A BLOCKCHAIN-BASED MODEL FOR EDUCATIONAL CERTIFICATE MANAGEMENT

Mr. Suresh R[1], Kavitha M[2], Sharmili M[3], Subalakshmi P[4]

[1]Assistant Professor, Department of Information Technology, Sri Manakula Vinayagar Engineering College, Puducherry-605107

[2,3,4]UG Students, Department of Information Technology, Sri Manakula Vinayagar Engineering College, Puducherry-605107

---***---

Abstract - *The Educational certificates issued by educational institutions are important documents for students and graduates. Fake certificates are easy to make because the issuing process is not transparent and verifiable. The credibility of both the document holder and the issuing authority is jeopardized as the number of forged documents rises. Physical documents are also susceptible to structural damage over a course of time. Therefore, Self Sovereign Identity based model leveraging the use of technologies like Public Key Infrastructure and blockchain is proposed for digitizing the physical certificates to overcome the downside. Blockchain technology is a distributed ledger of transactions, a multi-tiered technology that potentially orchestrates the behavior of consumers and their assets based on a series of transaction ledgers.*

Key Words: **Physical Certificate, Digitizing, Self Sovereign Identity, Public Key Infrastructure, Blockchain**

1. INTRODUCTION

A degree can possibly pave the way for a better life, empowering an individual intellectually and socially to live a more meaningful and successful life. It is often a distinguishing factor among group of people, classifying them into various sections of society. Despite the fact that it is not finite, it is an extremely useful tool in the selection of candidates for companies during recruitment. While certificate ownership has many advantages, not everyone is ready and able to obtain them through legal means.

Educational certificates enable employers to evaluate employees, and organizers of educational events to raise their value for students. These documents contain information confidential to the individuals and should not be easily accessible to others. As a result, there is a critical need for a method that can ensure that the details in such a document is original, that is, that it came from a legitimate source and is not a forgery. Furthermore, the information in the document should be kept private so that only authorized people can see it. Blockchain and Public Key Infrastructure (PKI) technology is used to reduce the incidence of certificate forgeries and ensure that the security, validity and confidentiality of educational certificates would be improved. Simply put, blockchain technology is a distributed database that sequentially stores a chain of data in blocks. However, the scope of this paper is to determine a Self Sovereign Identity (SSI) based model leveraging the use of technologies like Blockchain and Public Key Infrastructure for implementing security requirements in educational certificate authentication, verification and issuing by publishing the public key in the blockchain network. The model is intended to avoid the problem of fake certificates or fraudulent in educational certificates.

2. RELATED WORK

Various approaches have been proposed to secure the certificate but later proved flawed. In the work implemented in [1], the author proposed a paper-based document authentication based on signature and QR code, in which document is in the form of a paper and certificate provides the authentication. It provides cryptographic functionality such as digital signature and digital certificate. Keytool of Java was used to generate 1024-bit RSA public or private key pairs and certificates. The digital certificate complies with X.509 standard. The certificate can then be exported and distributed after it has been created. The authors propose signing the document's message and compressing and encoding the signature generated into a QR code that can be attached to the document. However, forgery is possible due to current document printing and scanning technologies.

In the idea focused in [2], author has proposed Secure E-Qualification Certificate System in which the institute generates a signed, time stamped, and access-controlled electronic certificate to the specified user through a secured emailing system. Then, user downloads the document and a design a new access control list in the downloads e-certificate through the central system before forwarding it to the verifier. The reviewers also use the central system to verify the e-certificate which is access controlled by the user. This project focused on the creation of an eCertificate that guarantees prevention of forgery, provision of privacy and interoperability between different systems, particularly in the field of ePortfolios (EP).

The work submitted in [3], author proposed Cloud Based Graduation Certificate Verification Model in which he tries to accomplish certificate verification and also tries to provide security, validity and confidentiality. To enhance certificate verification, it is proposed that the university generates a secret key for each graduate. To ensure confidentiality in the proposed model, this key is given to the graduate.

In the novel method in [4], author proposed blockchain and Smart Contract for Certificate to solve the problem of counterfeiting certificates. On a blockchain, a smart contract runs on its own that automates the implementation of the terms of a contract between two parties. The application provided a user-friendly interface to issue and retrieve an academic certificate. Smart contracts based on the blockchain could provide a number of advantages, including dynamic, fast and latest updates, low operational costs, higher accuracy and lesser intermediaries. By the immutable property of blockchain, the certificates solve the problem of anti-counterfeit and verifiability.

In the idea focused in [5], the author implemented a platform that keeps track of achievements beyond certificates or transcripts, maintaining the digital hashes of learning activities and governing permissions with the use of blockchain smart contracts. He proposed every institute to provide access via smart contracts to its data stores which is used for storing student's records and enables student's privacy. Because the data resides in plaintext and the databases are highly centralized, this architectural proposition raises numerous security and privacy concerns. The author also proposed automated batch certificate generation and verification system which enables an end-user to define certificate template format and its format in system GUI, clicking and typing buttons and then, verifying the certificate.

The idea implemented in [6], author has proposed Blockchain Imperative for Educational Certificates that used to generate certificates in a way that is stored in the blockchain. The user can then easily share the certificate with the recipients. Rather than having to rely on issuing third authorities.

In the work proposed in [7], author has proposed universal verifiability using blockchain that provides tamper proof data distribution in electoral process but privacy is breached for everyone. Using a secure group communication and control mechanism, the task of distributing electoral information in the form of blocks and a temper-proof Blockchain ledger was completed. The offline feature of our proposed scheme protects the electoral process from the attacks which may occur during online scenario. Its geographic location feature limits a voter's ability to vote only in a registered ward.

In model developed in [8] author proposed peer to peer improved file system using IPFS and blockchain to solve high throughput problem for a user. They have added a blockchain to the original IPFS so that each node's information can be saved to the blockchain. They use the BitSwap protocol which can work better and faster theoretically. They also optimize the large data storage scheme of IPFS for content service providers and propose a novel scheme which combines three replication scheme and erasure codes storage scheme. For the specific choice of erasure codes, we think that choosing zigzag is very reasonable.

In the model implemented in [9], the study concentrates on the development of a central platform for academic institutions in order to have the ability to quickly approve the provision of the certificates. The author has developed a prototype for a platform based on cloud computing model to provide and facilitate verification process and which is accessible from anywhere any time for any organization that wishes to ensure the accuracy of academic certificates presented to them. Test results of Online Certificate Verification (OCV) shows that the system could discourage people against forgery because they know that their forgeries would be discovered within minutes so no one would buy fake documents from them.

In [10], the author has built Gradubique, a blockchain network built on top of Hyperledger Fabric. Gradubique is a network that allows instructors from any school to post exam and course grades. Gradubique allows employers and graduate schools to extract transcripts. Security is guaranteed by the blockchain technology. Transcript standardisation and translation can be built into the network, and the network's distributed nature can make it virtually cost-free. The proposed framework employs the hashing methods, i.e., SHA-256, to ensure data integrity.

2. PROPOSED METHODOLOGY

The proposed system is implemented using Self Sovereign Identity which leverages use of technologies like Public Key Infrastructure (PKI) and blockchain to provide the holder (Student) with the ability to control their data and the verifier (Company), the ability to verify credentials without making a request to the issuer(Institute). This works on the concept of Issuance�verification paradigm. The credentials are cryptographically signed not just by the issuer but also by the holder that gives guarantee about the data authenticity and integrity to the company.

- **Self Sovereign Identity:**

Self Sovereign identity intends to give control of user data back to the user by leveraging the use of technologies like Public Key Infrastructure (PKI) and Blockchain. In the SSI ecosystem, each party (issuer, holder, verifier) can create their own identifier, called Decentralized Identifier (DID), by publishing their public key on the public blockchain network and can verify each other independently. One of the problems which SSI solves is, it gives the ability to all participants to authenticate each other and to the verifier to verify the data independently - without making a call to the issuer. It is not necessary for the issuer to be online at the time of verification.

- **Decentralized Identifier:**

A globally unique persistent identifier that does not require a centralized registration authority because it is generated and registered cryptographically. A Decentralized Identifier (DID) is a new type of identifier that is globally unique, resolvable with high availability, and cryptographically verifiable. The

DID are addresses on the DLT of those public keys of users. DID is associated with cryptographic materials such as public key and service endpoints and are used to establish secure communication channels. Also note that one user can have more than one DIDs.

In short it fulfils 4 requirements of SSI system:

i. Permanent - It never need to change

ii. Resolvable – Used to get metadata

iii. Cryptographically verifiable – Ownership is proved using cryptography

iv. Decentralization - No centralized registration authority is required.

• DID Document:

DID documents contain metadata associated with a DID. They typically express verification methods (such as public keys) and services relevant to interactions with the DID subject. A DID document represents an abstract data model. The purpose of the DID document is to describe the public keys, authentication protocols, and service endpoints necessary to bootstrap cryptographically verifiable interactions with the identified entity.

It includes six components:

i. DID (for self-description)

ii. Set of public keys (for verification)

iii. Set of auth methods (for authentication protocol)

iv. Set of service endpoint (for interaction)

v. Timestamp (for audit history)

vi. Signature (for integrity)

3. FLOW OF THE PROCESS

The student requests for the certificate from the institute providing all his details which is in the form of the DID that is present in the open blockchain network. The institute verifies student credentials and creates schema to issue the certificate. The institute then issues the certificate to the student along with its digital signature and digital signature is generated by using the institute's private key with the certificate. The institute now sends the digital signature along with the certificate to the student. The student can use the institute's public key to verify the digital signature and hence can ensure whether the certificate has been issued from the respective and correct Institute. The student with the certificate now applies for a job in a company. The student provides the certificate to the verifier along with two digital signatures, one that was already issued to him as a credential and along with that the student generates a presentation consisting of his digital signature too. Now this is sent for verification to the verifier, and the verifier now uses the issuer's and student's public key from the DID to authenticate and confirm data collection.

4. CONCLUSION

The certificate management system through blockchain proves to be the best system when compared to the traditional systems because blockchain is meant for its security and most importantly it is a distributed system. Although the verifier does not belong to the same system where the issuer and the holder belongs, it proves to check the credential of the student by the verifier independently without contacting the issuer. Also, since the information in the blockchain network is public and distributed, there could not be any chance of duplicating or modifying the certificate. These benefits provide an added advantage of enhancing the security and integrity of the certificate management system through blockchain.

REFERENCES

[1] M. Warasart and P. Kuacharoen, "Paper-based Document Authentication using Signature and QR Code," ICCET, 2012.

[2] Lisha Chen-Wilson, Dr David Argles," Towards a framework of A Secure E-Qualification Certificate System", 2010.

[3] Osman Ghazali, Omar S. Saleh, "Cloud Based Graduation Certificate Verification Model", 2017.

[4] Jiin-Chiou Cheng, Narn-Yih Lee, Chien Chi, and Yi-Hua Chen," Blockchain and Smart Contract for Certificate", 2018.

[5] Ocheja, Patrick & Flanagan, Brendan & Ueda, Hiroshi & Ogata, Hiroaki. (2018). Managing lifelong learning records through blockchain.

[6] X. Technologies, "Blockchain imperative for educational certificates," Xanbell Technologies, 2017.

[7] Safdar Hussain Shaheen, Muhammad Yousaf, Mudassar Jalil: Temper Proof Data Distribution for Universal Verifiability and Accuracy in Electoral Process Using Blockchain, IEEE Conference, 2017.

[8] Chen, Y., Li, H., Li, K., and Zhang, J. (2017, December). An improved P2P file system scheme based on IPFS and Blockchain. In 2017 IEEE International Conference on Big Data (Big Data) (pp. 2652- 2657). IEEE.

[9] Ahmed, Bashir & Abshir, Abdirashid & Mohamud, Iqra & Karshe, Mohamed & Abdullahi, Mohamed. (2018). Discouraging Against Certificate Falsifications by Implementing a Cloud Based Certificate Validation System.

[10] Nguyen, Thinh, "GRADUBIQUE: AN ACADEMIC TRANSCRIPT DATABASE USING BLOCKCHAIN ARCHITECTURE" (2018)