A New Technique of digital Certificate Using Blockchain Technology

Leelavathy S R, S Divyashree, Sneha P, PreethiSPattar, Sananth Kumar R S

Department of Computer Science and Engineering
Dr. T. Thimmaiah Institute of Technology,
Kolar Gold Field, Karnataka, India

leelav48@gmail.com

Abstract. The authorizations granting certification are highly compromised in terms of security details, due to lack of authentication and antiforge mechanism. We adopt block chain technology to overcome the problem of certificate forgery which will confirm users similar to digital signature with his/her identity and accessing authorization. Block chain technology is an open distributed ledger which contains unchallengeable information in a highly protected and encrypted approach and also it ensures that each transactions can by no means be changed. In accord to a high requirement for the method that can pledge to facilitate the information in such a certificate is original, this means that the document has been originated from authoritative resource and is not fake. Interplanetary file system makes use of the content address to exclusively identity every individual file in a overall namespace involving all computing device. A quick response (qr) code is a bi- dimensional barcode which provisions data in the form of black dots and white dots. The system comprises of black squares set in a square framework on a white environment, that can be captured by an imaging mechanism like a camera.

Keywords: block chain, hash, digital certificate, interplanetary file system, quick response code.

1 Introduction

1.1 Blockchain

Block chain was invented by Satoshi Nakamoto in 2008.Block chain facilitate distributed public ledgers which adhere to unchallengeable data in the secure and encrypted method plus guarantee that the transactions can by no means be indistinct. Though Bitcoin and further crypto currencies are the most chic example of blockchain. Distributed ledger technology (DLT) which is a digital system intended for recording the transaction of resources in which the transactions and their information are recorded at different places at the identical time. A block in blockchain is a set of data. The data is further added onto the block in blockchain. The primary block in the

ICASISET 2020, May 16-17, Chennai, India

DOI 10.4108/eai.16-5-2020.2304045

Block chain is known as Genesis Block signature. Each transaction generates a hash. If the transaction has been agreed by a greater part of the nodes next it is wrote onto a block. every block refers to the preceding block and jointly create the Blockchain.

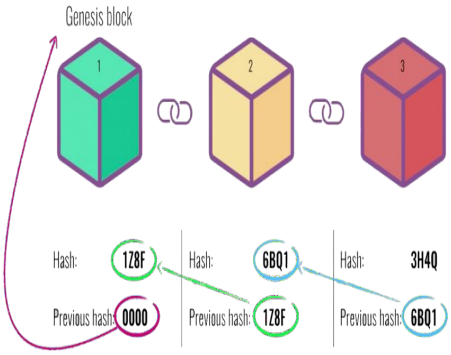


Fig.1: Block chain

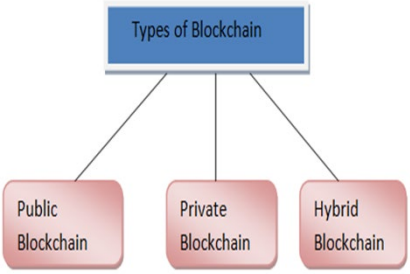


Fig.2: Types of Blockchain

1.2 Classification of Blockchain

Depending on the requirement of the application, Block chain can be alienated into 3 types [4]: Type 1block chain as Public, Type 2 block chain as Private, Type 3 block chain as Hybrid, Public block chain. As the name suggest, Public Block chain is freely accessible and has no control on who can join or be a Validates. In Public Block chain, no individual has complete power over the network. These ensure data security and helps immutability since a single person cannot operate the Block chain. The influence on the Block chain is uniformly divided among each node in the system, and due to this, Public Block chain is identified to be entirely distributed. Public Block chains are chiefly used for crypto currencies similar to Bitcoin, Ethereum, and Litecoin.

2 Literature Survey

Jiin-chioucheng[1] proposed “Block chain and concept of smart contract fordigital documentation or digital certificate” is a system in which degree certificates issued by school/colleges are converted into the form e- certificate. This method’s applications were been programmed on Ethereum platform and also run by the Ethereum virtual machines (EVM). Nithinkumavat[2] proposed” the method of Certificate authentication System making use of Block chain” for storing digital certificates on to the block chain. Ethereum gives the platform for generating the new application Dapp which stands for decentralized application that was based on smart contract. Dapp is connected to smart contract using web3js. Inter planetary file system and SHA-256 algorithm. And by the immutable and transparency property of the block chain it can be used to generate the digital certificates which are anti-counterfeit and easy to verify. Nadir Abdelrahman Ahmed Farah[3] formulated The“Block chain : categorization, Opportunities, and the Challenges” the discussion is about the block chain technology beside with variousadded advantages.
Deepak puthal[4]proposed “Everything You Wanted to Know about the Block chain” that tells about the promise, components, process, current trends and problems of block chain. The block chainused globally for securing peer-to-peer infrastructure with decentralization.NeethuGopal and VaniPrakash [5] proposed “Survey on Block chain Based Digital Certificate System” the unmodified properties of the block chain helps to overcome this problem to ensure validity; confidentiality and security of graduation certificate would be improved. A new block chain intended system gradually reduces the certificate counterfeit. Vijayamumar et. Al [9][10], proposed a students performance analysis system using cumulative predictor algorithm

3 Consensus Algorithms

In the application of block chain, we should to resolve two problems double spending[6] and Byzantine Generals Problem[7]. Double spending problem functions by reuse of the currency in couple of transactions at the same instance time. PoW (Proof of work) is a consensus policy used in the Bitcoin network [8]. In a decentralized system, a person/entityhave to be chosen to record the transactionsThe very easy way is random assortment. Proof of stake (PoS) had mentioned in the primary bitcoin project, but it wasn’t used due to robustness and further reasons. The initial function of PoS is PPCoin . It is an energy-saving substitute to proof of work (PoW). Miners in Proof of Stakemust prove ownership of the total currency. Ripple is a consensus algorithm that uses jointly trusted sub networks contained by the bigger network.

4 ARCHITETURE

1. Schools contribution a grade certificate and record the student's statistics into the structure after that, the system manually reports the unique number of the learner in a block chain.
2. The documentation method verifies the entire data.
3. As a replacement for of sending usual hard/manual copies, schools endowment e-certificates consisting an additional quick response (QR) code to the former students of which the records have been effectively validated and verified. Every graduate will get an electronic file of respective certificate.
4. While applying for a work, a former student merely sends the unique number or an electronic certificate with ease Quick Respond code to the applied companies.
5. The companies then send the inquiries to the organization and are learned if the unique numbers are verified. The QR code enable to identify if the certificate have been modified or counterfeit.
6.

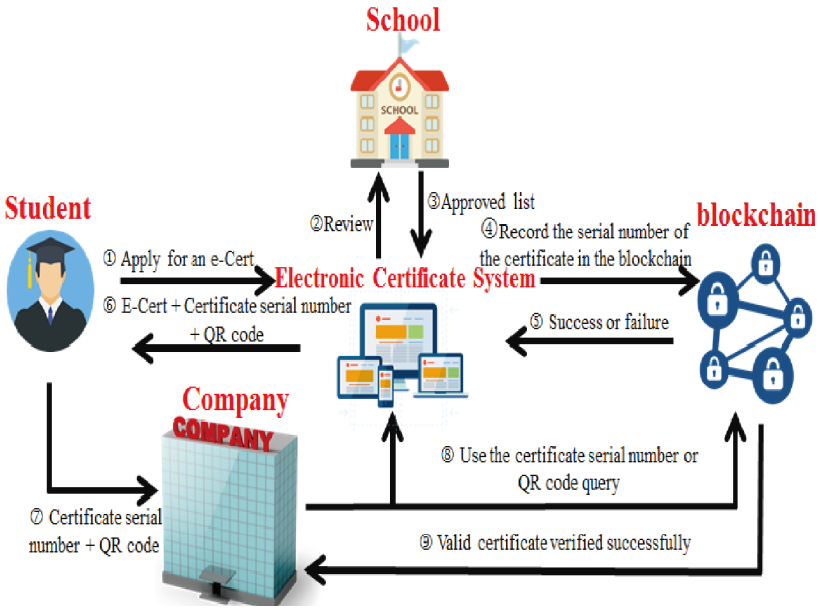
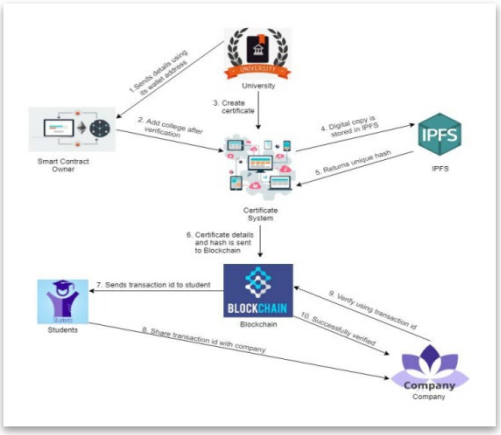


Fig.3: Working Process of the System

5 Data Flow Diagram



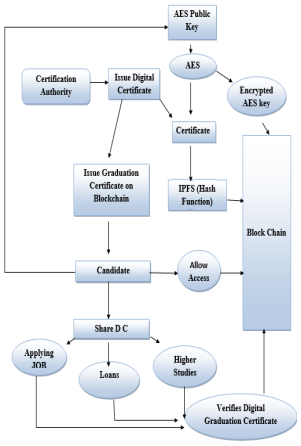


Fig. 4: Data Flow Diagram, **Fig. 5:** Block diagram

6 Methodology

In Existing scheme the certificate are stored in centralized method and confirmed manually, so it takes too much time to verify. There is no protection to the certificate that are specified to any private sectors (example banks).But, the data may be distorted, deleted or customized. Certificates are effortlessly hacked and make replica of that certificate. The charge of creating fake certificate is less costly and method of create fake certificate is fairly simple. Students get their certificates on interview places. There is no protection for certificates. There are some other disadvantage in the existing scheme like wastage of paper, complexity in applying for replica certificate and also loss risk of a variety of type of certificate. Using the proposed system we first, generate an electronic file of the paper certificate with associated data onto the record, for the meantime estimate the electronic record for its hash code. Finally store the hash code onto the block in the chain structure. The proposed scheme then generates a linked Quick Response code and inquest sequence code to affix to respective paper certificate. It will give the demand component to verify the legitimacy of the paper certificate by cell phone scan or the website inquiries. Using the integrity feature of the block chain, the scheme will enhance the integrity of a range of paper base certificates.

6.1 Results

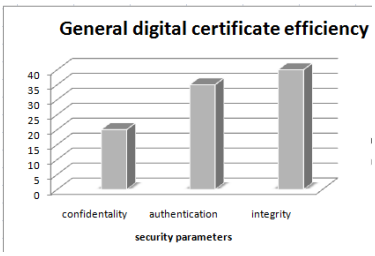


Fig. 6: Digital Certificate

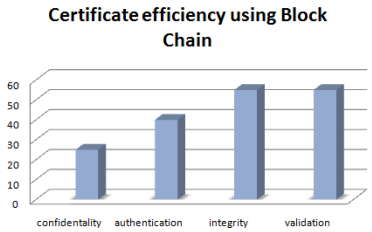
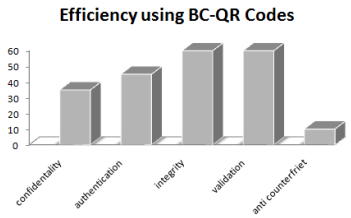


Fig. 7: Digital Certificate using Block Chain



,

Fig. 8: Digital Certificate using Block Chain and QR codes

7 CONCLUSION

Summarizing a decentralized digital certificate system on the basis of Ethereum block chain is been generated. This expertise was preferred as it is imperishable, decrypted/encrypted, and tracked in addition authorize data management. By combining the properties of blockchain, the technique improves the effectiveness at all stages. The system cuts the custom of paper, cuts executive expenses, avoid certificate copy, and gives precise and consistent data on digital certifications. Looking into the graphs above the efficiency in terms of security parameters which include confidentiality, authentication, integrity, validation and anti-counterfeit the digital certificates using block chain combined with quick response code yield better efficiency. Data protection being the foremost entity of block chain . Blockchain is a huge and freely-access online ledger where every system saves later verify the similar data. By the method of

newly proposed block chain intended system will reduce the probability of record or certificate counterfeit. In accord to apply for an electronic-copy can hoard paper documentation and point in time. Accordingly, institutions and organizations cannot instantaneously authenticate the documentation credentials they dispatch. The process of certificate submission granting is unwrapping and clears in the organization. Institution or companies can there by request for data documented on any certificate from the organization.

REFERENCES

1. Cheng, Jiin-Chiou, et al. "Blockchain and smart contract for digital certificate." 2018 IEEE international conference on applied system invention (ICASI). IEEE, 2018.
2. Khandelwal, Harshita, et al. "Certificate Verification System Using Blockchain." Advances in Cybernetics, Cognition, and Machine Learning for Communication Technologies. Springer, Singapore, 2020. 251-257.
3. Farah, Nadir Abdelrahman Ahmed. "Blockchain Technology: Classification, Opportunities, and Challenges." International Research Journal of Engineering and Technology 5.5 (2018): 3423-3426.
4. Puthal, Deepak, et al. "Everything you wanted to know about the blockchain: Its promise, components, processes, and problems." IEEE Consumer Electronics Magazine 7.4 (2018): 6-14.
5. Dumitrescu, George Cornel. "Bitcoin–a brief analysis of the advantages and disadvantages." Global Economic Observer 5.2 (2017): 63-71.
6. Ahmed, S.T., Sandhya, M. & Sankar, S. TelMED: Dynamic User Clustering Resource Allocation Technique for MooM Datasets Under Optimizing Telemedicine Network. Wireless PersCommun 112, 1061–1077 (2020). https://doi.org/10.1007/s11277-020-07091-x
7. S. T. Ahmed and S. Sankar, "Investigative Protocol Design of Layer Optimized Image Compression in Telemedicine Environment", Procedia Computer Science, vol. 167, pp. 2617-2622, 2020, [online] Available: https://doi.org/10.1016/j.procs.2020.03.323
8. Gunashree, M., Ahmed, S. T., Sindhuja, M., Bhumika, P., Anusha, B., &Ishwarya, B. (2020). A New Approach of Multilevel Unsupervised Clustering for Detecting Replication Level in Large Image Set. *Procedia Computer Science*, *171*, 1624-1633.https://doi.org/10.1016/j.procs.2020.04.174
9. J. Dafni Rose, K. Vijayakumar and S. Sakthivel, “Students performance analysis system using cumulative predictor algorithm”, Int. J. Reasoning-based Intelligent Systems, Vol. 11, No. 2, 2019.
10. Vijayakumar. K, Nawaz Sherif. T, Gokulnath.S, “Automated Risk Identification using Glove algorithm in Cloud Based Development Environments”, International Journal of Pure and Applied Mathematics Volume 117 No. 16 2017.