IOSR Journal of Computer Engineering (IOSR-JCE)
e-ISSN: 2278-0661,p-ISSN: 2278-8727 PP 53-55
www.iosrjournals.org

A Blockchain-Based Decentralised Identity Framework using Elliptic Curve Cryptography

S.Suganthi[1], Dr.T.Sree Kala[2]
[1.]Research Scholar, Department of Computer Science,VISTAS, Chennai,India
[2.] Associate Professor, Department of Computer Science,VISTAS, Chennai,India.
[1.]dinesh.suganthi@gmail.com,[2.]sreekalatm@gmail.com

Abstract—*The vast majority of authentication methods depend on the existence of TTP (Trusted Third Party), which might be in the authentication server or Certificate Authority form. The major objective of this study is to provide an independent mechanism through which users may safely retain credentials without needing to rely on TTPs. This can only be achieved via the usage of a decentralised network, where each user's individuality serves as their login ID. Our proposed framework is a decentralised identity management system in which users generate their own identities using Elliptic curve cryptography(ECC).*

Keywords—Block Chain; Self generated identity; Elliptic Curve Cryptography; Self generated certificates; Cybersecurity;

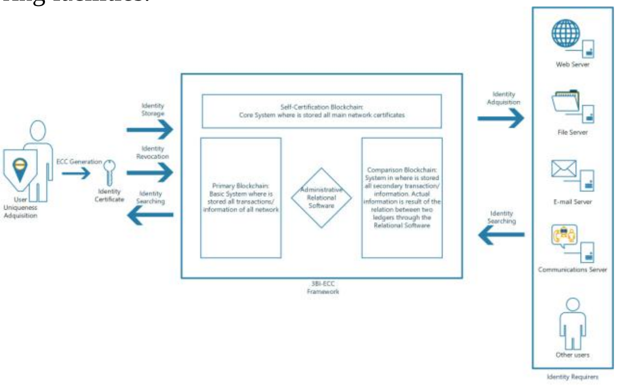
I. INTRODUCTION

At the present time, networks do not have an authentication mechanism that can verify an individual's identity in the same way which it does in the physical world. Anyone may attempt to register a name and use it to fool others online. Centralized systems including VeriSign or other conventional certificate authority collect extra personal data from the user to ensure his authenticity and keep an assured online monitoring in order to give digital identities as well as key management for customers. Other systems, including Decentralized Public Key Infrastructure (PKI) [1], are either fully or partly decentralised, with the users themselves being the sole source of trust rather than the network itself. There are many possible uses for blockchain technology outside the realms of digital money and smart contracts. The Internet of Things (IoT) is a popular use case for ledgers because they can be used to record data about connected devices, including metadata that can be utilised to understand how those devices function. As it can store vast amounts of data in its raw or smart contract forms, blockchain is potent ally of Big Data [2] in this context. This facilitates more reliable analysis. The problem of identification remains a constant. A TTP is always required since either the user's real identity is revealed by a centralised system or the user is vulnerable to identity theft. This study presents an architectural framework for the generation of digital assets utilising ECC as a cryptography suite and blockchain as an interactive storage system.

A mathematical procedure using ECC will be performed over the user's uniqueness to produce user's identity, making it impossible to misuse or steal. By relying on users' individuality, you may avoid problems like those detailed in PGP's WoT [3], where any user is free to choose whatever name they want.

II. 3BI-ECCFRAMEWORK

Our framework's main components are shown in Fig. 1, with the focus being on the blockchain tandem and the interactions between all system stakeholders. Each blockchain performs a unique task to fortify the system's identification search and storing facilities.


User Uniqueness Adquisition
ECC Generation
Identity Certificate
Identity Storage
Identity Revocation
Identity Searching
Self-Certification Blockchain: Core System where is stored all main network certificates
Primary Blockchain: Basic System where is stored all transactions/ information of all network
Administrative Relational Software
Comparison Blockchain: System in where is stored all secondary transaction/ information. Actual information is result of the relation between two ledgers through the Relational Software
3BI-ECC Framework
Identity Adquisition
Identity Searching
Web Server
File Server
E-mail Server
Communications Server
Other users
Identity Requirers

“Fig.1.3BI-ECCFrameworkDiagram

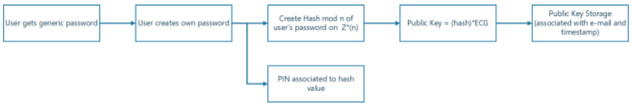

User gets generic password
User creates own password
Create Hash mod n of user's password on Z*(n)
Public Key = (hash)*ECG
Public Key Storage (associated with e-mail and timestamp)
PIN associated to hash value

Fig.2.Keypaircreationandstorage process.

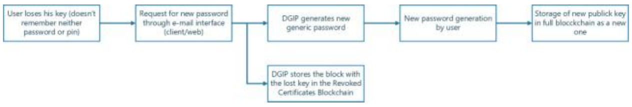

User loses his key (doesn't remember neither password or pin)
Request for new password through e-mail interface (client/web)
DGIP generates new generic password
New password generation by user
Storage of new publick key in full blocckchain as a new one
DGIP stores the block with the lost key in the Revoked Certificates Blockchain

Fig.3.Recovering password process

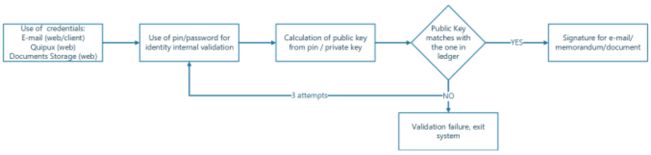

Use of credentials: E-mail (web/client) Quipux (web) Documents Storage (web)
Use of pin/password for identity internal validation
Calculation of public key from pin / private key
Public Key matches with the one in ledger
YES
Signature for e-mail/ memorandum/document
3 attempts
NO
Validation failure, exit system

Fig.4.Basicuse of credentials in the enter prise communications system."

Initialization of the fundamental blockchain.

The integrity of the network is checked against a primary blockchain. When a network is first set up, a subset of nodes are selected to host the primary blockchain. Each participant in this central ledger creates a private/public key pair using random data and stores its self-signed public key in a digital certificate. These certifications act as master records for all other blockchains.

Identity Storage. The creation of a key pair is seen in Figure 2 above. A default, changeable password is generated for every new account. One may generate a private key for a user as well as link it to a PIN by hashing their newly-obtained password. The PIN is used to authenticate the user in connected systems, but it is not part of the private key itself. The public key is produced and kept on the main blockchain utilizing ECC on the private one. In addition to managing disqualifications, relational middleware software also does certificate searches. To ensure the validity of all other certificates and keys, the first block of every identity blockchain includes a certificate from the main blockchain.

Identity Revoction. The user's main identification is comprised of the public key and their email address. The steps required to reset a lost password are shown in Figure 3. This is analogous to making a pair of keys. Now incorporating long-term storage for the first time. The second blockchain, appropriately termed the "revoked blockchain," is where all keys that have been revoked will be stored. The public cannot access any of these blockchains at this time. Since the hash of the password is the secret half of the pair, passwords and/or PINs are utilized to verify the authenticity of key exchanges.

Identity SearchingA key pair, such as the one seen in Fig. 4, may be used to cypher or sign a message. Class scheduling and classroom allocation are two examples of non-critical systems where the PIN is employed. Passwords are used for very important things including registration, email, and financial transactions. In order to verify the accuracy of the information recorded in blockchains, it is always necessary to first compute the hash from the password and then derive the public key from the hash.

III. Features of the Framework

Complete integration with existing secure identity and communication infrastructure. The 3BI-ECC may be linked with a system to generate, store, and utilise any credentials. Email or a document management programme is required to access the public key vault. The network utilises specialised algorithms for launching core and identity blockchains. To have many blockchains operate in parallel on the same node, an algorithm that defines this is required. Not one of these books corresponds to another. Handling repeated password changes without compromising security. The user's password is essential since it serves as the security system's germinal. When this password is forgotten, changing it renews all thesecurity features. The user benefits from transparency and security. Even if most security features are translucent to users, they must learn how to create an effective system password and how they can preserve their credentials.

IV. Analysis

Identity Privacy. A revoked public key is recorded on both blockchains, and when a user requests a new key, the middleware checks both chains to see whether it matches. When signing a document, the system generates a private key on the fly without saving the original, so that only the owner may use it. That is, the system as a whole is not privy to the user's individuality that was utilised to produce the key.

Identification of nodes. Every node will have its own unique identifier to use in establishing connections with other nodes. There will be a single network name that all users will use to communicate with the blockchain.

Users will use a network of identities for searching stores, with the goal of making the framework's workings transparent.

Attacks. Blockchain's decentralized nature and its built-in security features are among the most essential approaches for protecting the suggested framework. Each node has permanent access to both ledgers, which makes manipulation very difficult. If there is just one server in the chain, then it's simple for an attacker to pose as it and flood the network with fake certificates. The unique Proof of Work used by 3BI-ECC makes it impossible for a malicious actor to fork the network and pretend to be one of the three blockchains.

Types of Certificate. Rather of relying only on a series of CAs to confirm an individual's identification, a new kind of certificate is required. In order to create this novel certification, it is necessary to determine which certain characteristics constitute an identity that may be unique throughout the network.

V. Conclusion

Numerous frameworks as well as pseudo-frameworks have been built to facilitate ad hoc and persistent communication, but none have been used to create and manage users' identities in the online world. Therefore, although the fact that each user is different helps make this research more secure, the participation of individual users does not. Furthermore, there is currently no blockchain or ECC implementation which can be used to create and store key pairs and identity certificates.

References

[1]. E. Karaarslan and E. Adiguzel, “Blockchain Based DNS and PKI So- lutions,” 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. Mau- rakirinathan, 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.

[4]. C. Xu, H. Yang, Q. Yu and Z. Li,“Trusted and flexible electronic certificate catalog sharing system based on consortium blockchain”, In proceedings of 2019 IEEE 5th International Conference on Computer and Communications (ICCC), pp. 1237-1242, 2019.

[5]. Y. Hao, C. Piao, Y. Zhao and X. Jiang, “Privacy preserving government data sharing based on hyperledger blockchain”, In proceedings of International Conference on e-Business Engineering, pp. 373-388, 2019.

[6]. N.W. Lo, S.C. Chen and S.C. Chang, “A Flexible Electronic Data Exchange Framework Based on Consortium Blockchain”, Journal of Internet Technology, vol.21, no.5, pp.1313-1324, 2020.

[7]. H. AlAbdali, M.AlBadawi, M.Sarrab and A. AlHamadani, ,“Privacy Preservation Instruments Influencing the Trustworthiness of e-Government Services”, Computers, vol.10, no.9, pp.114, 2021.

[8]. I.T. Javed, F. Alharbi, T. Margaria, N. Crespi and K.N. Qureshi, “PETchain: A Blockchain-Based Privacy Enhancing Technology’, IEEE Access, vol.9, pp.41129-41143, 2021.