International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 05 Issue: 11 | Nov 2018 www.irjet.net p-ISSN: 2395-0072

Survey on Blockchain Based Digital Certificate System

Neethu Gopal[1], Vani V Prakash[2]

[1]M.Tech. Student, Computer Science and Engineering, Sree Buddha College Engineering, Kerala, India.
[2]Assistant Professor, Computer Science and Engineering, Sree Buddha College Engineering, Kerala, India.

Abstract – *According to various researches about one million graduates passing out each year, the certificate issuing authorities are seems to be compromised for the security credentials of student data. Due to the lack of effective anti-forge mechanism, events that cause the graduation certificate to be forged often get noticed. In order to solve this problem digital certificate systems are introduced even though security issues are still exist. 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. Various examples of the digital certificate system is mentioned in this paper.*

***Key Words*: Blockchain, Digital Certificate, Hashing, Ethereum.**

1. INTRODUCTION

Graduation certificates and transcripts contain information confidential to the individuals and should not be easily accessible to others. Hence, there is a high need for a mechanism that can guarantee that the information in such a document is original, which means that document has originated from an authorized source and is not fake. In addition, the information in the document should be confidential so that it can only be viewed by authorized persons. 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 exist in related domains, such as digital signatures, which are used in e-documents to provide authentication, integrity, and non-repudiation. However, for the requirements of an e-qualification certificate, it has critical security holes and missing functions: for example, it uses the keys to verify the modification of the document, but doesn't start the validation of the public key certificates' status automatically. This may result in a forgery being accepted if the key has been compromised. Furthermore, even the signer's public key certificate has been validated, but the signed document itself hasn't. In our case of an e-qualification certificate, the signed document itself is also a certificate, which may have a valid period (e.g. The problem we are dealing with is a (certificate) issue, therefore, a simple digital signing of the document alone doesn't solve the problem.

1.1 Digital Certificate

Digital certificate which adopts digital signature technology, presents to the user by the authority to confirm the user himself in the digital fields used to confirm a user's identity and access authorization to the network resources [1]. Digital certificates can be applied to e-commerce activities on the internet and e-government activities, whose scope get involved in application of identity authentication and data security, including traditional commercial, manufacturing, retail online transactions, public utilities etc.

1.2 Blockchain

BLOCKCHAIN is the fundamental technology underlying the emerging cryptocurrencies including Bitcoin [2]. The key advantage of blockchain is widely considered to be decentralization, and it can help establish disintermediary peer-to-peer (P2P) transactions, coordination, and cooperation in distributed systems without mutual trust and centralized control among individual nodes, based on such techniques as data encryption, time-stamping, distributed consensus algorithms, and economic incentive mechanisms. As such, blockchain can offer a novel solution to the long-standing problems of high operation costs, low efficiency and potential security risks of data storage in traditional centralized systems. Blockchain can be considered as the next generation of cloud computing, and is expected to radically reshape the behavior model of individuals and organizations, and thus realize the transition from the Internet of Information today to the future Internet of Value.

Blockchain is a distributed database that is widely used for recording distinct transactions. Once a consensus is reached among different nodes, the transaction is added to a block that already holds records of several transactions. Each block contains the hash value of its last counterpart for connection. All the blocks are connected and together they form a blockchain. Data are distributed among various nodes (the distributed data storage) and are thus decentralized. Consequently, the nodes maintain the database together. Under blockchain, a block becomes validated only once it has been verified by multiple parties. Furthermore, the data in blocks cannot be modified arbitrarily. A blockchain-based smart contract, for example, creates a reliable system because it dispels doubts about information's veracity.

2. LITERATURE REVIEW

Ethereum

Ethereum is an open and decentralized platform featuring Turing completeness and supporting various derivative applications. Most smart contracts and decentralized autonomous organizations are created by using Ethereum [3]. If the Bitcoin blockchains are considered a global payment network, Ethereum would be the global computing

system. Furthermore, Ethereum is an open-source platform similar to Android (developed by Google). It provides an infrastructure that enables developers to create applications. The infrastructure is developed and maintained by both Ethereum and those developers. The major characteristics of Ethereum are as follows:

1) Incorruptible: third-parties are not able to modify any data;
2) Secure: errors derived from personnel factors are avoided because the decentralized applications are maintained by entities rather than individuals;
3) Permanent: blockchain does not cease to operate even if an individual computer or server crashes.
Ethereum Virtual Machine (EVM) is a programmable blockchain. Unlike Bitcoin, which provides a fixed set of commands, the EVM allows developers to run any programs in the manner they wish. Developers instruct the EVM to execute applications by using a high-level language called Solidity[4].

The literature on the certificate ecosystem is immense. A comprehensive survey on the security issues with HTTPS as employed by web browsers is in [5], which also provides a comparative evaluation of enhancements to the certificate infrastructure used in practice. The survey takes the CA/browser (CA/B) trust model into consideration, as the sophistication and difficulty of directly attacking the SSL/TLS protocol has shifted attention over time to the security of the CA/B infrastructure as well as human factors [6]. Particularly, the survey points out that it has become common for the research literature to assume threat models where the adversary can compromise a target site's certificate. The MCPKI proposes addresses such threats by importing the idea of moving target defense [7], which is materialized with self services including spontaneous substitution and reissue after revocation for certificate users like web sites.

A new framework to generate correlated digital certificates embracing major signature schemes including RSA, ECDSA, and DSA to better satisfy the security and privacy requirements of certificate users. One case study, the multi-certificate public key infrastructure (MCPKI), supports user certificates' spontaneous substitution as well as self-reissue after self-revocation. Another application, the anonymous digital certificate (ADC), features a self service of de-anonymization, allowing the user to reveal her identity-key binding to preferred communication peers only.

A Secure E-Qualification Certificate System

The development of the system will adopt the SOA of the e-framework to meet the distributed stakeholder user case. SOA allows developers to build applications from sets of services with well defined interfaces and is achieved without "tight coupling between transacting partners"[8]. When used with interoperable e-portfolio XML schemas, this makes it easy for any e-portfolio vendor to integrate e-certificate services into their application; hence enabling and encouraging user take up and participation between users using software from potentially different providers.
The system design overview: The institution will create and issue a digitally signed, time stamped, and access-controlled e-certificate to the specified student through a secured emailing system. The student view and set new access controls to the received e-certificate through a central system before sending it out to further reviewers. The reviewers also use the central system to view and verify the access-controlled e-certificate. It is shown diagrammatically in Figure 1.

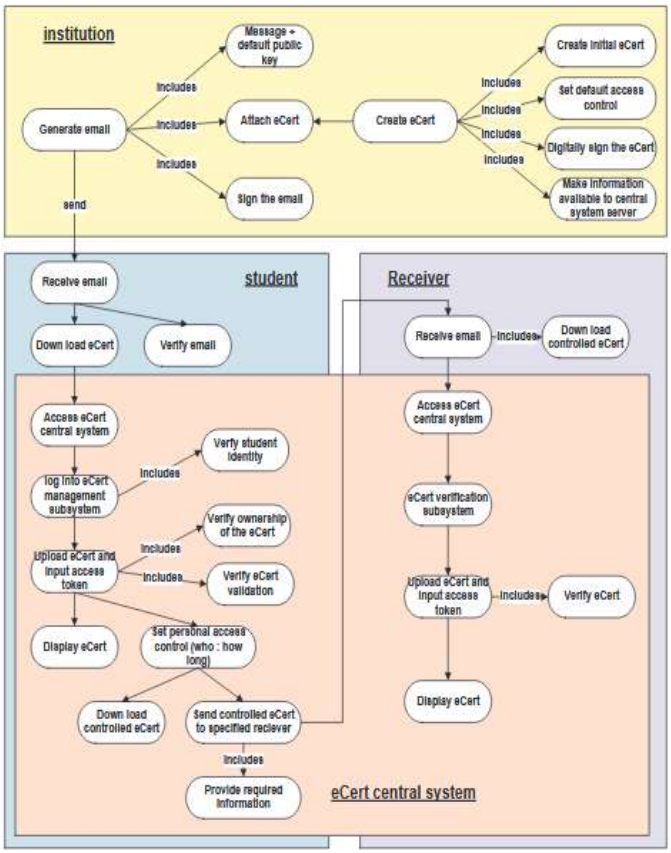

Figure 1. E-Certificate system overview[17]

The system design does not require any e-certificate copies and sensitive data, such as private keys, to be stored in the system, while it provides all the required services through a secured environment. This feature has a huge advantage of minimizing the chances of being attacked and saving storage, especially when its usage is nationwide, and the e-certificates need to last for life. This becomes increasingly significant as the system grows in size.

Authorization and Delegation in IoT-Cloud based on Blockchain

When compare with a datacenter-oriented Cloud middleware, the administrator and the owner of the infrastructure are not one and the same. It shows the requirement to support delegation-enabled authorization. The authors carryout research for an authorization and delegation model for the IoT-Cloud based on blockchain

technology. This scheme is implemented in the form of smart contracts over the Ethereum platform. It enables the user to audit authorization operations and inspect how access control is actually performed, without blindly trusting the Cloud as a proxy for access to resources.

The implementation of the Ethereum-based authentication and delegation mechanisms in Stack4Things has been conducted by an agile development process and use solidity as the reference language due to its similarity with Java script and the better support that the Ethereum community provides. It first designed and implemented all the mechanisms within a single smart contract, with complete functionality. Remix IDE is used as solidity compiler and allows to test simple transactions for checking correctness and removing bugs. In order to maintain the smart contracts code size two separate contracts are designed, Role. sol contract captures the association of each role with the corresponding allowed operation and delegation. sol, represents the relationship between users, resources, and roles. The coupling between the two smart contracts are reduced by using Composition design strategy over inheritance. For code development Truffle framework is used. Ruffle is a more powerful development environment compared to Remix as it not only acts as a Solidity compiler but also allows testing smart contracts in a flexible way, supporting different testing environments.

Traditional access control models, like Role-Based Access Control (RBAC) model [9], depend on a trusted third-party authorization engine to grant access. This creates mistrust in the system. Also, such models are based on a centralized model, which does not overlap with the distributed architecture of the IoT. This led us to explore blockchain technology as an access control mechanism, due to its distributed nature. A. Ouaddahet al. [10] used blockchain to store and audit access control policies. L. Chen and H. Reiser [11] store access rights for a resource in a blockchain and manage them via transactions. MeD Share proposed by Xia, Qi, et al. [12], for controlling access to sensitive medical data, uses blockchain to store the history of operations performed on the data and smart contracts to enforce access control.

Cloud based Graduation Certificate Verification Model

Certificate verification is essential in order to ensure that the holder of the certificate is genuine and that the certificate itself comes from a real source. However, the verification of graduation certificates is a challenge for the verifier (the prospective employer who wants to verify the certificate). To address this issue, a cloud-based model for certificate verification is proposed. The university, the graduate and the verifier are the three parties involved in the proposed solution in order to accomplish accurate certificate verification. Three key aspects security, validity and confidentiality are considered in the proposed model. Several internal and external benefits can be obtained by using the proposed model. Internal benefits include improved work processes and ease of use for university staff due to the digitization of the verification process. External benefits include the receipt of faster and more efficient verification results by students/alumni and employers. The proposed model could also improve the links between universities and government entities.

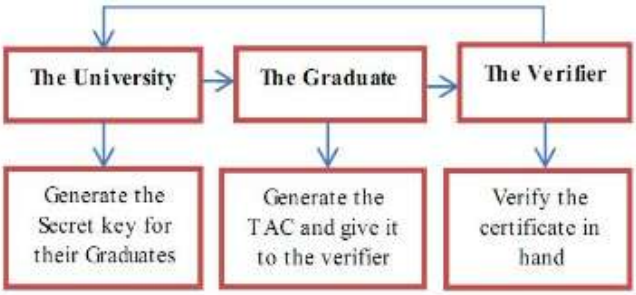

Figure 2. Suggested process for certificate verification[16]

Several methods can be used to verify a document and can guarantee the originality and confidentiality of a document, including cryptography techniques and cloud services [13], [14]. Both cryptography techniques and cloud services are incorporated into the suggested solution.

Validate the Integrity and Confidentiality of Backup Versions on the Cloud based on blockchain

The introduction of cryptocurrency was an account of digital revolution that changed the lifestyle worldwide. One of the successful examples of cryptocurrency is bitcoin, which was established by Satoshi Nakamoto who introduced a new financial system based on blockchain technology to enable payment transactions between two without the need for a financial intermediary(bank). The system aims to find solutions for the issues that are facing researchers who pay huge amounts of money for hosting data on local servers rather than using cloud services. They have several concerns about using cloud services like: Hosting sensitive data in the cloud, could cloud solutions keep sensitive data safe, could cloud solutions achieve confidentiality, integrity, availability. A system was created with a graphical interface that enables system administrators to take backups of specific data. For example, patient files saved in an encrypted format using blockchain technique (each backup request means a new transaction based on the previous one). Admin of the system can use the previous key to check the file integrity. Blockchain technology provides strong encryption process for the confidential data. Also the system admin can detect unauthorized modifications on any version of backup files through reverse hashing operations.

The blockchain technology that has greatly improved the global economy since it is possible for parties to trust each over a long distance through the blockchain records and be able to conduct business operations suitably. It is important to be more facilitated on its numerous operations to achieve better future for currency transaction and improve trust amongst business operators. There are many benefits of blockchain technology, but there are some limitations too, the time required to calculate the value of the hash each

time, the expected problems of scalability and the need to know the hash number of the backup versions.

Automated Batch Certificate Generation and Verification System

Nowadays a numbers of certificate generation and verification systems have been developed to overcome the difficulties faced in the manual system and minimize the processing time for generating a certificate. The systems works based on the predefined template and predefined template format by the system developer. Also, some systems allow end-user to define template and template format by the use of XML. The technology mentioned here requires an end-user to have minor knowledge of XML to be able to define template and template format. The automated batch certificate generation and verification system enables an end-user to define certificate template and template format without the requisite of XML knowledge by using the system GUI, verifying the certificate and generating one or more certificates concurrently in an instantaneous manner. Certificate verification process is unavoidable in many institutions as students are issued admissions and grants in view of the certificate they presented and staffs are employed based on the qualification they provided to an institution [10]. The system explores a new technique to address the problem of certificate generation system that uses predefined certificate template by proposing a module that enabled an end-user to define certificate template and its format in the system GUI by typing and clicking buttons. In variance to Dejan [3] work that requires an end-user to have a minor knowledge of XML to be able to define certificate template and certificate template format.

Blockchain and Smart Contract for Digital Certificate

During the course of study, the students' all kinds of excellent performance certificates, score transcripts, diplomas, etc., will become an important reference for admitting new schools or new works. As schools make various awards or diplomas, only the names of the schools and the students are input. Due to the lack of effective anti-forge mechanism, events that cause the graduation certificate to be forged often get noticed. In order to solve the problem of counterfeiting certificates, the digital certificate system based on blockchain technology would be proposed. By the unmodifiable property of blockchain, the digital certificate with anti-counterfeit and verifiability could be made. The procedure of issuing the digital certificate in this system is as follows. First, generate the electronic file of a paper certificate accompanying other related data into the database, meanwhile calculate the electronic file for its hash value. Finally, store the hash value into the block in the chain system. The system will 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.

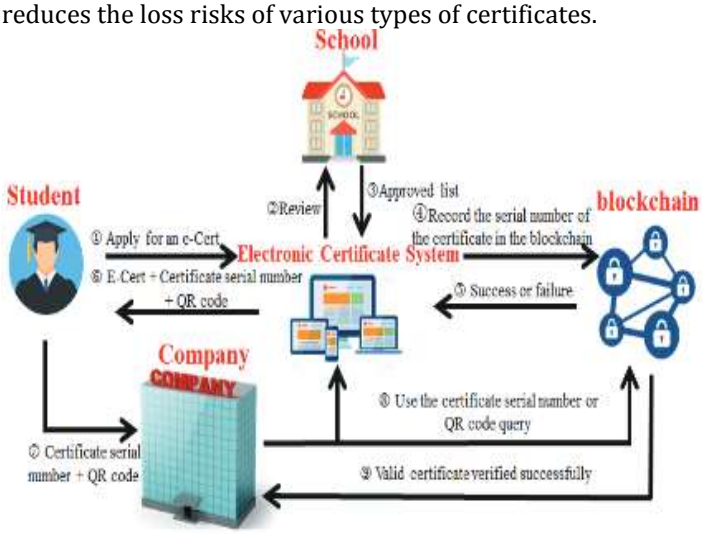

Figure 3. System overview[18]

3. CONCLUSION

Various technologies has been discussed to reduce the incidence of certificate forgeries and ensure that the security, validity and confidentiality of graduation certificates, even though there are many limitations regarding the security and privacy of data. A new blockchain-based system reduces the certificate forgery. Automated certificate granting are open and transparent in the system. Companies or organizations can thus inquire for information on any certificate from the system. The system saves on paper, cuts management costs, prevents document forgery, and provides accurate and reliable information on digital certificates.

REFERENCES

[1] C. K. Wong and S, S. Lam "Digital signatures for flows and multicasts", WEEE/ACM Transactions on Networking, 7(4): 502- 513, 1999.

[2] A. M. Antonopoulos, Mastering Bitcoin: Unlocking Digital. Sebastopol, CA, USA: O'Reilly Media, 2015.

[3] 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.

[4] Chris Dannen, Introducing Ethereum and Solidity, https://www.apress.com/br/book/9781484225349

[5] J. Clark and P. C. van Oorschot, "SoK: SSL and HTTPS: Revisiting past challenges and evaluating certificate trust model enhancements," in proc. IEEE S&P'13, May 2013, pp. 511–525.

[6] L. Zhang, D. Choffnes, D. Levin,et al., "Analysis of SSL certificate reissues and revocations in the wake of

Heartbleed," in proc. ACMIMC'14, Nov 2014, pp. 489–502.

[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] Papazoglou, M., Service-Orientated Computing: Concepts, Characteristics and Directions, in International Conference on Web Information Systems Engineering. 2003, IEEE: Rome.

[9] D. Ferraiolo, R. Kuhn, and R. Sandhu, "Rbac standard rationale: Comments on "a critique of the ansi standard on role-based access control", "IEEE Security Privacy, vol. 5, no. 6, pp. 51–53, Nov 2007.

[10] A. Ouaddah, A. A. Elkalam, and A. A. Ouahman, "Towards a novel privacy-preserving access control model based on blockchain technology in iot," in Europe and MENA Cooperation Advances in Information and Communication Technologies. Springer, 2017, pp. 523–533.

[11]L. Y. Chen and H. P. Reiser, "Distributed applications and interoperable systems, 17th ifip wg 6.1 international conference, dais 2017, held as part of the 12th international federated conference on distributed computing techniques, discotec 2017, neuchtel, switzerland, june 1922, 2017." Springer, 2017.

[12]Q. Xia, E. B. Sifah, K. O. Asamoah, J. Gao, X. Du, and M. Guizani, "Medshare: Trust-less medical data sharing among cloud service providers via blockchain," IEEE Access, vol. 5, pp. 14 757–14 767, 2017.

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

[14] J. van Beusekom, F. Shafait, and T. M. Breuel,"Text-line examination for document forgery detection," Int. J. Doc. Anal. Recognit., vol. 16, no. 2, pp. 189–207, 2013.

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

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

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

[18] Jiin-Chiou Cheng, Narn-Yih Lee, Chien Chi, and Yi-Hua Chen," Blockchain and Smart Contract for Digital Certificate".

BIOGRAPHY

Neethu Gopal, she is currently pursuing Master's Degree in Computer Science and Engineering in Sree Buddha College of Engineering, Elavumthitta, Kerala, India. Her research area of interest includes the field of Security and Blockchain Technology.