International Journal of Research Publication and Reviews

Journal homepage: www.ijrpr.com ISSN 2582-7421

Digital Certificate Verification Using Blockchain Technology

Khushal Y. Bheke[1], *Aniket R. Misal*[2], *Nilkanth S. Pokharkar*[3], *Prof. Gunjal T. S.*[4]

[1,2,3] UG Student, Department of Computer Engineering, Samarth Group of Institution College of Engineering Belhe, India
[4]Guide, Department of Computer Engineering, Samarth Group of Institution College of Engineering Belhe, India
khushalbheke8@gmail.com, aniketmisal086@gmail.com, nilkanthpokharkar@gmail.com

ABSTRACT:

While the number of universities, tertiary education students and number of graduates per year constantly increase, the need to easily verify degree certificates generates new business opportunities. In this paper we project two financial models balancing where the price for the service is balanced between the graduate and the employer as the main stakeholders of that service. Students demand a proof-of-certification at low cost and easy to check, employers also demand quick and trustable verification of degrees when recruiting. According to the researches done till date millions of students graduate every year. The problem of fake certificates is a big issue. Getting fake educational certificates in India is not that difficult. Companies hiring thousands of fresher spend large amount of money to get the educational certificates and transcripts verified of applicants. A Digital Certificate using blockchain technology can address this problem. Blockchain is a decentralized distributed digital ledger collectively maintained by a network of computers, called nodes. The data in the blockchain cannot be modified by a person without the consent of everyone else who maintains the records. This makes the data secure.

Keywords: Blockchain, Document Verification, Digital Certificate distributed, Preprocessing, etc.

INTRODUCTION

The blockchain technology opens today opportunities to deliver new business models on quite consolidated markets. The use of blockchain 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 blockchain can provide a timely and solid solution thanks to the use of widely extended that offer a stable public blockchain that can be used for secondary uses such as a verification tool in several markets. Here, the selection of an appropriate public blockchain in terms of availability, flexibility and cost is crucial to develop a sustainable business model on top.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 nonrepudiation. 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. 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. The problem we are dealing with is a (certificate) issue, therefore, a simple digital signing of the document alone doesn't solve the problem.

PROBLEM DEFINITION AND OBJECTIVES

Problem Defination

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 blockchain technology.

Objectives:

- The system saves on paper, cuts management costs, prevents document forgery and provides accurate and reliable information on digital certificates.
- The system assures information accuracy, security and immutability.
- To implement a verification algorithm which can validate each peer on every access request.

LITERATURE REVIEW

Jiin-Chiou Chen, Narn-Yih Lee, Chien Chi, and Yi-Hua Chen “Blockchain and Smart Contract for Digital Certificate” [1] In order to solve the problem of counterfeiting certificates, the digital certificate system based on blockchain technology would be proposed. By the unmodifiable property of blockchain, 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 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 unmodifiable properties of the blockchain, 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” [2] Blockchain technology is a highly popular yet highly misunderstood concept that is used today and in future applications. 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” [3] 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 services 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 blockchain, introduced for the use in cryptocurrencies, 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” [4] In this paper we introduce BlockSIM, a comprehensive and open source blockchain system simulation tool which can assist blockchain architects better evaluate the performance of planned private blockchain networks by running scenarios and decide the optimal system parameters suited for their purposes. We compare the results of our simulation with real blockchain networks and demonstrate that BlockSIM can be used effectively by architects of blockchain systems to plan and implement scalable, stable and resilient blockchain networks. Finally, we demonstrate via a real life example how architects can apply BlockSIM to plan and design real-world blockchain systems. Christopher Ehmke, Florian Wessling and Christoph M. Friedrich “Proof-of-Property - A Lightweight and Scalable Blockchain Protocol” [5] 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. This enables other participants to validate incoming transactions without having to download the whole blockchain initially. Following this idea use cases can be supported that require scalable blockchain 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 proposing system along with the degree certificate entire personality and behavior activities of the person using personal id will be uploaded in blockchain. Because of unmodifiable 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. 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” [7] In this work, we leverage blockchain 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. We 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” [8] In this paper, we 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. 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” [9] 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. Jialiang Chang, Bo Gao, Hao Xiao, Jun Sun and Zijiang Yang “sCompile: Critical Path Identification and Analysis for Smart Contracts” [10] In this work, we 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. We 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. Satoshi Nakamoto et.al [4] mentioned a peer to peer electronic cash system (Bitcoin). 2016. Online Payments or transaction where directly send from one party to another without going through a financial institution which undergoes peer to peer communication. Digital signatures play a role in protection at a limit. The proposed system uses a verification of data and secure transmission of money through bank validation. Smart Contracts also called crypto-contract, it is a computer program used for transferring / controlling the property or digital currents in specific parties. It does not only determine the terms and conditions but may also implement that policy / agreement. These smart contracts are stored on block-chain and BC is an ideal technology to store these contracts due to the ambiguity and security. Whenever a transaction is considered, the smart-contract determines where the transaction should be transferred / returned or since the transaction actually happened. Currently CSIRRO team has proposed a new approach to integrate Block on IOT with [2]. In its initial endeavor, he uses smart-home technology to understand how IOT can be blocked. Block wheels are especially used to provide access control system for Smart- Devices Transactions located on Smart-Home. Introducing BC technology in IOT, this search again provides some additional security features; however, every mainstream BC technology must have a concept that does not include the concept of comprehensive algorithms.

MOTIVATION

These certificates while applying for jobs at public or private sectors, where all these certificates are needed to be verified manually. There can be incidents where students may produce the fake certificate and it is difficult to identify them. This problem of fake academic certificates has been a longstanding issue in the academic community. Because it is possible to create such certificates at low cost and the process to verify them is very complex, as they are manually needed to be verified. This problem can be solved by storing the digital certificates on the Blockchain.

PROPOSED SYSTEM

System Feature

A system failure can occur because of a hardware failure or an every software issue, causing the system to freeze, reboot, or stop functioning altogether. A system failure may or may not result in an error being displayed

on the screen. The computer may shut off without warning and without any error message. If an error message is displayed, it often is displayed as error.

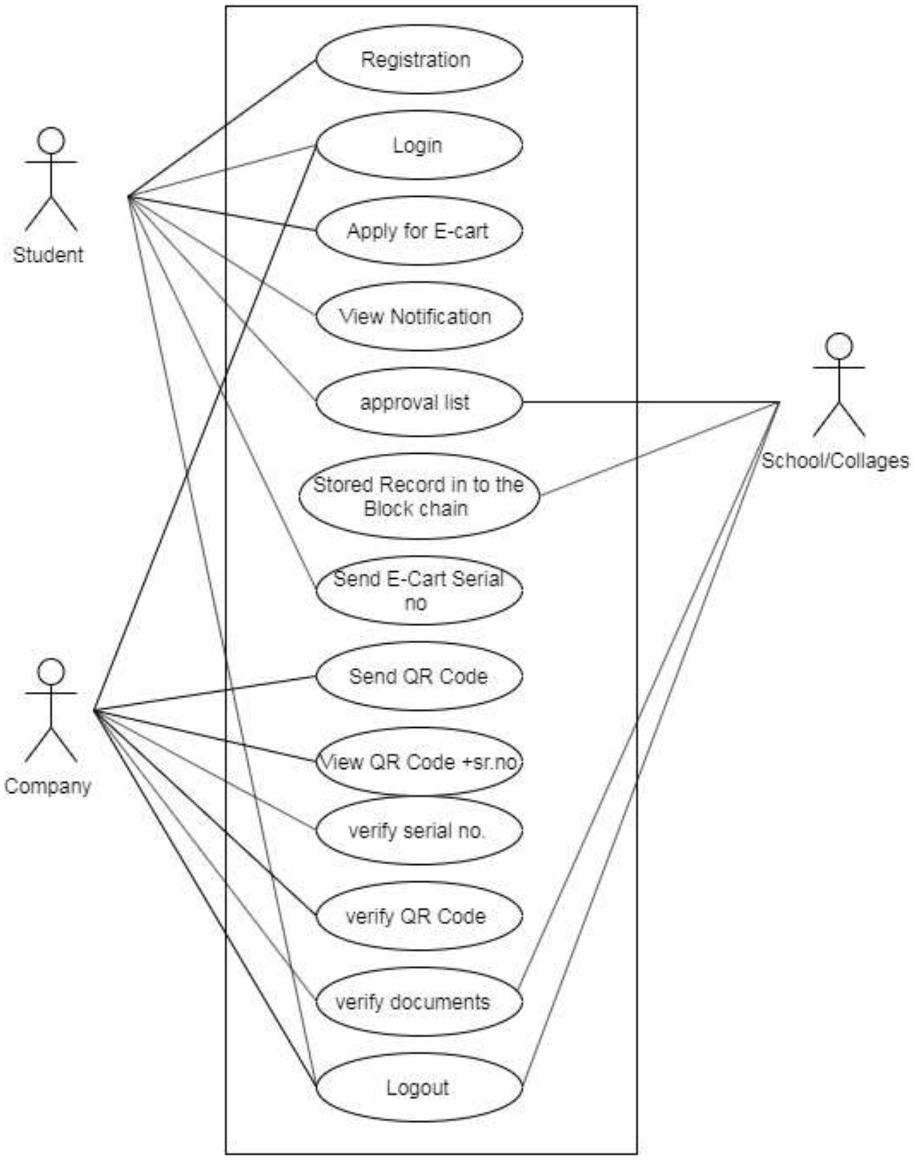
System Feature2 (Functional Requirement)

This section describes the functional requirements of the application and the features it provides. System features are described in detail to help the future extension and testing of the system. Features stated here are already parts of the implemented system so no prioritization is needed. Priority is needed for features to be developed that will be added to this document later.

ALGORITHMS

- **Smart Contract:** Smart contracts are simply programs stored on a blockchain that run when predetermined conditions are met. They typically are used to automate the execution of an agreement so that all participants can be immediately certain of the outcome
- **SHA256 Hash generation:** SHA-256 stands for Secure Hash Algorithm 256-bit and it's used for cryptographic security. Cryptographic hash algorithms produce irreversible and unique hashes. The larger the number of possible hashes, the smaller the chance that two values will create the same hash.
- **Mining:** "Mining" is a metaphor for the computational work that nodes in the network undertake in hopes of earning new tokens. In reality, miners are essentially getting paid for their work as auditors.

USE CASE DIAGRAM



ARCHITECTURE OF SYSTEM

To create the blockchain based unmodifiable 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 blockchain 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.

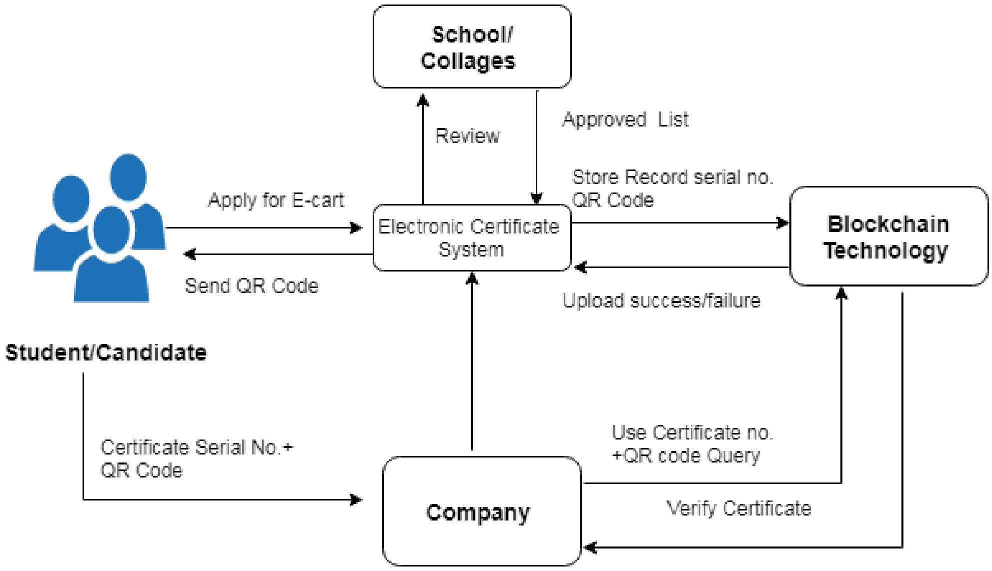


Fig. Architecture Of System

RESULT

- To implement a decentralized application and designed a certificate system based on Custom blockchain.
- To address the feature of this technology which is it is incorruptible, encrypted, and trackable and permits data synchronization.
- To improves the efficiency operations at each stage.
- Proposed system address the system saves on paper, cuts management costs, prevents document forgery, and provides accurate and reliable information on digital certificates.

CONCLUSION

Various technologies have been discussed to reduce the incidence of certificate forgeries and ensure that the security, validity and confidentiality of graduation certificates, even though there are many limitations regarding the security and privacy of data. A new blockchain-based system reduces the certificate forgery. Automated certificate granting is open and transparent in the system. Companies or organizations can thus inquire for information on any certificate from the system. In the proposed system, we save the cuts management costs, prevents document forgery, and provides accurate and reliable information on digital certificates.

REFERENCES

[1] Jiin-Chiou Chen, Narn-Yih Lee, Chien Chi, and Yi-Hua Chen "Blockchain and Smart Contract for Digital Certificate" Proceedings of IEEE International Conference on Applied System Innovation 2018 IEEE ICASI 2018- Meen, Prior & Lam (Eds)

[2] Austin Draper, Aryan Familrouhani, Devin Cao, Tevisophea Heng, Wenlin Han "Security Applications and Challenges in Blockchain" Published in IEEE International Conference on Consumer Electronics (ICCE) 2019

[3] Marco Baldi, Franco Chiaraluce, Emanuele Frontoni, Giuseppe Gottardi, Daniele Sciarroni and Luca Spalazzi Certificate "Validation through Public Ledgers and Blockchains" In Proceedings of the First Italian Conference on Cybersecurity (ITASEC17) 2017

[4] Neethu Gopal, Vani V Prakash "Survey on Blockchain Based Digital Certificate System" International Research Journal of Engineering and Technology (IRJET) Nov 2018

[5] Santosh Pandey, Gopal ojha, Rohit Kumar and Bikesh Shresha "BlockSIM: A practical simulation tool for optimal network design, stability and planning" 2019 IEEE International Conference on Blockchain and Cryptocurrency (ICBC).

[6] Christopher Ehmke, Florian Wessling and Christoph M. Friedrich "Proof-of-Property - A Lightweight and Scalable Blockchain Protocol" 2018 IEEE/ACM 1st International Workshop on Emerging Trends in Software Engineering for Blockchain (WETSEB)