International Journal of Engineering & Technology, 7 (4.6) (2018) 394-397

International Journal of Engineering & Technology

Website: www.sciencepubco.com/index.php/IJET

Research paper

Blockchain and Smart Contract for Digital Document Verification

S.Sunitha kumari[1]*, D.Saveetha [2]

[1]Department of Information Technology- SRM Institute of Science and Technology
[2]Department of Information Technology- SRM Institute of Science and Technology
**Corresponding author E-mail: [1]sunithakumari_su@srmuniv.edu.in*

Abstract

Every year lakhs of students graduating from different university, after passing from university different students have different plans. All students who graduated will have different certificate such as marksheets, degree certificate, best performance certificate and etc. Some students have plans to get employed in companies or to do higher studies. Wherever students go they need submit the certificate for important reference. Due to lack of anti-forge mechanism some started to forge the certificate to get the employed or for further steps. In the digital certificate verification based on blockchain done only for the degree certificates. In the proposing system along with the degree certificate entire personality and behaviour activities of the person using personal id will be uploaded in blockchain. Because of unmodifiable property it is stored in block chain. Initially the student request for the e-certificate by uploading certificate or personal id to electronic certificate system. If requesting for e-cert then the system will review certificate from the university or schools or from organization and get the assurance and store the serial number and e-certificate to the block chain. The system will be generating the QR code and send it to the user. when applying for company user will send only the certificate serial number and QR code received from the e-certificate company.

Keywords: *blockchain, Hyperledger, digital certificate, hashing*

1. Introduction

In Information technology Advances the data innovation, the wide accessibility of the Internet, and normal use of cell phones have changed the way of life of the person. Virtual money, computerized coins initially intended for the use on the web, has started to broadly embraced, all things considered. As a result of the comfort of the Internet, different virtual monetary forms are flourishing, including the most well know Bitcoin, Ether, and Ripple to estimate 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 ethical database that has high potential for a different scope of employments.

An Electronic Certificate is an arrange of information empowering distinguishing proof of the holder of the Certificate, secure trade of data with different people and organizations, and electronic marking of information sent to allow check of its trustworthiness and root. Since data innovation has grown quickly as of late, information insurance is more important than any other time in recent memory. Graduates, regardless of whether they keep examining or begin work chasing, require different authentication for meetings. Notwithstanding, they often find that they have lost their instructive and acclamation endorsements. Reapplying for printed versions will be tedious in light of the fact that authentication is allowed by various associations and in-person application are important. By complexity, applying for an e-duplicate can spare paper and time. By giving facts to character check, graduates can apply for any authentication effortlessly. By the by, in view of this comfort, manufactured degree testaments, licenses, and authentication are main. Thus, schools and organizations can't in a split second approve the archives they get. To tackle this issue, an authentication framework in light of blockchain was plan in this investigation. Information is put away in various hubs, and any person who wishes to alter a specific in datum must demand that different hubs adjust it at the same time. Along these lines, the framework is profoundly solid.

In this we built up a decentralized application and planned an endorsement framework in light of Ethereum blockchain. This innovation is chosen since it is ethical, scrambled, and trackable and grants information synchronization. By incorporating the highlights of blockchain, the framework enhances the skill activities at each stage. The framework saves money on paper, cuts administration costs, forestalls archive fabrication, and gives exact and solid data on computerized testaments.

2. Literature Review

A. Electronic certificate

In a regularly changing business condition that keeps on modernizing continuously, the electronic conveyance of Certificates of Origin (CO) has turned out to be fundamental. Numerous assemblies of business offer online CO administrations to ease the application and issuance process, and additionally security. The Electronic Certificate ensures:

The valid people and substances that are engage with the data trade. Privacy: just the backer and the beneficiary see the data. The respectability of the data traded, guaranteeing that no control is delivered. Agreeableness, which ensures the holder of the authentication that nobody else may produce a mark connected to her/his declaration, and keeps her/him from denying proprietorship in the messages she/he has marked

B. Blockchain

Blockchain is like the mechanism of the singly linked list. Each block of blockchain have number of transactions. It is shared and immutable data stored which can be used across the network. It is transparency and trust to all parties.

-In need of validating and consolidating the individual or organization will have the copy of the data

-Inter-organization data sharing
-Digital registry
-Cryptographic identification
-From blockchain interested parties can pull the data.

Trust

Blockchain is the decentralized database and also collectively owned by multiple people. Data stored in the blockchain cannot be deleted and also cannot modified. Even if someone try to delete or modify the data the hash value of block will get changed.

Autonomy

In the blockchain there is no single owner for Blockchain based applications. Blockchain can't be controlled by anyone but everyone participates into its activities. Manipulated or induce corruption can't be done in the blockchain.

Integrity

The state and transactions are cannot be modified easily and secured cryptographically

Intermediaries

Blockchain based application will removes the intermediaries from present processes. Generally, central body like license issuing, Vehicle registration etc. who acts as issuing driver license as well as registrar for registering vehicles. There is no central body without Blockchain based systems.

Symmetric Key

Symmetric cryptography is technique of using single key to encrypt and decrypt the messages. The same will be used for encryption and decryption

Asymmetric Key

Asymmetric cryptography is technique of using two keys for encryption and decryption. Public key or private key can be used for encryption and decryption. Messages encrypted with public key can be decrypted with private key and messages encrypted using private key can be decrypted with public key.

Hashing

Hashing is the technique that used to transform the fixed or variable length of string input to the fixed length of output. In this it is not possible to find the original input or data or regeneration of the input data from output string is not possible. In hashing small or simple changes that completely changes the output. Size is not a matter in hashing. And it is mathematically not feasible for the two different type of input string

C. Ethereum

Ethereum is a platform for the unstoppable application. The component of Ethereum are Ethereum virtual machine, Blocks, Transactions, Miner, Smart contracts, mining nodes, Consensus algorithm, Accounts, Ether and Gas.

The network of blockchain consist multiple nodes which belongs to miner. From some nodes mining can't be done but helps in transaction and execution of smart contract

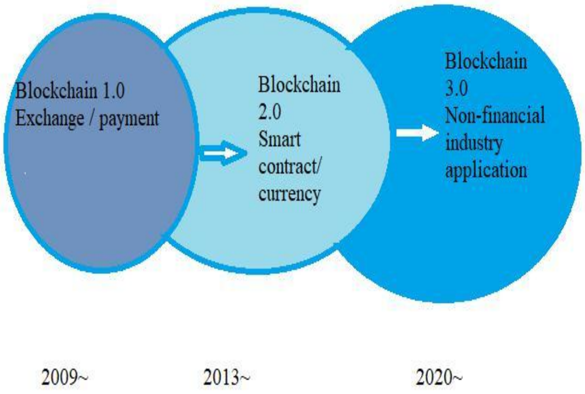

Fig.1: Blockchain development

1.Ethereum virtual machine

The Ethereum Virtual Machine centre around giving security and executing not trusted code by PCs everywhere throughout the world. To be more particular, this undertaking centre around counteracting Denial-of-benefit assaults, which have turned out to be fairly basic in the digital money world. Besides, the EVM guarantees programs don't approach each other's state, guaranteeing correspondence can set up with no potential obstruction.

2. Solidity

solidity is known as an agreement based, abnormal state programming language. This stage has comparable punctuation to the scripting language of JavaScript. Solidity as a programming dialect is made to upgrade the Ethereum Machine.

Virtual Strength is statistically composed the way scripting language which does towards checking and implementing the requirements at total time and not runtime.

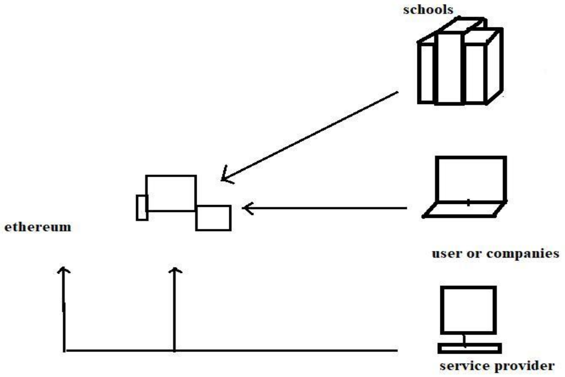

Fig 2: Blockchain configuration

3. System Process

Initially user register for digital e-certificate system and upload the certificate in the digital e-certificate system. the system will review the certificate and personal id from the university and the id card verification site. If the certificate and id card is original then it saves the serial number of the certificate and id card number in the blockchain. If successfully finished saving the e-certificate system generate QR code and send to the user along with the e-certificate and serial number. While applying for the job user will only send the QR code and serial number. The company will verify using the certificate and id card using digital certificate system and serial number in the blockchain.

In Blockchain hashing used for data securing. Digital verification system uses the blockchain for the verification of the data. Here asymmetric is used for the key generation. Because the asymmetric key has public key and private key. If data is modified using the private key using the public key original message can be received. Otherwise if modified using the public key then private key is used for the receive the original message.

In the QR code all verified certificate and personal identity cards are encrypted into the single link. Here all the data are stored into the single node. The encryption will be using the private key. The company for verification of the certificates use the users public key connect to the user's network and the verify the data. When the company or organization able to connect the user's network with the public key.

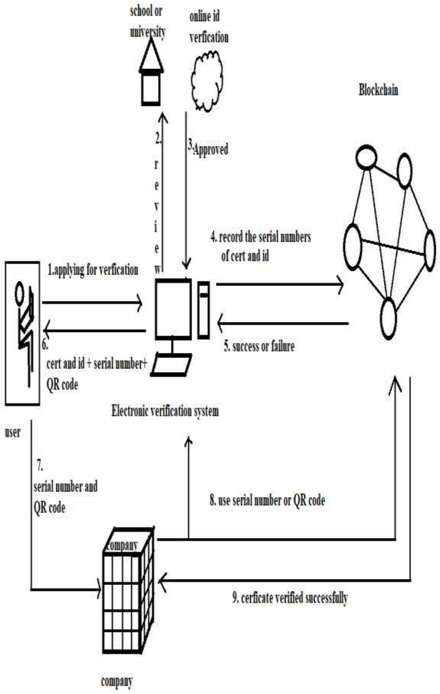
school or university
online id verfication
Blockchain
2. review
3.Approved
4. record the serial numbers of cert and id
1.applying for verfication
6. cert and id + serial number+ QR code
5. success or failure
Electronic verification system
user
7. serial number and QR code
8. use serial number or QR code
company
9. cerficate verified successfully
company

Fig 3: System architecture.

The process flow of the system

1. Schools grant a degree certificate and assure the certificate. the system automatically records the serial number of the student in a blockchain.
2. Next step is verification
3. Instead of sending convention hard copy QR code and the serial number will be sent.
4. For applying job only QR code and serial number will be given.
5. Verification will be done from the data stored in the blockchain

4. Module Description

The digital certification has four modules

1. User module
2. Electronic verification system
3. E-verification
4. Block chain
5. company

1. User

In the user module initially register to application. After registering the application user upload all certificate and the Id for the verification

2. Electronic verification system

This system will verify the uploaded file of users by sending it to school or university if it is education related certificate or if it's the personal id card verify using the online websites for verification. After the e-verification, e-certificate QR code and serial number will be delivered to system

3. E-verification

Documents will send to the school or university for the verification and personal id card verified in online using the number

4. Blockchain

Electronic verification system will store the serial number of the certificate and personal id to blockchain

5. Company

While applying for the job user will send only the QR code and the serial number. Company verify using the serial number and QR code.

5. Conclusion

One of the most important features of the blockchain security for the data. Here certificate verified using the data stored on to the blockchain. Since it stored to blockchain document forger can be reduced. In conclusion security and accuracy assured in the system.

References

[1] Xiuping Lin, "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., 2017.

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

[3] Zhenzhi Qiu, "Digital certificate for a painting based on blockchain technology", Department of Information and

[4] Finance Management, National Taipei University of Technology, Taiwan, R.O.C., 2017.

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

[6] Yin-Jen Chiang, Pei-Yu Lin, Ran-Zan Wang, Yi-Hui

[7] Chen,” Blind QR Code Steganographic Approach Based upon Error Correction Capability”, KSII Transactions on Internet and Information Systems.

[8] Peter Kieseberg, Manuel Leithner, Martin Mulazzani, Lindsay Munroe, Sebastian Schrittwieser, Mayank Sinha, Edgar Weippl “QR Code Security “,2014.

[9] S. Uma Maheswari, D. Jude Hemanth “Frequency domain QRcode based image steganography using Fresnelet transform”.

[10] The KECCAK sponge function family, http://keccak.noekeon.org

[11] Bertoni, G., Daemen, J., Peeters, M., Van Assche, G.: Keccak sponge function family main document. NIST (2009)

[12] Certicom Research, Standards for efficient cryptography, SEC 1: Elliptic Curve Cryptography, Version 2.0, May 21, 2009

[13] Ms. P. G. Rajeshwari and Dr. K. Thilagavathi, "An Efficient Authentication Protocol Based on Elliptic Curve Cryptography for Mobile Network," IJCSNS, Vol 9, feb 2009.

[14] Johnson D, Menezes A, Vanstone S, The Elliptic Curve Digital Signature Algorithm (ECDSA). Certicom Corporation.

[15] W. Zhanyi, Y. hanato, Z. huanguo, "Analysis of elliptic curve cryptosystem", comput Eng., vol. 28, pp. 161-163, 2002

A. khalique, k. Singh, S. Sood, "Implementation of elliptic curve digital signature algorithm", International journal of computer applications, vol. 2, May 2010.

[16] N. Koblitz , "Elliptic curve cryptosystems", Mathematics of Computation, vol. 48, pp. 203-209

[17] Bin Chen, Wenliang Wu, Yao Zhang, "The Design and Implementation of Digital Signature System Based on Elliptic Curve", 2012 International Conference on Cybernetics and Informatics, vol. 163, pp. 2041-2047, 2014.

[18] B. Glas, O. Sander, V. Stuckert, Klaus D. Müller-Glaser, J. Becker, "Prime Field ECDSA Signature Processing for Reconfigurable Embedded Systems", International Journal of Reconfigurable Computing, vol. 2011, pp. 12, February 2011.

[19] Ms P.G.Rajeshwari and Dr K. Thilagavathi, “An Efficient Authentication protocol based on Elliptic Curve Cryptography for Mobile Network.

[20] M. Ashok Mohammed and Dr S. Suresh babu , “Realisation of Elliptic curve cryptography based on ECDSA, Current Trends in Technologies and sciences” Vol1 issue2 sept 2012.

[21] J.Kelly, A.Williams, “Forty Big bank theory Blockchain based Trading System , 2016.

[22] https://www.blockchain-council.org/blockchain/how-does-blockchain-use-public-key-cryptography

[23] https://www.blockchaincouncil.org/blockchain/howdoes-blockchain-use-public-key-cryptography

[24] https://medium.com/@ganeshdipdumbare/use-of-asymmetric-encryption-in-blockchain-fb12ae1be83c