International Journal of Future Generation Communication and Networking
Vol. 13, No. 3s, (2020), pp. 1677–1684

Generation of E-Certificates using Custom Blockchain for Peer to Peer Network

Priyanka R Balage and Dr. Kishor R Kolhe
School of computer engineering & technology, MIT World Peace University,
Pune, Maharashtra, India

Abstract

Blockchain is very emerging trend in recent years; it is basically decentralized approach which provides transparency to transactional data. While data security is the most essential requirement in the 21st century, distributed as well as the centralized environment. Identifying or validate the user's identity based on educational histories is a very tedious task. Many commercial applications validate by respective organizations based on physical verification. Search systems do not provide trustworthy information when declared on a centralized data basis, due to two database security concerns. Various database and software base intrusion attacks can harm centralized data and change the actual information. This paper, the system illustrates blockchain base e certificate generation for the educational field. In a real- time scenario, many organizations make document verification of particular employees on traditional approaches like physical verification, etc. The system proposes is E-certification and token generation using a strategic process which provides hassle-free e verification for the organization of specific employee. This system also carried out custom blockchain implementation with dynamic smart contract, and mining policy, which generate the Unique Identification (UID) number and QR code for each user for online verification. The final phase provides various consensus algorithms for drastic data verification and majority voting in the P2P network. The partial implementation of the system shows the effectiveness of the proposed system over the traditional approaches.

Keywords*: Blockchain, E-Certificate, Proof of Work, Consensus algorithm, Smart contract, mining.*

Introduction

Basically the document certificate and privacy is a very essential to provide security to private information, various platform has already exist to store such a kind of large data in a secure manner. Some centralized cloud storage provides data Encryption strategies for achieve highest security for documentation. In real time large document verification is very tedious process which required much resources as well as time also. Where manual systems are has been followed by different organization since couple of years, for employee verification, student document

ISSN: 2233-7857 IJFGCN

verification as well as any other government document verification by particular agencies. Sometime industrial organizations and colleges should be verifying the students and employees documentation. This research basically eliminate such time consuming process introduce the cost of traditional existing systems.

Background of System

Blockchain : Basically blockchain is the technique which provides decentralized approach data storage for different transactional systems. Basically it is introduced to achieve the highest data security during the data transactions and eliminate various network as well as data attack from malicious requests.
Decentralization: We need a decentralized system to guarantee power and adaptability, and to wipe out all to one sources of traffic. Through using these decentralized systems, we can also eliminate the sole aim of regret or data delay problems. In our model we use a modular network of overlays.
Authentication of data: Service or cloud administrations of users store unpreserved information that should be passed to blockchain systems. It may be altered or lost while transmitting information. Protecting these off-base altered information adds the weight to the system and can result in the patient's loss (demise). We use a lightweight advanced label plot along these lines to ensure the information is not changed [2]. On the destination hand, information is checked with the advanced mark of the provider, and it gives the patient a receipt of information once it has been effectively received.
Adaptability: Solving Proof of Work (PoW) is increased computationally; IoT gadgets are in any case limited to properties. Similarly, the IoT network includes countless hubs and blockchain scales inadequately as the number of hubs in the network increments. In our overlay method we hand out the concept of PoW and divide our overlay into a few bunches instead of a single chain of squares Rather than we spread the hubs between a few groups. Our model depending on the system's transmission function and other extensive security capabilities.
Data Storage:: Protecting IoT massive information over blockchain isn't reasonable and this way we use cloud servers to store fragmented squares of information. The information is secured over the cloud due to extra cryptographic protection such as the advanced signature and exclusive encryption criteria that will be examined later. In any case, it might give outsiders a concern about being confided. This is why we store all trades in different squares and make a combined hash of each square using Merkle Tree and transfer it to the spread method . Some changes in cloud information can be viewed effectively along those lines. Doing the potential as such also saves the degree of decentralization over.
Anonymity of users: A patient's medical information can contain touchy details, and this mode involves timestamping of the information over the network. We use lightweight ring structure[2] alongside advanced marks for insignificance. Ring mark permits an endorser to sign details unidentified, that is, the mark is mixed with different gatherings (named ring), and no one (other than the actual underwriter) knows which part of the message was labelled.

Security of data: Health devices or knowledge about health must be error-free and unchangeable for all. To spare programmers 'information, we use a dual encryption plot. Here dual encryption does not relate to scrambling similar information using two but rather information encryption keys and again key encryption used to decipher information. We scramble the details using lightweight ARX calculations and encrypt afterwards the data using the beneficiary's open data. Similarly, we are using the Diffie Hellman key exchange technique to transfer the open keys so it is practically indecipherable for an assailant to get the keys thereby.
Digital Certificate : Digital Certificate is a one kind of document which illustrate the data into to soft format. In today's era various sections in computer science is E- certificate has used fore end uses of

ISSN: 2233-7857 IJFGCN

indication as well as private data transmission. In this work who proposed E- certificate generation for educational documents using blockchain Technology. Basically this certificate has generated by system based on automatic methodology using various secure algorithms.

1 1

Literature Survey

A.G. Said et. al. [1] proposed a system E-Certificate Authentication System Using BlockchainIn short, the program's purpose is: a valid registry with electronic certificates, i.e. an electronic credential is generated at the applicant's request. At the same time, that student's record is preserved by using hash values in blockchain blocks. The customer is also presented with a particular QR code or serial number, in accordance with the E-certificate. And instead the demand unit (e.g. company to which the applicant has applied for a job) must verify the authenticity of the electronic file using the QR code or the relevant serial number based on the reported details in the blockchain Jiin-Chiou Cheng et. al. [2] proposed a system Blockchain and smart contract for digital certificate, Then build an electronic paper document file that follows those related details into the database and thus decides the hash value of the electronic file. Finally, the hash value within the ring is stored in the chain process.

To be affixed to the paper credential, the software will produce a related QR code and question string data. It will involve the demand device for paper certificate validity verification via mobile phone scanning or web site inquiries. Since of the blockchain's unchangeable property, the network not only increases the credibility of unique paper-based certificates but also the authentication risks of various types of certificates electronically types of certificates

Marco Baldi et. al. [3] Certificate Validation The program solves the problem through Shared Ledgers and Blockchains by introducing a mechanism in which several CAs share a transparent, shared and stable database where CRLs are received. To this end, we find the concept of blockchain-based shared ledgers implemented for use of cryptocurrencies, which is becoming a common solution for many web applications of high protection and reliability requirements.

Oliver et. al. [4] illustrates Using blockchain as a Government degree tracking and assessment tool: a business analysis based on two financial factors comparing the service price as the main players between the customer and the employer. Students need a low-cost and easy-to-check evidence of competence, and employers also need swift and accurate documentation of their degree before recruiting. All models are built for growing regional markets and shares to discover ways of extending this sector in the European Union.

Because of the The arbitrary existence of hashing is never a guarantee of producing an appropriate object. Thus, Bitcoin mining is a competitive enterprise where miners are effectively hashed and admitted into the blockchain by awarding new Bitcoin for each block[5].

Miners, a collaborative consumer network, verify and check transactions and set up specialized computation equipment called "hashes." They vote with their CPU strength, demonstrating their approval of legitimate blocks by working to expand them and by declining to operate on invalid blocks[6]. These record strings (hashes) that keep track of any Bitcoin transaction and are repeated on any device in the Bitcoin network.

Blockchain is a decentralized LEDGER used for safe trading of digital currencies, deals and transactions[7], and peer-to-peer network management. All nodes adopt the same internode contact protocol, and verify new objects. If the data is validated in every block no block will change it. To modify individual block data, all corresponding block data will be modified, resulting in network cooperation and denial of the transaction by all nodes

ISSN: 2233-7857 IJFGCN

The The power used to "farm" the cryptocurrency is a key aspect since its costs are rising. According to the Bitcoin statistics site Digiconomist, citizens worldwide use more than 30 terawatts-hours of electricity are mining the crypto-currency. This is greater than, at least, the human energy use 159 countries like Hungary, Oman, Ireland, and Lebanon [8].

Bitcoin mining is a Creation of new Bitcoin process by verifying Bitcoin Network transactions. That transaction is stored in a shared ledger, and all of the machines involved in the Bitcoin network check and manage the ledger. This "net" of transactions is known as the ledger, and. transaction is basically a timestamp for the database that may involve data [9].
Narayanan et al. [10] Describe a block string as a data structure composed of a related array of hash pointers. Every entity in the list is a block containing some previous block data and hash. This renders it a tamper-evident file, implying the data can only be applied to the list and the prior data can not be changed without detection. Hyperledger Sawtooth employs a flexible design, which distinguishes different sections of the device. This means the degree of blockchain is decoupled from stage of implementation. The flexible architecture often ensures that it is possible to modify various elements of thenetwork, based on the project requirement. Examples of the modules that can bemodified involve transaction laws, making and consensus

algorithm. [11] Lamport et al. [12] present algorithms Under different circumstances, that let the generals reach consensus. In a structure where the generals can send recorded, unforgeable letters, the writers illustrate that the dilemma can be solved with any number of generals and traitors. Nonetheless, because of the huge number of communications this approach would be very costly necessary.

Proof of elapsed time (PoET) is a Built consensus approach to be more effective than PoW. PoET can be seen as a function which makes a node wait randomly. In a "trusted execution setting" the feature to determine the amount of time a node should wait This helps the system to identify any users who try to function until their random time elapses. [13]

A distributed ledger, or a website, they have a global environment. The global state is all the material that is contained in the ledger, including the present status. The knowledge used in the global state differs considerably depending on the context of blockchain. [14]

ISSN: 2233-7857 IJFGCN

In Hyperledger Sawtooth, and For other blockchain applications, the transactions are put in batches. Batches are used where transaction order is important. The transactions should be done in the right order by placing certain transactions in the same set. If a transaction does not rely on every other transaction than those that have already been authenticated and deposited in the blockchain, the sender may build a new batch only for that transaction. [15].

System Overview

The system proposed blockchain-based e certificate generation for educational documents. The below figure 1 illustrates the propose system execution to generate a certificate as well as a unique Identification number for specific education students. The verification process per organization has also described in propose execution, the basic objective of the system to eliminate traditional certificate verification and documentation verification time-consuming process. The system follows the blockchain architecture to distribute the data in different data nodes like a distributed environment, in which insurance data can be extracted from different nodes using consensus algorithms. In the below section, we briefly explain our propose system execution with the strategic process.

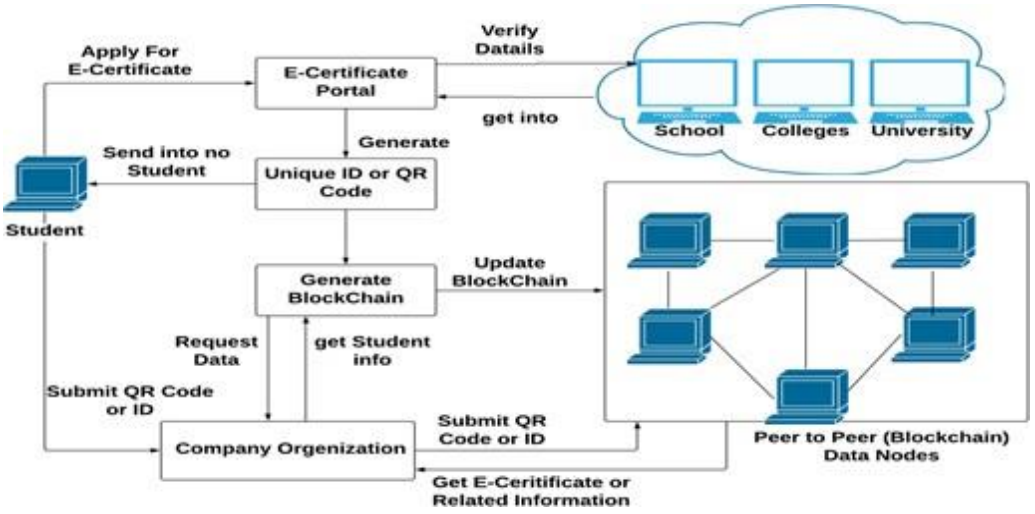


Figure 1 : System Architecture

The above Figure 1 shows e certificate generation using blockchain in P2P environment. In the first phase user or student upload educational documentary on the web portal, the basic assumption behind the system web portal is the trustworthy organization which provide an authentic process of document verification from respective organizations.

ISSN: 2233-7857 IJFGCN

This process system follows once whenever user submit his documents. According to the verification process web, admin generates unique Identification (UID) number and QR code for a particular user. When the system generates those documents data has been automatically stored in different data nodes, and such data should be immutable. When data has Store into the blockchain it follows entire blockchain process as well as algorithms simultaneously. When specific organisation once to validate any user's educational history then they can only submit UID or or can returned QR code and access the E-certificate from the blockchain. This processing difficulty eliminates traditional document verification time-consuming processes and provide a trustworthy framework for organizations.

Results and Discussion

For the measurement of system efficiency the system determines the accuracy matrices. The system is introduced with INTEL 2.8 GHz i3 processor and 4 GB RAM with a distributed environment on java3-tier framework platform. The graph below (b) shows the time taken to validate the blockchain in 4 nodes by a consensus algorithm. The x-axis shows the blockchain scale, and Y shows the time needed for validation in millisec

.

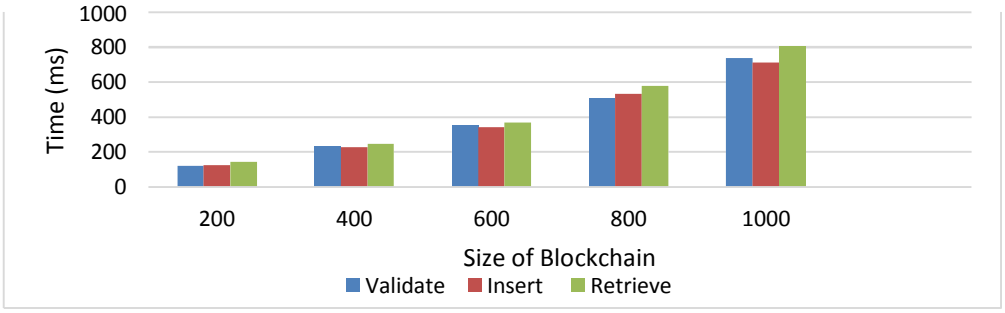
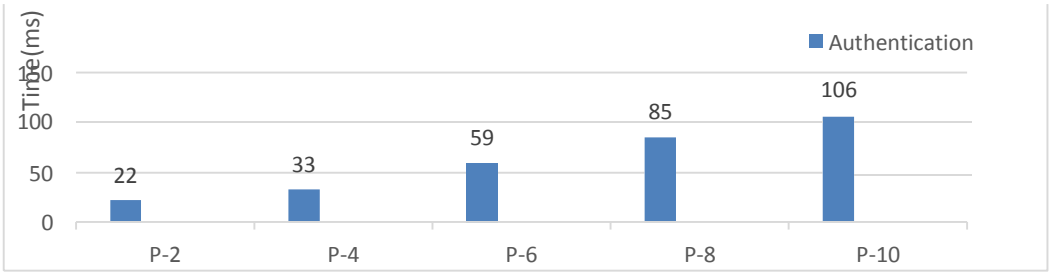


Fig. (b): Time taken in millisec for complete transaction with different blockchain records using 4 data nodes in Peer to Peer Network

In another test case we analyze the proposed model by consensus algorithm with smart contract validation in specific number of peer to peer nodes.



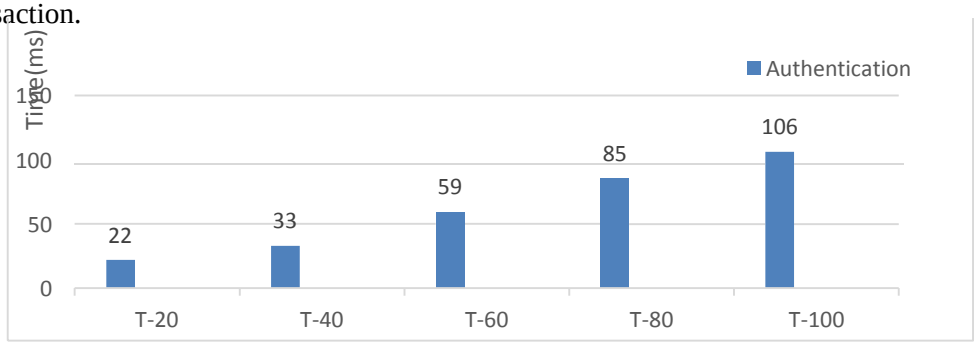
ISSN: 2233-7857 IJFGCN

Size of Blockchain

Fig. (c): Time taken in millisec for smart contract validation with different no. of Peer to Peer network in blockchain.

1 1

The number of variation taken by algorithm from propose SHA value are evaluated in the third test case. This was basically needed to determine whether or not the proposed hash string is true in compliance with the mining policy. In many times when the system generates SHA code for transactional data, the mining policy is never met. To fulfill the proposed mining policy to produce multiple variations on the given string according to the given scenario. The below figure (d) shows the time required to generate the valid SHA string for specific transaction.



No. of Transactions

Fig. (d): Time in milliseconds required for mining for number of transactions

Conclusion

System proposed a new dynamic certificate generation approach using own custom blockchain. First student apply for e-certificate on web portal with upload all educational documents. Web portal is authenticating trusted third party which validate all documents from university, school, colleges etc. Once successfully verification has done from university, school, colleges it will store data into blockchain and same time it generates the unique certificate id or QR code and returns to student. Student can submit the received QR code or certificate id to organization instead of physical hard copy of documents. Organization can submit QR code or id to portal and pool the e-certificate of respective student and make the validation. The entire process has performed into the blockchain manner with smart contract which is written by us. To execute the system in vulnerable environment and to explore and validate how proposed system eliminate different network attacks like DOS and MiM etc. The system also provides automatic data recovery when specific node has destroyed, as well as secure communication between a data node and end-user

Future Work

To implement the system based custom blockchain and some existing clock change like it Ethereum, Ripple, Cordono, etc, ensure the effectiveness of how custom blockchain provide additional significance over the available blockchain frameworks.

References

[1] A.G. Said, R.P. Ashtaputre, B. Bisht, S.S. Bandal, P.N. Dhamale, “E- Certificate

ISSN: 2233-7857 IJFGCN

Authentication System Using Blockchain," International Journal of Computer Sciences and Engineering, Vol.7, Issue.4, pp.191-195, 2019.

[2] Cheng JC, Lee NY, Chi C, Chen YH. Blockchain and smart contract for digital certificate. In2018 IEEE international conference on applied system invention (ICASI) 2018 Apr 13 (pp. 1046-1051). IEEE.

[3] Baldi M, Chiaraluce F, Frontoni E, Gottardi G, Sciarroni D, Spalazzi L. Certificate Validation Through Public Ledgers and Blockchains. InITASEC 2017 (pp. 156-165 Oliver M, Moreno J, Prieto G, Benítez D. Using blockchain as a tool for tracking and verification of official degrees: business model.

[4] George F. Hurlburt and Irena Bojanova, "Bitcoin: Benefit or Curse?," in IEEE, 2014

[5] Satoshi Nakamoto, Bitcoin: A Peer-to-Peer Electronic Cash System, 2008, White Paper.

[6] Nirmala Singh and Sachchidanand Singh, "Blockchain: Future of financial and cyber security," in IEEE, Noida, 2016.

[7] Henrique Rocha ,Marcus Denker and Stephane Ducasse Santiago Bragagnolo, "SmartInspect: solidity smart contract inspector," in IEEE, Itly, p. 2018.

[8] GWYN D'MELLO. (2017, Dec.) https://www.indiatimes.com/technology/news. [Online]. https://www.indiatimes.com/technology/news/bitcoin-miners-are-using-more- electricity-than-irelandother-159-countries-no-kidding-335114.html

[9] Narayanan A., Bonneau J., Felten E., Miller A. & Goldfeder S. (2016) Bitcoin andCryptocurrency Technologies: A Comprehensive Introduction. Princeton: Princeton University Press

[10] Introduction to Hyperledger Sawtooth (2018) Retrieved January 4, 2019 from https://sawtooth.hyperledger.org/docs/core/releases/latest/introduction.html) 49

[11] Lamport, L., Pease, M., & Shostak, R. (1982). The Byzantine generals problem.Menlo Park, CA: SRI International.

[12] PoET 1.0 Specification (2018) Retrieved January 4, 2019 fromhttps://sawtooth.hyperledger.org/docs/core/releases/latest/architecture/poet.ht ml

[13] Global State (2018) Retrieved January 4, 2019 from https://sawtooth.hyperledger.org/docs/core/releases/latest/architecture/global_state. ht ml

[14]Transaction and Bathces (2018) Retrieved January 4, 2019 f

ISSN: 2233-7857 IJFGCN