IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

A REVIEW ON DIGITAL DEGREE CERTIFICATE USING BLOCKCHAIN TECHNOLOGY

Roshani S. Bele[1], Jayant P. Mehare[2]

[1]M.Tech. Student, Department of Computer Science And Engineering, G H Raisoni University, Amravati, India

[2]Assistant Professor, Department of Computer Science And Engineering, G H Raisoni University, Amravati, India

Abstract: Blockchain technology provides an ability to create new academic models and solves counterfeit issues efficiently. Therefore, this technology has a potential to lead many research opportunities and Academic Innovations. Here, we presented a system design to be used in the decentralized application for a certificate verification system based on the blockchain technology. As per the statistics provided by Ministry of Education (MOE), India had approximately 37 million students enrolled for graduation each year. After completing the degree, some of them prefer to go to foreign countries for higher education while some will be ready to enter the workplace employment. During this process, counterfeiting of the documents is become a major concern. In order to solve this problem, we would like to propose a digital certificate system that is based on the blockchain technology. By the virtue of blockchain's unmodifiable property, a digital certificate with verifiable ability and anti-counterfeit could be made. In this system, the basic procedure to issue the digital certificate can be divided in two main parts. Firstly, generation of a paper certificate along with other related data that need to be affixed with unique code. This can provide a unique identity to the certificate. Later, it can be uploaded in block of public blockchain.

Keywords— Blockchain, Cryptography, Digital Certificate, Hash code, Tansaction.

I. INTRODUCTION

University student's daily lives are continuously evolving into the digitized form every day. This is also true in case of the digital degree certificates which is generated by the universities, college authorities and different employment application that contain all degree related information. During their life, students encounter with large number of employment agencies or jobs. Each of them stores these personal data into their respective information technology (IT) systems, leading to a fragmented system and databases which are not interconnected.

Certificates are important when applying for job whether at public or private sector. It is usually produced in hard copies and difficult to keep it safe. Certificates that has been issued need to verify manually which is very time consuming and costly. Therefore, the efficiency of the system can be increased by the digital certificate verification based on block chain technology.

In this paper we propose an innovative model of certificate verification system based on privacy preserving. In this model, users will have control on their data and be recognize as owners of their own data. They can apply various security policies, such as sharing data with verification of certificates and documents like results, academic performance certificates etc can submitted on various authorities which verify every documents indetails. Verification time is considerably high so this time consuming task that is to minimize.

During this process of manual certificate verification, a lot of time will be wasted either to reach out to the university for certification verification or awaiting a reply from university that confirms the certificate's accuracy and validity. Overall, this process can be extremely laborious and expensive especially, if a company has several hundreds of certificates to be checked. Based on this background, in the current research, we attempts to propose a theoretical model that can offer a potential solution for academic certificate verification using Blockchain technology.

II. LITERATURE REVIEW

Blockchain

Satoshi Nakamoto proposed the concept of using Blockchain technology in 2008. The blockchain is basically an online ledger that has an advantage to provide a decentralized and transparent data sharing. All the data is stored in nodes and can be compressed and separated into different blocks for transaction with distributed recordings. This features enables the verifications without using intermediaries. All the nodes then form a blockchain with timestamps. Once the data is entered, it becomes inalterable and the data stored in each block can be verified at the same time. The whole process is open to the public, transparent, and secure which is a major advantage of using this technology. Since 2013, the blockchain technology was mainly boosted by the emergence of the Ethereum Smart Contracts which is known as blockchain 2.0. Earlier, blockchain 1.0 was mainly adopted by Bitcoin which was used to deal with the problems concerning cryptocurrencies and decentralized payments. In contrary, blockchain 2.0 mainly focuses on decentralizing the entire market and is employed to transform assets through smart contracts. This approach will create a value through the emergence of alternatives to Bitcoin. Blockchain is basically categorized into two types as follows:

1. Public Blockchain

A public blockchain is open access that means it does not require any permission. It is free for everyone to join the network in the blockchain and then can read, write or participate within the blockchain. It is a decentralized blockchain that does not have any single entity to control the network. Once the data on the blockchain is validated, it is not possible to modify or alter the data and therefore, the public blockchain are considered as secured. Bitcoin and Ethereum are well-known examples of a public blockchain.

2. Private Blockchain

In contrast to the public blockchain, the private blockchain requires a permission. This means that a private blockchain work will be based on the access controls which can restrict the number and type of people who would like to participate in the given network. Unlike the public blockchain, one or more entities can control the network and therefore it has to depend on the third parties to transact. . In a private blockchain, only the entities participating in a transaction will have knowledge about it, whereas the others will not be able to access it. Hyperledger Fabric of Linux Foundation is one of the perfect examples of a private blockchain.

Ethereum: Ethereum is an open and decentralized platform that features Turing completeness. It also supports different derivative applications. Ethereum has been used to create most of the decentralized autonomous organizations as well as smart contracts. Ethereum can be considered as global computing system, if compared to the Bitcoin blockchains that are considered a global payment network. Also, it is similar to that of other open-source platforms such as Google's android. It provides an infrastructure that enables developers to create applications. The infrastructure is developed and maintained by both Ethereum and those developers.

Smart Contract: Smart contract is a function that run over a blockchain. It contains set of rules which the parties has to agree for interacting with each other on certain conditions through smart contract. Smart contracts are written in the Remix IDE programming language, similar to the JAVA script and therefore this program can also be consider as reliable which allows the contract to be deployed onto the blockchain using Metamask and Web3.js injection.

Ze Wang, Jing Qiang Lin, Quan Wei Cai, QiongXiao Wang [2] explains X.509 public key infrastructures a certification authority signs the records to the conjunct hash key of a document in the chain to know its identity. After this step, the certificates are then securely validated by using SSL/TLS in the network. In all the cases, it has been shown that the Certificate Authority is not at all dependable in late security episodes as it were thought to be previously. This infrastructure can also avoid signing of dishonest authentications which may cause due to neglectful personality approvals, misoperations, defective cryptographic calculations, or government impulses.

Mohamed Laarabi, Abdelilah Maach, Abdelhakim Senhaji Hafid [3] uses a case of litigation to explain the possibilities and demerits of the transferring properties of the blockchain using a digital record that may be used as a back support. Authors proposed to store a registry catalog for handling the historical data of the property as well as criminal records of its owners. A digital identity of two parties can then be enforced to execute the smart contract. They also design the necessary components required to be in a registry to integrate with a blockchain infrastructure. Further, they also analyze and discuss the required government endorsement for the successful implementation.

Alexander Grech, Anthony F. Camilleri [4] describe the process to distribute the endorsements. In order to sign the certificate transaction, each web server has a unique distributing key pair which is related to the key pair bound in the authentication. By using such structure of a subject-controlled certificate distribution can allow the web server dealing with its authentications helpfully with Certificate Authorities.

Jiin-Chiou Cheng, Narn-Yih Lee, Chien Chi, and Yi-Hua Chen [5] according to the authors, blockchain technology is used to tackle the problem of counterfeiting certificates. First, electronic file of a paper certificate accompanying other related data into the database will be generate and calculate the electronic file for its hash value. The hash store into the block in the chain system. The system will then 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.

Wei Cai, Zehua Wang, Jason B. Ernst, Zhen Hong, Chen Feng, and Victor C.M Leung [6], traces the development of blockchain systems to reveal the importance of decentralized applications (DApps) and the future value of blockchain. Firstly, decentralized ledger where Bitcoin representative the classic of blockchain system. The most important contribution of Bitcoin is that it solves the double spending issue to make digital asset unique and valuable. In fact, the success of Bitcoin opened the door of blockchain applications to the public. Next, decentralized of smart contract. In order to add more values to the blockchain ecosystem, Ethereum is designed to be a platform to facilitated centralized smart contracts via Ether. Equipped with Solidity, a Turing-complete programming language, Ethereum developers are able to implement a series of smart contracts, which are executable programs written into blocks. Lastly, decentralized application. The ultimate blockchain application should be a DApp that is completely hosted by peer-to-peer blockchain system. In other words, ideal blockchain application or service should be operable without any human intervention, which forms a Decentralized Autonomous Organization (DAO). A DAO is an organization that is run through rules encoded as smart contracts running on the blockchain.

Nitin Kumavat, Swapnil Mengade, Dishant Desai and Jesal Varolia [7], according to these authors, problem of fake academic certificates has been a longstanding issue in the academic community. In order to solve this issue, digital certificates are stored on the Blockchain. In this system, 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. 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.

Osman Ghazali and Omar S. Saleh [8], the educational institution has the primary responsibility to issue a digitally signed academic certificate. This research proposes that this can be done using the blockchain because it contains several functions including hash, public/private key cryptography, digital signatures, peer-to-peer networks and proof of work.

Firstly, for hashing. A hash is a short code of fixed length. Data input from a document into hash-generator results in a hash output containing a certain number of digits. This hash then forms a unique ID. This research recommends the use of SHA-256hash generator to generate hashes because of its reliability and because it is an open-source online tool which can be used to generate the SHA-256hash of any string of data. Next, public and private key. The model proposed in this paper also uses private and public keys. The public key is issued to the university. The university, in turn, issues the student with a private key which is to be kept confidential. Then, digital signatures where both the hash and the public key are used to create a digital signature mechanism which may be used to validate the authenticity of information sent over the Internet.

Second, peer-to-peer network means architecture of computers or networks that share task, work or files between peers. Peers are partners in the network with equal privileges and powers in the environment. In aP2P network, each computer or user is called a node, and collectively they comprise ofaP2P network of nodes.

Decentralized Application (DApp):

Decentralized Application (DApp) is the also a type of blockchain enabled website that runs on peer to peer network of computers. DApp stores the data in decentralized manner and changes made in a single ledger will reflects in every other ledger. DApp function as front-end of the system which is allow user to use and interact with system based on blockchain.

III. DECENTRALIZED CERTIFICATE SYSTEM

Block chain document verification system was developed based on relevant technology. The system's application will be programmed on the public block chain platform. In the system, three groups of users are involved; user-1 is university or certification issues committee, user-2 is student or document owner, and user-3 is the authority of third party or company, have access to the system, and can add data to block chain. After full filling the requirements, authorities will grant a certificate through the system. After the students have received their certificate, they are able to inquire about any certificate they have gained. The certificate provider is responsible for system to upload has of certificate in Blockchain which is decentralized distributed database.

Working:

Block chain document verification system was developed based on using the described technology. The system's application will be programmed on the public block chain platform. In the system, three groups of users are involved, university or certification issues comity, have access to the system, and can add data to block chain. In this system the authorities will grant certificate after full filling certain requirements by students. Students will be free to inquire about any certificate they have obtained even after receiving the respective certificate. The certificate provider is responsible for system to upload has of certificate in a decentralized distributed database blockchain.

Following is the working process of the system that is developed in this study:

1) University grant a degree certificate and enter the student's data into the system. Next, the system automatically generate block form blockchain by adding hash of the certificate or it can be a collection of certificates.

2) The certificate hash is generated by uploading all documents to website then this website generates hash value of all the certificates.

3) Instead of sending or uploading conventional hard copies, university can grant e-certificates containing a hash value which have been authentically generated.

4) When some student is applying for a job, a graduate simply sends the all e-certificate.

5) The companies upload all e certificates to website and generate new hash value this hash should be match to existing hash value which is already uploaded by certificate issuing authority.

6) If Hash value matches then all e certificates are valid else there may be document forgery might be carried out.

Here Data security is one of the major features of blockchain technology so Hash values stored in block chain that cannot be altered. Blockchain can acts like an online ledger in which every node can be used to save and verify the data. The use of proposed blockchain-based system has a potential to reduce the chances of certificate counterfeiting and fabrication. The process described here for the certificate application and automated certificate granting are open and transparent in the system.Companies or the organizations can therefore ask for the information about any certificate from the system.

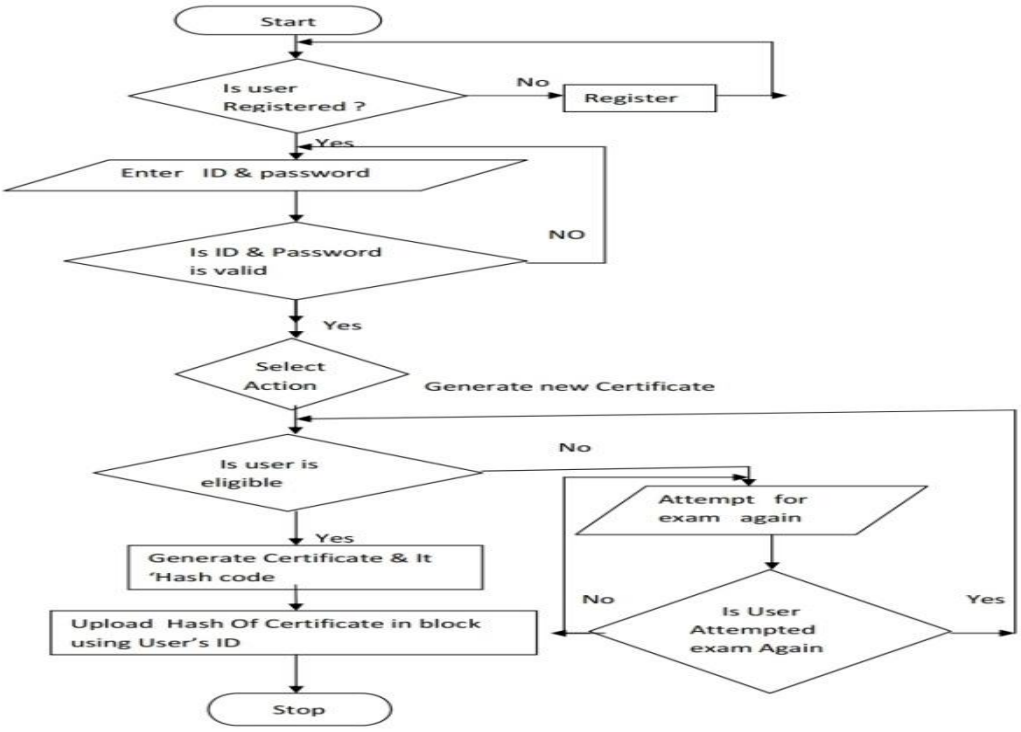

Fig.1.university dataflow diagram

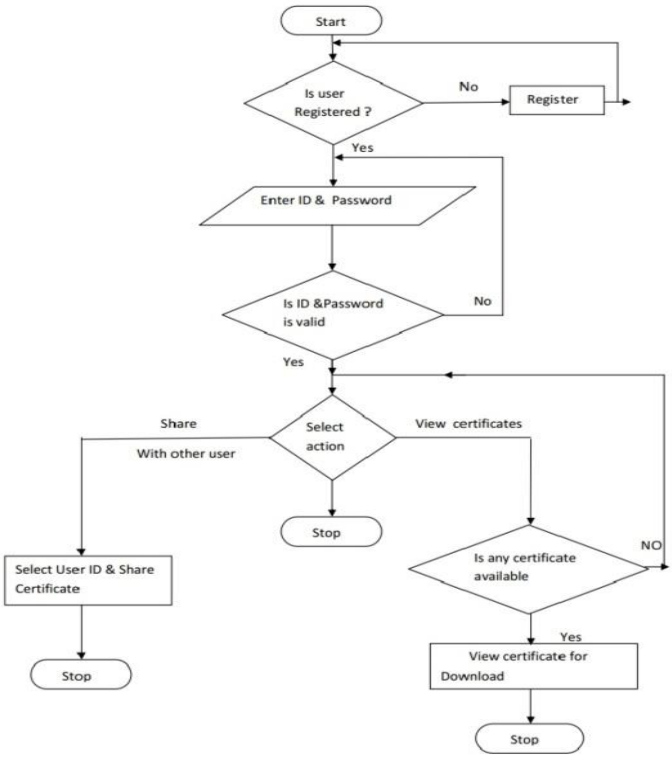

fig.2. student dataflow diagram

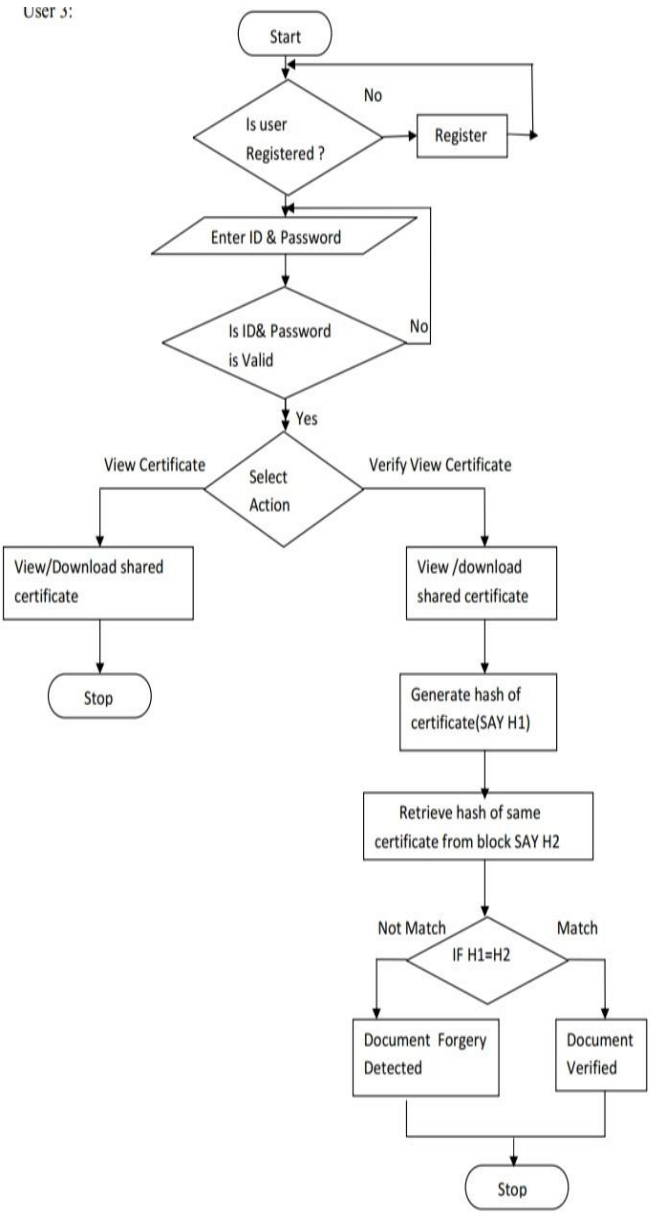

Fig.3.company or document verifying authorities dataflow diagram

IV. CONCLUSION

In the current time, blockchain is one of the leading concept throughout the world. It has a potential to revolutionize the field of education. For instance, blockchain technology can be used to avoid a risk of falsifying the educational certificates and there are many other applications too. Traditionally, easiest way to forge the document is simply by taking someone else's document and changing the owner's name on it. Blockchain technology can be used to tackle this issue. In this research, we have shown how the blockchain technology can be used to for document verification and the security of the document. Our research shows that the blockchain technology is able to provide upto 85% security to the educational documents. Therefore, Securecert developed based on Blockchain technology has added the extra security to the student's assets by securing each certificate into the blocks. The following are the future enhancements of Securecert every student can have the same certificate template instead of a different template for a different university.

REFERENCES

1] Liviu Hirtan, Ciprian Dobre,Piotr Krawiec,Jordi Mongay Batalla "Blockchain-based approach for e-health data access management with privacy protection" IEEE 978-1-7281-1016-5/19/ ©2019 ,/CAMAD.2019

2] Ze Wang, Jingqiang Lin, Quanwei Cai, Qiongxiao Wang, Daren Zha, Jiwu Jing, "Blockchain-based Certificate Transparency and Revocation Transparency", PP(99):1-1 · March 2020,IEEE.

3] Mohamed Laarabi, Abdelilah Maach, Abdelhakim Senhaji Hafid," Smart Contracts and Over-Enforcement: Analytical Consideration On Smart Contracts as Legal Contracts ",IEEE/978-1-7281-4979-0/20/IRASET.2020

4] Alexander Grech, Anthony F. Camilleri, Andreia Inamorato dos Santos," Blockchain in Education", JRC Science Hub, ISBN 978-92- 7973497-7, DOI: 10.2760/60649,2017

5] Jiin-Chiou Cheng, Narn-Yih Lee, Chien Chi and Yi-Hua Chen. (2018) Blockchain and Smart Contract for Digital Certificate. Available: DOI : 10.1109/ICASI.2018.8394455

6] Wei Cai, Zehua Wang, Jason B. Ernst, Zhen Hong, Chen Feng and Victor C.M Leung. (2018) Decentralized Applications: The Blockchain Empowered Software System. Available: https://arxiv.org/pdf/1810.05365.pdf

7] Nitin Kumavat, Swapnil Mengade, Dishant Desai and Jesal Varolia. (April 2019) Certificate Verification System Using Blockchain. International Journal for Research in Applied Science & Engineering Technology (IJRASET), (Volume 7 Issue IV). Available: http://ijraset.com/fileserve.php?FID=20914

8] OsmanGhazalianOmarS.Saleh.AGraduationCertificateVerificationModelviaUtilizationoftheBlockchainTechnology.Available :http://journal.utem.edu.my/index.php/jtec/article/download/4707/3640

9] Guang Chen, Bing Xu, Manli Lu and Nian-Shing Chen. (3 January 2018) Exploring Blockchain Technology and its Potential Applications for Education.Available: https://slejournal.springeropen.com/articles/10.1186/s40561017-0050-x

10] Ali Alammary Samah Alhazmi, Marwah Almasri and Saira Gillani. (13 June 2019) Blockchain-Based Applications in Education: A Systematic Review. Available: https://doi.org/10.3390/app9122400

11] Rakibul Hasan Sayed. (2019)Potential of Blockchain Technology to Solve Fake Diploma Problem.Available:https://jyx.jyu.fi/bitstream/handle/123456789/64817/1/URN%3ANBN%3Afi%3Ajyu-201906253406.pdf

12] RujiaLiandYifanWu.BlockchainbasedAcademicCertificateAuthenticationSystemOverview.Available:https://intranet.birmingham.ac.uk/it/innovation/documents/public/Experiments/Blockchain-based-Academic-Certificate-Authentication-System verview.pdf

13] Gowri Shankar, Dravid, Kamesh, and Dr.Jaison. (March2019) Blockchain based Certificate Issuing and Validation. International Research Journal of Engineering andTechnology(IRJET)(Volume6Issue3).Available: https://irjet.net/archives/V6/i3/IRJET-V6I3369.pdf

14] Benyuan He, "AnEmpirical Study of Online Shopping Using Blockchain Technology", Department of Distribution Management, Takming University of Science and Technology, Taiwan, R.O.C., 2017.

15] NeethuGopal, Vani V Prakash,"Survey on Blockchain Based Digital Certificate System", International Research Journal of Engineering and Technology (IRJET), Volume: 05 Issue: 11, e-ISSN: 2395-0056 Nov 2018.

16] Esmat Mirzamany, Mansoor Hani, 'Blockchain: An Enabler of Efficiency, Choice and Agility in Education", JISC, August 2018

17] DavidMcArthur,"WillBlockchainsRevolutionizeEducation",21stMay 2018.

18] L Morhaim,"Blockchain and cryptocurrencies technologies and network structures: applications, implications and beyond", September 6, 2019 version-1 Hal archive .

19] Cristiane Dias Lepiane , Fernando Lauro Pereira , Giovani Pieri , Douglas Martins , Jean Everson Martina , Mauro Luiz Rabelo "Digital Degree Certificates for Higher Education in Brazil", September 23–26, 2019, ACM ISBN 978-1-4503-6887-2/19/09