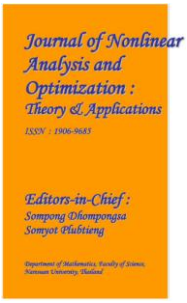
Journal of **N**onlinear **A**nalysis and **O**ptimization
Vol. 13, Issue. 2 : 2022
ISSN : **1906-9685**



REVOLUTIONIZING CREDENTIAL VERIFICATION: BLOCKCHAIN-POWERED CERTIFICATES

Dr. Mahesh Kumar Porwal, Associate Professor, Department Of ECE Sree Chaitanya College of Engineering, Karimnagar
S Ranjith Kumar, Assistant Professor Department Of ECE Sree Chaitanya College of Engineering, Karimnagar

Abstract. Blockchain technology has the abilities that are Decentralized, Distributed, Secure and Faster, Transparent, and non- modifiable. These are more beneficial than the existing technologies. For students, educational certificates are the most important documents issued by their universities. However, as the issuing process is not that transparent and verifiable, fake certificates can be easily created. Blockchain technology has recently emerged as a potential mean for authenticating the document verification process and a significant tool to struggle document fraud and misuse. This research aimed to enhance the document verification process using blockchain technology. And also this paper centers around broadening information about blockchain and on recognizing the benefits, hazards and therefore the related difficulties with regard to the effective execution of application supported blockchain technology with principles and rules for educational certificate verification. Finally this review paper proposed the Academic Certificate Authenticity system using blockchain technology to avoid the fake.
Keywords: Blockchain Technology; Digital certificates; Blockchain in Education; Technical Challenges

Introduction

Blockchain innovation may be a rising innovation and offers highlights like decentralized, straightforward, and sealed information stockpiling. It alright could also be utilized to tackle issues, for instance, absence of trust, misrepresentation, high exchange cost, sharing, security and evaluating reliability of an expected entertainer in an exchange [2]. Consequently, blockchain innovation may be a hopeful innovation to forestall the misrepresentation exercises in our present certificate issuing and verification system or advanced declaration framework. During a large portion of the universities, a paper-based final degree testament is given hooked in to the understudies finished courses recorded within the college's information database. Thanks to increasing demand, there's a continuing threat of scholars taking shortcuts during a successful market of forged degrees and credentials. It's not a specific stretch to seek out fake universities and degree mills that operate purely to form money, copycat websites, also as sites and individuals that issue and print fake degrees and academic credentials.

There are many websites which issue fake degrees and certificates. They exploit the lack of a system that checks the authenticity and validity of degrees/certificates. Individuals who employ fraudulent academic credentials dilute the perceived quality of an institution's graduates, may perform poorly in business, and demonstrate a willingness to commit fraud for personal gain . Fake certificates may delay the admission process in foreign universities (According to a recent survey by UK's National Qualification Agency, it found that only one in four university admission staff feel condiment spotting fake qualification documents)[28]. This review paper focused on the certificate verification using blockchain technology to avoid the fake. This paper contains five sections deals about the concept of blockchain, research methodology which is employed to collect the varied article

associated with BT in education, research objectives and eventually the overview o of literature review. And also analyze the some technical challenges and future trends of Blockchain technology. However, the scope of this research is to determine a framework for implementing security requirements in educational certificate verification in the blockchain. The framework is intended to avoid the problem of fake certificates or fraud in educational certificates.

LITERATURE REVIEW

This exploration comprises of insightful research papers from supposed diaries, gatherings and books which are comprising of 35 notable assets top world colleges articles by IEEE papers, Frontiers of Computer Science - Springer, Frontiers of Computer Science - Springer, Scopus, Journal of NCA, Computer Communications, Transactions on Emerging Telecommunications Technologies, Journal of super computing, ACM, Elsevier and Science Direct. The reason for this writing audit is to distinguish the current instruments, approaches, philosophies, and really understudy's information and squares chains that are reliably working in the industry. In writing audit we watched its most recent innovative patterns and analysts and industrialists who are all the while taking a shot at it and improving this innovation dependent on the current weaknesses. Our examination depends on four basic research inquiries so as to discover the proper research bearings in the space of blockchain and its applications. They looked into writing permits depicting standards and the establishment of blockchain innovation, just as its applications in various genuine use cases. It merits referencing that practically all papers show a requirement for additional exploration in the field. A great deal of creators accepts that blockchain has huge potential, yet at the same time there are a ton of snags and difficulties for genuine execution. For instance, there isn't a single, overall acknowledged meaning of blockchain; in this way, creating normal principles and guidelines (both specialized and legitimate) is profoundly important. Normalization would-be the initial move towards planning bound together methodologies in blockchain programming improvement and security practices, without which a sensible work of blockchain is not feasible.

What is blockchain?

Blockchain, or a se**q**uence of knowledge blocks, may be a specific data- recording structure that operates during a decentralized way. Each block contains a knowledge record and a hash of the previous block, and new data can only be inscribed on a replacement block appended to the chain. This suggests all the blocks before it are hashed and can't accept any alterations, edits, or changes without these being detected.

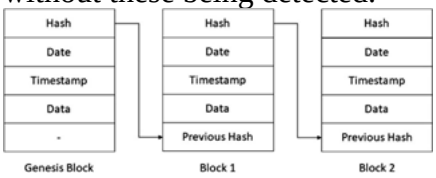


Fig. 1. Blockchain structure

When a transaction is executed, its hash is generated and broadcasted to the network. There are several hashing algorithms in use but the most dominant is the Merkle Tree. This algorithm allows easy hash and easy de-hashes options which are why Merkle Trees is a common choice.

2.2. How does blockchain works

Blockchain technology may be a peer to see and distributed ledger system of combined several computers. A blockchain network is actually an internet of computers or nodes over the web. A block can have transaction data, timestamp, transaction root hash and nonce value. Whenever a replacement block are often created, the miner any node within the blockchain network can verify it by solving a cryptographic mathematical puzzle or problems and gain rewards [3]. Then this node distributes the newly created block to other nodes within the network to validate. This has accomplished by means of consensus algorithm proof of work (PoW). Then the transaction within the newly created block is valid then only that's added to the blockchain network. It is a linked list

like data structure that maintains details of data and its transactions via a peer to peer network publically. Each movement of data is secured with hashing SHA-256 algorithm and then all the transaction summary will be grouped and kept as blocks of data. Then the blocks are joined with hash value of previous block and so on and secured from tamper-proof. This entire functionality of the blockchain will produce secure and non-modifiable record of the transactions that happened across the P2P network.

What are the main Advantages of blockchain?

Fig.1 shows the main Advantages of Blockchain technology are illustrated as follows.

Process Integrity: Due to the safety reasons, this program was made in such how that any block or maybe a transaction that adds to the chain can't be edited which ultimately provides a really high range of security. **Traceability**: The format of Blockchain designs in such how that it can easily locate any problem and proper if there's any. It also creates an irreversible audit trail. **Security**: Blockchain technology is very secure due to the rationale each and each individual who enters into the Blockchain network is given a singular identity which is linked to his account. This ensures that the owner of the account himself is working the transactions. The block encryption within the chain makes it tougher for any hacker to disturb the normal setup of the chain **Faster processing**: Before the invention of the blockchain, the normal banking organization takes tons of your time in processing but after the introduction of Blockchain, the time reduced to just about minutes or maybe seconds

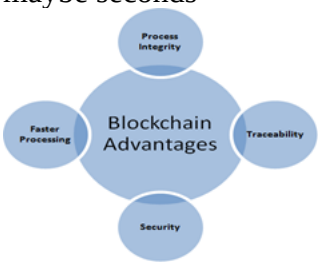


Fig.2. Main Advantages of blockchain

Key Weakness related with blockchain technology

Blockchain technology is an emerging solution, which still suffers from some inherent challenges and issues, as summarized in Fig. 1. **Consumption of power:** The consumption of power within the Blockchain is relatively high as during a particular year the facility consumption of Bitcoin miners was alone quite the per capita power consumption of 159 individual countries. Keeping a real-time ledger is one among the explanations for this consumption because whenever it creates a replacement node, it communicates with each and each other node at an equivalenttime. **Cost:** As per the studies as a mean cost of the Bitcoin transaction is $75-$160 and most of this cost cover by the energy consumption. There are very fewer chances that this issue will resolve by the advancement within the technology. Because the other factor that's the storage problem could be covered by the energy issues can't be resolved. **Lack of Awareness and understanding**: The chief test related with blockchain is an absence of consciousness of the innovation, particularly in areas other than banking, and an across the board absence of comprehension of how it functions. As the blockchain biological system develops and distinctive use cases rise, associations in all industry areas will confront a complex and possibly disputable exhibit of issues, just as new conditions.

Blockchain Application in Academic certificate authencity

The blockchain is a generally new innovation and the utilization of blockchain in academic domain is incredibly new. By the by, there as of now is an enormous number of blockchain-based recommendations to improve a few parts of education system. A portion of these are introduced in the table-I. Blockchain in academic is at the pinnacle

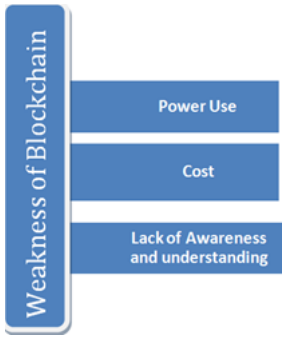


Fig.1. Weakness of Blockchain technology

of Gartner Hype Cycle for Blockchain Business, 2018 and will take 5-10 years to reach plateau [5]. The table-I Illustrate the few education institutes such as schools and universities who are creating and some as of now have created blockchain based authentication frameworks to give endorsements utilizing blockchain technology, such as, University of Nicosia, National University of La Plata, and Holberton School [6].

This literature study depicts those projects in the table-I are not publically available .But have also searched coin based projects which are related to academic certificate verification system, if there are any white papers available in order to find he implementation strategy. But this study find Ethereum coin Ether based applications related to academic degree certificate system to protect from fraud activity. Through Google scholar and online search, these reviews have found four projects related to academic certificate verification system where they have made the project details publicly available. Only 'Blockcerts' project, initiated by Massachusetts Institute of Technology (MIT) and Learning Machine, have made their project open-source and shared their learning experiences[7]. Three other projects, "EduCTX", "Gradbase" records on Bitcoin blockchain to verify the certificates based on coins. Most of the papers dictate the prototype of "Blockchain for Education" and blockchain based certificate system and publishedtheir finding as research paper.

Table 1. Blockchain-Based Applications in Education

Application	Feature	Blockchain Platform / Implementation/ Accessibility	Coin/ gas based/	Year
Edgecoin	Fraud protected ensured great arrangements	Dapps/public	YES	2016
Tutellus	solve the current educational costs for college level students	Dapps and smart contracts TUT token as the gas/public	YES	2016
Blockcerts	produce secure, validate and issue e-certificate	MIT Lab,wallet Bitcoin and Ethereum/public	YES	2016
GradBase	Eeducational record verification system	Bitcoin QR code/public	YES	2016
EduCTX	Ssupporting only Higher education certificates	Ark private/consortium network/private	NO	2017
Teach Me Please (TMP)	database of learning institutions for both online and offline schools	TMP used permission less blockchain, as Ethereum or EOS/public	YES	2017
Success Life	The world-leading seminar and workshop organizer	Ethereum blockchain SXL Token/ public	YES	2018
Sony Global Education(SGE)	secure and share the record of a student	Partnership with IBM/public	YES	2018
Origin-Stamp	Ssecure time-Stamping for ensuring the security	Bitcoin blockchain technology/public	YES	2018
Echolink	Oorganizes a relationship between educational entities	Eko token permission-less blockchain/public	YES	2019

Related works

This study clearly mentioned that the student's degree certificate and other performance abilities are stored in blockchain which definitely provide high security and real time access those data within minimum cost. This literature study is analyzed based on some authenticate factors such as operation security, data security, network security and privacy and find answers for the research questions and that are evaluated in this paper as follows.

RQ1: What are the Challenges today to trait the fake degree certificates problem?

It is clear that the method of verifying the validity of instruction certificates comes with flaws. These may reveal the overall patterns of ways in which universities, education providers, and fellow students may be harmed, yet additionally, businesses that hire deceitful students, their staff, and clients.

- The growing size and complexity of the market
- Highly inefficient, confusing, and expensive check
- Different testimonial interpretations are confusing to everyone

The most important job screening challenges are minimizing hiring time, increasing overall energy in the screening process, verification of information, high prices of complete checks and lack of power to conduct or support international screening. As centralized businesses and approaches focus on leaks and cracks in the current system, decentralized solutions with blockchain technology schools continue to take drugs a lot more often in strategic conversations.

RQ2:What are the solutions and applications suggested with blockchain technology for educational system?

A variety of blockchain applications since from Bitcoin to research on blockchain could have a huge impact on the way researchers build their reputation and become recognized. These applications have been developed for different purposes. Most of the articles focused on supply chain and digital certification verification to keep up with for long time with secure data. In this paper focus on applications have been developed for educational purposes those are analyzed its aim of the application and implementation mechanism and challenges which are required to resolve in future functionality are summarized as shown in Table2. This review process on different articles and papers depicted the applications for educational system can be classified into different categories such as a decentralized publically distributed system for educational student details, students performance report and reward,a tool for chase and verification of authorized degrees: Enterprise form, accreditation and degree verification system, academic certificate authentication system, issuing and verifying digital certificates, universities can incorporate an efficient blockchain education program, secured university results system, learning outcome and meta-diploma and student data privacy and consent, lifelong learning, protecting learning objects, examination review, enhancing students interactions in online learning. The most of applications were studied in this review were centered on students degree certificates verification management.

The system provides the digital certificate platform by making use of a secret session key. It generates the key and uses it to authenticate the user [8]. This system makes use of private key optimized digital identity for digital certificate generation and authentication [9]. The system can be used by an institution for its official website. The purpose of the system was to design an online certificate system based on verification which can be used by the institution [10]. A unique ID is generated using facial particular region, which is used for one to one verification of documents [11].

Table 2. Sum-up the comparison of various applications, implementation mechanism and challenges

Title	Authors	Implementation of the application benefits	Challenges in future process
A Distributed System for Educational Record, Reputation and Reward	Sharples, M., Domingue, J	Micropayments Kudos currency to access records	No separate verification service Vulnerable to proofing attacks
learning outcome and meta-diploma	Bin Duan,Ying Zhong, Dayu Liu	POA Consensus Mechanism (Prove of Accreditation)	Lack of consensus mechanism. Not clear picture of authenticity
How Universities Can Incorporate an Efficient Blockchain education program	Rajarshi Mitra	Blockchain Education Network (BEN) to Kerala Blockchain Academy (KBA)	Universities curriculum only via partnerships Not clear picture about authenticity
Blockchain for Student Data Privacy and Consent	Gilda, S., & Mehrotra, M.	Hyperledger Fabric &and Hyperledger Composer nested authorization	Lack of consensus mechanism The certificate is vulnerable to manipulation
Certificate Verification System using Blockchain	Nitin Kumavat Swapnil Mengade ,Dishant Desai	(IPFS) SHA-2S6 algorithm Ethereum platform	University can be added only by the owner of the smart contract Not clear method of authority of experts
EUniCert: Ethereum based digital certificate verification system	Trong Thua Huynh1, Dang-Khoa	EUniCert based on UniCoin digital currency	Requirements for an employer to verify the certificate A student cannot authorize Not clear method of authenticity
Secured University Results System using Block Chain Features	Prashik Thul, Tushar Raut, Kunal Yadav	Administrator & Student Administrator	Not for the employer and hides the privacy of student Lack of consensus mechanism
Degree Verification over Blockchain	BlockchainTech Private Limited,	Proof of Existence (PoE) consensus	Vulnerable to proofing attacks Need for basic

	Karachi, Pakistan	mechanism	information security measures No clear method of authenticity of parties

The system makes use of QR code for authentication of digital certificates. The server database is used for the record of all generated QR codes. Using the client- server model, the system is developed which generates the certificates in batches and not individually [12]. Most of the papers enclosed for this literature review conferred the applications which are used to verify the validity of issuing, storing, and sharing students' academic certificates. Still, these artifacts focused on blockchain applications to maintain student details, sharing the degree certificates and mark statements (learning outcomes) which are earned by students. The concept of applications focuses on student's evaluation and academic abilities [13]. Some of these articles present the blockchain based applications that are used by companies to verify the student's academic achievements and professional skills [14]. The category is concerned with protecting learning objects from destruction and unauthorized change, and it includes articles. The applications found int he reviewed articles are related to the combined learning the job and higher education. These applications benefit from the high security and less cost and credit transfer [15]. This paper is concerned with bring off academic competitions and deepen the degradation and clearness of these competitions and also related to copyrights management and protective the ownership rights of learning materials [16]. However few of the reviewed papers focus on e-learning process to enhancing students' interactions by rewarding them with virtual currencies. This paper deals about auditing and sharing of exam papers to validate the student's academic achievements.[17].This review shows that the out of thirty five papers stated education based applications that have been already formulated and are now being used. This study clearly mentioned that the student's degree certificate and other performance abilities are stored in blockchain which definitely provide high security and real time access those data within minimum cost.

Proposed Work

The Education organization awards and degree certificates may also have only the names of the group and the student's data. In this state of affairs, there is a lack of superb anti-forgery mechanism, due to these occasions many times the graduation certificates to be cast frequently is found. To remedy the trouble of faux certificates, the architecture that would be proposing leverages the permissioned network points of the Hyperledger Distributed Ledger Technology (DLT) to grant the following advantages [7],[8]. Transparent Network, Permissioned Access, Uniquely Identifiable Digital Certificate, and Grievance Redress, the blockchain science would shop the certificate in digital form. The immutability nature of blockchain makes digital certificate in the disbursed ledger is very difficult to tamper with or regulate additionally it is very easy to verify the originality of digital certificate. This system utilizes quite a number of features of blockchain science is a machine for industry-institute interaction the use of Hyperledger. Universities, institutes, or certification units will furnish certificates, will have to get admission to the system, and will be in a position to browse the system database. When students will fulfil certain requirements, the authorities will furnish a certificate via the system. After the students have received their certificates, they will be able to inquire about any certificates they have gained. The service provider will be responsible for system renovation [5].

Process

To process the digital certificate verification system follows the following steps. The first step the blockchain must endorse the users. In this use case universities, institutes, students, and employers are users who verified by using multiple authentication systems through user id, password, biometric (face scanning, retina,fingerprint), and OTP generation. In step two, the valid user can upload the

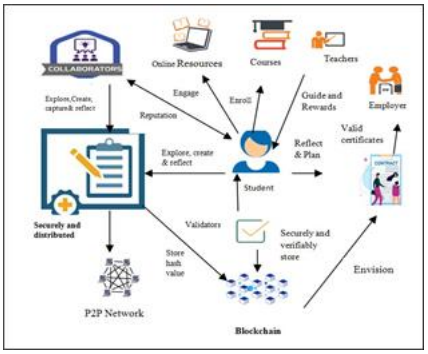


Fig.4. Model of Blockchain Based Certificate Verification System

certificate details into the blockchain network with required certificate details and each created certificate will be stored in CouchDB which in turn will return the unique hash generated using the SHA-2S6 algorithm. CouchDB used to store scanned certificate since only the essential details student id, serial no, date and time of issuing the certificate, issuing authority id, qualification along with the hash value. Once the block is created and then verified by a suitable consensus algorithm and the valid block is added to the blockchain network. Then the system will generate a QR code, OTP, and inquiry string to affix with a hard copy certificate to authenticate the hardcopy of the certificate through phone and website. With the immutability nature of the distributed ledger, the system provides not only verification of certificate and also stores the certificate in digital form forever [8]. And it is almost impossible to modify this certificate or to create a fake certificate with the same data. Hence with this, we can solve the problem of counterfeit certificates.

Technical Challenges

In today's world, at most of the industries and application developers are focusing to increase their productivity through the blockchain technology because of its nature such as transparency, immutability, accountability. In order to bring out this emerging technology as stand out required experts in technical support and also there is an uncertainty as how Blockchain technology does is desirable for business regulative strategy. There are some technical issues while try to implement the blockchain technology that are security and reliability due to its open source the change in code, bugs, new exposure may cause huge loss of users. Another issue is storage-space , Bitcoin supports seven and Ethereum blockchain can supports twenty transaction per second so if block size increase, the existing blockchain is not feasible to have huge storage. Since its transparency the usershas to maintain their hash key in order to direct access the data, it is difficult to remember. And also this technology is required to full fill the communication gap between blockchain application developers and users.

Conclusion

This review analyzed the reasonable applications based on blockchain technology activities and furthermore introduced a correlation among the highlights exist in various educational applications. For analysts, blockchain can possibly be tryingto concentrate all the more intently on subjects like identity management, document management, certificate verification ,health care, insurance, e-voting,supply chain management, property management etc. While physical anti- counterfeiting features prevent tampering chances, digital solutions help in intelligence and identifying culprits in the systems as well as facilitating fast and convenient authentication. Many Universities are now using digital track and trace solutions such as QR Code. Prospective employer/university professionals can check the authenticity of the degree through scanning these QR codes. However the application of blockchain technology in education domain are more beneficial but still this research topic is in exploratory phase and the proceeding of blockchain standards and regulations is necessary to expand its use in this education domain.

References

1. Sharples, M., The blockchain and kudos: A distributed system for educational record, reputation and reward. 2016 https://doi.org/10.1007/978-3-319-45153-4_48
2. Bruce Dorris, J.D, (2018) "Report to the Nations,Global study on occupational fraud and abuse", Association of Certified Fraud Examiners. DOI: 10.5121/ijnsa.2019.11502
3. Trong Thua Huynh1, Dang-Khoa Pham2. eunicert: ethereum based digital certificate verification system October 14, 2019 by IJCNC JOURNAL
4. Inamorato dos Santos, A. (2017) Blockchain in Education –European Commission's JRC report preview, Blockchain in Education Conference,DOI:10.2760/60649
5. Mesropyan, E. (2017). 21 Companies Leveraging Blockchain for Identity Management and Authentication. Vol.8 (2018) No. 4-2 ISSN: 2088-5334
6. Perry, R.E. (2017). Blockchain technology: From Hype to Reality. DOI: 10.1016/j.jii.2020.100125
7. H. Watanabe, S. Fujimura, A. Nakadaira, Y. Miyazaki, A. Akutsu, and J. Kishigami, ''Blockchain contract: Securing a blockchain applied to smart contracts,'' in Proc. IEEE Int. Conf. Consum. Electron. (ICCE), Jan. 2016, pp. 467–468.
8. Z. Zheng, S. Xie, X. Chen, and H. Wang, ''Blockchain challenges and opportunities: A survey,'' in Proc. IJWGS, vol. 14, 2018, pp. 352–375.
9. S. Wang, Y. Yuan, X. Wang, J. Li, R. Qin, and F.-Y. Wang, ''An overview of smart contract: Architecture, applications, and future trends,'' in Proc. IEEE Intell. Vehicles Symp. (IV), Jun. 2018, pp. 108–113.
10. Androulaki, E., Barger, A., Bortnikov, V., Cachin, C., Christidis, K., De Caro, A., et al. (2018). DOIhttp://doi-org-443.webvpn.fjmu.edu.cn/10.1007/978-3-319-67729-3_17
11. Konstantinidis, G Siaminos, C Timplalexis.Blockchain for business applications: A systematic literature review, 2018 - http://doi-org- 443.webvpn.fjmu.edu.cn/10.1007/978-3-319-93931-5_28
12. Blockcerts (2018). Blockcerts.The Open Standard for Blockchain Credentials. Available
13. Fenwick, M., Legal education in the blockchain revolution. 2017.
14. Durant Elizabeth, Trachy Alison (2017). Digital Diploma debuts at MIT.
15. Yang, X., The application model and challenges of blockchain technology ineducation. 2018.