IJCSE International Journal of Computer Sciences and Engineering Open Access
Research Paper Vol. 9, Issue.7, July 2021 E-ISSN: 2347-2693

Digital Certificate System for Verification of Educational Certificates Using Blockchain

P.S. Gayke[1*], Jayesh Chennur[2], Mulla Muzzamil[3], Jathin Joy[4], Kunal Gosavi[5]

[1,2,3,4,5]Department of Information Technology, DVVP COE Ahmednagar, Maharashtra

[*]*Corresponding Author: pratibha.gayke@gmail.com*

DOI: https://doi.org/10.26438/ijcse/v9i7.6973 | Available online at: www.ijcseonline.org

Received: 18/Jul/2021, Accepted: 20/Jul/2021, Published: 31/Jul/2021

***Abstract*—** In India Ministry of Education statistics, about one million graduates each year, some of them will goto countries, high schools or tertiary institutions to continue to attend, and some will be ready to enter the workplace employment. During the course of study, the students' all kinds of excellent performance certificates, score transcripts, diplomas, etc., will become an important reference for admitting new schools or new works. As schools make various awards or diplomas, only the names of the schools and the students are input. Due to the lack of effective anti-forge mechanism, events that cause the graduation certificate to be forged often get noticed. In order to solve the problem of counterfeiting certificates, the digital certificate system based on block chain technology would be proposed. By the modifiable property of block chain, the digital certificate with anti-counterfeit and verifiability could be made. The procedure of issuing the digital certificate in this system is as follows. First, generate the electronic file of a paper certificate accompanying other related data into the database, meanwhile calculate the electronic file for its hash value. Finally, store the hash value into the block in the chain system. The system will create a related QR-code and inquiry string code to affix to the paper certificate. It will provide the demand unit to verify the authenticity of the paper certificate through mobile phone scanning or website inquiries. Through the modifiable properties of the block chain, the system not only enhances the credibility of various paper-based certificates, but also electronically reduces the loss risks of various types of certificates.

***Keywords*—** Custom Blockchain, Digital Certificate, Hashing, Mining, Smart Contrast

I. INTRODUCTION

The block chain technology opens today opportunities to deliver new business models on quite consolidated markets. The use of block chain in the education sector is one of the most challenging areas where results in the mid and long term can be achieved. The easy, trustable and cheap verification of official documents, such as university degrees, is one of the areas where block chain can provide a timely and solid solution thanks to the use of widely extended that offer a stable public block chain that can be used for secondary uses such as a verification tool in several markets. Here, the selection of an appropriate public block chain in terms of availability, flexibility and cost is crucial to develop a sustainable business model on top[1]. As the data used for scientific research increases exponentially, ensuring information quality and preventing data manipulation has emerged as an important factor in validating the research results. Graduation certificates and transcripts contain information confidential to the individuals and should not be easily accessible to others. Hence, there is a high need for a mechanism that can guarantee that the information in such a document is original, which means that document has originated from an authorized source and is not fake. In addition, the information in the document should be confidential so that it can only be viewed by authorized persons. Blockchain technology is used to reduce the incidence of certificate forgeries and ensure that the security, validity and confidentiality of graduation certificates would be improved. Technologies exist in related domains, such as digital signatures, which are used in e-documents to provide authentication, integrity, and non-repudiation. However, for the requirements of an e-qualification certificate, it has critical security holes and missing functions: for example, it uses the keys to verify the modification of the document, but doesn't start the validation of the public key certificates' status automatically[2]. This may result in a forgery being accepted if the key has been compromised. Furthermore, even the signer's public key certificate has been validated, but the signed document itself hasn't. In our case of an e-qualification certificate, the signed document itself is also a certificate, which may have a valid period (e.g. he problem we are dealing with is a (certificate) issue, therefore, a simple digital signing of the document alone doesn't solve the problem.

The purpose of the proposed system is:

- To eliminate time consuming certificate verification process, for organizations.
- To reduce the database frauds from various attacks.
- To enhance the transaction clarity.
- To improve the trust of system.

The objectives of proposed model are:
- To design and develop a system for dynamic and secure e certificate generation system using smart contract in block chain environment.
- To design own block chain in open source environment with custom mining strategy as well as smart contract.
- To validate and explore system performance using consensus algorithm for proof of validation.

II. Related Work

Jiin-Chiou Chen, Narn-Yih Lee, Chien Chi, and Yi-Hua Chen "Blockchain and Smart Contract for Digital Certificate". In order to solve the problem of counterfeiting certificates, the digital certificate system based on block chain technology would be proposed[3]. By the un-modifiable property of block chain, the digital certificate with anti-counterfeit and verifiability could be made. The procedure of issuing the digital certificate in this system is as follows. First, generate the electronic file of a paper certificate accompanying other related data into the database, meanwhile calculate the electronic file for its hash value. Finally, store the hash value into the block in the chain system. The system will create a related QR-code and inquiry string code to affix to the paper certificate. It will provide the demand unit to verify the authenticity of the paper certificate through mobile phone scanning or website inquiries. Through the un-modifiable properties of the block chain, the system not only enhances the credibility of various paper-based certificates, but also electronically reduces the loss risks of various types of certificates.

Austin Draper, Aryan Familrouhani, Devin Cao, Tevisophea Heng, Wenlin Han "Security Applications and Challenges in Blockchain" Blockchain technology is a highly popular yet highly misunderstood concept that is used today and in future applications[4]. To enhance security and privacy, many applications adopt Blockchain. However, there are intrinsic drawbacks and emerging challenges. In this paper, we study popular security applications in Blockchain, present their major problems, as well as other challenges in Blockchain which allows future research to be conducted more efficiently. Marco Baldi, Franco Chiaraluce, Emanuele Frontoni, Giuseppe Gottardi, Daniele Sciarroni and Luca Spalazzi Certificate "Validation through Public Ledgers and Blockchain". Public key infrastructures (PKIs) are of crucial importance for the life of online services relying on certificate-based authentication, like e-commerce, e-government, online banking, as well as e-mail, social networking, cloud service[5]s and many others. One of the main points of failure of modern PKIs concerns reliability and security of certificate revocation lists, that must be available and authentic any time a certificate is used. Classically, the CRL for a set of certificates is maintained by the same (and sole) certification authority (CA) that issued the certificates, and this introduces a single POF in the system. We address this issue by proposing a solution in which multiple CAs share a public, decentralized and robust ledger where CRLs are collected. For this purpose, we consider the model of public ledgers based on block chain, introduced for the use in crypto-currencies, that is becoming a widespread solution for many online applications with stringent security and reliability requirements.

Santosh Pandey, Gopal ojha, Rohit Kumar and Bikesh Shresha "BlockSIM: A practical simulation tool for optimal network design, stability and planning". In this paper authors introduce BlockSIM, a comprehensive and open source blockchain system simulation tool which can assist blockchain architects better evaluate the performance of planned private block chain networks by running scenarios and decide the optimal system parameters suited for their purposes[6]. Authors compared the results of our simulation with real block chain networks and demonstrate that BlockSIM can be used effectively by architects of block chain systems to plan and implement scalable, stable and resilient block chain networks. Finally, we demonstrate via a real life example how architects can apply BlockSIM to plan and design real-world block chain systems.

Christopher Ehmke, Florian Wessling and Christoph M. Friedrich "Proof-of-Property - A Lightweight and Scalable Blockchain Protocol". The approach proposed in this paper is based on the idea of Ethereum to keep the state of the system explicitly in the current block but further pursues this by including the relevant part of the current system state in new transactions as well[7]. This enables other participants to validate incoming transactions without having to download the whole block chain initially. Following this idea use cases can be supported that require scalable block chain technology but not necessarily an indefinite and complete transaction history.

S. Sunitha kumara, D. Saveetha "Blockchain and Smart Contract for Digital Document Verification" [6] In the system along with the degree certificate entire personality and behavior activities of the person using personal id will be uploaded in block chain. Because of un-modifiable property it is stored in block chain. Initially the student request for the e-certificate by uploading certificate or personal id to electronic certificate system[8]. If requesting for e-certificate, then the system will review certificate from the university or schools or from organization and get the assurance and store the serial number and e-certificate to the block chain. The system will be generating the QR code and send it to the user. when applying for company user will send only the certificate serial number and QR code received from the e-certificate company.

Arvind Ramachandran, Dr. Murat Kantarcioglu "Using Blockchain and smart contracts for secure data provenance management". In this work, authors leverage block chain as a platform to facilitate trustworthy data provenance collection, verification and management. The developed system utilizes smart contracts and open provenance model (OPM) to record immutable data trails[9]. Authors show that our proposed framework can efficiently and securely capture and validate provenance data, and prevent any malicious modification to the captured data as long as majority of the participants are honest.

Ahmed Ben Ayed “Secure storage service of electronic ballot system based on block chain algorithm”. In this paper, authors are going to leverage the open source Blockchain technology to propose a design for a new electronic voting system that could be used in local or national elections[10]. The Blockchain-based system will be secure, reliable, and anonymous, and will help increase the number of voters as well as the trust of people in their governments.

Kaidong Wu “An Empirical Study of Blockchain-based Decentralized Applications”. This paper presents a comprehensive empirical study on an extensive dataset of 734 dapps that are collected from three popular open dapp marketplaces, i.e., ethereum, state of the dapp, and DAppRadar. We analyze the popularity of dapps, and summarize the patterns of how smart contracts are organized in a dapp. Based on the findings, we draw some implications to help dapp developers and users better understand and deploy dapps[11].

Jialiang Chang, Bo Gao, Hao Xiao, Jun Sun and Zijiang Yang “sCompile: Critical Path Identification and Analysis for Smart Contracts”. In this work, authors propose an alternative approach to automatically identify critical program paths (with multiple function calls including inter-contract function calls) in a smart contract, rank the paths according to their criticalness, discard them if they are infeasible or otherwise present them with user friendly warnings for user inspection[12]. Authors identify paths which involve monetary transaction as critical paths, and prioritize those which potentially violate important properties. For scalability, symbolic execution techniques are only applied to top ranked critical paths. Our approach has been implemented in a tool called sCompile, which has been applied to 36,099 smart contracts. The experiment results show that sCompile is efficient, i.e., 5 seconds on average for one smart contract.

III. METHODOLOGY

In Existing system, the problem of fake certificates is a big issue. Companies hiring thousands of fresher spend large amount of money to get the educational certificates and transcripts verified of applicants. To address this problem, we implementation of a Digital Certificate System for verification of educational certificates using block chain technology. To design own block chain in open source environment with custom mining strategy as well as smart contract. E-certificate generation system which manually creates the certificates based on current 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[13]. 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[14]. 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.

Proposed Outcome

- No dummy transaction has accepted by system on same documentary.
- Peer-to-peer global transactions.
- Automatic attack recovery by system.
- Quality assurance during the transaction
- Immediate show all historical transaction is single click, without any third party interface.

Educational documents verification is very tedious and time consuming process in real time environment. E-Certificate generation for entire educational history is easy process to eliminate such consuming tasks. Dynamic QR-code and unique certificate generation for each students document in proposed system. Data e-certificate stored into the blockchain in secure manner which enhance the security. According to the smart contract system also allow the updates in entire block chain. This research proposed a custom blockchain generation on open source platform[15].

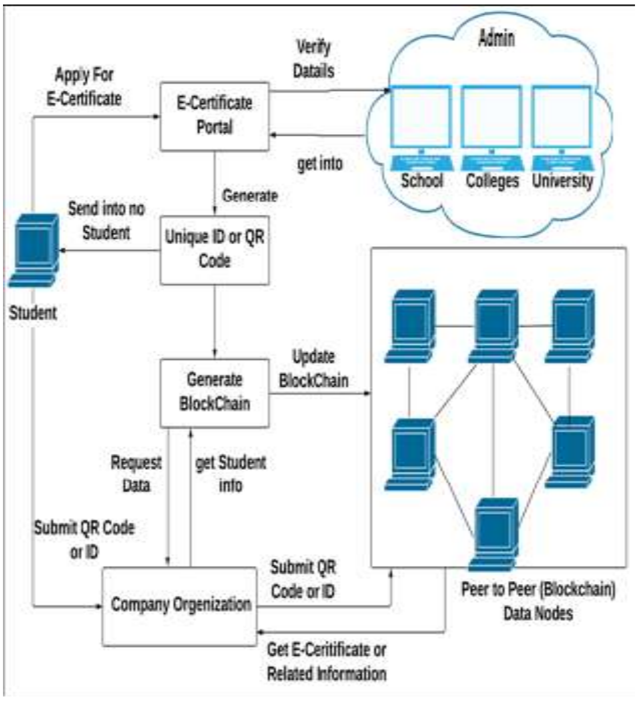

Figure 1 Architecture Diagram

To create the block chain based un-modifiable certificates, initially the university needs to get registered. Each university will be having its wallet address from which it is going to send transaction. University can be added only by the owner of the smart contract. Once added the university can access the system and can create certificates with data fields. Each created certificate will be stored in the Inter planetary file system (IPFS) which in turn will return the unique hash generated using SHA-2S6 algorithm. This will serve as unique identity for each document. Along with this generated hash and detail of certificates, all this data will be stored in the block chain and the resultant transaction id will be sent to the student. Anyone can use this transaction id to verify the certificate details and can view the original copy of certificate using IPFS hash stored along with data. And it is almost impossible to modify this certificate or to create fake certificate with same data. Hence with this we can solve the problem of counterfeit certificates[16].

IV. Results and Discussion

System proposed a new dynamic certificate generation approach using own custom block chain.

- First student apply for e-certificate on web portal with upload all educational documents.
- Web portal is authenticate 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 block chain 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 perform into the block chain 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.

Algorithm 1: Hash Generation

Input : Genesis block, Previous hash, data d,

Output : Generated hash H according to given data

```
• Step 1 : Input data as d
• Step 2 : Apply SHA 256 from SHA family
• Step 3 : CurrentHash= SHA256(d)
• Step 4 : RetrunCurrentHash
```

Algorithm 2: Protocol for Peer Verification

Input: User Transaction query, Current Node Chain CNode[chain], Other Remaining Nodes blockchain NodesChain[Nodeid] [chain],

Output: Recover if any chain is invalid else execute current query

```
• Step 1 : User generate the any transaction DDL, DML or
  DCL query
• Step 2: Get current server blockchain Cchain Cnode
• Step 3 : For each
        $NodesChain\ [Nodeid, Chain] \sum_{i=1}^{n} (GetChain)$
  End for
• Step 4 : Foreach (read I into NodeChain)
        If (!.equals NodeChain[i] with (Cchain))
        Flag 1
        Else Continue Commit query
• Step 5 : if (Flag == 1)
• Count = SimilaryNodesBlockchian()
• Step 6 : Calculate the majority of server
• Recover invalid block chin from specific node
• Step 7: End if
  End for
End for
```

Algorithm 3: Mining Algorithm for valid hash creation

Input: Hash Validation Policy P[], Current Hash Values hash Val

Output : Valid hash

```
• Step 1 : System generate the hash Val for ith transaction
  using Algorithm 1
• Step 2 : if (hash Val.valid with P[])
• Valid hash
        Flag =1
        Else
        Flag=0
• Mine again randomly
• Step 3 : Return valid hash when flag=1
```

Overview of Project Modules:

- System proposed a new dynamic certificate generation approach using own custom block chain.
- 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.
- Once successfully verification has done from university, school, colleges it will store data into block chain 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 hard copy of documents.
- Organization can submit QR code or id to portal and pool the e-certificate of respective student for validation.
- The entire process has perform into the block chain 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.

Module Split-Up

1. **Student:** First student apply for e-certificate on web portal with upload all educational documents. Student can submit the received QR code or certificate id to organization instead of physical hard copy of documents.
2. **University, School and Colleges(Admin):** 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 block chain and same time it generates the unique certificate id or QR code and returns to student.

3. **Organization:** Organization can submit QR code or id to portal and pool the e-certificate of respective student and make the validation. Entire process has performed into the block chain manner with smart contract which is written by us. To execute system in vulnerable environment and to explore and validate how proposed system eliminate different network attacks like DOS and MiM etc.

V. 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.

REFERENCES

[1] Sukhodolskiy, Ilya, and Sergey Zapechnikov. "*A blockchain-based access control system for cloud storage*" Young Researchers in Electrical and Electronic Engineering (EIConRus), IEEE Conference of Russian.IEEE, **2018**.

[2] D. Vidhate, P. Kulkarni,"*Performance comparison of multiagent cooperative reinforcement learning algorithms for dynamic decision making in retail shop application*", International Journal of Computational Systems Engineering, Inderscience Publishers (IEL), Vol **5**, Issue **3**, pp **169-178**, **2019**.

[3] A. Dorri, S. S. Kanhere, and R. Jurdak, "*Blockchainin internet of things: Challenges and Solutions*,"arXiv:1608.05187, **2016**.

[4] D. Vidhate, P. Kulkarni, "*A Framework for Dynamic Decision Making by Multi-agent Cooperative Fault Pair Algorithm (MCFPA) in Retal Shop Application*",Information and Communication Technology for Intelligent Systems, Springer, Singapore, pp **693-703**, **2018**.

[5] Yang, Huihui, and Bian Yang "*A Blockchain-based Approach to the Secure Sharing of Healthcare Data*"Proceedings of the Norwegian Information Security Conference **2017**.

[6] D. Vidhate, P. Kulkarni,"*A Novel Approach by Cooperative Multiagent Fault Pair Learning (CMFPL)*", Communications in Computer and Information Science, Springer, Singapore, Volume **905**, pp **352-361**, **2018**.

[7] Goyal, Vipul, et al. "*Attribute-based encryption for fine-grained access control of encrypted data*" Proceedings of the 13th ACM conference on Computer and communications security.Acm, **2006**.

[8] D. Vidhate, P. Kulkarni,"*Exploring Cooperative Multi-agent Reinforcement Learning Algorithm (CMRLA) for Intelligent Traffic Signal Control*", Smart Trends in Information Technology and Computer Communications, Volume **876**, pp **71-81**,**2018**.

[9] Wang, Hao, and Yujiao Song. "*Secure cloud-based EHR system using attributebased cryptosystem and blockchain*" Journal of medical systems 42.8 (**2018**), 152.

[10] D. Vidhate, P. Kulkarni, "*A Framework for Improved Cooperative Learning Algorithms with Expertness (ICLAE)",* International Conference on Advanced Computing and Communication Technologies Advances in Intelligent Systems and Computing, Springer Singapore, Volume **562**, pp. **149-160**, **2017**.

[11] Khan S, Khan R. "*Multiple authorities attribute-based verification mechanism for Blockchain mircogrid transactions*"Energies May;11(5), **1154**, **2018**.

[12] Guo, Rui, et al. *"Secure attribute-based signature scheme with multiple authorities for Blockchain in electronic health records systems"* IEEE Access 776.99, **1-12**, **2018**.

[13] Ouaddah, Aafaf, AnasAbouElkalam, and AbdellahAitOuahman. "*FairAccess: a new Blockchain-based access control framework for the Internet of Things*." Security and Communication Networks 9.18, **5943-5964**, **2016**.

[14] Wu, Axin, et al "*Hidden policy attribute-based data sharing with direct revocation and keyword search in cloud computing*" Sensors 18.7, 2158, **2018**.

[15] Rahulamathavan, Yogachandran, et al. "*Privacy-preserving block chain based IoT ecosystem using attribute-based encryption*" IEEE International Conference on Advanced Networks and Telecommunications Systems (ANTS), IEEE, **2017**.

[16] D.Vidhate, P. Kulkarni,"*Expertise Based Cooperative Reinforcement Learning Methods (ECRLM)",* International Conference on Information & Communication Technology for Intelligent System, Springer book series Smart Innovation, Systems &Technologies,Vol.**84**,Springer Cham,pp**350-360**, **2017** .