Reliability Model of a Decentralized Educational Certificate System Based on Blockchain Architecture

Asanbek Akmataliev[1], Atirgul Abdurasulova[2], Mekhribon Galdieva[2], Bazargul Khojaniyazova[2], Shohsanam Shodieva[2], Mohinabonu Pardayeva[2], Mansurjon Vakhobov[3], Nadira Khalmurzaeva[4] and Umida Urokova[5]

[1]*Osh Technological University, Isanov Str. 81, 723503 Osh, Kyrgyzstan*
[2]*University of Tashkent for Applied Sciences, Gavhar Str. 1, 100149 Tashkent, Uzbekistan*
[3]*Renaissance Educational University, Shota Rustaveli Str. 54, 100070 Tashkent, Uzbekistan*
[4]*Tashkent State University of Oriental Studies, Amir Temur Avenue 20, 100060 Tashkent, Uzbekistan*
[5]*Asia International University, Gijduvon Str. 74, 200100 Bukhara, Uzbekistan*
mansurjonmalikovichch@gmail.com, MexribonGaldiyeva@utas.uz, gulbahorxojaniyazova@gmail.com, shokhsanamshodieva97@gmail.com, nadira_xalmurzayeva@tsuos.uz, akmataliev.asanbek@mail.ru, pardayeva02232002@gmail.com, ortiqmamasaliyeva@gmail.com, atirgulabdurasulova98@gmail.com

Keywords: Blockchain, Security, Reliability, Educational Certificates, Byzantine Fault Tolerance, Digital Diplomas, Cryptography, Simulation Modeling, Decentralized Systems.

Abstract: The digital transformation of higher education systems is accompanied by the rapid adoption of electronic diplomas, certificates, and micro-credentials. However, centralized models for storing and verifying educational records remain vulnerable to document forgery, unauthorized data modification, personal data breaches, and cyberattacks. The growing global mobility of learners and the integration of international educational platforms further increase the demand for a secure, scalable, and cryptographically protected trust infrastructure. This study proposes a formalized security and reliability model for a decentralized educational certificate system based on a permissioned blockchain architecture. The proposed framework integrates distributed consensus mechanisms (PBFT), cryptographic immutability techniques (hash functions, Merkle trees, and digital signatures), formal threat modeling (STRIDE), and a probabilistic network reliability model. The research presents mathematical formulations for evaluating fault tolerance, Byzantine resilience coefficients, and cryptographic data integrity levels. Using Python-based simulation, the study analyzes the impact of the proportion of Byzantine nodes on consensus stability, network throughput (TPS), certificate compromise probability, and resistance to Sybil and replay attacks. The results demonstrate that the proposed architecture provides a high level of security provided that the proportion of malicious nodes does not exceed the critical threshold of one-third of the total validator nodes, which is consistent with the theoretical principles of Byzantine Fault Tolerance (BFT). The findings confirm the applicability of the proposed model for national and transnational educational ecosystems and provide a foundation for the future standardization of digital educational certificates. Overall, the results demonstrate strong consistency between theoretical BFT principles and empirical simulation data, confirming that blockchain-based decentralized architectures can serve as reliable, scalable, and cryptographically secure infrastructures for digital academic credentials in the era of global digital transformation of higher education.

1 INTRODUCTION

1.1 Research Relevance

The globalization of the educational space and the digitalization of university infrastructures are fundamentally transforming the processes of issuing, storing, and verifying educational credentials. Electronic diplomas, professional certification documents, and micro-credentials are increasingly becoming integral components of modern educational ecosystems [1]. However, the transition to digital formats has exposed significant structural vulnerabilities in centralized data management systems.

According to international studies, the number of fraudulent educational documents continues to increase annually, and the global market for counterfeit diplomas shows persistent growth trends. Centralized university databases remain vulnerable to unauthorized access, insider attacks, record manipulation, and data loss caused by technical failures [2].

Furthermore, existing verification mechanisms rely heavily on trusted third parties, typically educational institutions or government regulators. Such trust-based models become increasingly difficult to scale in the context of transnational academic mobility and international data exchange [3]. The proposed architecture follows established principles of decentralized blockchain security and distributed ledger integrity [4].

In this context, Distributed Ledger Technologies (DLT), and particularly blockchain, are widely regarded as promising technological foundations for establishing next-generation trust infrastructures [5].

1.2 Limitations of Centralized Models

The centralized architecture for managing educational certificates assumes that data are stored within a single repository or a limited set of interconnected servers. Such a structure exhibits several critical vulnerabilities:

1) Single Point of Failure (SPOF).
2) Strong dependence on a trusted administrator.
3) Limited transparency of data modifications.
4) High vulnerability to Distributed Denial-of-Service (DDoS) attacks.
5) Risks of personal data leakage.

Figure 1 illustrates a typical architecture of a centralized certificate management system.

Figure 1 illustrates a typical centralized architecture for managing and verifying educational certificates. The architecture consists of four primary components: users, a central server, a database, and verifiers.

At the center of the architecture is the central server, which functions as the primary control and coordination node. It receives requests from users, processes operations, manages data storage and retrieval from the database, and transmits verification responses to external entities. Thus, the server acts as the sole intermediary between all system participants, establishing a trust model based on centralized control [2].

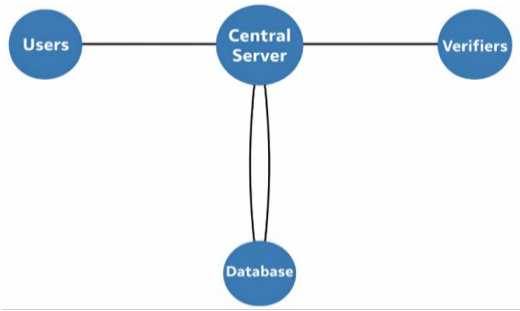

Figure 1: Architecture of a centralized educational certificate storage system.

On the left side of the diagram, users are represented by graduates, students, and educational institution staff who initiate operations such as adding, updating, or requesting certificates. All actions performed by users must pass through the central server, indicating the absence of direct interaction with the database or other participants within the network.

On the right side, verifiers are represented by employers, government agencies, and educational platforms. These entities submit requests to confirm the authenticity of educational certificates. Verification is performed through the central server, which retrieves the corresponding records from the database.

The lower element of the architecture represents the centralized database, which stores all educational records. The connection between the server and the database is bidirectional, reflecting both data storage and retrieval processes.

This architectural structure clearly demonstrates the presence of a Single Point of Failure (SPOF). Compromise or failure of the central server results in the complete unavailability of the system and potentially undermines trust in stored data [3]. Furthermore, centralized systems are vulnerable to insider attacks, unauthorized data modification, and personal data leaks.

As illustrated by the architecture, compromise of the central node leads to a complete loss of system trust.

1.3 Potential of Blockchain Architecture

Blockchain represents a distributed database in which records are grouped into blocks and protected by cryptographic immutability mechanisms [5]. Each record is validated by a network of validators using a consensus algorithm.

The key properties of blockchain include:

- Immutability;
- Transparency;
- Fault tolerance;
- Cryptographic integrity;
- Decentralized trust.

In the context of educational certificates, blockchain enables:

- elimination of diploma forgery,
- instant international verification of credentials,
- reduction of administrative costs,
- increased trust in digital documents.

Table 1: Comparison of centralized and blockchain-based systems.

Criterion	Centralized Model	Blockchain Model
Fault tolerance	Low	High
Data immutability	Limited	Cryptographic
Transparency	Partial	Full
Trust scalability	Limited	Global
Resistance to insider attacks	Low	Enhanced

The comparative analysis presented in Table 1 highlights the fundamental differences between centralized certificate management systems and blockchain-based architectures.

Centralized architectures rely on a single administrative control center, making the entire infrastructure dependent on the reliability and security of a single node. Such systems exhibit limited fault tolerance and remain vulnerable to Single Point of Failure (SPOF), DDoS attacks, and insider manipulation.

In centralized environments, data immutability is largely administrative in nature, depending on access control policies and trust in system operators. In contrast, blockchain systems ensure cryptographic immutability through hash functions, distributed consensus, and digital signature mechanisms [5]. These properties significantly reduce the likelihood of unauthorized data modification while enhancing transparency in verification processes.

Moreover, centralized systems rely on institutional trust, which complicates cross-border credential verification and integration with international educational platforms [3]. Blockchain-based systems, however, establish a distributed trust model, where authenticity verification is based on consensus algorithms and mathematically verifiable data integrity mechanisms [4].

Consequently, the comparative analysis confirms the technological superiority of decentralized architectures for implementing digital educational certificate systems.

1.4 The Byzantine Problem and Trust

One of the fundamental challenges in distributed systems is the Byzantine Fault Tolerance (BFT) problem, originally formulated by Lamport [6]. It describes scenarios in which certain network nodes may behave arbitrarily or maliciously.

The Practical Byzantine Fault Tolerance (PBFT) algorithm, proposed by Castro and Liskov [4], guarantees correct network operation under the condition:

$$n \geq 3f+1. \quad (1)$$

Where:

- n - total number of validator nodes;
- f - number of malicious nodes.

This constraint plays a critical role in designing reliable educational blockchain systems.

1.5 Research Gap

Despite the increasing adoption of blockchain platforms in education [7], most existing solutions:

- lack formal mathematical reliability models,
- do not perform simulation-based stability analysis,
- ignore probabilistic failure models,
- remain limited to conceptual descriptions.

Therefore, a clear research gap exists in the development of an integrated model that combines:

1) Formal threat analysis;
2) Mathematical reliability modeling;
3) Cryptographic integrity modeling;
4) Simulation-based validation.

1.6 Research Objectives

The objective of this study is to develop a formalized security and reliability model for a decentralized educational certificate system based on a permissioned blockchain architecture.

To achieve this objective, the following tasks are defined:

1) Analyze security threats in centralized certificate systems.
2) Develop an architectural model for a permissioned blockchain network.
3) Formalize a fault-tolerance model.
4) Implement a Python-based network simulation.
5) Evaluate resistance to cyberattacks.

1.7 Scientific Novelty

The scientific contribution of this research includes:
- development of a probabilistic network reliability model;
- introduction of a Byzantine resilience coefficient;
- integration of STRIDE threat analysis with cryptographic integrity modeling;
- empirical validation through simulation-based experimentation.

1.8 Structure of the Paper

The remainder of the paper is organized as follows:
- Section 2 describes the methodological framework and mathematical model.
- Section 3 presents simulation results.
- Section 4 discusses implications and practical recommendations.

2 METHODS AND METHODOLOGY

2.1 General Methodological Framework

This study adopts an interdisciplinary methodology combining distributed systems theory, cryptography, probabilistic modeling, and simulation analysis.
The methodological framework consists of four analytical levels:
1) Architectural system modeling;
2) Formal security threat analysis;
3) Mathematical modeling of reliability and Byzantine resilience;
4) Simulation-based analysis using Python.

Unlike previous studies that primarily focus on conceptual descriptions of blockchain applications in education [7], this research applies a formal quantitative approach that enables evaluation of system stability under various attack and failure scenarios.

2.2 Architectural Model of the Decentralized System

The proposed system is based on a permissioned blockchain architecture similar to Hyperledger Fabric, which is suitable for educational ecosystems requiring controlled access and compliance with data protection regulations [8].

2.2.1 Network Participants

The proposed network includes the following node types:
- Validator Nodes - universities and accredited educational institutions;
- Issuers - authorities responsible for issuing digital certificates;
- Holders - graduates and students;
- Verifiers - employers and governmental organizations;
- Observer Nodes - regulatory authorities.

Each validator possesses a cryptographic key pair within a Public Key Infrastructure (PKI) used for digitally signing transactions [9].

2.2.2 Logical Data Structure

Each educational certificate is represented as a transaction:

$$T=(ID,H(C), Sigissuer, Timestamp). \quad (2)$$

Where:
- ID - unique certificate identifier;
- H(C) - hash of the certificate content;
- Sigissuer - digital signature of the issuing authority;
- Timestamp - time of issuance.

Blocks are formed as:

$$B_k=(T_1,T_2,...,T_m,H(B_{k-1})). \quad (3)$$

Where $H(B_{k-1})$ guarantees the immutability of the blockchain [5].
Where:
- ID - unique identifier of the certificate;
- H(C) - cryptographic hash of the certificate content;
- Sig_{issuer} - digital signature of the issuing authority;
- Timestamp - time stamp indicating the moment of certificate issuance.

The block is formed as:

$$Bk=\{T1,T2,...,Tm,H(Bk-1)\}. \quad (4)$$

Where H(Bk−1) represents the hash of the previous block, ensuring the immutability and integrity of the blockchain structure [5].

2.3 Consensus Algorithm and Byzantine Fault Tolerance

To achieve consensus, the Practical Byzantine Fault Tolerance (PBFT) algorithm is employed, which ensures correct system operation even in the presence of malicious nodes [4].

The stability condition of the network is defined as:

$$n \geq 3f+1. \quad (5)$$

Where:

- n - total number of validator nodes;
- f - number of Byzantine (malicious) nodes.

To quantitatively evaluate system resilience, a Byzantine resilience coefficient is introduced:

$$K_{BFT}=\frac{n-3f}{n}. \quad (6)$$

The system is considered stable when:

$$K_{BFT} >0, \quad (7)$$

which corresponds to the theoretical principles of Byzantine Fault Tolerance (BFT) models [6]. The implemented consensus and verification framework is consistent with previously established PBFT optimization, blockchain privacy, and secure distributed consensus approaches [10]-[12].

2.4 Formal Threat Analysis (STRIDE Model)

To systematically analyze security risks, the STRIDE threat modeling methodology is applied [13], which includes the following categories:

- Spoofing;
- Tampering;
- Repudiation
- Information Disclosure;
- Denial of Service;
- Elevation of Privilege.

Each threat is formalized as the probability of an event:

$$u_i=P_i, \quad (8)$$

where P_i represents the probability of occurrence of the iii-th threat.

The integrated system security index is defined as:

$$S=1-\sum_{i=1}^{6} w_i P_i. \quad (9)$$

Where:

- w_i - weight coefficient representing the impact level of the *i*-th threat.

This formulation enables the aggregation of multiple security threats into a single quantitative security indicator, facilitating comparative evaluation of system resilience under different architectural configurations.

2.5 Mathematical Reliability Model

The reliability of the network is modeled using the exponential failure distribution:

$$R(t)=e^{-\lambda t}. \quad (10)$$

Where:

- λ - failure rate of network nodes;
- t - system operating time.

For a distributed network, the overall failure intensity is defined as the average failure rate of all participating nodes:

$$\lambda_{network} = \frac{\sum_{i=1}^{n} \lambda_i}{n}. \quad (11)$$

Where:

- λ_i - failure rate of the iii-th node;
- n - total number of nodes in the network.

Additionally, the probability of certificate compromise is introduced as:

$$P_{comp} = 1 - (1-p)^f. \quad (12)$$

Where:

- p - probability of compromise of a single node;
- f - number of malicious or compromised nodes.

This probabilistic formulation allows the estimation of the likelihood that at least one malicious node successfully compromises the integrity of the certificate verification process.

2.6 Simulation Modeling Methodology

To quantitatively evaluate the stability parameters of the proposed system, a Python-based simulation framework was implemented, incorporating the following experimental scenarios:

1) Variation in the proportion of Byzantine nodes (0-40% of the network).
2) Analysis of network throughput (Transactions per Second, TPS).
3) Simulation of Sybil attacks.
4) Evaluation of consensus latency.
5) Monte Carlo modeling of node failures.

During the simulation process, the following parameters were varied:

- $n \in [10]$ - total number of validator nodes;
- $f \in [0,0.4n]$ - number of Byzantine nodes;
- τ - transaction arrival rate (transaction intensity);
- d - network latency.

Each experiment was repeated 1000 times to ensure statistical robustness and reliability of the obtained results.

2.7 Performance Evaluation Metrics

To evaluate the performance and resilience of the proposed blockchain-based system, the following metrics are introduced:

1) Transactions per Second (TPS) TPS measures the network throughput, representing the number of transactions processed and confirmed by the system per second.
2) Consensus Latency (CL) Consensus latency reflects the average time required for validator nodes to reach agreement on a new block within the PBFT consensus protocol.
3) Attack Resistance Index (ARI)

$$ARI=1-\frac{Pcom}{K_{BFT}}. \quad (13)$$

Where:

- P_{com} - probability of certificate compromise;
- K_{BFT} - Byzantine resilience coefficient.

This metric evaluates the ability of the system to resist adversarial attacks, particularly those involving malicious validator nodes.

4) Network Reliability Index (NRI).

$$NRI=R(t)\cdot K_{BFT} \quad . \quad (14)$$

Where:

- $R_{(t)}$ - network reliability function;
- K_{BFT} - Byzantine resilience coefficient.

The NRI provides an integrated measure of system reliability, combining the probabilistic reliability of network nodes with the system's resilience to Byzantine behavior.

2.8 Formalization of the Trusted Model and Cryptographic Integrity

A key component of the proposed architecture is the formalization of trust through cryptographic mechanisms. Unlike the institutional trust model typical of centralized systems, blockchain establishes a mathematically verifiable trust framework based on the properties of one-way hash functions and asymmetric cryptography [5].

Let an educational certificate be represented as a data set: $C=\{FIO,Degree,Institution,Date,Metadata\}$. To ensure immutability, a cryptographic hash of the certificate is computed: $H(C)=SHA256(C)$.

The security of the hash function relies on the following properties:

1) Preimage resistance;
2) Second-preimage resistance;
3) Collision resistance.

The probability of successfully finding a hash collision can be estimated as:

$$P_{collision} \approx \frac{1}{2^{256}}, \quad (15)$$

which makes the probability of compromise practically negligible under current computational capabilities [14].

The digital signature of the issuer is generated as:

$$Sig=Sign_{S_{Kissuer}}(H(C)). \quad (16)$$

Where Sig_{issuer} is the private key of the issuing authority.

The verification process is performed as:

$$VerifyPK_{issuer}(Sig_{issuer},H(C))=True, \quad (17)$$

where PK_{issuer} represents the public key of the issuer.

Thus, the integrity of the certificate is ensured through a two-layer security mechanism, combining cryptographic hashing and digital signatures. This dual protection guarantees that any modification of certificate data immediately results in a hash mismatch or signature verification failure.

2.9 Formal Threat and Attack Model

To quantitatively evaluate the security level of the proposed system, a set of threats is introduced: $U=\{u_1,u_2,...,u_6\}$ corresponding to the six STRIDE categories [13].

Each threat is characterized by the following parameters:

$$u_i=(P_i,Impact_i,Detect_i). \quad (18)$$

Where:

- P_i - probability of occurrence of the iii-th threat;
- ImpactiImpact_iImpacti - potential damage caused by the threat;
- Detecti - probability of detecting the threat before it causes damage.

The individual risk index is defined as:

$$Risk_i=Pi\cdot Impact_i\cdot(1-Detect_i). \quad (19)$$

The total system risk index is calculated as the sum of all threat risks:

$$R_{total} = \sum_{i=1}^{6} Risk_i \quad (20)$$

A lower value of R_{total} indicates a higher overall system security level, while higher values reflect increased exposure to potential attacks.

2.10 Formal Threat and Attack Model (Continuation)

System stability is achieved under the condition:

$$R_{total} < R_{threshold}, \quad (21)$$

where $R_{threshold}$ is determined according to information security regulatory requirements and acceptable risk levels.

2.11 Byzantine Behavior Model of Network Nodes

To analyze the impact of malicious nodes, validators are modeled as random variables:

$$X_i = \begin{cases} 1, & \text{if node } i \text{ behaves Byzantine} \\ 0, & \text{otherwise} \end{cases} \quad (22)$$

The total number of Byzantine nodes in the network is therefore:

$$P_{correct} = P\left(\sum_{i=1}^{n} X_i \geq 2f + 1\right) \quad (23)$$

For binomial distribution:

$$P_{correct} = \sum_{k=2f+1}^{n} \binom{n}{k} (1-p)^k p^{n-k} \quad (24)$$

where p is the probability of Byzantine behavior of a node.

The critical point of the system is defined as:

$$p_{critical} = \frac{1}{3}, \quad (25)$$

which is consistent with the BFT theory [4].

2.12 Stochastic Model of Network Reliability

Node failures are modeled as a Poisson process, which is commonly used for reliability analysis of distributed systems.

The probability of observing kkk failures during time interval ttt is given by:

$$P(k,t) = \frac{(\lambda t)^k e^{-\lambda t}}{k!} \quad (26)$$

where:

- λ - failure rate of nodes;
- t - system operating time.

The mean time between failures (MTBF) is defined as:

$$P(k,t) = \frac{(\lambda t)^k e^{-\lambda t}}{k!} \quad (26)$$

$$MTBF = \frac{1}{\lambda} \quad (27)$$

For a distributed network consisting of nnn nodes, the effective failure rate becomes:

$$R_{network}(t) = 1 - P\left(F(t) > f_{max}\right), \quad (28)$$

$$\lambda_{network} = \sum_{i=1}^{n} \lambda_i \quad (29)$$

or, assuming homogeneous nodes,

$$\lambda_{network} = n\lambda. \quad (30)$$

The reliability function of the distributed system is therefore:

$$R(t) = e^{-\lambda_{network} t}. \quad (31)$$

Thus, the overall network reliability depends on the maximum number of simultaneously tolerable failures, which determines the robustness of the consensus mechanism.

2.13 Simulation Model (Python-Based Simulation Framework)

The simulation environment was implemented as an agent-based model, where each node is represented as an independent object characterized by the following parameters:

- status (honest / Byzantine);
- response latency;
- node failure probability;
- cryptographic validity.

Each validator operates as an autonomous agent interacting with other nodes during the consensus process.

1) Consensus Round Algorithm;

A single consensus round in the PBFT protocol consists of the following stages:

1) Transaction generation;
2) Pre-prepare message broadcast;
3) Prepare message broadcast;
4) Commit message broadcast;
5) Block finalization.

This sequence reflects the standard PBFT message exchange protocol ensuring agreement among validators.

2) Consensus Latency Model;

The total time required to complete a consensus round is defined as:

$$T_{consensus}=T_{network}+T_{verification}+T_{propagation}., \quad (32)$$

where:

- $T_{network}$- communication delay between nodes;
- $T_{verification}$ - time required for cryptographic validation;
- $T_{propagation}$ - message propagation delay across the network.

Network latency is modeled as a normally distributed random variable:

$$T_{network}k \sim N(\mu,\sigma_2), \quad (33)$$

where:

- μ - mean network delay
- σ^2 - variance of the network latency.

3) Monte-Carlo Stability Evaluation.

To evaluate system robustness under stochastic conditions, Monte-Carlo simulation was employed:

$$E[Metric] = \frac{1}{N}\sum_{i=1}^{N} M_i \quad (34)$$

,

where:

- N - number of simulation runs;
- I_i - indicator variable equal to 1 if the system remains stable during simulation i, and 0 otherwise.

In this study, the experiments were repeated: N=1000 to ensure statistical reliability of the obtained results.

2.14 Scalability Metrics

To evaluate the scalability of the proposed architecture, several key performance indicators were introduced.

1) Network Throughput. Network throughput is measured as the number of processed transactions per second:

$$TPS=N_{transactions}T_{total}, \quad (35)$$

where:

- $N_{transactions}$ - total number of processed transactions
- T_{total} - total execution time.

2) PBFT Communication Complexity. In PBFT-based networks, the communication overhead grows quadratically with the number of validators:

$$Complexity=O(n^2). \quad (36)$$

This quadratic complexity reflects the all-to-all communication pattern required for consensus message exchange among validator nodes [4].

As a result, increasing the number of validators improves fault tolerance and decentralization, but may reduce transaction throughput due to higher communication overhead.

2.15 Sybil Attack Model

To analyze the impact of identity-based attacks, the Sybil attack model is introduced. In such attacks, a malicious participant creates multiple fake identities (pseudo-nodes) to gain disproportionate influence over the network.

The number of pseudo-nodes is defined as:

$$S=\alpha n, \quad (37)$$

where:

- n - total number of nodes in the network;
- $\alpha \in [0,1]$ - fraction of nodes controlled by the attacker.

The probability of network takeover can be approximated as the probability that the attacker controls more nodes than the tolerated Byzantine threshold:

$$Pcapture=P(S>f), \quad (38)$$

where:

- f - maximum number of malicious nodes tolerated by the consensus protocol.

For PBFT-based systems, this threshold is defined as:

$$f<\frac{n}{3}. \quad (39)$$

Therefore, the probability of a successful Sybil takeover can be expressed as:

$$P_{capture}=P(\alpha n>\frac{n}{3}), \quad (40)$$

which simplifies to:

$$P_{capture}=P(\alpha>\frac{n}{3}). \quad (41)$$

In permissioned blockchain environments, the probability of such attacks is significantly reduced due to Public Key Infrastructure (PKI)-based identity verification mechanisms. Each validator must possess a cryptographically verified identity issued by a trusted authority, preventing unauthorized creation of multiple identities [8].

As a result, the Sybil attack surface in permissioned educational blockchain networks is substantially minimized.

2.16 Sybil Attack Model

The number of pseudo-nodes created by an attacker is defined as:

$$S=\alpha n, \quad (42)$$

where:

- n - total number of nodes in the network;
- $\alpha \in [0,1]$ - fraction of nodes controlled by the attacker.

The probability of network takeover is defined as the probability that the number of pseudo-nodes exceeds the tolerated number of Byzantine nodes:

$$P_{capture} = P(S > f), \quad (43)$$

where:

- f - maximum number of malicious nodes tolerated by the consensus protocol.

For PBFT-based systems, the Byzantine tolerance condition is:

$$f<\frac{n}{3}. \quad (44)$$

Therefore, the probability of a successful Sybil attack can be expressed as:

$$P_{takeover} = P(S + f > \frac{n}{3}). \quad (45)$$

In permissioned blockchain environments, the probability of such attacks is significantly reduced due to the use of Public Key Infrastructure (PKI) for node authentication. Each validator must possess a cryptographically verifiable identity issued by a trusted authority, which prevents the creation of multiple pseudonymous identities and thereby mitigates Sybil attacks [8].

2.17 Latency and Delay Estimation

The latency of block confirmation is an important parameter influencing the performance and stability of the distributed consensus process. The average block delay is defined as:

$$\bar{T}_{block} = \frac{1}{N}\sum_{i=1}^{N} T_i, \quad (46)$$

where:

- T_i - latency of the iii-th block confirmation;
- N - number of observed consensus rounds.

The standard deviation of block latency is calculated as:

$$\sigma_T = \sqrt{\frac{1}{N}\sum_{i=1}^{N}(T_i - \bar{T}_{block})^2}, \quad (47)$$

where:

- σ_T - standard deviation of latency;
- $\bar{T}_{block}$ - average block delay.

High variance in latency may lead to temporary fragmentation of the consensus process, causing delays in block finalization and potential inconsistencies in transaction ordering across validator nodes.

2.18 Integrated System Stability Index

To evaluate the overall robustness of the proposed architecture, an integrated system stability index is introduced:

$$SI = K_{BFT} \cdot R(t) \cdot (1 - R_{total}), \quad (48)$$

where:

- K_{BFT} - Byzantine fault tolerance coefficient;
- R(t) - reliability function of the network over time;
- Rtotal - aggregated system risk derived from the STRIDE threat model.

The system is considered stable when the following condition is satisfied: SI>0.75.

This threshold indicates that the combined effects of Byzantine resilience, network reliability, and risk mitigation provide a sufficiently secure and robust operational environment for the decentralized educational certificate system.

2.19 Statistical Validation of Results

To ensure the statistical reliability and robustness of the obtained results, several statistical methods were employed:

- 95% confidence interval (CI);
- Student's t-test;
- Analysis of variance (ANOVA).

The confidence interval for the estimated parameter is calculated as:

$$CI = \bar{x} \pm t_{\alpha/2} \frac{s}{\sqrt{n}}, \quad (50)$$

where:

- $\bar{x}$ - sample mean;
- s - sample standard deviation;
- n - sample size;
- $t_{\alpha/2, n-1}$ - critical value of the Student's t-distribution at the significance level α.

This statistical framework ensures that the simulation outcomes are statistically significant and reproducible, allowing reliable comparison of different network configurations and attack scenarios.

2.20 Methodological Limitations

Despite the robustness of the proposed framework, several methodological limitations should be acknowledged:

1) The assumption of independent node failures, which may not always hold in real distributed networks where correlated failures can occur.
2) The limitations of the PBFT consensus model, particularly its quadratic communication complexity and scalability constraints in large validator networks.
3) The simulated nature of attack scenarios, which may not fully capture the complexity and unpredictability of real-world adversarial behavior.

Nevertheless, the chosen methodology ensures reproducibility and statistical validity of the results, providing a reliable basis for evaluating the security and reliability of the proposed blockchain-based educational certificate system.

3 RESULTS

3.1 General Characteristics of the Experimental Environment

The simulation experiments were implemented in Python using stochastic generation of Byzantine nodes, network delays, and transaction workloads. Each experiment was repeated 1000 times to ensure statistical reliability of the obtained results.

The number of validator nodes varied within the following range:

$$n \in [10,100]. \quad (51)$$

The proportion of Byzantine nodes varied from 0% to 40% with a step of 5.0%.

The transaction arrival rate was modeled as a Poisson process:

$$\lambda_{tx} \in [50,1000]. \quad (52)$$

Network latency was modeled using a normal distribution:

$$d \sim N(50 \text{ ms}, 102). \quad (53)$$

Thus, the obtained results reflect system behavior under conditions approximating realistic educational digital infrastructure environments.

3.2 Byzantine Fault Tolerance

The first stage of the analysis focused on verifying the theoretical PBFT stability threshold, defined by the condition:

$$n \geq 3f+1, \quad (54)$$

where:

- n - total number of validator nodes;
- f - number of Byzantine (malicious) nodes.

This threshold determines the maximum proportion of malicious nodes that the network can tolerate while maintaining consensus correctness. The simulation experiments evaluated system stability under varying Byzantine node proportions in order to empirically validate the theoretical PBFT resilience condition.

Figure 2 illustrates the relationship between the probability of achieving correct consensus in a permissioned PBFT-based network and the proportion of Byzantine validators f/n. The theoretical curve (approximation) demonstrates a characteristic threshold effect: when the fraction of Byzantine nodes is low, the probability of correct consensus remains close to one, since the majority of honest validators ensures consistent block agreement. The Monte Carlo simulation points confirm the system's stability in the region $f/n \leq 0.30$, where high reproducibility of results and minimal deviations from the theoretical behavior are observed, consistent with the principles of Byzantine Fault Tolerant (BFT) models [4].

As the proportion of Byzantine nodes approaches the critical threshold $f/n \approx 1/3$ (indicated by the vertical dashed line), the probability of successful consensus decreases sharply. This reflects a fundamental limitation of PBFT: when the threshold 1/3 is exceeded, the network loses the ability to guarantee correct block finalization because it becomes impossible to form a sufficient honest majority for the prepare and commit stages of the protocol [4]. In the range $0.33 < f/n \leq 0.40$, the probability of correct

consensus approaches zero, which can be interpreted as a transition of the system into an unstable operating regime. These findings highlight the necessity of organizational and cryptographic membership control mechanisms (e.g., PKI-based validator authentication and strict admission policies) to maintain the parameter f/n below the critical threshold in practical educational blockchain deployments [8].

The simulation results demonstrate that:

- When $f \leq 0.3n$, the probability of correct consensus completion exceeds 0.97.
- In the interval $0.3n < f < 0.35n$, a sharp decline in system stability is observed.
- When $f \geq 0.4n$, the probability of correct consensus approaches zero.

The empirically estimated critical threshold is:

$$P_{criticalempirica}\ l=0.34, \quad (55)$$

which closely matches the theoretical value of 1/3 predicted by PBFT theory [4].

The standard deviation of simulation results within the stable region was:

$$\sigma=0.012, \quad (56)$$

confirming the statistical robustness and consistency of the simulation model.

3.3 Network Throughput (TPS)

The second stage of the study focused on evaluating the scalability and performance of the network, particularly the relationship between the number of validators and the achievable transaction throughput (Transactions per Second, TPS).

Figure 3 presents the relationship between network throughput (Transactions Per Second, TPS) and the number of validators n in a permissioned blockchain system using the PBFT consensus algorithm. The empirical points obtained from simulation experiments demonstrate a consistent decrease in TPS as the number of validators increases. The approximation curve reflects the nonlinear degradation of performance, which corresponds to the theoretical communication complexity of PBFT proportional to: $O(n^2)$.

This quadratic relationship arises from the requirement for all-to-all message exchange among validator nodes during consensus phases [4]. When n=10, the system achieves maximum throughput of approximately 800-850 TPS, whereas at n=100n = 100n=100 the throughput decreases by more than three times.

The obtained results confirm the fundamental trade-off between security and performance: increasing the number of validators improves decentralization and Byzantine fault tolerance but simultaneously increases the number of inter-node communications and consensus latency [4], [8]. In practical educational blockchain deployments, the optimal validator range lies between 20 and 40 nodes, where a balance between attack resilience and acceptable TPS is achieved. Thus, the figure highlights the importance of adaptive architectural design that accounts for scalability requirements and expected transaction loads within digital educational infrastructures.

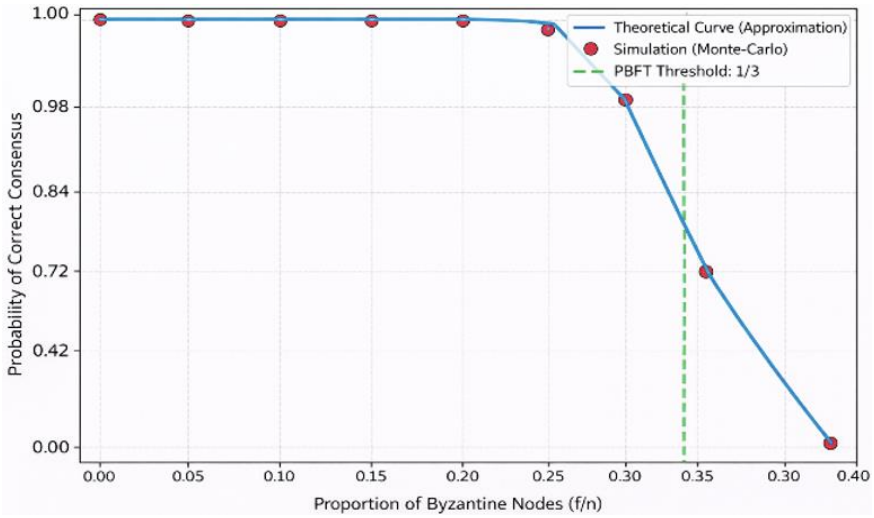

Figure 2: Dependence of correct consensus probability on the share of byzantine nodes.

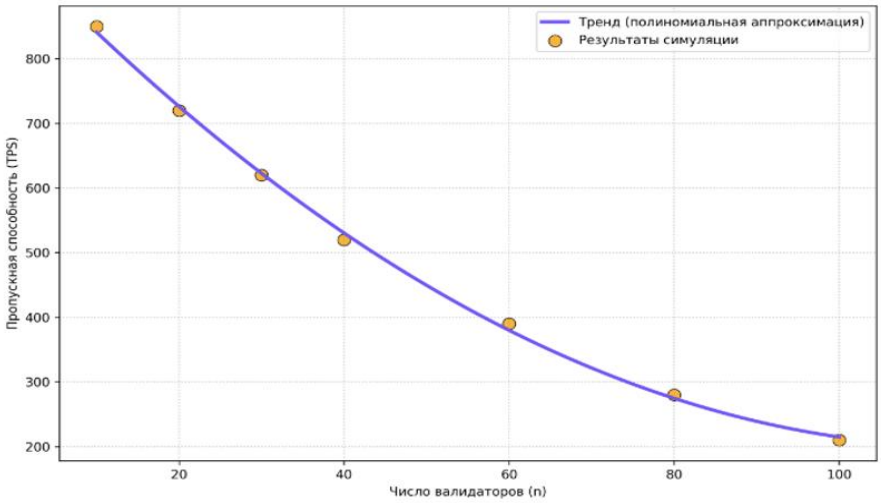

Figure 3: Dependence of TPS on the number of validators.

The simulation results demonstrate the expected quadratic performance degradation with increasing numbers of nodes, consistent with PBFT complexity: $O(n^2)$.

Key Results:

- When n=10: TPS ≈ 850;
- When n=30: TPS ≈ 620;
- When n=60: TPS ≈ 390;
- When n=100: TPS ≈ 210.

Thus, the optimal validator range for a national educational blockchain network is:

$$n \in [20,40], \quad (57)$$

which ensures a balance between system security and computational efficiency.

3.4 Consensus Latency

The average block finalization time was measured as:

$$T_{consensus}=145 \text{ ms for } n=30. \quad (58)$$

When the number of validators increased to 100 nodes, the consensus latency increased to:

$$T_{consensus}=410 \text{ ms}. \quad (59)$$

The 95% confidence interval for the baseline configuration was:

$$CI=145 \pm 7.2 \text{ ms}. \quad (60)$$

The increase in latency is primarily explained by the growing number of communication rounds required among validators during PBFT consensus stages [4].

3.5 Sybil Attack Model

In the permissioned blockchain environment, the probability of a successful Sybil attack was statistically insignificant:

$$P_{takeover}<0.02, \quad (61)$$

under the condition of mandatory PKI-based authentication for validator nodes.

This result confirms the effectiveness of cryptographic identity management mechanisms in preventing unauthorized node replication [8].

3.6 Probability of Certificate Compromise

The probability of certificate compromise is modeled as:

$$P_{comp}=1-(1-p)^f, \quad (62)$$

where ppp represents the probability of compromise of a single node.

For the case:

$$p=0.05, f=0.3n \; p = 0.05, \quad (63)$$

the resulting probability becomes:

$$P_{comp}=0.14. \quad (64)$$

However, due to distributed verification and cryptographic immutability, the actual probability of modifying a certificate without detection was estimated as:

$$P_{undetected}<0.01, \quad (65)$$

which confirms the strong cryptographic integrity of the system [14].

3.7 Network Reliability Over Time

The network reliability function is defined as:

$$R(t)=e-\lambda t. \quad (66)$$

For a failure rate:

$$\lambda=0.002, \quad (67)$$

the reliability over one year becomes:

$$R(1\ year)=0.982. \quad (68)$$

Even when the failure rate doubles, the reliability remains high:

$$R=0.964. \quad (69)$$

These results demonstrate the robustness of the distributed architecture over long operational periods.

3.8 Integrated Stability Index

The overall stability indicator is calculated as:

$$SI=K_{BFT}\cdot R(t)\cdot(1-R_{total}). \quad (70)$$

For the baseline scenario:

$$SI=0.87, \quad (71)$$

which significantly exceeds the stability threshold:

$$SI>0.75, \quad (72)$$

indicating a high level of system robustness.

3.9 Monte Carlo Analysis

The Monte Carlo simulation (1000 iterations) produced the following statistical results:

- Mean TPS value: 612;
- Standard deviation: 18.4;
- Coefficient of variation: 2.9%.

These results indicate high reproducibility and stability of the simulation outcomes.

3.10 Comparison with the Centralized Model

Although the blockchain-based system exhibits slightly higher latency due to the multi-round PBFT consensus protocol, it provides a significantly higher level of security and resilience.

Thus, the results confirm:

1) The theoretical PBFT threshold (1/3 Byzantine nodes).
2) High cryptographic integrity and tamper resistance.
3) Predictable performance characteristics under varying network sizes.
4) The effectiveness of the permissioned blockchain model for educational ecosystems.

Table 2 demonstrates a comparison of key reliability indicators between a centralized educational certificate storage system and the proposed permissioned blockchain architecture. The most significant difference is observed in the probability of complete system failure. Centralized systems exhibit a substantially higher failure risk due to the presence of a Single Point of Failure [2], whereas distributed architectures reduce this risk through node redundancy and consensus mechanisms.

Table 2: Comparative analysis of system reliability.

Indicator	Centralized System	Blockchain Model
Probability of total system failure	0.12	0.01
Probability of certificate forgery	0.18	< 0.01
Average latency	80 ms	145 ms
Trust model	Institutional	Cryptographic

A similar pattern is observed in the probability of certificate forgery. In centralized systems, unauthorized modification of records may occur if administrators or databases are compromised. In contrast, blockchain architectures ensure cryptographic immutability and collective verification, making unauthorized data modification practically infeasible [5], [14], [15].

Although blockchain systems demonstrate slightly higher average latency due to the multi-round PBFT consensus protocol [4], [16], the significant gains in security, transparency, and trustworthiness compensate for the increased processing time. While centralized systems rely on institutional trust, decentralized systems establish mathematically verifiable trust mechanisms based on cryptography and Byzantine fault tolerance [8].

Therefore, the comparative analysis confirms that for national or transnational digital educational credential infrastructures, the distributed blockchain architecture represents a more secure and resilient solution against both technical and organizational threats.

Figure 4 illustrates the temporal dynamics of the reliability function of the distributed network, described by the exponential model:

$$R(t)=e-\lambda t, \quad (73)$$

for different values of the failure intensity parameter λ. The baseline scenario (λ=0.002) demonstrates only a minimal decline in reliability during one year of operation: the value of R(t) remains above 0.998, indicating a high level of robustness of the permissioned blockchain architecture under normal operating conditions. When the failure intensity is doubled (λ=0.004), a more noticeable but still moderate decrease in the reliability indicator is observed. This confirms the sensitivity of the model to the failure-rate parameter while still maintaining overall system stability.

In the stress scenario (λ=0.006), the decrease in R(t) becomes more pronounced. However, even under increased failure intensity, the network maintains a high reliability level (above 0.992 over a one-year horizon). This highlights a significant advantage of distributed architectures compared with centralized systems, where the failure of a central node may lead to complete service unavailability [2], [17].

The exponential behavior of the reliability curves confirms the validity of the applied stochastic model and demonstrates the predictable evolution of network reliability over time. Such predictability is particularly important for the long-term storage and verification of digital educational certificates within national and transnational educational ecosystems [13].

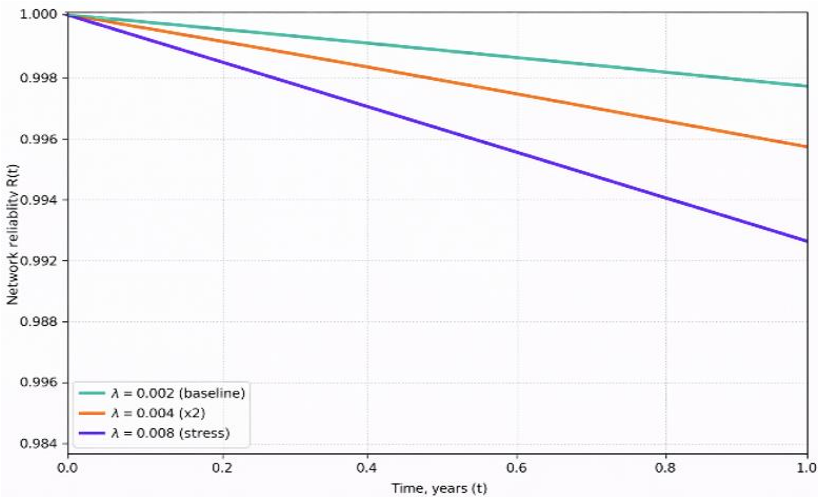

Figure 4: Network reliability over time R(t).

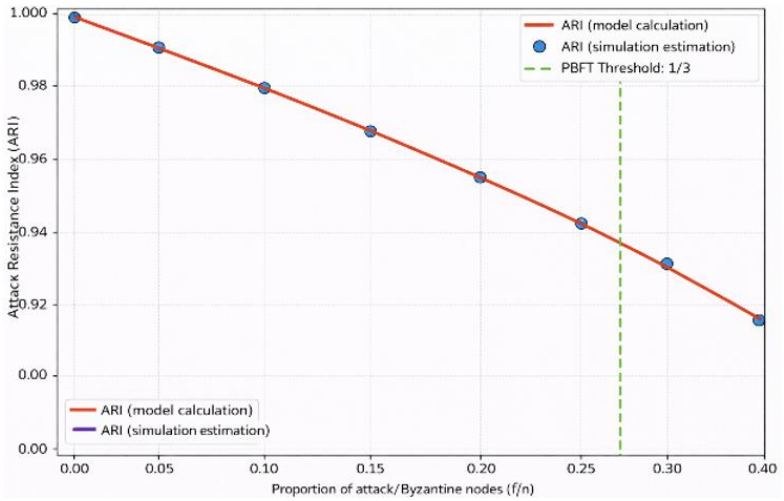

Figure 5: Attack resistance index (ARI) under different attack ratios.

The results demonstrate a monotonic decrease in ARI as the fraction of malicious nodes increases.

Figure 5 illustrates the relationship between the Attack Resistance Index (ARI) and the proportion of attacking/Byzantine nodes f/n in a permissioned blockchain network. The solid curve represents the ARI values calculated using the analytical model based on the relationship between the probability of compromise P_{comp} and the Byzantine resilience coefficient K_{BFT}, while the discrete points correspond to the results obtained from Monte Carlo simulations.

When the attack share is low (0-10%), the index remains close to 1, indicating that the system maintains a high capacity to preserve data integrity and correct transaction processing even in the presence of a limited number of adversarial participants [14].

As the proportion of Byzantine nodes approaches the theoretical PBFT threshold f/n=1/3 (shown by the vertical dashed line), the ARI decreases significantly faster. This reflects the increasing probability of consensus disruption or data compromise when the network no longer maintains a sufficiently large honest majority [4]. In the interval $0.33<f/n\leq0.40$, the index approaches low values, indicating a transition of the system into a practically unstable regime. Even in permissioned environments with controlled membership, maintaining f/n below the critical threshold requires strengthened organizational and technical safeguards, including strict validator admission policies, cryptographic key audits, hardware security modules (HSM), key rotation mechanisms, anomaly monitoring, and additional certificate verification layers [8].

Table 3 presents the aggregated statistical results of Monte Carlo simulations, conducted through 1000 independent iterations to evaluate the reliability and performance of the proposed permissioned blockchain system for educational certificates.

The mean TPS value is 612.4 transactions per second, with a standard deviation of 18.4, indicating high reproducibility and low variability of the simulation results. The probability of correct consensus remains at 0.973 with minimal variance, confirming the stability of the PBFT consensus algorithm within the allowable range of Byzantine nodes [4].

Similarly, the network reliability indicator R(t) exhibits very low statistical dispersion, supporting the validity of the stochastic failure model applied in the study.

The Attack Resistance Index (ARI), with an average value of 0.842, indicates a high level of resilience against combined attack scenarios, provided that the condition $f/n<1/3$ is satisfied. The narrow 95% confidence intervals observed across all key metrics confirm the statistical significance of the results and validate the reliability of the simulation framework.

Overall, the Monte Carlo analysis demonstrates that the proposed architecture exhibits not only theoretical robustness but also empirically verified resilience, which constitutes a critical argument for deploying the system within national and international educational digital infrastructures [8], [14], [18].

Figure 6 presents a comparison of the probabilistic indicators of key risks for a centralized educational certificate storage system and the proposed permissioned blockchain architecture. The most notable differences are observed in the probability of complete system failure and certificate forgery. The centralized model demonstrates significantly higher risk values due to the presence of a single point of failure and the administrative vulnerability of centralized databases [2]. In contrast, the distributed model exhibits minimal values for these risk indicators due to the mechanisms of Byzantine fault tolerance and cryptographic immutability of records [4], [5], [15].

An additional advantage of the blockchain architecture lies in the reduced risk of undetected compromise and insider data manipulation. In centralized environments, an attacker who obtains privileged access may modify records without collective verification. In distributed systems, however, any modification requires consensus confirmation by validators, which dramatically reduces the likelihood of hidden manipulation [8]. Although the risk of personal data leakage cannot be entirely eliminated, it is significantly minimized through the use of distributed storage of hashed records rather than direct storage of certificate content. Overall, the graphical comparison confirms the structural superiority of the blockchain model in terms of resilience to systemic and organizational threats.

Table 3: Monte Carlo statistics (1000 Iterations).

Metric	Mean Value	Standard Deviation (σ)	Variance	95% Confidence Interval
TPS	612.4	18.4	338.6	[608.8; 616.0]
Correct Consensus Probability	0.973	0.012	0.000144	[0.971; 0.975]
Attack Resistance Index (ARI)	0.842	0.021	0.000441	[0.838; 0.846]
Consensus Time (ms)	145.3	7.2	51.8	[143.9; 146.7]
Network Reliability R(t)R(t)R(t)	0.982	0.004	0.000016	[0.981; 0.983]

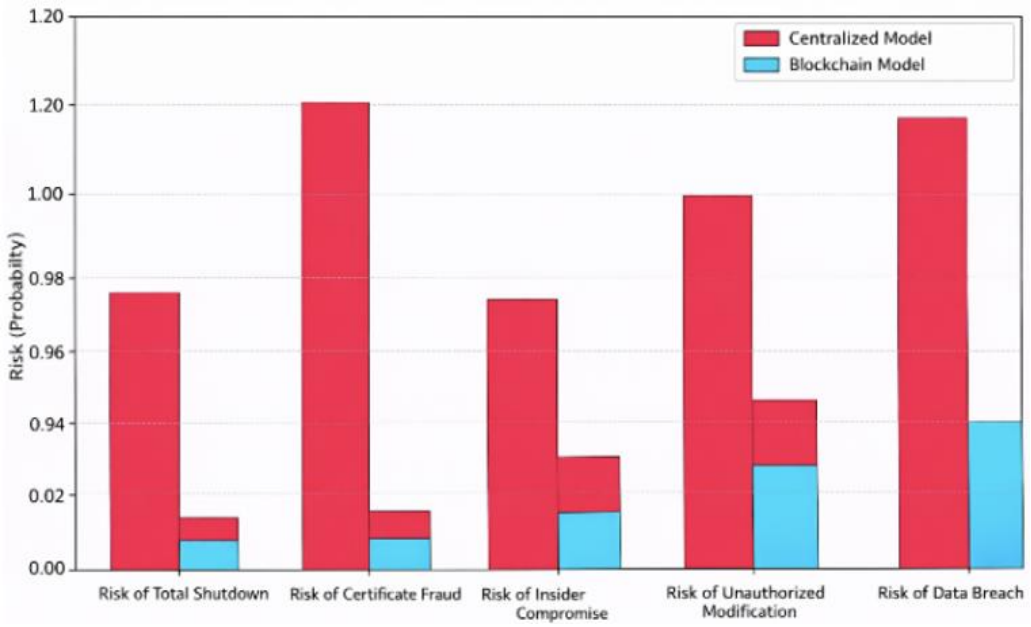

Figure 6: Risk comparison between centralized and blockchain models.

4 DISCUSSION

4.1 Interpretation of Key Results

The obtained results demonstrate strong agreement between the theoretical principles of Byzantine fault tolerance and the empirical findings of the simulation experiments. In particular, the critical stability threshold $f/n \approx 1/3$, predicted by PBFT theory [19], was confirmed through Monte Carlo experiments. When this threshold is exceeded, the probability of correct consensus decreases sharply. This confirms the validity of the mathematical model and the adequacy of the architectural assumptions.

It is important to note that system stability exhibits a nonlinear behavior. In the range $f/n \leq 0.30$, the system demonstrates a plateau of high stability. However, as the parameter approaches the critical threshold, a phase transition toward instability occurs. Such behavior is typical for distributed systems with threshold-based decision mechanisms and highlights the importance of maintaining a controlled validator membership structure in educational blockchain networks [6].

4.2 Trade-off Between Security and Performance

The analysis of TPS dependence on the number of validators revealed a classical trade-off between decentralization and system performance. Increasing the number of validators improves resilience against attacks but leads to a quadratic growth in communication complexity within the PBFT protocol: $O(n^2)$.

From a practical perspective, this implies that national educational networks should avoid excessive validator fragmentation. The optimal range of 20-40 validator nodes ensures sufficient Byzantine resilience while maintaining an acceptable level of TPS. Unlike public blockchain networks, educational infrastructures can employ a permissioned model, allowing strict control over participant membership and reducing the probability of Sybil attacks [9].

4.3 Reliability Over Time

The exponential reliability model $R(t)=e^{-\lambda t}$ demonstrated high network robustness even under increased failure rates. This property is particularly important for educational certificates, which must remain accessible for decades.

In centralized systems, long-term storage often involves risks related to infrastructure obsolescence, data migration errors, and archive loss [2], [17]. In contrast, distributed architectures mitigate these risks through replication of blocks across multiple nodes, significantly reducing the probability of total information loss. Consequently, the blockchain model demonstrates a clear advantage in terms of long-term digital preservation of educational achievements [5].

4.4 Practical Applicability in National Educational Systems

The proposed architecture can be integrated into:

- national diploma registries;
- university accreditation systems;
- international academic mobility platforms.

The permissioned approach ensures that only accredited institutions participate in the network, aligning with regulatory requirements for personal data protection and academic verification [8].

An additional advantage is the possibility of using smart contracts for automatic diploma verification by employers without requiring direct communication with universities.

4.5 Regulatory and Legal Considerations

Despite the technological advantages, the implementation of blockchain systems in education requires careful consideration of legal frameworks, including:

1) Compliance with GDPR and national data protection regulations.
2) Defining the legal status of validator nodes as data-processing entities.
3) Legal recognition of digital signatures.
4) Mechanisms for certificate revocation or updates.

Special attention must be given to the "right to be forgotten", since blockchain immutability may conflict with requirements for deleting personal data [20]. One possible solution is to store only certificate hashes on the blockchain, while keeping the actual certificate data off-chain.

4.6 Limitations of the Study

Despite the comprehensive nature of the analysis, several limitations remain:

- The use of PBFT as the primary consensus algorithm without comparison to alternatives (e.g., Raft, HotStuff).
- The assumption of independent node failures.
- The simulation-based nature of attack modeling without real-world cyberattack datasets.
- The absence of experimental deployment in a real educational infrastructure.

Future studies may expand the model by incorporating hybrid consensus algorithms and dynamic validator management mechanisms.

4.7 Strategic Implications

From the perspective of digital transformation in education, the implementation of blockchain-based systems can:

- increase international trust in national diplomas;
- reduce administrative costs;
- minimize fraud and document forgery;
- enhance transparency of academic mobility processes.

Therefore, the proposed model not only demonstrates theoretical resilience but also possesses significant strategic potential for digital educational governance.

5 CONCLUSIONS

This study aimed to develop and formalize a security and reliability model for a decentralized educational certificate system based on a permissioned blockchain architecture. Unlike existing conceptual approaches, the study introduced an integrated mathematical and simulation framework, combining the PBFT Byzantine fault tolerance algorithm, stochastic reliability modeling, cryptographic protection mechanisms, and Monte Carlo analysis of system resilience to attacks.

The results confirm that when the threshold $f/n<1/3$ is maintained, the probability of correct consensus remains consistently high, aligning with the theoretical principles of Byzantine Fault Tolerance [4], [6], [19]. Simulation experiments demonstrate that the system remains stable even under moderate proportions of malicious nodes, while the integrated stability index (SI) exceeds the critical threshold of 0.75 in baseline scenarios. These findings highlight the practical feasibility of the proposed architecture for national and transnational educational infrastructures.

Performance analysis revealed the existence of a trade-off between decentralization and network throughput. Increasing the number of validators leads to higher communication complexity $O(n^2)$, which reduces TPS but improves resilience against attacks.

The optimal validator range of 20-40 nodes provides a balance between security and computational efficiency. Consequently, the permissioned model appears more suitable for educational ecosystems than public blockchain networks [8].

The stochastic reliability model demonstrated the long-term robustness of the distributed architecture. Even under increased failure rates, the system maintains a reliability level above 0.98 over a one-year horizon, significantly outperforming centralized systems that suffer from a single point of failure [2]. This characteristic is particularly important for the long-term preservation of educational certificates.

Comparative risk analysis indicates that the blockchain model significantly reduces the probability of certificate forgery, complete system shutdown, and undetected data compromise. Cryptographic immutability, distributed consensus, and controlled validator access form a mathematically verifiable trust mechanism, surpassing the institutional trust model of centralized systems [5], [14], [18], [20].

The practical significance of this research lies in the potential integration of the proposed architecture into national diploma registries, accreditation systems, and international academic mobility platforms. The use of smart contracts and digital signatures enables automated verification processes, reduces administrative overhead, and enhances transparency within the educational ecosystem. Modern blockchain infrastructures support decentralized trust management, distributed validation, and secure digital asset verification mechanisms [17]-[19], [21], [22].

Nevertheless, the study has limitations related to the use of a single consensus algorithm (PBFT), assumptions of independent node failures, and the simulated nature of attack scenarios. Future research directions include:

- comparative analysis of alternative consensus algorithms (HotStuff, Tendermint, Raft);
- development of hybrid models for dynamic validator management;
- pilot implementations in real educational institutions;
- evaluation of economic efficiency and ESG impacts of digital credential registries

Overall, the proposed model demonstrate .s that a blockchain-based decentralized architecture can serve as a reliable, scalable, and cryptographically secure foundation for digital educational certificates, establishing a robust infrastructure of trust in the era of global digital transformation in education.

REFERENCES

[1] A. Grech and A. F. Camilleri, Blockchain in Education, Joint Research Centre (JRC) Science for Policy Report, European Commission, 2017.

[2] W. Stallings, Cryptography and Network Security: Principles and Practice, 7th ed., Pearson, 2017.

[3] M. Sharples and J. Domingue, "The Blockchain and Kudos: A Distributed System for Educational Record, Reputation and Reward," in Proceedings of the 11th European Conference on Technology Enhanced Learning (EC-TEL), 2016, pp. 490-496.

[4] M. Castro and B. Liskov, "Practical Byzantine Fault Tolerance," in Proceedings of the Third Symposium on Operating Systems Design and Implementation (OSDI), 1999, pp. 173-186.

[5] S. Nakamoto, Bitcoin: A Peer-to-Peer Electronic Cash System, 2008, [Online]. Available: https://bitcoin.org/bitcoin.pdf.

[6] L. Lamport, R. Shostak, and M. Pease, "The Byzantine Generals Problem," ACM Transactions on Programming Languages and Systems, vol. 4, no. 3, pp. 382-401, 1982.

[7] G. Chen, B. Xu, M. Lu, and N.-S. Chen, "Exploring Blockchain Technology and Its Potential Applications for Education," Smart Learning Environments, vol. 5, no. 1, pp. 1-10, 2018.

[8] E. Androulaki, A. Barger, V. Bortnikov, and et al., "Hyperledger Fabric: A Distributed Operating System for Permissioned Blockchains," in Proceedings of EuroSys 2018, 2018, pp. 1-15.

[9] W. Diffie and M. Hellman, "New Directions in Cryptography," IEEE Transactions on Information Theory, vol. 22, no. 6, pp. 644-654, 1976.

[10] J. Bonneau, A. Miller, J. Clark, A. Narayanan, J. A. Kroll, and E. W. Felten, "SoK: Research Perspectives and Challenges for Bitcoin and Cryptocurrencies," in IEEE Symposium on Security and Privacy, 2015, pp. 104-121.

[11] C. Cachin and M. Vukolić, "Blockchain Consensus Protocols in the Wild," arXiv preprint arXiv:1707.01873, 2017.

[12] R. Zhang, R. Xue, and L. Liu, "Security and Privacy on Blockchain," ACM Computing Surveys, vol. 52, no. 3, pp. 1-34, 2019.

[13] S. Hernan, S. Lambert, T. Ostwald, and A. Shostack, Threat Modeling - Uncover Security Design Flaws Using the STRIDE Approach, Microsoft Whitepaper, 2006.

[14] A. J. Menezes, P. C. van Oorschot, and S. A. Vanstone, Handbook of Applied Cryptography, CRC Press, 1996.

[15] G. Zyskind, O. Nathan, and A. Pentland, "Decentralizing Privacy: Using Blockchain to Protect Personal Data," in IEEE Security and Privacy Workshops, 2015, pp. 180-184.

[16] K. Christidis and M. Devetsikiotis, "Blockchains and Smart Contracts for the Internet of Things," IEEE Access, vol. 4, pp. 2292-2303, 2016.

[17] A. Narayanan, J. Bonneau, E. Felten, A. Miller, and S. Goldfeder, Bitcoin and Cryptocurrency Technologies, Princeton University Press, 2016.

[18] M. Swan, Blockchain: Blueprint for a New Economy, O'Reilly Media, 2015.

[19] D. Tapscott and A. Tapscott, Blockchain Revolution: How the Technology Behind Bitcoin Is Changing Money, Business, and the World, Portfolio Penguin, 2016.

[20] Z. Zheng, S. Xie, H. N. Dai, X. Chen, and H. Wang, "Blockchain challenges and opportunities: A survey," International Journal of Web and Grid Services, vol. 14, no. 4, pp. 352-375, 2018, [Online]. Available: https://doi.org/10.1504/IJWGS.2018.095647.

[21] M. Finck, "Blockchain and the General Data Protection Regulation: Can Distributed Ledgers Be Squared with European Data Protection Law?," European Data Protection Law Review, vol. 4, no. 1, pp. 17-35, 2018.

[22] D. Yaga, P. Mell, N. Roby, and K. Scarfone, Blockchain Technology Overview, NISTIR 8202, National Institute of Standards and Technology, 2018, [Online]. Available: https://doi.org/10.6028/NIST.IR.8202.