International Research Journal of Innovations in Engineering and Technology (IRJIET)

ISSN (online): 2581-3048

Volume 7, Special Issue of ICRTET-2023, pp 44-47, June-2023

International Conference of Recent Trends in Engineering & Technology (ICRTET-2023)

A Survey Paper on Academic Certificate Verification Using Blockchain

[1]Prof. Sushma Shinde, [2]Avadhoot Chavan, [3]Dhananjay Sadhu, [4]Shubham Mane, [5]Sujay Chalke

[1,2,3,4,5]Department of Computer Engineering, Siddhant College of Engineering, Pune, Maharashtra, India

***Abstract* - In According to the statistics of the Indian Ministry of Education, there are around 1 million graduates every year, of whom 4,444 will go to the country, high school or university to continue their education and 4,444 will be ready to enter a job. All certificates of achievement, transcripts, graduation certificates etc. received by the students during their education will be important documents for new school or new job admission. Only schools and students entered as schools awarded many awards or certificates. Because there is no effective way to prevent fraudulent transactions, there are often situations that lead to fraudulent certificates. To solve the certificate fraud problem, a digital certificate based on blockchain technology will be prepared. Using modified tools of the blockchain, digital certificates can be created that prevent fraud and have proofs. The process of issuing a digital certificate through the system is as follows. Before creating the electronic file of the certificate, add and store other important information in the file and also calculate the hash value of the electronic file. Finally, the hash value is stored in a block in the chain system. The system will generate an interactive QR code and a question string code to be added to the certificate. The application verifies the authenticity of the certificate by sending a mobile or web query. The system changes the nature of the blockchain, not only increasing the reliability of various certificates, but also electronically reduces the risk of various types of certificates.**

Keywords: Academic Certificates, University, Fraudulent Certificates, Blockchain System.

1. Introduction

E-certificate generation system which manually creates the certificates based on cur- rent students data. Various centralized methods follow the similar approach for verification. The centralized approaches can't defend the various network attacks like SQL injection, Collusion, bruited force etc. Blockchain approach using decentralized approach. Fog computing or fog networking, also known as fogging, is pushing frontiers of computing applications, data, and services away from centralized cloud to the logical stream of the network edge. Fog networking system works on to build the control, configuration, and management over the Internet backbone rather than the primarily control by network gateways and switches those which are embedded in the LTE network. We can illuminate the fog computing framework as highly virtualized computing infrastructure which provides hierarchical computing facilities with the help of edge server nodes. These fog nodes organize the wide applications and services to store and process the contents in close proximity of end users.

2. Existing System

During our research, we were able to find some of the works done which were related to our field. Following are some of the findings:

In [1], in a permissioned Blockchain (Hyperledger Fabric), a user, depending upon the kind of authorization given to it, on login can query or manipulate any Blockchain data. This paper highlights the effects of resume fraud. Authors have created a platform for companies and universities using Hyperledger. Institutions can store student data and companies can store recruiting info on the platform. Users can query or manipulate student or recruit info.

In [2], the main method is to create a hash of the fingerprints of the students which will be stored in the block and for verification, the recruiter just needs to scan the fingerprints of the candidate.

In [3] published in the year 2020, Simply using the hash number which was generated while creating a block as a corresponding to the original document and verifier can use this 'hash-key' to fetch the original document from the Blockchain.

In [4], before handing certificates to the students, a hash of its digital version would be calculated and stored in a chain-system when students apply for a job in any company. The recruiters would just have to upload the digital document given by the candidate, a hash will be generated and then compared, and the result of real or forged will be displayed.

In [5], A Blockchain application wherein, a digital version of the paper certificate would be obtained, then the

International Research Journal of Innovations in Engineering and Technology (IRJIET)

ISSN (online): 2581-3048

Volume 7, Special Issue of ICRTET-2023, pp 44-47, June-2023

International Conference of Recent Trends in Engineering & Technology (ICRTET-2023)

related data will be stored in a database and a hash of that digital file would be created which would be stored in the block in the chain system. The application would generate a QR code and an inquiry string code which would be affixed to the paper certificate. So, the genuineness of the certificate can be known by scanning that QR code using the application on the verifier's side.

In [6], published in the year 2018, A DApp created using permissioned Blockchain, users are divided into three categories based on the privileges assigned to them. A `low risk` user can send a request and receive information. A `medium risk` user can issue certificates. A `High Risk` user can mine and administer the chain. Here, the certificate information is stored in JSON files, a verifier can verify the certificate and on request, it can access more details about the candidate's certificate that is granted by the candidate. It makes use of streams and the Multichain Blockchain technology is used.

In [7], the certificate's data is stored in the permissioned and secured network, a student can request for its certificate and the employers can verify the certificate using the hash. Using OpenZepellin to make this p2p model more secure and IPFS (Interplanetary File System) for storing certificates.

In [8], it describes the existing systems of credential verification and its downfalls along with the various advantages of the Blockchain Ethereum platform that can be used for implementing the Blockchain. The hash of the fingerprint and a secret phrase is given to the concerned entity. System will retrieve the hash stored on the Blockchain and compare the input with the hash stored on the Blockchain.

In [9], text extraction from the certificate during the verification and hash that extracted data. The hash created then will be compared within the existing blocks in the consortium of the Ethereum network and the result will be displayed based on the search result. An IoT based camera has been used in this project with red and green lights used as indicators. Red light will indicate that OCR extraction has failed to find the hash (forged) and green indicates that the OCR has found the hash (Real).

In [10], published in the year 2019, students will get a QR code with their certificate, which has the SHA512-hash of that certificate, the verifier would just need to scan the code, and the result of genuineness will be sent from the Ethereum network and displayed on the interface.

3. Proposed System

The students achievements available in the form of degree certificate, mark sheet, value added certificate, etc., will become an important weightage for recruitment or higher studies. The Education institution awards and degree certificates may have only the names of the institution and the student's data. In this scenario there is a lack of effective anti-forge mechanism, due to this events many times the graduation certificate to be forged often is found. To solve the problem of fake certificates, the blockchain technology would stores the certificate in digital form. The immutability nature of blockchain makes digital certificate in the distributed ledger is very difficult to tamper or modify also it is very easy to verify the originality of digital certificate.

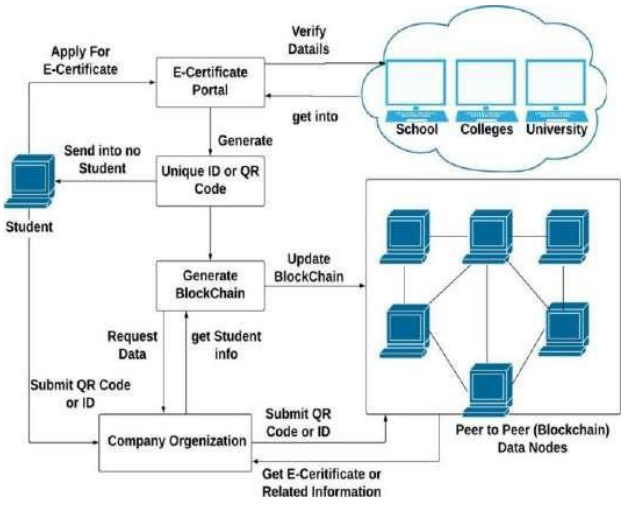
The process of issuing digital certificates in the system is as follows. First step, generate the hash value for certificate using double SHA256. Store the fixed length hash value as a transaction in the block. This transaction is validated by the members in the blockchain, once it is trusted as valid transaction then the block is added with existing blockchain. Accepting and rejecting will be done using consensus algorithm. The consensus algorithm may be chosen based on number of nodes, and transactions. The system will generate the related QR code and inquiry string code to affix in the hardcopy certificate. The system provides the unit to authenticate the hardcopy certificate through phone scanner or website. The immutability nature of the distributed ledger, the system provides not only verification of certificate and also it stores the certificate in digital form forever.

Algorithm of proposed system:

1) User will upload the certificate
2) Details like name, branch, batch will be extracted
3) Hash of the extracted details will be calculated
4) The hash will be queried in the Blockchain
5) If such hash exists then the certificate is valid

4. System Design

Block Diagram



ISSN (online): 2581-3048
Volume 7, Special Issue of ICRTET-2023, pp 44-47, June-2023
International Conference of Recent Trends in Engineering & Technology (ICRTET-2023)

5. Conclusion

There are many research directions in applying Blockchain technology to the E- certificate transaction due to the complexity of this domain and the need for more robust and effective information technology systems. An interoperable architecture would undoubtedly play a significant role throughout many E-certificate transaction use cases that face similar data sharing and communication challenges. From the more technical aspect, much research is needed to pinpoint the most practical design process in creating an interoperable ecosystem using the Blockchain technology while balancing critical security and confidentiality concerns in E-certificate transaction. Whether to create a decentralized application leveraging an existing Blockchain, additional research on secure and efficient software practice for applying the Blockchain technology in E- certificate transaction is also needed to educate software engineers and domain experts on the potential and also limitations of this new technology. Likewise, validation and testing approaches to gauge the efficacy of Blockchain-based health care architectures compared to existing systems are also important (e.g., via performance metrics related to time and cost of computations or assessment metrics related to its feasibility).

ACKNOWLEDGEMENT

We would like to take this opportunity to thank all the people who were part of this seminar in numerous ways, people who gave un-ending support right from the initial stage.

In particular we wish to thank Prof. Shushma Shinde as internal project guide who gave their co-operation timely and precious guidance without which this project would not have been a success. We thank them for reviewing the entire project with pains taking efforts and more of her, unbanning ability to spot the mistakes.

We would like to thank our H.O.D of Computer Department Prof. Shushma Shinde for her continuous encouragement, support and guidance at each and every stage of project.

And last but not the least we would like to thank all my friends who were Associated with us and helped us in preparing our project. The project named "Academic certificate verification using blockchain" would not been possible without the extensive support of people who were directly or indirectly involved in its successful execution.

REFERENCES

[1] Sharples, M., The blockchain and kudos: A distributed system for educationalrecord, reputation and reward. 2016 https://doi.org/10.1007/978-3-319-45153-448.

[2] Bruce Dorris, J.D, (2018) "Report to the Nations, Global study on occupational fraud and abuse", Association of Certified Fraud Examiners. DOI: 10.5121/ijnsa.2019.11502.

[3] Trong Thua Huynh1, Dang-Khoa Pham2. eunicert: ethereum based digital certificate verification system October 14, 2019 by IJCNC JOURNAL.

[4] Inamorato dos Santos, A. (2017) Blockchain in Education – European Commission's JRC report preview, Blockchain in Education Conference, DOI:10.2760/60649.

[5] Mesropyan, E. (2017). 21 Companies Leveraging Blockchain for Identity Management and Authentication. Vol.8 (2018) No. 4-2 ISSN: 2088-5334 Perry, R.E. (2017).

[6] Blockchain technology: From Hype to Reality. DOI: 10.1016/j.jii.2020.10012

[7] H. Watanabe, S. Fujimura, A. Nakadaira, Y. Miyazaki, A. Akutsu, and J. Kishigami, "Blockchain contract: Securing a blockchain applied to smart contracts," in Proc. IEEE Int. Conf. Consum. Electron. (ICCE), Jan. 2016, pp. 467–468.

[8] Z. Zheng, S. Xie, X. Chen, and H. Wang, "Blockchain challenges and opportuni- ties: A survey," in Proc. IJWGS, vol. 14, 2018, pp. 352–375.

[9] Marco Baldi, Franco Chiaraluce, Emanuele Frontoni, Guiseppe Gottardi, "Certificate Validation through Public Ledgers and Blockchains," In Proceedings of the First Italian Conference on Cyber security (ITASEC17), Venice, Italy.

[10] Tarek Kanan, Ahamd Turki Obaidat, Majduleen Al-Lahham, "SmartCert BlockChain Imperative for Educational Certificates", 2019 IEEE Jordan International Joint Conference on, pp. 629-633, 2019.

[11] Xiuping Lin, "Semi-centralized Blockchain Smart Contracts: Centralized Verification and Smart Computing" Department of Information Engineering, National Taiwan University, Taiwan, R.O.C., 2017.

[12] Karuppanan Komathy. (2018). Verifiable and Authentic Distributed Blockchain Shipping Framework for Smart Connected Ships. Journal of Computational and Theoretical Nanoscience. 15. 3275-3281. 10.1166/jctn.2018.7610.

[13] Dinesh Kumar K, Komathy K, Manoj Kumar D.S "Blockchain Technologies in financial sectors and industries", International Journal of Scientific and Technology Research Volume 8, Issue 11, pp. 942 - 946, 2019.

International Research Journal of Innovations in Engineering and Technology (IRJIET)

ISSN (online): 2581-3048

Volume 7, Special Issue of ICRTET-2023, pp 44-47, June-2023

International Conference of Recent Trends in Engineering & Technology (ICRTET-2023)

Citation of this Article:

Prof. Sushma Shinde, Avadhoot Chavan, Dhananjay Sadhu, Shubham Mane, Sujay Chalke, "A Survey Paper on Academic Certificate Verification Using Blockchain" in proceeding of International Conference of Recent Trends in Engineering & Technology ICRTET - 2023, Organized by SCOE, Sudumbare, Pune, India, Published in IRJIET, Volume 7, Special issue of ICRTET-2023, pp 44-47, June 2023.

****

