BEdShare: A Scalable and Privacy Preserving Blockchain Scheme for Education Credentials Sharing and Verification in Nigeria

Abdurrashid Ibrahim Sanka[1], Adamu Sani Yahaya[2,*], Aminu Rabiu Ladodo[3], Bashir Yusuf Bichi[4], Sagir Lawal[5] and Farouk Lawan Gambo[6]

[1]Department of Electrical Engineering,
Bayero University, Kano, Nigeria

[2]Department of Information Technology,
Bayero University, Kano, Nigeria

[3]Department of Electrical/Electronic Engineering,
Nigerian Defence Academy, Kaduna, Nigeria

[4]Department of Computer Science,
Kano University of Science and Technology, Wudil, Kano, Nigeria

[5]Department of Accounting,
Nigeria Police Academy Wudil, Kano Nigeria

[6]Department of Computer Science, Federal University Dutse, Jigawa, Nigeria

Corresponding Author: asyahaya.it@buk.edu.ng

Abstract
Blockchain technology is a powerful emerging tool that transforms and improves existing systems with better performance, security, computational cost-saving, transparency, and traceability. It evicts central authorities and grants systems autonomy. On the other hand, sharing and verifying education credentials are arduous tasks that take time and costs. This paper proposes a scalable blockchain scheme that simplifies sharing and verification of education credentials globally with complete privacy preservation. We propose a scalable scheme and use the interplanetary file system database to scale the blockchain for better performance and storage. The scheme also adopts access controls and encryption schemes for privacy preservation. The blockchain prototype is implemented on the Hyperledger Fabric blockchain platform. The performance is measured using the Hyperledger Caliper that shows the prototype system achieves good performance scalability.

Keywords: Blockchain, Credentials, Education, Scalability, and Privacy

INTRODUCTION

Blockchain technology has emerged as a powerful and beneficial technology capable of disrupting many systems and industries to enhance their performance and bring new values [1]. Blockchain works without the need for central authorities or intermediaries [2]. It provides autonomy, speed, cost savings, data security, privacy, transparency, and efficiency. For these and more reasons, several companies and countries adopt the technology to improve their systems. Bitcoin was the first application of blockchain developed as a peer-to-peer cash payment system in 2008 by Satoshi Nakamoto [3]. Other several blockchain applications appear after realizing the success of Bitcoin and the capabilities of blockchain technology.

Nowadays, blockchain has seen significant adoptions. Deloitte's *et. al* survey revealed that blockchain would finally reach mainstream adoption [4]. Price Waterhouse Coopers (PwC) also forecasted that the global Gross Domestic Product (GDP) would be on the blockchain, and the blockchain GDP will reach $2.58 billion by 2025 [5]. Currently, there is a large number of blockchain use cases, and many are on trial. IBM, Microsoft and Oracle all have blockchain cloud platforms, and partners in developing several blockchain platforms like the Hyperledger. Corda is a blockchain platform of R3, which is a consortium of over 200 financial institutions globally [6]. Maersk and over half of global shipping companies use a blockchain platform Trade-lens for their supply chain. Estonia, Georgia, UAE, USA, UK, and many countries use blockchain for the betterment of their systems, such as the healthcare in Estonia and the land registry in Georgia [7].

On the other hand, education sharing and verification experience delays, monetary cost, privacy, and data loss issues are not addressed. To verify an applicant's credentials, institutions and companies have to wait for the credentials to be sent from the applicant's institutions upon request. Normally, the applicant makes the request and has to pay some processing fees. Due to inefficiencies and the large queue of similar requests, the process takes an unimaginable long time for the certified credentials to be produced and sent to the requesting institution or company. Secondly, the applicant institutions use a centralized model, which causes a single point of failure. Moreover, data loss may occur due to an attack or system failure. A security breach can also lead to privacy issues in which applicants' credentials may be leaked to unintended persons. Luckily enough, most of the issues mentioned can be resolved using blockchain technology.

This paper proposes a scalable and privacy preserving blockchain-based scheme, BEdShare, to efficiently share and verify education credentials across the globe. The scheme preserves privacy through access control and encryption. Due to the inherent scalability issue in blockchain, we use the InterPlanetary File System (IPFS) to reduce the size of the blockchain data as well as improve

its storage scalability. Institutions can directly and securely verify education credentials without the interference of the awarding institutions. The credentials are shared with the awardees using symmetric key encryption, i.e., Advanced Encryption Standard 128 (AES-128). The system performance was evaluated and found to be scalable and efficient. Our contributions are summarized as follows:

1. We review the bottlenecks in education credentials sharing and verification.
2. We give an overview of blockchain technology.
3. We propose a scalable blockchain scheme for global sharing and verification of education credentials
4. We propose a secure use of IPFS to further scale the system by reducing its size.
5. We propose an access control and encryption to preserve privacy in the scheme.

The rest of the paper is organized as follows: Section II gives the background of blockchain technology, education sharing and verification methods, and related work. Section III discusses the proposed blockchain scheme. Section IV discusses the system's implementation and performance evaluation, while the conclusion is made in section V.

BACKGROUND

In this section we give the general overview of blockchain technology and also review related work.

Blockchain Architecture

Blockchain is a distributed and decentralized technology that originated from Bitcoin cryptocurrency proposed by Satoshi Nakamoto in 2008 [3]. In a nutshell, blockchain is a distributed ledger linked in a decentralized fashion [8]. It contains blocks grouped during transactions. The blocks are cryptographically hashed and connected to generate the blockchain. Every block contains a hash that is directly pointing to its previous block. Moreover, with the help of a consensus protocol, new blocks are connected to the chain and validated. Blockchain automatically detects any modifications in its data, and everyone can see and verify the transactions in a block.

As shown in Figure 1, each block of a blockchain contains the block header and the transaction data. The block header contains elements such as the timestamp, nonce, previous block hash, and Merkle root. On the other hand, the transaction data contains all the transactions in the block. These transactions contain signatures and other data. In Bitcoin, there can be over 2000 transactions per block. Blocks are ordered in chronological order such that they are searched by their height or hash values.

At the start, the technology was directly connected with cryptocurrencies and was known as blockchain 1.0. The emergence of smart contracts brought the surge of blockchain 2.0. Several blockchain solutions have been developed with a rapidly growing interest in blockchain in many

industries and businesses due to the essential benefits of blockchain characteristics. Blockchain characteristics include decentralization, speed, immutability, transparency, and more [9].

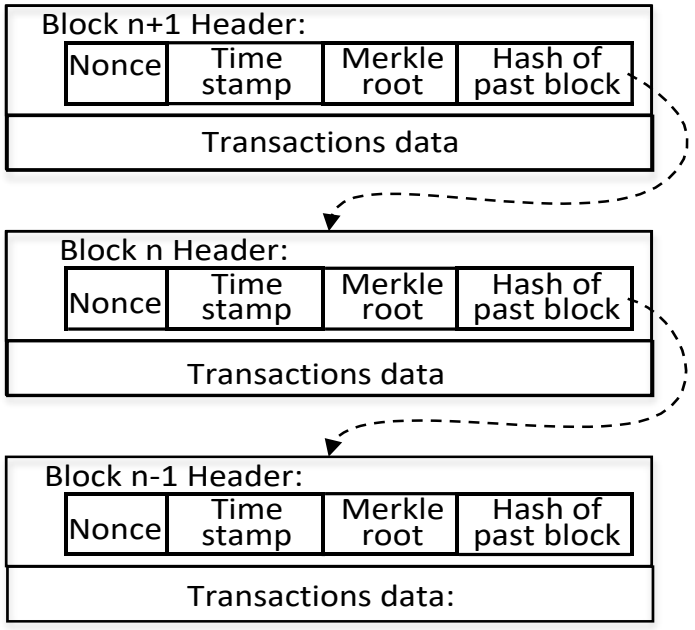

Figure 1: Blockchain structure

Types of Blockchain

Blockchain has been classified into three, namely the open or public, private, and consortium blockchains. The public blockchain is permissionedless, while the private and consortium blockchains are permissionedless [10].

1. Public blockchain: All participants verify transactions and participate in the consensus processes without prior permission in a public blockchain. A well-known example of a public blockchain is Bitcoin.
2. Private blockchain: In this type of blockchain, participation requires prior permission. Only a few known nodes participate in block creation, and the other nodes will have restrictions in terms of data access. Private blockchains are owned by a single organization. Multichain is a typical example of private blockchain.
3. Consortium blockchain: This blockchain also requires permission for participation and is formed by a group of organizations (consortium). Some nodes are identified and given higher priority than others in consortium blockchain. These nodes usually have higher computing power than the normal nodes. One example of a consortium blockchain is Hyperledger Fabric.

RELATED WORK

The initiation of certificate management systems through blockchain technology is not limited to a specific group of researchers or geographical location. It is distributed from the Americas, Europe, and to Asia; as discussed in the previous works [11]-[16]. While, African countries are still working with the conventional management system, leading to a single point of failure, security, privacy, and scalability concerns. Furthermore, the existing system is identified as costly, manually intensive, time-consuming, and inefficient. These issues bring attention to the certificate forgery problem that is a huge concern in the system and affects the community in various ways [16]. Surveys show significant issues with certification information presented in job and other applications, i.e., fraudulent and forgery information.

Universities can provide some verification methods to minimize the issues. However, the methods still suffer from a lack of unification and standardization [12]. Blockchain technology is a potential solution to enhance the process, achieve decentralization, bring added efficiency, increase transparency, and reduce certification fraud. It is also used to establish a global document verification system [16]. Its immutability feature reduces the risk of information loss and enhances credibility [3]. From the students' perspective, the system can simplify tasks when validating students' documents and also remove the third party in the process [9]. On the other hand, from the university's perspective, its validation and issuance solutions can be advantageous, e.g., joint degree, internationalization programs, and international student application reducing costly processes and administrative tasks.

In [17], the authors identify the security themes needed for verification of documents in the blockchain. They also identify the loopholes and gaps in the present educational certificate verification solution based on blockchain models. Finally, they also propose a blockchain model for checking the educational certificates considering ownership, privacy, confidentiality, authorization, and authentication. The authors in [18] analyze blockchain privacy, trust, and security. They further discuss the application of blockchain technology in the educational sector and their present problems. The authors propose a reliable and secure blockchain model that manages students' records.

In [19], the authors develop a Qualichain platform that offers educational qualifications, which focus on the blockchain technology potentials and conducts data analysis that supports the curriculum optimization method. The authors in [20] propose a blockchain-based framework for digital academic records verification. Also, in the proposed work, a proof of concept is implemented as the consensus mechanism. In [21], the authors propose a blockchain-based certification verification platform that is incorporated with a cloud server. The proposed platform is capable of

providing publicly and immutably verifiable transactions.

The authors in [22] evaluate the role of e-learning based on blockchain technology. In the research, implications, prospects, and challenges of implementing the new technology are discussed. However, these related works do not consider the inherent scalability issue of the blockchain. In contrast, we propose a scalable and secure blockchain scheme based on IPFS and AES encryption for education credential verification and sharing.

BEdShare Design Methodology

In this section, we discuss the design and architecture of our proposed BEdShare system. The system will allow institutions including university, companies and ministries to easily share and verify education certificates and transcripts against the traditional system. Figure 2 and Figure 3 show BedShare architecture and its activity diagram, respectively.

BEdShare Architecture

BEdshare is designed so that the system will be secure, scalable, and guarantees privacy. Figure 2 shows the architecture of BEdShare. The system consists of the blockchain network, which comprises of the certificate issuing institutions (CIIs), certificate verifying institutions (CVI), the network peers, validators (endorsers), and the certificate authorities (CA). The other entities in the system are the students and the IPFS storage system. The working of the scheme is described using the steps as follows:

Assuming a certificate 'A' is awarded to a student 'B' from a CII. In the first step (step 1), the CII generates the SHA-256 hash of the certificate (cert_hash) and encrypts the certificate using an AES symmetric key (k) to be shared with the student later. The CII uploads the encrypted certificate (AES (cert)) on the IPFS data storage in step 2. In step 3, the CII uploads the address of the certificate (cert_addr) and its hash value (cert_hash) to the blockchain by submitting a new blockchain transaction. The transaction creates a new record on the blockchain and will be used later by the CVI to retrieve the data on the IPFS. The CII records the transaction ID (tran_id) before sending it to the student. In step 4, the CII sends the symmetric key and the transaction ID (k + tran_id) to the student for his record. When a CVI requires getting and verifying the student's certificate, they request the key and the transaction ID from the student in step 5. In step 6, the student responds with the key and the certificate's transaction ID (k + tran_id). The CVI uses the transaction ID and downloads the transaction from the blockchain in step 7 and 8. They then extract the IPFS address of the encrypted certificate and its hash value. In step2 9 and 10, the CVI retrieves the encrypted certificate from the IPFS using the address obtained from the blockchain. They get the certificate by decrypting the encrypted certificate using the symmetric key obtained from the student. The CVI finally computes the certificate's SHA-256 hash and compares it with the hash obtained from the blockchain. If the hashes are the

same, the certificate is verified; otherwise, it is rejected.

The Certificate Authorities (CA)

For security purposes, we selected a permissioned blockchain for BEdShare. The network participants are authorized and permitted before joining the blockchain network. Hence, a CA is required for the system. The CA is responsible for registering the network participants upon request. He also issues the digital certificates, keys, and permissions required for carrying activities in the network, including reading and writing the blockchain ledger.The BedShare CA in Nigeria could be formed by representatives from the various national education overseers such as the National University Commission (NUC), National Board for Technical Education (NBTE), Ministry of Education, and the Joint Admissions and Matriculation Board (JAMB). These entities provide the delegates who run the affairs of CA of this blockchain network. Every institution, agency, ministry, company, or business interested in joining the network submits its permission request formally to the CA office. The CA then verifies its submission and checks if it meets the joining requirements before issuing the certificates and keys to the applicant.

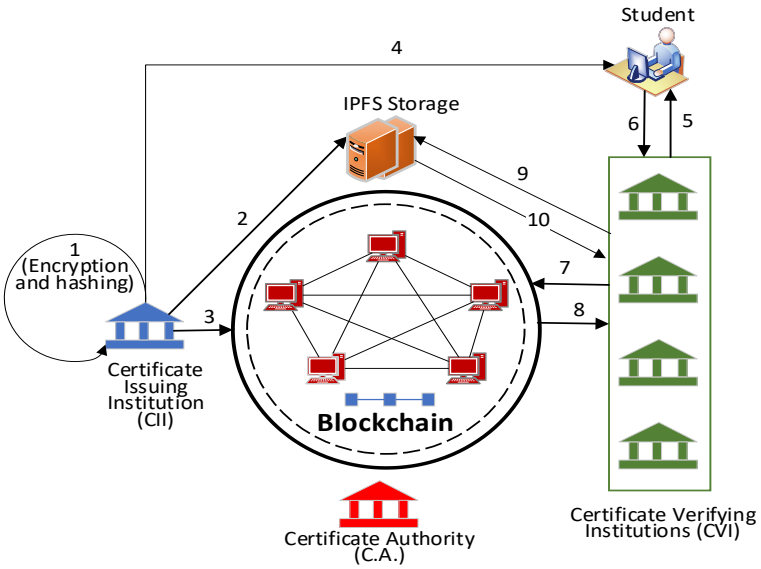

Figure 2: BEdShare Architecture

The Certificate Issuing Institution (CII)

The CIIs are the various institutions that offer certificates to students. The certificates may be required for jobs or other appointments and registrations by other institutions. In Nigeria, verifiable certificates are issued by universities, polytechnics, colleges, and examination bodies such as the JAMB, West African Examination Council (WAEC), and the Nigerian Examination Council (NECO).

In BEdShare, a certificate refers to both the education certificate and associated transcripts. For some institutions such as JAMB or WAEC, it will only be a

UTME certificate, while for universities and polytechnics; it is a combination of a certificate and its transcript. However, the hash of each document is computed separately. The hashes of the files are put together in a single transaction and uploaded to the blockchain. Hence a verifier may like to verify only a certificate or a transcript, or both.

The Certificate Verifying Institution (CVI)

The CVI is the institution that wants to verify and have a copy of the student's certificates for a job or other purposes. They can be other universities, polytechnics, companies, or other participants in the blockchain network. For security and privacy purpose, these institutions need to request the symmetric key of the encrypted certificate on the IPFS. Hence only the institutions having the key can open and read the certificate on the IPFS. Upon his approval, the student provides the required information (the symmetric key and the transaction ID) for the CVI to retrieve and verify his certificates.

The Interplanetary File System (IPFS) Storage

IPFS is a distributed storage system where the storage of a piece of data is shared among the members of the distributed network (using a distributed hash table and the content-addressable memory) instead of the traditional centralized storage system. If 10 MB of data is to be stored on an IPFS of 5 Members of equal capacity, therefore, each member will store 2 MB of the data. A user software automatically uses the addresses of the data to fetch and combine the actual data. IPFS provides more security over a central data storage system. It also reduces the storage overheads of enormous data systems such as blockchain.

IPFS is used in BEdShare to scale the blockchain based on storage by reducing its huge storage requirement. Instead of each blockchain node storing the huge blockchain data, the data is hence stored on the IPFS, where its storage burden is shared among several nodes. For fear of privacy and security issues, the education certificates are encrypted before uploading on the IPFS. In this way, the confidentiality of the stored certificates is protected since only the intended user can download and decrypt the certificate to see its content. The hash of the data is compared with the original hash stored on the blockchain to ensure the integrity of the certificates.

The blockchain network

The blockchain network facilitates the sharing and verification of the education certificates. It allows the CVI to verify and ensure the integrity of the certificates by comparing the stored hash on the blockchain and the hash of the retrieved document from the storage server. It also eases the certificate verifications as well as improves its speed. The certificates could be retrieved and verified as soon as they are uploaded on the blockchain. The blockchain is made up of the CA, education ministries/agencies and parastatals, CIIs, and CVIs. These entities each run a full blockchain node, thus keeping all the blockchain

transaction records for security, efficiency, and transparency.

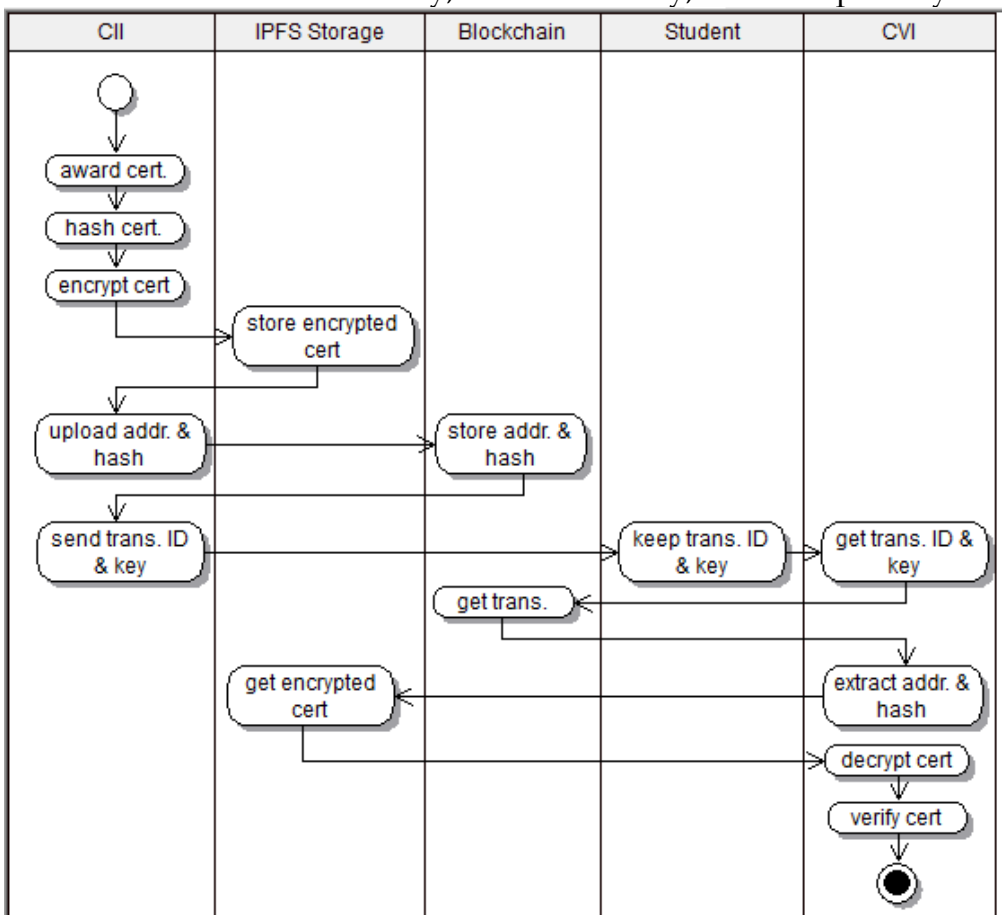

Figure 3: Activity diagram of BEdShare

Implementation and Discussion of Results

Implementation

The prototype of the propose blockchain framework was implemented using Hyperledger Fabric platform. The Hyperledger Fabric provides the platform and tools for the implementation of private and consortium blockchains. The BEdShare blockchain network prototype was implemented on a Dell precision server desktop having 8GB RAM, 500GB hard disk, Intel processor and running Windows Operating system. To run the network on Linux system, Vagrant tool and an Oracle Virtual Box was used to provide the Ubuntu8 OS environment which was used for the network implementation and testing.

We used the 'cryptogen' tool provided by the Fabric to generate the cryptographic materials (i.e. digital certificates and keys) required for the network member identification and the member service provider (MSP). Furthermore, the prototype was implemented to have six nodes and an ORDERER node. Each of the nodes in the prototype represents a chosen institution in Nigeria acting as a participant in the network. The nodes

were created in docker containers using a docker-compose file for the creation of independent nodes. Finally, a sample chaincode was packed, installed, approved, and committed following the right order of the Fabric chaincode life cycle. The network performance was then measured using the Hyperledger Caliper tool based on the installed chaincode.

Figure 3 shows a snapshot of the network creation. It could be seen from the figure that six nodes and an orderer node were created and up running. In addition, Figure 4 shows the network status after all the nodes and channel creations. It shows the container IDs of the nodes together with their PORT numbers.

```
================ Launch the network ================
Creating network "bedshare_BEdShareNet" with the default driver
Creating volume "bedshare_orderer.bayerouniversity.com" with default driver
Creating volume "bedshare_bayero-peer1.bayerouniversity.com" with default driver
Creating volume "bedshare_abu-peer1.abuuniversity.com" with default driver
Creating volume "bedshare_kust-peer1.kustuniversity.com" with default driver
Creating volume "bedshare_fud-peer1.fuduniversity.com" with default driver
Creating volume "bedshare_northwest-peer1.northwestuniversity.com" with default driver
Creating volume "bedshare_unilag-peer1.unilaguniversity.com" with default driver
Creating cli                                ... done
Creating orderer.bayerouniversity.com ... done
Creating northwest-peer1.northwestuniversity.com ... done
Creating unilag-peer1.unilaguniversity.com       ... done
Creating bayero-peer1.bayerouniversity.com       ... done
Creating fud-peer1.fuduniversity.com             ... done
Creating abu-peer1.abuuniversity.com             ... done
Creating kust-peer1.kustuniversity.com           ... done
CONTAINER ID        NAMES                                       STATUS
71f1164a0b1f        kust-peer1.kustuniversity.com               Up 5 seconds
ebe83ea60c1e        abu-peer1.abuuniversity.com                 Up 6 seconds
c9e97bf42be1        unilag-peer1.unilaguniversity.com           Up 6 seconds
b3e6384b7d92        bayero-peer1.bayerouniversity.com           Up 6 seconds
f974ed777caa        fud-peer1.fuduniversity.com                 Up 6 seconds
0e1459abdb15        northwest-peer1.northwestuniversity.com     Up 5 seconds
c913a4d9ad61        orderer.bayerouniversity.com                Up 8 seconds
af64f1477645        cli                                         Up 8 seconds
=== Submitting txn for BEdShareNetchannel creation as ABU University Admin ======
```

Figure 4: Evidence of the network creation

```
vagrant@vagrant:/vagrant/network/bin$ docker ps -a --format="table {{.ID}}\t{{.Names}}\t{{.Status}}\t{{.
CONTAINER ID   NAMES                                       STATUS          PORTS
71f1164a0b1f   kust-peer1.kustuniversity.com               Up 6 minutes    0.0.0.0:7055->7055/tcp, 7051/tcp,
ebe83ea60c1e   abu-peer1.abuuniversity.com                 Up 6 minutes    0.0.0.0:7054->7054/tcp, 7051/tcp,
c9e97bf42be1   unilag-peer1.unilaguniversity.com           Up 6 minutes    7051/tcp, 0.0.0.0:7062-7064->7062
b3e6384b7d92   bayero-peer1.bayerouniversity.com           Up 6 minutes    0.0.0.0:7051-7053->7051-7053/tcp
f974ed777caa   fud-peer1.fuduniversity.com                 Up 6 minutes    7051/tcp, 0.0.0.0:7056-7058->7056-
0e1459abdb15   northwest-peer1.northwestuniversity.com     Up 6 minutes    7051/tcp, 0.0.0.0:7059-7061->7059-
c913a4d9ad61   orderer.bayerouniversity.com                Up 6 minutes    0.0.0.0:7050->7050/tcp
af64f1477645   cli                                         Up 6 minutes
vagrant@vagrant:/vagrant/network/bin$
```

Figure 5: Status of the created network

Table I: BEdShare performance evaluation result

Name	Send Rate (TPS)	Max Latency (s)	Min Latency (s)	Avg Latency (s)	Throughput (TPS)
ChangeRecord	325.8	4.24	0.46	2.50	325.7
QueryAllRecords	372.6	0.17	0.01	0.04	372.5
QueryARecord	317.8	1.32	0.01	0.20	317.6

Table II: Computational cost comparison between the proposed and existing encryption techniques

Techniques	Proposed technique	3-DES
Encryption	35 ms	200 ms
Decryption	20 ms	161 ms

DISCUSSION OF RESULTS

The network was setup and ran successfully. The chaincodes is also installed and tested working successfully. The chaincodes facilitate the read and write operations on the blockchain. Hyperledger Caliper tool is used to take the network performance results. We provide the benchmark and the network configuration files in addition to the workload nodejs sources for the test. We send 1500 transactions for both query (read) and invoke (write) requests. Table I shows the performance evaluation results. The results show a performance of 325 transactions per second (TPS) and 372.5 TPS for the invoke and query requests respectively. We expect the full network implementation under high performance computers to reach up to 3500TPS as achieved by the hyperledger Fabric. Our system achieves better performance when compared to Bitcoin and Ethereum having a throughput of 3-4 TPS and 15-20 TPS, respectively.

Privacy and security analysis

We used a permissioned blockchain to provide the desired privacy and security for the system. Only authorized participants can join the network as well as read or write the blockchain. Hence the system is protected against several security attacks such as the 51% attack, eclipse attack, and selfish mining attacks. The system inherits all the useful features of the blockchain, including data integrity, immutability, authentication, anonymity, and transparency.

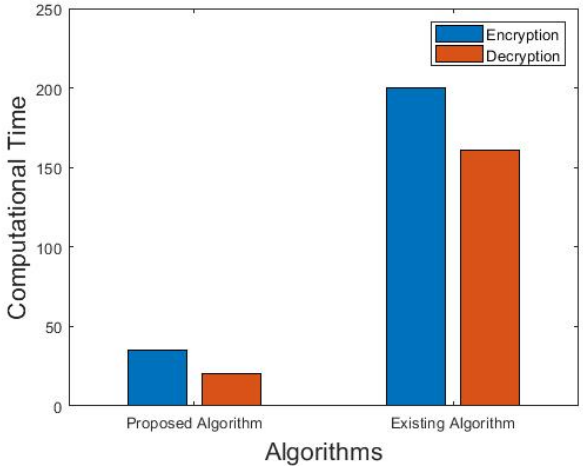

Figure 6: Comparison of computational time

Because we use IPFS storage for the certificates storage, we provide additional security and privacy by encrypting the certificates using symmetric key encryption (AES) on top of the security of the IPFS and that of the blockchain. Hence only the authenticated participants having the symmetric key pair can view the certificate content. The comparison between the proposed encryption technique and the existing technique is presented in Table II and Figure 5. The techniques are compared in terms of computational cost. The table shows that the existing technique has a higher computational cost for encryption and decryption processes than the proposed technique. This shows that the proposed technique is better than the techniques and can increase the system efficiency. Moreover, the encryption process helps preserve the privacy of the data and reduces the rate of malicious activities.

CONCLUSION

In this paper, a scalable and privacy preserving blockchain based scheme is proposed, which simplifies sharing and verification of education credentials in Nigeria. In the model, an IPFS storage is proposed to improve the scalability of the blockchain for better performance and reducing the storage overhead. Access control and encryption technique are used to improve the security of the system and provide system's privacy. The performance measured using the Hyperledger Caliper shows that the prototype system achieves good performance scalability. Moreover, the proposed encryption technique shows better performance in terms of computational cost than the existing technique.

REFERENCES

[1] Cao, Bin, Zhenghui Zhang, Daquan Feng, Shengli Zhang, Lei Zhang, Mugen Peng, and Yun Li. "Performance analysis and comparison of PoW, PoS and DAG based blockchains." Digital Communications and Networks (2020): 1-25.

[2] Zhang, Shijie, and Jong-Hyouk Lee. "Analysis of the main consensus

protocols of blockchain." ICT express 6, no. 2 (2020): 93-97.

[3] Nakamoto, Satoshi. "Bitcoin: A peer-to-peer electronic cash system." Decentralized Business Review (2008): 21260.

[4] Deloitte. 2019. Blockchain technology use cases in organizations worldwide as of October 2021. Statista. Available at https://www2.deloitte.com/content/dam/Deloitte/se/

[5] PwC 2021. Statista. Available as of October 2021 at https://www.pwc.com/gx/en/news-room/press-releases/2020/blockchain-boost-global-economy-track-trace-trust.html

[6] Valenta, Martin, and Philipp Sandner. "Comparison of ethereum, hyperledger fabric and corda." ebook Frankfurt School, Blockchain Center (2017).

[7] maersk tradelens blockchain Available as of October 2021 at https://www.maersk.com/apa-tradelens

[8] Cheng, Jiin-Chiou, Narn-Yih Lee, Chien Chi, and Yi-Hua Chen. "Blockchain and smart contract for digital certificate." In 2018 IEEE international conference on applied system invention (ICASI), pp. 1046-1051. IEEE, 2018.

[9] Kamisalic, Aida, Muhamed Turkanovic, Sasa Mrdovic, and Marjan Hericko. ``A preliminary review of blockchain-based solutions in higher education.'' In International workshop on learning technology for education in cloud, pp. 114-124. Springer, Cham, 2019.

[10] Cachin, Christian, and Marko Vukolić. "Blockchain consensus protocols in the wild." arXiv preprint arXiv:1707.01873 (2017).

[11] Duan, Bin, Ying Zhong, and Dayu Liu. "Education application of blockchain technology: Learning outcome and meta-diploma." In 2017 IEEE 23rd International Conference on Parallel and Distributed Systems (ICPADS), pp. 814-817. IEEE, 2017.

[12] Vidal, Fernando, Feliz Gouveia, and Christophe Soares. "Analysis of blockchain technology for higher education." In 2019 International Conference on Cyber-Enabled Distributed Computing and Knowledge Discovery (CyberC), pp. 28-33. IEEE, 2019.

[13] Vidal, Fernando, Feliz Gouveia, and Christophe Soares. "Analysis of blockchain technology for higher education." In 2019 International Conference on Cyber-Enabled Distributed Computing and Knowledge Discovery (CyberC), pp. 28-33. IEEE, 2019.

[14] San, Aye Mi, Nopporn Chotikakamthorn, and Chanboon Sathitwiriyawong. "Blockchain-Based Learning Credential Verification System with Recipient Privacy Control." In 2019 IEEE International Conference on Engineering, Technology and Education (TALE), pp. 1-5. IEEE, 2019.

[15] Nikolskaia, Kseniia, Daria Snegireva, and Aleksey Minbaleev. "Development of the application for diploma authenticity using the blockchain technology." In 2019 International Conference Quality Management, Transport and Information Security, Information Technologies (IT\&QM\&IS), pp. 558-563. IEEE, 2019.

[16] Serranito, Diogo, Andre Vasconcelos, Sergio Guerreiro, and Miguel Correia. "Blockchain ecosystem for verifiable qualifications." In 2020 2nd Conference on Blockchain Research \& Applications for Innovative Networks and Services (BRAINS), pp. 192-199. IEEE, 2020.

[17] Saleh, Omar S., Osman Ghazali, and Muhammad Ehsan Rana. "Blockchain based framework for educational certificates verification." Studies, Planning and Follow-up Directorate. Ministry of Higher Education and Scientific Research, Baghdad, Iraq. School (2020).

[18] Alam, Shadab. "A Blockchain-based framework for secure Educational Credentials." Turkish Journal of Computer and Mathematics Education (TURCOMAT) 12, no. 10 (2021): 5157-5167.

[19] Cahyadi, Dede, Adam Faturahman, Hendriyanti Haryani, and Ellen Dolan. "BCS: Blockchain Smart Curriculum System for Verification Student Accreditation." International Journal of Cyber and IT Service Management 1, no. 1 (2021): 65-83.

[20] Aamir, Muhammad, Rehan Qureshi, Furqan Ali Khan, and Muhammad Huzaifa. "Blockchain Based Academic Records Verification in Smart Cities." Wireless Personal Communications 113, no. 3 (2020).

[21] Hasan, Mahmudul, Anichur Rahman, and Md Jahidul Islam. "Distb-cvs: A distributed secure blockchain based online certificate verification system from bangladesh perspective." In 2020 2nd International Conference on Advanced Information and Communication Technology (ICAICT), pp. 460-465. IEEE, 2020.

[22] Pfeiffer, Alexander, Stephen Bezzina, Thomas Wernbacher, and Simone Kriglstein. "Blockchain Technologies for the Validation, Verification, Authentication and Storing of Students' Data." In European Conference on e-Learning, pp. 421-XIX. Academic Conferences International Limited, 2020.