

*Article*

# **Blockchain Adoption in Education with Enhancing Data Privacy through Hyperledger Fabric**

**Khadeejah Abdullah<sup>1</sup>, Kassem Saleh<sup>1</sup> and Paul Manuel<sup>1</sup>**

<sup>1</sup> Kuwait University, Kuwait

Khadeejah.abdullah@ku.edu.kw

(Article history: Received December 05, 2025; Received in revised form January 04, 2026;  
Accepted February 10, 2026; Available online June 15, 2026)

**Abstract:** Blockchain technology adoption has influenced several fields, including healthcare, finance, and supply chain systems. Lately, this technology has expanded its application in education because of its unique attributes, which are decentralization, immutability, consensus, and security. Despite the bright side of centralized credentialing and implementation, there are some challenges that need to be addressed. Thus, a comprehensive literature review of the reasons that blockchain adoption in the education field is considered necessary and effective. To do so, we investigate and explore the benefits and gaps of decentralized credentialing systems that are utilized to securely issue, verify, and share digital credentials such as grades, degrees, diplomas, and certificates through the simulation of blockchain and smart contract embedded logic. In this paper, we focus on two major themes: the adoption of blockchain in education and enhancing data privacy on blockchain through the means of a consensus algorithm. We express and analyze the results conducted as experimental simulations by stakeholders, which are university administrations, professors, and students, when combining the two themes to propose a solution in terms of trust and adoption to enhance the privacy and security of student learning data and maintain individual privacy rights. We have discussed the methodology which is Design Science Research (DSR) and evaluated the results to emphasize the significance of blockchain in education. We believe there is future work in enhancing the logic and validation of smart contract through means of hashing and cryptography.

**Keywords:** Blockchain, Smart Contract, Consensus, Hash, Distributed Ledger, Timestamp, Immutability, P2P

## **1. Introduction**

A whitepaper [18] was published by Satoshi Nakamoto in 2008, revealing Bitcoin and its underlying technology, named blockchain. Blockchain [1,19] is referred to as a distributed database that chronologically stores a chain of data sealed into blocks that run in a secure, immutable manner, known as a ledger. New blocks are appended to the end of the chain, in which each block holds a reference to the previous block's content using the SHA256 hash algorithm [13], ensuring immutability and compactness of the block. This startling concept has attracted a lot of attention from the financial industry. Following the financial institutions, different fields such as healthcare, software industries, and education began to introduce and apply this technology. Blockchain is a technology that eliminates the presence of centralized authority, as all blockchain operations and transactions must be stored securely on a decentralized distributed ledger. As a result, blockchain consists of different layers, and each layer comprises its unique functionality and objective, such as infrastructure, consensus algorithm, smart contract, and application. In financial institutions, to this date, processing of transactions traditionally utilizes intermediation or third-party collaboration. However, the collapse of the investment bank Bear Sterns in 2008 [17] has established the necessity and reliability of distributed digital transactions. This is the starting point towards blockchain, built on proven hash signatures and digital cryptographic algorithms. Blockchain [16] can maintain the history of all transactions by means of timestamps and asymmetric cryptography. Another notable institution that adopted blockchain technology is education [1]. The future of learning will be upgraded using blockchain technology in terms of data privacy and usability. By means of this technology, teachers, university administrators, and students create academic records in a chronological list of events in real time and store the records in an immutable ledger with a high degree of visibility and transparency.

The content of the ledger is synchronized across peer-to-peer (P2P) network as a distributed ledger. There are three main types of blockchains, which are public (not permissioned), private (permissioned), and consortium blockchain (hybrid) [18].

### *1.1. Problem Statement*

A vast amount of sensitive data about students is collected and stored in educational institutions in centralized data centers, including personal information, academic records, and financial data. Any failure in privacy and security on the students' data management will be a disaster to the education institutions.

### *1.2. Research Hypothesis*

Blockchain applied in education can revolutionize the learning experience and the data management of students' data. It will protect the data privacy of students and teachers while allowing participants to reach a consensus by creating an immutable record in the distributed ledger.

### *1.3. Research Objectives*

- Study the impacts of privacy and safety of students' data in transit under a blockchain environment by simulation.
- Assess how blockchain can overcome the current limitations in the education system.

#### *1.4. Research Outcomes*

- Enhanced data privacy of student data and related documents.
- Optimized processes and transactions under the blockchain environment.

## **2. Literature Review**

The evolution of blockchain began with cryptocurrency and has paved the way toward developing smart contracts in areas such as healthcare [10], supply chain, real estate management, etc. The emphasis on blockchain adoption is due to its ability to build a trusted and decentralized environment. Hence, the higher education sector is a potential user for implementing blockchain technology because of its capability to give control to stakeholders to validate learning records and identity management [1,2,3,4,5]. For instance, different institutions can decide with which other institutions to share data to avoid falsified grades or certificates. Additionally, the removal and lack of need for a trusted third party can introduce distributed ledgers that improve smart-contract-based protocols throughout multiple levels of administration, which is automatically enforced for the higher education field, with the ability to ease processes while mitigating the probability of error.

A global blockchain-based higher education credit platform, named EduCTX, is based on the concept of the European Credit Transfer and Accumulation System (ECTS), which offers a globally unified viewpoint for students and higher education institutions (HEIs) involving potential stakeholders, such as companies and organizations [2]. Basically, it presents a prototype implementation of the environment based on the open-source Ark Blockchain platform as a distributed peer-to-peer network that processes, manages, and controls ECTX tokens, which represent student credits that they gain for completed courses. EduCTX utilizes the benefits of blockchain, for instance, a decentralized architecture, security, immutability, integrity, transparency, anonymity, and longevity, to create a global grading system using a proof-of-concept prototype. The adoption and implementation of EduCTX faces challenges in terms of data privacy due to the fact that students' academic records are sensitive and have complicated management regulations [2].

The process in which a next block is generated by solving a complex cryptographic puzzle using lot of computational power is known as Proof of Work (PoW) consensus [5], while Byzantine Fault Tolerance is an algorithm objective is to safeguard the system from failure by employing collective decision making (correct and faulty nodes) to limit the influence of the faulty nodes, and it is based on Byzantine Generals' problem [18, 11]. There is a common alternative to PoW, which is Proof of Stake (PoS) that Ethereum have shifted to because this type of consensus rather than invest on expensive hardware, it employs validators that invest in the coins of the system by locking up them as stakes, and a validator

chooses to generate a new block based on its economic state in the network. The PoS mechanism requires validators to lock up their assets in a smart contract; hence, blockchains utilizing the PoS mechanism must ensure their smart contracts are secure. The consequences of dishonesty in PoS and PoW are similar, as validators lose staked assets in PoS, whereas, in PoW, they lose money spent on hardware and power.

### **3. Methodology**

#### *3.1. Design Science Research*

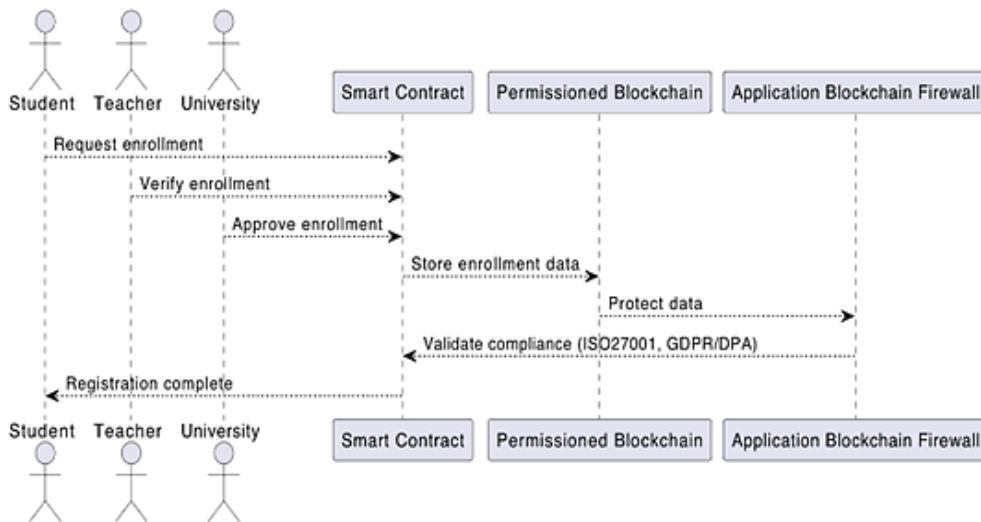
In this paper, we select the Design Science Research (DSR) problem solving paradigm that aim to improve human knowledge by following the creation of innovative artifacts, DSR seek to create artifacts to enhance technology and science knowledge for a problem in an environment which lead to results that include both design knowledge and newly designed artifacts providing better understanding in the design theory of how the artifact can enhance the relevant concept and context [12]. The artifacts are created as sequence diagrams with an activity diagram explaining the algorithm for building a blockchain for education.

#### *3.2. Network Design Description*

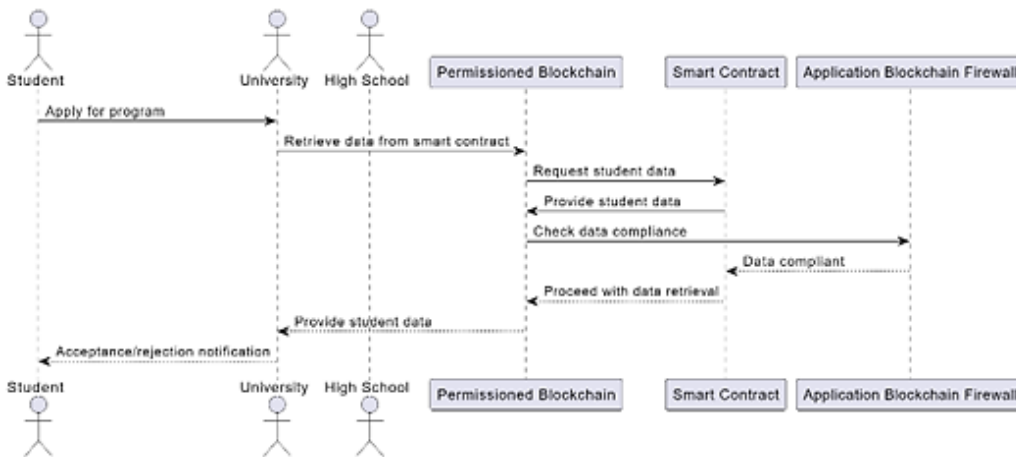
In education, we can apply blockchain following a benchmark and best practices as the amount of encryption is Asymmetric-key algorithm and hash function across every node, privacy of data is secured in every block due to the fact every node consist of private key and public address, and when a node takes part in any transaction, only public address get shared, consensus algorithm is embedded to ensure identity verification, where we can utilize legal framework ISO27001 in conjunction with GDPR to protect Personal Identification Information (PII) following a smart contract as a function of blockchain which is validated and implemented then shared across a peer-to-peer network to form distributed ledger technology. The smart contract policy is established with cryptography as a cybersecurity control method, and it provides a powerful capability of code execution for embedding business logic on the blockchain. The smart contract could be directed toward three main classifications of blockchains, such as public, private, and permissioned [14].

The artifact design or diagram emphasizes the role of smart contracts in the contract layer as an algorithm and mechanism to provide a robust framework for managing student enrollments, exam results, and certifications on the blockchain, which allows for seamless payment and certification process [3]. The smart contract for education is a self-executing agreement with predefined conditions, and the contract can optimize the learning experience by accepting payments in a certain cryptocurrency that students can hold in their digital wallet. We can introduce smart contracts to educational institutions to provide transparency. We can leverage the verifiable records of grades and achievements of students by complying with regulatory frameworks such as ISO27002 and GDPR/DPA for data privacy and security.

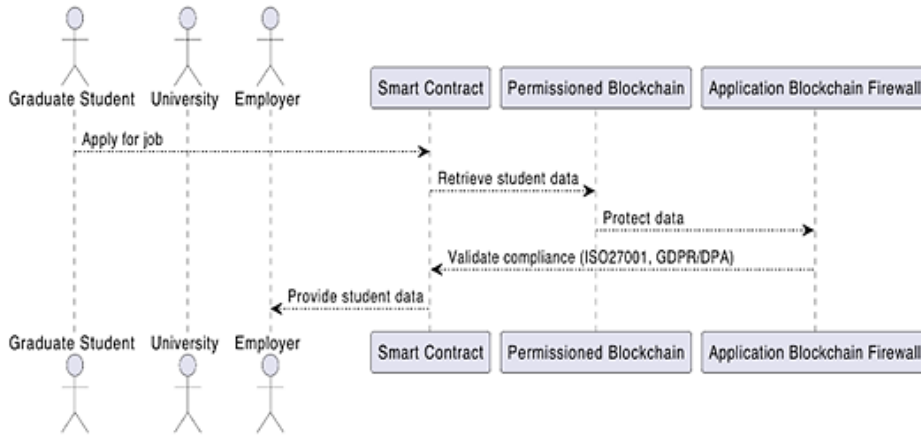
The figures (1-4) illustrate the flow of student processes chronologically throughout the phases of their academic life, for instance, when the student graduates from high school and applies to a program at university. After graduation, students decide to apply for a job at an employer, or they decide to continue studying at a higher education program. In all cases, a blockchain is utilized to store student data securely with integration with an application blockchain firewall to validate compliance with regulation frameworks, such as ISO27001 and GDPR/DPA. Student data is decentralized and available over the permissioned blockchain that communicates directly with universities amongst each other, and for employment, facilitating the transfer of student data reliably and securely.



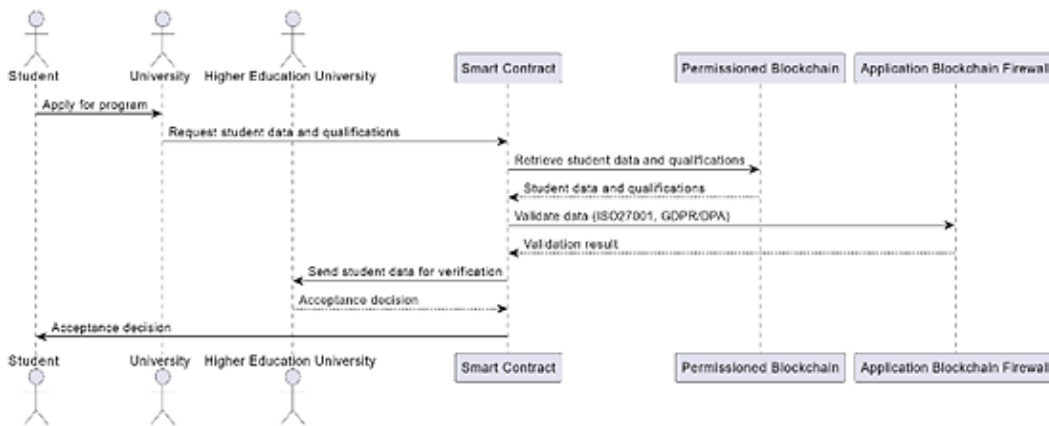
**Figure 1.** Sequence diagram of a high-school student's application to a university.



**Figure 2.** Sequence diagram of student registration for a university program.



**Figure 3.** Sequence diagram of a graduate student's application for employment.



**Figure 1.** Sequence diagram of a graduate student's application for higher education.

Figures (1-4) showcase how the flow of activities happens when we implement blockchain technology in adherence with school processes and employment. The actors are students, university, teachers, and employers; they undergo a validation and verification procedure when a smart contract requests data retrieved from the blockchain. And the blockchain is protected by a specific firewall-based blockchain to ensure traffic in transit is not tampered with or modified. Moreover, the data are cross-checked with regulatory frameworks for enhanced data privacy and integrity.

### 3.3. Construction

Simulating a blockchain in education involves creating a simplified version to demonstrate how a decentralized ledger could be used for tasks like storing student records securely. In this example, we will provide a simple Python simulation of a blockchain for educational records using a basic block structure and hashing mechanism.

In addition to blockchain code simulation, we add another security layer and that is Blockchain Application firewall, it inspects traffic and instills rules and policies to direct the incoming and outgoing traffic between nodes where security is optimized and monitored, this

allows for best-practice cyber hygiene in controlling the way this permissioned blockchain transmit data and perform transactions.

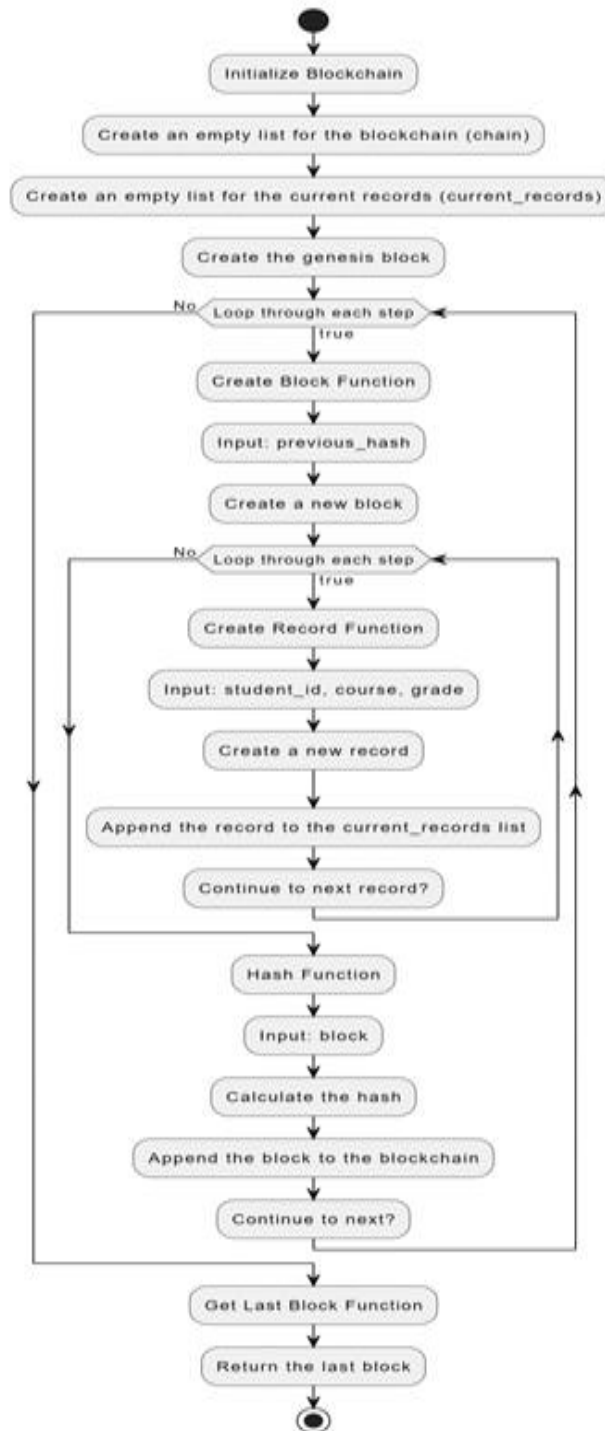
This smart contract allows users to transfer tokens between addresses, and the token balances are stored on the blockchain. This is a simple example, and real-world smart contracts can be significantly more complex depending on the use case. To simulate the interaction with this smart contract, we would typically deploy it on a blockchain testnet (like Ropsten for Ethereum) and use a development environment or a tool like Remix to send transactions to the contract.

### 3.3.1. Consensus Algorithm

The algorithm outlines the basic operations performed by each function in the provided Python code, offering a step-by-step explanation of how the blockchain is initialized, blocks are created, and records are added [13]. The algorithm is represented in a flow activity diagram, see figure 5. Here is the algorithm [3]:

- **Initialize Blockchain:**
  - Create an empty list for the blockchain (chain).
  - Create an empty list for the current records (current\_records).
  - Create the genesis block using - the create\_block function with a predefined previous hash.
- **Create Block Function:**
  - Input: previous\_hash (hash of the previous block).
  - Create a new block with the following attributes:
    - index: Incremented index based on the length of the blockchain.
    - timestamp: Current timestamp.
    - records: List of records from the current block.
    - previous\_hash: Hash of the previous block.
    - Reset the current\_records list.
    - Append the new block to the blockchain.
    - Return the created block.
- **Create Record Function:**
  - Input: student\_id, course, and grade.
  - Create a new record with the given attributes.
  - Append the record to the current\_records list.
  - Return the created record.
- **Hash Function:**
  - Input: block (a block from the blockchain).
  - Convert the block to a JSON string and encode it.
  - Calculate the SHA-256 hash of the encoded string.
  - Return the hash.
- **Get Last Block Function:**
  - Return the last block in the blockchain.

The Blockchain class represents the entire blockchain. And each block contains an index, timestamp, a list of educational records, and the hash of the previous block. The create\_record method adds an educational record to the list of current records. The create\_block method creates a new block with the current records and adds it to the chain. The hash method generates the SHA-256 hash of a given block [20].



**Figure 5.** Activity diagram of blockchain algorithm.

This is a basic illustration, and a real-world implementation for educational records; it would require additional features, security considerations, and likely the use of a specialized

blockchain platform. This simulation serves as a conceptual starting point for understanding the principles of blockchain in an educational context.

Simulating a smart contract in a blockchain involves creating a simplified version to demonstrate how the contract can be deployed and interacted with. Below is a basic example of a smart contract written in Solidity, the programming language for Ethereum smart contracts? This example represents a simple token contract component [14].

- **SimpleToken** is a basic smart contract representing a token system.
- The **balanceOf** mapping stores the token balances for each address.
- The **Transfer** event is emitted whenever tokens are transferred.
- The **Constructor** initializes the token supply with the address of the deploying contract.
- The **Transfer** function allows users to transfer tokens to other addresses.

### 3.4. Results

In a blockchain simulation for education, the results would typically be a series of blocks containing educational records. The simulation could be visualized or analyzed to demonstrate how a decentralized ledger could store and secure student records. Below is a hypothetical finding of what the results might look like after simulation:

The first block is the genesis block, containing no educational records and a previous hash of "1". The second block contains a record for student 123 who took the Math course and received a grade of A. The hash of the previous block is used to link the blocks. The third block contains a record for student 456 who took the History course and received a grade of B. The hash of the second block is used as the previous hash.

In a real-world scenario, each block would be cryptographically linked to the previous one, ensuring the integrity and immutability of the educational records. The simulation provides a visual representation of how a blockchain could be used to securely store and link educational data over time.

The findings found in these simulations are that which relate to how blockchain operate and their classes with respect to functions and objects representing the education processes such as transferring grades and records in conjunction with tokenized operations that are a result of smart contract, as a result, we obtained a proposed solution to overcome current centralized systems such as security concerns that involve transparency and immutability, hence, we can validate the hypothesis that blockchain in education does improve security and performance.

PWC reports that 24% of executives are initiating investments in blockchain to enhance the education system [15]. In 2020, Europe held a significant market share of 27.3% in the blockchain education sector. Projections indicate that educational institutions will adopt blockchain technology at a compound annual growth rate (CAGR) of 16.0% by 2026. According to JRC science hub, the implementation of blockchain in the education sector has the potential to reduce operational costs by over 5%. Despite the promising outlook, a survey

by Gartner reveals that only 1% of Chief Information Officers (CIOs) have indicated any form of blockchain adoption within their educational organizations [15].

### 3.5. Discussion

Applying blockchain technology with smart contracts in education holds the promise of significantly improving both performance and security within academic systems. By leveraging the decentralized and tamper-resistant nature of blockchain, educational institutions can establish a robust framework for managing student records, course data, and administrative processes. The use of smart contracts automates various tasks, streamlining workflows and reducing the reliance on manual intervention. This not only enhances overall system performance by minimizing processing delays but also significantly reduces the risk of human errors in data entry and record-keeping. The transparency and immutability of blockchain contribute to enhanced security, ensuring the integrity of academic records and protecting sensitive information. Additionally, the decentralized nature of blockchain mitigates the risk of a single point of failure, providing a resilient and secure environment for academic data. While challenges such as integration complexity and regulatory compliance need careful consideration, the potential for better performance and heightened security in education through blockchain and smart contracts is a compelling prospect that merits further exploration and implementation.

### 3.6. Evaluation

When applying a smart contract in a blockchain for enhancing data security, the results can be demonstrated through various improvements in the handling and storage of sensitive information. Here is a conceptual representation of the results:

**Immutability:** Smart contracts on a blockchain provide data immutability. Once data is recorded, it cannot be altered or deleted. As a result, protection is enhanced against unauthorized tampering or modification of critical information [6].

**Decentralization:** Blockchain operates on a decentralized network of nodes, reducing the risk of a single point of failure or malicious attacks. And as a result, resilience is increased and security optimized due to the absence of a central authority that could be exploited [7].

**Transparency:** Smart contracts facilitate transparent and auditable transactions. All interactions are transparent with the contract and are recorded on the blockchain and can be publicly verified. Hence, accountability and traceability of data access and modifications are improved [8].

**Access Control:** Smart contracts can implement sophisticated access control mechanisms, ensuring that only authorized parties can interact with specific functions or data. Strengthening security by restricting access to sensitive data and operations [9].

**Automation:** Smart contracts automatically execute predefined rules without the need for intermediaries. The trustless execution reduces the reliance on third parties or vendors.

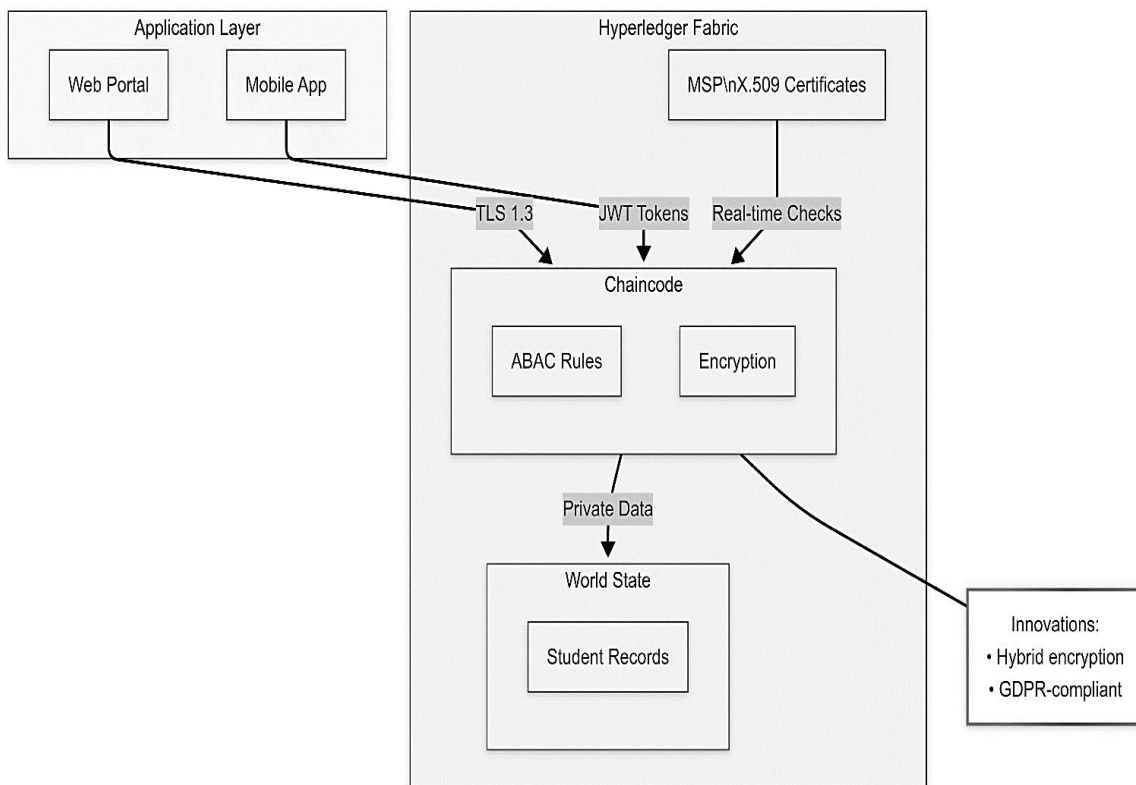
This allows to minimize trust issues and less probability of human error which increase efficiency in data [15].

**Cryptography:** Blockchain relies on cryptographic techniques to secure transactions and ensure data confidentiality and integrity. Therefore, data security is enhanced through robust cryptographic procedures, protecting sensitive information from unauthorized access [11].

It's important to emphasize that the effectiveness of data security measures in a blockchain depends on the specific implementation, configuration, and underlying blockchain platform. Additionally, ongoing monitoring, testing, and updates are essential to address emerging security challenges.

### 3.6.1. Data Privacy Architecture

Figure 6 presents a privacy-focused academic records system based on Hyperledger Fabric. It integrates a multi-layered security model comprising TLS 1.3, JWT authentication, and MSP-issued certificates for trust management. Smart contracts (chaincode) enforce attribute-based access control (ABAC) and encrypt data before storage in the private data collection of the blockchain's world state (see Table 1). The system achieves full GDPR compliance by embedding privacy-by-design principles, such as consent-driven access control and encryption-based data minimization (see Table 2). Its hybrid encryption and real-time verification capabilities make it a scalable and compliant solution for national-level education credentialing platforms.



**Figure 6.** Activity diagram of blockchain algorithm.

**Table 1.** Technical Description of Data Privacy Architecture.

Component	Entity	Function	Technical Description
Application Layer	Web Portal, Mobile App	User Access Interface	End-users (e.g., students, institutions) interact with the blockchain system through a web or mobile interface.
Secure Communication	TLS 1.3	Data-in-transit Encryption	Ensure secure and encrypted transmission between the application layer and the blockchain network.
Authentication Layer	JWT Tokens	Access Control	JSON Web Tokens authenticate and authorize users before accessing chaincode functions.
Identity Management	MSP/X.509 Certificates	User Identity Verification	Membership Service Providers issue digital certificates to ensure trusted identities in the network.
Access Control Logic	ABAC Rules	Fine-grained Authorization	Attribute-Based Access Control (ABAC) policies enforce who can access which student records and under what conditions.
Data Privacy Layer	Encryption	Data Confidentiality	Student data is protected using a hybrid encryption approach to ensure GDPR compliance.
Blockchain Logic	Chaincode	Smart Contract Execution	Business logic, including access validation and data processing, is executed in the chaincode.
Storage Layer	World State	Secure Data Storage	Verified student records are stored in the world state ledger as private data collections to restrict access.

**Table 2.** Feature Description of Data Privacy Architecture.

Feature	Description
Hybrid Encryption	Combines symmetric and asymmetric encryption to balance performance and security.
GDPR Compliance	Ensures user consent, data minimization, and right to erasure are supported in the system architecture.
Real-time Checks	Enables live verification and access auditing for high-trust environments.

## 3.6.2.

## Experimental Setup

## Recap

The experimental implementation of the blockchain-based academic credentialing system took place in a controlled virtual environment, running on Ubuntu 20.04 LTS. The setup was established with the help of Docker and Docker Compose, which were used to

containerize all parts belonging to Hyperledger Fabric so that orchestration would be enabled as well as modular deployment, together with secure isolation of services. There were several peer nodes in the network, an ordering service that made use of the Raft consensus protocol, certificate authorities (CAs) for issuing digital identities, and chaincode containers for carrying out smart contracts. The test net emulated a consortium of educational establishments and job providers. Every group was given its own Membership Service Provider (MSP) setup, enabling role-centered entry control and identity check. Transport Layer Security (TLS) was made mandatory to ensure secure communication between network parts, protecting the system from being compromised and tampered with during data transmission.

The academic system's core logic, comprising student creation, course registration, grade assignment, and certificate issuance, was smart contracts written in the Go programming language. The chain codes were managed using the Hyperledger Fabric chain code lifecycle process, which facilitated packaging, approval, instantiation, and version control of the chain code. Endorsement policies were used to ensure that a transaction met at least the minimum validation criteria before it was committed to the ledger.

A series of simulated academic transactions was initiated both from the side of Fabric CLI and an external client application, which thus emulated real-world users-university registrar, students, and employer verifiers- to rigorously test the system. The network was also evaluated during this simulation for its performance, security, and scalability. Some of the metrics used in analyzing how efficient operations were under different loads included transaction latency and throughput, as well as chaincode execution time.

Private Data Collections (PDCs) were configured as an approach to ensuring data privacy. Results and certificates-those are sensitive data shared only with the authorized intended parties, while their hash is kept on the public ledger for verification and audit trails. The cryptographic identities govern access to both functions and data, together with attribute-based access control policies enforced through MSP and Certificate Authority configurations.

In general, the experiment validated that Hyperledger Fabric could indeed host a secure, efficient, and privacy-preserving platform in operations with educational credentials. It maintained consistency and integrity while under simulated pressure, thereby validating its potential for actual deployment in real academic environments where transparency, decentralization, and tamper-proof record management have to be ensured.

### 3.6.3. Blockchain Performance Metrics

The performance of the prototype solution was measured in terms of those KPIs that are generally referred to while benchmarking any distributed ledger. More particularly, it has been analyzed in terms of transaction throughput, latency, and endorsement policy validation rate. Throughput denotes how many transactions have successfully completed per second (TPS). At a moderate load on a network and under realistic education workflows, TPS was attained. On average, latency is calculated as the time gap between submitting a transaction

and its confirmation. This comes out to be milliseconds per transaction, indicating responsiveness towards real-time academic operations.

The endorsement policy setup was tested, which required approvals from several organizational peers, to gauge its effect on performance and security. The said network has always performed transaction validation under the indicated endorsement policy, meaning that it has maintained efficiency with no compromise in integrity. The above metrics were collected and analyzed by making use of Hyperledger Caliper, a benchmarking framework and tool for measuring blockchain performance. A set of custom monitoring scripts was also added to the network for extracting fine-grained metrics that would give more comprehensive insights relating to transaction execution, chaincode performance, and block commit times.

This performance evaluation proves the practicality of initiating Hyperledger Fabric for secure, high-integrity recordkeeping of academic achievements with a proper balance between decentralization, privacy, and speed. It also tested positive for resilience and efficiency under simulation and can hence be scalable if applied in actual institutional setups.

Transaction throughput is measured in transactions per second (TPS) by simulating the parallel submission of transactions on several nodes across the network. The resultant throughput under different workloads reveals at what point maximum throughput can be attained when heavy loads are imposed on the system, thus providing insight into how large volumes of transactions can be handled by the network. Just as importantly, latency—reported in minutes—was determined from timestamps captured at proposal submission and at final validation; hence an indication of how responsive the system was.

The endorsement policy, which determines how many and which peers must validate a transaction, is tested under different settings, starting from single-peer validation up to multiple peers in a consensus. Measurements were taken of the rate of approvals as well as network delay. Only those transactions that garnered the required endorsements were considered valid, thus ensuring compliance with the defined governance structure.

Private Data Collections tested the confidentiality and integrity of data. Their effectiveness was proven by trying to gain unauthorized access to restricted data. Testing of encryption through Transport Layer Security and authentication through Membership Service Provider was also carried out via logs of access attempts. These successfully prevent unauthorized access, hence boosting the confidence level on data privacy protection by the blockchain itself.

#### 3.6.4. Data Privacy Outcomes

The Hyperledger Fabric network proved very effective in the implementation of privacy features to keep confidentiality, access control, and audit trails end-to-end. Private Data Collections (PDCs) were applied to separate and limit sensitive information— such as marks and details of certificates — so that only the concerned organizations, mainly the issuing university and selected verifiers, could access this content. The main ledger kept hashed pointers to these private records such that validation for consistency could be done without throwing open confidential information to every participant inside the network.

Besides PDCs, all data-in-flight communications among the network components were secured with Transport Layer Security (TLS), by which encryption ensured safeguarding the data from any type of interception or tampering while in transit. Access was accorded to every transaction that was properly authenticated by the Membership Service Provider (MSP) by validating who the participating nodes are and their corresponding roles. It comes out clearly that with TLS encryption plus MSP-based identity management, attacking access will be effectively stopped, and stringent role-based trust boundaries can be enforced inside a blockchain ecosystem.

The design ensured complete audibility. Every transaction-whether an enrollment, a grade, or the issuing of a certificate-was immutably recorded to the ledger. Records could not be altered or deleted to make transparent audibility support both accountability and compliance with academic data governance standards. These privacy outcomes, taken together, evidence that the system is capable of maintaining an equilibrium state between transparency and confidentiality, a requirement that is fundamental for blockchain to find its way into real-world educational environments.

#### 4. Conclusion

The integration of blockchain technology and smart contracts in education offers a transformative approach to securing and validating school-related items. By leveraging the immutability, transparency, and automation capabilities of these technologies, educational institutions can create a more secure, efficient, and trustworthy system for managing academic data. While challenges exist, the potential benefits make blockchain and smart contracts a promising avenue for enhancing security and validation in education. Ongoing research, collaboration, and technological advancements will play a crucial role in further refining and optimizing these solutions for widespread adoption in the education sector.

**Acknowledgments:** We would like to express our sincere gratitude to our advisors, professors, and colleagues whose invaluable guidance and support have greatly contributed to the completion of this research. We extend our thanks to Kuwait University for providing the resources necessary for this study.

**Conflicts of Interest:** The authors declare no conflict of interest.

#### References

- [1] Raimundo, R.; Rosário, A. Blockchain system in the higher education. *Educ. Sci.* **2021**, *11*, 21.
- [2] Dajti, D.; Laanpere, M.; Põldoja, H.; et al. EduCTX: A blockchain-based higher education credit platform. *IEEE Xplore*.
- [3] Solidity Academy. Revolutionizing education with smart contracts. *Medium*. Available online: <https://medium.com/@solidity101/revolutionizing-education-with-smart-contracts-742e570a414f> (accessed on 24 July 2025).

- [4] Alammary, A.; Alhazmi, S.; Almasri, M.; Gillani, S. Blockchain-based applications in education: A systematic review. *Appl. Sci.* **2019**, *9*, 2400.
- [5] Kholishotulaila, S.; Laila, K.; Angga, A.L. Benefits provided by blockchain technology in the field of education. *Blockchain Front. Technol.* **2022**, *1*, 74–83.
- [6] Llambias, G.; González, L.; Ruggia, R. Blockchain interoperability: A feature-based classification framework and challenges ahead. *CLEI Electron. J.* **2023**, *25*.
- [7] Fan, S.; Min, T.; Xiao, W.; Cai, W. Altruistic and profit-oriented: Making sense of roles in Web3 community from an airdrop perspective. *ACM Digital Library* **2023**.
- [8] Gulen, K.; Karaagac, A. Agricultural food supply chain with blockchain technology: A review on Turkey. *J. Glob. Strateg. Manag.* **2024**.
- [9] Almajed, H.; Almogren, A. Simple and effective secure group communications in dynamic wireless sensor networks. *Sensors* **2019**, *19*, 1909.
- [10] Barbaria, S.; Mont, M.; Ghadafi, E.; Mahjoubi, H.; Rahmouni, H. Leveraging patient information sharing using blockchain-based distributed networks. *IEEE Access* **2022**, *10*, 106334–106351.
- [11] Yang, Z.; Salman, T.; Jain, R.; Di Pietro, R. Decentralization using quantum blockchain: A theoretical analysis. *IEEE Trans. Quantum Eng.* **2022**, *3*, 1–16.
- [12] Peffers, K.; Tuunanen, T.; Rothenberger, M.; Chatterjee, S. A design science research methodology for information systems research. *J. Manag. Inf. Syst.* **2007**, *24*, 45–77.
- [13] Dutta, S.; Saini, K. Blockchain implementation using Python. In *Advances in Systems Analysis, Software Engineering, and High-Performance Computing*; IGI Global: Hershey, PA, USA, 2022; pp. 123–136.
- [14] Pierro, G.; Tonelli, R.; Marchesi, M. An organized repository of Ethereum smart contracts' source codes and metrics. *Future Internet* **2020**, *12*, 197.
- [15] ZipDo. Essential blockchain in education statistics in 2023. Available online: <https://zipdo.co/statistics/blockchain-in-education> (accessed on 24 July 2025).
- [16] Johar, S.; Ahmad, N.; Asher, W.; Cruickshank, H.; Durrani, A. Research and applied perspective to blockchain technology: A comprehensive survey. *Appl. Sci.* **2021**, *11*, 6252.
- [17] Grund, S.; Nomm, N.; Walch, F. Liquidity in resolution: Comparing frameworks for liquidity provision across jurisdictions. *SSRN Electron. J.*
- [18] Nakamoto, N. Centralised bitcoin: A secure and high-performance electronic cash system. *SSRN Electron. J.* **2017**.
- [19] Kurniawan, R.; Oktaviani, D. Characteristics of blockchain technology in educational development. *Blockchain Front. Technol.* **2022**, *1*, 23–28.
- [20] Tang, Q. Towards using blockchain technology to prevent diploma fraud. *Unpublished work*. Stage of publication unknown.