International Journal of Applied Engineering and Technology ISSN: 2277-212X (Online)
Online International Journal Available at http://www.cibtech.org/jet.htm
2020 Vol. 9, pp.156-160/Mangaiarkarasi et al.
***Research Article** (Open Access)*

BLOCKCHAIN BASED CERTIFICATE VALIDATION

***Mangaiarkarasi, T. Prem, M. Madhavan, R. Vijaya Kumar and J. Jaisurya**
**Computer Science and Engineering, SJCET*
**Author for Correspondence*

ABSTRACT

The main objective of the project is to validate the certificates whether the submitted certificate is a valid one or not. This can be checked by any of the company sectors and educational institutions to validate the received certificate. All the certificate authorities has to involve in uploading their certification details in a node, which helps the company sectors and educational sectors to check the certificates. The information shared is highly secured through Block chain. The information will not be shared with any of the companies who check for validation rather it says whether the asked certification details is TRUE or FALSE. The application is used as the platform to check the updated certification details. This isn't the best use case for individual company or institution involved rather it works well on the incorporation of multiple companies and institutions in a single system. The hesitation of sharing the certification details is overcame in this proposing project, since the details are not been shared with the one who checks for the validation and are highly secured through Block chain. The involvement of the certificate providers is the major key to success to this project. The concerned data are going to be with the concerned party securely. Any changes or updation of mistakes made on the already uploaded certificates notifies every other systems involved. The certificates are of Municipal Certificates, Educational certificates, Employment certificates and other certificates.

***Keywords:** Hash Value, Blockchain*

INTRODUCTION

In the real world, people are valuated and judged by the qualification and the achievements. These qualification and achievements are trusted by the certificates provided for each achievement on either education or employment. The birth of the citizen is even approved by a birth certificate. As everything depends on the certificates, the rate of duplicate certificates and fake certificates have also increased. How do we check for the genuinity ?

- ✓ Agents work on it.
- ✓ Tele-Verification to the concerned university

To overcome these difficulties this project is proposed. The project consists in designing and implementing the system which overcomes the above problems. The project also involves a comprehensive evaluation of the system security, and therefore the assessment outcomes provide compelling evidence to prove that implementation is practical, reliable, secured, which could give some hints of important architectural considerations about the safety attributes of other blockchain-based systems. Certificates distributed in colleges or universities are mostly within the sort of text. Whenever applicants apply for the job at any public or private sector they have to produce those hard copies, while the organizations have to verify all certificates manually which is very time-consuming process and there are chances that some may have produce the certificate which is not legit and that may get unnoticed by the verifier during the process because of this ineligible candidate will get an opportunity. There had been lots of cases in past where people are caught selling fake certificates of different organization at low cost. To eradicate such problem and diminish the production of fake certificates we can use the Blockchain technology. Blockchain can be used to store the data of the certificate that can be validated by anyone from any place. The blockchain is a decentralized shared distributed ledger; the data stored in the blockchain is almost un-modifiable. It is a type of database which is not centralized and governed by the set of rules.

WORKING

To create the block chain based unmodified certificates, initially the university must get registered. Each university getting to blare are going to be having its wallet address from which it's 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 may create certificates with data fields. Each created certificate are going to be stored within the Inter planetary filing system IPFS which successively will return the unique hash generated using SHA-256 algorithm. This will function unique identity for every document. Along with this generated hash and detail of certificates, all this data will be stored in the block chain. Anyone can use this transaction id to verify the certificate details and can view the original copy of certificate using IPFS hash stored along with data. And it's almost impossible to switch this certificate or to make fake certificate with same data. Hence with this we can solve the problem of counterfeit certificates.

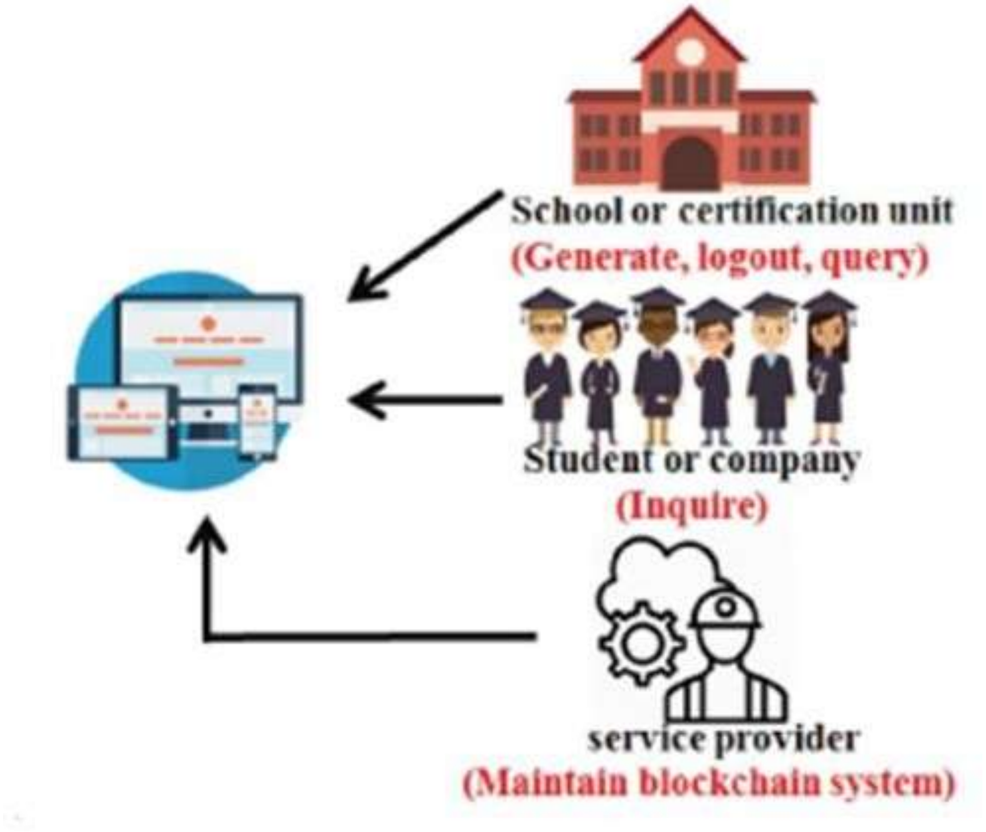

School or certification unit
(Generate, logout, query)
Student or company
(Inquire)
service provider
(Maintain blockchain system)

Figure1: Over all Working Diagram

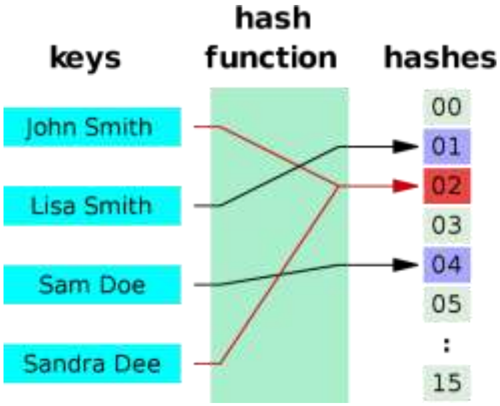
Here, Blockchain is the common medium of technology going to be used in the security of data.

Blockchain

The concept of blockchain was first proposed by an individual (or a gaggle of persons) named Satoshi Nakamoto in 2008. It's a shared distributed ledger governed by the set of rules where each node participating within the blockchain network keeps record of all the info in network. the info of multiple transactions is stored within the sort of blocks alongside its timestamp, each transaction are often separately verified by using its hash value, since it's open, publicly verifiable and thus the info once entered cannot be altered which help in preventing forgery. In blockchain each block of transactions is joined to the previous block by the hash value of preceding block. Hence if anyone tries to vary any data within the blockchain the hash value of that block is getting to be changed.

a. Hash Values

A hash value may be a numeric value of a hard and fast length that uniquely identifies data. Hash values represent large amounts of knowledge the maximum amount smaller numeric values, in order that they are used with digital signatures. You can sign a hash value more profitable than signing the larger value.



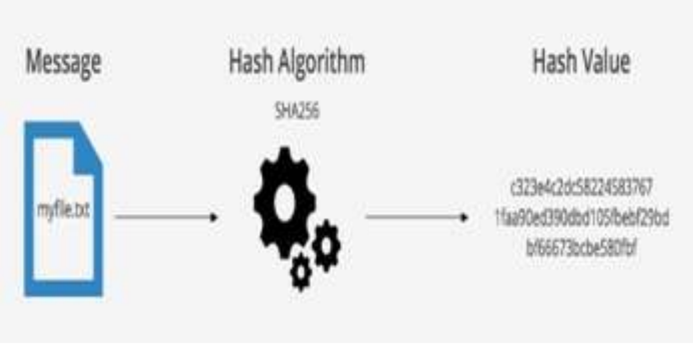


Figure: 2.A

Figure: 2.B

Fig 2 SHA-256 may be a one-way function that converts a text of any length into a string of 256 bits. This is known as a hashing function. In this case, it's a cryptographically secure hashing function, therein knowing the output tells you little or no about the input. It is a modified version of SHA1, which successively may be a modified SHA0. All three are now broken, to some extent. SHA-256 (Secure Hash Algorithm, FIPS 182-2), is one of the cryptographic hash functions which has digest length of 256 bits. It's a keyless hash function, means a Manipulation Detection Code (MDC). In other words, Secure Hash Algorithm (SHA) was developed by the National Institute of Standards & Technology, and further, they came with a replacement version called SHA-256 (the SHA-2 family), where the amount is represented because the hash length in bits.

CONCLUSION

The proposed system works well on the involvement of multiple companies and institutions for the uploading of the certification details.

This system plays a safer role in guarding the data secure with the help of the discussed technology. Overcomes the issues discussed above. The conversion of data into hash values play a major role in security and the interconnection of those hash values through blockchain makes it even stronger in security. The validator can be of any party, either an educational institution or a company sector. Any of the interested sectors could possibly check the received certificates for the genuinity. The certificate uploaders would need the permission and access from the smart contract owner to upload the details. The smart owner checks the requested client for they are a proper certificate issuers. After validating the certificate issuer a unique ID and Password helps them to upload the certification details. The updation of any existing certificates would lead to notify all the other certificate issuers in the node.Thus it is in a highly safer hands.

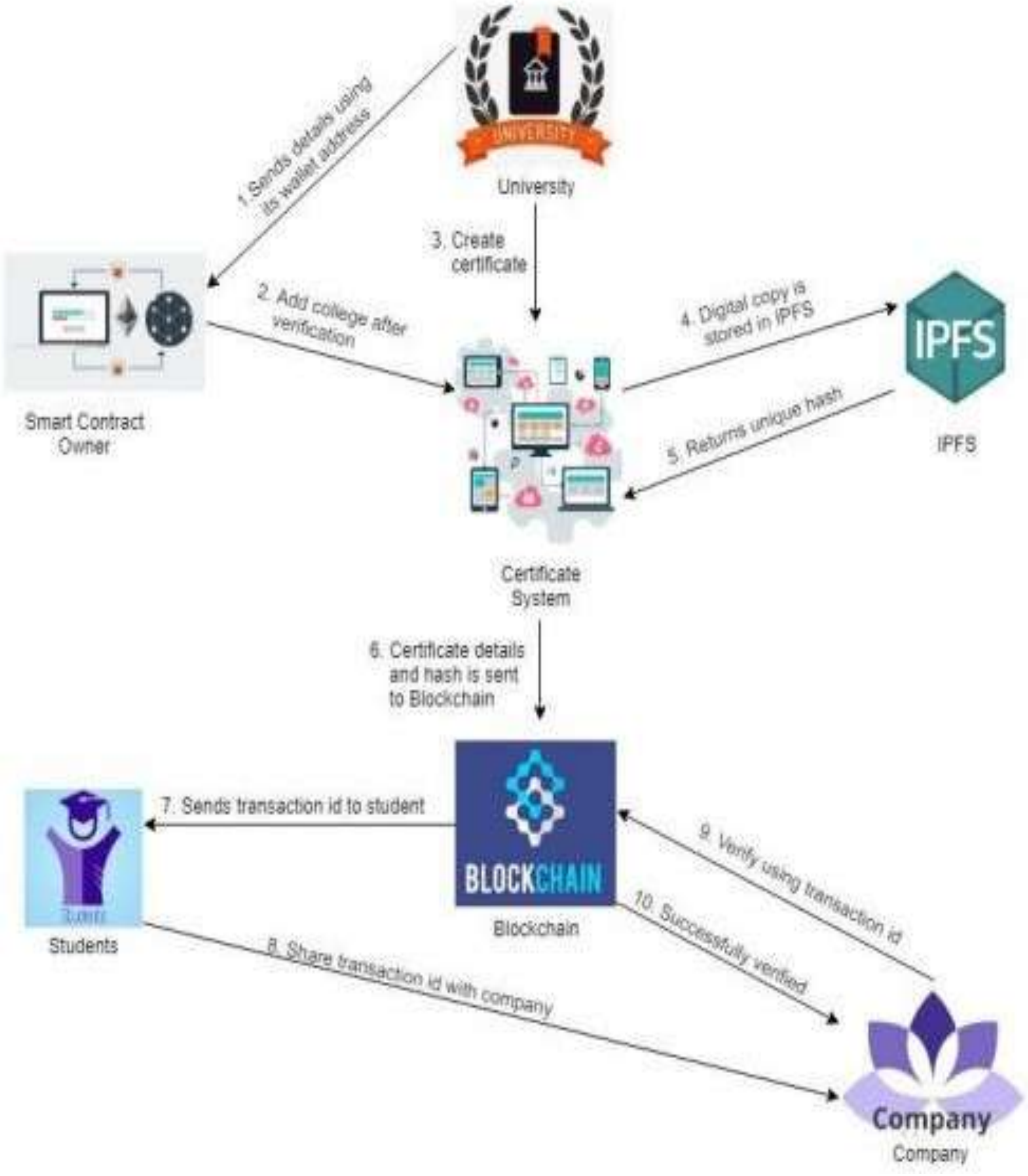

UNIVERSITY
University
1. Sends details using its wallet address
3. Create certificate
Smart Contract Owner
2. Add college after verification
4. Digital copy is stored in IPFS
IPFS
IPFS
5. Returns unique hash
Certificate System
6. Certificate details and hash is sent to Blockchain
BLOCKCHAIN
Blockchain
7. Sends transaction id to student
Students
Students
9. Verify using transaction id
10. Successfully verified
8. Share transaction id with company
Company
Company

Figure: 3.Data flow diagram

Fig 3, diagrammatic sketch represents the data flow in the proposed system. The procedure and algorithm through which the system follows.

REFERENCES

[1] Benyuan He, **(2017)**. *An Empirical Study of Online Shopping Using Blockchain Technology, Department of Distribution Management, Takming University of Science and Technology, Taiwan,* R.O.C.,.

[2] G. Hurlburt, Might the Blockchain, no. [April, pp. 12–16, 2016].

[3] G. O. Karame, E. Androulaki, S. Capkun, **(2012)**. Double-spending fast payments in bit coin, Proceedings of the (2012) ACM conference on Computer and communications security, pages 906-917. ACM.

[4] Hailong Yao, Caifen Wang, **(2018).** *A Novel Blockchain-Based Authentication Key Exchange Protocol and Its Applications, IEEE Third International Conference on Data Science in Cyberspace.*

[5] Jiin-Chiou, Narn-Yih Lee, Chien Chi, YI-Hua Chen, (2017).*Blockchain and Smart Contract for Digital Certificate, Proceedings of IEEE International Conference on Applied System Innovation*

[6] Marco Baldi, Franco Chiaraluce, Emanuele Frontoni, Guiseppe Gottardi, Certificate Validation through Public Ledgers and Blockchains, In Proceedings of the First Italian Conference on Cyber security (ITASEC17), Venice, Italy.

[7] Satoshi Nakamoto, Bit coin: A Peer-to-Peer Electronic Cash System, www.bitcoin.org.

[8] S. Underwood, Blockchain beyond bit coin,"Commun. [ACM, vol. 59, no. 11, pp. 15–17, 2016].

[9] Tareq Ahram, Arman Sargolzaei, Saman Sargolzaei, Jeff Daniels, Ben Amaba, (2017). *Blockchain Technology Innovations, IEEE Technology & Engineering Management Conference* (TEMSCON).

[10] T. Bui, T. Aura, Key Exchange with the Help of a Public Ledger, F. Stajano, J. Anderson, B. Christianson, V. Matyáš (eds) (2017). Security Protocols XXV. Security Protocols (2017). Lecture Notes in Computer Science, vol 10476. Springer

[11] W. Diffie, P. C. Van Oorschot, M. J. Wiener, **(1992)**. Authentication and authenticated key exchanges, Designs, Codes and cryptography **2**(2), 107-125.

[12] Xiuping Lin, **(2017)**. Semi-centralized Blockchain Smart Contracts: Centralized Verification and Smart Computing under Chains in the Ethereum Blockchain, Department of Information Engineering, National Taiwan University, Taiwan, R.O.C.,.

[13] Yong Shi, **(2017)**. Secure storage service of electronic ballot system based on block chain algorithm, Department of Computer Science, Tsing Hua University, Taiwan, R.O.C.,.

[14] Zhenzhi Qiu, (2017). Digital certificate for a painting based on blockchain technology, Department of Information and Finance Management, National Taipei University of Technology, Taiwan, R.O.C.,.