Security Enhancement Digital Certification System Using Blockchain Technology

Win Zaw Latt
Information Technology Department
Metro IT and Japanese Language Center
Yangon, Myanmar
winzawlatt@ ucsy.edu.mm

Prof. Mie Mie Su Thwin
Head of Cyber Security Research Lab
University of Computer Studies
Yangon, Myanmar
drmiemiesuthwin@ucsy.edu.mm

Abstract— **Education is an important part of human life and it is also valuable asset for career achievement. Nowadays, people gained certificates from the institution they had learnt and, those graduation documents are presented as the testimony of their knowledge. Most graduation documents are traditionally issued as paper document and, so it is easy to damage and loss. There are many documents hand overs in career introducing, for testimonies of educational certification and personal information. Moreover, information expressed in the certificates are critical to the certificate holder. That is why, damage or loss of certificate is needed to be safe and, forge in graduation document must be prevented and secured as well. To overcome above drawback of paper certificate, this paper proposed to issue digital graduation document by utilizing blockchain technology as an enhancement of information security. In this work, we examine a basic understanding of what blockchain technology is and how it can achieve security with its immutability feature. Moreover, by using off-chain storage, digital graduation documents are no longer needs to be hosted the personal information on blockchain and computational performance become efficient.**

Keywords—Blockchain, On-chain, Off-chain, electronic Graduation Document, consortium blockchain

I. INTRODUCTION

Human studied education for their life development. They studied different subjects at different institutions, colleges and universities. And they would be certificated with diploma or graduated degree at what they studied. Then, they would attend further course to improve their career skill or to continue studying for more valuable specialist. And they would start hunting job for their career concern with what they have studied or they would try to continue studying. Many government ministries and business organizations, institutions alike require original graduation documents to be provided when the graduates apply for job or further course. Although the paper certificate does not directly contain the knowledge they acquired, the graduation document approves that they have acquired a skill.

However, they often lost their educational graduation documents and commendation letters among intermediary handling. Reapplying hard copy certificate is time consume because some certificates are issued by different organizations and may require in-person application. At the worst, some document such as birth certificate, attending conferences or participating in hackathons are issued only once. So intermediary persons may reluctant in handling these important documents as they could get damaged, lost in transfer, etc.

By contrast, utilizing for a digital-copy documentation saves paperwork and time. Graduated students can easily apply for their graduation documents by providing required information. Nevertheless, because of this easy process, it is possible to forge the graduation documents and certificates can be widespread. Although widespread is not a serious, easy to forge is the main problem of digital graduation documents. Most of fake academic certificates can be found as “Degree Mills”, “Fabricated Documents”, “Modified Documents”, “In-house Product” and, “Inaccurately Translated Documents”.

Degree Mills: selling counterfeit products to customers [10].

Fabricated Documents: pretend to represent a fictitious degree or organization.

Modified Documents: alter the facts of legitimate documents such as changing in enrollment / graduation dates, grades, course content, date of birth, specialization etc.

In-House Produced: the employees of legitimate institutions fabricate fake documents and printed on authentic paper and bearing the seals, stamps and signatures of the institution.

Inaccurately translated documents: to indicate as academic graduation documents issued by institutions that are not registered or lack government authority to grant such credentials [7]

Consequently, educational institutions and business organization cannot instantly validate the graduation documents they receive. As the above findings is raised, the problem of fake certifications become serious and needs to be urgently tackled. It is absolutely need to verify the authenticity of a particular digital asset from anywhere without having to rely on third party or intermediary.

Nowadays, it is a demanding issue to provide legitimate digital graduation documents which can be accessed and referenced from anywhere. On the other hand, it is also necessary to create a digital proof that a digital graduation document has been signed by an authorized organization or government ministries. Apart from the “banking” “financial services” and “insurance” sector, universities, educational institutions and business organization can also make use of the blockchain technology. Verification of degrees and graduation documents can be achieved through the use of off-chain data storage and blockchain verification methods. Universities can issue digital graduation documents instead of printing degree graduation documents and storing physical copies. We propose a data security enhancement with off-chain storage system based on the consortium blockchain.

This paper is divided into eight sections: we introduced the need of digital graduation document first, and then reviewing the blockchain network, suggestion of a suitable blockchain network, architecture of hyperledger fabric, related work of proposed paper, proposed approach, discussing the proposed approach and, conclusion of the proposal.

II. Blockchain Review

With the advances in information technology and the wide availability of the Internet, and common usage of mobile devices have changed the lifestyle of human being. Since utilizing the Internet technology become convenience, various digital currencies are appeared such as popular Bitcoin, Ether, and Ripple. People begin to interested in Blockchain technology, as the backbone technology of currency revolution. Besides the currency sectors, educational institutions such as colleges or universities, can also make use of the technology. Both issuance and verification of degrees and graduation documents can be done through the blockchain security and verification methods, and off-chain storage transaction.

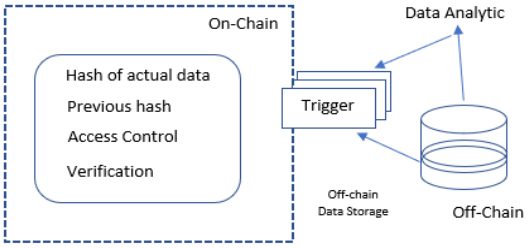

Figure 1. Over view of On-chain and Off-chain storage

A) *Blockchain Mechanism*

Among the exciting features of blockchain, "immutability" plays as a key feature of technology. The word “Immutability” means something that can’t be changed or altered. Each node in the blockchain system has a copy of the immutable digital ledger [2]. To add a transaction every node needs to check validity immutable digital ledger. If it’s valid, then transaction is added to the ledger. It increases transparency and prevents corruption. This immutability feature can solve the existing problem of verifying the validity of digital graduation document at a very low implementation cost. In our system, the blockchain is used for a very specific task of storing digital signatures of graduation documents that prove their validity. On the other hand, due to the characteristic of blockchain’s decentralized information ledger, digital signatures of graduation documents can be accessed by providing registered keys. Hence anyone with access to the blockchain can now verify the authenticity of a digital graduation document without having to rely on trusted intermediaries.

There is a process at making a block that need to create an encrypted code as the “hash value”. The process produces “hash value” with a fixed length on a given block and it cannot be modified arbitrarily. The result of hashing becomes block’s header. The header becomes part of cryptographic puzzle solved by manipulating a number called “nonce”. And a hash of the previous block’s header and timestamp are also included in the block.

B) *“Off-chain” Storage and transaction*

In the transactional flow of any blockchain platform, there are two different layers; “on-chain transaction” and “off-chain transaction”. Some transactions are committed to blockchain network as the distributed ledger. We regarded such transaction as “on-chain transaction” [11]. And “off-chain transaction” is defined as transactions that performed outside the blockchain and stored into any database.

In our system, we do not store the digital graduation document on the blockchain (on-chain). Instead the blockchain only stores the proof that a digital graduation document has been certified by an institution on the blockchain through determining the hash, validating the block with trusted signatures.

In contrast, the off-chain transactions will not be stored for every node in the storage space. Instead it is used to store specific transactions “digital graduation documents”. Some transactions are performed with the agreement between transacting parties. We regarded such transaction as off-chain transaction [11]. It means that “off-chain transaction” is performed depending on the verification of blockchain transaction.

An off-chain transaction allows data values movement outside blockchain. The agreement to use the particular transaction method is needed to accept between all parties.

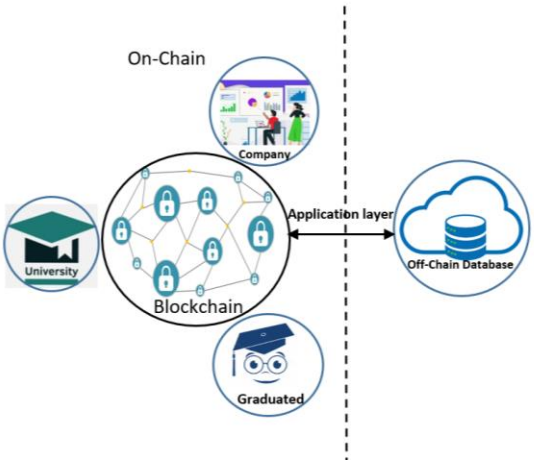

Figure 2. Blockchain users and Off-chain

If anybody would want to verify the legitimacy of a digital graduation document, they can simply verify the digital asset by vetting it using the proof provided. The role of blockchain in this solution is to provide an immutable storage container for these proofs. Off-chain is required when a party wants to verify the information of digital graduation document with blockchain, but necessarily want to restrict the availability of information.

III. Choosing the Suitable Network

Blockchain is a peer to peer network technology. Its ledger is distributed among the network. The data in the ledger are hashed and maintained as a LinkedList data structure and so its gained immutable features. The transaction on the network are needed to be validated by a consensus algorithm before adding to blockchain. Depending on the consensus algorithm, blockchain can be categorized in to three types;

The first type is “Public Blockchain” which allow to join everyone without needing permission from someone. Data access to this type of blockchain is permission-less and transparent to anyone. The transaction validation is based on the “Proof of Work” PoW consensus algorithm. [20]

The second type is “Private Blockchain” which allow to only known participants. This type blockchain need mutual trust among the group of participants. Data access to this type of blockchain is need permission from the network. So, it was called permissioned blockchain. The transaction validation is controlled by single entity or single organization. It was based on the use of “Byzantine-Fault Tolerant” BFT consensus algorithm. [14]

The third type of blockchain is “Consortium Blockchain”. It is also known as hybrid blockchain. In this type of blockchain, group of participants are equally acknowledged in the consensus. The data access to this type of blockchain are partially decentralized. The “practical Byzantine-Fault Tolerance” pBFT algorithm was preferred in this type of blockchain. [3]

Among the three types of blockchain, ("Public Blockchain ", " Private Blockchain "," Consortium Blockchain") we implement the consortium blockchain approach. Because, hyperledger fabric is implemented the consortium blockchain technology and, node must be identified authorization in advance. On the other hand, in public blockchain, everyone can check the transaction and verify it as well and, privacy is weak. In private blockchain, not every node can participate the blockchain, the nodes will have restricted in term of data access. Consortium blockchain is hybrid.

IV. HYPER LEDGER FABRIC ARCHITECTURE

Linux Foundation promote blockchain technology with an open-source project, naming hyperledger framework which facilitates the advancement of blockchain technology. This framework can solve various problems across industries. The hyperledger project was surrounded by the community from companies, software developers and academic instructions. Distributed ledgers, libraries and tools are the three prominent parts of hyperledger project. There are six solutions in hyperledger (Besu, Burrow, Fabric, Indy, Iroha and, Sawtooth). Since the hyperledger can be used in the area of identity and user management across consortium blockchain network, we choose to use hyperledger fabric framework in our proposed project.

Fabric solution support privacy of both identities and data. It also allows plug-and-play distributed ledger creation. As the consortium blockchain used the hyperledger fabric, it become permissioned blockchain and which gain higher security level than permission-less blockchains.

A) Fabric Overview

In the fabric architecture, the transaction flow can be divided into three phases (execute, order, validate) and its application has two parts (chaincode and endorsement). First part is chaincode program which lead the execution phase as the smart contract of etherum network. It was responsible to work with ledger. Second part is endoser which evaluated the transactions according to the endorsement policies in the validation phase. Endorsement policies can be parameterized by the chaincode. The endorsement policies are static and nobody can modify it, except designated administrator who can perform system management functions [5].

In this part, endoser verify whether transaction proposal is properly authorized to perform the proposed operation on the channel.

Since the fabric is the permissioned blockchain, all the nodes request to participate in its network are needed to have permission. There is a Certificate Authority (CA) in hyperledger fabric which issue digital certificates for the organizations identities to manage the identities of all member and users. (e.g. users, client applications, peers, orderers). Although hyperledger fabric has default CA service, we can use our own public-private key pairs management. In hyperledger fabric network, Membership Service Provider (MSP) module identified the organizations. MSP module, can provides one of three roles. *Client role*: it has permission to submit transaction proposals at execution phase. *Peer role*: it has permission to execute transaction proposals, to validate transactions and to maintain blockchain ledger. Any application to get or put data to ledger must connect to a peer. *Orderer role*: it has permission to order services and collect ordering services and share communication between peers and clients. It orders transaction for multiple channels only for chaincode invoke requests. Orderer does not participate in the execution and the validation of transactions.

B) Execution Phase

In the execution phase, client will sign in the network with its private key and submit transaction proposal to the peers. Then, the correctness of transaction proposal will be checked with endorsement policy. Being on the correctness of transaction proposals, those transaction proposals will be executed in this phases. The proposal must contain the identity of client, the identifier of transaction, the identifier of chaincode, parameters and nonce value.

C) Ordering Phase

In the ordering phase, transactions are ordered per channel and establishes consensus on the transactions. [22] In this phase, the block of transactions is put into the ledger by peers as ordering. Multiple transactions are hashed and linked as the sequence of block, in this phase.

D) Validation Phase

The endorsement policy evaluation appears together with the transactions block. Each transaction block will contain the read/write sets, the Channel ID and the endorsing peers' signatures. Validation system chaincode (VSCC) is responsible for validating the endorsement. When a transaction is simulated, read-set is prepared for transaction. a list of unique keys and committed versions will be included in the read-set. Contrary is write-set which included a list of unique keys and new value to be write transaction. In the validation phase, read-write conflict check will be performed for all transactions.

V. RELATED WORKS

Jiin-Chiou Cheng et al. proposed a Digital graduation document System, which transform assets through smart contracts, thereby creating value through the emergence of alternatives to Bitcoin[2]. The system’s application was programmed with Solidity programing language on the Ethereum platform and is run by the EVM. Aravind Ramachandran and Dr.Murat Kantarcioglu leverage Blockchain as a platform to facilitate trustworthy data provenance collection[1]. Their system was utilized smart contracts and open provenance model (OPM) to record immutable data trails.Their system was experimented on the scenario of a clinical drug trial.

Khuat Thanh Son et al. developed an application to guarantee the Integrity and transparency of document, based on the nature of Blockchain's data security [3]. They analyzed their application to deal with the problem of data integrity and transparency for text documents stored in the network for external queries.

Knowledge Media Institute (KMI) of the Open University UK used of Ethereum blockchain for UK higher education qualifications. KMI focused on the application layer, user control and, wallet of private keys.

University of Nicosia (UNIC) developed a Bitcoin blockchain application to accept bitcoin for tuition for degree program and, issued academic certificates on Bitcoin blockchain.

MIT Media lab issued digital certificates by using Blockcerts framework. In MIT's certification, Issuer signed digital signature on certificate and stored the hash of certificate within the blockchain transaction. The recipient was assigned with the transaction output.

Blockcerts, which is used to build verifying blockchain applications such as academic credentials and, professional certificates, is a well-known certificate solution. Blockcerts has create, issue, view and verify certificates components in its blockchain.

another blockchain verification platform was SmartCert. It was developed to authenticate academic credentials on a blockchain and to verify fake certificates problem. To provide transparency, SmartCert cryptographically sign on the certificates. the employer verified with the hash of graduation document which shared from the student.

TABLE 2. EXISTING SOLUTION AND THEIR SHORTCOMING

Institution/ Solution	Salient features, functionalities	Shortcomings in feature/ functionality
KMI -UK	Badges, certificate and web reputation in the blockchain	Does not support employers as an entity. Data is stored on public blockchain. The certificate is vulnerable to manipulation, No clear method of authenticity of parties
UNIC	Resolve fake certificate, Tools available for authenticity of certificate, Good in integrity, privacy, ownership	Requirement for an employer to verify the certificate is inadequate. A student cannot authorize the prospective employer to verify the certificate, No clear method of authenticity of parties
MIT Media lab	Offer more control to students, Use digital keys	Level of trust is low, the certificate can be accessed by anyone, No clear method of authenticity of parties
Blockcert	Open standard platform	No separate verification service, vulnerable to spoofing attacks
SmartCert	Resolve problem of fake certificate, Student share hash with the employer	Vulnerable to attack, Need for basic information security measures, No clear method of authenticity of parties
RecordKeeper	Proof of authenticity in the Graduation Document, The entire verification is based on ownership	Certificate vulnerability, Participants can verify after obtaining ownership

Another blockchain based solution is Records Keeper which verified academic graduation documents. Educational institutes can issue graduation documents by using Records Keeper. The issued certificates receipt was provided to the users and users shared the receipt with third party to verify the graduation document is authentic.

VI. PROPOSE APPROACH

In this section, we will mention the digital graduation documents system which consists of four layers: namely- client application layer, consortium blockchain layer, network layer, and off-chain storage layer. The client application layer comprises of graduation documents, students' other credentials, students and, employeers etc.., In the consortium blockchain layer, employers and University's Registrar are needed to register as the predefined user or validators. They are responsible to verify and validate transactions gradational documents. All the connectivity tasks between application, consortium blockchain and off-chain storage are performed by network layer. off-chain storage layer stored the large files that can be burden to the blockchain, such as images, pdfs and docs etc. Since the blockchain database is immutable, some temporary information that are to be deleted or change in the future, should not be store in blockchain. In this case, off-chain storage will store such data.

A) Client Application Layer

At this layer, graduation ID, QR code and other credentials convey by graduated student will be included. Those things will interact with University's consortium blockchain nodes. Second essential are employers and other digital assets, such as private key, public key and block address. If the employer wants services blockchain services, he/she must request by signing in with private key and then get communicate with government P2P consortium blockchain network. For the client application, we will use hyperledger fabric SDK to interact with the Fabric network. This layer provided to realize the interface between digital graduation information and users. In our system, Fabric Certificate Authority will be sit on this layer. As mention in Certificate Authority, although hyperledger fabric has default CA service, we can use our own public-private key pairs management to enhance security of the application.

B) Consortium Blockchain Layer

The employer who desire to verify students' graduation document are participants of consortium blockchain network. They needed to register at University's Web portal as pre-defined users of the consortium blockchain network. After registration, pre-defined users will receive a key pair, private key for signing, public for verifying transaction and blockchain address. Any transaction attempting to add to blockchain ledger are needed to validate before adding and many validators will be required among the consortium peers. Predefined user and other validators can be reacted as grant or deny access to blockchain ledger, depending on the ordering policies of fabric.

C) Network Layer

This layer is the main connectivity layer of the system. The network layer performed connections between application layer, consortium blockchain layer and off-chain storage layer. All the participants of this system will have to use this layer to perform to and from user transaction, to store new block to blockchain and off-chain storage layer. Nowadays, wireless communication is globally connected and widely accessible in everywhere.

D) Off-chain Storage Layer

Off-chain storage layer stored the large files that can be burden to the blockchain, such as images, pdfs and docs etc. It is also used to store replication of students' personal data and other facts that are required to be deleted or changed in the future. Since the blockchain database is immutable, the facts to be deleted or changed should not include in the blockchain. As the off-chain data and documents are also required to verify, a hash value for the off-chain data and documentation will be produced and attached in the consortium blockchain ledger [3]. Nevertheless, the actual data and document will be kept in the off-chain storage. Moreover, the data processed by blockchain participants are also replicated and stored in the off-chain storage layer.

The users of our system are graduated student, employer and registrar (university's digital certificate providers). Each of student, or employer is a network application client of the system a digital graduation document system. They need to register and enroll with the Certificate Authority (CA) of University's web portal and acquire necessary cryptographic material such as private key and public key which is used to authenticate to the network. And then they will be able to communicate the digital graduation document system with read only access. In hyperledger fabric, network was segregated into channels, where participants can be authorized to access data for the chaincodes through those channel. The registrar can explore the entire system and Off-chain database.

When a student has offered a degree, he/she is able to access his/her digital graduation document at the University's blockchain network. The maintenance of digital graduation documents was done by offchain storage. The working processes of the system developed in this study are as follows:

After granting degree to the students, the registrar will hash and store graduation document information into blockchain and same time it generates the unique graduation id or QR code. The graduation id and QR code will be sent email to each student. Student can submit the received QR code or Graduation document id to employer organization instead of physical hard copy of documents.

The employer can submit QR code or graduation id to the blockchain for verification purpose. To verify and submit graduation information, employer must register at the University blockchain network. The digital graduation document will be inscribed in (JavaScript Object Notation) JSON format. In the digital graduation document, there will also inscribe hashed link to off-chain storage. In the off-chain storage detail information of graduated student, some temporary information which will be modified or deleted in the future. Since the information store in the blockchain are immutable some temporary information should not be in blockchain. Moreover, some information format such as image file, pdf or doc format are burden to the blockchain. That information will be kept in the off-chain storage. To

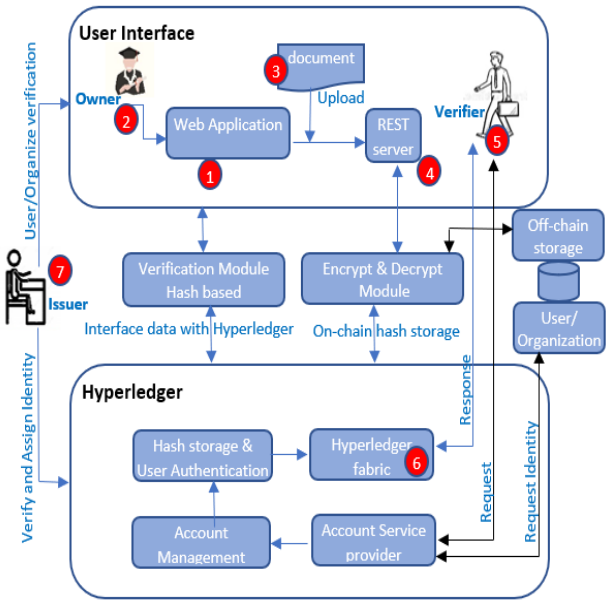

Figure 3. System Overview

access the off-chain will also need user's private key.

If the particular graduation document is issued to the graduate, then the graduate can look up his/her own graduation document by signing into the system. When an employer acquires a QR code and graduation id, he/she can register and sign into the system to verify the veracity of the associated graduation document. If the information in the Blockchain system match with applicants' information, validation message is displayed and graduation Document is approved by the system.

The numbered notations in figure 3. are referred to the following:

1) Web application is the starting point for all users.
2) Each user will be assigned unique identity on hyper ledger from system administer.
3) Document will be uploaded by owner and will be linked to owner identity ensuring ownership.
4) Authenticated access to the flow of data to and from hyperledger.
5) Verifier will be performed graduation document verification.
6) Data is only visible to concern entity who has permission to access ensuring privacy.
7) The issuer can be the admin of whole system. Would be responsible for verification of new organization or users and issuing identity users after physical verification.

VII. Discussion about the System

we compared digital graduation documents and those issued on paper. And we found some advantages of digital graduation Document over paper-based certificate. The digital graduation documents need fewer resources than paper-based graduation document for issuance and maintenance. In case of improper use of graduation document owner, the digital graduation document can be revoked by the issuing

institution. Moreover, digital graduation documents are difficult to modify or forgery then paper-based graduation document. Since the digital certification system is based on blockchain technology, our graduation documents gain the immutability feature.

However, digital graduation document can have some disadvantages, if there are lack of digital signatures, they are easy to forge. The digital graduation documents issued from our system can be verified within the system. Pushing all the data directly into the blockchain (i.e. on-chain) is not feasible, due to the huge volume and variety of data generation [8]. Instead, off-chain storage maintained the actual data and, on-chain transaction carried the hash of the real data. Also, the consensus mechanism can be designed for the Off-chain and on-chain to ensure an agreement among the participating peers [16]

Since our blockchain architecture has two parts: such as on-chain and off-chain, we gain the immutable feature and distributed feature from on-chain part and The on-chain information are non-sensitive data. Information privacy was secured from off-chain part by using private keys. The digital certification system can distribute the students' information resources from off-chain storage in a reasonable manner through distributed synchronization and coordination.

In our system, the on-chain transaction is linked with the current hash code which encrypted the graduation document information and previous hash code and, the security of on-chain transactions is depend on the hashing algorithm. Moreover, off-chain transaction is secured by verifying private keys between parties, and the privacy of graduation document owner's detail information become confidential. when we try to save the digital graduation document of a document ("cryptographic hash") - not the certificate document itself to blockchain without using off-chain, it was terribly time-consuming. So, the questions how to manage the documents were raised. Since the personal data should be confidential, we plan to use off-chain storage, which processed outside the blockchain environment .

Nevertheless, the distributed feature of blockchain technology was lost because the off-chain storage was centralized at the specific server. If the central server is damaged or out of service, we will lost detail information of graduation document owner. The difference between Ethereum smart contract and hyperledger fabric chaincode is that former is public and latter is hybrid.

VIII. CONCLUSION

For innovation in information security, there has a great potential in blockchain technology. Significant changes to existing systems and processes can be done with blockchain technology and it can also promote the emergence of new business models. In this paper, the use of consortium blockchain technology and the issue ensuring transparency are analyzed. Moreover, to make transaction cost less, we reduce the content relating to the blockchain by storing only requires a small amount of data. The digital graduation documents are stored in the off-chain. The likelihood of graduation document forgery is prevented by the security features of blockchain technology. Graduated students can prove and organization can verify for the information on the graduation document from the system.

REFERENCES

[1] Aravind Ramachandran and Dr.Murat Kantarcioglu , "Using Blockchain and smart contracts for secure data provenance management", The University of Texas At Dallas, 800 W Campbell Rd, Richardson, Texas 75080, axr156530@utdallas.edu.

[2] B. Xia, D. Ji, and G. Yao, "Advances in Information and Computer Security," vol. 7038, no. 2016, pp. 56–66, 2011.

[3] Castro, M., & Liskov, B. (1999). Practical byzantine fault tolerance. OSDI '99: Proceedings of the Third Symposium on Operating Systems Design and Implementation SE - OSDI '99 (pp. 173–186). https://doi.org/doi: 10.1145/4221.214134

[4] Dinesh Kumar K et..al: " Educational Certificate Verification System Using Blockchain", International Journal of Scientific & Technology Research Volume-9, Issue 03 March, 2020.

[5] Elli Androulaki et..al, "Hyperledger Fabric: A Distributed Operating System for

[6] Permissioned Blockchains" Artem Barger, Vita Bortnikov, IBM, 17 Apr 2018

[7] F. Angiulli, F. Fassetti, A. F. B, A. Piccolo, and D. Sacc, "Information Systems in the Big Data Era," vol. 317, pp. 16–23, 2018.

[8] Jiin-Chiou Cheng et..al, "Blockchain and Smart Contract for Digital Certificate",Department of Computer Science and Information Engineering, Southern Taiwan University of Science and Technology, Tainan, Taiwan.

[9] Khuat Thanh Son et..al:, "Application of Blockchain Technology to Guarantee the Integrity and Transparency of Documents", IJCSNS International Journal of Computer Science and Network Security, VOL.18 No.12, December 2018.

[10] K. Ikeda, Security and Privacy of Blockchain and Quantum Computation, 1st ed., vol. 111. Elsevier Inc., 2018

[11] Lu, Q., & Xu, X. (2017). Adaptable blockchain-based systems: A case study for product traceability. IEEE Software, 34(6), 21–27. https://doi.org/10.1109/MS.2017.4121227

[12] Nitin Kumavat et..al: "Certificate Verification System using Blockchain", International Journal for Research in Applied Science & Engineering Technology (IJRASET), Volume 7 Issue IV, Apr 2019.

[13] Omar S. Saleh et..al:, " Blockchain based framework for educational certificates verification", Journal of Critical Reviews, Vol 7, Issue 3, 2020

[14] Shanmuga Priya R and Swetha N, "Online Certificate Validation Using Blockchain", Department of Computer Science and Engineering, Prathyusha Engineering College, Thiruvallur,TamilNadu.

[15] Sousa, J., Bessani, A., & Vukolic, M. (2018). A byzantine fault-tolerant ordering service for the hyperledger fabric blockchain platform. Proceedings – 48th Annual IEEE/IFIP International Conference on Dependable Systems and Networks, DSN 2018 (pp. 51–58). https://doi.org/10.1109/DSN.2018.00018

[16] S.Sunitha kumari and D.Saveetha, "Blockchain and Smart Contract for Digital Document Verification", International Journal of Engineering & Technology, 7(4.6)(2018).

[17] T. Keerthana et..al: "Integration of Digital Certificate Blockchain and Overall Behavioural Analysis using QR and Smart Contract", International Journal of Research in Engineering, Science and Management Volume-2, Issue-3, March-2019.

[18] U. Jamsrandorj, "Decentralized Access Control Using Blockchain (Thesis)," no. August, 2017.

[19] Xu, Y., Ren, J., Wang, G., Zhang, C., Yang, J., & Zhang, Y. (2019). A blockchain-based non-repudiation network computing service scheme for industrial IoT. IEEE Transactions on Industrial Informatics, https://doi.org/10.1109/tii.2019.2897133

[20] Z. Qian and Z. Bi, "Decentralizing Privacy: Using Blockchain to Protect Personal Data."

[21] Zheng, Z., Xie, S., Dai, H., Chen, X., & Wang, H. (2017). An overview of blockchain technology: Architecture, consensus, and future trends. Proceedings – 2017 IEEE 6th International Congress on Big Data, BigData Congress 2017 (pp. 557–564). https://doi.org/10.1109/BigDataCongress.2017.85

[22] https://www.blockchain-council.org/blockchain/document-verification-system-using-blockchain/

[23] https://blockgeeks.com/guides/what-is-blockchain-technology/