for building it applications," *Annals of Telecommunications*, pp. 1–14, 2020.

[5] D. Maldonado-Ruiz, M. Badra, N. El Madhoun, and J. Torres, "Secure and internet-less connectivity to a blockchain network for limited connectivity bank users," *MSPN 2020: International Conference on Mobile, Secure and Programmable Networking*, 2020.

[6] A. Dorri, S. S. Kanhere, R. Jurdak, and P. Gauravaram, "Blockchain for IoT security and privacy: The case study of a smart home," *2017 IEEE International Conference on Pervasive Computing and Communications Workshops (PerCom Workshops)*, pp. 618–623, mar 2017.

[7] D. W. Kravitz and J. Cooper, "Securing user identity and transactions symbiotically: IoT meets blockchain," *2017 Global Internet of Things Summit (GIoTS)*, pp. 1–6, jun 2017.

[8] S. Bragagnolo, M. Marra, G. Polito, and E. Gonzalez Boix, "Towards scalable blockchain analysis," *2019 IEEE/ACM 2nd International Workshop on Emerging Trends in Software Engineering for Blockchain (WETSEB)*, pp. 1–7, May 2019.

[9] L. Yue, H. Junqin, Q. Shengzhi, and W. Ruijin, "Big data model of security sharing based on blockchain," *2017 3rd International Conference on Big Data Computing and Communications (BIGCOM)*, pp. 117–121, Aug 2017.

[10] E. Bandara, W. K. NG, K. De Soysa, N. Fernando, S. Tharaka, P. Maurakirinathan, and N. Jayasuriya, "Mystiko—blockchain meets big data," *2018 IEEE International Conference on Big Data (Big Data)*, pp. 3024–3032, Dec 2018.

[11] H. Tewari, A. Hughes, S. Weber, and T. Barry, "X509Cloud — Framework for a ubiquitous PKI," *MILCOM 2017 - 2017 IEEE Military Communications Conference (MILCOM)*, pp. 225–230, 2017.

[12] E. Karaarslan and E. Adiguzel, "Blockchain Based DNS and PKI Solutions," *IEEE Communications Standards Magazine*, vol. 2, no. 3, pp. 52–57, sep 2018.

[13] L. Axon and M. Goldsmith, "PB-PKI : a Privacy-Aware Blockchain-Based PKI," *Proceedings of the 14th International Joint Conference on e-Business and Telecommunications (ICETE 2017)*, vol. 4, pp. 311 —- 318, 2017.

[14] J. Won, A. Singla, E. Bertino, and G. Bollella, "Decentralized Public Key Infrastructure for Internet-of-Things," *MILCOM 2018 - 2018 IEEE Military Communications Conference (MILCOM)*, pp. 907–913, oct 2018.

[15] B. Shahzad and J. Crowcroft, "Trustworthy Electronic Voting Using Adjusted Blockchain Technology," *IEEE Access*, vol. 7, pp. 24 477–24 488, 2019.

[16] L. Carr, A. J. Newtson, and J. Joshi, "Towards Modernizing the Future of American Voting," *2018 IEEE 4th International Conference on Collaboration and Internet Computing (CIC)*, pp. 130–135, oct 2018.

[17] R. Hanifatunnisa and B. Rahardjo, "Blockchain based e-voting recording system design," *2017 11th International Conference on Telecommunication Systems Services and Applications (TSSA)*, pp. 1–6, oct 2017.

[18] C. G. Harris, "The risks and dangers of relying on blockchain technology in underdeveloped countries," *NOMS - IEEE/IFIP Network Operations and Management Symposium*, pp. 1–4, apr 2018.

[19] Y. Liu, Y. Wang, and G. Chang, "Efficient Privacy-Preserving Dual Authentication and Key Agreement Scheme for Secure V2V Communications in an IoV Paradigm," *IEEE Transactions on Intelligent Transportation Systems*, vol. 18, no. 10, pp. 2740–2749, oct 2017.

[20] J. Choi and S. Jung, "A Security Framework with Strong Non-Repudiation and Privacy in VANETs," *2009 6th IEEE Consumer Communications and Networking Conference*, pp. 1–5, jan 2009.

[21] W.-T. Zhu and J. Lin, "Generating Correlated Digital Certificates: Framework and Applications," *IEEE Transactions on Information Forensics and Security*, vol. 11, no. 6, pp. 1117–1127, jun 2016.

[22] C. Sun, J. Liu, Y. Jie, Y. Ma, and J. Ma, "Ridra: A Rigorous Decentralized Randomized Authentication in VANETs," *IEEE Access*, vol. 6, pp. 1–1, 2018.

[23] J. Li, H. Lu, and M. Guizani, "ACPN: A Novel Authentication Framework with Conditional Privacy-Preservation and Non-Repudiation for VANETs," *IEEE Transactions on Parallel and Distributed Systems*, vol. 26, no. 4, pp. 938–948, apr 2015.

[24] C. Caballero-Gil, J. Molina-Gil, P. Caballero-Gil, F. Martín-Fernández, and D. Yanes-García, "Introducing secure and self-organized vehicular ad-hoc networks," *Proceedings of the 12th International Conference on Computer Systems and Technologies - CompSysTech '11*, pp. 454–459, 2011.

[25] A.-R. Sadeghi, C. Wachsmann, and M. Waidner, "Security and privacy challenges in industrial internet of things," *Proceedings of the 52nd Annual Design Automation Conference on - DAC '15*, vol. 17, pp. 1–6, 2015.

[26] I. Tomić, P.-Y. Chen, M. J. Breza, and J. A. McCann, "Antilizer: Run Time Self-Healing Security for Wireless Sensor Networks," *Proceedings of the 15th EAI International Conference on Mobile and Ubiquitous Systems: Computing, Networking and Services - MobiQuitous '18*, pp. 107–116, 2018.

[27] R. Makhloufi, G. Doyen, G. Bonnet, and D. Gaïti, "Towards self-adaptive management frameworks: The case of aggregated information monitoring," *2011 7th International Conference on Network and Service Management, CNSM 2011*, pp. 474–478, 2011.

[28] M. O. Ozmen and A. A. Yavuz, "Low-Cost Standard Public Key Cryptography Services for Wireless IoT Systems," *Proceedings of the 2017 Workshop on Internet of Things Security and Privacy - IoTS&P '17*, pp. 65–70, 2017.

[29] K. Han and S. O. Hwang, "A PKI without TTP based on conditional trust in blockchain," *Neural Computing and Applications*, vol. 6, aug 2019.

[30] Z. Wan, Z. Guan, F. Zhuo, and H. Xian, "BKI: Towards Accountable and Decentralized Public-Key Infrastructure with Blockchain," *Lecture Notes of the Institute for Computer Sciences, Social-Informatics and Telecommunications Engineering, LNICST*, vol. 238, pp. 644–658, 2018.

[31] C. Patsonakis, K. Samari, M. Roussopoulos, and A. Kiayias, "Towards a smart contract-based, decentralized, public-key infrastructure," *International Conference on Cryptology and Network Security*, pp. 299–321, 2017.

[32] P. Boontaetae, A. Sangpetch, and O. Sangpetch, "RDI: Real Digital Identity Based on Decentralized PKI," *2018 22nd International Computer Science and Engineering Conference (ICSEC)*, pp. 1–6, nov 2018.

[33] J. Chen, S. Yao, Q. Yuan, K. He, S. Ji, and R. Du, "CertChain: Public and Efficient Certificate Audit Based on Blockchain for TLS Connections," *IEEE INFOCOM 2018 - IEEE Conference on Computer Communications*, pp. 2060–2068, apr 2018.

[34] A. Sonnino and G. Sonnino, "Elliptic-Curves Cryptography on High-Dimensional Surfaces," *International Journal of Advanced Engineering Research and Science*, vol. 4, no. 2, pp. 140–146, 2017.

[35] D. Maldonado-Ruiz, E. Loza-Aguirre, and J. Torres, "A Proposal for an Improved Distributed Architecture for OpenPGP's Web of Trust," *2018 International Conference on Computational Science and Computational Intelligence (CSCI)*, pp. 77–81, dec 2018.