Computer Systems Science & Engineering
DOI:10.32604/csse.2022.023508
Article

Blockchain for Education: Verification and Management of Lifelong Learning Data

Ba-Lam Do*, Van-Thanh Nguyen, Hoang-Nam Dinh, Thanh-Chung Dao and BinhMinh Nguyen

School of Information and Communication Technology, Hanoi University of Science and Technology, Hanoi, Vietnam
*Corresponding Author: Ba-Lam Do. Email: lamdb@soict.hust.edu.vn
Received: 11 September 2021; Accepted: 19 November 2021

Abstract: In recent years, blockchain technology has been applied in the educational domain because of its salient advantages, i.e., transparency, decentralization, and immutability. Available systems typically use public blockchain networks such as Ethereum and Bitcoin to store learning results. However, the cost of writing data on these networks is significant, making educational institutions limit data sent to the target network, typically containing only hash codes of the issued certificates. In this paper, we present a system based on a private blockchain network for lifelong learning data authentication and management named B4E (Blockchain For Education). B4E stores not only certificates but also learners' training data such as transcripts and educational programs in order to create a complete record of the lifelong education of each user and verify certificates that they have obtained. As a result, B4E can address two types of fake certificates, i.e., certificates printed by unlawful organizations and certificates issued by educational institutions for learners who have not met the training requirements. In addition, B4E is designed to allow all participants to easily deploy software packages to manage, share, and check stored information without depending on a single point of access. As such, the system enhances the transparency and reliability of the stored data. Our experiments show that B4E meets expectations for deployment in reality.

Keywords: Training data; certificate; verification and management; private blockchain

1 Introduction

Education is always one of the fields that all people, organizations, and countries pay attention to most. Through diversified learning activities, the human becomes more mature in knowledge and skills, thereby improving the quality and value of the work we will be doing. After completing a learning program, organizations typically grant degrees or certificates for learners to record the results they achieved. Unfortunately, there is a considerable part of workers who want to own these certificates without going through actual training. In 2020, the Association of Certified Fraud Examiners estimated that 64% of occupational fraudsters had a university degree or higher [1]. This situation can create immeasurable risks because fake diplomas could help many people find a job beyond their genuine ability.

Currently, we can divide the fake certificate problem into two main categories. The first one is forged by individuals and organizations outside the educational institutions. For example, just by few simple searches, users can find such diploma mills that can provide fake certificates of any prestigious university in the world. In addition, with only about 200 USD, these fake records are printed and promised to be undetected. The latter category refers to fake degrees issued by educational institutions for people who have not completed the training program or participated in an unlicensed program. For example, in Feb. 2021, Vietnam government discovered at least 626 fake English bachelor's degrees granted by Dong Do University, Vietnam [2]. Next, at least 55 people have used these certificates to meet requirements for defending master or doctoral dissertations. These examples above show that the need to own fake certificates is significant in multiple countries. Buyers believe that the complicated and expensive checking process can make it difficult for verifiers to detect counterfeit diplomas that look like the real ones.

In recent years, a significant number of universities, organizations, and governments such as MIT [3], Blockchain Certified Data [4], and Singapore government [5] have introduced blockchain-based systems for certificate authentication. Blockchain technology which has salient advantages of transparency, decentralization, and immutability [6] is expected to address the fake certificate problem successfully. However, existing solutions which rely on public blockchain networks such as Ethereum [7] and Bitcoin [8] face two main issues that can reduce the adopted capability to the current problem. First, the cost of writing data on these networks is significant, which makes educational institutions limit data sent to the target network. Therefore, these institutions typically focus on storing hash codes of the certificates and ignoring information about the learning process. This choice makes students hard to possess a complete record of lifelong education. Second, current solutions concentrate on showing that stored certificates are validated without providing evidence such as transcripts and educational programs for this confirmation. As a result, these systems can not handle the case that a university offers fake certificates.

In this paper, we introduce a blockchain-based system named B4E for verifying and managing educational data. B4E utilizes a private blockchain network that has the participation of management organizations (e.g., ministry of education, departments of education), universities, and high schools within a country. Compared to a public blockchain network in which anyone can take part and does not trust another, a private blockchain restricts participation to authorized and invited entities. In addition, incentive mechanism through transaction fees used in public networks to make them popular is not necessary for private networks. Therefore, B4E, which possesses significant advantages of cost, privacy, and speed, is a suitable choice for governments who want to apply blockchain technology in the educational field for all their educational institutions. Currently, B4E allows organizations to securely store the entire training process of learners, including training time, score history, educational program to confirm the certificate's value. In addition, users can conveniently manage all results obtained and easily share these results with examiners. To this end, B4E first relies on Hyperleger Sawtooth [9]–a private blockchain to store data. Next, all students' data are encrypted by the public keys of learners; hence, only students can decrypt and share their data. Furthermore, to enhance transparency and decentralization, B4E can be packaged on independent software components that allow educational institutions, management organizations, learners, and employers to easily manage and validate data without depending on a single access point. Currently, the source code of B4E is published at https://gitlab.com/blockchain-for-education.

To sum up, the main contributions in our paper include: (i) we present a private blockchain-based system named B4E, which allows each country to manage and verify the lifelong learning data of citizens. In particular, learners can privately store and efficiently share a complete document of their learning process, including transcripts and certificates issued by educational institutions within the country. In addition, B4E not only ensures requirements of transparency, decentralization, and immutability but also obtains advantages of cost, privacy, and speed. The source code of B4E is public on GitLab to allow developers and organizations to contribute and use; and (ii) we enhance the confidence of data by linking learners' training process and their obtained diplomas. As a result, B4E can address both types of fake certificates, i.e., certificates printed by criminal organizations and certificates issued by educational institutions for learners who have not met the training requirements.

The remainder of this paper is shown as follows. In Section 2, we introduce efforts related to our work. Next, Section 3 describes the architecture and implementation of B4E. We evaluate the system performance in Section 4. Finally, we conclude in Section 5 with an outlook on future research.

2 Related Work

In recent years, blockchain technology has been used in a wide range of domains because of its salient advantages such as supply chain management [10], agriculture [11], health [12,13], power [14], etc. In the education domain, applying blockchain technology to verify certificates has received considerable interest from universities, organizations, and governments [15–17]. We can classify existing efforts into three main groups, including internal systems in universities, global systems, and national systems.

In the first category, a huge number of universities, including University of Zurich (Switzerland) [18], University of Raharja (Indonesia) [19], and HCMC University of Technology (Vietnam) [20] have developed blockchain-based systems for managing diplomas at these universities. These systems share the same goal towards digitizing physical certificates and meeting the requirements of each university, such as be easy to integrate into existing IT infrastructures. As a result, these systems can be independently deployed at only a university without connecting to other educational institutions. To ensure reality of the data, the systems need to utilize public blockchain networks such as Ethereum. In particular, the UZHBC system of University of Zurich aims to meet seven main requirements of shareholders, including issuers, recipients, and verifiers. The system of University of Raharja can add a QR-code to each physical certificate and print these certificates with QR-code attached in paper format. Finally, CVSS system of HCMC University of Technology can simultaneously issue both physical and digital degrees without making a significant change to the existing certificate system.

The second group refers to global solutions expected to conveniently apply to any higher education institutions (HEI) to issue and verify certificates. For example, BCDiploma [4] is a European project which has been deployed at more than 90 HEIs in 12 countries on four continents. This platform utilizes Ethereum network to store certificates of graduates securely. To pay the service fee, HEIs need to use BCDT token issued by the project or fiat currency. EduCTX [21] is a platform for certificate management and authentication. This platform enhances the privacy of data through encryption of users' certificates by their public keys. An IPFS network [22] is also utilized as a place to store encrypted certificates. As a result, only students can decrypt and share their learning results. Blockcerts [3] developed by the MIT Media Lab and Hyland Credentials, includes a set of open-source applications, tools, and libraries to verify official certificates. The issuers first calculate the hash value of the certificate, then utilize a public network such as Bitcoin or Ethereum to store this value. After that, universities send students a receipt of this certificate, which includes transaction ID, certificate, and the issuer information. To check the validity, an examiner uses the issuer's signature and compares data on the chain with input data on the receipt.

In the final category, OpenCerts [5,23] is a certificate authentication system developed by the Singapore government. Universities can make use of provided tools and defined standards to format and compress learning data, including transcripts and certificates, before writing them on Ethereum network.

The system will generate a file containing learners' results and transaction information and then send it to the students through email and mobile application. To authenticate data, employers upload checking files to a unique website managed by the government. Although OpenCerts opens a huge opportunity for educational organizations to store transcripts, the system does not create a connection between transcripts and certificates. In addition, the verification process is centralized at a single point of access, which reduces the transparency of the system.

Compared to existing systems, B4E aims to create a national verification and management system similar to OpenCerts's goal. However, B4E has four differences compared to all related efforts, i.e., (i) B4E relies on a private blockchain to remove transaction fees and allow educational institutions to write a tremendous number of learning data; (ii) B4E makes use of educational programs and transcripts to provide an additional checking mechanism for verifying stored certificates; (iii) Users can own a complete record of lifelong learning including transcripts and certificates from educational institutions; and (iv) B4E enhances the transparency by allowing participants to independently deploy software packages to manage, share, and verify data. Tab. 1 provides a comparison of the related efforts and our research.

Table 1: A comparison of the related work

Authors	Year	Developed by	Blockchain type	A	B	C	D	E
Gresch et al. [18]	2018	University of Zurich	Public	Yes	No	No	No	No
Aini et al. [19]	2020	University of Raharja	Public	Yes	No	No	No	No
Nguyen et al. [20]	2018	HCMC University of Technology	Public	Yes	No	No	No	No
BCDiploma [4]	2021	Blockchain Certified Data	Public	Yes	No	No	No	No
EduCTX [21]	2018	Blockchain Lab:UM	Public	Yes	No	Yes	No	Yes
Blockcerts [3]	2016	MIT Media Lab & Hyland Credentials	Public	Yes	No	No	No	Yes
OpenCerts [5,23]	2021	Singapore GovTech & OpenCerts	Public	Yes	Yes	No	Yes	No
Our propoal	2021	BKC Lab, Hanoi University of Science and Technology	Private	Yes	Yes	Yes	Yes	Yes

Notes: A: Certificate verification; B: Transcript verification; C: Encryption by student identification/Ownership; D: Lifelong learning management; E: Distributed management.

3 System Design

In this section, we first present the architecture of B4E in Section 3.1. Next, main characteristics of B4E are mentioned in Section 3.2. Finally, main business processes and deployment of B4E will be shown in Sections 3.3 and 3.4, respectively.

3.1 System Architecture

Fig. 1 introduces an overview of the B4E architecture, which contains three main layers:

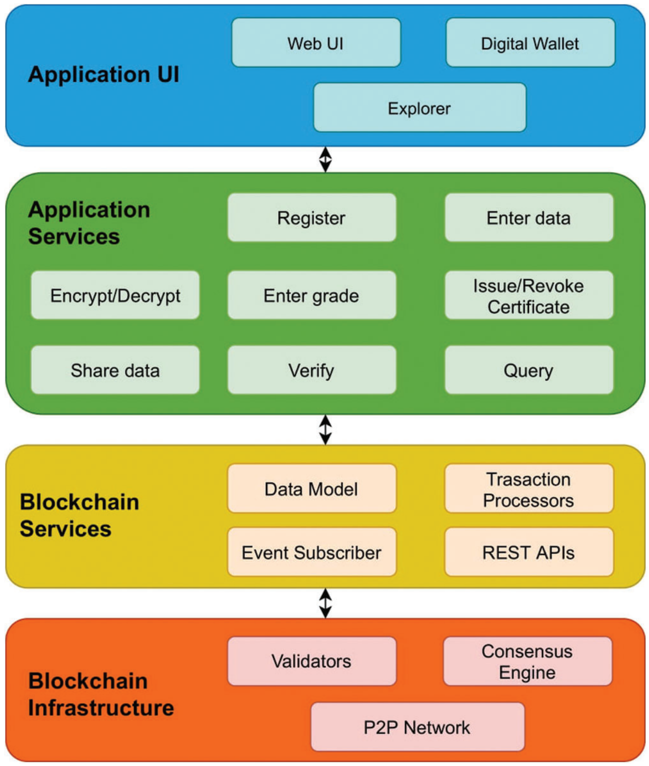


Figure 1: Overview of B4E architecture

Application UI layer provides users three ways to communicate with the system. First, each user will have a web-based interface corresponding with their role in the system. In addition, executing each transaction requires a digital signature generated from the executor's private key. Therefore, B4E provides a wallet application that acts as an extension for Chrome browser to help users use and manage their key pairs. Finally, an explorer application allows users to exploit information of the blockchain network such as existing transaction processors, history of transactions and blocks, and a list of participant nodes.

Application Services layer consisting of multiple services is responsible for implementing business logic of the system. For example, universities and high schools need to register to become official members of the system. After passing the voting step, they are provided services to issue and revoke certificates, add lecturers for entering grades, etc. For lecturers, they mainly make use of Entering grade service to write learning outcomes for their students on the network. In Section 3.3, we will describe the linkage of these services through several main business processes.

Blockchain Services layer plays an important role in connecting the application layer and the physical blockchain network. This layer contains four core services, i.e., Data model provides a standardized definition of data objects that are stored and processed on the blockchain network; Transaction Processors handle the system's transactions to ensure that they are always validly executed before being written to the blockchain network; REST API provides access to blockchain network to read and write data through the use of HTTP/JSON standards; and Event Subscriber is responsible for listening events taking place on the blockchain network, filtering and updating system-related events into a database to optimize the process of tracing data executed by the explorer application.

Blockchain Infrastructure layer that refers to configuration and deployment of the blockchain network contains three main components, i.e., Validators are nodes on the network, used to validate batches of transactions, combine them into blocks, maintain consensus within the network, and coordinate communication; Consensus engine allows all validators to unify on verifying the transactions; and P2P network consists of multiple nodes participating in the network. They can be located near together or geographically distributed at many places and connected through Internet network.

3.2 Main Characteristics

B4E is an application based on blockchain technology; hence, it owns inherent characteristics of this technology. In addition, we facilitate advantages of B4E by developing multiple functionalities and utilities. We can list five important characteristics of B4E, including:

- **Ownership**: Results of each student, including grades and certificates, are encrypted by the student's public key before writing them on the blockchain network. Therefore, students are the only owners of their data. To read and share data, they need to rely on the Decrypt service, which utilizes their private keys to obtain plain-text from the ciphertext. Next, they can generate a token to share the result of a course, the whole transcript, or a certificate to examiners through the use of the Share data service.
- **Lifetime**: Our system allows any educational institution within a country, for example, university, colleague, high school, etc. can join the system through registration and voting mechanisms. As a result, these organizations can write learning results, including grades, certificates, confirmations, etc., to the same person. These documents help to create a complete record of lifelong education of each citizen in a country.
- **Authorization**: We rely on the Transaction Processors component and access mechanism to ensure the validity and correction of data. In particular, processors are responsible for checking the role of each user. For example, lecturers can enter the grade for students in their classes. They have no permission to issue certificates or share students' results with external organizations. Furthermore, access mechanisms such as private keys stored on the wallet and TOTP (Time-based One-time Password) provide two-factor authentication for entering grades of lecturers.
- **Linkage**: One salient characteristic of B4E that differentiates it from existing related systems is that B4E provides linkage between certificates and training process including grades, educational program, courses in each semester, etc. As a result, B4E can provide convincing explanations of the value of certificates that students have obtained in their lifetime.
- **Independence**: B4E contains a set of components designed and developed for different actors such as university, student, employer, etc. We can pack relevant services and interfaces for each user into software packages that can be deployed independently. As a result, users can easily self-check and validate data without depending on a single access point.

3.3 Main Business Processes

To illustrate how the system works, we provide detailed descriptions of some business flows of the B4E. We first introduce main actors of B4E, then present three main processes relating to these actors.

Main Actors: B4E has the participation of six actors named ministry, educational institution, lecturer, student, and verifier. The ministry refers to management organizations who are responsible for supervising educational activities, for example, the ministry of education and departments of education. This actor initializes the blockchain network to store learning outcomes of pupils and students. Next, the educational institution actor mentions universities, colleges, and high schools where provide training programs to learners. They have permissions such as adding educational programs, lecturers, and students and issuing/revoking certificates. At these institutions, lecturers will conduct teaching activities, then provide grades to learners. Finally, the student actor consists of students and pupils, whereas the verifier actor can be employers at companies.

Register: Fig. 2 illustrates the registration process of an educational institution to become a system's member. First, these institutions should declare email, domain name, and other contact information. Next, they must prove ownership through a confirmation email and DNS lookup. After that, B4E supports the institutions to create a registration transaction and write it on the blockchain network. When a new registration appears, the ministry and current institutions participating in the system will receive a notification to consider the application. With the ministry's consent or more than 50% of the member institutions, the candidate will be accepted.

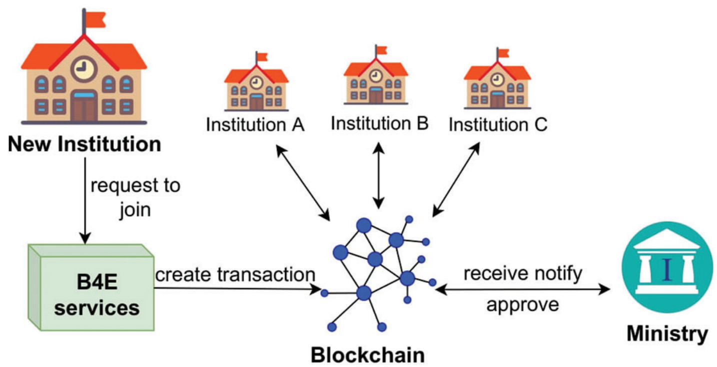


Figure 2: Registration process

Write Learning Data: Fig. 3 depicts steps of writing grades and certificates for students. In the first step, the university creates identifiers and grants scoring permissions to the lecturers. Next, students' information, including ID and training program, needs to be written to the blockchain network. At the beginning of each semester, the university records information about classes (lecturer, course, and student list) on the network. Next, at the end of the semester, lecturers will enter grades for students in their classes. B4E relies on the scoring transaction processor to verify whether the lecturer has the right to write scores for students. In the final step, when the university wants to grant a degree to the student, the degree transaction processor will check if the student has completed the training program or not, such as checking if the number of credits accumulated and the learning time. Thanks to the identification mechanism and tight constraints on recording learning data, B4E allows the system to eliminate possible fraud.

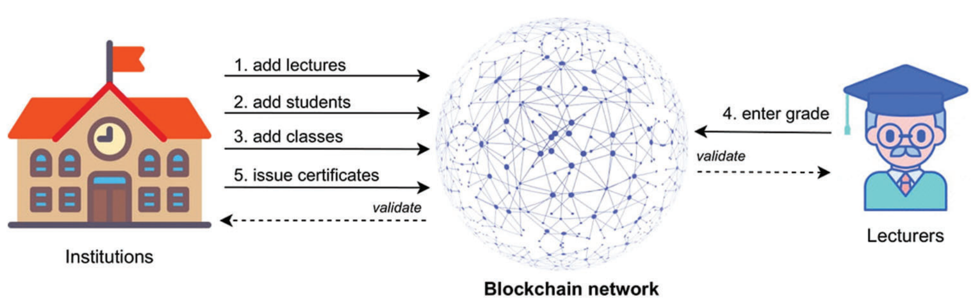


Figure 3: Learning data writing process

Share and Verify: Fig. 4 shows process of sharing data. To this end, B4E first uses students' identification (i.e., public key) to search for their data on the blockchain network. Relevant data consist of transcripts and certificates that students have obtained throughout the life. Next, students utilize their private keys stored on the wallet application for the decryption. After that, the decrypted data will be encoded by the JSON Web Token (JWT) library [24] to generate a token code. Finally, students can send the token to verifiers to show evidence of their capability.

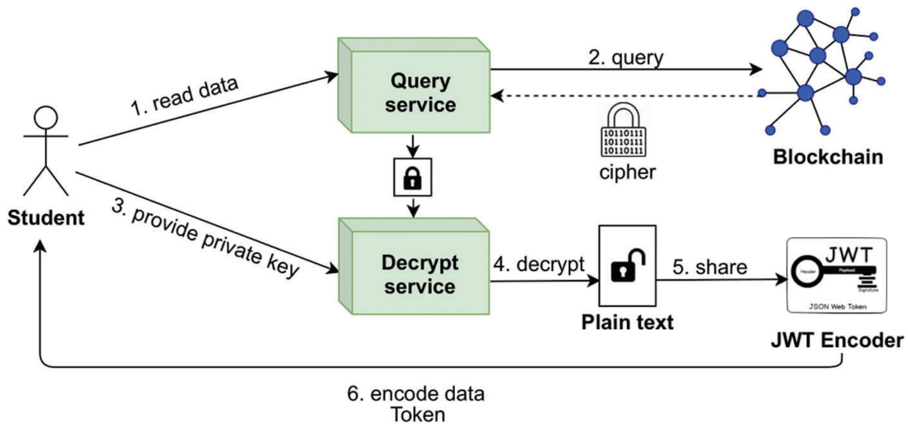


Figure 4: Data sharing process

On the other way, Fig. 5 illustrates how the verifier can use B4E to check the validity of transcripts and certificates. First, the system will decode the token to retrieve the plain-text data. Next, B4E will compare the hash values of data on the plain-text and the data on the blockchain network. A set of requirements, including integrity, timestamp, educational program, total credits, etc., will be used by the Verify service. Finally, the checking result will be informed to the user.

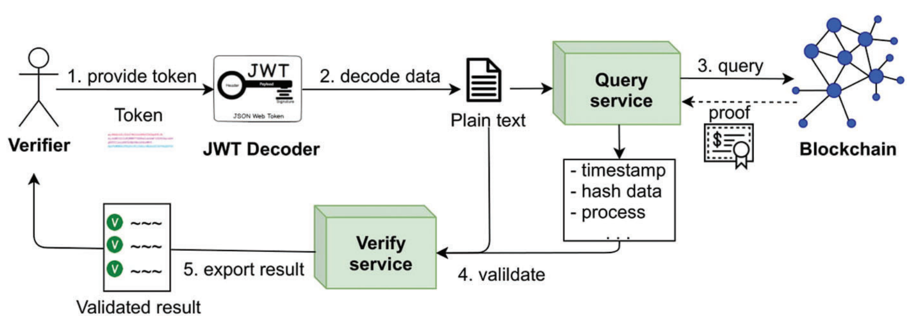


Figure 5: Data verifying process

3.4 System Deployment

Fig. 6 illustrates the system deployment for the ministry, educational institutions, students, verifiers, and an explorer application. Each actor manages a set of individual services; hence, we separate and pack entire system services into Docker images for each user to allow them to conveniently and consistently deploy at separate servers. Each image is named with a tag as a version and pushed to Docker Hub.

The ministry's installation package provides the starting point of the entire system. This package's Infrastructure includes four Sawtooth nodes to initialize the network for all participants. The University package for universities and high schools is similar to the installation package of the ministry, except that the Sawtooth network nodes in this package are configured to connect to the Sawtooth network created by the ministry. Note that the services of lecturers are integrated into the University package. The packages for student, verifier, and an explorer application do not contain blockchain infrastructure and processors because they have no permission to write educational results to the network. Instead of missing these components, the packages contain REST APIs (for student's and verifier's packages) or an event subscriber (for explorer's package) to communicate with the infrastructure layer. Finally, all packages are provided Web UI and Services in order to provide intuitive communication for users in interacting with the system.

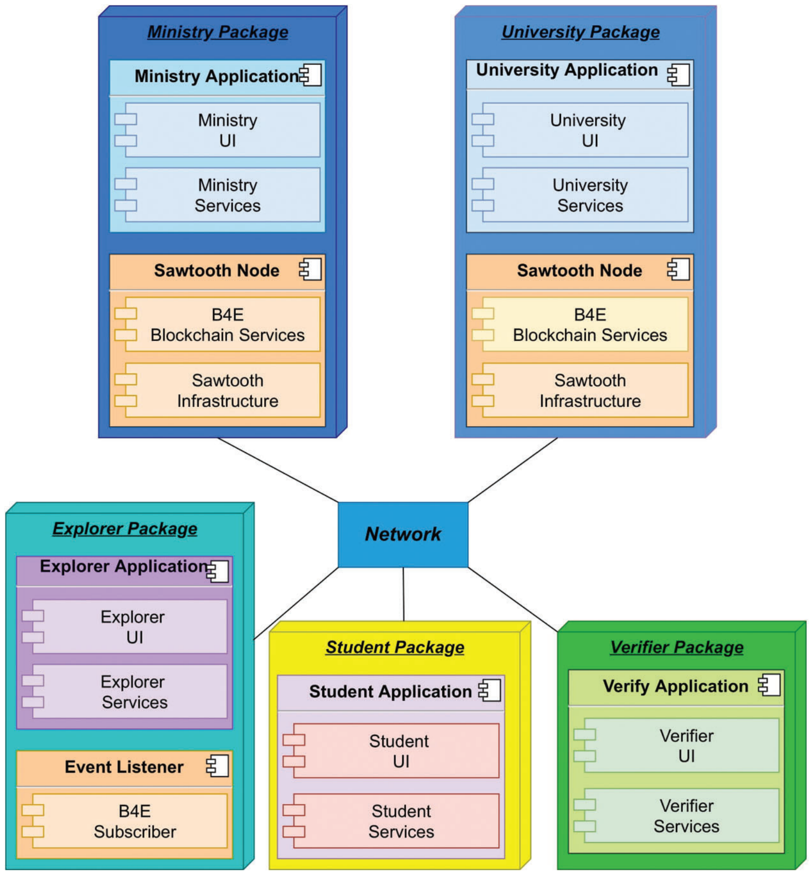


Figure 6: B4E deployment

4 Evaluation

The purpose of this section is to provide evaluations of the B4E's performance with the current architecture and deployment. Because B4E can be divided into two tiers, i.e., web application and blockchain network, hence, we perform experiments for these tiers. Among B4E's deployment packages, the university's system has the largest number of users and activities. As a result, we select the university's system to evaluate the performance of B4E. First, we measure the capability of handling concurrent requests from lecturers for obtaining class information. Next, we calculate the speed of reading and writing transactions on the blockchain network.

4.1 Experiment Information

We utilize two machines on Digital Ocean to deploy a private blockchain network and a university's web application. The first machine is used to initialize the network containing four blockchain nodes of the ministry, using PBFT consensus algorithm [25] and Hyperledger Sawtooth version 1.2. The second machine allows us to set up another blockchain node for the university and its web backend. The configuration for the first machine is Ubuntu 18.04, 8-Core CPU, 16GB RAM, and 310GB SSD, whereas the second machine installs Node 14.16-alpine and Mongo 4.4.6 and uses Ubuntu 18.04, 4-Core CPU, 8GB RAM, and 155GB SSD.

4.2 Evaluation of Web Application

We assume that there are many lecturers using the system at the same time to query information about their teaching classes. The system's backend will return a list of classes and students participating in each class. Assuming that each lecturer teaches three classes in a semester, and each class consists of 50 students. We measure the system's response if there are n lecturers simultaneously sending requests to retrieve information about their classes. We make use of Apache JMeter software [26] to create n threads; each thread simulates for one lecturer. In addition, for each thread, we repeat the request ten times after receiving the response from the system. Therefore, the total of requests sent to the server is 10*n, but at each time, the number of concurrent requests that the system has to handle is still n.

Fig. 7a shows the measurement results for the case n = 100. The first stage is the warm-up process. During this phase, JMeter software gradually generates threads from 0 to 100 and sends requests to the system. It can be seen that, as the number of threads is gradually increased, which means that the number of requests the system has to process simultaneously increases, the average response time for a request also increases. At the end of the warm-up process, in the next phase, the number of threads does not change (i.e., 100 threads)-also the number of simultaneous requests the system has to handle, the system performance reaches a stable state. Although the response time for each request is still different, the difference is not large. In the final stage when JMeter gradually ends the testing process, the number of concurrent requests that the system has to handle is reduced, the response time for each request is significantly reduced. The success rate of the requests is 100%, the average response time is 530 ms, and the standard deviation is 103 ms. These results show the feasibility and ability to meet the actual needs of the system.

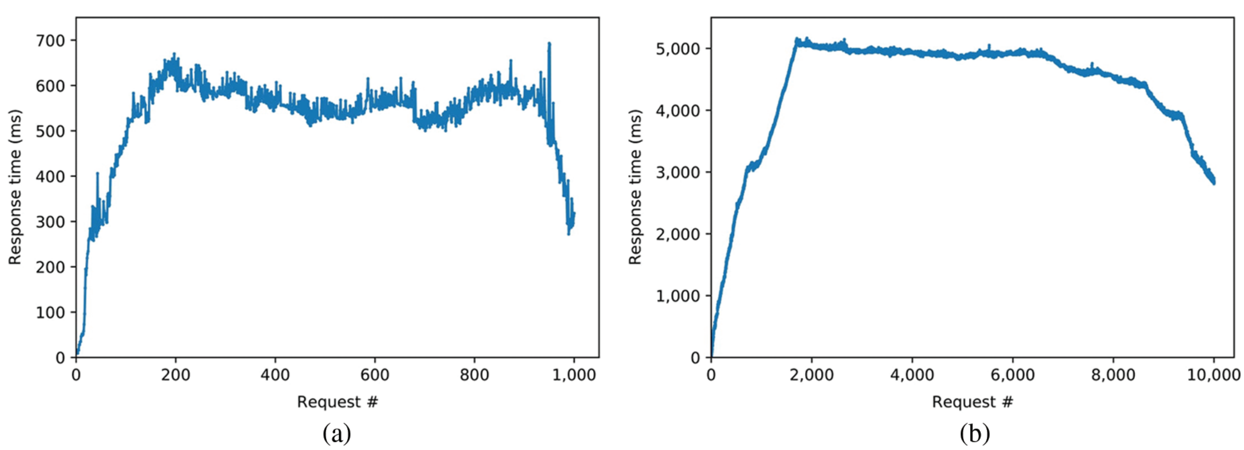


Figure 7: Performance of university web app. (a) 100 concurrent requests (b) 1,000 concurrent requests

Fig. 7b shows the evaluations for the case n = 1,000. It can be seen that the test results in this case have many similarities with the case of n = 100. The graphs of the two cases have similar shapes: the response time increases gradually during the warm-up process and the success rate of 100%. However, the average response time of each request is up to 4,356 ms. In practice, the situation of encountering concurrent requests from thousands of lecturers is scarce, so it can be considered that the system has met realistic expectations.

4.3 Evaluation of Blockchain Network

We conduct four different experiments to calculate the speed and response time of the blockchain network for activities of reading and writing data.

Firstly, we measure the impact of batch size on throughput (transactions per second-TPS) for two types of transactions, i.e., writing certificate and writing grade. The batch size, which is equivalent to block size, wraps multiple transactions inside to commit state together or not at all. In our experiment, the execution time is determined from the moment the batch is sent to the blockchain network until entire transactions in the batch are processed on all nodes and the batch status becomes "COMMITTED". The initial batch size is 50 and increases in arithmetic progression with a difference of 50. To increase the TPS, we rely on the parallel scheduler and multiple transaction processors. In particular, Sawtooth includes an advanced parallel scheduler that splits transactions into multiple parallel flows to increase performance compared to the serial mechanism. The use of multiple transaction processors can help to process a huge number of transactions in a quick manner. However, creating a scheduler, making consensus, and processing block must be done sequentially. Fig. 8 shows how changing the batch size affects transaction execution speed, leading to the selection of the optimal batch size parameter for transaction throughput. The best performance is achieved when the batch size is 200. At this value, the throughputs for writing grades and certificates obtain 58.92 and 59.86 tx/sec, respectively.

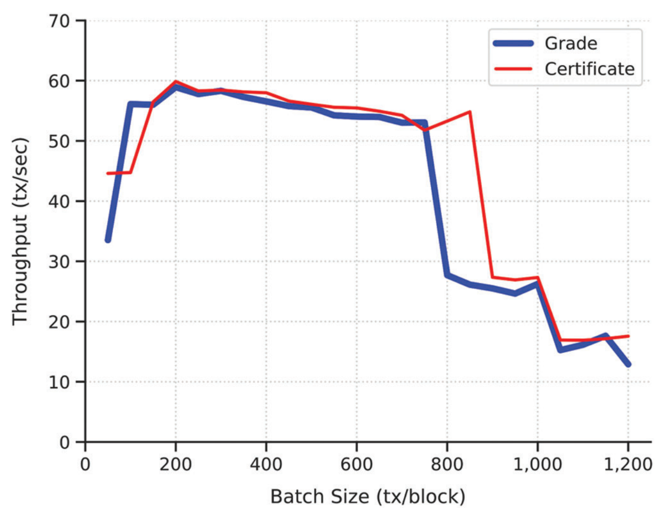


Figure 8: Effect of batch size on writing data

Next, we utilize JMeter tool to measure the data reading capability on the Sawtooth network. In this experiment, we concurrently generate requests for reading transactions within one minute. The experiment is repeated ten times to get average values. Fig. 9 depicts that the TPS decreases slightly from 610 to 521 tx/s when the number of concurrent requests increases from 100 to 500. The concurrent reading speed decreases because the capacity of each network node is limited; hence the requests that come later will have to wait in line to be served.

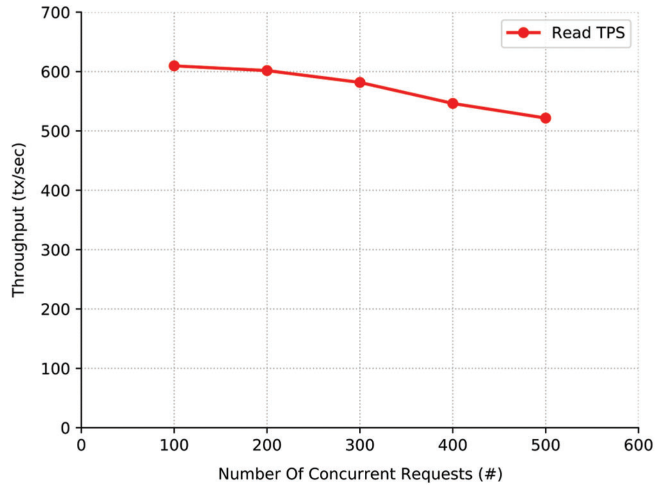
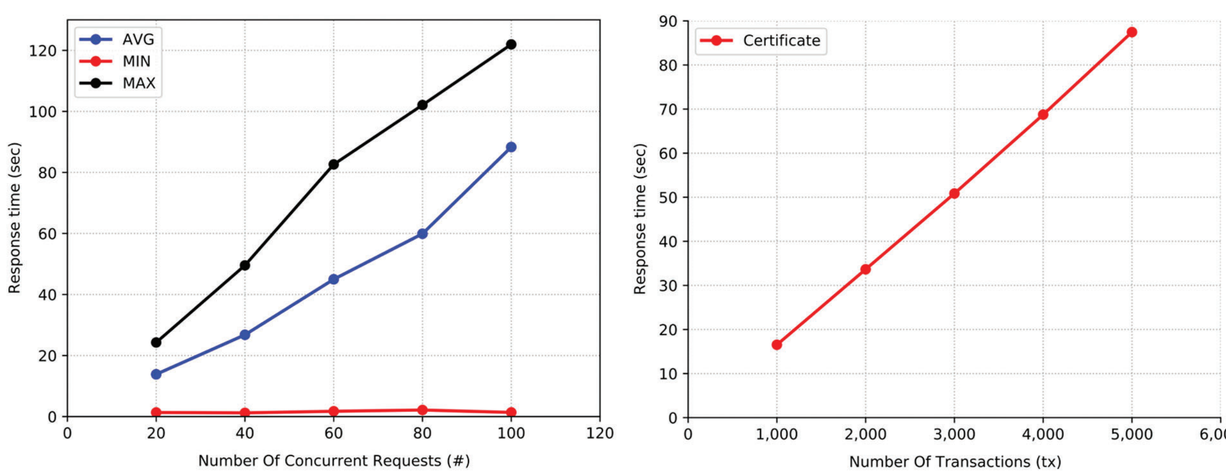


Figure 9: Throughput for reading data

Finally, we measure the consuming time for writing grades and certificates. First, we assume that there are n lecturers simultaneously writing scores on the blockchain network; each generates 50 transactions for 50 students. Fig. 10a shows the response times for this experiment. The red and black lines show the time to get the first and last responses, whereas the blue line shows the average waiting time. For example, when having 100 lecturers writing scores at the same time, the average waiting time is 88 s. Next, Fig. 10b shows the response time when writing multiple certificates on the blockchain. In case of uploading 5,000 certificates, the university needs to wait 87 s.



(a) (b)

Figure 10: Response time for writing data. (a) Write grade (b) Write certificate

5 Conclusion

In this paper, we present B4E–a national system used for verification and management of lifelong learning data. In particular, B4E has the participation of management organizations (e.g., ministry of education, departments of education), educational institutions (e.g., universities, high schools), lecturers, students, and verifiers. To store data, B4E relies on a private blockchain network to allow it to write a huge number of educational data, including certificates, transcripts, and educational programs, etc., in a private, cost-effective, and high-speed manner. In addition, B4E provides an additional authentication layer through the linkage between training history and the certificate obtained. As a result, B4E can address the fake certificate problem and create a complete learning record for each person. We also develop utilities and functionalities to enhance transparency and trust of B4E. Our experiments show that B4E meets expectations for deployment in reality.

In the future, we plan to develop the system with new functionalities such as warning mistakes and providing statistics and evaluation of the learning data. In addition, developing APIs to provide certified data on the system to other systems such as CV is necessary. Finally, we also consider the connection between B4E and existing solutions to gain acceptance of our solution.

Funding Statement: This research was supported by the Vietnamese MOET's project "Researching and applying blockchain technology to the problem of authenticating the certificate issuing process in Vietnam", No. B2020-BKA-14.

Conflicts of Interest: The authors declare that they have no conflicts of interest to report regarding the present study.

References

[1] Association of Certified Fraud Examiners, "Report to the nations–global study on occupational fraud and abuse," 2020. [Online]. Available: https://www.acfe.com/report-to-the-nations/2020/.

[2] Tuoi Tre News, "Officials found using fake degrees issued by university in Hanoi," 2020. [Online]. Available: https://tuoitrenews.vn/news/education/20201126/officials-found-using-fake-degrees-issued-by-university-in-hanoi/57970.html.

[3] Blockcerts, "The open standard for blockchain certificates," 2016. [Online]. Available: https://www.blockcerts.org/about.html.

[4] Blockchain Certified Data, "Digital credentials on the blockchain," 2021. [Online]. Available: https://www.bcdiploma.com/en.

[5] Singapore Government Developer Portal, "Opencerts–an easy way to check and verify your certificates," 2021. [Online]. Available: https://www.developer.tech.gov.sg/technologies/blockchain/opencerts.

[6] D. Puthal, N. Malik, S. P. Mohanty, E. Kougianos and G. Das, "Everything you wanted to know about the blockchain: Its promise, components, processes, and problems," *IEEE Consumer Electronics Magazine*, vol. 7, no. 4, pp. 6–14, 2018.

[7] G. Wood, "Ethereum: A secure decentralised generalised transaction ledger," *Ethereum Project Yellow Paper*, vol. 151, pp. 1–32, 2014.

[8] S. Nakamoto, "Bitcoin: A peer–to–peer electronic cash system," 2008. [Online]. Available https://bitcoin.org/bitcoin.pdf.

[9] K. Olson, M. Bowman, J. Mitchell, S. Amundson, D. Middleton *et al.,* "Sawtooth: An introduction," 2018. [Online]. Available: https://www.hyperledger.org/wp-content/uploads/2018/01/Hyperledger_Sawtooth_WhitePaper.pdf.

[10] G. Kumar, R. Saha, W. J. Buchanan, G. Geetha, R. Thomas *et al.,* "Decentralized accessibility of e-commerce products through blockchain technology," *Sustainable Cities and Society*, vol. 62, pp. 1–9, 2020.

[11] A. Vangala, A. K. Das, N. Kumar and M. Alazab, "Smart secure sensing for iot-based agriculture: Blockchain perspective," *IEEE Sensors Journal*, vol. 21, no. 16, pp. 17591–17607, 2020.

[12] W. Wang, C. Qiu, Z. Yin, G. Srivastava, T. R. Gadekallu *et al.,* "Blockchain and puf-based lightweight authentication protocol for wireless medical sensor networks," *IEEE Internet of Things Journal*, 2021. https://ieeexplore.ieee.org/document/9559388.

[13] H. Xiong, C. Jin, M. Alazab, K. -H. Yeh, H. Wang *et al.,* "On the design of blockchain-based ecdsa with fault-tolerant batch verication protocol for blockchain-enabled iomt," *IEEE Journal of Biomedical and Health Informatics*, 2021. https://ieeexplore.ieee.org/document/9540329.

[14] M. M. Ahmed, M. K. Hasan, M. Shafiq, M. O. Qays, T. R. Gadekallu *et al.,* "A Peer-to-peer blockchain based interconnected power system," *Energy Reports*, vol. 7, pp. 7890–7905, 2021.

[15] W. Gräther, S. Kolvenbach, R. Ruland, J. Schütte, C. Torres *et al.*, "Blockchain for education: Lifelong learning passport," in *Proc. of 1st ERCIM Blockchain Workshop*, Amsterdam, Netherlands, 2018.

[16] F. Schär and F. Mösli, "Blockchain diplomas: Using smart contracts to secure academic credentials," *Journal of Higher Education Research*, vol. 41, no. 3, pp. 48–59, 2019.

[17] H. A. Deenmahomed, M. M. Didier and R. K. Sungkur, "The future of university education: Examination, transcript, and certificate system using blockchain," *Computer Applications in Engineering Education*, vol. 29, no. 1, pp. 1–23, 2021.

[18] J. Gresch, B. Rodrigues, E. Scheid, S. S. Kanhere and B. Stiller, "The proposal of a blockchain-based architecture for transparent certificate handling," in *Proc. of the Int. Conf. on Business Information Systems*, Berlin, Germany, pp. 185–196, 2018.

[19] Q. Aini, U. Rahardja, M. R. Tangkaw, N. P. L. Santoso and A. Khoirunisa, "Embedding a blockchain technology pattern into the qr code for an authentication certificate," *Jurnal Online Informatika*, vol. 5, no. 2, pp. 239–244, 2020.

[20] D. H. Nguyen, D. N. Nguyen-Duc, N. H. Tuong and H. A. Pham, "Cvss: A blockchainized certificate verifying support system," in *Proc. of the Ninth Int. Symp. on Information and Communication Technology*, Danang, Vietnam, pp. 436–442, 2018.

[21] 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.

[22] J. Benet, "IPFS-content addressed, versioned, p2p file system," 2014. [Online]. Available: https://arxiv.org/abs/1407.3561.

[23] D. Sachdev, A. Khanna, S. K. Pokhriyal, S. S. Sundaram and T. Choudhury, "Education 4.0: A systematic industrial case based review of barriers and applications of decentralized trust using blockchain," *Psychology and Education Journal*, vol. 57, no. 8, pp. 882–893, 2020.

[24] Auth0, "Introduction to json web tokens," 2021. [Online]. Available: https://jwt.io/introduction.

[25] M. Castro and B. Liskov, "Practical byzantine fault tolerance," *ACM Transactions on Computer Systems (TOCS)*, vol. 20, no. 4, pp. 398–461, 2002.

[26] Apache Foundation, "Apache jmeter," 2021. [Online]. Available: https://jmeter.apache.org/.