EMPIRICAL STUDY OF BLOCK CHAIN TECHNOLOGY BASED ON SPECIAL REFERENCE WITH CERTIFICATE VERIFICATION

C.RUKUMATHI[1] ,Dr.E. MANOHAR[2]

[1]II ME CSE (specialization inNetworks) [2] Associate professor

[1, 2,] Department of CSE, Francis Xavier EngineeringCollege,Tirunelveli

ABSTRACT

The graduation certificates issued by universities and other educational institutions are among the most important documents for graduates. A certificate is a proof of a graduate's qualification and can be used to apply for a job or other related matters. The advance of information technology and the availability of low-cost and high-quality office equipment in the market have enabled forgery of important documents such as certificates, identity cards, and passports. However, verification of certificates using traditional methods is costly and very time-consuming. Therefore, the goal of this work is to propose a model that can offer a potential solution for academic certificate issuing and verification using blockchain technology. The blockchain technology contains several functions including hash, public/private key cryptography, digital signatures, peer-to-peer networks and proof of work. The model uses various elements to formulate the block which is divided into two main processes, namely issuing a digitally signed academic certificate and verifying the academic certificate. The proposed model showed that academic certificate authentication could leverage the blockchain technology. It meets all the conditions necessary for a modern academic certificate verification system. In addition, it closes the gaps and challenges in the existing methods to verify academic certificate authenticity

KEYWORD-Blockchain ,Cryptography,Anti-forge

I.INTRODUCTION

Blockchain is one of the most important and much needed advances in information technology. It has its main application in cryptocurrencies which is considered as a part of the industrial revolution. Bitcoin, being the most successful cryptocurrency until now has its safe and steady usage because of the underlying technology – Blockchain. Blockchain has become a hot topic for researchers, entrepreneurs, institutions and mainly to the countries. People are being aware of the potential of this technology which has its arms widespread. Blockchain is a distributed ledger which is used to store the distinct transactions in a secure, permanent

and verifiable manner. Being a distributed ledger, blockchain can be used on P2P network. This is also known as decentralization property. Data is distributed among various nodes in the network and are so decentralized. P2P network adheres to communication among the nodes in the network and they collectively maintain the database. The transactions are stored in a chain of blocks linked to each other, thus name-Blockchain. Each block is created with a unique hash value using a hash function and timestamp. And the next block created knows the hash value of its previous block, which helps to connect the blocks with each other. Blockchain makes use of cryptography to store data in the blocks, that is the data is encrypted using cryptographic function and then it is stored in the blocks. This avoids any kind of mis-usage of data. The data stored in the blockchain is unmodifiable once it is validated by all the involved parties. If there is a need of alteration then the consensus needs to be taken and based on the majority of consensus it is decided whether the data can be altered or not. Although blockchain records are unalterable. Thus technically, blockchain technology has key characteristics of decentralization, unmodifiability, traceability and cryptography. Advantages of using this technology are reliability, trust, security, efficiency and many more.

Graduation certificate is mostly in the form of a paper-based document as an electronic document cannot effectively replace a physical graduation certificate. However, due to low quality and cheap scanning and printing technologies available, the forgery of graduation certificates has increased. This threatens the integrity of the graduation certificate holders and the government bodies that issued the certificate. Therefore, graduation record of an individual's validation and verification are the major challenge. It is necessary to validate that the graduation certificate presented by any person is genuine and the holder is the rightful owner. Moreover, graduation record has to be verified to ensure that its content is correct and also to ensure that the graduation certificate has been issued from an authentic source.

With these motivations we have used blockchain technology for storing each individual graduation record. This emerging technology is an asset database that aggregates transactions in blocks, and these blocks are appended to a chain of existing blocks. This is suitable for decentralized and transactional sharing of data across a large network of untrusted participants. By using this technology one can maintain continuously growing list of records called blocks and link them in a distributed manner (blockchain), potentially in such a way that these are secured against

tampering. Blockchain is maintained as distributed database of records of transactions (Distributed Ledger) that are shared among participants. This technology uses cryptographic algorithms to validate the logged transactions and ensures that no record is duplicated and also permanent records are updated on each node of the network. This technology allows new type of distributed software architecture where components can establish trust by finding concurrence on their shared states.

II LITERATURE REVIEW

In Blockchain based Academic Certificate Authentication System Overview Rujia Li, YifanWutificate**[1]**Evolved from the Merkle Tree, Blockchain Technology is a fully decentralized digital register which keeps a secure history of data exchanges. In A Graduation Certificate Verification Model via Utilization of the Blockchain Technology Osman Ghazal and Omar **[2]** This paper introduces the fundamental principles of the Blockchain leading to a design of a system on its potential for the creating digital certificates which overcomes limitations of Paper Certificates and (non-Blockchain) Digital Certificates. In Blockchain-based Certificate Transparency and Revocation Transparency? ZeWang ,Jingqiang Lin, Quanwei Cai1**[3]** Blockchain is one of the most recent technology that can be adopted for the data security. The unmodifiable property of the block chain helps to overcome the problem of certificate forgery.In Survey on Blockchain Technologies and Related Services,Nomura Research Institute **[4]**The advancement of technology in modern era everything needs to be digitalized to make it more secure and reliable.InS. Thompson, "The preservation of digital signatures on the blockchain**[5]**There is a need to adopt a process that can verify and ensure the authenticity of a document. In order to prevent the circulation of fake degree certificates a method is proposed where the integrity of the contents with in the certificate can be verified with the use of QR Code and Smart Phone Application. In C. F. Bond, F. Amati, and G. Blousson, "Blockchain, academic verification use case**[6]** The authenticity of academic certificates we propose employing a digital signature scheme and timestamps using blockchain technology, because of its greater transparency, less maintenance and lower cost than traditional alternatives. InM. Carvalho and R. Ford, "Moving-target defenses for computer networks," [7] One of the criticisms of traditional security approaches is that they present a static target for attackers. Critics state, with good justification, that by allowing the attacker to reconnoiter a system at leisure to plan an attack, defenders are immediately

disadvantaged. In LeinHarn and Jian Ren, —Generalized Digital Certificate for User Authentication and Key Establishment for Secure Communication [8] Public-key digital certificate has been widely used in public-key infrastructure (PKI) to provide user public key authentication. However, the public-key digital certificate itself cannot be used as a security factor to authenticate user. In C. V. Malone, E. J. Barkie, B. L. Fletcher, N. Wei, A. Keren, A. Wyskida, —Mobile Optimized Digital Identity (MODI): A framework for easier digital certificate use **[9]** Traditional authentication methods such as passwords no longer meet all the security requirements of today's enterprise. Digital certificates provide a much more secure, resilient alternative solution. InIgbajar Abraham, —Designing an Automatic Web Based Certificate Verification System for Institutions.**[10]** The aim of this study is to design an online certificate verification system based on the verification process adopted by the university to verify her results.InRavinder Reddy B, Pavan Kumar, —Access Control and Data Security in Online Document Verification System**[11]** Document or certificate verification is a crucial part wherein a document or certificate issued by an authority will be verified for its authenticity. In a typical system it will be performed through exchange of mails or post, it is a time consuming process and not foolproof due to human intervention. In SajanAmbadiyil, HarithaSree G S, V.P.Mahadevan Pillai ,—Facial Periocular Region based Unique ID Generation and One to One Verification for Security Documents**[12]** The unique ID thus generated is converted to QR code and it is printed in the security documents for one to one verification. The developed method is analyzed for finding out the typical performance parameters. InHamdi A. Ahmed, Jong Wook Jang, —Higher Educational Certificate Authentication System Using QR Code Tag**[13]** The Quick Response (QR) code was designed for storage information and high-speed readability.In Ahmed Dalhatu Yusuf, Moussa MahamatBoukar, ShahriarShamiluulu, —Automated Batch Certificate Generation and Verification System**[14]** systems are functioning based on the predefined template and predefined template format by the system developer.InN.S.Tinu, —A Survey on Blockchain Technology- Taxonomy, Consensus Algorithms and Applications**[15]** Blockchain is a buzzword in the current technology trends. It is usually coupled with the cryptocurrency terms: Bitcoin and Ethereum. Any applications that can be optimized by decentralization and that needs to be highly secured could opt for this technology.

III PROPOSED SYSTEM

In proposed system architecture of the block chain and its methodology are explained

A. BLOCK CHAINARCHITECTURE

It is a shared distributed ledger governed by the set of rules where each node participating in the blockchain network keeps record of all the data in network. In fig.1 architecture is explained.

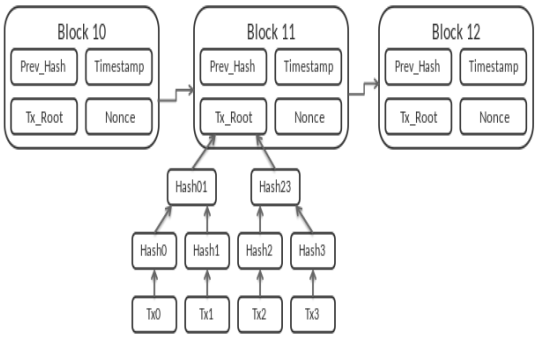


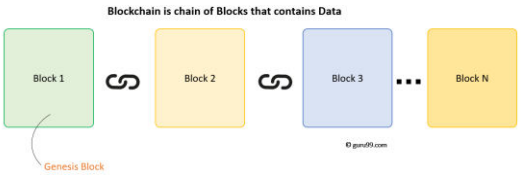
Fig 1. Block Chain Architecture

The data of multiple transactions is stored in the form of blocks along with its timestamp, each transaction can be separately verified by using its hash value, since it is open, publicly verifiable and the data once entered cannot be altered which help in preventing forgery. In fig.1 In blockchain each block of transactions is linked to the previous block by the hash value of preceding block. Hence if anyone tries to change any data in the blockchain the hash value of that block will be changed.

B .METHODOLOGY

Thesystems of methods used in a particular area of study are given through some steps they are;

A Blockchain is a chain of blocks which contain information. The data which is stored inside a block depends on the type of blockchain.



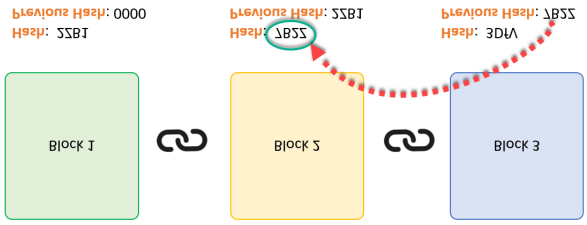
A block also has a hash. A can be understood as a hash key which is unique to each block. It identifies a block and all of its contents, and it's always unique, just like a fingerprint. So once a block is created, any change inside the block will cause the hash to change.

Therefore, the hash is very useful when you want to detect changes to intersections. If the hash key of a block changes, it does not remain the same block.

Each Block has

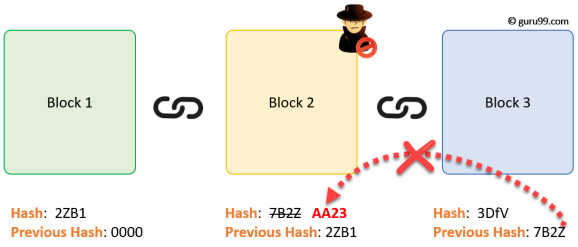
1. Data
2. Hash
3. Hash of the previous block

Consider following example, where we have a chain of 3 blocks. The 1st block has no predecessor. Hence, it does not contain has the previous block. Block 2 contains a hash of block 1. While block 3 contains Hash of block 2.



Hence, all blocks are containing hashes of previous blocks. This is the technique that makes a blockchain so secure.

Assume an attacker is able to change the data present in the Block 2. Correspondingly, the Hash of the Block also changes. But, Block 3 still contains the old Hash of the Block 2. This makes Block 3, and all succeeding blocks invalid as they do not have correct hash the previous block.



Therefore, changing a single block can quickly make all following blocks invalid.

Proof of Work

Hashes are an excellent mechanism to prevent tempering but computers these days are high-speed and can calculate hundreds of thousands of hashes per second. In a matter of few minutes, an attacker can tamper with a block, and then recalculate all the hashes of other blocks to make the blockchain valid again.

In the system, three groups of users are involved, Schools or certification units grant certificates, have access to the system, and can browse the system database. When students fulfilled certain requirements, the authorities 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 service provider is responsible for system maintenance.

Users

- **Certificate Unit**
- **Student/Company Unit**
- **Service Provider**

B. ALGORITHM

SHA-256ALGORITHM

Pad the message M

Break into N 512-bit blocks

Initialize *H*

for i = 1 to N {

Populate *W* with block i and rotate

Initialize intermediate variables a,b,c,d,e,f,g,h

64 rounds

Update *H*

TABLE 1

}

Output *H*

IV. RESULT AND DISCUSSION

The result of the paper and comparison of SHA algorithm is descripted using the table 1 **A.COMPARISONOF SHA ALGORITHSHA-0** output is given as 160 input is given as 160 and blocksize, word and rounds are given as 512,32, and 80 respectively. **SHA-1** output is given as 160 input is given as 160 and blocksize, word and rounds are given as 512,32, and 80 respectively.**SHA-256/224** output is given as 256/224 and input is given as 256 block size,word size and rounds are given as 512,32 and 64 respectively. **SHA-512/384** output is given as 512/384 input is given as 512 and blocksize, word and rounds are given as 1024,64 and 80 respectively.

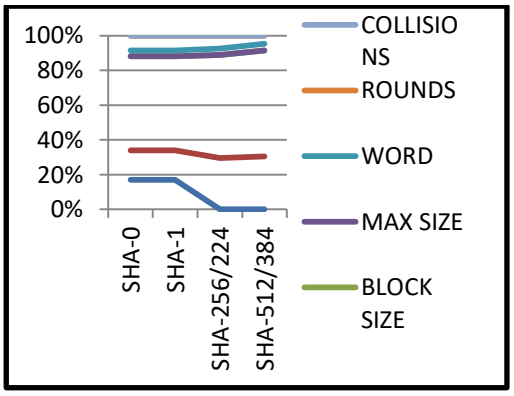


Figure:2

Version	Output (bits)	Input (bits)	Block Size (bits)	Max Size/ Message	Word size	Rounds	Collisions?
SHA-0	160	160	512	2^{64}-1	32	80	Yes
SHA-1	160	160	512	2^{64}-1	32	80	Yes (2^{51})
SHA-256/224	256/224	256	512	2^{64}-1	32	64	None
SHA-512/384	512/384	512	1024	2^{128}-1	64	80	None

COMAPRISON OF SHA ALGORITHMSSHA-0 output is given as 160 input is given as 160 and blocksize, word and rounds are given as 512,32, and 80 respectively. SHA-1 output is given as 160 input is given as 160 and blocksize, word and rounds are given as 512,32, and 80 respectively.SHA-256/224 output is given as 256/224 and input is given as 256 block size,word size and rounds are given as 512,32 and 64 respectively. SHA-512/384 output is given as

512/384 input is given as 512 and blocksize, word and rounds are given as 1024,64 and 80 respectively.

CONCLUSION

In this work, a blockchain-based model for graduation certificate verification was proposed to enhance the verification mechanism. Thereby will reduce the incidence of certificate forgeries and ensure that the security, validity, and confidentiality of graduation certificates would be improved. The proposed model offers many benefits for both the issuing authorities and recipients and consumers. The advantage of the proposed model is that all the information that is required to validate and authenticate the certificate is hosted on the blockchain itself. In order to validate the certificate,the prospective employer need not contact the university at all. All it needs to do is to ensure that the hash generated by the verification software matches that which is contained in the digital signature and that the key issued by the university matches the one incorporated into the digital signature.

Our proposed system uses blockchain technology which is a distributed ledger means its each node stores and verifies the same data. Due to this feature of blockchain, our system enhances the credibility of the electronic files i.e. Ecertificates and also reduces the chances of certificate forgery. The process of E-certificate application and its automated generation is very reliable and transparent. The overall system assures information accuracy and security.

REFERENCES

1. Blockchain based Academic Certificate Authentication System Overview Rujia Li, Yifan Wu, IT Innovation Interns yxw689@bham.ac.uk, rxl635@bham.ac.uk
2. A Graduation Certificate Verification Model via Utilization of the Blockchain Technology Osman Ghazal and Omar S. Saleh School of Computing, Universiti Utara Malaysia, 06010 UUM Sintok, Kedah, Malaysia osman@uum.edu.my

3. Blockchain-based Certificate Transparency and Revocation Transparency? Ze Wang1,2,3 , Jingqiang Lin1,2,3??, Quanwei Cai1,2 , Qiongxiao Wang1,2,3 , Jiwu Jing1,2,3 , and Daren Zha1,2
4. Nomura Research Institute, "Survey on Blockchain Technologies and Related Services," 2016.
5. S. Thompson, "The preservation of digital signatures on the blockchain - Thompson - See Also," *Univ. Br. Columbia iSchool Student J.*, vol. 3, no. Spring, 2017.
6. C. F. Bond, F. Amati, and G. Blousson, "Blockchain, academic verification use case," 2015.
7. M. Carvalho and R. Ford, "Moving-target defenses for computer networks,"IEEE Security & Privacy, vol. 12, no. 2, pp. 73–76, Mar.-Apr.2014.
8. LeinHarn and Jian Ren, —Generalized Digital Certificate for User Authentication and Key Establishment for Secure Communication‖, IEEE Transactions on Wireless Communications, Vol. 10, Issue 7, July 2011.
9. C. V. Malone, E. J. Barkie, B. L. Fletcher, N. Wei, A. Keren, A. Wyskida, —Mobile Optimized Digital Identity (MODI): A framework for easier digital certificate use‖, IBM Journal of Research and Development, Vol. 57, Issue 6, December 2013.
10. Nwachukwu-Nwoceafor K.C, Igbajar Abraham, —Designing an Automatic Web Based Certificate Verification System for Institutions‖, Journal of Multidisciplinary Engineering Science and Technology (JMEST), Vol. 2, Issue 12, December 2015.
11. Ravinder Reddy B, Pavan Kumar, —Access Control and Data Security in Online Document Verification System‖, In the proceedings of 2016 IEEE International Conference on Computational Intelligence and Computing Research (ICCIC), India, 2016.
12. SajanAmbadiyil, HarithaSree G S, V.P.Mahadevan Pillai ,—Facial Periocular Region based Unique ID Generation and One to One Verification for Security Documents‖, In the proceedings of 2016 2nd International Conference on Advances in Electrical, Electronics, Information, Communication and Bio-Informatics (AEEICB), India, 2016.
13. Hamdi A. Ahmed, Jong Wook Jang, —Higher Educational Certificate Authentication System Using QR Code Tag‖, International Journal of

Applied Engineering Research, Vol. 12, Issue 20, 2017.

14. Ahmed Dalhatu Yusuf, Moussa MahamatBoukar, ShahriarShamiluulu, ―Automated Batch Certificate Generation and Verification System‖, In the proceedings of 2017 13th International Conference on Electronics, Computer and Computation (ICECCO), Nigeria, 2017.
15. N.S.Tinu, ―A Survey on Blockchain Technology- Taxonomy, Consensus Algorithms and Applications‖, International Journal of Computer Sciences and Engineering(IJCSE), Vol. 6, Issue 5, May 2018.