3BI-ECC: a Decentralized Identity Framework Based on Blockchain Technology and Elliptic Curve Cryptography

Daniel Maldonado-Ruiz*, Jenny Torres*, Nour El Madhoun†
*Departamento de Informática y Ciencias de la Computación, Facultad de Sistemas, Escuela Politécnica Nacional, Ecuador
†LISITE Laboratory, ISEP, 10 Rue de Vanves 92130 Issy-les-Moulineaux, France
Email: {daniel.maldonado02, jenny.torres}@epn.edu.ec; nour.el-madhoun@isep.fr

***Abstract*—Most of the authentication protocols assume the existence of a Trusted Third Party (TTP) in the form of a Certificate Authority or as an authentication server. The main objective of this research is to present an autonomous solution where users could store their credentials, without depending on TTPs. For this, the use of an autonomous network is imperative, where users could use their uniqueness in order to identify themselves. We propose the framework "Three Blockchains Identity Management with Elliptic Curve Cryptography (3BI-ECC)". Our proposed framework is a decentralize identity management system where users' identities are self-generated.**

***Index Terms*—blockchain, elliptic curves cryptography, self-generated certificates, self-generated identity, cybersecurity**

I. Introduction

Nowadays, networks still cannot provide an authentication procedure which validate an identity as in the real world. In the Internet, any user can impersonate others just by registering a name. These days, there are many centralized systems that provide online identities and key management for users, but these systems require multiple personal information from the user to maintain his identity and keep a guaranteed online tracking, like VeriSign or other classic certificate authorities. In addition, there are other systems that are totally or partially decentralized, where the only trust is provided by other users, and not by the network itself like Decentralized Public Key Infrastructure (PKI) [1]. Also, besides the cryptocurrency and smart contracts applications, there are some other implementations of blockchain. One of the main uses is with Internet of Things (IoT), because the ledger can store not only identities of the devices but other features that are used to analyze the behaviour of the 'things'. In that case, blockchain is a strong ally of Big Data [2], because can store a lots of information, either raw or through smart contracts, making the analysis easier and more trustable. In all cases, the identity problem remains. Some kind of TTP is always needed: a centralized system tells the user who he is, or the user is exposed to identity theft. This research proposes an architectural framework where, with blockchain as a interactive storage system and ECC as a cryptographical suite, users will be allowed to create and manage their own identities without any TTP. A distributed and decentralized system is proposed to validate itself, making it a standalone network where users can create and manage his own identity and can store their own identities. The identity of the user will be created by a mathematical calculation based on ECC over the uniqueness of the user; thus, becoming hard for someone on the Internet to vulnerable or steal it. Using users' uniqueness allows avoiding problems like the ones documented in PGP's WoT [3] where any user could use any name without restriction.

II. 3BI-ECC Framework

Fig. 1 shows the main structure of our proposed 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 in order to improve the security of searching and storage of identities in the system.

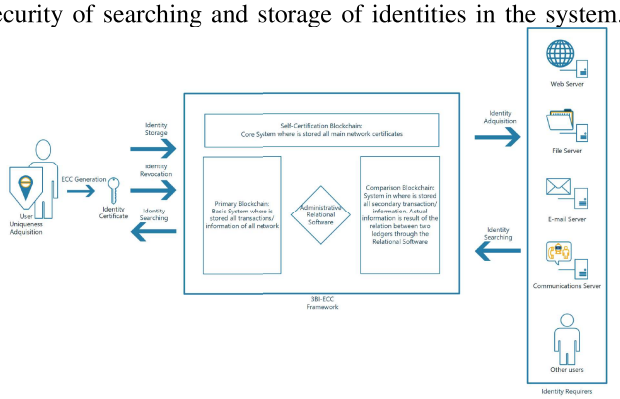

Fig. 1. 3BI-ECC Framework Diagram

Fig. 2. Key pair creation and storage process.

Fig. 3. Recovering password process

Core Blockchain Initialization. To validate all the network by itself, a prime blockchain is used as a cornerstone. When

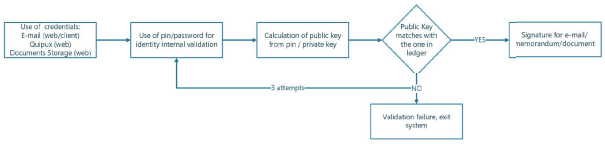

Fig. 4. Basic use of credentials in the enterprise communications system.

the network is initialized, some nodes are chosen in order to contain this core blockchain. Every node generates a key pair with random information and stores the self-signed public key in a customized certificate in this core ledger. These certificates validate the other blockchains as their primary records.

Identity Storage. Fig. 2 describes how users create key pairs. When a new account is created, a need-to-be-changed generic password is assigned. The hash obtained of the new password allows to create the private key for the user and to associate it with a PIN. The PIN simplify the user authentication in related systems and is not part of the private key. Applying ECC on the private one, the public key is created and stored in the primary blockchain. The searches of certificates are performed by a relational middleware software, which also do the revocations. Every identity blockchain has in its first block a certificate from the core blockchain, which allows the validation of all the other stored keys and certificates.

Identity revocation. The public key is associated with the e-mail, creating the main identity of the user. Fig. 3 shows the recovering a lost password. It is similar to creating a key pair the first time, including the storage. In order to differentiate revoked keys from the valid ones, the second blockchain, called revoked blockchain, will store all the revoked keys. None of these blockchains are open for users. 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.

Identity searching. Fig. 4 shows that a key pair can be used to sign or cipher. The PIN is used on non-critical systems like class schedules or the distribution of classrooms. Passwords are used in critical systems like e-mail, inscriptions, payment information. 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, all of these on-the-fly.

III. Framework features

Full integration with current secure identity and communication infrastructures. A system can be integrated to the 3BI-ECC, in order to create, store and use all the credentials. Users need the e-mail or the document manager application to access to the public key storage. **Specific algorithms for deploy core and identity blockchains in the network**. It is necessary to define an algorithm that allows concurrent blockchains working in the same node. All of these ledgers have no relation between them. **Password managing for multiple changes without modifying the identity**. User's password is required, as the seed of the entire security system. When this password is lost, the change of it renews all the security features. **Transparency and security for the user**. Even when most of the security mechanisms are transparent to the users, they need to learn how to create a efficient password for the system and how to protect their credentials.

IV. Analysis

Identity Privacy. The public key will be stored in both blockchains when it is revoked, and when a user needs a key, the search is made by the middleware software, so any user can interact with the blockchains in any time. When users need to sign any document, the system will calculate on-the-fly the private key, without storing it, so only the owner could generate it. That means that in the user uniqueness used to create the key remains private for all the system.

Node Identification. Every node will have an internal identification in order to establish communications between nodes. Users will communicate with the blockchain through an unified network name. For the users, the store-searching identities network will be used by a unique identifier, making the framework mechanisms all transparent.

Attacks. The blockchain decentralization and its inner features is one of the most important methods to avoid attacks over the proposed framework. Every node have at any time the two ledgers to avoid any tampering attack. When exist a unique point of failure it is easier to impersonate that server and fill the network with fraudulent certificates. 3BI-ECC, having its own Proof of Work, avoids that any third party could create a new branch and impersonate the three blockchains.

Type of Certificates. A new type of certificate must be created which could manage an actual identity and not only the chain of CAs that could validate a specific identity. In order to create this new type of certificate it is important to define which specific features define an identity that could be unique in all the network.

V. Conclusion

Despite the existence of several frameworks and pseudo framework which allow ad-hoc and permanent communications, no one has been implemented to generate and maintain on-line user identities, nor on the Internet or Intranets. That is why part of the security of this research is with user's uniqueness, but not with the user intervention. Technologically it is important to notice that there are not implementations of blockchain and ECC to generate and storage identity certificates and key pairs.

References

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

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

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