International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 06 Issue: 03 | Mar 2019 www.irjet.net p-ISSN: 2395-0072

Blockchain based Certificate Issuing and Validation

Gowri Shankar K[1], [2=]Dravid A[2], Kamesh M[3], Dr. Jaison B[4]

[1,2,3]B.E Computer Science and Engineering, RMK Engineering College, Tamil Nadu, India
[4]M.E, M.phil Associate Professor, RMK Engineering College, Tamil Nadu, India

---

Abstract*: According to recent researches about three million graduates are passing out each year and the certificate issuing authorities seems to be compromised for the data credentials of student information. Due to the absence of effective antiforge mechanism, events that led to the graduation certificate to be forged often skips getting noticed. In order to solve this problem digital certificate systems were introduced even though security limitations still prevailed. Blockchain is one of the most recent and secure technology that can be adopted for the storage data security. The immutable property of the block chain along with multisig functionality and public key cryptography helps us overcome the problem of certificate forgery and modification. Various issuing and hashing mechanisms have also been used to prevent the usage of duplicate certificates.*

Key Words: Blockchain, Digital Certificate, Hashing, Multisig, Public key cryptography

1. INTRODUCTION

Graduation certificates and transcripts hold information that is easily tampered illegally by individuals and should not be easily accessible to outside entities. Hence, there is a high need for a efficient mechanism that can guarantee the information in such certificates is original, which means the document has originated from an reliable and authorized source and is not forged .Various systems has been designed to secure e-certificates for education institutions[16][17] and to store them securely in cloud based systems[15].Public key cryptography is a main tool to felicitate this need and when combined with different hashing techniques, this becomes a powerful method for issuing and transmission of certificates over the internet. It also helps in eliminating the need for constant verification of certificates. Blockchain technology is used to reduce the incidence of certificate forgeries and ensure that the security, validity and confidentiality of graduation certificates would be improved. Technologies that exist in security domains include digital signatures [14], which are used in digital documents to provide authentication, integrity and non-repudiation. Also with blockchain in play, storage of certificates are most secure. With these technologies a portal has been created that facilitates the need for safe issuing and transfer of certificates that cannot be tampered with.

2. LITERATURE REVIEW

Holt [1] has suggested a different method to store log in a encrypted fashion which makes it difficult to modify, and incase if it is modified it can be detected easily. He emphasizes on the security aspects by explaining log creation and verification process separately.

And Rew Sutton and Reza Samavi[2] have presented a paper on "blockchain enabled privacy audit logs" which concentrates on integrity and authenticity of the data based on the linked data technique.

The Main Concept of blockchain is immutability it is attained by calculating checksum using previous checksum value in that link which makes it impossible to modify[3].are stored in a cloud by concatenating the previous log hash with the current log hash. In log validation process, generated local hash and cloud hash will be compared, and it returns valid if both hash values are same[4].

DApp(Decentralized Apps) stores the data in decentralized manner and changes made in a single ledger will reflects in every other ledger. Token mechanism is employed in it[5][6].

There are three architectural patterns of DApps. In first pattern (Self-Generated Transactions), Users can directly send a transaction or use a web frontend such as MyEtherWallet [7] or use a browser such as Chrome with Metamask [8], Cipher [9], Status [10]. It doesn't depend on third party provider.

In second pattern(Self-Confirmed Transactions), User should trust the DApp provider since DApp provider generates the transaction and further verification will be done by the user[11].

In third pattern(Delegated Transactions), User can interact with the website offered by DApp provider without the support of cryptobrowsers. Interaction with blockchain and sending transactions will be done by backend of website offered by DApp provider. Common example for this pattern is Kraken[12].

Naota Yanai[13] has suggested a ID based multi signatures, In that signer generates a partial signature and combines it with signatures of group of signers.

3. PROPOSED SYSTEM

Our system is being proposed to issue, store and retrieve university certificates through a common portal. Companies can retrieve valid certificates of students through this portal

through permission from both the student and the institution that's hosting the certificates. Initially that issued certificates are scanned and upload to the portal through proper validation. The certificates are stored alongside the student credentials in various servers. The hashes of the certificates are stored in blockchain. A Comb structure similar to that of blockchain has been implemented to alter few certificates if required. When a company requests a certificate from the institution, it retrieves the certificate after checking it with the blockchain. If the hashes don't match then the system is compromised and new certificate is issued. Else the institution hashes the certificate with its private key and sends a request to the student. When the student accepts the request, the certificate is again hashed with his/her private key and is sent to the organization. The organization uses the public keys of both entities to validate the transaction and maintain authenticity. This eliminates the need for redundant verification at different organizations. Confidentiality can also be enforced by using private key cryptographic methods. The system uses PHP as it main functional language and Angularjs for it frontend operations.SHA-256 is used for hashing purposes. Below is the use case of the system that briefly portrays the entire function of the proposed system. Ledger is the database that contains all the required certificates along with the hashes. Multisig functionality is used to involve the user in every authentication process.

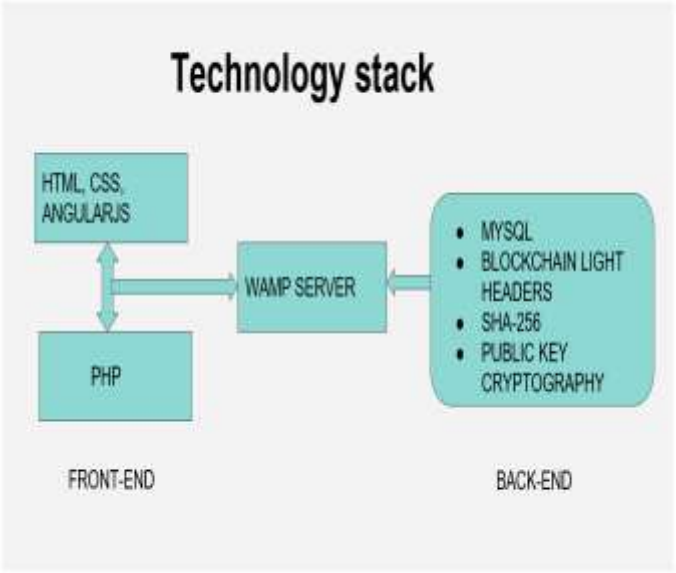

Fig2. TECHNOLOGY STACK FOR BLOCKCHAIN BASED CERTIFICATION SYSTEM

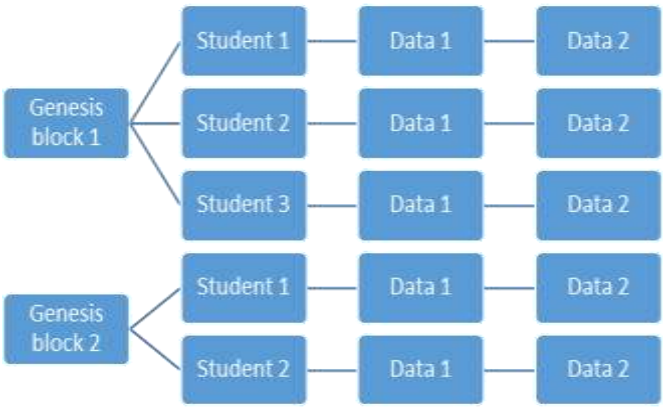

Fig1. BLOCKCHAIN STRUCTURE OF STUDENT CERTIFICATE DATABASE

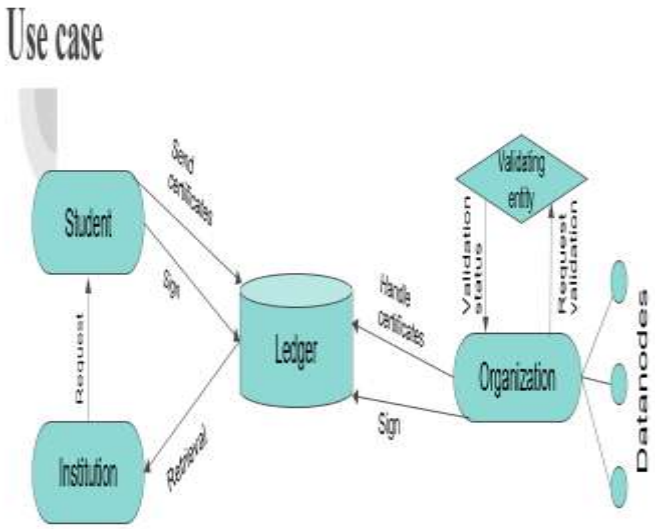

Fig3-USE CASE FOR BLOCKCHAIN BASED CERTIFICATION SYSTEM

4. CONCLUSION

A blockchain-based certificate storage system eliminates the certificate forgery. Automated certificate issuing mechanism is open, compatible and transparent to the system and its users. Companies and institutions can thus inquire for information on any certificate from the system itself. The system saves on paper use, reduces management and maintenance costs, prevents document forgery and provides accurate, reliable and verifiable information on digital certificates.

5. REFERENCES

[1] Holt JE. Logcrypt: forward security and public verification for secure audit logs. Proceedings of the 4th Australasian workshops on grid computing and e research (ACSW '06), Tasmania, Australia, 2006; 203–211.

[2] Sutton A., Samavi R. (2017) Blockchain Enabled Privacy Audit Logs. In: d'Amato C. et al. (eds) The Semantic Web – ISWC 2017. ISWC 2017. Lecture Notes in Computer Science, vol 10587. Springer, Cham

[3] Cucurull J., Puiggalí J. (2016) Distributed Immutabilization of Secure Logs. In: Barthe G., Markatos E., Samarati P. (eds) Security and Trust Management. STM 2016. Lecture Notes in Computer Science, vol 9871.Springer, Cham.

[4] Dr. Manish Kumar, Ashish Kumar Singh, Dr. T V Suresh Kumar (2018) Secure Log Storage Using Blockchain and Cloud Infrastructure (ICCCNT).

[5] D. Johnston, S. O. Yilmaz, J. Kandah, N. Bentenitis, F. Hashemi, R. Gross, S. Wilkinson, and S. Mason. Decentralized Applications: Decentralized applications white paper and spec. (Accessed 2018-03-15). [Online]. Available: https://github.com/DavidJohnstonCEO/DecentralizedApplications

[6] S. Raval, Decentralized applications: harnessing Bitcoin's Blockchain technology, 2016, ISBN 978-1-4919-2452-5.

[7] MyEtherWallet LLC. Myetherwallet. (Accessed 2018-03-15). [Online].Available:https://www.myetherwallet.com

[8] ConsenSys. Metamask. (Accessed 2018-03-15). [Online]. Available: https://metamask.io

[9] HardFork Inc. Cipher. (Accessed 2018-03-15). [Online]. Available: https://www.cipherbrowser.com

[10] Status Research & Development GmbH. Status – a mobile ethereum os. (Accessed 2018-03-15). [Online]. Available: https://status.im

[11] Florian Wessling, Volker Gruhn (2018) Engineering Software Architectures of Blockchain-Oriented Applications (ICSA).

[12] Payward, Inc. Kraken. (Accessed 2018-03-15).[Online]. Available: https://www.kraken.com

[13] Naota Yanai(2017) Tightly Secure Identity-Based Multisignatures (ICCE-TW).

[14] M. Warasart and P. Kuacharoen, "Paper-based Document Authentication using Digital Signature and QR Code," no. Iccet, 2012.

[15] Osman Ghazali, Omar S. Saleh, "Cloud Based Graduation Certificate Verification Model".

[16] Mahamat, M. B. (2016), A Web Service Based Database Access for Nigerian Universities' Certificate Verification System.

[17] Lisha Chen-Wilson, Dr David Argles,"Towards a framework of A Secure E-Qualification Certificate System