Multidisciplinary Review Journal

Journal of Critical Reviews

ISSN- 2394-5125 Vol 7, Issue 3, 2020

Review Article

BLOCKCHAIN BASED FRAMEWORK FOR EDUCATIONAL CERTIFICATES VERIFICATION

OMAR S. SALEH[1], OSMAN GHAZALI[2], MUHAMMAD EHSAN RANA[3]

[1]Studies, Planning and Follow-up Directorate, Ministry of Higher Education and Scientific Research, Baghdad, Iraq.
School of Computing, University Utara Malaysia, Kedah, Malaysia. omer.saad10@gmail.com
[2]School of Computing, University Utara Malaysia, Kedah, Malaysia. osman@uum.edu.my
[3]Asia Pacific University of Technology and Innovation (APU), Technology Park Malaysia (TPM), Kuala Lumpur, Malaysia.
muhd_ehsanrana@apu.edu.my

Received: 14.11.2019 *Revised: 16.12.2019* *Accepted: 18.01.2020*

Abstract
Document verification is a complex domain that involves various challenging and tedious processes to authenticate. Moreover various types of documents for instance banking documents, government documents, transaction documents, educational certificates etc. might involve customized verification and authentication practices. The content for each type vary significantly, hence requires to be dealt in a distinct manner. For students, educational certificates are the most important documents issued by their universities. However, as the issuing process is not that transparent and verifiable, fake certificates can be easily created. A skilfully generated fake certificate is always hard to detect and can be treated as the original. With the increase of forged documents, credibility of both the document holder and the issuing authority is jeopardized. Blockchain technology has recently emerged as a potential mean for authenticating the document verification process and a significant tool to combat document fraud and misuse. This research aimed to enhance the document verification process using blockchain technology. In this research, authors have identified the security themes required for document verification in the blockchain. This research also identifies the gaps and loopholes in the current blockchain based educational certificate verification solutions. At the end, a blockchain based framework for verifying educational certificates focusing on themes including authentication, authorization, confidentiality, privacy and ownership is proposed using the Hyperledger Fabric Framework.

Keywords: Authentication, Blockchain Technology, Confidentiality, Educational Certificate Verification, Privacy.

DOI: http://dx.doi.org/10.31838/jcr.07.03.13

INTRODUCTION

According to [1], academic certificates are highly esteemed as they serve as an indicator of the human capital of their bearers. Human capital refers to the skills, competencies, knowledge and aptitudes achieved through education [2]. Academic qualifications are particularly important in employment situations as they serve as a guarantee of not just the knowledge, expertise and skills of the holders but also of their abilities, reliability and dedication [3]. From the perspective of the bearers, [4] found a positive correlation between educational attainment levels and better employment prospects and economic security. [5] pointed out that academic qualifications are deemed to be genuine when they are conferred by a university that is legally authorized to award such certificates.

Because they are so valuable, people often lie about their academic qualifications by producing fake certificates. [6] mentioned that in the United States there are currently 2 million fake degree certificates in circulation and 300 unauthorized universities operating. [7] indicated that the United Sates has the highest number of fake institutions in the world followed by the United Kingdom which has about 270 fake institutes. Healy (2015) found that up to 35% of candidates in Australia falsified their academic credentials for the sake of employment. [8] observed that most candidates lie at least about some part of their educational credentials and experience. [9] mentioned that academic certificate fraud costs employers about $ 600 billion every year.

There are five (5) different sources of fake academic certificates. These include 'Degree Mills' where bogus qualifications are generated and sold to clients[10], 'Fabricated Documents' that represent a fictitious degree or institute, 'Modified Documents' that are alterations in legitimate documents such as changes in enrollment / graduation dates, grades, course content, date of birth, specialization etc, 'In-House Produced' which are fake documents fabricated by the employees of legitimate institutions and printed on authentic paper and bearing the seals, stamps and signatures of the institution and 'Translations' or documents inaccurately translated to match requirements in a receiving country. [7] also indicated academic certificates issued by institutions that are not registered / unaccredited / lack government authority to grant such credentials / make unsubstantiated claims about recognition and accreditations are fake. The implication arising from the above findings is that the problem of fake certifications has assumed serious and alarming proportions and needs to be urgently tackled. Blockchain technology is recently introduced to improve the document verification process and combats the document fraud and mise use. Blockchain technology simply can be defined as a distributed database, that chronologically stores a chain of data packed into sealed blocks [11]. However, the scope of this research is to determine a framework for implementing security requirements in educational certificate verification in the blockchain. The framework is intended to avoid the problem of fake certificates or fraud in educational certificates.

BLOCKCHAIN TECHNOLOGY: FEATURES AND CHARACTERISTICS

Blockchain technology is not only a single technique, it is a combination of many techniques such as cryptography, mathematics, algorithms and distributed consensus algorithms [12], [13], [14]. A blockchain is composed of six key elements [15] as follows:

Decentralized. Blockchain doesn't have to rely on a single centralized node any more like a master node, each node can record, store and update the ledger, and together they form the blockchain.

Transparent. The block's data recorded by each node and distributed among other connected nodes is visible to each node which creates transparency among connected nodes.

Anonymous. In order to make the transactions anonymous, data is hashed before sharing by using a secure algorithm.

Consensus Base. Since node are publicly connected on blockchain and changes can only happen when majority of nodes accept the change, all nodes are eligible to transfer and update data safely providing a consensus base to the system.

Immutable. All records are permanently kept which cannot be altered unless someone can take control of more than 51% nodes simultaneously.

Open Source. Most Blockchain systems are open to everyone, allowing participants to modify the code and technology in ways that best suits their needs. However this does not mean that anyone can modify a running blockchain solution. Making any modification to a running solution means all connected nodes are publicly accepting the change.

Blockchain Structure

Each block in the blockchain contains five elements which are: 1) the main data; 2) the hash of the pervious block; 3) the hash of the current block; 4) the timestamp and 5) other information [15]

Main Data. The data depends on the type of transaction; it is generally a transfer between nodes A and B however it can be of any type like money transfer or record transfer.

Hash of the Previous Block. When a transaction is executed, its hash is generated and broadcasted to the network. There are several hashing algorithms in use but the most dominant is the Merkle Tree. This algorithm allows easy hash and easy de-hash options which is why Merkle Trees is a common choice.

Hash of the Current Block. The final hash value is recorded in block header (hash of current block), while the content itself is stored in the body of the block. Blocks are generally bound to a size hence allowing a limited number of transactions per block.

Timestamp. The time the block was generated.

Nonce and Other Information. Like signature of the block, Nonce value, or other data that the user defines.

The data structure of a typical blockchain application is indicated in Fig. 1.

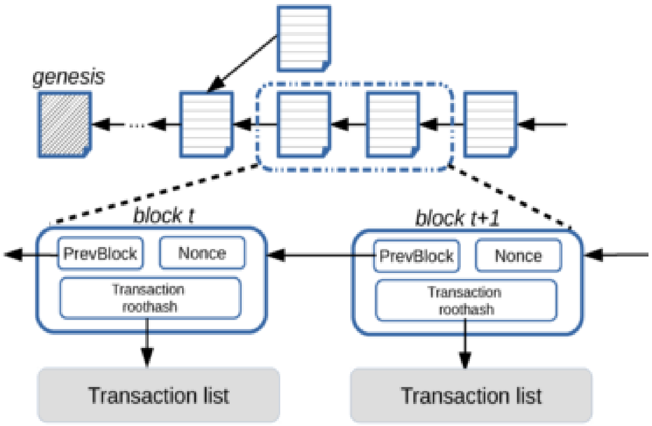


Figure 1: Blockchain Data Structure

Blockchain Types

Blockchain technologies are divided into three types: 1) Public Blockchain (permissionless); 2) Consortium Blockchains and 3) Private Blockchain (permissioned) [15],[16]. In public blockchain, everyone can check the transaction and verify it as well and participate in the process of getting consensus. One of the most well-known examples of public blockchain is Bitcoin [14]. In consortium blockchain, there is a possibility to identify the node that has the authority in advance. Hyperledger is one of examples of consortium blockchain[17]. In private blockchain, not every node can participate this blockchain, the nodes will have restricted in term of data access. Every blockchain network has different rules regarding what kind of assets it trades, and under which conditions trading takes place. These rules are encoded into its software. The node in the blockchain network is every device running the blockchain software and connected to the network[18],[19].

SECURITY THEMES FOR EDUCATIONAL CERTIFICATES IN BLOCKCHAIN

Educational certificates on a blockchain must fulfill certain essential themes namely,

Authentication: The blockchain must authenticate users. In this case, the users are students, universities, institutes, employers, etc. Each user in a blockchain ledger will be verified for accessing the certificate stored on it. Authentication for users is through a username and password, or some system can also have multiple authentication systems such as biometric, etc. for example, the employer requiring to verify the certificate must first join the blockchain and the recipient will authorize the employer to view the certificate and verify it [20].

Authorization: Provides the permissions for the users to perform transactions in the blockchain. For example, the student has the authority to share his/her certificate with an employer. The issuer will authorize the student to have full control on the certificate after it is issued. All these actions and functions must be authorized in the system [21].

Confidentiality: The requirements for confidentiality include the student's private information which can be maintained by the academic institute along with the student. Here the student has control to divulge information as appropriate to third parties (employers) for verification [22].

Ownership: The ownership of a digital certificate rests on the users in the blockchain ledger. In the case of an educational certificate, the recipient has full ownership of the certificate. Here, the use of public and private keys are important and shared with all the users owning a blockchain [23].

Privacy: Public keys are maintained anonymously. Creation of hash functions is required along with the use of cryptographic algorithms [24].

The above themes are important to ensure the certificate is not fake. Employers can verify the credentials claimed by the student on the blockchain.

RELATED WORKS

Knowledge Media Institute (KMI) of the Open University UK (OU) has initiated the use of badges, certificate and web reputation using blockchain as a trusted ledger. KMI is leveraging the use of Ethereum for turning badges into smart contracts and have developed a prototype for issuing micro-credentials on the blockchain. KMI activities are focused on creating blockchain for use in UK higher education qualifications and to spearhead blockchain projects in higher education. KMI is partnering with other institutes such as the University of Ghent, University of Texas and others to collaborate on blockchain activities. However, this initiative by OU does not focus on the end-user and is not available with the aim to fulfill third-parties, employers, etc. KMI is focusing on the application layer and in principle, users can control their data and wallet of private keys. However, for the average user, there could be complexities in understanding how the blockchain works and would require the support of a technical intermediary [25]. Despite the short-comings on their initiatives, OU believes blockchain will provide significant opportunities for educational institutes across the UK. Privacy of users in their model is ensured using end-to-end encryption, however, risks exist because private data is released on a public blockchain. In this scenario, there is no mechanism to protect the recipient's privacy and ownership.

Universit of Nicosia (UNIC) is using the Bitcoin blockchain for many activities such as accepting bitcoin for tuition for any degree program, issuing academic certificates on Bitcoin blockchain, and so on [26]. Educational certificates in the blockchain initiated by the University of Nicosia is intended to eliminate fraud and also overcome fraud in payments from international students. The main goal is to overcome the problems of tampering with the numbers of student cohorts. UNIC has commenced issuing all diplomas using the blockchain since 2017 and provides software tools through which users can confirm the authenticity of the certificate. The current open source standards are used in their user-facing systems and UNIC is a part of the Blockcerts consortium. The hash algorithm namely, SHA-256 is used for sharing certificates as a PDF file other entity. SHA-256 is used for its ability to create a hash from the certificate, but the reverse is not possible. The authenticity of the certificate is preserved by searching the certificate's SHA-256 within the index document. If the code is matched, the certificate is authentic. Despite these features to preserve the privacy, ownership, and integrity of certificate, improvements are needed to publicly validate the hash, this is one requirement to allow employers to view the certificate. In addition, the recipient may not be able to authorize a potential employer to verify the certificate using the hash [27].

MIT Media lab uses Blockcerts to issue digital certificates to groups of students to provide more control to recipients over certificates earned by them. In this initiative, the recipients may not depend on a third party intermediary to store, verify and validate credentials. MIT's certification architecture works on the process of the issuer signing a digital certificate and stores its hash within the blockchain transaction. The output of this transaction is assigned to the recipient. In this initiative, there was the issue of ownership because MIT faced the issue of rolling out certificate based on user-created key-pairs for their graduation and workshop participation certificates. In addition, a high level of trust is required in this system. Privacy is another important aspect because when everyone can access the data, and certificates are useful only when it belongs to one recipient. The issue faced here is that the recipient could share the certificate with one employer, and at the same time he/she could not hide the certificate with another employer as required. The hashing technique is used, but here again when an employer needs to verify the validity of a certificate, along with disclosing both the certificate and the hash of the certificate located in the blockchain. In this case, the theme of privacy is not completely fulfilled.

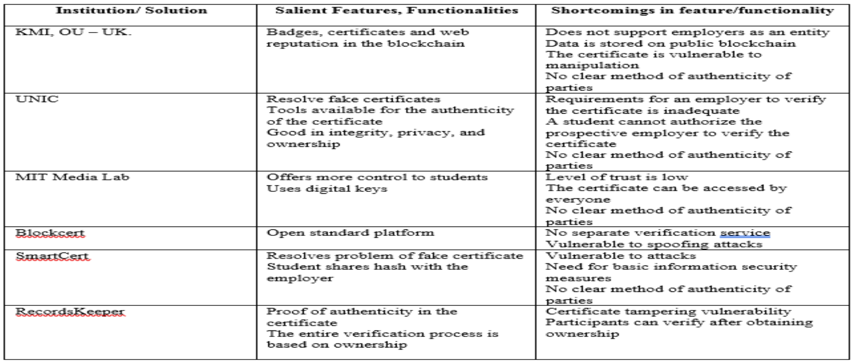
In another initiative, an open standard named Blockcerts is used to build apps to verify blockchain based academic credentials, professional certificates, and so on. Blockcerts is based on the self-sovereign identity of all the participants by providing components to create, issue, view and verify certificates in the blockchain. The certificates stored in the blockchain are tamper proof, but Blockcerts does not have a separate verification service for verifying its validity. Hence, there is a possibility to spoof the certificate. In addition, the aspects of privacy and security is still a concern because there is no registration process in the system and any issuer can issue certificates to recipients who can, in turn, provide any bitcoin address. Ownership of a certificate cannot be demonstrated unless the issuer and recipient provide public addresses owned by them. Blockcerts does not certify the mapping of public keys to individuals or organizations (Blockcerts).

SmartCert is another blockchain based digital credentials verification platform. SmartCert is developed to establish the authenticity of academic credentials on a blockchain and to overcome the problem of fake certificates. SmartCert makes use of cryptographic signing of educational certificates to provide transparency in the case of recruitment. The student will share the hash with the prospective employer to verify the certificate. However, in the case of hash or digitally signed certificate, it can be difficult for a legitimate user to gain access because the computer accessing this data can be attacked by an intruder. Another issue in this application is that, cryptography does not ensure data security, and therefore the fundamental security measures must be implemented to guard against threats. At the same time, cryptographically secured certificates in SmartCert does not allow the certificates to be faked easily [28].

Records Keeper is another blockchain based solution to verify academic certificates. With RecordsKeeper, educational institutes can issue certificates and provide a receipt to the user which can be shared with a third party to prove the certificate is authentic. The receipt obtained from the student will be used by the third party to verify the certificate authenticity in the RecordKeeper ledger. There are not many complications in this mechanism, but the parties interested to view the certificate in the Record Keeper blockchain must have ownership rights. This amounts to a transfer of ownership to the third-party which may lead to tampering. This may work well on a private blockchain to ensure the security of the certificate [29].

Table 1 provides details of existing solutions and highlights the major short-comings in each solution.

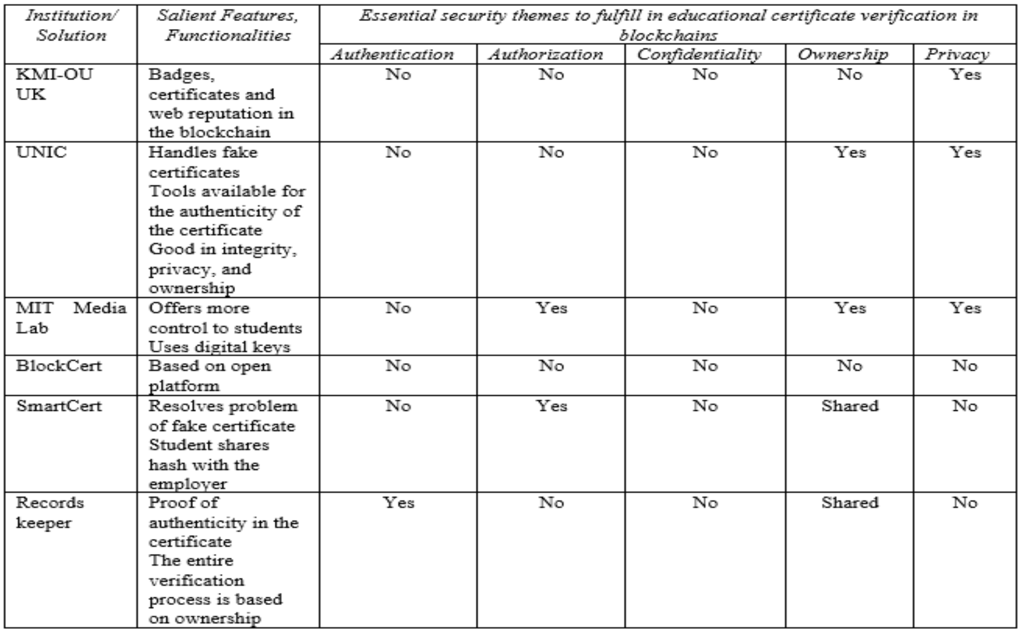
Table 1: Existing Solutions and their Short-comings



Institution/ Solution	Salient Features, Functionalities	Shortcomings in feature/functionality
KMI, OU – UK.	Badges, certificates 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 certificates Tools available for the authenticity of the certificate Good in integrity, privacy, and ownership	Requirements 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	Offers more control to students Uses digital keys	Level of trust is low The certificate can be accessed by everyone No clear method of authenticity of parties
Blockcert	Open standard platform	No separate verification service Vulnerable to spoofing attacks
SmartCert	Resolves problem of fake certificate Student shares hash with the employer	Vulnerable to attacks Need for basic information security measures No clear method of authenticity of parties
RecordsKeeper	Proof of authenticity in the certificate The entire verification process is based on ownership	Certificate tampering vulnerability Participants can verify after obtaining ownership

Based on reviews of online solutions (Table 1) and in the absence of technical aspects of reviewed solutions, a detailed analysis of gaps or drawbacks based on technical functionalities could not be determined. However, the drawbacks of each reviewed solution were found and recorded based on security themes discussed earlier. The existing solutions mapped with the requirements themes and provided in table 2.

Table 2: Educational Certification Solutions Maps with Requirements Themes



Institution/ Solution	*Salient Features, Functionalities*	*Essential security themes to fulfill in educational certificate verification in blockchains*				
		Authentication	*Authorization*	*Confidentiality*	*Ownership*	*Privacy*
KMI-OU UK	Badges, certificates and web reputation in the blockchain	No	No	No	No	Yes
UNIC	Handles fake certificates Tools available for the authenticity of the certificate Good in integrity, privacy, and ownership	No	No	No	Yes	Yes
MIT Media Lab	Offers more control to students Uses digital keys	No	Yes	No	Yes	Yes
BlockCert	Based on open platform	No	No	No	No	No
SmartCert	Resolves problem of fake certificate Student shares hash with the employer	No	Yes	No	Shared	No
Records keeper	Proof of authenticity in the certificate The entire verification process is based on ownership	Yes	No	No	Shared	No

From Table 2, it may be noted that the security themes were identified for each reviewed solution and have been marked as either 'Yes' or 'No'. All 'Yes' at different cells indicate the security theme is addressed, and 'No' refers to the theme is not addressed or it is a gap. From the table, it may be found that,

The authentication theme is addressed by the solution named RecordsKeeper. The RecordsKeeper blockchain solution provides educational certificate verification through their proprietary API. The authenticity and integrity are verified for the published records on the blockchain. The solution features are available as a public blockchain (RecordsKeeper, 2018). In the case of MIT solution, the authentication of the education certificate is handled by the use of public/private key pairs. The key pairs are used to authenticate both the student and the university. However, the concept was not implemented by MIT because students can create their own key pairs and share them as a public key with the requesting user (employer). The MIT solution did not implement this method of key sharing because it is practically prohibitive due to the technical sophistication required to make this method more effective [30].

The other solutions presented in table 2 did not highlight the theme of authentication in their offers. While the solution provides details related to the working of the system, technical details are not available that explain the mechanism of authentication on their online website. Hence, authentication is understood as a gap in existing solutions.

In the case of authorization, MIT Media Lab and SmartCerts provide authorization in their certificate verification solution, but MIT solution is based on Blockcert which is an open platform. Likewise, SmartCert claim they provide authorization in their solutions website, however, technical details are not available. The other solutions do not provide many details on authorization theme.

The confidentiality theme is not ensured by the solutions and found during reviews. The ownership theme is addressed by MIT and UNIC solutions. The solutions namely, Smartcert and Recordskeeper have shared ownership. The 'Shared' ownership here refers to the ownership of the educational certificate lies with both, the student and the university. The privacy aspect is ensured in KMI OU UK and MIT solutions. The other reviewed solutions do not provide much information on this theme. Hence, the proposed framework in the next section will close the mentioned gaps.

THE PROPOSED FRAMEWORK

It may be noted from the previous section that in some solution cases reviews indicate certain themes of security are addressed and other themes are not addressed. However, it was observed that all the solutions provide inadequate security in terms of addressing all the five themes discussed in research. Therefore, it is found that in the reviewed solution cases the certificate is open to vulnerability and data security is inadequate. Hence, from the online solution reviews, the gaps found in the existing certificate verification solutions are authentication, authorization, confidentiality, privacy, and ownership. Because of that, this research aimed to close the mentioned gaps by proposing a blockchain based framework for the academic certificates verification focusing on authentication, authorization, confidentiality, privacy, and ownership themes. The proposed framework showed in Fig (2) is proposed to be build based on Hyperledger Fabric framework due its benefits that will be discussed in detail in next section.

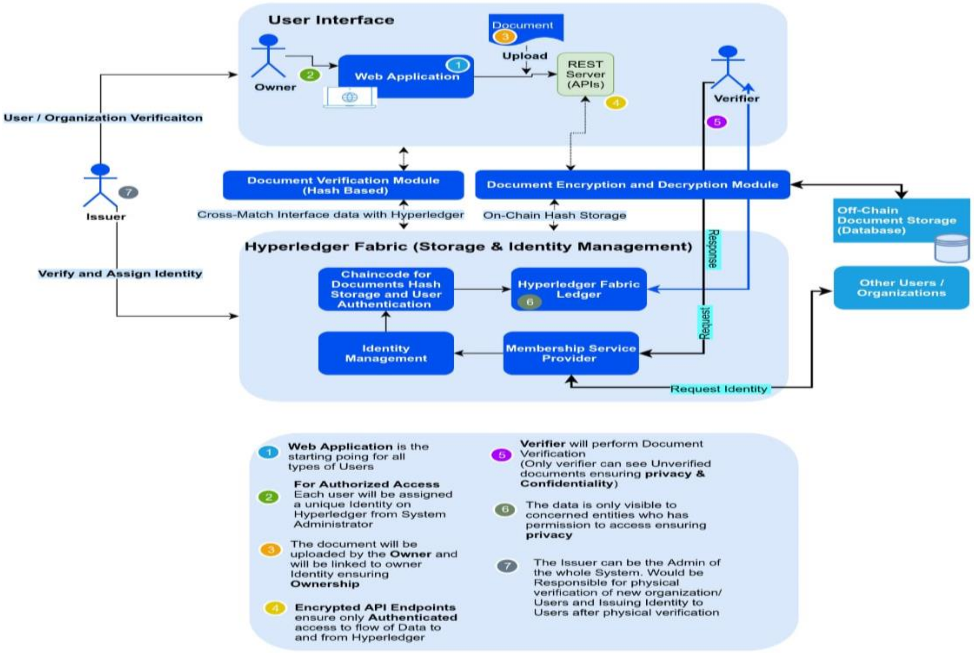

User Interface
Document
3
Upload
Owner
2
Web Application
1
REST Server (APIs)
4
Verifier
5
User / Organization Verificaiton
Issuer
7
Document Verification Module (Hash Based)
Document Encryption and Decryption Module
Cross-Match Interface data with Hyperledger
On-Chain Hash Storage
Off-Chain Document Storage (Database)
Hyperledger Fabric (Storage & Identity Management)
Response
Verify and Assign Identity
Chaincode for Documents Hash Storage and User Authentication
Hyperledger Fabric Ledger
6
Other Users / Organizations
Request
Identity Management
Membership Service Provider
Request Identity
1 Web Application is the starting poing for all types of Users
2 For Authorized Access Each user will be assigned a unique Identity on Hyperledger from System Administrator
3 The document will be uploaded by the Owner and will be linked to owner Identity ensuring Ownership
4 Encrypted API Endpoints ensure only Authenticated access to flow of Data to and from Hyperledger
5 Verifier will perform Document Verification (Only verifier can see Unverified documents ensuring privacy & Confidentiality)
6 The data is only visible to concerned entities who has permission to access ensuring privacy
7 The Issuer can be the Admin of the whole System. Would be Responsible for physical verification of new organization/ Users and Issuing Identity to Users after physical verification

Figure 2: The Proposed Framework

There are various blockchain platforms available, however the top three dominant blockchain platforms include Bitcoin, Ethereum and Hyperledger [31]. Ethereum and Bitcoin are permission less blockchains, where anyone can join the network as well as write and read transactions. On the other hand, Hyperledger is a permissioned blockchain, where only predefined participants can join a network, view and make transactions.

Based on the requirements of educational certificates in the blockchain which are clearly mentioned in Section 3, Hyperledger would be the most suitable platform in our case due to its inherent privacy and role based access mechanism for accessing the documents. Hyperledger offers some key advantages over other blockchains as specified by [32],[33]:

- Hyperledger is a private blockchain hence records are not in public domain.
- In Hyperledger, if someone wish to tamper with the document, we will be notified immediately as it will create a new hash.
- Access levels can be customized as per requirement as it is a role based blockchain.
- As Hyperledger is not coin (“token”) based blockchain, the environment is less complex to develop.
- Unlike Bitcoin or Ethereum blockchain, Hyperledger does not require transferring a virtual currency to publish a transaction.

Hyperledger comes with several frameworks such as (Iroha, Sawtooth, Fabric, Indy, and Burrow), however Hyperledger fabric (HLF) has been selected to be utilized in our work due its features that would be suiting our needs. HLF comprises six core components which are 1) Membership Service Provider (MSP), 2) Chaincode , 3) Peers , 4) Channels, 5) Shared Ledger, and 6) Gossip Network Protocol [17],[32],[34]. Fig (3) shows the transaction flow between the components in the Hyperledger Fabric framework which is adopted from [35].

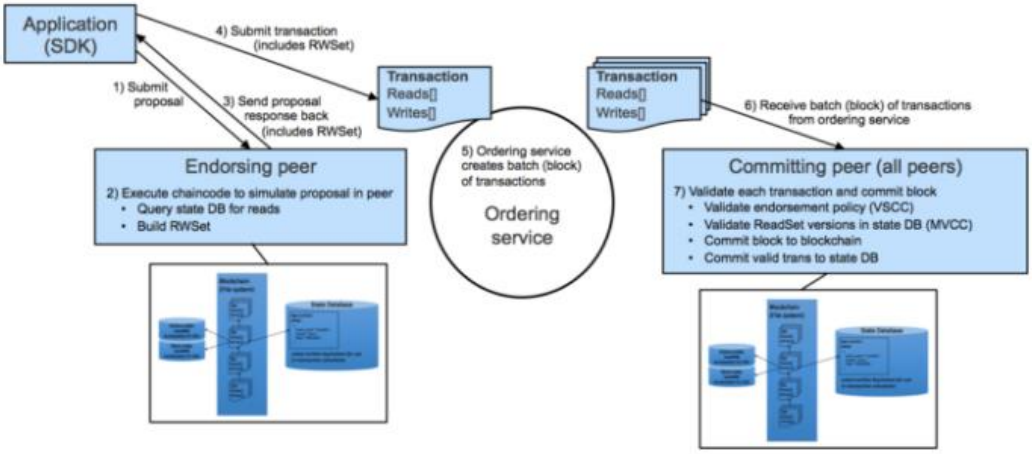

Application (SDK)
4) Submit transaction (includes RWSet)
1) Submit proposal
3) Send proposal response back (includes RWSet)
Transaction
Reads[]
Writes[]
Transaction
Reads[]
Writes[]
6) Receive batch (block) of transactions from ordering service
Endorsing peer
2) Execute chaincode to simulate proposal in peer
Query state DB for reads
Build RWSet
5) Ordering service creates batch (block) of transactions
Ordering service
Committing peer (all peers)
7) Validate each transaction and commit block
Validate endorsement policy (VSCC)
Validate ReadSet versions in state DB (MVCC)
Commit block to blockchain
Commit valid trans to state DB

Figure 3: Transaction flow between the components in the Hyperledger Fabric framework adopted from [35]

BENEFITS OF THE HYPERLEDGER DISTRIBUTED LEDGER

The architecture that we would be proposing leverages the permissioned network features of the Hyperledger Distributed Ledger Technology (DLT) to provide the following benefits [17],[32],[34]:

1. Transparent Network: The proposed architecture has the ability to create private channels between certain actors to enable certain information to flow freely and transparently between them. For example, a channel will include the owner, the issuer, and the verifier to enable a transparent flow of data between them pertaining to a particular product.
2. Permissioned Access: The documents uploaded by the owner can be viewed on demand, for fixed durations of time, for example, 10 hours.
3. Uniquely Identifiable Digital Certificate: The digital certificate will be embedded with a uniquely identifiable hash of the <owner> <issuer> <verifier> which is impossible to tamper without changing the hash itself. The changed hash will not match with the original hash present on the Hyperledger and refuse to accept the verified document.
4. Grievance Redressal: All disputes arising on account of the information can be redressed by simply matching the hash of the digital data present on the blockchain against the hash presented by the owner as an embedded entity within the information provided by the owner.

CONCLUSION

This research identified and discussed the security themes required for educational certificates verification in the blockchain. In addition to that, a blockchain-based framework for educational certificate verification focusing on specific themes is proposed based on Hyperledger Fabric Framework. The security themes required for educational certificates verification in the blockchain are authentication, authorization, privacy, confidentiality and ownership. Authentication will prove to the employer that the student is trustful and will be able to physically verify the educational claims made by the student. Authorization will ensure that the student has necessary permissions to perform tasks that he/she is entitled to. Privacy and confidentiality will prove that both identity and information exists in the certificate are protected. For future work, the proposed framework will be implemented and adopted in selected educational institutions.

ACKNOWLEDGMENTS

Authors would like to sincerely thank Universiti Utara Malaysia, Asia Pacific University of Technology and Innovation (APU) and Ministry of Higher Education, Iraq for supporting this research.

REFERENCES

1. T. Healy, S. Cote, J. Helliwell, and S. Field, “The Well-Being of Nations - The Role of Human and Social Capital,” *Oecd*, p. 118, 2002.
2. S. Baum, J. Ma, and K. Payea, “Education Pays 2013,” *Coll. Board*, pp. 1–48, 2013.
3. S. Marginson, *Dynamics of national and global competition in higher education*, vol. 52, no. 1. 2006.
4. S. Baum, “Higher Education Earning Premium Value , Variation , and Trends,” *Urban Inst.*, no. February, pp. 1–12, 2014.
5. M.G. Moore, “A Sad Reminder That Diploma Mills Are Still With Us,” *Am. J. Distance Educ.*, vol. 23, no. June, pp. 175–178--, 2009.
6. G. Grolleau, T. Lakhal, and N. Mzoughi, “An introduction to the Economics of Fake Degrees,” *J. Econ. Issues*, vol. 42, no. 3, pp. 673–693, 2008.
7. E. Ben Cohen and R. Winch, “Diploma and accreditation mills: New trends in credential abuse,” 2011.
8. E. Share, M. Memorable, and L. They, “Fifty-eight Percent of Employers Have Caught a Lie on a Resume,” 2014. .
9. E. Chiyevo Garwe, “Qualification, Award and Recognition Fraud in Higher Education in Zimbabwe,” *J. Stud. Educ.*, vol. 5, no. 2, pp. 119–135, 2015.
10. *Corrupt schools, corrupt universities: What can be done?* .
11. A. Grech and A. F. Camilleri, *Blockchain in Education*. 2017.
12. J.A. Garay, “The Bitcoin Backbone Protocol : Analysis and Applications The Bitcoin Backbone Protocol : Analysis and Applications,” no. June 2017, pp. 1–44, 2015.
13. A. Gervais, G.O. Karame, V. Capkun, and S. Capkun, “Is Bitcoin a Decentralized Currency?,” *IEEE Secur. Priv.*, vol. 12, no. 3, pp. 54–60, 2014.
14. S. Nakamoto, “Bitcoin: A Peer-to-Peer Electronic Cash System,” *Www.Bitcoin.Org*, p. 9, 2008.
15. I.C. Lin and T.C. Liao, “A Survey of Blockchain Security Issues and Challenges,” *Int. J. Netw. Secur.*, vol. 1919, no. 55, pp. 653–659, 2017.
16. D.T.T. Anh, M. Zhang, B.C. Ooi, and G. Chen, “Untangling Blockchain: A Data Processing View of Blockchain Systems,” *IEEE Trans. Knowl. Data Eng.*, vol. 4347, no. c, pp. 1–20, 2018.
17. Moses Sam Paul, “Hyperledger — Chapter 1 | Blockchain Foundation – The Startup – Medium,” *Medium.Com*, pp. 1–24, 2018.
18. K. Kuvshinov, I. Nikiforov, J. Mostovoy, and D. Mukhutdinov, “Disciplina : Blockchain for Education,” pp. 1–17, 2018.
19. M. Turkanovic, M. Holbl, K. Kosic, M. Hericko, and A. Kamisalic, “EduCTX: A blockchain-based higher education credit platform,” *IEEE Access*, pp. 1–20, 2018.
20. B. Xia, D. Ji, and G. Yao, “Advances in Information and Computer Security,” vol. 7038, no. 2016, pp. 56–66, 2011.
21. 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.
22. U. Jamsrandorj, “Decentralized Access Control Using Blockchain (Thesis),” no. August, 2017.
23. Z. Qian and Z. Bi, “Decentralizing Privacy: Using Blockchain to Protect Personal Data.”
24. K. Ikeda, *Security and Privacy of Blockchain and Quantum Computation*, 1st ed., vol. 111. Elsevier Inc., 2018.
25. J. Domingue, “Blockchains as a Component of the Next Generation Internet,” 2017.
26. “The Global Universities embarcing cryptocurrency.pdf.” .
27. C.F. Bond, F. Amati, and G. Blousson, “Blockchain , academic verification use case,” 2015.
28. R.G. and M.K.S. Sharma, P. Pathak, “Blockkchain imperative for educational certificates,” 2017.
29. “Upload and verify academic certifications over RecordsKeeper,” 2018.
30. MIT Media Lab, “What we learned from designing an academic certificates system on the blockchain,” *Medium*, no. December, p. 2016, 2016.
31. T. Nguyen, “Gradubique : An Academic Transcript Database Using,” 2018.
32. M.S. Paul, “Hyperledger — Chapter 2 | Hyperledger Frameworks & Modules,” *The Startup*, pp. 1–12, 2018.
33. Hyperledger Architecture Working Group, “Hyperledger Architecture , Volume 1,” *Hyperledger.org*, vol. 1, p. 15, 2017.
34. E. Androulaki *et al.*, “Hyperledger Fabric: A Distributed Operating System for Permissioned Blockchains,” no. 1, 2018.
35. C.B. Invoices, “Hyperledger Fabric in practice . Main components and running them locally,” pp. 1–6, 2019.
36. Shrivastava, S., Jeyanthi, P.M. and Singh, S., 2020. Failure prediction of Indian Banks using SMOTE, Lasso regression, bagging and boosting. Cogent Economics & Finance, 8(1), p.1729569.