# A New Privacy-Preserving Protocol for Academic Certificates on Hyperledger Fabric

Omar S. Saleh[1], Osman Ghazali[2*], Norbik Bashah Idris[3]
Studies, Planning and Follow-up Directorate, Ministry of Higher Education and Scientific Research, Baghdad, Iraq[1]
School of Computing, Universiti Utara Malaysia, Kedah, Malaysia[1, 2]
Kulliyyah of Information and Communication Technology, International Islamic University Malaysia, Kuala Lumpur, Malaysia[3]

***Abstract*—Academic certificates are integral to an individual's education and career prospects, yet conventional paper-based certificates pose challenges with their transport and vulnerability to forgery. In response to this predicament, institutions have taken measures to release e-certificates, though ensuring authenticity remains a pressing concern. Blockchain technology, recognised for its attributes of security, transparency, and decentralisation, presents a resolution to this problem and has garnered attention from various sectors. While blockchain-based academic certificate management systems have been proposed, current systems exhibit some security and privacy limitations. To address these issues, this research proposes a new Decentralised Control Verification Privacy-Centered (DCVPC) protocol based on Hyperledger Fabric blockchain for preserving the privacy of academic certificates. The proposed protocol aims to protect academic certificates' privacy by granting complete authority over all network nodes, creating channels for universities to have their private environment, and limiting access to the ledger. The protocol is highly secure, resistant to attacks, and allows improved interoperability and automation of the certificate verification process. A proof-of-concept was developed to demonstrate the protocol's functionality and performance. The proposed protocol presents a promising solution for enhancing security, transparency, and privacy of academic certificates. It guarantees that the certificate's rightful owner is correctly identified, and the issuer is widely recognised. This research makes a valuable contribution to the area of blockchain-based academic certificate management systems by introducing a new protocol that addresses the present security and privacy limitations.**

***Keywords*—Blockchain technology; hyperledger fabric blockchain; privacy preservation; decentralized control verification privacy-centered (DCVPC) protocol; academic certificates***

## I. Introduction

Academic certificates such as diplomas and transcripts are essential documents that certify an individual's successful completion of a course of study and enable them to pursue diverse employment opportunities within their field [2]. Nonetheless, conventional paper-based certificates are challenging to transport and susceptible to fraudulent activities. As a result, employers and job seekers have lost trust in the verification process, which is now costly and time-consuming.

In response, several institutions have introduced electronic certificates. However, determining authenticity continues to be a prevalent issue. The application of blockchain technology presents a possible solution to this issue by utilising digital certificates that guarantee authenticity and discourage counterfeiting. Blockchain-based systems like Blockcerts and Block.co have been developed by universities such as MIT and the University of Nicosia (UoN), where students are given control of their own digital credentials and can share them with potential employers [1],[2],[3],[4],[5],[6],[7],[8],[9]. The implementation of decentralisation, peer-to-peer networking, and cryptography in these systems ensure security and immutability. Although the present systems solve the problem of authenticity, they do not tackle other challenges such as fake universities and impersonation.

The objective of this research is to propose a novel protocol based on Hyperledger Fabric to address the challenges associated with managing academic certificates and safeguarding the privacy of identities. In comparison to other blockchain technologies, Hyperledger Fabric provides increased access control and flexibility in protecting privacy. To showcase the efficacy of the proposed protocol, a proof-of-concept will be developed as part of the study.

This paper presents an innovative approach to address a crucial issue in the education sector, which is the secure, transparent, and privacy-preserving management of academic certificates. Academic certificates, such as diplomas and transcripts, play a vital role in enabling individuals to access education and career opportunities. However, traditional paper-based certificates are inconvenient to transport and prone to forgery. Although e-certificates have been developed to address this issue, verifying their authenticity is still a significant challenge. Blockchain technology has emerged as a promising solution due to its features of security, data integrity, transparency, and decentralisation for managing academic certificates.

However, current blockchain-based systems have some limitations when it comes to ensuring security and privacy, which this research aims to address. This study aims to address the following research questions and objectives: How can a protocol based on the Hyperledger Fabric blockchain that is decentralised, privacy-centred and ensures the privacy of academic certificates be developed? Can this proposed protocol enhance the security, transparency, and privacy of academic certificates while facilitating automation and interoperability in the certificate verification process?

This paper introduces the proposed protocol and its implementation and evaluates its functionality and performance, contributing to the development of more secure

*Corresponding Author.

and privacy-preserving systems for managing academic certificates. The DCVPC Protocol presents a novel and privacy-centred approach to academic certificate verification that utilises the capabilities of the Hyperledger Fabric blockchain. This protocol offers an innovative means of preserving the privacy of academic certificates by enabling decentralised control and verification of these crucial documents. The protocol empowers individuals to regulate access to their certificates, allowing them to disclose only the necessary information. Furthermore, the use of blockchain technology guarantees that certificates are tamper-proof and immutable, enhancing the overall security of the verification process.

The DCVPC Protocol represents a significant advancement in the area of academic certificate verification, providing a secure and innovative solution that has the potential to become an industry standard.

## II. Blockchain Technology and its Benefits for Academic Certificates Issuance and Verification

The concept of blockchain was first introduced in the Bitcoin white paper in 2008. This distributed ledger leverages consensus and cryptographic techniques to provide a secure and transparent record-keeping system [10],[11],[12],[13],[16]. Since each block contains transactions and a unique hash value, it is difficult to alter or tamper with a block without being detected [16]. Before a transaction can be added to a block in a blockchain network, a consensus must be reached among a group of nodes. As shown in Fig. 1, a block consists of a header and a body, where the body contains the transaction data. The header contains several components, including the Merkle root, a Nonce, a timestamp, and the hash of the previous block. The hash of the previous block is passed to a hash function, which returns a hash value. By recording the hash of the previous block in the current block, the blockchain expands when new blocks are added and linked to it, while also providing an efficient way to detect any attempts at tampering with previous blocks. The timestamp is used to timestamp every newly generated block. The block creation and verification processes only need to be executed once. Merkle trees are binary trees where the labels of non-leaf nodes are the concatenation of the hashes of its child nodes, and the labels of leaf nodes are the hashes of individual transactions in the block body. The Merkle root, also known as the root hash of a Merkle tree, is used to verify the transactions in a block. Instead of verifying each individual transaction in a block, it is sufficient to compare their Merkle root [27]. The structure of a blockchain network is illustrated in Fig. 1, which shows that each block header contains information about the previous block, including its Merkle root, Nonce, timestamp, and hash. The Merkle root refers to the hash of the initial node in a Merkle tree. To further explain the structure of a Merkle tree, let us take the third block as an example of a transaction representation, TX.

The education sector can greatly benefit from the use of blockchain technology due to its various advantages, such as increased security, low cost, improved data access controls, increased accountability and transparency, identity authentication, increased trust, effective student record management, support for learners' career decisions, and enhanced learner interactivity [28]. The use of blockchain technology in the education sector provides a secure and efficient way of managing academic records and transactions. Due to its decentralised nature, blockchain ensures that only intended recipients have access to shared data or transacted funds, reducing concerns about data safety. The ability to control who can view the saved information is one of the main characteristics and benefits of blockchain. Academic documents such as transcripts, degrees, and student and instructor files can be securely stored, and the blockchain ensures the authenticity of digital certificates and the security of users' identities.

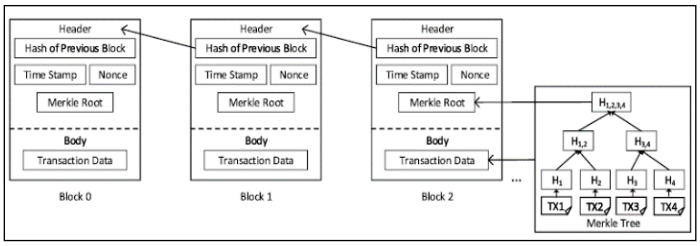


Fig. 1. Blockchain structure.

Blockchain technology also streamlines the process of managing students' personal information, and its adoption in education may reduce the possibility of trading mistakes between parties [28]. Blockchain technology is becoming increasingly important for academic certificate issuance and verification. Traditionally, verifying academic credentials has been a cumbersome and often unreliable process that involved contacting educational institutions and relying on paper records.

The implementation of blockchain technology offers a potential solution for the challenges associated with managing academic certificates. By using a secure and decentralised system, digital credentials can be stored and shared, providing a higher level of trust and transparency in the credential verification process. Utilising blockchain technology allows for tamper-proof certificates to be issued by academic institutions, which can be easily verified by employers and other interested parties. This not only enhances the efficiency of credential verification but also improves the overall integrity of the hiring process.

Furthermore, blockchain technology allows students to exert greater control over their academic records and share them securely and selectively, creating new prospects within the education sector. The implementation of blockchain technology in the issuance and verification of academic certificates has the potential to revolutionise the education industry by enhancing the accuracy and accessibility of academic credentials.

Blockchain technology is widely recognised as a transformative technology for academic certificate issuance and verification. This innovative technology provides a secure, decentralised system for storing and sharing digital certificates, which allows academic institutions to issue tamper-proof credentials that can be easily verified. By leveraging blockchain technology, students can exercise greater control

over their academic records and share them securely and selectively with potential employers and other interested parties.

Moreover, blockchain technology is increasingly recognised as a game-changer for academic certificate issuance and verification. This innovative technology provides a secure, decentralised system for storing and sharing digital certificates, allowing academic institutions to issue tamper-proof credentials that are easily verifiable in real-time, thereby speeding up the hiring process and reducing the risk of fraud. Additionally, the use of blockchain technology enables students to have greater control over their academic records and share them securely and selectively with potential employers or other interested parties. The immutability and tamper-proof nature of blockchain technology ensure that academic certificates cannot be altered or duplicated, providing a higher level of trust and transparency. In summary, the use of blockchain technology for academic certificate issuance and verification offers significant benefits, including greater efficiency, transparency, and security [30],[31].

## III. Importance of Hyperledger Fabric for Preserving the Privacy during the Process of Academic Certificates Issuance and Verification

The use of Hyperledger Fabric in the process of academic certificate issuance and verification is essential in preserving privacy and security [41]. Academic certificate management involves the exchange of sensitive personal information, making privacy a significant concern. Hyperledger Fabric's architecture enables academic institutions to maintain control over their data, ensuring that private information is not shared with unauthorised parties. The platform provides a secure and private environment where all participants have access to information necessary for the verification process without compromising privacy.

Furthermore, the modular design of Hyperledger Fabric allows for the integration of various identity management systems, providing more precise control over information access. This feature empowers academic institutions to uphold privacy and data security throughout the process of certificate issuance and verification, guaranteeing that sensitive information is only accessible by authorised parties. Consequently, the platform offers a more efficient, reliable, and secure approach to academic certificate management that safeguards the privacy of both students and institutions [25],[26].

Hyperledger Fabric is a highly flexible and scalable platform that enables the deployment of various solutions through a modular subsystem architecture. This feature makes it possible for institutions to scale up to increasingly complex systems. In academic certificate management, Hyperledger Fabric is essential in maintaining privacy and data security during the issuance and verification process. The platform has several key components that work together to preserve privacy. Firstly, its modular architecture allows academic institutions to define their own data access policies and identity management systems, providing control over who has access to sensitive information. This ensures that only authorised parties can view and verify academic credentials. Additionally, Hyperledger Fabric uses distributed ledger technology to provide a tamper-proof record of all transactions on the network. This feature ensures that certificates cannot be altered or duplicated, which enhances the credibility of the verification process.

Furthermore, Hyperledger Fabric employs a consensus mechanism to ensure that all network participants agree on the authenticity of a transaction before it is recorded on the ledger. This approach guarantees that all participants have a shared view of the network, making it more secure and reliable. Hyperledger Fabric also offers a modular and flexible framework that can be tailored to the unique requirements of various academic institutions. This adaptability enables institutions to integrate their existing systems and processes with the Fabric network, preserving the privacy of their data. Collectively, these components make Hyperledger Fabric an influential tool for academic certificate issuance and verification. It safeguards privacy while ensuring the security and authenticity of academic credentials [29].

The transaction flow in Hyperledger Fabric begins when a client initiates a transaction request by submitting a proposal to the endorsing peer. The endorsing peer then checks the validity of the proposal and simulates the transaction to ensure that it meets the defined rules and regulations. If the transaction is deemed valid, the endorsing peer endorses it by adding a digital signature to the transaction.

Once endorsed, the transaction is sent to the ordering service, which is responsible for ordering the transactions and creating a block. The ordering service ensures that transactions are ordered based on a consensus algorithm and sends the ordered transactions back to the peers. The peers then validate the transaction by checking the endorsement policy and comparing the digital signature of the endorsing peers. If the transaction is valid, the peers commit the transaction to the ledger, making it immutable and tamper-evident.

Hyperledger Fabric also supports private data, which is only visible to parties that have explicit access to it. This is achieved by storing private data off the main ledger and providing access to authorized parties only.

In summary, the transaction flow in Hyperledger Fabric involves several parties, including clients, peers, and orderers, and ensures secure and efficient transactions by utilizing endorsement policies, consensus algorithms, and distributed ledgers. The platform's modular architecture and support for private data make it an ideal solution for enterprises looking to implement blockchain-based systems.

The use of private channels in Hyperledger Fabric enables network participants to have secure and private communication within a subset of the network. The transaction flow in Hyperledger Fabric is carefully designed to ensure the security, scalability, and reliability of the blockchain network, making it an ideal solution for enterprise-grade applications [29]. Fig. 2 illustrates the transaction flow in the Hyperledger Fabric blockchain.

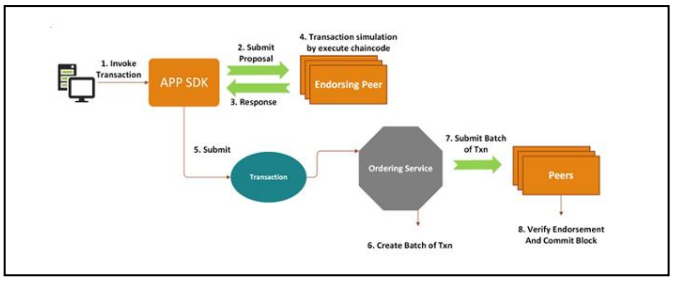


Fig. 2. Transactions flow in hyperledger fabric blockchain.

## IV. Security and Privacy Features Adopted in Hyperledger Fabric Blockchain

Hyperledger Fabric employs several techniques to ensure the security and privacy of academic certificate issuance and verification processes [18],[33],[34]. Firstly, Fabric employs a permissioned blockchain architecture that restricts access to authorised parties, offering a high level of security against unauthorised access. This feature is particularly crucial in academic certificate management, where the exchange of sensitive personal information necessitates robust security measures. Secondly, Fabric's modular architecture allows for the integration of various identity management systems, enabling academic institutions to maintain control over their data and define their data access policies. This feature is crucial in preserving the privacy of student data, ensuring that private information is not disclosed to unauthorised parties. Thirdly, Fabric leverages distributed ledger technology, which offers a tamper-proof record of all transactions within the network. This feature guarantees the integrity and immutability of academic certificates, ensuring that they cannot be altered or duplicated [24]. This provides a high level of security and authenticity to the certificate issuance process. Fourthly, Fabric's consensus mechanism ensures that all participants in the network agree on the authenticity of a transaction before it is added to the ledger. By achieving consensus, Fabric ensures that all network participants share a unified view of the network, resulting in a more secure and reliable system. Finally, Fabric's private channels enable the creation of secure and private communication within a subset of the network, further preserving the privacy of sensitive data. In summary, the security and privacy preservation techniques utilised in Hyperledger Fabric are well-suited for academic certificate issuance and verification applications. These techniques provide a reliable and secure way for academic institutions to manage certificates while maintaining the confidentiality and data security of all relevant parties [35], [36], [37], [47].

## V. Literature Review

Blockchain technology offers a potential solution for secure and reliable management of academic certificates due to its distributed ledger architecture and tamper-proof design. Academic institutions can use blockchain technology to issue and verify certificates efficiently and securely. The use of blockchain technology in academic certificate management has gained significant attention in recent years, with various studies exploring its benefits and limitations.

This literature review aims to provide a comprehensive overview of the existing research concerning the use of blockchain technology for academic certificate issuance and verification. The review will cover various aspects of blockchain technology, including its distributed ledger architecture, consensus mechanisms, privacy features, and security protocols. Additionally, the review will discuss the challenges and opportunities associated with the use of blockchain technology in academic certificate management, and identify areas where future research is needed to further explore this field. The survey aims to offer a thorough comprehension of the present research state concerning the application of blockchain technology in the issuance and verification of academic certificates, and the possible ramifications for academic institutions and stakeholders.

The research [42] explores the potential of blockchain technology in providing a transparent and secure method of recording and maintaining educational certificates and important records. The study highlights the use of digital certificates for evaluating students' academic and extracurricular achievements, and proposes blockchain technology as a secure platform for storing and maintaining them. The research provides an overview of various blockchain-based digital certificate verification systems that employ different authentication techniques and blockchain platforms. It stresses the importance of blockchain technology in ensuring the safety, accessibility, and up-to-date status of digital assets. The study also identifies potential challenges and issues related to academic certification processes in the future. In summary, the research underscores the significance and potential of blockchain technology for academic certificate issuance and verification.

The study [43] introduces a blockchain-based system for the issuance and verification of academic certificates. The system comprises four principal components, namely a verification application with federated identity, an issuing application that involves multi-signature and BTC-address-based revocation, a blockchain, and a local database implemented using MongoDB. The issuing applications manage the primary business logic associated with certificate application, examination, signing, and issuance. They merge the certificate hash with a Merkle tree and send the Merkle root to the blockchain while also handling certificate revocations. The verification application is responsible for verifying the authenticity and integrity of the issued certificates. It includes a web-based page and an Android-based application that retrieves transaction messages through the blockchain API and compares them with the verification data from the receipt. The blockchain acts as a trust infrastructure and a distributed database for storing authentication data, while the MongoDB database manages JSON-based certificates and provides high availability and scalability. Overall, the proposed system leverages blockchain technology to ensure the security and integrity of academic certificates and offers a dependable platform for their issuance and verification.

The study [44] suggests a blockchain-based resolution to tackle the issue of counterfeit educational certificates in Vietnam. The proposed system, referred to as the Vietnamese Educational Certification blockchain (VEcefblock), utilises blockchain technology's features such as anti-forgery information, transaction verification, and smart contracts to

guarantee data transparency and user confidence. The investigation analyses the latest blockchain research and applications to provide insight into the proposed solution. It also presents the development principles of VEcefblock, which involves designing the architecture, business processes, and data mapping structure. Hyperledger Fabric is the blockchain platform used, and the proposed solution is evaluated for performance on the Amazon EC2 cloud. The study underscores the practicality and feasibility of using blockchain technology to address certificate management issues and social problems in Vietnam.

The study [45] introduces a prototype for digital education certificates that uses blockchain technology to enhance the administration and validation of distance education. The prototype is built with a permissioned blockchain, PKI-CA, a digest algorithm, and interactive data authentication via digital signatures. Digital certificates can be issued and verified instantaneously through QR codes or dynamic authorisation codes. Test results demonstrate the prototype's accurate performance with a high throughput of transactions. The proposed system aims to guarantee impartiality and authenticity in education management by ensuring the traceability of student activities and preventing data leakage.

The ongoing research [46] aims to employ blockchain technology to enhance the verification of certificate authenticity. The first stage has led to the development of a prototype, which enables the registration of academic institutions, their faculties, student cohorts, and the issuance of certificate awards. The certificates issued are recorded on the blockchain, ensuring that third parties can verify their authenticity independently of the academic institution, even in the event of its closure. The next stage seeks to expand the prototype to include the registration of medical records, with a focus on ensuring the privacy of sensitive data and granting the owner control over user access to the documents. The final stage involves collecting user and corporate feedback on the proposed prototypes.

MIT Media Lab collaborated with Learning Machine to develop Blockcerts, which uses the Bitcoin blockchain for security. However, this approach slows down transactions, increases prices, and reduces usability. To obtain a diploma using Blockcerts, candidates must install the Blockcerts Wallet software and generate public and private keys. The private keys are stored on users' mobile devices, while MIT receives their public ones. The blockchain stores the diploma's hash value and the date and time it was generated. Graduates can receive digital diplomas that include their public and private keys, which they can use to prove ownership. Graduates can also use the Blockcerts Wallet to share their diplomas with third parties, such as school administrators, future employers, or educational institutions for further education. The system's advantages and drawbacks are discussed in [7], [8], and [11].

There are several benefits for students to use Blockcerts. First, it offers 24/7 access to accredited certification from any location and is valid for the life of the blockchain. Second, students' identities remain private since the blockchain stores only the encrypted hash of their diplomas. Lastly, Blockcerts reduces costs for students by digitising certificates, empowering schools with greater control over students' academic qualifications, and simplifying the verification process [14].

It has been found that an unauthorised individual could potentially create a fraudulent academic credential using the methods employed by Blockcerts, although [15] found this to be feasible. It is not possible to authenticate the Blockcerts issuing public key. Nevertheless, the use of Blockcerts helps to standardise credentials across universities, streamline the verification process for verifiers, and digitise certificates, all of which have a positive impact on students' time and financial investments.

According to a study [15], one issue with Blockcerts is that it does not provide evidence that the owner of a public key is the authorised issuer. This shortcoming allows unauthorised individuals to produce counterfeit academic credentials that appear to be genuine by impersonating the credential-granting organisation. To tackle this issue, researchers at Birmingham University have proposed a cryptographic digital certificate system called BTCert. BTCert aims to establish a dependable federal ID to verify the legitimacy of the issuing institution, enhance certificate authentication through multiple signatures, and devise a secure revocation method to increase the credibility of certificate revocation.

Birmingham University students and alumni can view their certificates by logging in using their BU credentials. The system allows students to submit their credentials to a third party for verification, and institutional administrators can use it to manage student enrolment, issue certificates with digital signatures, and authorise certificate revocation [6],[11]. Similar to Blockcerts, BTCert generates digital certificates by linking transaction hash values with certificate hashes, and the Merkle root for a certificate set is included in the transaction. The authenticity of the certificate is verified by comparing it to the hash value of the local receipt on the Bitcoin blockchain. The BTCert system comprises a blockchain, an issuing application, a local database, and a verification application. The issuing application is primarily responsible for handling certificate revocation, publishing the Merkle root to the Bitcoin blockchain, and combining the certificate's hash value with a Merkle tree. JSON-based certificates are managed using the local database, while the blockchain stores authentication data [19].

The University of Nicosia was the first institution to use Bitcoin's blockchain to create digital credentials. Students' digital fingerprints are saved on the blockchain, and they can use a verification tool to send a certified PDF version of their diploma to others, avoiding any unnecessary costs. Block.co makes it easy to safely and quickly trade credentials, thus preventing diploma mills. Block.co decides whether to grant a degree after compiling a list of qualified students and assessing a sample application. Diploma forgery is impossible due to the blockchain's digital fingerprinting capabilities, and the degree may be quickly earned and verified by anyone [6],[20].

According to a study [21], a proposed blockchain infrastructure for sharing student information could benefit educators, students, and businesses. The infrastructure is mostly decentralised, as it does not depend on a single server to

access learner data but instead utilises a centralised database. The paper does not provide specifics on implementation or experimental analysis. The authors suggested a blockchain-based infrastructure for archiving student records [22], and the results indicate that storing academic information on the blockchain is more cost-effective than using cloud storage. Smart contracts could utilise access control management to protect users' personal information, which would need to be stored securely with multiple database vendors. However, the study does not provide any concrete outcomes that can be tested or implemented.

According to the authors [23], BcER2 is a database based on blockchain technology for storing academic credentials, including diplomas. The researchers implemented their design using an open-source framework called Hyperledger Composer, as described in the article, which provides a high-level design overview, but no implementation details or test results. Central New Mexico Community College uses blockchain to store student records, enabling students to have greater control over their academic information. Students can download their credentials to any device by using their wallet address. However, their strategy appears to rely on on-chain storage, which is both expensive and inherently unscalable.

## VI. Gaps and Issues in Terms of Privacy-preserving with Current Blockchain-based Platforms in the Context of Academic Certificates Issuance and Verification

Although blockchain-based platforms offer several benefits regarding the secure, transparent and decentralised storage and verification of academic certificates, privacy preservation issues remain. One concern is that current blockchain-based platforms may not prioritise privacy and could expose sensitive information to unauthorised parties [32]. Additionally, the public visibility of blockchain transactions and certificates could jeopardise students' privacy and academic records. Furthermore, current platforms may lack reliable mechanisms for identity verification and access control, which can lead to fraudulent activities or unauthorised access to academic records. The non-compliance of current platforms with data protection regulations such as GDPR may also cause legal and ethical problems. Researchers and developers are working on privacy-enhancing solutions, such as the use of zero-knowledge proofs, homomorphic encryption, and multi-party computation, to address these gaps and issues [38], [39], [40], [41]. Therefore, this study aims to suggest a design for the Certificate Verification Control Protocol (DCVPC) based on the Hyperledger Fabric blockchain.

## VII. Research Methodology

The Design Science Research Methodology (DSRM) could be a suitable research methodology for this study. DSRM is widely used in information systems research and concentrates on creating and assessing creative solutions to practical problems [48]. This approach is particularly appropriate for this study since it entails designing and executing a new protocol based on the Hyperledger Fabric blockchain to protect the confidentiality of academic certificates. The first phase of the methodology defines the problem, which in this case is the lack of privacy in conventional paper-based academic certificates. The second phase involves designing a solution to the problem, which in this case is the proposed DCVPC protocol. The third stage involves creating a model of the suggested solution, which would necessitate constructing and testing the protocol in a real-world setting. Finally, the fourth phase involves assessing the efficiency and effectiveness of the proposed solution. In general, the DSRM methodology could offer a structured approach to developing and evaluating the suggested protocol and could lead to an innovative solution to the issue of preserving the privacy of academic certificates.

## VIII. The Proposed Design of Certificate Verification Control Protocol (DCVPC)

The initial stage in the design process was to develop a privacy-focused system that allows schools to issue certificates while giving the recipients centralised access to their data. To preserve the confidentiality and integrity of the parties in the network, only approved entities can join the network. However, this does not fully address the importance of decentralisation in this study. Decentralisation ensures that no single entity can exert undue control over the information, and the distribution of power is equalised. Additionally, tracking every alteration can prevent fraudulent and illegal adjustments. Transferring the solution to the Hyperledger network would be the next step towards achieving decentralisation. The previous sections explained why Hyperledger was chosen over competing alternatives. In comparison to other options, Hyperledger's orderer node distinguishes it. Bitcoin and Ethereum, two of the most prominent blockchains, use a consensus form known as probabilistic [25]. In this setting, nodes do not delegate decision-making authority to a central authority; instead, they compete to solve a computational problem f(x). When a node successfully solves the problem and adds it to the chain, the probability of the previous block being legitimate increases as the number of blocks in the chain grows, as shown by the expression P(blocki-1 valid) > P. (blocki valid). This means that the consensus is based on the P value, which indicates how likely it is that the newly added blocks are valid (Blocki valid). Hyperledger, on the other hand, uses a deterministic consensus rather than a probabilistic one [28]. When the orderer determines that a transaction should be recorded in the ledger, that decision is conclusive and applies to all affiliated organisations. Each organisation's peers will validate the transaction before sending it to the orderer, who will then package it and send it back to the peers for a final commit.

The proposed protocol comprises several entities, including the ministry, the university, and the student. The ministry is integrated into the system as a hardcoded entity, while universities are represented as organizations, and the channel encompasses the smart contracts. Fig. 3 shows the overall design of the proposed protocol.

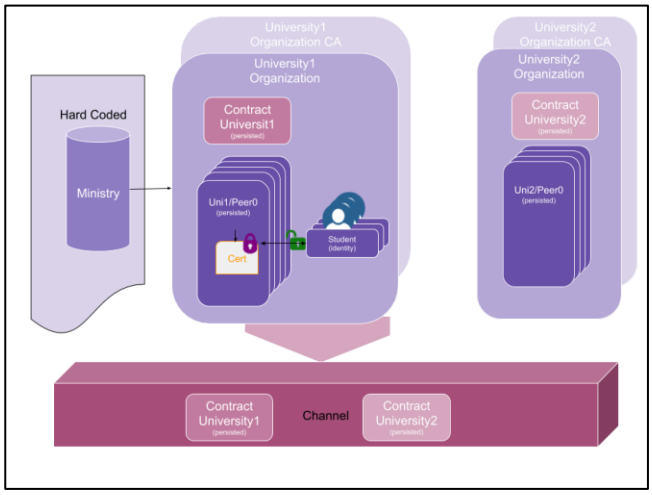


Fig. 3. The desing of the proposed decentralised certification verification privacy control protocol.

Since there is a finite number of ministries, they must be hard-coded into the Hyperledger's inception state. As an alternative, a trustworthy ministry may be hard-coded into the system and would then be able to invite other ministries to join the blockchain, granting them administrative access and allowing them to establish their own affiliated institutions. To maintain confidentiality, a channel is integrated into the suggested architecture.

Knowing one another is a precondition or perhaps a need in educational settings. Anonymity shouldn't play a defining role in the system since it runs counter to the logic of the actual world, where universities should be well-known institutions; it's also crucial to distinguish between anonymity and privacy, which are sometimes confused with one another. It makes no sense that different ministries or universities in other nations have no connection with each other, nor does it make sense that the ministry's own institutions are completely separate. In the actual world, the infrastructure dictates that the entities must be acquainted with one another and work together in some kind.

As a result of the channel implemented by Hyperledger, a relationship can exist among the network's nodes. Assume there are universities under various ministries, and these institutions have partnership programs, such as students taking classes at other universities. In this instance, the suggested protocol can ensure this. Using Hyperledger channels, governments can link together educational institutions so that students, faculty, and researchers from all over the world can easily share data. Hyperledger's architecture makes it possible to propose a solution that preserves privacy on the network and organisational level, making it an excellent place to introduce the protocol. This will ensure that universities worldwide can maintain control over their own data, regardless of which ministry or country is responsible for it. Within the bounds of etiquette, they are free to pursue a romantic partnership in secret. To protect the confidentiality of the network planned for issuing and verifying academic credentials, we present a novel protocol based on the Hyperledger fabric network. The following are the 11 steps of the suggested protocol, and its mathematical algorithm representation is presented in Fig. 4.

Step 1: The ministry, which is the higher authority in the network, creates organisations which are universities.

Step 2: Each ministry creates a channel that connects the universities, authenticated by that ministry.

Step 3: Each university (organisation) creates its own peers under it.

Step 4: Each company's peers maintain their own copy of the ledger and check all transactions before they are permanently recorded.

Step 5: Only universities can host the ledger.

Step 6: The university organization generates Identities for students.

Step 7: The university organization (admin) is the only entity that can issue certificates in the network.

Step 8: All certificates issued are locked in their initial state until the student issues an unlock command.

Step 9: The student can lock and unlock certificates.

Step 10: Third-party entities only need the certificate id, keys and the owner's name to validate and authenticate the certificate.

Step 11: No entity can authenticate a certificate if it is locked.

The suggested protocol gives unrestricted power over the network nodes. By using the channel to merge universities, they can have their own private domain, allowing for information sharing and complete privacy control over each entity. Ministries generate channels to prevent dubious organisations from operating within the network. Universities generate students, which limits the number of random users in the network. In addition, only peers generated by universities are authorised to host the ledger, reducing the risk of an attack and limiting the amount of access. With a decentralised approach, the final commit takes place only when the majority of connected peers approve.

1. MinistryN, N ∈**{**list of countries**},** n(Ministry) = *x, x is a constant*

*2.* Each MinistryN has *{University1,.....,University | i >0, i= identification of university}*

*3.* MinistryN → ChannelM, M= MinistryN

4. MinistryN → UniversityMi | UniversityMi ∈**{**MinistryN**},** M = MinistryN, i={identification of university},

5. ∀UniversityMi ∃ MinistryM

6. {UniversityM1…..,UniversityM} ⊆ ChannelM, M= MinistryN

7. UniversityMi → Peeri, {i ∈ N}

8. Ledger ⊆ Peer0,.....,Peeri

9. $University_{admin}$ → Identitys, {s ∈ Students}

10. $University_{admin}$ → Certificates, {s ∈ Students}

11. Students, s ∈ Students → Lock/Unlock(Certificates)

Fig. 4. The mathematical representation of the proposed protocol for preserving the privacy of identities of hyperledger fabric blockchain.

## IX. Implementation and Results

The implementation of the DCVPC protocol for privacy preservation in a blockchain-based academic certificates management system using Hyperledger Fabric would involve the following steps:

- Setting up the Hyperledger Fabric network: This would include installing the necessary software and dependencies, creating the network, and configuring the various components, such as the peer nodes and the ordering service.
- Developing the smart contract: The smart contract would be responsible for managing the academic certificates on the blockchain. It would include functions for creating, issuing, and verifying certificates and managing access control.
- Creating channels: channels would be created for each university participating in the network. These channels would provide a private environment for each university to manage its own academic certificates.
- Implementing access control: Access to the ledger would be restricted and controlled through the use of digital identities and verifiable credentials. Only authorised entities, such as universities and students, could access and make changes to the ledger.
- Implementing the certificate verification process: The certificate verification process would be automated using smart contracts. Verifiers would be able to easily access and verify the authenticity of certificates using the public key of the university.
- Developing the user interface: A user-friendly interface would be developed for universities and students to interact with the blockchain and manage their academic certificates.
- Testing and evaluating the proposed protocol: The proposed protocol would be tested and evaluated using a proof-of-concept to demonstrate its functionality and performance.
- Deployment: The final implementation would be deployed on a production network and made available for use by universities and other stakeholders. In the next subsections, the implementation steps are discussed.

### *A. Installing the Hyperledger Fabric on the Local System*

Setting up a Hyperledger Fabric network involves several steps including the following:

- Installing the Hyperledger Fabric software: This includes downloading the Hyperledger Fabric binaries, setting up the necessary environment variables, and installing any additional dependencies such as Go, Docker, and Node.js.
- Setting up the network: This includes creating the necessary configuration files for the network, such as the network topology and the configuration of the peer nodes and ordering service.
- Starting the network: This includes launching the peer nodes, ordering service, and other components of the network using the command line interface.
- Joining peers to the network: After the network is started, other peers can join the network by connecting to one of the existing peer nodes and obtaining the necessary configuration files.
- Creating channels: channels can be created by one of the existing peer nodes on the network, and other peers can join these channels by obtaining the necessary configuration files.
- Installing and instantiating chaincode: Smart contracts, also known as chaincode, can be installed and instantiated on the network by one of the existing peer nodes.
- Setting up the SDK: In order to interact with the network, a software development kit (SDK), such as the Hyperledger Fabric SDK for Node.js needs to be installed and configured.

To set up the Hyperledger Certificate-VPC network, certain prerequisites needed to be fulfilled. The network requires the use of Linux/MacOS operating systems to function correctly. The latest version of Hyperledger Fabric (v. 2.2) was installed on the Linux operating system version, as depicted in Fig. 5.

The aforementioned prerequisites were installed successfully by following the official Hyperledger documentation. For the installation, Hyper-V containing Ubuntu 14.04.3 LTS was used on a Windows 10 operating system. Fig. 6 displays a screenshot of Hyperledger Fabric running on the local system.

1. cURL — latest version
2. Docker — version 17.06.2-ce or greater
3. Docker Compose — version 1.14.0 or greater
4. Golang — version 1.11.x
5. Nodejs — version 8.x (other versions are not in support yet)
6. NPM — version 5.x
7. Python 2.7
8. Install Samples, Binaries and Docker Images

Fig. 5. Prerequisites needed to run the hyperledger fabric.

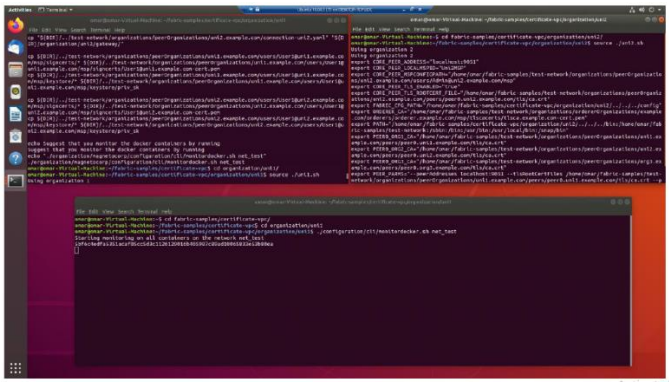

Fig. 6. Screenshot of hyperledger fabric running on the local system.

### B. Hyperledger Certificate-VPC Network

There are several requirements needed to be considered before creating the Certificate-VPC network, and they are as follows:

- Define the network actors.
- Define the peers.
- Define the channel.
- Define the transactions.

The proposed Hyperledger Certificate-VPC infrastructure setup is easily scalable, and the prototype proposed would contain one ministry that creates two universities, and each university creates two users and a peer. The network will suffice for the following:

- Certificate-VPC represents the whole network. One ministry over Hyperledger, which contains two organisations.
- Currently, there are two universities: university1 and university2. There are one or more peers for every organisation.
- A peer can be either a committing peer or an endorsing peer. We set up each organisation with one peer where chaincodes are installed in order to streamline the network configuration. Additionally, this peer commits to verifying transactions within a block.
- Despite the fact that a network may have more than one channel, as shown by the prior design, the Hyperledger Certificate-VPC is only constructed with one channel (the privacy channel).
- A channel is connected to a ledger (blockchain file) to log channel transactions.
- Transactions in Hyperledger Certificate-VPC are issuing, locking, unlocking, and requesting to verify the certificates.

After defining the requirements mentioned previously, setting up the Certificate-VPC network design is described in the next sections.

### C. Setting up the Hyperledger Certificate-VPC Network

To set up the Certificate-VPC network, certain Hyperledger Prerequisites are required, with Linux/MacOS being the preferred operating system. Running the network on Windows can be problematic due to issues with docker. Each main component of the network operates on its own docker. The key components of any Hyperledger network are organisations (in this case, universities) with their respective certificate authority and orderer, which has its own certificate authority. In this study, a ministry with the highest authority in the network will establish two universities/organisations, with the term "university" used to represent an organisation in the Hyperledger to avoid confusion. Uni1 and Uni2 are two hypothetical universities that belong to the ministry in the blockchain's genesis state. The namespace for the Hyperledger network is the URL for the solution, such as CertificateVerificationPrivacyControl.com. To simplify things, example.com is used, and components in the network are reached via a subdomain, such as order.example.com for the orderer and uni1.example.com and uni2.example.com for the universities. Each university has at least one peer represented in its own node as peer0.uni1.example.com. The universities and the orderer have been established, with each university having its own set of users, including students and peers. The administrators possess administrative privileges, whereas the users are granted client access, as demonstrated in Fig. 6. The only missing component is the channel that links these organizations together, as depicted in the illustration provided in Fig. 7. Once the CA server has been set up and all the necessary components have been added to the network, the network is considered to be partially operational. At this stage, two organizations and the orderer have been established, as displayed in Fig. 7. Each organization consists of both users and peers, with administrators possessing administrative privileges, while users are granted client rights.

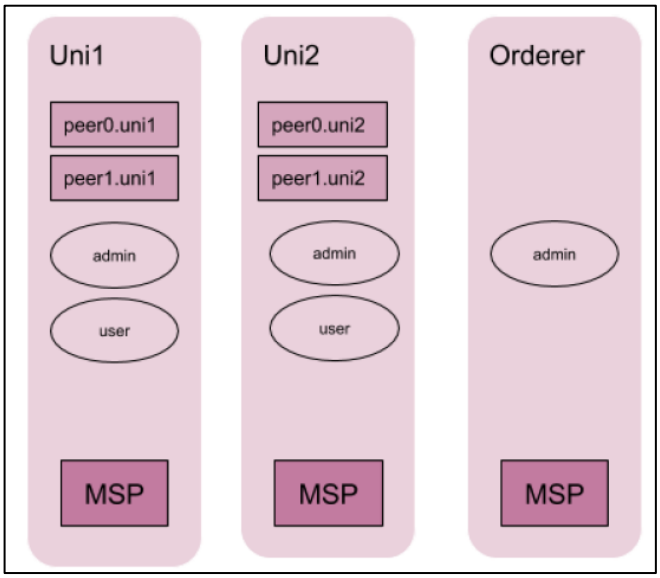


Fig. 7. Components of the created protocol.

With the DCVPC protocol, different types of policies at different layers have to be considered including the following:

*1) Network layer policy:* The policy describes the administrative capabilities of the network, which include the role of the ministry in adding universities and channels as outlined below.

- MinistryN, N ∈ {list of countries}, n(ministry) = x, x is a constant.
- Each MinistryN has {University1,.....,Universityi | i >0, i= identification of university}.
- MinistryN → add Universityi | i >0, i= identification of university.

*2) Channel layer policy:* This policy outlines the administrative privileges of members at the channel level. This policy permits universities operating under a particular ministry to share a channel and host replicas of the ledger to facilitate their contribution to the network. During the initial phase, all universities created by the ministry will share a single network.

Fig. 8 shows that a channel has been successfully created on Hyperledger Fabric, which includes three organizations represented as universities. The process involved defining the channel configuration, including the policies, orderer settings, and member organizations, where the three universities would be the member organizations. The channel was then created using the Hyperledger Fabric CLI tool or SDK, and during the channel creation process, each university was required to join the channel by creating and signing a certificate and submitting a request to the orderer to join the channel. Once all three universities had joined the channel, they were able to interact with each other and share data, such as academic certificates. This channel provided a secure and private means of communication between the member organizations, ensuring that all transactions were validated and recorded accurately.

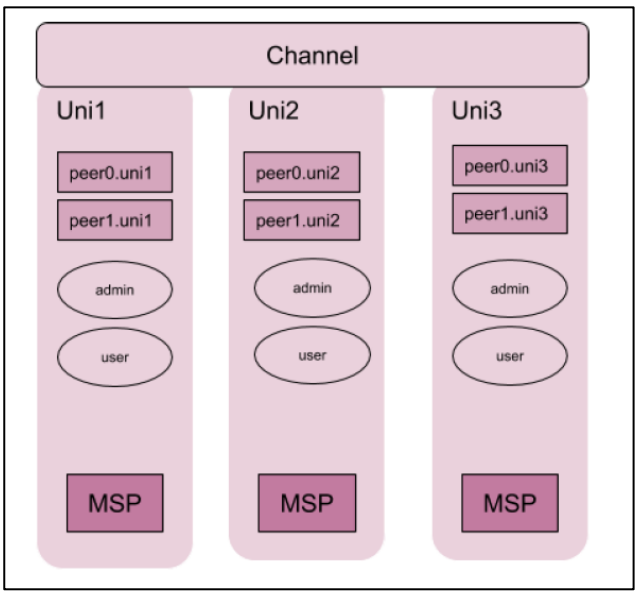


Fig. 8. Channel generation.

*3) Endorsement policy:* The policy being discussed outlines the criteria that must be met to establish the legitimacy of a transaction before it can be recorded on the blockchain. It's important to note that the endorsement policy, if set to something other than the default, would be defined in the configtx.yaml file. By default, the majority of organizations must approve the chaincode before it can be committed to the channel, which will be detailed in the following steps. This policy is sufficient for the design of DCVPC. Once the peers have joined the network, the ledger will consist of three blocks: the initial block created when the channel was established, and two additional blocks for each peer that joins the channel. With this step, most of the proposed design requirements for DCVPC are satisfied.

### *D. Universities Set Up Network starter*

To set up the Hyperledger Fabric network, the first step is to generate all required digital certificates, identities of users, and components in the network. This involves using tools such as Hyperledger Fabric's cryptogen or a certificate authority deployed to each organization. To allow entities to use the network, each organization has a Membership Service Provider (MSP) or Certificate Authority (CA) responsible for generating crypto material, which includes private keys and digital certificates. The MSP acts as an identifier for each organization, and all organizations must know each other's MSPs to validate resulting identities. It is essential for university identities to be known and not anonymous, reflecting real-life situations where ministries oversee and monitor universities. Therefore, it is important to identify all file paths for each identity file in the docker-compose configuration file. After generating the crypto material, the necessary components such as organizations, peers, and orderers are started through the use of docker containers. All organizations participating in the network must know each other's MSPs to ensure the validity of transactions [17].

In the design of the blockchain network, the Membership Service Provider (MSP) is essential to identify the organisations participating in the network. An example of this is if an organisation called UUM generates a user named Ahmed using its MSP, other organisations should be able to identify from the signature that Ahmed belongs to UUM, and that UUM is a part of the network. All organisations within the network know each other's MSPs, making it crucial for university identities to be known and not anonymous. This reflects real-life situations where ministries tend to publicise and monitor the universities they oversee. It is also essential for external entities to identify the existing universities. Hiding the identity of universities within the network does not reflect real-life situations, so it was critical to consider this in the design process. The docker-compose configuration file identifies all file paths for each identity file. As shown in Fig. 9, Uni1's identity files are identified in the Docker-Compose configuration file.

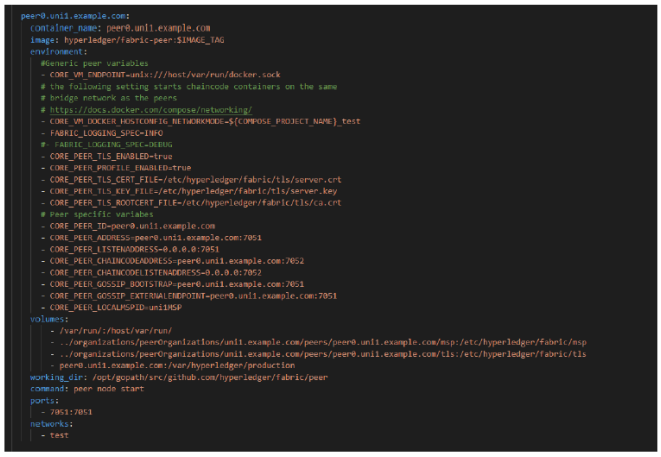


Fig. 9. Uni1 identity files are identified in the docker-compose configuration file.

In the volumes block, we can observe that the MSP configuration is mapped to the path peers/peer0.uni1.exampl.com/msp. When the network is loaded, all the necessary files will be installed in this location. Hyperledger Fabric provides two methods to generate crypto material in the network: using a tool called cryptogen or a certificate authority server. Cryptogen streamlines the identity setup process by automating the generation of crypto material with minimal manual setup. Hyperledger also includes ready-made scripts, such as network.sh, to accelerate the setup process. By executing the network.sh script, the required identities are created using cryptogen and all necessary files are loaded into the corresponding folder path specified in the docker-compose configuration. The command to accomplish this is "cryptogen generate --config=<> --output=<>," with "config" referring to the configuration file defined for each organisation and orderer node inside the cryptogen/*.yaml folder. Certain configurations must be in place before starting the network, including each node's configuration in the cryptogen configuration file. The "Count" parameter under "Users" sets the number of users to generate for the university. Once the network.sh script has been executed, the running docker images can be listed, as shown in Fig. 10. Each docker container hosts a specific component in the network.


Fig. 10. List of the docker images running.

The Docker configuration file that sets up the network can be found in the file named docker-compose-test-net.yaml. Once the network is up and running, you can access the ledger on either peer using the command docker exec <container-id> peer channel getinfo -c <channel-name>.

By starting the necessary containers and setting up the network, we can observe that the blockchain height is seven blocks, and we will explain the reason behind this shortly. Instead of using the container ID, we can refer to the peer using its name, which in this prototype includes two organizations, uni1 and uni2, and one orderer. For each organization, we have added specific files, and you can find the list of Hyperledger Fabric files in Fig. 11.

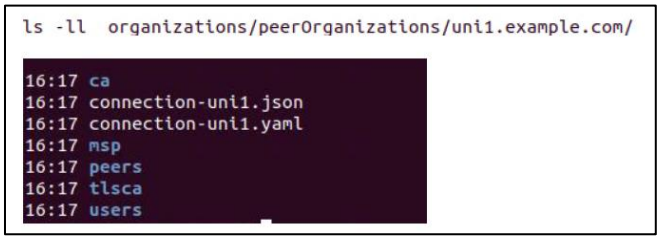


Fig. 11. List of hyperledger fabric files.

The directories for peers and users contain lists of the respective peers and users associated with the organisation. An example of this can be seen in Fig. 12, which displays two main users - Admin and User1.

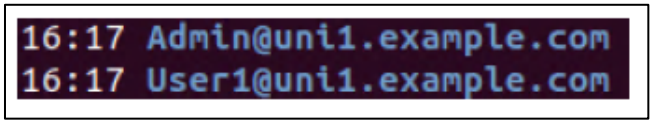


Fig. 12. Users of each organisation.

When we navigate to the users' folders, we can find two sub-folders - msp and tls. The msp folder contains information related to the Membership Service Provider, including the credentials for the user. For instance, for the admin user, we can see the following information inside the msp folder. Additionally, the tls folder contains Transport Layer Security certificates that ensure secure communication between nodes. To get a better understanding of the contents of these folders, refer to Fig. 13, which displays their contents for all users.

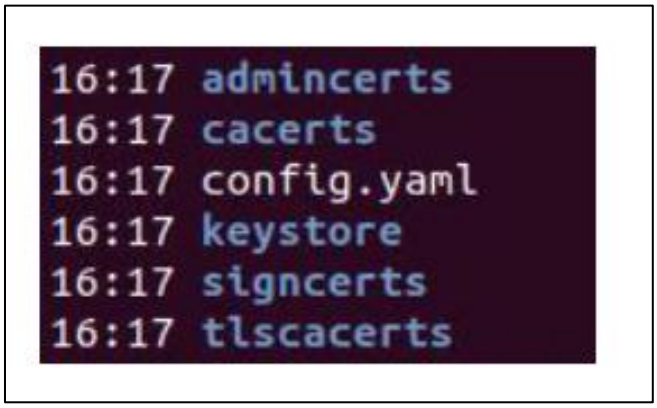


Fig. 13. Users of MSP and TLs folder.

The "keystore" directory stores the private key, while the "signcerts" directory contains the certificate for each user. We can determine a user's assigned role by running the command 'openssl x509 -in organizations/peerOrganizations/uni1.example.com/users/User1@uni1.example.com/msp/signcerts/User1@uni1.example.com-cert.pem -noout -subject'. In the case of User1, the role is set as a client. The "ca" directory holds all cryptographic materials, including the private key and certificate for uni1, which can be viewed by running the 'ls'

command. Although "cryptogen" is fast and easy to use, it lacks flexibility when adding or loading entities to the network after deployment. For more control over the certificate generation process, we can use the Fabric CA server. This server hosts the CA, which consists of the private key and CA certificate. To start the network using the Fabric CA server, we can use the same script as before but with the option '-ca'. This will prompt the Fabric-CA-Client tool, which assigns a Fabric CA Admin to manage the addition of entities to the network. To assign the admin for the first university (admin:adminpw are the login details, which can be changed), we can execute the command shown in Fig. 14.

```
fabric-ca-client enroll -u https://admin:adminpw@localhost:7054 --caname ca-uni1 --tls.certfiles ${PWD}/organizations/fabric-ca/uni1/tls-cert.pem
```

Fig. 14. Sample code for fabric-CA-client to assign a fabric CA admin

When adding users to the network, the script "./network.sh" calls another script named "registerEnroll.sh". This script is responsible for registering and adding users to the network, along with their respective roles. To add a user named Ahmed to the first university, we need to follow these two steps:

Register Ahmed as a client by executing the following code shown in Fig. 15:

```
fabric-ca-client register --caname ca-uni1 --id.name ahmed --id.secret ahmedpw --id.type client --tls.certfiles ${PWD}/organizations/fabric-ca/uni1/tls-cert.pem
```

Fig. 15. Sample code for registering the users.

Note that if Ahmed were an admin instead of a client, the "type" parameter would be set to "admin".

Generate Ahmed's MSP by executing the code shown in Fig. 16.

```
fabric-ca-client enroll -u https://ahmed:ahmedpw@localhost:7054 --caname ca-uni1 -M ${PWD}/organizations/peerOrganizations/uni1.example.com/users/Ahmed@uni1.example.com/msp --tls.certfiles ${PWD}/organizations/fabric-ca/uni1/tls-cert.pem
```

Fig. 16. Sample code for generating the users' MSP.

Once the network is up and running, Ahmed will be successfully registered, as shown in Fig. 17.

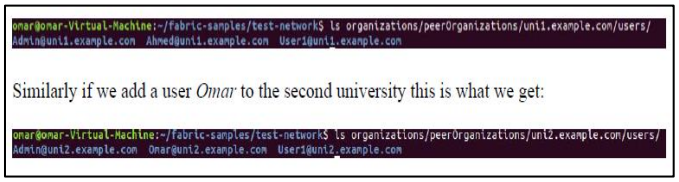


Fig. 17. Output of user get registered.

### E. Channel Creation

Creating a channel in Hyperledger Fabric can be easily accomplished by using the same script used to start the network with the command ./network.sh createChannel. In this command, $CHANNEL_NAME is the variable that sets the channel title. Behind the scenes, a tool called configtxgen is used to create the initial transactions, including the configuration transaction and the peer update transaction for each peer in the intended organizations. These initial transactions prepare the genesis block in the network, which is block #0 and sets the channel. Once the genesis block is set, peers can join the channel using the same block. For example, Fig. 18 displays sample code for creating a channel, while Fig. 19 shows the configuration file of the created channel.

```
peer channel create -o localhost:7050 -c $CHANNEL_NAME --ordererTLSHostnameOverride orderer.example.com -f ./channel-artifacts/${CHANNEL_NAME}.tx --outputBlock ./channel-artifacts/${CHANNEL_NAME}.block --tls --cafile $ORDERER_CA
```

Fig. 18. Sample code for creating the channel.

```
Configtx.yaml
Profiles:
TwoOrgsOrdererGenesis:
<<: *ChannelDefaults
Orderer:
<<: *OrdererDefaults
Organizations:
- *OrdererOrg
Capabilities:
<<: *OrdererCapabilities
Consortiums:
SampleConsortium:
Organizations:
- *Uni1
- *Uni2
TwoOrgsChannel:
Consortium: SampleConsortium
<<: *ChannelDefaults
Application
<<: *ApplicationDefaults
Organizations:
- *Uni1
- *Uni2
Capabilities:
<<: *ApplicationCapabilities
```

Fig. 19. The configuration file of the created channel.

After the process of setting up the CA server and adding the components to the network, the network is somewhat ready. So to package the smart contract into a chaincode, the command is as follows:

peer lifecycle chaincode package unicontr.tar.gz --lang node --

path ~/contract --label cp_0 ./contract

In the above command, the lang specifies the execution language. ~/contract is the path to the smart contract to package. The end result of the above command is a tar.gz file that the admin of that active university can install. The installation is straightforward using the command install. Peer lifecycle chaincode install unicontr.tar.gz . After the installation step is done, the approval process should take place. Each installed chaincode has its own identifier which will allow for determining which chaincode to approve. Because the identifier is a long string, it is easier just to export it as an environment variable. The approval command initiated by the admin is as follows:

peer lifecycle chaincode approveformyorg --orderer localhost:7050 --ordererTLSHostnameOverride orderer.example.com --channelID mychannel --name papercontract -v 0 --package-id $PACKAGE_ID --sequence 1 –tl

An example of the results of implementing a Certificate Verification Privacy Control Protocol (DCVPC) based on the Hyperledger Fabric blockchain might include:

- Improved security: The use of Hyperledger Fabric blockchain ensures that the certificate issuance and verification process is secure, as all transactions are recorded on a tamper-proof ledger.
- Increased transparency: The CVPC protocol allows for increased transparency during the certificate issuance and verification process, as all transactions are recorded on the blockchain and can be easily audited.
- Reduced fraud: The use of smart contracts and digital signatures in the CVPC protocol can greatly reduce the possibility of fraud, as all certificates are verified and authenticated on the blockchain.
- Improved privacy: The CVPC protocol includes privacy-preserving protocols such as zero-knowledge proofs (ZKP) and homomorphic encryption (HE) to ensure that the personal information of certificate holders is protected during the process of issuance and verification.
- Better interoperability: The use of Hyperledger Fabric blockchain allows for better interoperability among different systems, as the CVPC protocol can communicate with other blockchain networks.
- Automated certificate verification process: smart contracts and blockchain technology automate the certificate verification process and make it more efficient.

## X. Discussion

In this study, we introduce a novel protocol, called Decentralised Control Verification Privacy-Centered (DCVPC), which utilizes Hyperledger Fabric blockchain technology to preserve the privacy of academic certificates. The DCVPC protocol aims to address the limitations of current blockchain-based academic certificate management systems in terms of security and privacy. This is achieved by providing complete authority over all network nodes, establishing private environments for universities, and limiting access to the ledger.

The DCVPC protocol has been designed with a strong emphasis on security, and it is resistant to attacks by restricting access to the ledger and requiring approval from the most connected peers before committing any changes. Additionally, the use of Hyperledger Fabric blockchain technology improves interoperability and automation in the certificate verification process.

We implemented the proposed protocol and developed a proof-of-concept, demonstrating its effectiveness in preserving privacy during the academic certificate issuance and verification process. Our proof-of-concept provided valuable insights into the strengths and weaknesses of the DCVPC protocol and highlighted its potential for preventing forgery and unauthorized access to academic certificates.

One of the significant advantages of the DCVPC protocol is its use of digital identities and verifiable credentials for access control. This ensures that only authorized entities can access and manage academic certificates on the network, which helps to prevent fraud and forgery. Consequently, only deserving individuals can utilize their certificates for education and career opportunities.

In conclusion, the DCVPC protocol has shown promising results in preserving the privacy and security of academic certificates, preventing unauthorized access, and providing a trusted and reliable verification process. By utilizing Hyperledger Fabric blockchain technology and digital identities, our proposed protocol presents a significant step towards achieving a transparent and trustworthy academic certificate management system.

In conclusion, the proposed DCVPC protocol, based on the Hyperledger Fabric blockchain, is a promising solution for improving academic certificates' security, transparency and privacy. Furthermore, we can apply the protocol to other blockchain-based systems to manage educational credentials and enhance it further by incorporating other privacy-enhancing technologies, such as zero-knowledge proofs.

## XI. Conclusion

Academic fraud is a significant concern, including both impersonation of certificate recipients and the fabrication of educational institutions. The fake university problem arises when a non-legitimate institution creates a seemingly acceptable academic certificate, while the impersonated receiver problem arises when a person pretends to be the legitimate certificate recipient. Managing authority is also a significant challenge in academic certificate management. Access to resources should be tailored to the responsibilities of

each role. The diploma system involves students, universities, and verifiers, but educational authorities play a crucial role in overseeing institutions at all levels, despite not directly issuing certificates.

This study highlights the importance of Hyperledger Fabric for managing the privacy aspect of academic certificate management systems. We have developed Decentralised Control Verification Privacy-Centered (DCVPC) based on the Hyperledger Fabric blockchain to address these issues. The DCVPC protocol can significantly improve the certificate issuance and verification process by leveraging the security and transparency of the blockchain, as well as privacy-preserving protocols such as zero-knowledge proofs (ZKP) and homomorphic encryption (HE). Additionally, the interoperability and automation of the process provided by the Hyperledger Fabric blockchain can make the process more efficient and streamlined.

It is important to note that the specific results will depend on the particular requirements and constraints of the application, as well as the specific implementation of the DCVPC protocol on the Hyperledger Fabric blockchain. Nonetheless, the DCVPC protocol based on the Hyperledger Fabric blockchain shows great promise in significantly improving the certificate issuance and verification process while preserving the privacy of certificate holders. By addressing the challenges of authority management, academic fraud, and privacy, the DCVPC protocol presents a significant step towards achieving a trustworthy and transparent academic certificate management system.

## ACKNOWLEDGMENT

This research was supported by Ministry of Higher Education (MoHE) of Malaysia through Fundamental Research Grant Scheme (FRGS/1/2018/ICT04/UUM/02/17).

## REFERENCES

[1] KTBS.com (2021). Caddo school employee accused of selling fake diplomas, transcripts. Retrieved July 10, 2021, from https:// www. ktbs. com/ news/ caddo- school- emplo yee- accus ed- of- selli ng- fake- diplomas- trans cripts/ artic le_ 0d8e4 eee- e0ea- 11eb- ae2a- af6ce 64324 33. Html.

[2] Abreu, A. W. S., Coutinho, E. F., & Bezerra, C. I. (2020). A blockchain-based architecture for query and registration of student degree certificates. In Proceedings of the 14th Brazilian Symposium on Software Components, Architectures, and Reuse, 151–160.

[3] Aini, Q., Rahardja, U., Tangkaw, M. R., Santoso, N. P. L., & Khoirunisa, A. (2020). Embedding a blockchain technology pattern into the QR code for an authentication certificate. Jurnal Online Informatika, 5(2), 39–244.Alam, S. (2021). A blockchain-based framework for secure educational credentials. Turkish Journal of Computer and Mathematics Education, 12(10), 5157–5167. https:// doi. org/ 10. 17762/ turco mat. v12i10. 5298.

[4] Ataşen, K., & Aslan, B. A. (2020). Blockchain Based Digital Certification Platform: CertiDApp. Journal of Multidisciplinary Engineering Science and Technology, 7(7), 12252–12255. From https:// www. jmest. org/ wp- conte nt/ uploa ds/ JMEST N4235 3434. Pdf.

[5] Caldarelli, G., & Ellul, J. (2021). Trusted academic transcripts on the blockchain: a systematic literature review. Applied Sciences, 11(4), 1842.

[6] Capece, G., Levialdi Ghiron, N., & Pasquale, F. (2020). Blockchain technology: redefining trust for digital certificates. Sustainability, 12(21), 8952.

[7] Castro, R. Q., & Au-Yong-Oliveira, M. (2021). Blockchain and higher education diplomas. European Journal of Investigation in Health, Psychology and Education, 11(1), 154–167.

[8] Chaniago, N., Sukarno, P., & Wardana, A. A. (2021). Electronic document authenticity verification of diploma and transcript using smart contract on Ethereum blockchain. Register: Jurnal Ilmiah Teknologi Sistem Informasi, 7(2), 149–163.

[9] Kshetri, N. (2017). Blockchain's roles in strengthening cybersecurity and protecting privacy. Telecommunications policy, 41(10), 1027–1038.

[10] Vidal, F. R., Gouveia, F., & Soares, C. (2020a). Revocation mechanisms for academic certificates stored on a blockchain. In 2020 15th Iberian Conference on Information Systems and Technologies, 1–6.

[11] Karamachoski, J., Marina, N., & Taskov, P. (2020). Blockchain-based application for certification management. Technical Journal, 14(4), 488–492.https:// doi. org/ 10. 31803/ tg- 20200 81111 3729.

[12] Rahardja, U., Kosasi, S., & Purnama Harahap E., & Aini Q. (2020). Authenticity of a diploma using the blockchain approach. International Journal of Advanced Trends in Computer Science and Engineering, 9(1.2), 250-256.

[13] Bapat, C. (2020). Blockchain for Academic Credentials, from https:// arxiv. org/ abs/ 2006. 12665.

[14] Baldi, M., Chiaraluce, F., Kodra, M., & Spalazzi, L. (2019). Security analysis of a blockchain-based protocol for the certification of academic credentials, from https:// arxiv. org/ abs/ 1910. 04622.

[15] Nakamoto, S. (2008). Bitcoin: A peer-to-peer electronic cash system. Decentralised Business Review, 21260.

[16] Wang, Y., & Kogan, A. (2018). Designing confidentiality-preserving blockchain-based transaction processing systems. International Journal of Accounting Information Systems, 30, 1–18.

[17] Hyperledger (2020). A blockchain platform for the enterprise. Retrieved July 10, 2021, from https:// hyperledger- fabric. readt hedocs. io/ en/ latest.

[18] Li, R. & Wu, Y. (2018). Blockchain based academic certificate authentication system overview. IT Innov. Centre, Univ. Birmingham, 8.

[19] Block.co (2021). Retrieved July 10, 2021, from https:// block. Co

[20] Andreev, O., & Daskalov, H. (2018). A framework for managing student data through blockchain. In Proceedings of international scientific conference e-governance and e-communications.

[21] Han, M., Li, Z., He, J., Wu, D., Xie, Y., & Baba, A. (2018). A novel blockchain-based education records verification solution. In Proceedings of the 19th annual SIG conference on information technology education (pp. 178–183).

[22] Bessa, E. E., & Martins, J. S. (2019). A blockchain-based educational record repository. arXiv preprint arXiv:1904.00315.

[23] Hope, J. (2019). Give students ownership of credentials with blockchain technology. The Successful Registrar, 19(1), 1–7.

[24] Wang, R., He, J., Liu, C., Li, Q., Tsai, W. T., & Deng, E. (2019). A Privacy-Aware PKI System Based on Permissioned Blockchains. Proceedings of the IEEE International Conference on Software Engineering and Service Sciences, ICSESS, 2018-Novem, 928–931. https://doi.org/10.1109/ICSESS.2018.8663738.

[25] Fabric, H. (2018). A Distributed Operating System for Permissioned Blockchains.

[26] Brotsis, S., Kolokotronis, N., Limniotis, K., Bendiab, G., & Shiaeles, S. (2020, October). On the security and privacy of hyperledger fabric: Challenges and open issues. In 2020 IEEE World Congress on Services (SERVICES) (pp. 197-204). IEEE.

[27] Liang, Y. C. (2020). Blockchain for dynamic spectrum management. In Dynamic Spectrum Management (pp. 121-146). Springer, Singapore.

[28] Alammary, A., Alhazmi, S., Almasri, M., & Gillani, S. (2019). Blockchain-based applications in education: A systematic review. Applied Sciences, 9(12), 2400.

[29] Iftekhar, A., Cui, X., Tao, Q., & Zheng, C. (2021). Hyperledger fabric access control system for internet of things layer in blockchain-based applications. Entropy, 23(8), 1054.

[30] K. Verma, R. Singh, and A. Verma, "Blockchain technology for secure and efficient management of academic certificates," International

Journal of Advanced Research in Computer Science, vol. 9, no. 1, pp. 1–7, 2018.

[31] A. Kshetri, "Blockchain technology for privacy and security in online social networks," IEEE Communications Magazine, vol. 56, no. 9, pp. 34–40, 2018.

[32] Y. Chen, Y. Liu, Y. Zhang, and D. Li, "A privacy-preserving blockchain-based framework for academic certificate verification," IEEE Access, vol. 8, pp. 152428–152437, 2020.

[33] S. H. L. Leong, J. H. M. Lee, and K. W. Chan, "A blockchain-based framework for secure and privacy-preserving academic certificate verification," IEEE Access, vol. 8, pp. 57826–57835, 2020.

[34] J. H. Lee, H. S. Kim, and Y. S. Lim, "A blockchain-based secure and privacy-preserving framework for academic certificate verification," IEEE Access, vol. 7, pp. 123361–123369, 2019.

[35] K. Verma, R. Singh, and A. Verma, "Blockchain technology for secure and efficient management of academic certificates," International Journal of Advanced Research in Computer Science, vol. 9, no. 1, pp. 1–7, 2018.

[36] T. Islam, M. R. Chowdhury, and S. A. R. Hossain, "A blockchain-based secure and privacy-preserving framework for academic certificate verification," IEEE Access, vol. 8, pp. 99788–99798, 2020.

[37] J. Xiong, Y. Li, and X. Shen, "A blockchain-based secure and privacy-preserving framework for academic certificate verification," IEEE Access, vol. 8, pp. 141530–141538, 2020.

[38] Y. Chen, Y. Liu, Y. Zhang, and D. Li, "A privacy-preserving blockchain-based framework for academic certificate verification," IEEE Access, vol. 8, pp. 152428–152437, 2020.

[39] S. H. L. Leong, J. H. M. Lee, and K. W. Chan, "A blockchain-based framework for secure and privacy-preserving academic certificate verification," IEEE Access, vol. 8, pp. 57826–57835, 2020.

[40] J. H. Lee, H. S. Kim, and Y. S. Lim, "A blockchain-based secure and privacy-preserving framework for academic certificate verification," IEEE Access, vol. 7, pp. 123361–123369, 2019.

[41] Saleh, O. S., Ghazali, O., & Rana, M. E. (2020). Blockchain based framework for educational certificates verification. Journal of critical reviews, 7(03), 79-84.

[42] Pathak, S., Gupta, V., Malsa, N., Ghosh, A., & Shaw, R. N. (2022). Blockchain-Based Academic Certificate Verification System—A Review. Advanced Computing and Intelligent Technologies: Proceedings of ICACIT 2022, 527-539.

[43] Awaji, B., Solaiman, E., & Albshri, A. (2020, July). Blockchain-based applications in higher education: A systematic mapping study. In Proceedings of the 5th international conference on information and education innovations (pp. 96-104).

[44] Nguyen, B. M., Dao, T. C., & Do, B. L. (2020). Towards a blockchain-based certificate authentication system in Vietnam. PeerJ Computer Science, 6, e266.

[45] Cheng, H., Lu, J., Xiang, Z., & Song, B. (2020). A permissioned blockchain-based platform for education certificate verification. In Blockchain and Trustworthy Systems: Second International Conference, BlockSys 2020, Dali, China, August 6–7, 2020, Revised Selected Papers 2 (pp. 456-471). Springer Singapore.

[46] Curmi, A., & Inguanez, F. (2019). Blockchain based certificate verification platform. In Business Information Systems Workshops: BIS 2018 International Workshops, Berlin, Germany, July 18–20, 2018, Revised Papers 21 (pp. 211-216). Springer International Publishing.

[47] Din, I. U., Guizani, M., Kim, B. S., Hassan, S., & Khan, M. K. (2018). Trust management techniques for the Internet of Things: A survey. IEEE Access, 7, 29763-29787.

[48] Peffers, K., Tuunanen, T., Rothenberger, M. A., & Chatterjee, S. (2007). A design science research methodology for information systems research. Journal of management information systems, 24(3), 45-77.