Literature Survey on Certificate Authenticity Verification Solutions Using Blockchain Technology

Dr. J. Cynthia[1], G. Adithya[2], Raajakishore R[3], Amudhan S.M[4]
[1]Professor, Dept of CSE
[2, 3, 4]Dept of CSE
[1, 2, 3, 4] Kumaraguru College of Technology, Coimbatore.

Abstract- *Digitization is an essential driver for change, also influencing universities in their operation. However, the graduation certificate is still paper-based and does not fit employers' digitized recruitment processes. Digitizing the graduation certificate is overdue to align with the digitized processes of employers and universities.*

Further research into the matter makes it clear that several areas of industry would benefit form a digitized process that will prevent counterfeit certificates from diminishing the value of legitimate recipients. This paper aims to conduct a systematic literature analysis and propose a new type of digital certificate that is hashgraph-backed to prevent any fraud and counterfeiting.

We investigated 4 articles in the context of existing research on digital credentials. The paper gives an overview of research made so far and contributes by identifying gaps in existing proposals and proposing a system that fulfils those gaps, based on distributed ledger technology.

Keywords- Convolutional neural network (CNN), deep learning, tomato leaf disease, image datasets.

I. INTRODUCTION

One of the most important documents is certificates for graduates from universities and other educational institutions. Advancement of IT and low cost and high-quality office supplies on the marketplace have contributed to the development of essential documents such as certificates, identification cards and passports.

Certificates play an important role in the lives of all graduates, they are a proof of knowledge for the candidate presenting them to prospective employers or clients. Organizations often hire and fire people based on these certifications and credentials. Multiple cases have been observed where people were caught selling counterfeit certificates of various organizations at low value. The cost and time overhead for verification of certificates by organizations is very high thereby slowing down the entire speed of processing individuals.

The presence of counterfeit certificates fundamentally undermines the value of the issuing institution and the credibility of existing, valid recipients. The hiring of individuals based on counterfeit certificates incur heavy loses to organizations in the form of quality and finances.

There have been multiple efforts happening across the globe to provide an easy to use and commercially viable solution for the purpose of verifying the authenticity of certificates using distributed ledger technologies. This paper explores some of the proposed systems for certificate authenticity verification using blockchain technology.

II. LITERATURE REVIEW

Blockchain based academic certificate authentication system overview

This paper (Li, R., & Wu, Y., 2018) proposes a solution to overcome the counterfeit academic certificates and to do authentication of certificates, exerting revocation of certificates and a mechanism to establish the identity confirmation of the issuing organization. There are four components involved in this.

- Verifying the applications
- Issuing the applications
- BTC-based address revocation
- Blockchain and local database by MongoDB to store the certificates.

In the issuing process, the application component is the central node of the project where certificate application, examination, signing and issuance and certificate revocation occurs. Using the hash of the issued certificate the issuing application generates a Merkle tree root and broadcasts it to the Bitcoin blockchain. The verification application primarily focuses on verifying the authenticity of issued certificates. The verification application uses blockchain API to fetch the

transaction message and compares it with the verification data from the receipt.The general mechanism of the verification application follows the below mentioned steps:

- Check validity of authentication code
- Cross validate hash with local certificate
- Check if the certificate has been revoked or if it has expired

MongoDB is deployed to store the JSON-based certificates. The database has 2 main silos of data stores: authentication data which is public and the private certificate data. The public authentication data is released to the internet for public access using blockchain whereas the certificate data is securely stored in the MongoDB server. The verification application only needs access to the public data on the blockchain to verify the authenticity and integrity of the issued certificates. The functionalities available in the verification app are upload of PDFs, hash value calculation, blockchain interaction via APIs and verification of certificates. The functionalities of the issuing application are access control for individuals, approval process for certificate issuance, certificate auditing and certificate revocation. This paper dealt with the methods of issuing, verifying, storing and revocation of certificates. It uses a multi-signature model to sign certificates rather than using a single private key in the issuance process. This also makes the issuance process more time consuming as each member in the issuance flow needs to sign the certificate before issuing it to the Bitcoin blockchain. While issuing a certificate to the Bitcoin blockchain a gas fee needs to be paid to confirm the transaction on the blockchain, this makes this system expensive while issuing certificates in huge quantities. Moreover, the time taken for a transaction to be confirmed on the Bitcoin blockchain is 10 minutes making this impractical for issuing large quantities of certificates.

Certificate Verification using Blockchain and Generation of Transcript

In this paper (Lamkoti, R. S., Maji, D., Gondhalekar, A. B., & Shetty, H., 2021), the main focus is on generation and validation of certificates for Indian high school graduates seeking admissions into colleges. Three main stakeholders are mentioned in this paper - college, student and enterprises. Colleges act as the issuing authority responsible for issuing certificates to students. Colleges generate templates for the certificates and enter the details of a student or upload a CSV file to generate certificates for a large number of students. The students' details are injected into the certificates. Each certificate has a unique ID associated with it. Once the issuing authority approves a certificate, a byte array is constructed from the certificate and stored in the IPFS (Inter Planetary File System). The IPFS passes the data to the blockchain, and a hash is generated for that document and stored along with the document. Students must register themselves on the website in order to access to the hash of the certificate or the digital certificate, using which they can apply to any organization. To implement this, Ethereum nodes are used and Solidity language to write contracts. The IPFS is integrated with the blockchain (Nyaletey, E., Parizi, R. M., Zhang, Q., & Choo, K. K. R., 2019) and is thus distributed, and no single entity has the access to all parts of the certificates and the document can be accessed using hash. In the verification part, the applicant submits either the unique ID of the certificate or the certificate itself. When a certificate is submitted, the hash value is calculated and checked against the record in IPFS to determine if it is valid or not. The unique ID will be searched against the certificate IDs available in the blockchain and the verifier is notified if the provided hash or certificate is authentic. While this method solves the main pain points associated with certificate verification, a means to legally modify certificates is not provided to address use cases such as name changes and human errors which are practically impossible to be avoided completely

.

Tamper proof Birth certificate using Blockchain Technology

This paper (Shah, M., & Kumar, P., 2019) seeks to provide a theoretical method for the issuance and verification of birth certificates. They seek to prevent the forgery of birth certificates using a blockchain network, interplanetary file system (Chen, Y., Li, H., Li, K., & Zhang, J., 2019). It stores the birth certificates of each individual in the blockchain. During the registration of a user, it will create an RSA key pair and a bigchain DB key pair. Using this, the user can login after the registration. User enters name and phone number as part of the registration. The RSA public key, bigchain DB public key, name and phone number will be registered in blockchain. When the issuing authority wants to create and add a birth certificate to the blockchain, it will find the phone number of the user from blockchain. It will create an AES key pair and using that, the file contents will be encrypted. After which the AES key is generated for the birth certificate. The generated AES key will be encrypted using the client's RSA public key. This ensures that only the person in possession of the RSA private key can access the birth certificate for decryption. During retrieval of the birth certificate, the person's phone number is used to retrieve the encrypted file from the blockchain. The RSA private key is used to decrypt the AES key. After which the AES key to the file is used to decrypt the contents of the file. To permit other people to see the contents of the file this paper has proposed a mechanism. The phone number of the person with whom the certificate needs to be shared is recorded on the blockchain and RSA key pair is generated. And the same process repeats, the file is

encrypted using AES key but instead of encrypting the AES key with users' RSA public key, it is encrypted using the person's RSA public key of the intended recipient. They can retrieve the file using the same mechanism as mentioned above. In this paper, issuing the certificates part is simple but the verification of certificates and sharing them with others is tedious, time consuming and computation. Main concerns that have not been addressed are the use case of the user changing mobile numbers and revocation of shared certificate for other users after verification. Also, an RSA keypair needs to be generated and the certificate needs to be encrypted and stored on the blockchain every time the certificate needs to be shared.

Certificate Verification System using Blockchain

This paper (Kumavat, N., Mengade, S., Desai, D., &Varolia, J., 2019) aims to tackle the problem of fake certificates being submitted by students to organizations for job opportunities by making use of the Ethereum blockchain to digitally disburse certificates making counterfeiting impossible and easily verifiable. Smart contracts are used in order for the backend of their system to interact with the blockchain. The hash value of the encrypted certificate is stored in the Ethereum blockchain. According to this paper the issuing organization issues certificates to the Ethereum blockchain using a service provider and the recipients then can query the application to view the certificates and the service provider will be the entity in charge for the maintenance of the system (Cheng, J. C., Lee, N. Y., Chi, C., & Chen, Y. H., 2018). Each issuing organization has a wallet ID through which the transactions are completed, and the original copy of the certificate is stored in an interplanetary file system which can be accessed by the recipients using the hash of the certificate. The proposed methodology solves the problem of fake certificates being provided by individuals to organizations but a simple and straightforward way for a recipient to share the issued certificates to other organizations is not available.

III. CONCLUSION

From this survey it is revealed that several systems have been proposed to use blockchain technology for the purpose of certificate authenticity verification with the caveat being that all the proposed systems are at the prototype level and have not been able to scale into real world solutions. Some of the issues faced by the current systems are high transaction time for bitcoin-based systems (Li, R., & Wu, Y., 2018), inefficient sharing mechanisms for certificates (Kumavat, N., Mengade, S., Desai, D., &Varolia, J., 2019) and immutability of certificates in case of changes in the future or human error (Lamkoti, R. S., Maji, D., Gondhalekar, A. B., & Shetty, H., 2021) (Shah, M., & Kumar, P., 2019).

These challenges are the primary reason for the inability of mainstream breakthrough for digital ledger technology-based certificate authenticity verification systems. A new area of development in the digital ledger technology space is hashgraphs and it overcomes some of the challenges faced by blockchain technology. Hashgraphs could potentially be better suited for the purpose of certificate authenticity verification.

IV. ACKNOWLEDGEMENT

We express our profound gratitude to the management of Kumaraguru College of Technology for providing us with the required infrastructure that enabled us to successfully complete the project.

We extend our gratitude to our Principal, **Dr. D. Saravanan,** for providing us the necessary facilities to pursue the project.

We would like to acknowledge **Dr. P. Devaki,** Professor and Head, Department of Computer Science and Engineering, for her support and encouragement throughout this project.

We thank our project coordinator **Dr. L. Latha,** Professor, Department of Computer Science and Engineering and our guide **Dr. J. Cynthia,** Professor, Department of Computer Science and Engineering, for their constant and continuous effort, guidance and valuable time.

Our sincere and hearty thanks to staff members of Department of Computer Science and Engineering of Kumaraguru College of Technology for their well wishes, timely help and support rendered to us during our project. We are greatly indebted to our family, relatives and friends, without whom life would have not been shaped to this level.

REFERENCES

[1] Li, R., & Wu, Y. (2018). Blockchain based academic certificate authentication system overview. IT Innov. Centre, Univ. Birmingham, 8.

[2] Nyaletey, E., Parizi, R. M., Zhang, Q., & Choo, K. K. R. (2019, July). BlockIPFS-blockchain-enabled interplanetary file system for forensic and trusted data traceability. In 2019 IEEE International Conference on Blockchain (Blockchain) (pp. 18-25). IEEE.

[3] Shah, M., & Kumar, P. (2019). Tamper proof birth certificate using blockchain technology. Int. J. Recent Technol. Eng.(IJRTE), 7.
[4] Chen, Y., Li, H., Li, K., & 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.
[5] Kumavat, N., Mengade, S., Desai, D., &Varolia, J. (2019). Certificate verification system using blockchain. Int. J. Res. Appl. Sci. Eng. Technol.(IJRASET), 7, 53-57.
[6] Cheng, J. C., Lee, N. Y., Chi, C., & Chen, Y. H. (2018, April). Blockchain and smart contract for digital certificate. In 2018 IEEE international conference on applied system invention (ICASI) (pp. 1046-1051). IEEE