A Blockchain Framework for Academic Certificates Authentication

Ruqaya Abdelmagid[1], Mohamed Abdelsalam[2], Fahad Kamal Alsheref[3]
Business Information Systems Dept.-Faculty of Commerce and Business Administration, Helwan University, Cairo, Egypt[1, 2]
Information Systems Dept.-Faculty of Computer Science and Artificial Intelligence, Beni-Suef University, Beni-Suef, Egypt[3]

***Abstract*—This paper proposes a framework to solve academic certificate fraud by implementing a blockchain network. A permissioned Hyperledger fabric network is deployed to store students' information and allows the proper access to guarantee the system security. The paper discusses several studies that introduce variants of solutions for the academic certification tampering problem by using blockchain technology. It finds Hyperledger Fabric secure, performant with higher TPS than Bitcoin and Ethereum; latency increases with participant number.**

***Keywords*—Academic certificates; tampering; security; blockchain; hyperledger fabric; Ethereum; channels; nodes; peers; chaincode**

I. Introduction

Education in the era of industry 4.0 is different from the old days, Nowadays, Technology becomes a part of everything, especially, one of the most important pillars of nations' development. Thus, technologies like the Blockchain had been employed to help developing education in many forms; education systems management, Institutional Accreditation, Academic records, academic credits, and degrees' verification. Hence, no wonder, Blockchain is a promising technology that had been adopted by a variety of industries such as health records, manufacturing, tourism, supply chain & logistics, financing & banking, and education [1], which is because of the immutable ledger that made it secured, decentralized, transparent, and accountable networking technology [2].

Credential fraud is one of the challenges that had been an obstacle for the education systems around the world, particularly, as it affects the education quality, trustworthiness, and creditability, thus, the country's education ranking. For instance, The United Kingdom was known for hosting the biggest amount of Diploma mills [3] while investigations resulted in the University of Wales shutting down its degree validation system and the registrar resigning [4]. Furthermore, one in every nine politicians in the lower house of the Russian Duma held a fake academic degree as per a study was conducted in 2015 [5]. Pakistan was not any far from that, where regulatory bodies were easily able to fake degrees of high-standard officials and it was discovered by the Federal Investigation Agency in January 2018 [6]. And when it comes to our Arab world, we can mention the 450.000.000$ revenues that were gained by an American-operated diploma mill that had offices in Europe and the Middle East [7].

As it was mentioned, the Credentials fraud is prevalent all over the world, however some recent project started to counter this, thanks to the new Blockchain network helps to store students' data safely and allow appropriate access to their records [8], Moreover, it supports the management system of the academic degrees and the learning outcomes [9]. That is why integrating a degree verification system for higher education can be a noted step in achieving the education development goals in Egypt.

Blockchain-based education solutions had been proposed and implemented in many higher institutions; in Massachusetts institute of technology in the United States of America has implemented a project named "Blockcert" that is an open-source developing platform that allows developers to develop certifications' validation applications for academic records [10]. Also, in Maribor University in Slovenia where the EDUCTX project was first introduced to be a peer-to-peer student and university network that allows students credit for fees payments [11].

This study is of utmost importance as it tackles the urgent requirement for secure and tamper-resistant validation of academic qualifications. Through Hyperledger fabric technology, this framework guarantees transparency, diminishes fraudulent activities, and strengthens confidence in the educational field. It holds substantial practical implications for educational institutions and employers globally, simplifying the validation procedure. Furthermore, it lays the groundwork for future progressions in digital credentialing and decentralized authentication systems.

Researchers opt for the blockchain-suggested framework to verify academic certificates because it effectively tackles the problem of certificate tampering for several compelling reasons:

1) Firstly, the immutability of the blockchain ensures that once academic certificates are recorded, they become tamper-proof, making it virtually impossible to alter certificate data without detection. Additionally, the blockchain's consensus mechanism maintains the integrity of the certificates by validating any changes to the records.

2) Furthermore, the transparency and auditability provided by the blockchain play a crucial role in addressing the problem of certificate tampering. The transparent ledger allows authorized participants to view all transactions related to certificates, aiding in the identification and tracking of any unauthorized changes. Moreover, comprehensive audit trails enable easy verification of certificate authenticity and detection of tampering attempts.

3) The decentralized verification offered by the blockchain framework also contributes to addressing the issue of certificate tampering. The use of a distributed network ensures that no single entity controls the certificate data, reducing the risk of tampering by internal or external actors. Additionally, consensus protocols used in blockchain ensure that changes are only accepted if agreed upon by multiple network participants, further mitigating tampering risks.

However, evaluating the security of this framework through penetration testing is valuable, but it has limitations. These limitations encompass its limited scope, the possibility of overlooking untested areas, time and resource constraints, and reliance on the testers' knowledge. Furthermore, the constantly changing threat landscape means that new vulnerabilities may arise after the testing process. Ethical and legal factors can also limit the extent of testing, and live system tests may cause disruptions in operations. Lastly, penetration testing may fail to identify certain issues, such as insider threats or subtle logical flaws, highlighting the necessity of a comprehensive, multifaceted security assessment approach.

II. Background

Blockchain was defined by (Wang) [12] as "an essentially a distributed database of records, or public ledger of all transactions or digital events that have been executed and shared among participating parties", originally, Bitcoin was first introduced and developed in 2008 as the base stone for Blockchain technology [13]. Simply, Blockchain is a series of blocks linked together using encrypted links or "Hashes", similarly, each of these blocks represents a database record and the Hash is the link between these blocks. Deenmohamed [14] explained the Blockchain that needs to contain at least "three constituents"; "Data" which is the record stored. "Previous hash" and its value of the preceding block hash, and "Hash" which is a calculated value of the block-stored data, and the "Previous hash" that references it.

The decentralized nature of a blockchain, along with its immutability, data encryption, and change transparency, are the key factors that contribute to its exceptional level of security [15].

Conventional client-server systems, such as centralized systems, store all data in a single repository, which exposes the system to potential hacking threats. Also, when maintenance or downtime occurs, the entire system becomes inaccessible; however, in the worst-case scenario, if the system becomes corrupted or irreparable, all the data will be permanently lost. On the other hand, blockchain, as a decentralized network, offers significantly higher security against hacking attempts as it operates without the control of any central authority or third-party controller, ensuring enhanced security measures. Moreover, blockchain technology ensures data immutability, making it tamper-proof once stored through the utilization of cryptographic hash functions. While blockchain maintains transparency by recording every transaction, it also safeguards user privacy by encrypting usernames, thereby protecting the user's identity [16].

Blockchain networks can be permissioned or permissionless. Aswin & Kuriakose [17] explained that Permissioned blockchains differ in that they are exclusively open to a specific group of verified participants. These participants operate within a governance model that fosters partial trust among them. Permissioned block chains serve as a means to secure interactions between entities that share a common objective but cannot fully trust one another. Unlike permissionless blockchains, permissioned blockchains do not require costly mining processes, and implementing a native currency is not obligatory. On the other hand, Permissionless networks stand out in blockchain networks as they are accessible to all individuals, with the added benefit of participant anonymity. This inclusive nature allows virtually anyone to partake in the network, ensuring anonymity for all involved. Trust within permissionless blockchains solely relies on the state of the blockchain itself, as no external factors influence participants' trust. Additionally, permissionless blockchains typically incorporate a native cryptocurrency, which necessitates either mining or transaction fees.

III. Related Work

Based on many studies, Blockchain proved its ability to overcome most of the security issues any other database technology faced before. Especially when the related field is education, as the educational process outcomes is meant to be certified to guarantee and authenticate students' qualification of specific study track. The following studies discussed the deployment of the blockchain in some educational areas in term of certifications' security and validity.

In [1]: The study of Huynh [18] was conducted to set a solution for the global spread of fake certificates which are becoming difficult to be managed or controlled. Today many institutions issue unlicensed certificates, this prolongs the validation process of certificates, especially with the increase in the number of certificate holders.

Thus, the author benefited from the advantages of blockchain and the potentials of Blockcert that can solve the problem of fake certificates more easily and securely. A blockchain called UniCert is deployed to issue and verify certificates which, in the future, will prevent the issuance of any fake certificates based on the author's mention.

The UniCert standard makes it possible to issue multiple certificates simultaneously by committing to the recipient list file format a certain way that each column is used to distinguish recipients. The recipient's UniCoin address is used to retrieve issued certificates. That title is called PubKey. After issuance, the certificate identification number issued to the recipient will be added.

The Merkle root algorithm (hash tree) is designed to be used in cryptocurrency to assure the data blocks' safety when passing through peer-to-peer networks, to be undamaged, complete, and unaltered.

After the target certificate is being hashed, all of those certificate hashes are merged into the Merkle root, and the evidence of this is the trend of Merkle Root that returns at Target Hash. As a result, UniCert Signature is a trust guarantee that every batch of certificates is secure.

In [2]: Problems related to the forgery of certificates lead to dire consequences on society. Certainly, the traditional method of printing paper certificates encourages forgery. It leads to a long wait for the certificate to be issued and then received. To avoid these issues, El-Dorry [19] proposed a digital certificate system that is based on the blockchain with the basic characteristics of consensus, source, immutability, and finality.

This study aims to develop a decentralized system for issuing digital certificates using the blockchain and according to the Hyperledger Fabric framework. This system is characterized by being able to prevent certificate fraud and reduce costs and time taken to issue those certificates. Blockchain was chosen because it is a trackable system that is maintained across synchronized ledgers. It is also a completely tamper-proof system. The use of Hyperledger Fabric is based on its privacy, scalability, and smart contract support.

A decentralized blockchain system consists of a network of participants, in our case, it consists of four organizations: public universities, private universities, corporations, and the MOHESR (Ministry of Higher Education and Scientific Research) in Egypt. As well as graduates with specific roles who represent their universities. All persons within the network, whether participants or actors have their permissions. Graduates query their degree through synchronized ledgers also called ledgers.

As for the Ministry of Higher Education, it can inquire about synchronized books and can issue certificates to graduates of private universities. Also, Companies have the right to verify the authenticity of the certificate, so they are considered actors where companies have access to the verification portal. Graduate certificates will have a period during which they will be valid.

This model was the result of this study where the network configured to accept MOHESR as network administration center, and the ordering service is a solo node for ordering transactions which is just used for development.

The solution consists of three applications, each is connected to the peer organizations to allow actors to interact with the blockchain network to issue, request, and verify a certificate, each according to the allowed permissions.

In [3], on the other hand, the study of Hasan [20] aimed to develop a proposal for a theoretical system to verify graduate certificates. It is a blockchain-based system on the cloud that can issue academic certificates, verify their validity, and block cryptocurrencies.

The study deals with the Blockchain (BC) technology used to solve these problems. It showed that the proposed "DistB-CVS" system found that banned cryptocurrencies can benefit from this BC technology. The research proposed a system model to verify the certificates according to the BC located in the cloud database.

The authors suggested the DistB-CVS architecture based primarily on BC as it is the most suitable solution for countries with crypto-bans.

The paper proposed a consensus algorithm that has a major role in improving the block validation mechanism. This study was able to enhance security by relying on a multi-signature scheme. (Block chain without cryptocurrencies). The research evaluated the performance of the displayed architecture while adding various criteria such as increased throughput and latency change.

It has been observed that the proposed "DistBCVS" architecture shows much better performance after a certain time. That's because of the strong authentication and privacy performance of the current model. Data becomes more secure when using a multi-signature scheme.

In [4], Gayathiri [13] discussed the validation of academic and sports certificates as it is tedious for organizations, and indicated how important it is to convert everything related to diplomas to a digital format. It is known that it is difficult for students to keep their academic degrees, but, in the digital world, SSLC, HSC, and Academic Certificates can become digital, easy-to-obtain, and validated for the students in educational institutions.

The suggested application can work even if it is disconnected from the network. Through it, the authenticity of the certificate and the accuracy of the documented information are quickly verified.

Through the proposed system, it is easy to convert academic and sports certificates to another type called digital certificates. The samples and quantity of the digital certificates are then added, hashed, and stored in blocks. The chaotic algorithm is used to generate the hash value as it takes input in various sizes and produces a fixed-size output. For blocks, each block consists of three sections which are the hash value, timestamp, and the hash value of the previous block. All those blocks are connected in the form of a blockchain.

In the proposed application, the administrator login is via the first page using their login ID and password, on the next page, the student and the certificate are added, and the last page allows validation of the certificate. After login, the administrator can add the student's data and certificates by clicking on the button designated for that. Later, the auditor or the employer can validate the certificate using the auditor's login ID and password. This method provides the student login ID and selects the type of certificate and validates the authenticity of the original certificates by clicking the Verify button.

In [5], Khandelwal [21] argued the certification fraud from a consequence perspective, as he mentioned that people who have worked hard and obtained legitimate degrees suffer from those who have fake degrees.

The system has three main users which are: the user, the organization, and the company that verifies. The user is the person who has the certificates and who can share them with the companies. Institutions are responsible for issuing original certificates. An auditor is an individual or company that verifies the authenticity of certifications.

Once a user has completed a particular course, diploma, or degree, the organization will make a digital copy of the certificate. The organization converts the digital certificate to a base-64 string, then, it hashes the certificate using the SHA-512 algorithm. This hash is sent to the blockchain using the

enterprise's private key signature, so the blockchain automatically verifies that signature before a transaction is triggered to add the hash to the blockchain.

Then, the transaction ID is generated successfully. It sends the user the transaction ID obtained and the digital certificate. When the user is in the system, it becomes visible on their control panel. It will also be uploaded to the portal via the user's account. The user can send a digital copy of the certificate to the company through the system. Thus, the company can view and verify all the certificates received from the user on the dashboard.

The system is secure and is a guarantee of the original identity of each of the three entities concerned which are the user, the organization, and the auditor.

In [6], from another view, monitoring personal fraudulent activities can help to detect certificates fraud as discussed by Priya [22] who proposed a system that is able to deploy unique monitoring by updating all personal identity activities and illegal activities carried out against a person. The whole personality and behavioral activities of a person can be monitored by the modification process.

The proposed system was developed on Ethereum platform and being run on Ethereum virtual machine (EVM), and it consists of multiple modules; user interface, verification, building block, android-based QR code generation.

The user can view his certificates after completing the correct authentication, if a third person scans the QR code beyond the allowed limit, that person's location will be sent to the authorized user with the permission link. Also, the user can allow or reject that person through this link.

The system has a transparency that allows the process of requesting and granting the certificate automatically. Thus, companies and organizations will be able to verify the data of any certificate from the system.

In [7], Bousaba & Anderson [23] highlighted the case when a student is going through requesting procedures of requesting an official copy of the certificate or validation of grade after graduation which can be demanded various reasons such as seeking a job or higher education. Usually, people who request verification of grades are bound by a specific time limit. The traditional methods of validating scores are very complex which makes them very time-consuming. It is known that these methods require human labor to maintain them. They often have security or privacy issues.

To solve this system problem, the study provided a solution via Ethereum smart contracts and using a decentralized application (DApp). Via a user profile application, the user is enabled to use the functionality of the Ethereum Smart Contract with a provided web graphical interface. The application allows the programming of transaction logic into the blockchain by connecting the Ethereum blockchain technology to the EVM (Ethereum Virtual Machine) using the Solidity programming language.

Students, universities, and trusted parties can retrieve student information after accessing the requestor's information and then using the private key to decrypt.

However, student data is not subject to change unless it has been intentionally modified and with a specific date for the modified data on the blockchain.

The results of the tests showed that the cost of gas remained constant even though the number of users increased. Another test was done using a third-party account which turns out that he was only able to view the students' profile information but not to edit it. All tests passed and were able to embrace the application's initial use cases.

In [8], another study highlighted that obtaining a fake graduation certificate has become easy due to the lack of an anti-counterfeiting system. This made tracking and validating those certificates in the traditional way arduous.

Devdoot [24] study proposed a system to solve this problem based on smart contracts and IPFS. The list of participants who can interact with our smart contract are university/College, students, and the company.

The certificate data will be collected and appended in a bit matrix then it will be given to IPFS. After it applies the hash algorithm, that hash will be stored with the original certificate.

IPFS will pass that data to the Blockchain. Then, the issuer will be approved for the generation fee in MetaMask. This hash will be stored in the Blockchain and is not subject to change under normal circumstances. The student will be able to send his digital certificate to different institutions and companies.

The issuer will be able to load that certificate or write the hash key. The system will be able to provide a response whether the document is legitimate or illegitimate.

In [9], also, Liu & Guo [25] proposed a scheme that can store certificates, validate scores and combine the properties of the blockchain. The study demonstrated the scheme as follows:

Platform: The front-end system of a web service through which the user of the system can interact with the blockchain. The platform user is mainly divided into three: system administrators, users, and auditors.

Sections. System administrators can manage and assign user rights. The users are the students. They are responsible for submitting, querying, and updating transaction requests for certificate registrations if necessary. The auditors refer primarily to the user of the colleges and to those responsible for checking the validity of certificates.

The system consists of the application layer, the business layer, the smart contract, and the Hyperledger Fabric.

The results of the tests showed that the system is characterized by a faster transaction processing rate than other blockchain systems. Based on this scheme, the transfer rate of transactions of this system is maintained at 180-250 tps. But the Bitcoin-based scheme makes seven transactions per second. And Ethereum is capable of doing dozens of transactions per second. The Hyperledger Fabric-based scheme has the highest transaction throughput.

In [10], the study of Tariq [26] discussed the credential data fraud that has become a common practice and negatively affects investment and trust in higher education systems. This study

proposed a blockchain-based solution that provides a comprehensive solution for validating certified data. It is the most influential Cerberus in the fight against fraud as it is connected to the existing validation ecosystem.

The accredited body works in partnership with multiple parties such as universities, and monitoring entities, such as organizations and citizen groups as it maintains the authorized blockchain network. The authorized body can periodically aggregate these transactions into blocks that are then added to the blockchain.

The university issues an academic paper certificate and a digital copy of it when the student graduates. The Registrar digitally signs that accredited certificate and then publishes it on the Cerberus network. Next, the authorized body verifies the digital certificate by the nodes mined in the block which are added to the blockchain. The certified certificate is then issued and certified digitally.

The university issues the student's degree certificate that includes a QR code. The business owner can verify the original certificates by scanning the code using the web portal or smartphone application.

The search prototype was implemented on Parity, an Ethereum client, version 1.10.4-fixed. Parity insists that it is the fastest and most advanced Ethereum client (89).

Cerberus is scalable because it is batch version dependent. It also maintains the privacy of user data.

The authors mentioned that one of the direct additions is to link several approved documents or student qualifications to the system. This ensures that you can check the most recent and that all data is also original. The system can easily integrate this by including the hashes of the previous original data in the parameters of the recently approved data.

In [11], further, the study of Hammi [27] spotted the light on the public key (PKI), as it has a primary function of the infrastructure which is revocation management as this mission is essential to the security of the PKI.

The study relies on the use of a public blockchain to store and publish data for revoked certificates. The proposal uses the same principles as the CRL distribution points to support scalability. When the certificate authority (CA) revokes the certificate, it recalculates the corresponding Bloom filter. It also provides a new transaction to store in the blockchain.

The proposal includes four entities; certificate authority (CA), blockchain (BC), server, and the client.

The Namecoin blockchain was used. Its role is to implement the bit top-level domain. It is also independent of the Internet Corporation for Assigned Names and Numbers (ICANN).

A mechanism based on bloom filters has been proposed because it reduces the time required to provide invalidation information. The study uses the same principles as the CRL distribution points. Each distribution point served by a Bloom filter is filled with revoked certificates. Then, Bloom filters and cancellation information are shared and published using the public blockchain.

Standard deviations calculated on the results of each trial were very low (<0.08 ms), however after the evaluation, it became clear that the revocation system was able to meet the security requirements in addition to its ability to outperform the current systems.

Focusing on the worst-case scenario of our solution, that is when the filter provides a positive response. The challenge is to provide an alternative solution that avoids the downloading of all the LRSIs from the server.

In [12], furthermore, Chengv [28] discussed distance education as it has become one of the most important educational means for students. Despite its advantages, online education makes it difficult to track student activities. There are also difficulties in managing the verification of paper documents and digital files. In this study, a digital education certification prototype is designed based on the use of blockchain, and the abstract algorithm.

Education data can currently be verified by the system, universities, and employers using the certification authorities as to the regulatory nodes of the blockchain consortium.

The student can use the application to issue a digital certificate. Next, a digital certificate is generated and then hashed into a digital fingerprint. The certificate is stored in an immutable position on the blockchain.

Employers are allowed to recognize the authenticity of the digital student certificate.

The mobile terminal software allows students to apply to the school to generate a digital certificate via a specific application. Students can authorize stakeholders to search for their original data.

In this prototype, the study considers that the Macau University of Science and Technology will serve as the university's participating node responsible for issuing digital documents. The test environment for Hyperledger Fabric V1.4 is configured with the goal of creating a blockchain framework. The model allows for the virtual deployment of blockchain nodes to three organizations and to share with two peers. To measure the performance of the educational blockchain platform, the Hyperledger Caliper tool is used. This tool also uses scalability and stability.

As a result, the creation of a new transaction recorded a transfer rate of 263.9 tps and a query of 1982.6 tps which verifies the efficiency and the superiority of the proposal over the traditional method.

The mentioned studies illustrate the characteristics and capabilities of the blockchain, which the researchers recommend for building a secure certificate ledger. Blockchain characteristics as revealed are: (1) Immutability, (2) Privacy, (3) Confidentiality, (4) Auditability, (5) Accountability, (6) Interoperability, (7) Data sharing, (8) Tractability, and (9) Data integrity.

IV. The Proposed Framework

The researcher proposes a framework that links the qualifications taken by the student under one account in a

blockchain system. Fig. 1 summarizes the general workflow of the proposed framework.

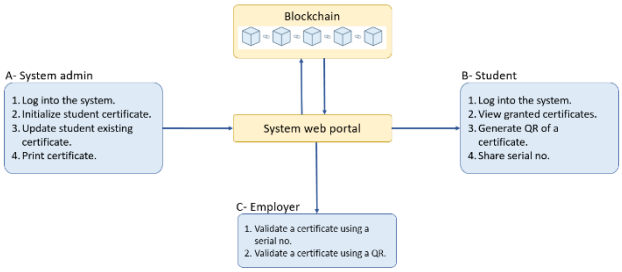

Fig. 1. System framework.

The system admin represents the graduation affairs administration in the faculty of commerce and business administration at Helwan University in Egypt. The admin can log into the system using a provided unique username and password to initiate or update an academic certificate of a student. The student account holds all academic certificates related to the concerned student that can be of graduation, masters, or doctorate certificate type.

To add a student's new certificate, the system admin needs to create a new student account by inserting basic information such as student ID, Name, birth place, birth date, nationality, national ID, gender, contact number, email, account user name, and the password.

The admin can add a new certificate by inserting details such as university and faculty name, degree type, degree name, specialization, general percentage, general grade, graduation project grade, total credit hours, the CGPA, graduation season, date of certificate initialization, date of certificate confirmation, thesis title, and the number of prints.

Once a certificate is saved, it is viewable in the student's account, so the student can generate a QR code and share the serial number with the employer. On the other hand, the employer can access the portal to validate a certificate using the certificate serial number provided by the graduate.

V. Framework Implementation

Aswin & Kuriakose [17] revealed that Ethereum operates as a public blockchain, making all data publicly accessible. Consequently, it is well-suited for applications that require interaction with a global audience, such as insurance and peer-to-peer gambling. On the other hand, Hyperledger Fabric is specifically designed for private use cases, particularly in supply chain scenarios where participants should only have access to relevant data. For instance, it allows selling goods at different prices without disclosing this information to all participants. Furthermore, the study found that Ethereum, the more popular framework, offers a diverse ecosystem of development tools. However, it lacks well-established support for various programming languages, resulting in limited options. Conversely, Hyperledger Fabric provides essential tools but supports widely used languages with extensive libraries, facilitating development [17].

The Hyperledger Fabric has been identified by researchers as an optimal choice for implementing the authentication framework for academic certificates due to a variety of key advantages. These advantages include:

1) A permissioned network that ensures controlled access and heightened security by permitting only authorized participants.

2) The modular architecture of the Hyperledger Fabric allows for the customization of components to align with specific requirements, including the integration of pluggable consensus mechanisms.

3) Hyperledger Fabric boasts scalability and performance capabilities, supporting parallel transaction execution to achieve high throughput and low latency, thereby enhancing its scalability.

4) In addition, the platform offers privacy and confidentiality features such as private channels and fine-grained access controls to safeguard sensitive data within the academic certificate authentication framework.

5) The rich query language of Hyperledger Fabric enables flexible and efficient data retrieval and verification processes, enhancing the overall functionality of the system.

6) Furthermore, the platform promotes interoperability by seamlessly integrating with existing systems and supporting cross-platform compatibility, ensuring smooth operation within diverse technological environments.

7) Hyperledger Fabric benefits from a strong community and support system, with an active development community and comprehensive documentation to assist users in navigating the platform effectively.

8) The platform provides features that aid in regulatory compliance, including audit logs and privacy controls, to help meet the necessary regulatory requirements for the authentication of academic certificates.

These combined benefits establish Hyperledger Fabric as a robust, secure, and scalable solution for the authentication framework of academic certificates.

Hyperledger fabric implemented system consists of:

1) Organizations (Peers): are the entities which the transactions are being transferred among, such as graduation affairs administration, student, and the employer, and each of them has its own ledger.

2) Chain code: is the smart contract that contains the transaction code – instructions- that is required to be executed, such as inserting student data, insert a new certification, and retrieve student's data, etc.

3) Consensus mechanism: serves as the validation principle through which all participating organizations reach an agreement on the data that is generated as a result of executing the Chaincode.

4) Endorsement policy: the agreement policy which verifies user authentication, creates a version of the asset that allows read and write operations, and has the authority to either accept or reject the proposal.

5) Channels: between the peers to execute transactions.

The Hyperledger Fabric network is deployed using single-organization model for executing the following Chaincode (a simplified textual representation):

Chaincode:

```
Procedure CreateAccount(ctx, studentID, Name, birthplace, birthdate, nationality, nationalID, gender, contactnumber, email, accountusername, password)
    studentExists = Call StudentExists(ctx, studentID)

    if studentExists
  return "Student already exists"

    student = {
  studentID, Name, birthplace, birthdate, nationality,
  national_ID, gender, contactnumber, email, accountusername, password}

    Call PutState(ctx.stub, studentID, Buffer.from(JSON.stringify(student)))
    return "Student account created successfully"

Procedure InsertCertificate(ctx, studentID, universityname, facultyname, degreename, specialization, generalpercentage, generalgrade, graduationprojectgrade, totalcredithours, CGPA, graduationseason, dateofcertificateinitialization, dateofcertificateconfirmation, numberofprints)
    studentExists = Call StudentExists(ctx, studentID)

    if not studentExists
  return "No student account found"

    degreeExists = Call DegreeExists(ctx, degreename)

    if degreeExists
  return "Degree already exists"

    certificateID = Call GenerateRandomCertificateID()
    certificate = {
  certificateID, studentID, universityname, facultyname, degree_name, specialization, generalpercentage, generalgrade, graduationprojectgrade, totalcredithours, CGPA, graduationseason,
dateofcertificateinitialization, dateofcertificateconfirmation, numberofprints    }
    Call PutState(ctx.stub, degreename, Buffer.from(JSON.stringify(certificate)))
    return "Student account created successfully. Certificate ID: " + certificateID

Procedure RetrieveCertificates(ctx, studentID)
    studentExists = Call StudentExists(ctx, studentID)

    if not studentExists
  return "No student account found"

    certificates = []
    iterator = Call GetStateByPartialCompositeKey(ctx.stub, 'certificate', [studentID])

    for each (key, value) in iterator
  certificates.push(JSON.parse(value.toString('utf8')))

    return if certificates.length > 0 then certificates else "No certificates found for this student"

Procedure StudentExists(ctx, studentID)
    studentData = Call GetState(ctx.stub, studentID)
    return bool(studentData and length(studentData) > 0)

Procedure DegreeExists(ctx, degreename)
    certificateData = Call GetState(ctx.stub, degreename)
    return bool(certificateData and length(certificateData) > 0)

Procedure GenerateRandomCertificateID()
    min = 1000
    max = 9999
    return random(min, max)
```

VI. Application Procedures

The process of inserting student data into the HLF network involves the following procedures:

1) The system admin initiates a request (proposal) to carry out the insertion transaction for the student's data.

2) The endorsing peer emulates the proposal by applying the endorsement policy, so it can either accept or reject the proposal.

3) If the proposal is approved, system sends the required transaction to the ordering service node.

4) The ordering service node maintains process concurrency and integrity by generating a batch (block) comprising the requested transactions and guarantees their sequential placement in the correct order.

5) Then it passes all the approved transactions to all peer to insert the data into their ledgers.

6) Peers validate each transaction by validating; the endorsement policy and the read/ write version.

7) Then the peers commit the transactions block to the blockchain, therefore, all peers will see the new inserted data.

In the realm of blockchain, the current data is stored in the world state ledger, which is constantly updated. Simultaneously, the log information ledger documents the historical transactions. This divergence in ledger functionality distinguishes hyper ledger fabric from Ethereum.

VII. Results

The study places utmost importance on ensuring the security of the Hyperledger fabric network. However, the process of gauging the security of a Hyperledger Fabric network is all-encompassing, involving a thorough examination of technical aspects, policy considerations, and ongoing monitoring. To

effectively address the ever-evolving threats and vulnerabilities, it is crucial to conduct regular security audits and implement necessary updates. Engaging with security experts and staying well-informed about the latest developments in blockchain security is of utmost importance in order to maintain a secure Hyperledger Fabric network. This highlights the role of security measures as a type of technological limitation.

Linux's security assessment of Fabric reveals that it is a robust and well-designed platform with a strong implementation. The platform has demonstrated a high level of security and functionality, positioning it well for future updates and addressing any potential flaws in the industry-standard cryptography [29].

Performance measurement of a blockchain network is as crucial as its security. To evaluating the read-write throughput of the network constructed, we utilized the Hyperledger caliper tool and conducted a comparative analysis with Ethereum and Bitcoin.

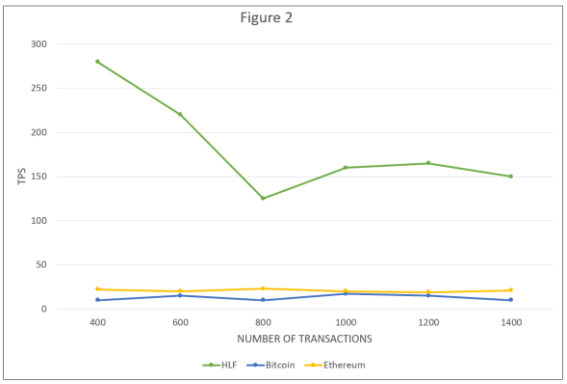

Fig. 2. No. of transactions HLF vs Bitcoin and Ethereum.

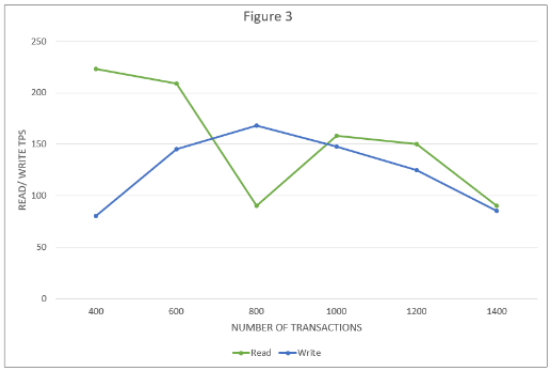

Fig. 3. Transactions read / write speed per second.

The outcomes of the tests are illustrated in Fig. 2 and Fig. 3. Notably, the Hyperledger network exhibited a higher TPS (Transactions per Second) compared to Bitcoin and Ethereum. This discrepancy can be attributed to the fact that the latter two are public blockchains, involving the issuance of coins and utilizing different consensus protocols. As the number of transactions increases, the reading performance surpasses the writing performance, primarily due to the requirement of consensus for writing. Consequently, the read and write performance of the blockchain is influenced as the transaction volume rises.

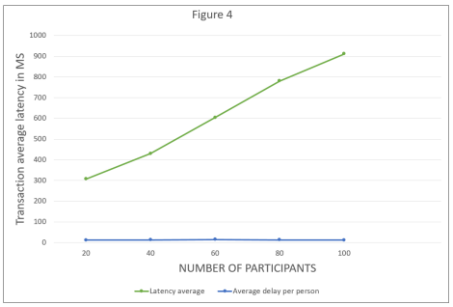

Fig. 4. Network latency test result.

The data in Fig. 4 clearly demonstrates the network latency test results (Time taken for a transaction to be committed). As the number of participants' increases, both the average delay and the average delay per person also increase. This relationship is evident when examining the results for 20, 40, 60, 80, and 100 participants, where the average delay values are 306.5ms, 430ms, 603.7ms, 780.9, and 911.3ms, respectively. It is worth noting that the average delay per person ranges from approximately 12-14ms.

VIII. Conclusion

In our research article, we presented a secure database for academic certificates utilizing Hyperledger Fabric. This innovative approach effectively addresses the issues of fraud and tampering associated with academic certifications. The framework showcased in our study emphasizes the significance of safeguarding academic data, particularly within a multi-peer network. The utilization of Hyperledger Fabric technology proves to be paramount in this context. Moving forward, our future investigations will focus on further enhancing academic accreditation through the integration of blockchain technology.

Acknowledgment

We sincerely appreciate the financial support from Watan First Digital, which played a crucial role in enabling this study. Their generous funding allowed us to carry out the essential research and bring this project to fruition.

References

[1] Bodkhe, U; Tanwar, S; Parekh,K; Khanpara, P; Tyagi, S; Kumar, N; Alazab, M. (April 2020). Blockchain for Industry 4.0: A Comprehensive Review, IEEE Access, vol. 8, pp. 79764-79800, 2020, doi:10.1109/ACCESS.2020.2988579.

[2] Verma, P. &Dumka, A. (2021). Perspectives of Blockchain in the Education Sector Pertaining to the Student's Records. Springer Nature Singapore Pte Ltd., V. Goar et al. (eds.), Advances in Information Communication Technology and Computing, Lecture Notes in Networking and Systems 135, pp. 419-425, retrieved from (https://link.springer.com/chapter/10.1007%2F978-981-15-5421-6_42).

[3] Cohin, E. B. & Winch, R. (2011). Diploma and accreditation mills: New trends in credential abuse, Bedford: VerifileAccredibase, retrieved from (https://www.esrcheck.com/file/Verifile-Accredibase_Diploma-Mills.pdf).

[4] Henry, J. (2011). University of Wales abolished after visa scandal, Retrieved from (https://etico.iiep.unesco.org/en/university-wales-abolished-after-visa-scandal), Access in (17/02/2021).

[5] Gribova, D. (January, 2016).Study finds that one in nine Russian Duma deputies are academic phonies. Global Voices Online,Retrieved from (https://www.pri.org/stories/2016-01-20/study-finds-one-nine-russian-duma-deputies-are-academic-phonies).

[6] Abbasi, W. (November, 2018). FIA probing fake degrees attestation by HEC officials. Retrieved from (https://www.thenews.com.pk/print/392649-fia-probing-fake-degrees-attestation-by-hec-officials, Accessed on (01/03/2021).

[7] Bear, J. (2012). Introduction from "Degree Mills: The Billion Dollar Industry That Has Sold Over A Million Fake Diplomas", Prometheus Books. Retrieved from (https://aaar.assembly.ca.gov/sites/aaar.assembly.ca.gov/files/reports/Intro%20to%20Degree%20Mills.pdf).

[8] Chen, Guang; Xu, Bing; Lu, Manli; Chen, Nian-Shing. (2018). Exploring blockchain technology and its potential applications for education, Smart Learning Environments (2018), Retrieved from (https://doi.org/10.1186/s40561-017-0050-x).

[9] Sharples, M and Domingue, J. (2016). The Blockchain and Kudos: A Distributed System for Educational Record, Reputation and Reward, Adaptive and adaptable learning (Springer, Cham, 2016), pp. 490–496, Retrieved from (https://doi.org/10.1007/978-3-319-45153-4_48).

[10] Schmidt, P. (2016). Blockcerts - An open infrastructure for academic credentials on the Blockchain, medium, Retrieved from (https://www.medium.com/mit-media-lab/blockcerts-an open-infrastructure-for-academic-credentials-on-the-blockchain-899a6b880b2f).

[11] Turkanović, M.; Hölbl, M.; Košič, K.; Heričko, M.; Kamišalić, A.(2018). EduCTX: A Blockchain-based higher education credit platform, in IEEE Access, vol. 6, pp. 5112-5127, 2018, DOI: 10.1109/ACCESS.2018.2789929.

[12] Wang, G.Y.,Zhangand, H.B., Xiao, B.W., Chung, Y.C. (2019). EduBloud: a Blockchain-based education cloud. In: 2019 Computing, Communications and IoT Applications (ComComAp). Shenzhen, China, pp. 352–357. Retrieved from (https://doi.org/10.1109/ComComAp46287.2019.9018818).

[13] A. Gayathiri, J. Jayachitra and S. Matilda, "Certificate validation using blockchain," 2020 7th International Conference on Smart Structures and Systems (ICSSS), 2020, pp. 1-4, doi: 10.1109/ICSSS49621.2020.9201988.

[14] Deenmohamed, Haïdar. A. M.; Didier, M. M.; Sungkur, R. K. (2021). The future of university education: Examination, transcript, and certificate system using Blockchain. Wiley Periodicals LLC., DOI: 10.1002/cae.22381.

[15] Darlington, Nick, “Blockchain for beginners: What is Blockchain technology? A step-by-step guide”, retrived from (https://blockgeeks.com/guides/what-is-blockchain-technology/).

[16] R. Moumita & S. Monisha. “Analytical study of blockchain enabled security enhancements methods for healthcare data”, IOP Conf. Series: Materials Science and Engineering, V. 1131, 4th international Conference on Emerging Technologies in Computer Engineering: Data Science & Blockchain Technology (ICETCE 2021). 3RD-4TH Februaey 2021, Jaipur, India, pp. 2.

[17] Aswin, A. V. & Kuriakose, B. (2020). An analogical study of hyperledger fabric and Etherum. ICICV 2019, LNDECT 33, pp 412-420, 2020. (https://doi.org/10.1007/978-3-030-28364-3_41).

[18] T. T. Huynh, T. Tru Huynh, D. K. Pham and A. Khoa Ngo, "Issuing and Verifying Digital Certificates with Blockchain," 2018 International Conference on Advanced Technologies for Communications (ATC), 2018, pp. 332-336, doi: 10.1109/ATC.2018.8587428.

[19] El-Dorry, Alley & Reda, Mohamed & Khalek, Sherif & Mohamed, Shehab & Mohamed, Radwa & Nabil, Ayman. (2020). “Egyptian Universities Digital

[20] 79-83. 10.1145/3436829.3436864.

[21] M. Hasan, A. Rahman and M. J. Islam, "DistB-CVS: A Distributed Secure Blockchain based Online Certificate Verification System from Bangladesh Perspective", 2020 2nd International Conference on Advanced Information and Communication Technology (ICAICT), 2020, pp. 460-465, doi: 10.1109/ICAICT51780.2020.9333523.).

[22] Khandelwal H., Mittal K., Agrawal S., Jain H. (2020) Certificate Verification System Using Blockchain. In: Gunjan V., Senatore S., Kumar A., Gao XZ., Merugu S. (eds) Advances in Cybernetics, Cognition, and Machine Learning for Communication Technologies. Lecture Notes in Electrical Engineering, vol 643. Springer, Singapore. https://doi.org/10.1007/978-981-15-3125-5_27.

[23] (Priya, S. (2019). Online Certificate Validation Using Blockchain.).

[24] Bousaba, Ch& Anderson, E. (2019). Degree validation Application Using Solidity and Ethereum Blockchain. SoutheastCon, Huntsville, AL, USA, pp. 1-5, doi:10.1109/SoutheastCon42311.2019.9020503.

[25] Devdoot Maji , Ravi Singh Lamkoti , Hitesh Shetty , Bharati Gondhalekar, 2021, Certificate Verification using Blockchain and Generation of Transcript, INTERNATIONAL JOURNAL OF ENGINEERING RESEARCH & TECHNOLOGY (IJERT) Volume 10, Issue 03 (March 2021).

[26] D. Liu and X. Guo, "Blockchain Based Storage and Verification Scheme of Credible Degree Certificate", 2019 2nd International Conference on Safety Produce Informatization (IICSPI), 2019, pp. 350-352, (doi: 10.1109/IICSPI48186.2019.9095961.).

[27] Tariq, A.; Haq, H. B., Ali, S. T,. (December, 2019). Cerberus: A Blockchain-Based Accreditation and Degree Verification System, Retrieved from (https://arxiv.org/pdf/1912.06812.pdf).

[28] Hammi, Badis & Serhrouchni, Ahmed & Zeadally, Sherali & Elloh Yves Christian, Adja. (2021). A Blockchain-based Certificate Revocation Management and Status Verification System. Computers & Security. (104. 102209. 10.1016/j.cose.2021.102209).

[29] Cheng, Hanlei & Lu, Jing & Xiang, Zhiyu & Song, Bin. (2020). A Permissioned Blockchain-Based Platform for Education Certificate Verification. (10.1007/978-981-15-9213-3_36.).

[30] Tevora Threat Research Group. (2021). “Linux Foundation 2021 HyperLedger Fabric Penetration Test”, pp 6. (https://wiki.hyperledger.org/download/attachments/13861997/2021%20HyperLedger%20Fabric%20Penetration%20Test%20v1.1.pdf?version=1&modificationDate=1621520080000&api=v2).