International Journal of Current Engineering and Technology
E-ISSN 2277 – 4106, P-ISSN 2347 – 5161

Available at http://inpressco.com/category/ijcet

Research Article

Maintaining Authenticity of Digital Certificates using Blockchain

Aniruddha Ashok Khadse and Dr. Sandeep. U. Kadam

Department of Computer Engineering TSSM's BSCOER Narhe, Pune-411041

Received 10 Nov 2020, Accepted 10 Dec 2020, Available online 01 Feb 2021, **Special Issue-8 (Feb 2021)**

Abstract

According to several researches huge number of graduates are passing out every year, the certificate issuing authorities are seems to be compromised for the security credentials of student data. Due to the lack of effective antiforge mechanism, graduation certificates which are copied often get noticed. We can conquer this problem by using digital certificate, though security issues still exist. Blockchain is one of the most recent technologies that can be adopted for the data security. It helps to overcome the problem of certificate forgery because of its unmodifiable property. Digital certificate is issued using following procedure. First, produce the electronic file of a paper certificate accompanying other related data into the database, meanwhile calculate the electronic file for its hash value. After that it will store the hash value into the block in the chain system. The system will generate a related QR- code and inquiry string code to attach to the paper certificate. It will provide the demand unit to verify the genuineness of the paper certificate through mobile phone scanning or website inquiries. Because of the unmodifiable properties of the blockchain, the system not only enhances the authenticity of various paper-based certificates, but also electronically reduces the loss risks of various types of certificates.

Keywords: *Blockchain, digital certificate, QR Code*

Introduction

Advances in data innovation, the wide accessibility of the Internet, and regular use of cell phones have changed the way of life of individuals. Virtual cash, computerized coins initially intended for utilize on the web, has started to be widely embraced, all things considered. As a result of the comfort of the Internet, different virtual monetary standards are flourishing, including the most well known—Bitcoin, Ether, and Ripple—the estimation of which has flooded as of late. Individuals are starting to focus on blockchain, the spine innovation of these progressive monetary standards. Blockchain highlights a decentralized and morally sound database that has high potential for a different scope of employments. Blockchain is a circulated database that is broadly utilized for recording particular exchanges. Graduation endorsements and transcripts contain data secret to the people and ought not be effectively open to other people. Thus, there is a significant requirement for a system that can ensure that the data in such a record is unique, which implies that report has started from an approved source and isn't phony. Furthermore, the data in the archive ought to be private with the goal that it must be seen by approved people. Blockchain innovation is utilized to decrease the occurrence of testament falsifications and guarantee that the security, legitimacy and secrecy of graduation authentications would be improved.

As instruction turns out to be increasingly expanded, decentralized and democratized, we despite everything need to look after notoriety, trust in affirmation, and evidence of learning. These days everybody needs to show his/her Document and Certificate to some other individual for some reason/work. In the wake of seeing the record third individual can't approve the innovation of the declaration.

Motivation

In previous years, it has been come into the light and come in our daily routine life, that we got to know, below cases, Some company has fired xyz employee due to fraud educational document.

- Someone is selling the same land to the number of peoples.
- The same driving license number is issued to the number of peoples.
- Same Voter ID is issued to many peoples.
- A doctor has a fake degree, and he is doing practicing.

Many people paste the other people photograph on some other ID proof and use the scan copy/ Photocopy as an Identity proof. From above we see that above incident happens as we have no channel to check the authenticity. If someone has a fake document, we have no options to verify the authenticity.

Objective

To design Blockchain and Smart Contract for Digital Certificate

Review of Literature

As indicated by the Taiwan Ministry of Education insights, around one million alumni every year, some of them will go to nations, secondary schools or tertiary foundations to proceed to join in, and some will be prepared to enter the work environment business. Over the span of study, the understudies' a wide range of astounding execution authentications, score transcripts, recognitions, and so on., will turn into a significant reference for conceding new schools or new works. As schools make different honors or recognitions, just the names of the schools and the understudies are input. Because of the absence of powerful enemy of fashion component, occasions that cause the graduation authentication to be produced regularly get took note. So as to take care of the issue of forging endorsements, the advanced declaration framework dependent on blockchain was proposed in [1]. By the unmodifiable property of blockchain, the computerized declaration with hostile to fake and evidence could be made. The method of giving the computerized authentication right now as follows. To begin with, produce the electronic document of a paper endorsement going with other related information into the database, in the mean time compute the electronic record for its hash esteem. At long last, store the hash an incentive into the square in the chain framework. The framework will make a related QRcode and request string code to attach to the paper declaration. It will give the interest unit to confirm the genuineness of the paper testament through cell phone filtering or site requests. Through the unmodifiable properties of the blockchain, the frame work not just improves the validity of different paper based endorsements, yet in addition electronically diminishes the misfortune dangers of different sorts of testaments As indicated by different explores around one million alumni spending out every year, the authentication giving specialists are is by all accounts traded off for the security qualifications of understudy information. Because of the absence of successful antiforge system, occasions that cause the graduation authentication to be manufactured frequently get took note. So as to take care of this issue computerized testament frameworks are presented despite the fact that security issues are still exist. Blockchain is one of the latest innovation that can be embraced for the information security. The unmodifiable property of the square chain assists with conquering the issue of declaration falsification. Different instances of the advanced testament framework is referenced in paper [2]. Over the span of training the understudies accomplish numerous endorsements. Understudy produce these testaments while going after positions at open or private segments, where every one of these declarations are should have been checked physically. There can be episodes where understudies may deliver the phony testament and it is hard to recognize them. This issue of phony scholarly endorsements has been a longstanding issue in the scholastic network. Since it is conceivable to make such testaments requiring little to no effort and the procedure to check them is unpredictable, as they are physically should have been confirmed. This issue can be illuminated by putting away the advanced declarations on the Blockchain. The Blockchain innovation gives permanence and freely irrefutable exchanges, these properties of Blockchain can be utilized to produce the computerized declaration which are hostile to fake and simple to check [3]. In the conventional instructive comprehension, people follow the way of getting graduate or post-graduate training in the event that they wish, in the wake of proceeding with their instruction from kindergarten to secondary school. Today, by escaping this generalization, each educated individual can pick distinctive learning situations. Presently, learning any subject is up to the tip of the fingers of a person without relying upon a school working with four dividers or on certain time period. In [4], it is planned to confirm advanced endorsements given to the members at the Turkish phase of the International Informatics and Computational Thinking occasion by utilizing Ethereum Block Chain based keen agreement. The assignments in the occasion were transmitted to the understudies in Turkey by means of utilizing test module of the Moodle Learning Management System. For this examination, initial a brilliant agreement was created in which the declaration data could be put away on the Ethereum blockchain and could be check for control purposes if essential. At that point the authentication module created by the scientist in 2014 which uses square structure in the Moodle Learning Management System was refreshed and afterward furnished to work as per the brilliant agreement in the Ethereum blockchain.

Lakhs of individuals getting Degrees a seemingly endless amount of time after year, because of the absence of successful enemy of fashion instrument, occasions that cause the graduation declaration to be manufactured regularly get took note. So as to take care of the issue of forging authentications, the computerized endorsement framework dependent on square chain innovation. All the criminal operations filled against an individual and all the exercises are refreshed in the Personal ID. Utilizing the adjustment procedure we would screen the degree cortication alone as well as whole character and social exercises of that individual. Priya R et al [5] convey Unique based checking utilizing this framework. Blockchain innovation has developed from being an unchanging record of exchanges for cryptographic forms of money to a programmable intelligent condition for building conveyed dependable applications. In spite of the fact that, blockchain innovation has been utilized to

address different difficulties, to creator's information none of the past work concentrated on utilizing blockchain to build up a safe and changeless logical information provenance the executives system that consequently confirms the provenance records. In [6], Aravind Ramachandran et al influence blockchain as a stage to encourage reliable information provenance assortment, check and the executives. The created framework uses shrewd agreements and open provenance model (OPM) to record changeless information trails. Creator show that our proposed system can effectively and safely catch and approve provenance information, and forestall any vindictive change to the caught information as long as lion's share of the members are straightforward The Main reason for paper [7] is to build up a hypothetical structure for blockchain. Our point is to recognize the hindrances and principle drivers of computerized development and investigate the conceivable outcomes of utilizations of blockchain. A contextual investigation approach is applied: the Norwegian seaward industry. Essential information is gathered through the meetings and auxiliary information is gathered from reports of businesses and organizations, the Internet, and national and global media reports. We have found that intensions of cost decrease, and the measure of enormous information that sea organizations should process, alongside the successful work intension, are the principle drivers of advanced development. Then again, the terrible nature of web, significant expense usage, the innovation situated culture, the absence of speculation activities, and hazard avoidance are the principle boundaries. A portion of the hindrances and thought processes of advanced development and the prologue to blockchain innovation were called attention to by before considers. Be that as it may, we have recognized numerous interesting drivers and hindrances explicit to the business. At last, the structure of blockchain process created. One of the examinations prescribes distinctive Learning Management Systems (LMS), Learning Record Stores (LRS), a square chain-based methodology for interfacing learning information among foundations and associations. Subsequently, it is attempted to exploit the blockchain innovation's capacity to give consistency, ease of use, changelessness, security, protection and access control of learning information. The highlights of the proposed framework can be recorded as follows: "Appropriated Consensus and Immutableness"; "Brilliant Contract Based Privacy, Security and Access Control" and "Single Ledger, Multiple Participants [8]. In light of the learning results, an investigation wherein instructive reason blockchain innovation is tended to utilized this innovation and a programmed appraisal programming as a learning apparatus dependent on the college's graduation condition record and expert accreditation. Subjective and quantitative surveyed evaluations, procedure and confirmations, name obviously, name of learning yield (graduation condition marker) and credit obviously, and so forth., are spared to the square. In the assessment of the understudies' accomplishment, the change towards the post- work capability assessments is finished and the educational program is constantly evolved by sending an educational program to assess the troubles confronting understudy achievement [9]. Another investigation portrays another square based engineering that considers security and protection for u- learning situations. With this engineering, a safe learning framework dependent on participation in decentralized topology is structured. This postgraduate exposition study tends to certain issues that concentrated e-learning stages may experience and stresses the significance of decentralized access control in tackling these issues. Right now, model proposition for decentralized access frameworks is introduced. In the acknowledgment of this model, blockchain structure was used. Hence, it is contended that the respectability, rightness, deniability, and detectability of e-learning sources can be accomplished. The mean reaction time was utilized as a metric when assessing the proposed model. The two diverse system situations, (for example, the Local Area Network (LAN) and the Cloud Web Service (for example Amazon Web Service)) are looked at. It is expressed that LAN condition speaks to the most fitting condition and the cloud condition speaks to the genuine circumstance in reality. The normal reaction time in the LAN condition is quicker (about 1.5 occasions) than in the cloud condition, however when the quantity of clients is huge, the distinction in normal reaction time between these two situations becomes irrelevant [10].

Proposed Methodology

A blockchain, initially square chain, is a consistently developing rundown of records, called squares, which are connected and verified utilizing cryptography. Each square regularly contains a cryptographic hash of the past square, a timestamp and exchange information. By structure, a blockchain is intrinsically impervious to change of the information. It is "an open, appropriated record that can record exchanges between two gatherings productively and in an undeniable and lasting manner". Blockchain is a decentralized record used to safely trade computerized money, perform arrangements and exchanges and oversaw by distributed systems. All hubs follow same convention for internode correspondence and approving new squares. When information is approved in any square it can't be adjusted by any square. To change specific square information all ensuing square information ought to be adjusted that will bring about intrigue of the system and that exchange will be dismissed by all hubs. Online records may not be state-of-the-art or have missing data. The blockchain innovation may have the option to tackle these issues by giving another approach to store advanced endorsements.

A. Architecture

Right now, blockchain endorsement framework was created dependent on pertinent innovation. The framework's application was modified on the Ethereum stage and is controlled by the EVM. In the framework, three gatherings of clients are included. Schools or accreditation units award authentications, approach the framework, and can peruse the framework database. At the point when understudies satisfied certain prerequisites, the specialists award an authentication through the framework. After the understudies have gotten their testament, they can ask about any declaration they have picked up. The specialist co-op is liable for framework support.

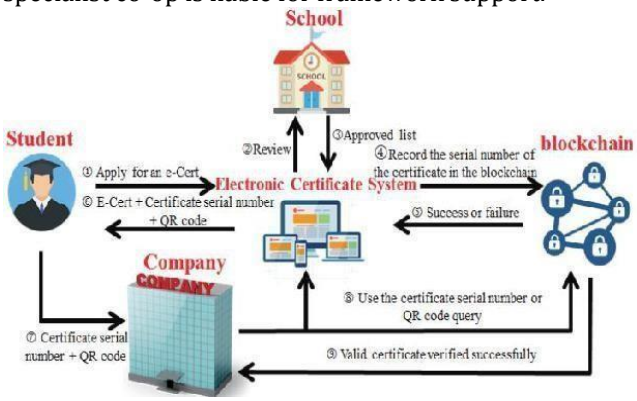

Fig 1 system architecture

Blockchain is a decentralized circulated database. The working procedures of the framework created right now as follows:

- Schools award a degree testament and enter the understudy's information into the framework. Next, the framework consequently records the sequential number of the understudy in a blockchain.
- The testament framework checks all the information.
- Instead of sending traditional printed versions, schools award e-authentications containing a brisk reaction (QR) code to the alumni whose information have been effectively confirmed. Each graduate additionally gets a request number and electronic record of their authentication.
- When going after a position, an alumni essentially sends the sequential number or e-declaration with a QR code to the objective organizations.

•The organizations send requests to the framework and are educated if the sequential numbers are approved. The QR code empowers them to perceive if the endorsement has been messed with or fashioned.

B. Algorithms

Since its 2008 appearance as a foundation of the cryptographic money Bitcoin, the blockchain innovation increased across the board consideration as a methodology to safely approve and store data without a confided in outsider. Blockchain is a decentralized exchange and information the board innovation grew first for Bitcoin digital currency. Blockchain highlights a decentralized and ethical database that has high potential for an assorted scope of employments. A blockchain, initially square chain, is a constantly developing rundown of records, called squares, which are connected and verified utilizing cryptography. Each square commonly contains a cryptographic hash of the past square, a timestamp and exchange information. By plan, a blockchain is innately impervious to change of the information. It is "an open, appropriated record that can record exchanges between two gatherings productively and in an evident and perpetual manner". Blockchain is a decentralized record used to safely trade advanced money, perform arrangements and exchanges and oversaw by distributed systems. All hubs follow same convention for internode correspondence and approving new squares. When information is approved in any square it can't be changed by any square. To modify specific square information all ensuing square information ought to be adjusted that will bring about plot of the system and that exchange will be dismissed by all hubs. In 2008, Satoshi Nakamoto imagined the blockchain for the utilization of digital currency and Bitcoin was its first execution. Bitcoin was the first open exchange record. The innovation of this cash tackled the twofold spending issue without the need of an outsider. After that other cryptographic money were designed on same idea. So, a blockchain is a disseminated database that contains a rundown of records (information). Circulated implies that as opposed to being put away on a focal gadget some place, the whole database is effectively synchronized and put away on a lot of different gadgets. This is known as a distributed system, much like how Napster was a distributed system for sharing music records. The primary bit of leeway this innovation gives is its capacity to trade exchanges without depending on confided in outsider elements of any methods. It can likewise give information respectability, in-manufactured validness and client straightforwardness.

Obstructs: A square contains set of substantial exchanges that are in hash structure and make a Merkle Tree. Each square normally contains a hash pointer as a connect to a past square, a timestamp and exchange information. By structure, blockchains are naturally impervious to alteration of the information. This connecting structures a square of chain. This procedure is iterative and that affirms that past square is dependable and right. Right now can return to beginning square

Square time: In blockchain square time alludes to when system can make 1 more square in the chain. It time shift from blockchain to blockchain some blockchain permits new square as often as possible as like clockwork. This time additionally remember the ideal

opportunity for which information gets evident. In digital currency term shorter square time implies quicker exchange. In Ethereum Blockchain Block time is inexact 14~15 seconds, while for Bitcoin is approx 10 minutes.

Decentralization: Blocks are put away in various areas (hubs) so blockchain dispenses with various dangers which comes if information is in single area/stockpiling. In which we don‟t have no essential issue of disappointment. . Information put away on the blockchain is commonly viewed as morally sound, while brought together information is all the more handily controlled, data and information control are conceivable

Blockchain Working: Blockchain can be considered as the "Web of significant worth". On the Internet, anybody can compose information and others can understand it. As far as digital currency Keys fills the job of recording the exchange, which is customarily done by banks. It likewise fills a subsequent job, building up trust and character, on the grounds that nobody can alter a blockchain. The significant capacities did by banks confirming characters to forestall misrepresentation and afterward recording genuine exchanges - can be completed by a blockchain all the more rapidly and precisely. Square requests in a Blockchain can be considered as a book where, Blocks in a chain = pages in a book.

C. Mathematical Model

Relevant mathematics associated with the Project

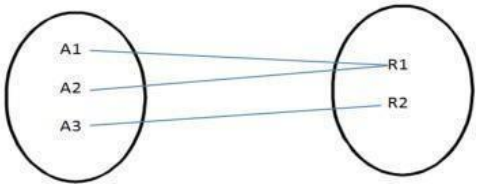

Figure 1: Mathematical Model

Where,
A1: document file provided by the user.
A2: Find out hashes by the user.
A3: Create digital sign by user.
R1: Upload File
R2: Result provided by QR code
Set Theory:
Let us consider S as a system.
S= INPUT: Identify the inputs
F= f1, f2, f3 ....., FN— F as set of functions to execute commands.
I= i1, i2, i3—I sets of inputs to the function set
O= o1, o2, o3.—O Set of outputs from the function sets,
S=I,F,O
I = user
O = Output i.e. QR Code
F = Functions implemented to get the output

Result and Discussions

Block chain is protected using QR code. Hacker can alter information of digital certificate but can't generate QR code. Every blockchain is transferred into unique QR code; this QR code is sent along with certificate. If data received and data from QR code is same then one can considered that data is authenticated otherwise it is altered. Figure 2 and 3 is digital certificate one wants to send and generated QR code respectively.

Fig 2 sent digital certificate

Figure 4 is digital certificate receiver received. Since QR code associated with document and digital certificate shows same information, received digital certificate is unaltered one.

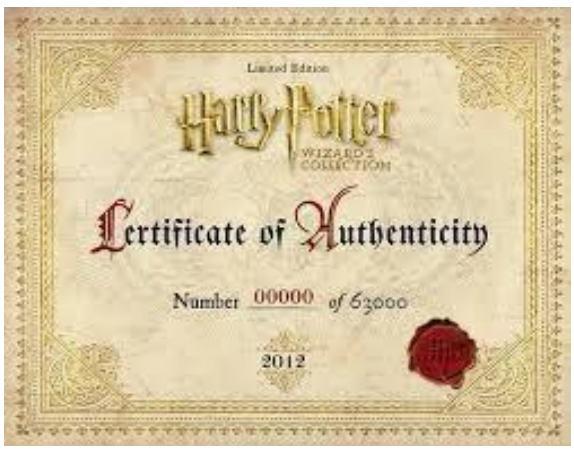

Fig 4 Received digital certificate

Fig 5 Received QR code

Conclusions

Data security is one of the most significant highlights of Blockchain. Blockchain technology is used to reduce the incidence of certificate forgeries and ensure that the security, accuracy and confidentiality of certificates would be improved.

References

[1]. 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]. Neethu Gopal1, Vani V, "Survey on Blockchain Based Digital Certificate System", International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056 Volume: 05 Issue: 11 | Nov 2018 www.irjet.net p-ISSN: 2395- 0072 © 2018, IRJET | Impact Factor value: 7.211 | ISO 9001:2008 Certified Journal | Page 1244

[3]. Nitin Kumavat, Swapnil Mengade , Dishant Desai, JesalVarolia, "Certificate Verification Systemusing Blockchain", International Journal for Research in Applied Science & Engineering Technology (IJRASET) ISSN: 2321- 9653; IC Value: 45.98; SJ Impact Factor: 6.887 Volume 7 Issue IV, Apr 2019

[4]. Erinç KARATAŞ, "Blockchain-Based Document Verification Smart Contract for Moodle Learning Management System",

[5]. International Journal of Informatics Technologies, Volume 11, Issue 4, October 2018 399 Developing Ethereum

[6]. Shanmuga Priya R, Swetha N, "Online Certificate Validation Using Blockchain", Special Issue Published in Int. Jnl. Of Advanced Networking & Applications (IJANA) Page 132

[7]. Aravind Ramachandran Dr.Murat Kantarcioglu "Using Blockchain and smart contracts for secure data provenance management", arXiv:1709.10000v1 [cs.CR] 28 Sep 2017

[8]. T. Keerthana1 , R. Tejaswini2 , V. Yamini3 , K. Hemapriya "Integration of Digital Certificate Blockchain and Overall Behavioural Analysis using QR and Smart Contract", International Journal of Research in Engineering, Science and Management Volume-2, Issue-3, March-2019

[9]. Ocheja, P., Flanagan, B., & Ogata, H, "Connecting decentralizd learning records: a blockchain based learning analytics platform", In Proceedings of the 8th International Conference on Learning Analytics and Knowledge (pp. 265- 269). ACM.