ISSN 2303-4521
Periodicals of Engineering and Natural Sciences *Original Research*
Vol. 10, No. 2 April 2022, pp.207-218

Blockchain-based student certificate management and system sharing using hyperledger fabric platform

Rana F. Ghani [1], Asia A. Salman [2], Abdullah B. Khudhair [3], Laith Aljobouri [4]

[1]Department of Computer Science, University of Technology-Iraq, Iraq
[2]Department of Computer Science, University of Technology-Iraq, Iraq
[3]Zain Iraq Mobile, Telecommunication Company, Iraq
[4]School of Design and Informatics, Abertay University, United Kingdom

ABSTRACT

One of the major capabilities of blockchain technology is the sharing of data in verifiable ways without losing control of information possession. Issuing and verifying student certifications for higher study applications or job recruitment require many steps that take days to complete and are considered time-consuming. Most universities around the world use centralized systems to control the entire procedure when a graduate applies for a job or postgraduate studies. Applying blockchain technology to certificate verification protocols through a comprehensive architecture provides authenticity and reduces time significantly. In this paper, a framework has been proposed to issue student certifications locally in addition to sharing them across the internet while maintaining control and ownership of the certifications. This framework leverages the advantages of blockchain technology to electronic certification sharing and verification. Applying the proposed blockchain-based certification system in universities will provide low latency for issuing, sharing, and verification of these certifications. The paper presents the proposed blockchain-based framework for e-certification sharing and an evaluation of the framework, which consists of measuring the average time to issue a certificate and transaction latency time.

Keywords: Computer Network, Distributed Systems, Blockchain, Hyperledger Fabric, Data Sharing, Student Certification

Corresponding Author:

Rana Fareed Ghani
Department of Computer Science
University of Technology- Iraq
Baghdad- Iraq
E-mail: 110016@uotechnology.edu.iq

1. Introduction

Because we live in a network-centric world, the internet has become intrinsic part of our daily routines. Computer networks have a tremendous impact on all the details of our lives, such as communications, learning systems, businesses, and economies. One of the main roles of the internet is to facilitate the sharing of data. We can use email, FTP, or social networks to share data. For many applications, a flexible mechanism for data sharing is needed. This mechanism should maximize the acquired knowledge from the data and ensure transparent access to the user's data. Transparent access to data means being aware of accessed data, the parties who access them, the purpose and the conditions to access them [1]. Advancements in technology have resulted in the emergence of various computational technologies to create safe data-sharing models, such as cloud computing services and email. Although these technologies can provide solutions for huge problems, they are sometimes criticized for security and centrality issues. Centralizing the service of storage and management of data makes these data vulnerable to being stolen, misused, or destroyed. Blockchain technology is considered a promising solution for data-sharing problems due to its characteristics of decentralization, immutability, scalability, trustlessness, and controlled privacy. In addition to these characteristics, blockchain technology makes it possible to share data domestically and/or overseas. This technology became popular because of cryptocurrencies, however it is also used for various applications and services nowadays. Different industries leverage the utilization of blockchain technology for data sharing. For example, blockchain data-sharing systems are widely used in e-governments [2-5], healthcare [6], and the internet of things (IoT) [7, 8]. In the field of education, blockchain is being used for various educational applications. The main benefits of using blockchain to support education include reductions in latency time and the cost of sharing data in a controlled environment [9-11]. The contributions of this paper may be considered as three aspects. First, we have performed a review to analyse the reasons, advantages, drawbacks and future challenges of applying blockchain technology for data sharing. Second, we developed a prototype using the Hyperledger Fabric private blockchain based system for students' certifications and the controlled sharing of the information for the parties who need it. Third, we measured the average time and latency time for the transactions to measure the efficiency of the proposed framework. We also compared the latency time of the current system being used to issue and verify students' certifications at the University of Technology (UOT) in Iraq with the latency time of the proposed system. The paper is organized as follows: Section 2 shows related works, section 3 presents the main concepts of blockchain technology. Smart contract concepts is presented in section 4 and the primary concepts of data sharing is presented in section 5. The design and implementation of the proposed framework are presented in section 6, which will demonstrate the architecture of the proposed system and the algorithms and functions of each part of the system. Section 7 presents the metrics used to test the performance of the system and the results according to these metrics. Finally, Section 8 presents the conclusion of this work.

2. Related works

Several researchers have noticed the potential inherent in blockchain technology regarding the sharing of information in the field of education. The blockchain has three primary features that make it suitable for education applications: decentralization, straightforwardness, and permanence [12]. For instance these features can ensure that the higher education system would never corrupted and allows for public verification of students' records. Furthermore, the information can be shared and protected at the same time , allowing users to employ intellectual efforts and guarantee reputational rewards [13]. In 2019, Li and Han [14] presented their work that demonstrated the use of blockchain for education. Blockchain technology was used to store students' records, and the role of the blockchain was to ensure that data were secure and reliable. In addition, they used smart contracts to share data. The assessment of the work focused on proving that the proposed system was safe and had a low computational cost. For future works, the authors suggested adding functions to support educational record certification for foreign institutions or employers and the recall of educational records. Turkanović et al. [15] created a globally trusted higher education credits platform by taking advantage of blockchain technology. Oliver et al. [16] developed a blockchain-based solution for automatic verification of university degrees using an easy interface. The proposed solution would depend on a key provided to the graduate to manage certification sharing; the student would be responsible for the security of the key. The main target of the proposed solution is to be economically-efficient and sustainable. In 2016, Sharples and Domingue [17] proposed a solution for permanently distributed record of intellectual efforts and academic reputations depending on blockchain technology. They used a private blockchain to store educational records. In their work, they resolved the problem of forgery of certificates by implementing a distributed ledger to store educational records.

3. Blockchain technology concepts

This section presents a generic view of blockchain technology and introduces the main features of a decentralized, trustless and immutable data storage system. The greatest growth in blockchain technology was introduced by Satoshi Nakamoto when it was invented and released by Satoshi Nakamoto in 2008 in a whitepaper titled "Bitcoin: A Peer-to-Peer Electronic Cash System" [18]. Over the last decade, this invention has developed into one of the most effective technologies that resulted in the improvement of various industries, such as finance, healthcare, education, and manufacturing. Blockchain has many technical features that make it a promising technology with a wide spectrum of applications, and it is said to be the solution for many of today's problems. This technology is described as a trustless and fully decentralised peer-to-peer data storage platform that is spread over all the participant nodes. Once information is committed to the blockchain, it becomes immutable. Therefore, a blockchain is defined as a decentralised, distributed, and immutable storage system. Data in the blockchain are structured logically in a sequence of blocks, and the technical features of a blockchain are defined as follows [19, 20].

- Decentralisation: In blockchain technology, trust is distributed across multiple or all nodes and is not reliant on a single entity.

- Immutability: Once data are accepted by a sufficient number of blockchain participants and added to the blockchain, the information is stored permanently and immutably.
- Consensus: It is the process of agreeing on the validity of transactions among a sufficient number of blockchain participants.
- Scalability: When a blockchain system is called scalable, it means that the system can achieve a higher transaction count per second than other existing systems, through modifying consensus mechanisms and/or the size of data blocks.
- Data validity and security: Combining consensus and immutability results in the ability to validate and secure data in blockchain networks.
- Controlled privacy: Privacy depends on the type of blockchain. Data can be visible to all participants or limited to a group of blockchain participants.

3.1. Types of blockchains

To implement a blockchain-based application, the three types of blockchains have to be considered according to the application requirements [21]:

- Public: A public blockchain is fully decentralised and permissionless, that means it is visible to everyone and there is no single owner of it. The consensus process is open to all who wish to participate. An example of a public blockchain is Bitcoin.
- Private: This type of blockchain is owned by a single entity that controls participation in the network of transactions. Therefore, it is also called a permissioned blockchain. In this type of blockchain, there is no need for a consensus algorithm to create blocks.
- Hybrid (consortium): This blockchain is both public and permissioned, which means that it is only public for a specific group of participants.

3.2. Blockchain development environments

Since the invention of blockchain, a collection of various blockchain development tools has been developed. These tools are used to write, verify, test and debug blockchain codes. In this study, Hyperledger was employed to implement the proposed student certification framework. Hyperledger is an open-source community hosted by The Linux Foundation [18]. Hyperledger provides all the potentials of blockchain technology, such as privacy, information sharing, and immutability. Several sub-projects that have different characteristics exist, and they include Hyperledger Fabric (used in this paper to implement the e-certification sharing system), Composer, Cello, Explorer, Burrow Sawtooth, and Caliper [22].

3.3. Hyperledger fabric

Hyperledger Fabric is a framework for implementing various blockchain-based applications. This framework's architecture support container technology to use a smart contract that contains the application rules. The main characteristics of Hyperledger Fabric are [22]: 1) it is a permissioned network, 2) it supports confidential transactions, 3) to participate, one does not need cryptocurrency, and 4) it is programmable. These characteristics establish trust, transparency, and accountability. The fabric consists of different components, as shown in Figure 1. These components are gathered by Hyperledger Fabric in trust domains and controlled by logical entities, and these nodes could be thought of as logical functions [23].

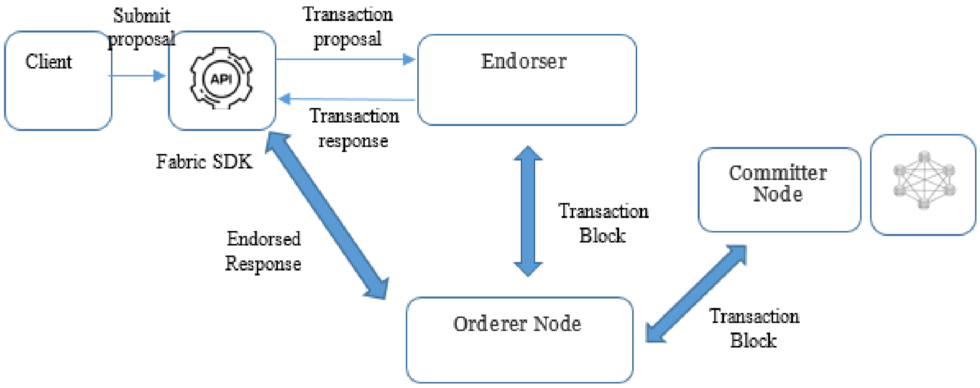

Figure 1. Hyper ledger Fabric components

Figure 1shows the relations between the blockchain nodes. the client submits the proposed transaction through the SDK. All endorsing peers receive this proposal of transaction, check the validity and execute the transaction. The orderer checks the transactions and arranges them in a block. Lastly, this block is sent to all committers who add the new block to their copy of the ledger.

3.4. Chained blocks

Blocks are records where the ledger's data are permanently stored. They can be thought of as pages in a ledger or record book. Once the block is written, it cannot be altered or removed. Blockchain uses linked list of blocks as a data structure to organize transactions. These transactions are stored as a flat file in the block. Typically, a block consists of three parts: Block header which consists of three fields: block number starting from zero and incremented by one for each newly added block, current block hash of all transactions contained in a block using a hash algorithm, previous block hash, data which consist of a list of transactions arranged in an orderly manner or any type of data, depending on the application requirements, and Metadata which contains the time when the block was written, the certificate, the public key, and the signature of the blocked writer. The transaction that organized within a block is consist of: header, signature, proposal, response and endorsement.

4. Smart contracts

A smart contract is a self-executing terms of agreement between two parties or more written directly into a code without the need for a central authority, legal system, or external enforcement mechanism. Therefore, a smart contract is defined as a piece of code that enforces logical rules to control digital assets. This code runs on top of a blockchain network. A smart contract defines contractual agreements that control the life cycle of a proposed transaction contained in the world state. Moreover, the smart contract packages the legally proposed transaction into the chain code, which is then deployed to the blockchain network [24]. Since 2016, there has been an increasing interest in blockchain-based smart contract applications. All these applications focus on the programmability of smart contracts in addition to security, privacy, and scalability [25].

5. Data sharing

Nowadays, data sharing is of significant importance in various industries. The traditional centralised services of data sharing suffer from many weaknesses. Blockchain technology has the potential to solve data-sharing problems due to its distributed architecture and characteristics [26, 27]. We can summarise the disadvantages of data sharing using traditional centralised services as follows:

- Data are stored in a third-party platform, which affects the traceability and control of the shared data.
- Centralised data sharing is vulnerable to intensive security threats.
- Centralised data sharing is limited to the database storage space.

Due to the properties of the blockchain, it may be the most promising solution to the problems faced by data-sharing applications. The advantages of blockchain technology for data sharing can be summarised as follows:

- Data storage is secure and transparent.
- Data transmission is secure and controllable.
- Data transactions are uniquely determined.
- Data can be traceable.

6. Protocol to issue and share student certifications in UOT

According to the central statistical organization in Iraq, the number of students who graduated from Iraqi universities and institutes is increasing constantly; table 1 shows the annual increasing numbers of graduates from Iraqi universities [23]. Consequently, there is a need for automatic and sustainable systems for issuing and verifying academic records. Issuing and sharing graduation documents are currently carried out in a number of stages, most of which are done manually and take a long time to complete. By the end of each course, the examination committee updates the student's records, and after completing all the graduation requirements, the student's certification is ready to be issued. The stages of issuing and sharing the graduation certificate with a recruitment office or university abroad where the student applies for a job vacancy or higher studies are as follows:

1. The student manually applies for their certification at the enrolment office.
2. After checking the student's records in the centralised database, the enrolment office prints the draft certification.
3. The enrolment office sends the draft certification to the dean's office and the chancellor's office for signing.
4. After the dean and chancellor sign the draft, the enrolment office issues the official certification.
5. The enrolment office sends the certification to the Ministry of Foreign Affairs for endorsement.
6. After receiving the certification from the Ministry of Foreign Affairs, the enrolment office hands the issued and endorsed graduation certification to the student.
7. At this stage, the student can hand-deliver or send their certification by email to a recruitment office or university for higher studies. The above stages are illustrated in figure 2.

Table 1. The number of Graduates from Iraqi Universities

No. of Graduates	**2015**	**2016**	**2017**	**2018**	**2019**
Public universities	58405	80426	90008	88028	91093
Private universities	21513	26951	27578	31633	24056
Technical universities	2134	3064	2858	3124	3126
Technical institutes	18796	20047	23757	29682	30126
Higher education	8081	7547	7959	9345	11039

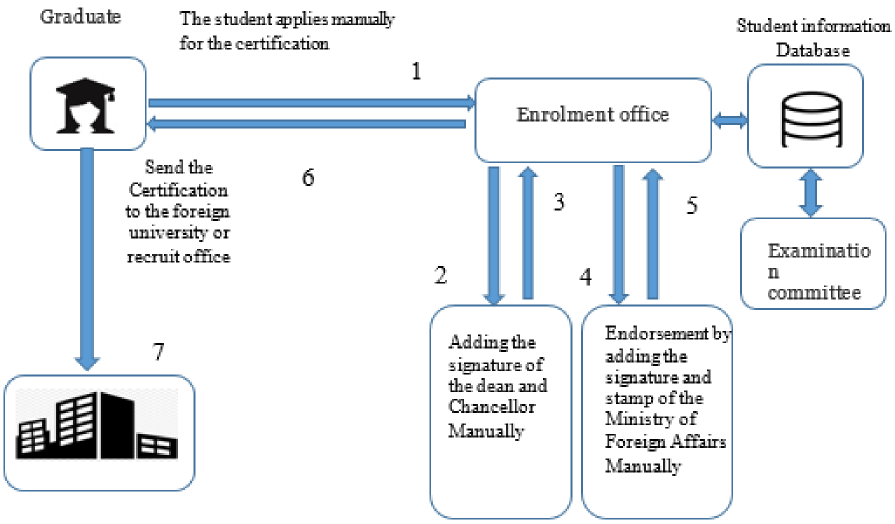

Figure 2. The stages of issuing a graduate certification at the University of Technology - Iraq

All of the stages of this protocol are performed manually and take days to complete. Figure 3 shows the timeline of the stages of the protocol.

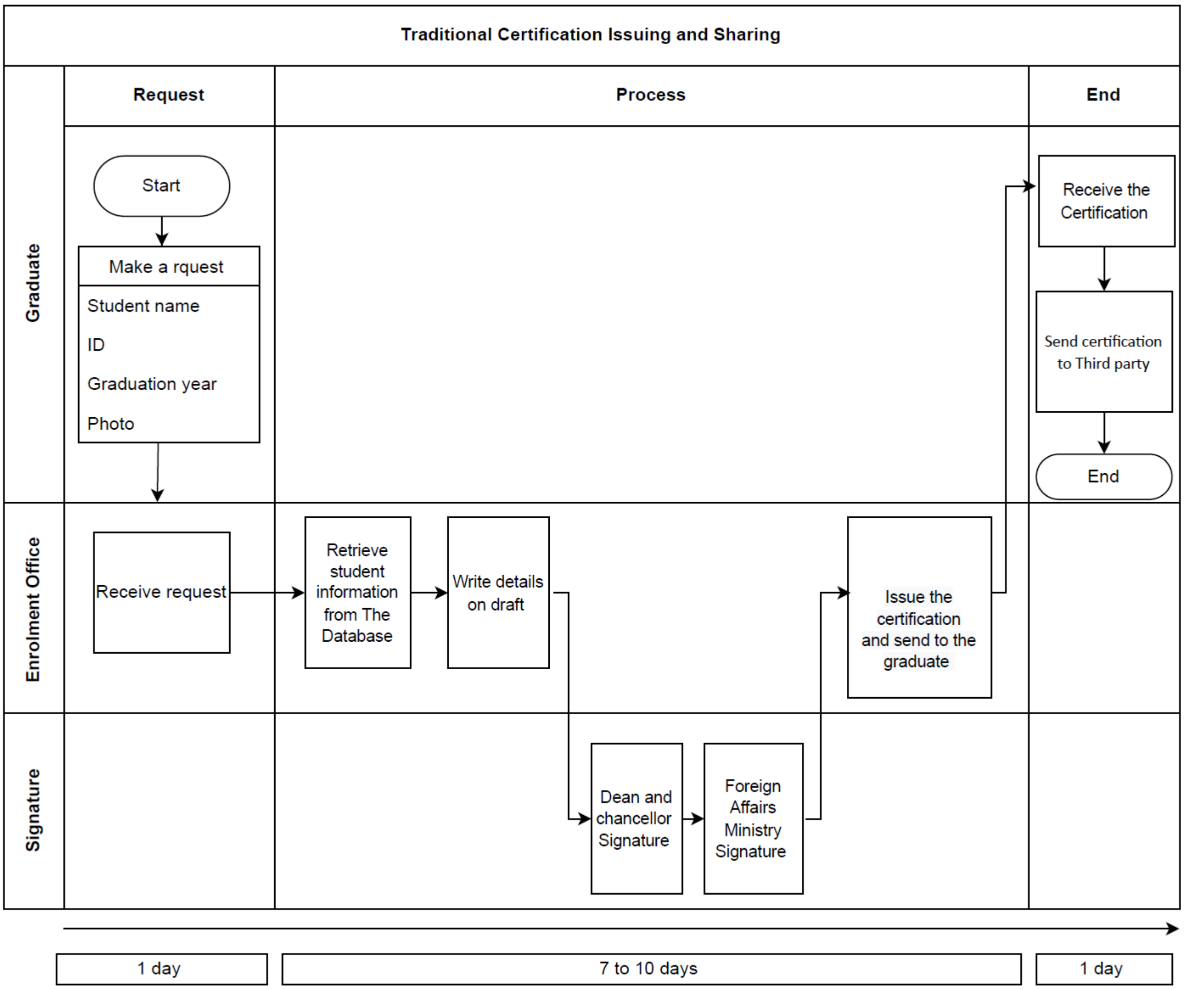

Figure 3. The timeline to issue a graduate certification at UoT -Iraq

6.1. The proposed framework

In this study, we proposed and implemented a graduation e-certification framework to exchange and approve students' certifications electronically. In addition to reducing paper-based work, the proposed system provides controlled sharing of students' information and maintains the privacy of the information through a private blockchain. The proposed framework provides two main services:

6.1.1. Issuing the electronic certificate

When the graduate applies for a job or postgraduate studies, they have to prove their graduation to the recruitment or postgraduate registering office. Therefore, the student requires a graduation certification to be issued, shared, and verified with these offices. For this to happen, the examination committee, enrolment office, and dean of the college must issue the graduation certification for the student who has completed all the requirements for graduation from the college. In this proposal, the graduation certification is issued, shared, and verified electronically. After the student successfully completed the study requirements, the examination committee will migrate all the courses that they studied along with the scores from the system database to the blockchain. For the issuance of the certification, the student applies using the web application, which sends the student's request to the university. The authorized entity sends the approval to issue the certificate after revising the student record and approving the process. In the next step, the student receives the e-certificate through the web application, which has the ability to export a PDF and share it with a third party. The steps of issuing a certification are illustrated in figure 4.

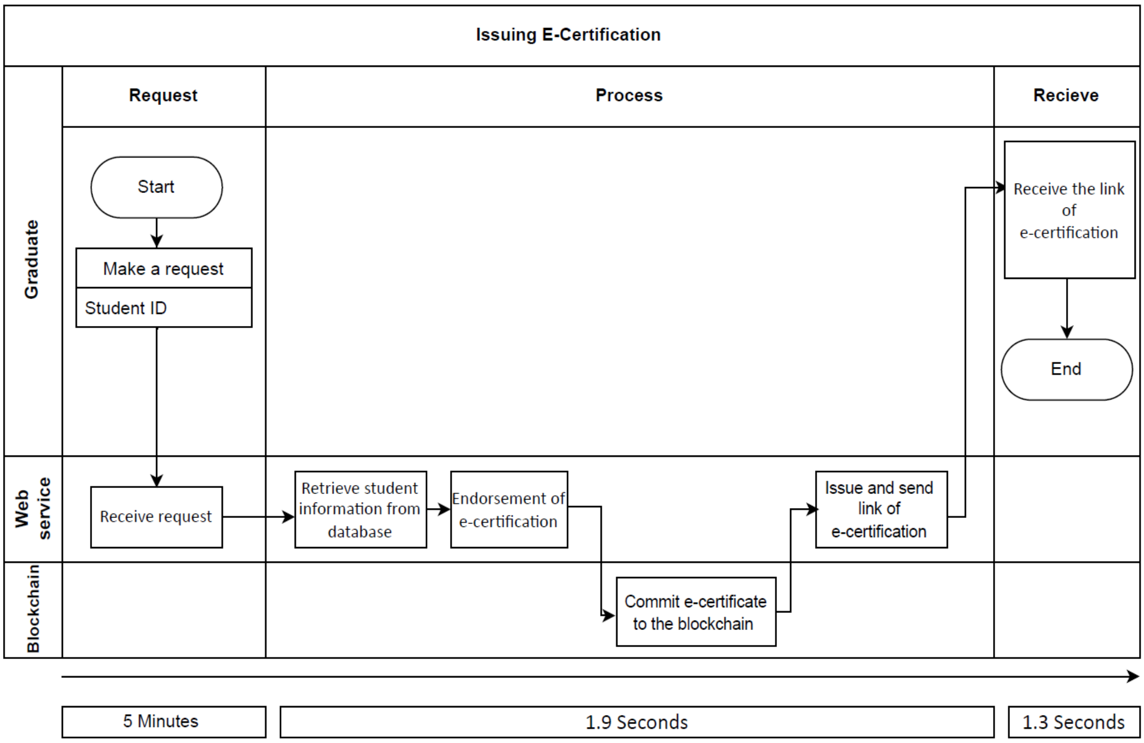

Figure 4. Issuing e-certificate process

6.1.2. Sharing the electronic certificate

As shown in figure 5, a web application has been developed to verify an e-certificate, which can be used by any party that wishes to verify an issued e-certificate. The verifier can be a recruiting office in a company, another educational institution, or even the graduates themselves. A student can provide any third party with a specific URL (in the web application) with an expiry date (for the generated URL), which can be used to verify the e-certificate.

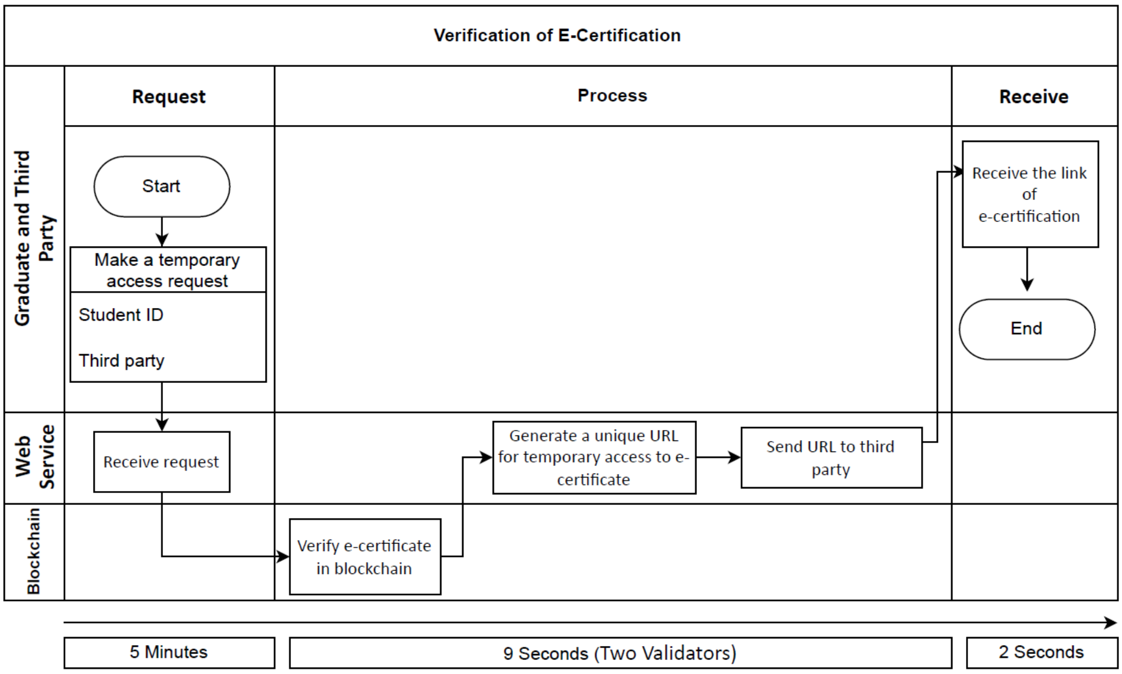

Figure 5. Certification verification service

The whole proposed framework is presented in Figure 6.

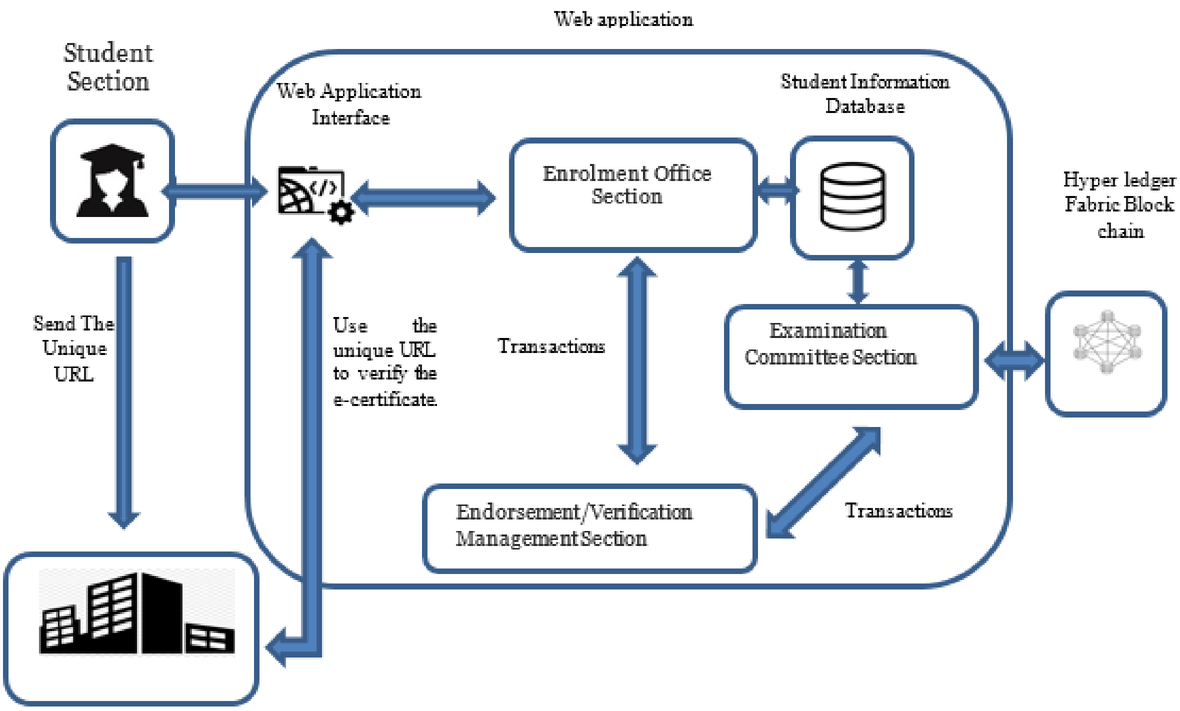

Figure 6. The proposed system

We can see five main sections here. Each section can be accessed by username and password as discussed below:

Enrolment office section (the endorser): This section of the web application is authorized to access the enrolment office to verify the student information and issue the e-certificate for the graduate. In other words, it is the node that verifies and declares the validity of the transaction. If the request is not legal, the endorsement node will reject it. This section and the examination committee section can access the local database. The local database is a MySQL database that is used to manage staff (university employees) information and student information (names, levels, branches, and scores) before they are migrated to the blockchain. Furthermore, the database provides authorization and authentication to each employee of the system sections (enrolment office, management approval, etc.) in the web application.

Algorithm 1: Enrolment office

```
Input: n request for e-certification
Output: approval to issue e-certification
1:  for counter = 1 to n do
2:          read student records in the local DB
3:          if (student graduate and satisfy all graduation requirements)
4:              send the transaction with approval to the Endorsement Node
5:          else
6:              reject the transaction
7:          end if
8:  end for
```

Management approval section (endorser/verifier): This section in the web application is authorised to access the dean of the college or any party who can sign the e-certification.

```
Algorithm 2: Management approval
Input: n request for e-certification
Output: endorsed transaction
1:  for counter = 1 to n do
2:          if (transaction approved from enrolment office section)
3:              endorse and sign the e-certification transaction
4:          end if
5:  end for
```

Examination committee section (committer): The authorized entity in this section has the capacity to allow the sharing of the issued e-certification from the blockchain to the student after receiving all the required approval. It also migrates all the courses (with the scores) that the student took to the Hyperledger Fabric blockchain from the system database after the student completes the study requirements.

```
Algorithm 3: Examination committee
Input: n request for e-certification
Output: approval for sharing e-certification with student
1:  for counter = 1 to n do
2:              if (transaction is endorsed from enrolment office section and from
                    management Section)
3:                  add e-certificate to the ledger
4:                  send the link of the e-certificate to the graduate
5:          end if
6:  end for
```

Student section (client): In this framework, the graduate can communicate with the other sections of the system through the web application to leverage the services provided by the system. The types of communication include making a request and receiving the result. The graduate may request an e-certification, verify the issued e-certification and share it with third parties. The third parties in this system may be recruitment offices or a foreign university.

```
Algorithm 4: Student section
Input: e-certification
Output share  e-certification with the third party
1:  if (third party requests graduate certification)
2:     graduate generates specific URL contains e-certification with time limit
3:       for time = current-time to (current-time + time-limit) do
4:               share URL for e-certification with the third party
5:       end for
6:  end if
```

Ledger: A ledger consists of chained blocks, with each block comprising a block header, block data, and metadata. The block header includes the hash code (Hi) of the block (Bi). The SHA256 algorithm was used to generate the hash code of each block. The hash code of the block (Bi-1) is included in the hash code of the block

(Bi). The block data represent the issued certifications. The block metadata includes any additional information that the university or college adds to the block. The blockchain ledger components are illustrated in figure 7.

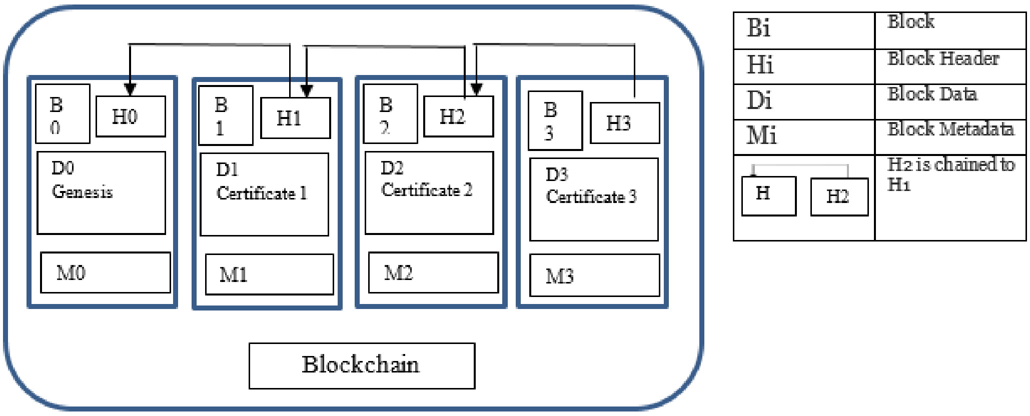

Figure 7. The blockchain components of the proposed system

7. Results of performance metrics

The implementation of blockchain-based student certifications was evaluated using two main performance metrics: the average time it takes to issue a certificate, measured in seconds, and the latency time, which is measured in seconds as well. Latency refers to the time the blockchain network takes to process the transaction. The implemented e-certification system using Hyperledger Fabric was tested for 1,000 transactions to issue 1,000 student certificates. The average computational time of certification deployment is shown in Table 2.

Table 2. Results for 1,000 input transactions

Service	Average time (in seconds)
Issuing certificate	1.9 (from examination committee to blockchain)
Latency time	1.4 (fetching the e-certification by the graduate)

The proposed e-certificate framework provides controlled data sharing through a smart contract. The whole record of all students are stored in a local database while the blockchain only contains e-certification data. However, access to private information is possible with the approval of the blockchain-authorized user.
The time required to verify each certificate depends on the number of validators in the system. We considered one to four validators and calculated the time required to verify one certification as shown in Figure 8.

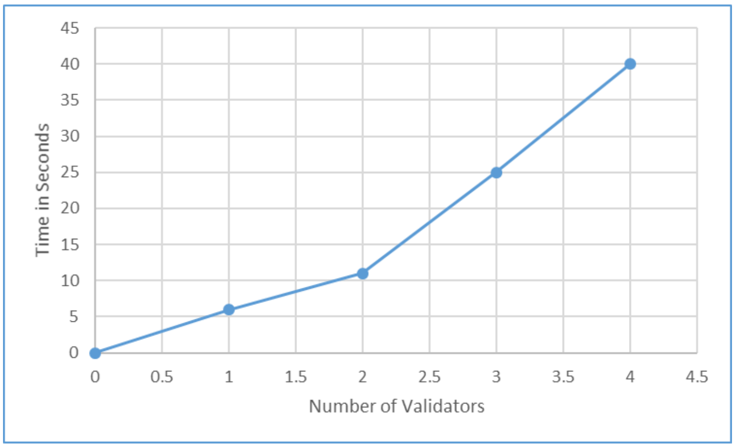

Figure 8. The relationship between validator number and time

Throughput, which is the relationship between the number of accomplished transactions and time, is shown in Figure 9. We see that the time required to fulfill the transaction requests increases exponentially as the number of concurrent transactions increases.

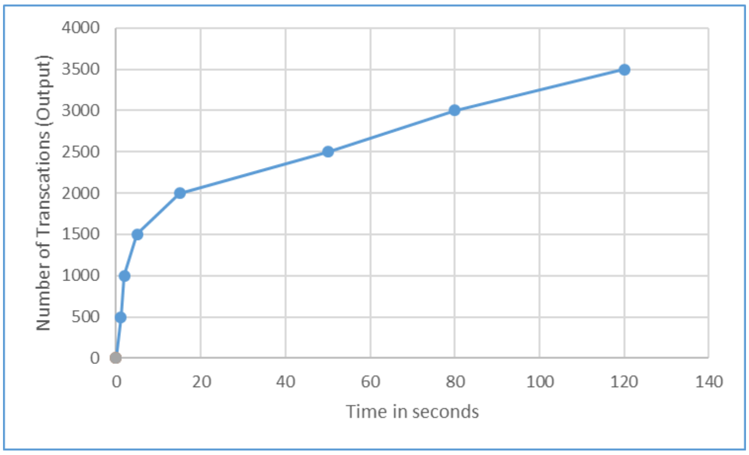

Figure 9. Throughput

8. Conclusion

This work developed a framework to store and share graduate certifications using blockchain. Storing these certifications using blockchain makes them immutable, private, and authenticated in a decentralised manner by multiple authorities. In this study, we have proposed and implemented an electronic system to deploy certificates. The system was created using the Hyperledger private blockchain. Hundreds of transactions can be sent to the blockchain in mere seconds. The proposed system used smart contracts and hashing to secure and control the deployment of the certifications. Testing the system showed low latency time in certificate deployment while guaranteeing privacy. The main advantages of the proposed system is the vast throughput of accomplished issued and verified certification in compare with the traditional methods to issue and verifying certification. The e-certification is issued and verified within 1 minuet while the traditional method takes about 1 week to 10 days. Also the proposed framework has the ability to control data sharing which keeps the client privacy. In addition, this framework allows the work of universities to be more transparent. Last but not least, digital transformation of certification issuing and verification participate tremendously in reversing the negative climate changes by reducing paper consuming.

References

[1] A. K. Shrestha and J. Vassileva, "User acceptance of usable blockchain-based research data sharing system: an extended TAM-based study," in *2019 First IEEE International Conference on Trust, Privacy and Security in Intelligent Systems and Applications (TPS-ISA)*, 2019, pp. 203-208: IEEE.

[2] A. Alketbi, Q. Nasir, and M. A. Talib, "Blockchain for government services—Use cases, security benefits and challenges," in *2018 15th Learning and Technology Conference (L&T)*, 2018, pp. 112-119: IEEE.

[3] H. Hou, "The application of blockchain technology in E-government in China," in *2017 26th International Conference on Computer Communication and Networks (ICCCN)*, 2017, pp. 1-4: IEEE.

[4] D. Geneiatakis, Y. Soupionis, G. Steri, I. Kounelis, R. Neisse, and I. Nai-Fovino, "Blockchain performance analysis for supporting cross-border E-government services," *IEEE Transactions on Engineering Management*, vol. 67, no. 4, pp. 1310-1322, 2020.

[5] Z. A. Kamal and R. Fareed, "Data retrieval based on the smart contract within the blockchain," *Periodicals of Engineering Natural Sciences*, vol. 9, no. 4, pp. 491-507, 2021.

[6] A. Hasselgren, K. Kralevska, D. Gligoroski, S. A. Pedersen, and A. Faxvaag, "Blockchain in healthcare and health sciences—A scoping review," *International Journal of Medical Informatics*, vol. 134, p. 104040, 2020.

[7] S. K. Lo, Y. Liu, S. Y. Chia, X. Xu, Q. Lu, L. Zhu, and H. Ning, "Analysis of blockchain solutions for IoT: A systematic literature review," *IEEE Access*, vol. 7, pp. 58822-58835, 2019.

[8] H. T. ALRikabi, and H. T. Hazim, "Enhanced Data Security of Communication System Using Combined Encryption and Steganography," *International Journal of Interactive Mobile Technologies*, vol. 15, no. 16, 2021.

[9] A. Alammary, S. Alhazmi, M. Almasri, and S. Gillani, "Blockchain-based applications in education: A systematic review," *Applied Sciences,* vol. 9, no. 12, p. 2400, 2019.

[10] R. A. Azeez, M. K. Abdul-Hussein, and M. S. Mahdi, "Design a system for an approved video copyright over cloud based on biometric iris and random walk generator using watermark technique," *Periodicals of Engineering Natural Sciences,* vol. 10, no. 1, pp. 178-187, 2022.

[11] H. Salim, A. M. Alaidi, and I. A. Aljazaery, "Encryption of Color Image Based on DNA Strand and Exponential Factor," *International Journal of Online and Biomedical Engineering (iJOE),* vol. 18, no. 3, 2022.

[12] S. Jayalakshmi, "The Impact of the Blockchain on Academic Certificate Verification System-Review," *EAI Endorsed Transactions on Energy Web,* p. e35, 2021.

[13] R. Raimundo and A. Rosário, "Blockchain system in the higher education," *European Journal of Investigation in Health, Psychology Education,* vol. 11, no. 1, pp. 276-293, 2021.

[14] H. Li and D. Han, "EduRSS: A blockchain-based educational records secure storage and sharing scheme," *IEEE Access,* vol. 7, pp. 179273-179289, 2019.

[15] M. Turkanović, M. Hölbl, K. Košič, M. Heričko, and A. Kamišalić, "EduCTX: A blockchain-based higher education credit platform," *IEEE access,* vol. 6, pp. 5112-5127, 2018.

[16] M. Oliver, J. Moreno, G. Prieto, and D. Benítez, "Using blockchain as a tool for tracking and verification of official degrees: business model," in *29th European Regional Conference of the International Telecommunications Society (ITS):" Towards a digital future: Turning technology into markets, Trento, Italy, 1st-4th August*, Trento, Italy,, 2018, vol. 10.

[17] M. Sharples and J. Domingue, "The blockchain and kudos: A distributed system for educational record, reputation and reward," in *European conference on technology enhanced learning*, 2016, pp. 490-496: Springer.

[18] S. Nakamoto, "Bitcoin: A peer-to-peer electronic cash system," *Decentralized Business Review,* p. 21260, 2008.

[19] Z. Zheng, S. Xie, H. Dai, X. Chen, and H. Wang, "An overview of blockchain technology: Architecture, consensus, and future trends," in *2017 IEEE international congress on big data (BigData congress)*, 2017, pp. 557-564: IEEE.

[20] S. Makridakis and K. Christodoulou, "Blockchain: Current challenges and future prospects/applications," *Future Internet,* vol. 11, no. 12, p. 258, 2019.

[21] Z. Alhadhrami, S. Alghfeli, M. Alghfeli, J. A. Abedlla, and K. Shuaib, "Introducing blockchains for healthcare," in *2017 international conference on electrical and computing technologies and applications (ICECTA)*, 2017, pp. 1-4: IEEE.

[22] N. Ullah, W. Mugahed Al-Rahmi, A. I. Alzahrani, O. Alfarraj, and F. M. Alblehai, "Blockchain technology adoption in smart learning environments," *Sustainability,* vol. 13, no. 4, p. 1801, 2021.

[23] C. Fan, S. Ghaemi, H. Khazaei, and P. Musilek, "Performance evaluation of blockchain systems: A systematic survey," *IEEE Access,* vol. 8, pp. 126927-126950, 2020.

[24] H. Zhao, M. Zhang, S. Wang, E. Li, Z. Guo, and D. Sun, "Security risk and response analysis of typical application architecture of information and communication blockchain," *Neural Computing Applications,* vol. 33, no. 13, pp. 7661-7671, 2021.

[25] D. Macrinici, C. Cartofeanu, and S. Gao, "Smart contract applications within blockchain technology: A systematic mapping study," *Telematics Informatics,* vol. 35, no. 8, pp. 2337-2354, 2018.

[26] M. A. Cyran, "Blockchain as a foundation for sharing healthcare data," *Blockchain in Healthcare Today,* 2018.

[27] Z. A. Kamal and R. Fareed, "A Proposed hash algorithm to use for blockchain base transaction flow system," *Periodicals of Engineering Natural Sciences,* vol. 9, no. 4, pp. 657-673, 2021.