sustainability

MDPI

Article

Enhancing Trust and Sustainability in Higher Education Through Blockchain-Based Academic Document Verification

Yenlik Begimbayeva [1,2,3,*], Olga Ussatova [1,2,*], Vladislav Karyukin [2,4], Galimkair Mutanov [2], Yerlan Kistaubayev [2,4] and Medet Turdaliyev [2]

[1] Department of Cybersecurity, Energo University, Almaty 050013, Kazakhstan
[2] Department of Information Security, The Institute of Information and Computational Technologies, Almaty 050010, Kazakhstan; vladislav.karyukin@kaznu.kz (V.K.); mutanov@ipic.kz (G.M.); kistaubayev_yerlan@kaznu.edu.kz (Y.K.); turdaliyev.medet@gmail.com (M.T.)
[3] School of Cybersecurity, Astana IT University, Astana 020000, Kazakhstan
[4] Faculty of Information Technologies, Al-Farabi Kazakh National University, Almaty 050010, Kazakhstan
* Correspondence: ye.begimbayeva@aues.kz (Y.B.); o.ussatova@aues.kz (O.U.)

Abstract

The sustainability of higher education systems increasingly depends on the integrity, transparency, and long-term verifiability of academic credentials. Widespread diploma fraud, unauthorized modification of academic records, and fragmented verification mechanisms undermine institutional trust, graduate mobility, and public confidence in educational outcomes. These challenges directly affect the social and governance dimensions of sustainable development, particularly in the context of universities' digital transformation. This study proposes a blockchain-based approach to support the sustainable governance of academic documents by strengthening transparency, accountability, and auditability. The proposed system employs cryptographic hash anchoring and smart contract–based enforcement to verify academic credentials such as diplomas, transcripts, and certificates. Document contents are processed and stored off-chain, while cryptographic representations and essential metadata are immutably recorded on an EVM-compatible blockchain, ensuring data privacy and resistance to tampering. Any modification to a document results in a mismatch between the original and recomputed hashes, making fraudulent alterations immediately detectable. A web-based application and a role-restricted smart contract were implemented to support document issuance, verification, and immutable audit logging. System evaluation based on blockchain transaction evidence confirms reliable document registration, deterministic verification outcomes, and verifiable linkage between institutional actions and on-chain records. The results indicate that blockchain-based document verification can contribute to the reduction in corruption risks and improve transparency, strengthening institutional trust and supporting sustainable digital governance in higher education systems.

Keywords: sustainability; higher education governance; blockchain; academic document verification; transparency; anti-corruption; digital transformation

Academic Editor: GuoJun Ji

Received: 18 February 2026
Revised: 29 March 2026
Accepted: 30 March 2026
Published: 4 April 2026

1. Introduction

The sustainable development of higher education systems depends not only on the quality of teaching and research, but also on institutional trust, transparency, and effective governance of academic processes [1,2]. Academic credentials—such as diplomas, transcripts, and certificates—serve as formal evidence of educational achievement and play a critical role in graduate employability, international mobility, and recognition of qualifications. The growing digitalization of academic records has intensified challenges related to document forgery, unauthorized modification, and long-term verifiability, which are closely related to broader cybersecurity threats such as social engineering and technical attacks targeting digital information systems [1–4].

Credential fraud and misrepresentation have become persistent problems across both developed and emerging education systems [2,5]. Forged diplomas and manipulated transcripts undermine institutional credibility, distort labor markets, and weaken public confidence in higher education. In many cases, verification processes remain centralized, manual, or institution-specific, making them vulnerable to corruption, insider manipulation, and loss of historical records. As higher education becomes increasingly global and digitally mediated, the sustainability of academic credential governance has emerged as a critical challenge.

From a sustainability perspective, these issues are closely linked to the social and governance dimensions of sustainable development. In particular, reliable credential verification contributes to Sustainable Development Goal 4 (Quality Education) by supporting fair recognition of learning outcomes, and to Sustainable Development Goal 16 (Peace, Justice, and Strong Institutions) by enhancing transparency, accountability, and trust in public institutions. Digital solutions that reduce administrative inefficiencies and corruption risks while strengthening institutional integrity are, therefore, essential for sustainable higher education ecosystems.

In this study, sustainability is defined primarily from a governance and institutional perspective, including:

(i) long-term verifiability of academic records,
(ii) transparency and auditability of institutional actions,
(iii) reduction in corruption risks and administrative inefficiencies.

Environmental sustainability is considered through the selection of energy-efficient blockchain mechanisms (e.g., Proof-of-Authority) and hybrid storage models that reduce computational overhead.

Blockchain technology has been widely discussed as a potential enabler of sustainable digital governance due to its properties of immutability, decentralization, and cryptographic verifiability. In academic contexts, blockchain can function as a long-term institutional memory that preserves evidence of credential issuance and resists post-issuance manipulation. Unlike traditional centralized databases, blockchain-based systems allow independent verification of records without relying on a single trusted authority, thereby enhancing transparency and auditability. In particular, cryptographic hash anchoring ensures that any post-issuance modification of academic documents can be reliably detected, providing a robust mechanism against diploma fraud.

Existing blockchain-based approaches in education have primarily focused on credential issuance platforms, proof-of-existence mechanisms, or interoperability frameworks such as verifiable credentials and decentralized identifiers. While these approaches address portability and user-centric identity management, their institutional adoption often remains limited due to governance complexity, operational costs, and regulatory constraints. Universities and public institutions frequently require solutions that prioritize accountability, auditability, and compliance with existing governance structures.

This study addresses these challenges by proposing a blockchain-based academic document verification system oriented toward sustainable institutional governance rather than credential portability alone. The proposed approach relies on cryptographic hash anchoring and smart contract–based enforcement to ensure the integrity, authorship, and long-term auditability of academic documents. Sensitive document contents are processed off-chain, while the blockchain serves as an immutable and publicly verifiable trust anchor.

The novelty of the proposed approach lies not in introducing new cryptographic primitives, but in formalizing blockchain-based academic document verification as a governance-oriented infrastructure integrated into a national higher education system.

Unlike prior work focused on isolated use cases, the proposed approach provides:

(i) system-level integration with institutional governance structures,
(ii) deterministic verification independent of administrative discretion,
(iii) an auditable and policy-aligned architecture for long-term credential management.

The main contributions of this paper are as follows:

- the design of a blockchain-based architecture that supports sustainable governance of academic documents through transparency and auditability;
- the implementation of smart contracts that enforce institutional accountability and role-based authorization;
- the evaluation of the system using on-chain evidence to demonstrate its practical feasibility and sustainability-oriented benefits.

By framing academic document verification as a component of sustainable digital governance, this work contributes to ongoing discussions on transparency, anti-corruption, and trust in higher education systems.

Unlike prior work that focuses primarily on isolated use cases such as diploma verification, credential tokenization, or academic credit transfer, this study proposes an integrated architecture designed for deployment within a national higher education infrastructure.

The main contribution of this work lies not in introducing new cryptographic primitives, but in the system-level integration of blockchain mechanisms with institutional governance processes. This includes the modeling of stakeholder roles, lifecycle management of academic records, and alignment with existing regulatory and administrative structures.

This approach shifts the focus from purely technical verification mechanisms to governance-oriented system design, addressing transparency, auditability, and long-term trust at the institutional level.

The remainder of this paper is organized as follows. Section 2 reviews related work on blockchain and academic document verification. Section 3 presents the system design and architecture. Section 4 describes the implementation and evaluation. Section 5 discusses the results and implications. Finally, Section 6 concludes the paper.

Recent studies have also explored complementary approaches, such as machine-learning methods, Bayesian models, and uncertainty-aware prediction techniques, for analyzing complex data patterns and improving system reliability in digital infrastructures [6]. While these approaches provide valuable tools for data-driven analysis and prediction, the present study focuses on blockchain-based mechanisms for ensuring data integrity, transparency, and verifiability in academic credential management.

2. Related Work on Blockchain, Sustainability, and Academic Governance

2.1. Blockchain for Document Notarization, Proof-of-Existence, and Timestamping

A significant body of research conceptualizes document verification as a notarization or proof-of-existence problem, where cryptographic hashes of documents are anchored on a blockchain to provide immutable evidence of their existence at a specific point in time. Such approaches are widely applied across multiple regulated domains, including biomedical data, academic records, and digital archives. By minimizing on-chain storage and relying on cryptographic commitments, these systems enhance data integrity while maintaining operational efficiency [1].

From a sustainability perspective, blockchain-based notarization contributes to long-term record preservation and institutional memory, reducing reliance on manual verification processes and on centralized repositories that are vulnerable to loss, manipulation, or organizational change. However, many proof-of-existence solutions focus primarily on technical immutability and do not explicitly address broader governance challenges, such as accountability of issuing institutions, auditability of verification actions, or corruption risks within administrative processes [7].

2.2. Blockchain-Integrated Document Lifecycle Management and Auditability

Beyond static notarization, several studies extend blockchain usage toward document lifecycle management, incorporating version control, approval workflows, and audit trails enforced by smart contracts. These systems enable traceability of document creation, modification, and validation events, providing improved transparency compared to traditional document management systems [8].

In the context of sustainable governance, lifecycle-oriented blockchain solutions are particularly relevant, as they support accountability over extended time horizons and across institutional transitions. Auditability and traceable workflows contribute to transparency and can mitigate corruption and insider manipulation. Nevertheless, existing implementations are often domain-specific and may lack generalizability or alignment with higher education governance requirements, where long-term institutional trust and regulatory compliance are critical [9].

2.3. Academic Credential and Certificate Verification Systems

Academic credential verification has emerged as a prominent application of blockchain technology, motivated by widespread diploma fraud and increasing global mobility of students and graduates. Prior research has proposed blockchain-based frameworks for issuing, verifying, and revoking diplomas and certificates, often emphasizing decentralization and reduction in verification costs [5].

While these systems demonstrate technical feasibility, their contribution to sustainability depends on institutional adoption and governance integration. Many credential-focused platforms prioritize portability and peer-to-peer verification, but under-specify how universities, accreditation bodies, and public authorities participate in governance and oversight. As a result, the long-term sustainability of such solutions remains contingent on their ability to align with institutional policies, legal frameworks, and accountability mechanisms [2].

Recent studies have also explored blockchain-based approaches to improving trust and transparency in information and document management systems within institutional environments. For example, the work presented in [10] analyzes the application of blockchain technologies to enhance reliability, traceability, and the protection of digital records, emphasizing their potential to reduce manipulation and strengthen trust in organizational processes. From a sustainability perspective, such approaches contribute to long-term institutional accountability and support governance mechanisms by ensuring verifiable and tamper-resistant data management.

2.4. Interoperability Frameworks: Verifiable Credentials and Decentralized Identifiers

Standardization efforts such as the W3C Verifiable Credentials (VC) and Decentralized Identifiers (DID) frameworks aim to enable interoperable, user-centric credential ecosystems. These models emphasize selective disclosure, privacy preservation, and cross-domain portability, and are increasingly referenced in discussions of digital identity and credential management [11].

From a sustainability and governance standpoint, however, institutional adoption of VC/DID-based systems faces several challenges. These include governance complexity, operational costs, regulatory uncertainty, and the need for organizational capacity to manage decentralized identity infrastructures. While VC/DID frameworks offer strong technical properties, universities and public institutions may require simpler, governance-oriented solutions that prioritize auditability, institutional accountability, and long-term record integrity over full decentralization and user-managed identity control.

2.5. Smart Contract Security, Trust, and Institutional Accountability

The reliability of blockchain-based verification systems critically depends on the correctness and security of smart contracts. Extensive literature has examined vulnerabilities, formal verification methods, and security analysis techniques for smart contracts, highlighting risks associated with immutable deployment and flawed logic [12].

In sustainability-oriented applications, smart contract security extends beyond technical correctness to institutional trust. Errors or ambiguities in contract logic can undermine confidence in verification outcomes and weaken governance mechanisms. Consequently, blockchain-based academic systems must emphasize transparency, role-based authorization, and auditable execution paths to ensure that smart contracts reinforce, rather than compromise, sustainable institutional governance [13].

2.6. Blockchain-Based Verification and Sustainability Challenges in Higher Education

Across the reviewed literature, several sustainability-related gaps remain evident. First, many blockchain-based verification systems prioritize technical innovation while giving limited attention to governance, policy alignment, and institutional accountability. Second, the integration of blockchain solutions into existing educational and regulatory ecosystems remains insufficiently explored, particularly in contexts where anti-corruption, transparency, and long-term trust are primary concerns. Third, while decentralized identity frameworks offer promising interoperability features, their practical adoption in higher education is constrained by organizational readiness and governance complexity [14–24].

These gaps highlight the need for blockchain-based approaches that explicitly address sustainability objectives in higher education. Systems that emphasize transparency, auditability, and institutional accountability can help reduce corruption risks, strengthen trust in academic credentials, and support Sustainable Development Goals related to quality education and strong institutions. This study builds on prior work by positioning blockchain-based academic document verification as a component of sustainable digital governance rather than solely a technical or identity-centric solution [14–24].

A comparison of Blockchain platforms is presented in Table 1.

Table 1. Comparative analysis of blockchain platforms.

Characteristic	Ethereum	Hyperledger Fabric	Corda
Blockchain type	Public	Private (permissioned)	Private (permissioned)
Consensus mechanism	Proof of Stake (PoS)	PBFT, Kafka, Raft	Raft, BFT-SMaRt
Throughput	15–30 TPS	Up to 20,000 TPS	Up to 10,000 TPS
Privacy	Public	Private	Private
Smart contracts	Solidity (EVM)	Chaincode (Fabric Smart Contracts)	Corda smart contracts
Programming languages	Solidity, Vyper	Go, Java, Node.js	Kotlin, Java
Primary use cases	Decentralized applications (dApps), DeFi	Enterprise solutions	Financial and enterprise solutions

Table 1. *Cont.*

Characteristic	Ethereum	Hyperledger Fabric	Corda
Token support	Supported (ERC-20, ERC-721, etc.)	Not supported	Not supported
Validation mechanism	Global validation by all nodes	Restricted transaction access, flexible privacy control	Transactions visible only to participating parties

Table 2 presents a comparative overview of blockchain-based document verification systems across key governance and sustainability dimensions, highlighting how design choices influence long-term trust, transparency, and practical applicability in higher education.

Table 2. Comparative analysis of blockchain-based academic document verification systems.

Ref.	System/ Approach	Blockchain Type	On-Chain Data	Off-Chain Storage	Lifecycle Support	Identity/ Standard	Smart Contracts	Security Level	Evaluation	Key Limitations
[1]	Kuo et al.	Public	Document hash	External DB	None	None	Optional	None	Conceptual	No lifecycle support
[7]	Zyskind et al.	Public	Hashes, access rules	User storage	Partial	None	Yes	Basic	Partial	Focus on data privacy
[8]	Lemieux et al.	Public	Hashes, events	Institutional repos	Full	None	Yes	Advanced	Case study	Limited interoperability
[9]	Li et al.	Public	Version hashes	Cloud/IPFS	Full	None	Yes	Advanced	Prototype	Domain-specific
[5]	Gräther et al.	Public	Certificate hashes	IPFS	Partial	Custom IDs	Yes	Basic	Prototype	Limited portability
[2]	Turkanović et al.	Public	Hashes, metadata	IPFS	Partial	Custom IDs	Yes	Advanced	Prototype	Limited standardization
[11]	W3C, 2022–2023	Agnostic	Status registries	Holder wallets	Full	VC/DID	Optional	Advanced	Reference impl.	Integration complexity
[12]	Alharby & van Moorsel,	Public	Contracts	External	Depends	None	Yes	Advanced	None	No system validation
[13]	Atzei et al.	Public	Contract state	External	N/A	None	Yes	Advanced	None	Security-focused only
[25]	Mylrea & Gourisetti	Public	Audit events	Cloud	Full	None	Yes	Advanced	Prototype	No credential model
[26]	Rathod et al.	Ethereum	Logs, hashes	IPFS	Full	None	Yes	Advanced	Prototype	No interoperability

As shown in Table 2, many existing solutions emphasize technical verification or credential portability, while providing limited support for institutional governance and long-term auditability. This gap motivates the design choices presented in Section 3, which focus on sustainability-oriented governance, transparency, and accountability in academic document verification.

While this comparison provides a qualitative assessment of system characteristics, a comprehensive quantitative performance evaluation remains an important direction for future research.

While existing systems such as EduCTX [27] focus on decentralized management of academic credits and blockchain-based credential exchange, they primarily address specific functional use cases and operate in fully decentralized environments.

In contrast, the proposed approach emphasizes integration with institutional governance structures, including ministries, universities, and regulatory bodies, within a permissioned blockchain framework. This distinction highlights a shift from decentralized credential ecosystems toward hybrid governance models aligned with national educational infrastructures.

3. Design of the Blockchain-Based Document Verification System

The design of a blockchain-based academic document verification system should be guided not only by technical efficiency but also by sustainability-oriented requirements related to institutional governance, transparency, and long-term accountability. In higher education, document verification systems are expected to function across extended time horizons, organizational changes, and regulatory environments. Therefore, system design must support the durability of trust, resistance to corruption, and auditability of institutional actions, rather than short-term transactional efficiency alone.

From a sustainability perspective, academic document verification systems should reduce dependence on manual administrative procedures, minimize discretionary decision-making, and provide verifiable evidence that remains accessible and trustworthy over time. Blockchain technology offers mechanisms that align with these objectives by enabling immutable record keeping, decentralized verification, and transparent execution of predefined rules. However, effective system design requires careful integration of blockchain components with institutional workflows and governance structures [28–31].

3.1. System Requirements and Sustainability-Oriented Design Principles

The proposed system is designed to satisfy both functional and non-functional requirements arising in sustainable higher education governance. Functionally, the system must support secure issuance, verification, and long-term validation of academic documents, including diplomas, transcripts, and certificates. Non-functional requirements include transparency, auditability, data protection, scalability, and institutional control over authorization processes.

A core sustainability requirement is long-term integrity of academic records. Verification evidence must remain valid even if issuing institutions undergo organizational restructuring, system migration, or policy changes. To address this requirement, the proposed system adopts a cryptographic hash-anchoring model, in which document contents are processed and stored off-chain. Meanwhile, immutable verification evidence is recorded on-chain. In this model, the blockchain does not store the original academic document; it stores only its cryptographic hash. Since even a minimal modification of the document results in a different hash value, any attempt to alter or forge the document can be immediately detected during verification. This property ensures strong tamper resistance and enables long-term integrity verification without exposing sensitive data. Such hybrid designs have been shown to enhance tamper resistance, long-term trust, and institutional transparency while reducing reliance on centralized storage mechanisms [3,32].

Another essential requirement concerns institutional accountability and governance. Verification systems should generate auditable traces of document issuance and validation actions that can be independently inspected by regulators, accreditation bodies, and external stakeholders. In the proposed design, accountability is enforced through smart contracts implementing role-based authorization and mandatory event logging. These mechanisms enhance transparency and reduce opportunities for unauthorized manipulation or corruption within academic administration.

3.2. Overall System Architecture

The system architecture follows a hybrid off-chain/on-chain model that balances sustainability, security, and operational feasibility. The off-chain layer consists of a web-based application and backend services responsible for document processing, user interaction, and transaction preparation. This layer is designed to integrate with existing institutional information systems, enabling gradual adoption without disrupting established administrative workflows.

https://doi.org/10.3390/su18073547

The on-chain layer serves as a decentralized and persistent trust anchor. It records cryptographic representations of academic documents and essential metadata through smart contracts deployed on an EVM-compatible blockchain. By separating document content from verification evidence, the architecture preserves privacy while ensuring long-term auditability and public verifiability of institutional actions.

Figure 1 illustrates the overall architecture of the blockchain-based academic document verification system. The figure highlights the interaction between institutional actors, off-chain application components, and the blockchain layer, emphasizing how governance enforcement and auditability are achieved without exposing sensitive academic data on-chain.

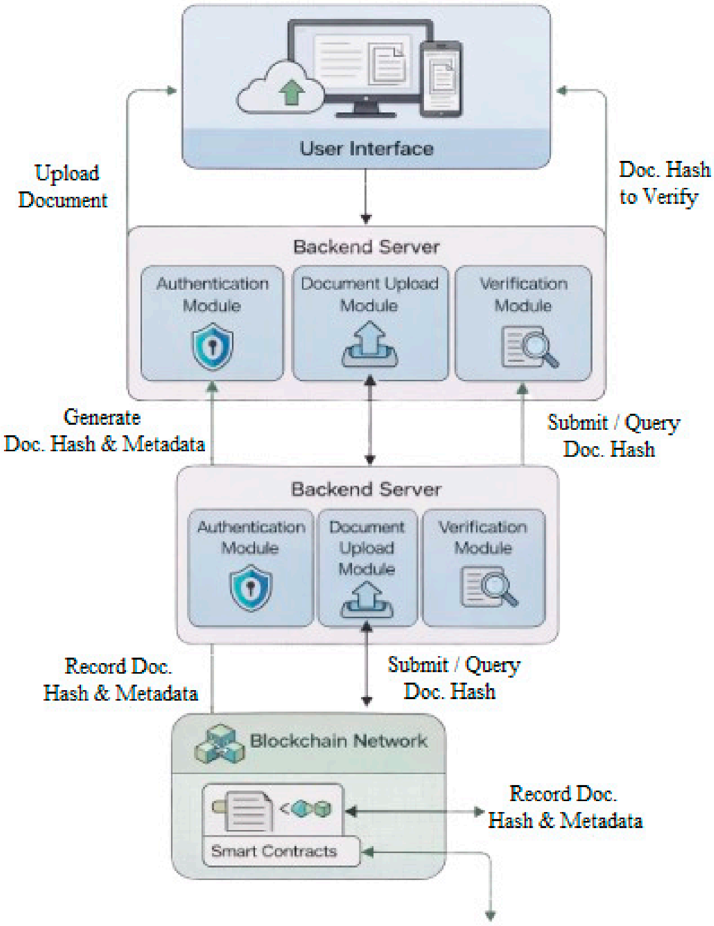

Figure 1. Architecture of the blockchain-based academic document verification system supporting governance enforcement, auditability, and privacy preservation.

The overall architecture of the academic document verification system is illustrated in Figure 2, which presents the main system components and their interactions.

In this architecture, the university (or system administrator) uploads a PDF document through a web-based interface. The document hash is then computed and recorded on the blockchain via a smart contract. To verify a document, a user (or employer) submits or uploads the document hash, which is subsequently compared with the corresponding record stored on the blockchain. Based on this comparison, the system verifies the authenticity and integrity of the document.

An important aspect of system design is selecting an appropriate blockchain type. Depending on security requirements, transaction processing speed, and the degree of decentralization, different blockchain models may be considered, including public, private, and consortium blockchains.

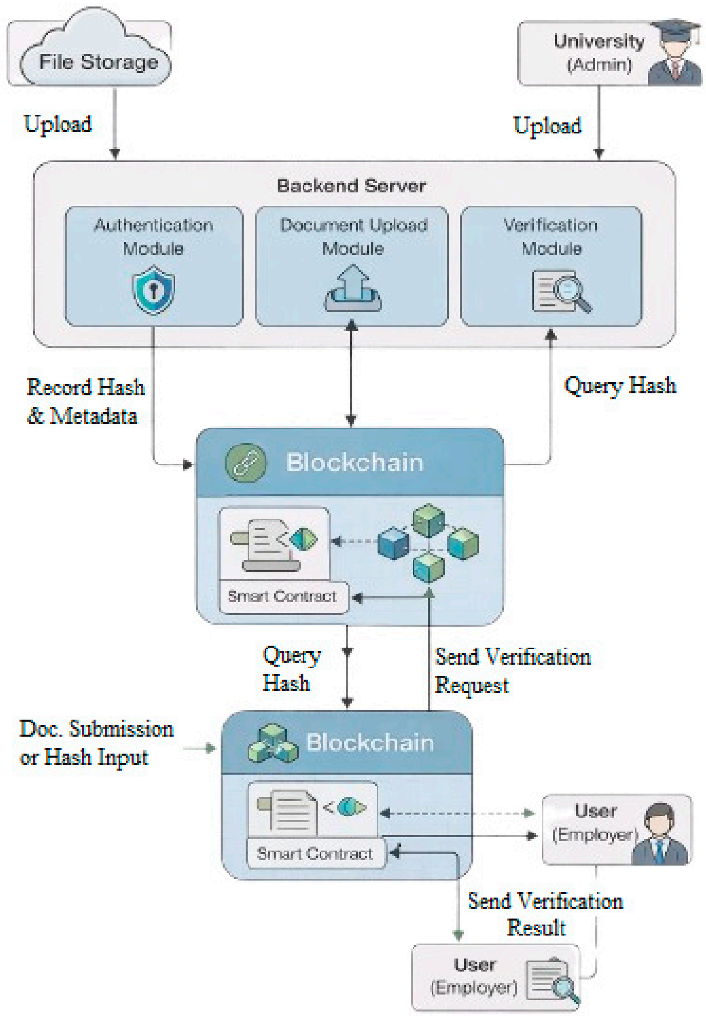

Figure 2. Overall architecture of the document verification system.

Public blockchains, such as Ethereum, provide a high level of decentralization and security; however, they are associated with scalability limitations and lower transaction throughput. Private blockchains, in contrast, offer higher performance and greater control but may be less secure due to centralized governance. Consortium blockchains represent a balanced approach, enabling multiple organizations to jointly manage the network while maintaining an acceptable level of decentralization and trust.

3.3. Workflow of Document Verification and Governance Enforcement

The document verification workflow is designed as a transparent and auditable sequence of actions aligned with sustainable governance principles. When an authorized institution issues an academic document, the system generates a cryptographic hash of the document and submits it to the blockchain via a smart contract. Prior to registration, the smart contract verifies the issuer's authorization based on predefined roles and access rules.

Once validated, the document hash and associated metadata are immutably recorded on-chain. Verification requests are processed by recomputing the document hash and comparing it with the corresponding on-chain record. This process is fully deterministic, as verification outcomes depend solely on cryptographic matching rather than subjective administrative decisions. As a result, the system eliminates discretionary control in the verification process, reducing reliance on institutional staff and significantly lowering the risk of insider manipulation or corruption.

Each document issuance and verification step is accompanied by immutable event records on the blockchain, allowing external stakeholders to independently verify institutional actions without direct access to internal systems. This design enhances transparency across the entire document lifecycle and supports sustainable governance by preserving verifiable evidence of compliance and accountability.

All issuance and verification actions generate immutable blockchain events, creating a verifiable audit trail that can be independently inspected. These audit trails support compliance verification, forensic analysis, and long-term institutional accountability.

Figure 3 presents the document verification workflow and governance enforcement mechanisms. The figure visualizes the sequence of off-chain and on-chain interactions, illustrating how transparency, authorization controls, and auditability are maintained throughout the document lifecycle.

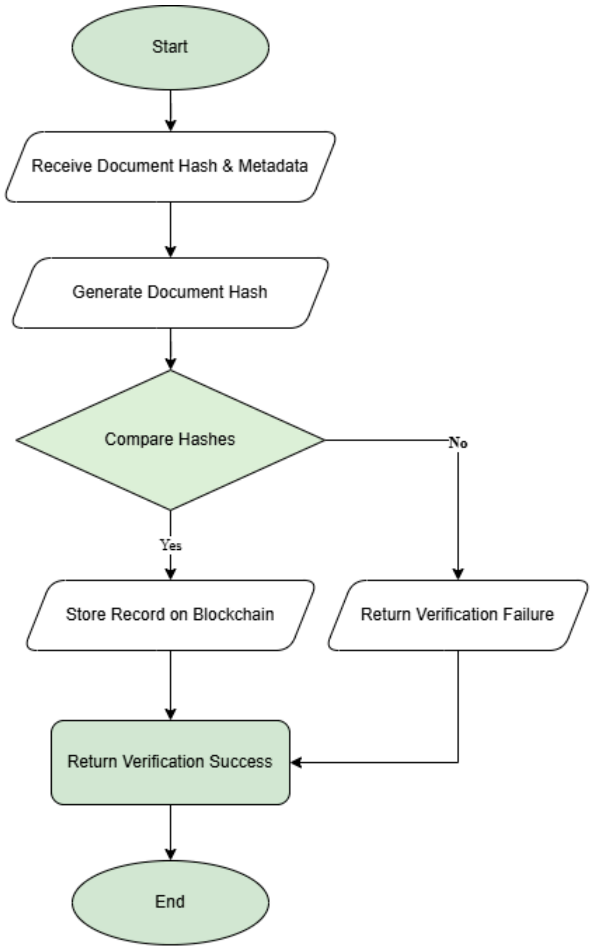

Figure 3. Document verification workflow and governance enforcement mechanisms.

3.4. Design Implications for Sustainable Higher Education Systems

The proposed system design demonstrates how blockchain-based document verification can support sustainable digital governance in higher education. By reducing administrative complexity, limiting centralized decision points, and providing verifiable evidence of academic achievements, the system contributes to transparency and institutional trust.

From a policy and sustainability perspective, the architecture supports anti-corruption objectives by preventing post-issuance manipulation of academic records and by enabling independent verification of institutional actions. These properties are particularly important in cross-border education contexts, where trust in credential authenticity underpins graduate mobility and international cooperation.

Overall, the design illustrates how technical mechanisms—such as cryptographic hash anchoring and smart contract–based governance enforcement—can be aligned with sustainability goals, including accountability, transparency, and long-term resilience of higher education systems.

Governance Enforcement Through Smart Contracts

Smart contracts in the proposed system serve as an institutional governance mechanism rather than a purely technical execution layer. Their primary role is to enforce predefined authorization rules, ensure consistency in verification procedures, and provide transparent and auditable execution of document-related actions. By encoding governance policies directly into the blockchain layer, the system reduces reliance on discretionary administrative decisions and strengthens institutional accountability.

A key sustainability-related property of smart contracts is immutability. Once deployed, the verification rules and authorization constraints cannot be altered without explicit redeployment, ensuring stability and predictability of governance over time. This property supports long-term trust in academic document verification, particularly in environments subject to organizational change or administrative turnover.

Role-based access control implemented within smart contracts ensures that only authorized institutions can register academic documents. Each issuance or verification action is recorded as an immutable blockchain event, creating a verifiable audit trail that can be independently inspected by external stakeholders. From a sustainability perspective, such auditability contributes to transparency, reduces corruption risks, and supports compliance with institutional and regulatory oversight requirements.

By combining deterministic execution, immutability, and event-based logging, smart contracts function as a sustainable enforcement layer that aligns technical verification mechanisms with long-term governance objectives in higher education systems.

All state-changing operations generate immutable blockchain events, creating a transparent and verifiable audit trail. From a sustainability perspective, event-based logging supports institutional accountability, enables external oversight, and reduces corruption risks by ensuring that document issuance and verification actions remain permanently traceable.

4. Web Application Development and System Testing

The practical feasibility of a blockchain-based academic document verification system depends not only on architectural design, but also on its ability to support transparent, auditable, and sustainable institutional workflows. In higher education environments, verification systems must operate reliably under real-world conditions while providing verifiable evidence of institutional actions. Therefore, system implementation and testing were conducted with a focus on transparency, reproducibility, and long-term governance support rather than performance optimization alone.

4.1. Web Application Architecture and Sustainability Considerations

The developed web application functions as an off-chain interaction layer between authorized educational institutions and the blockchain-based verification infrastructure. Its primary role is to support document issuance, the preparation of verification evidence, and the submission of transactions to the blockchain network, while abstracting protocol-level complexity from institutional users.

From a sustainability perspective, this separation of concerns is critical. The web application enables integration with existing institutional information systems and administrative workflows, reducing organizational barriers to adoption. At the same time, core trust enforcement is delegated to the blockchain layer, minimizing reliance on centralized application logic and strengthening long-term institutional accountability.

Document issuance is initiated through the web interface by authorized issuer accounts. The application preprocesses academic documents, generates cryptographic hashes, and submits corresponding transactions to the blockchain via smart contract calls. Role-based authorization is enforced at the smart contract level, ensuring that governance rules remain effective even if the off-chain application is modified or replaced over time.

4.2. System Testing and On-Chain Validation

System testing was performed to evaluate the correctness, transparency, and auditability of the proposed architecture under realistic conditions. The evaluation focused on the system's ability to generate verifiable evidence of institutional actions rather than solely on functional success.

Blockchain explorer data were used to validate transaction execution, event emission, and state changes resulting from document issuance. Successful transaction confirmation demonstrates that smart contract rules were applied consistently and that document hashes were immutably recorded on-chain.

Event-level validation provides an additional layer of transparency. Emitted blockchain events record essential attributes of document issuance, including issuer identity, timestamp, and cryptographic document representation. These immutable logs enable external stakeholders to verify institutional actions without accessing internal systems, thereby supporting auditability and governance oversight.

Figure 4 presents a representative transaction generated during transcript issuance. The successful execution status confirms that the smart contract logic was executed correctly and that sufficient gas was provided. The recorded confirmation time below 15 s in the test network suggests that the system can support timely academic document registration.

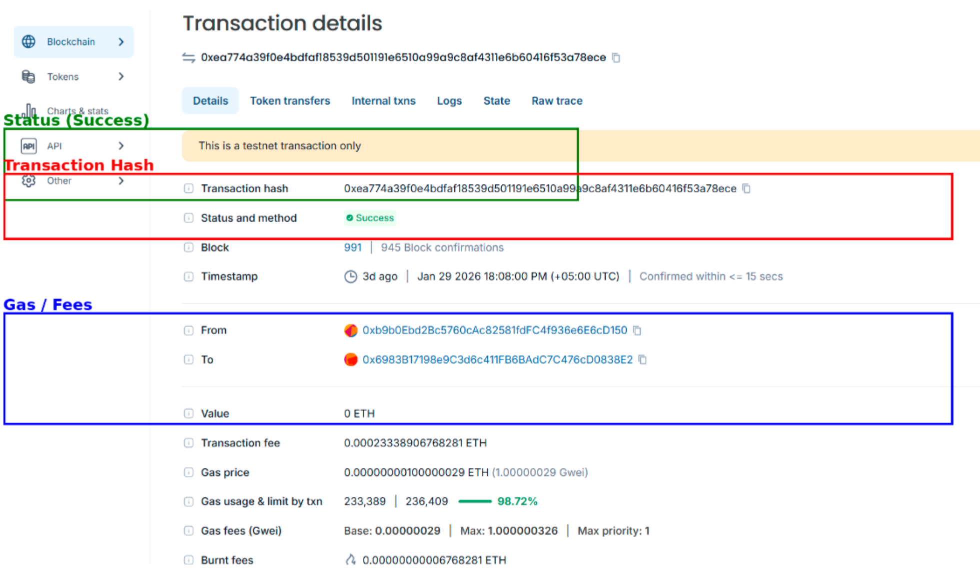

Figure 4. Verified blockchain transaction confirming the immutable registration of an academic document.

The observed transaction confirmation time (below 15 s in the test network) indicates that the system can support near real-time academic document registration. Given the relatively low frequency of document issuance events in higher education, such latency is sufficient for practical deployment and does not represent a performance bottleneck.

From a scalability perspective, the use of a permissioned blockchain architecture combined with a Proof-of-Authority consensus mechanism enables higher throughput and lower computational overhead compared to public blockchain systems. In addition, the hybrid on-chain/off-chain storage model significantly reduces on-chain data processing, improving system efficiency and scalability.

Although a comprehensive large-scale quantitative evaluation is beyond the scope of this study, the observed performance characteristics and architectural design choices indicate that the proposed system is suitable for institutional deployment scenarios.

Given the relatively low frequency of academic document issuance events, such latency is acceptable for institutional workflows and does not represent a bottleneck for practical deployment.

Compared to traditional verification processes, which may require manual requests and take several days, the proposed system enables near-instant verification based on cryptographic matching, significantly reducing administrative overhead and response time.

Event-level validation shows the immutable logs emitted by the smart contract. The presence of the TranscriptSaved event confirms that transcript registration logic was executed and provides cryptographic proof of issuance. These logs enable independent verification by third parties without requiring access to contract storage, thereby supporting efficient auditing and transparency.

5. Discussion

The results presented in this study suggest that blockchain-based academic document verification can be implemented in a manner that supports governance-oriented sustainability objectives in higher education.

The contribution of this study is positioned at the architectural and institutional level rather than at the level of individual technical components. While the underlying technologies are well-established, their integration within a governance-oriented framework enables new capabilities related to transparency, auditability, and regulatory alignment in higher education systems.

In this study, sustainability is conceptualized primarily from a governance and institutional perspective, including long-term verifiability of academic records, transparency and auditability of institutional processes, and reduction in corruption risks.

Environmental sustainability is considered through the use of energy-efficient blockchain mechanisms and system design choices that reduce computational overhead.

Unlike approaches that focus primarily on technical verification or credential portability, the proposed system emphasizes governance mechanisms that ensure transparency, accountability, and auditability. These properties are central to sustainable digital governance, particularly in environments where academic credentials must remain verifiable over extended time horizons and across organizational changes.

From an operational perspective, the proposed architecture incorporates several design choices aimed at improving system performance, including the use of a permissioned consortium blockchain, an energy-efficient Proof-of-Authority consensus mechanism, and a hybrid on-chain/off-chain data storage model. These features contribute to reduced latency and improved scalability compared to public blockchain infrastructures.

Although the proposed architecture minimizes data exposure through a hybrid on-chain/off-chain storage model, more advanced privacy-preserving techniques, such as zero-knowledge proofs, may further enhance confidentiality. In particular, such approaches would enable verification of academic credentials without disclosing sensitive information about the individual, thereby improving compliance with modern data protection regulations such as GDPR. The integration of zero-knowledge proof mechanisms is considered a promising direction for the future development of the system.

From an environmental perspective, the choice of a permissioned blockchain architecture with a Proof-of-Authority consensus mechanism can reduce energy consumption compared to traditional Proof-of-Work systems. This design choice aligns with sustainability considerations by minimizing computational requirements and associated carbon footprint. Although a full quantitative assessment of energy consumption and carbon footprint is beyond the scope of this study, existing research indicates that Proof-of-Authority mechanisms require significantly lower computational resources compared to Proof-of-Work systems, making them suitable for sustainability-oriented institutional deployments.

Furthermore, the hybrid storage model reduces the volume of data processed on-chain, contributing to improved efficiency and lower resource utilization.

To further illustrate these differences, Table 3 presents a comparative overview of energy consumption characteristics of common blockchain consensus mechanisms, highlighting their relevance for sustainability-oriented applications.

Table 3. Energy consumption comparison of blockchain consensus mechanisms.

Consensus Algorithm	Typical Energy Consumption	Hardware Requirements	Environmental Impact
Proof-of-Work (PoW)	Very high (requires continuous cryptographic mining)	Specialized mining hardware (GPU/ASIC)	High carbon footprint
Proof-of-Stake (PoS)	Low	Standard server infrastructure	Significantly reduced energy consumption compared to PoW
Proof-of-Authority (PoA)	Very low	Standard server infrastructure operated by trusted validators	Minimal environmental impact

While smart contract immutability ensures consistency of verification rules, it also introduces challenges related to system upgrades and error correction.

To mitigate these risks, practical implementations require governance mechanisms such as contract versioning, controlled updates, institutional oversight, as well as key management policies and dispute resolution procedures to ensure alignment with regulatory and operational requirements.

These considerations highlight the importance of complementing architectural design with further empirical evaluation and governance analysis, as discussed in the limitations section.

5.1. Contribution to Sustainable Governance and Institutional Trust

From a governance perspective, the proposed system strengthens institutional accountability by ensuring that academic document issuance and verification actions are immutably recorded and independently verifiable. The use of cryptographic hash anchoring and smart contract–based enforcement reduces reliance on discretionary administrative procedures, which are often vulnerable to errors, inconsistencies, or corruption. By encoding authorization rules and verification logic directly into the blockchain layer, the system provides predictable and transparent governance mechanisms that persist beyond individual software platforms or personnel.

These properties contribute directly to the sustainability of higher education institutions by reinforcing trust among stakeholders, including students, employers, accreditation bodies, and regulators. Trustworthy credential verification supports fair recognition of educational achievements and helps preserve institutional reputation, which is a critical but often overlooked component of sustainable educational systems.

In addition, the adoption of blockchain-based academic credential systems requires alignment with international frameworks for cross-border recognition of qualifications. In particular, standards such as the Lisbon Recognition Convention and ENIC-NARIC guidelines play a critical role in ensuring interoperability and institutional acceptance across different jurisdictions.

The proposed architecture is designed to integrate with existing institutional governance structures, allowing adaptation to national regulatory requirements and supporting international academic mobility through verifiable digital credentials.

5.2. Transparency, Auditability, and Anti-Corruption Implications

A key outcome of the system design and testing is the establishment of immutable audit trails through blockchain event logging. Each document-related action generates verifiable on-chain evidence that can be inspected without accessing internal institutional systems. This level of transparency enables effective external oversight and facilitates compliance verification, which are essential elements of sustainable governance.

From an anti-corruption perspective, the inability to alter or retroactively manipulate academic records without detection may reduce opportunities for certain types of fraudulent practices, particularly those involving post-issuance modification of academic records. Fraudulent modifications of academic documents become immediately detectable due to hash mismatches, ensuring that any unauthorized intervention leaves verifiable evidence. By shifting trust from discretionary institutional responses to cryptographically verifiable evidence, the proposed approach aligns with broader sustainability goals related to integrity, accountability, and the rule of law in public institutions.

However, the system does not prevent cases where valid credentials are intentionally issued to unqualified individuals, which remains an institutional governance issue beyond the scope of blockchain technology.

In this context, blockchain should be understood as a tool for ensuring the integrity, transparency, and traceability of academic records, rather than as a mechanism for eliminating all forms of institutional corruption.

Addressing such issues requires complementary institutional governance mechanisms beyond the scope of the proposed system.

5.3. Alignment with Sustainable Development Goals

The proposed system contributes to multiple dimensions of sustainable development. In particular, it supports Sustainable Development Goal 4 (Quality Education) by enhancing the reliability and recognition of academic credentials, thereby promoting equitable access to educational and employment opportunities. It also aligns with Sustainable Development Goal 16 (Peace, Justice, and Strong Institutions) by strengthening transparency, accountability, and institutional trust through verifiable digital governance mechanisms.

By addressing credential fraud and verification inefficiencies, the system helps create more resilient and trustworthy higher education ecosystems. Such ecosystems are better equipped to support international mobility, cross-border education, and lifelong learning, all of which are critical components of sustainable societies.

The observed transaction confirmation time (<15 s) indicates that the system can support real-time academic document registration under typical institutional workloads. Given the relatively low frequency of document issuance events, the system demonstrates sufficient scalability for practical deployment scenarios.

5.4. Comparison with Existing Approaches

Compared to existing blockchain-based credential systems, particularly those centered on verifiable credentials and decentralized identifiers, the proposed approach prioritizes institutional governance and auditability over full decentralization and user-managed identity control. While interoperability frameworks offer important advantages, their practical adoption in higher education is often constrained by governance complexity, regulatory uncertainty, and organizational readiness.

The findings of this study suggest that sustainability-oriented design choices—such as focusing on long-term auditability and institutional accountability—may offer a more feasible pathway for adoption in public and regulated educational environments. By complementing rather than replacing existing institutional structures, the proposed system supports gradual integration into established governance frameworks.

5.5. Transition Framework for Blockchain-Based Academic Document Verification

While the proposed architecture demonstrates technical feasibility and governance-oriented advantages, its practical adoption in higher education requires a structured transition framework aligned with existing institutional and regulatory infrastructures.

Based on the implemented system and integration architecture, this study proposes a practical framework for transitioning from manual and semi-digital academic document management systems to blockchain-based verification systems. The framework follows a hybrid approach that integrates institutional information systems, government digital services, and blockchain infrastructure, enabling gradual adoption without disrupting existing workflows.

The transition process consists of the following stages:

Stage 1: Digitization and Structuring of Academic Records

Academic documents (e.g., diplomas, transcripts) are digitized and standardized to ensure compatibility with cryptographic processing and reliable hash generation.

Stage 2: Integration with Government and External Verification Services

The system integrates with external services (e.g., SmartBridge and national databases) using secure XML-based requests signed with electronic certificates, ensuring legal validity and trusted identity verification.

Stage 3: Secure Data Exchange and Validation

Data are exchanged via structured XML messages with digital signatures to guarantee integrity, authenticity, and non-repudiation. Only verified data proceed to blockchain registration.

Stage 4: Smart Contract Deployment and Role-Based Governance

Smart contracts implement role-based access control (RBAC), allowing only authorized institutions to issue academic records. Governance rules are encoded to ensure transparency and auditability.

Stage 5: Blockchain Registration and Immutable Storage

Document data are transformed into cryptographic hashes and recorded on-chain. Event-based logging mechanisms provide efficient and transparent proof of document issuance.

Stage 6: Verification and Auditability

Verification is performed through deterministic comparison with on-chain records. Transaction hashes and logs enable independent validation without institutional intermediaries.

The proposed framework addresses key barriers such as governance complexity and organizational capacity by enabling incremental integration with existing systems. The use of standardized mechanisms (XML, SOAP, and digital signatures) ensures regulatory compatibility and facilitates adoption at institutional and national levels.

Overall, the framework demonstrates that blockchain-based academic document verification can be implemented as an extension of existing digital ecosystems, providing a scalable and practical pathway toward sustainable digital governance in higher education.

The proposed transition framework is illustrated in Figure 5.

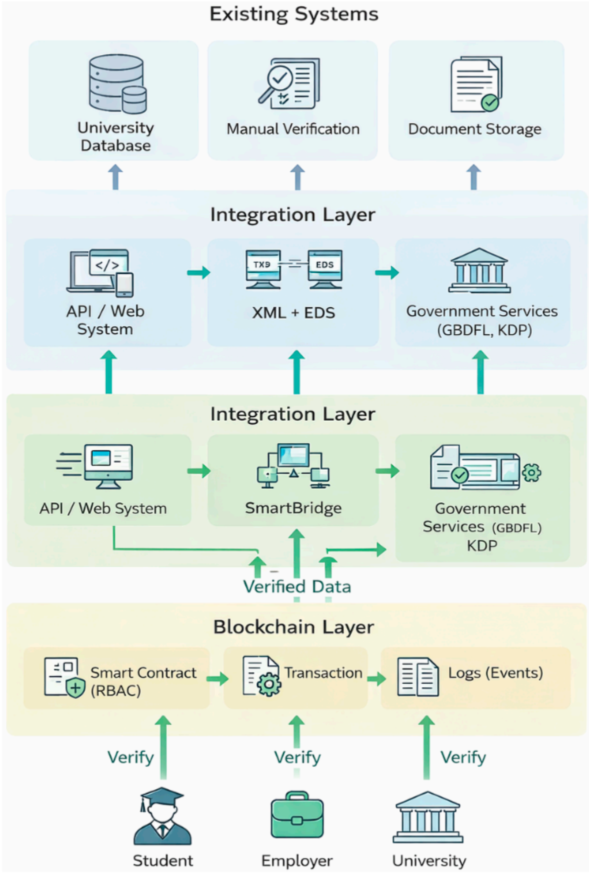

Figure 5. Framework for transition to blockchain-based academic document verification systems.

5.6. Limitations and Future Research Directions

Despite its contributions, this study has several limitations. The system evaluation focuses on functional validation and governance-related properties rather than large-scale performance or cost analysis. Future work could explore scalability under higher transaction volumes, comparative energy consumption, and integration with national or international credential frameworks.

Additionally, while the system demonstrates technical and governance feasibility, broader adoption will depend on regulatory alignment, policy support, and institutional willingness to adopt blockchain-based verification mechanisms. Further research is needed to examine legal, organizational, and socio-technical factors influencing long-term sustainability and adoption in diverse educational contexts.

6. Conclusions

This study presented a blockchain-based academic document verification system designed to support sustainable digital governance in higher education. By combining cryptographic hash anchoring, smart contract–based governance enforcement, and a hybrid off-chain/on-chain architecture, the proposed approach addresses key challenges related to transparency, accountability, and long-term trust in academic credential management.

The results demonstrate that blockchain technology can be applied not merely as a technical verification tool, but as an institutional trust infrastructure that strengthens governance and auditability of academic processes. Immutable on-chain records and event-based audit trails provide verifiable evidence of document issuance and verification actions, reducing reliance on discretionary administrative procedures and mitigating corruption risks. These properties are essential for ensuring the long-term integrity and sustainability of higher education systems.

From a sustainability perspective, the proposed system contributes to Quality Education (SDG 4) by enhancing the reliability and recognition of academic credentials, and to Strong Institutions (SDG 16) by promoting transparency, accountability, and institutional trust. Unlike approaches focused primarily on credential portability or user-centric identity management, this work emphasizes governance-oriented design choices that align with the practical needs of universities and public institutions.

The findings indicate that blockchain-based document verification can be integrated into existing institutional workflows without disrupting established governance structures, supporting gradual adoption and long-term resilience. While further research is required to assess scalability, regulatory integration, and cross-border interoperability, the proposed approach provides a practical foundation for sustainable digital transformation of academic credential verification.

Overall, this work highlights the potential of blockchain technology to function as an enabling mechanism for sustainable governance in higher education, supporting transparent, trustworthy, and resilient academic ecosystems.

Author Contributions: Conceptualization, Y.K., M.T. and G.M.; methodology, Y.K., M.T. and G.M.; software, Y.K., M.T. and G.M.; investigation, Y.K., M.T. and G.M.; resources, Y.K., M.T. and G.M.; writing—original draft preparation, all authors; writing—review and editing, Y.B., O.U. and V.K.; visualization, Y.B., O.U. and V.K.; funding acquisition, G.M. All authors have read and agreed to the published version of the manuscript.

Funding: This research was funded by the Science Committee of the Ministry of Science and Higher Education of the Republic of Kazakhstan (Grant No. BR24993014 "The development of an intelligent anti-corruption system for information protection and validation of the results of academic achievements and official documents of students and graduates of the universities of the Republic of Kazakhstan").

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: The original contributions presented in this study are included in the article. Further inquiries can be directed to the corresponding authors.

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

Abbreviations

The following abbreviations are used in this manuscript:

ABI	Application Binary Interface
API	Application Programming Interface
BC	Blockchain
DID	Decentralized Identifier
DApp	Decentralized Application
EVM	Ethereum Virtual Machine
GUI	Graphical User Interface
IPFS	InterPlanetary File System
SDG	Sustainable Development Goal
VC	Verifiable Credential

References

1. Kuo, T.-T.; Kim, H.-E.; Ohno-Machado, L. Blockchain distributed ledger technologies for biomedical and health care applications. *J. Am. Med. Inform. Assoc.* **2017**, *24*, 1211–1220. [CrossRef] [PubMed]
2. Turkanović, M.; Hölbl, M.; Košič, K.; Heričko, M.; Kamišalić, A. EduCTX: A blockchain-based higher education credit platform. *IEEE Access* **2018**, *6*, 5112–5127. [CrossRef]
3. Kistaubayev, Y.; Liébana-Cabanillas, F.; Shaikh, A.A.; Mutanov, G.; Ussatova, O.; Shinbayeva, A. Enhancing transparency and trust in higher education institutions via blockchain: A conceptual model utilizing the Ethereum consortium approach. *Sustainability* **2025**, *17*, 9350. [CrossRef]
4. Mambetov, S.; Begimbayeva, Y.; Joldasbayev, S.; Kazbekova, G. Internet threats and ways to protect against them: A brief review. In Proceedings of the 13th International Conference on Cloud Computing, Data Science & Engineering (Confluence), Noida, India, 19–20 January 2023; pp. 195–198. [CrossRef]
5. Gräther, W.; Kolvenbach, S.; Ruland, R.; Schütte, J.; Torres, C.; Wendland, F. Blockchain for education: Lifelong learning passport. In Proceedings of the 1st ERCIM Blockchain Workshop, Amsterdam, The Netherlands, 8–9 May 2018. [CrossRef]
6. Karyukin, V.; Ussatova, O.; Zhumabekova, A.; Matson, E.T.; Zhumabekova, K.; Ussatov, N.; Begimbayeva, Y. The development of a data protection system in healthcare using deep learning models. *J. Artif. Intell. Technol.* **2025**, *6*, 129–150. [CrossRef]
7. Zyskind, G.; Nathan, O.; Pentland, A. Decentralizing privacy: Using blockchain to protect personal data. In Proceedings of the IEEE Symposium on Security and Privacy Workshops, San Jose, CA, USA, 21–22 May 2015; pp. 180–184. [CrossRef]
8. Lemieux, V.L.; Hofman, D.; Batchelor, S.; Joo, A.; Hogg, D.; Shingala, K. Blockchain technology for recordkeeping: Help or hype? *Rec. Manag. J.* **2019**, *29*, 15–36.
9. Li, J.; Greenwood, D.; Kassem, M. Blockchain in the built environment and construction industry: A systematic review, conceptual models and practical use cases. *Autom. Constr.* **2019**, *102*, 288–307. [CrossRef]
10. Begimbayeva, Y.; Zhaxalykov, T.; Akhtanov, A.; Pashkevich, R.; Ussatova, O.; Arshidinova, M. Design of a QKD protocol resistant to insider attacks in fully connected decentralized networks. *East.-Eur. J. Enterp. Technol.* **2025**, *4*, 43–50. [CrossRef]
11. Sporny, M.; Longley, D.; Chadwick, D. Verifiable Credentials Data Model v2.0. In *W3C Recommendation*; World Wide Web Consortium: Cambridge, MA, USA, 2024.
12. Alharby, M.; van Moorsel, A. Blockchain-based smart contracts: A systematic mapping study. *Int. J. Netw. Secur. Appl.* **2017**, *9*, 1–17. [CrossRef]
13. Atzei, N.; Bartoletti, M.; Cimoli, T. A survey of attacks on Ethereum smart contracts. In *Financial Cryptography and Data Security*; Springer: Berlin/Heidelberg, Germany, 2017; pp. 164–186. [CrossRef]
14. Kolydas, T. Timestamping metadata using blockchain: A practical approach. In *Metadata and Semantic Research*; Springer: Cham, Switzerland, 2019; pp. 556–564. [CrossRef]
15. Zhang, Y.; Xue, R.; Liu, L. Security and privacy on blockchain. *ACM Comput. Surv.* **2019**, *52*, 1–34. [CrossRef]
16. Reed, D.; Sporny, M.; Longley, D. Decentralized Identifiers (DIDs) v1.0. In *W3C Recommendation*; World Wide Web Consortium: Cambridge, MA, USA, 2022.
17. OpenID Foundation. *OpenID for Verifiable Credential Issuance (OpenID4VCI)*; OpenID Foundation: San Ramon, CA, USA, 2023.
18. Khovratovich, D.; Law, J.; Sabadello, M. Revocation mechanisms for decentralized identifiers and verifiable credentials. *IEEE Secur. Priv.* **2021**, *19*, 48–55.
19. Derler, D.; Ramacher, S.; Slamanig, D. SD-BLS: Scalable distributed revocation for verifiable credentials. In Proceedings of the ACM CCS Workshops, Los Angeles, CA, USA, 7–11 November 2022; pp. 203–214.
20. MIT Media Lab. *Blockcerts—An Open Infrastructure for Academic Credentials on the Blockchain*; MIT Media Lab: Cambridge, MA, USA, 2019.
21. European Commission. *European Blockchain Services Infrastructure (EBSI)*; European Commission: Brussels, Belgium, 2023.
22. ETSI. *PAdES—Digital Signatures in PDF Documents*; ETSI: Sophia Antipolis, France, 2022.
23. Hoops, J.; Matthes, F. Universal sign-in with verifiable credentials. *IEEE Access* **2022**, *10*, 118456–118470.
24. Lux, T.; Thatmann, D.; Guggenmos, F. Distributed ledger–based authentication using decentralized identifiers. In *IEEE Blockchain*; IEEE: Piscataway, NJ, USA, 2019; pp. 307–314.
25. Mylrea, M.; Gourisetti, S.N.G. Blockchain for cyber-resilient industrial control systems. *IEEE Access* **2017**, *5*, 24705–24717.
26. Rathod, S.; Narkhede, P.; Mendhe, S.; Shah, A.D. A secure audit trail framework using blockchain. *Computers* **2020**, *9*, 44.
27. Xu, X.; Weber, I.; Staples, M. *Architecture for Blockchain Applications*; Springer: Cham, Switzerland, 2019.
28. Meng, W.; Tischhauser, E.; Wang, Q.; Wang, Y.; Han, J. When intrusion detection meets blockchain technology. *IEEE Access* **2018**, *6*, 10179–10188. [CrossRef]
29. Pahl, C.; El Ioini, N.; Helmer, S.; Lee, B. Trusted data sharing with blockchain. *IEEE Internet Comput.* **2018**, *22*, 19–27.
30. Xu, X.; Pautasso, C.; Zhu, L.; Gramoli, V.; Ponomarev, A.; Tran, A.B.; Chen, S. The blockchain as a software connector. In Proceedings of the 2016 13th Working IEEE/IFIP Conference on Software Architecture (WICSA), Venice, Italy, 5–8 April 2016; pp. 182–191.

31. Casino, F.; Dasaklis, T.K.; Patsakis, C. Blockchain-based applications: A systematic review. *Telecommun. Syst.* **2019**, *71*, 99–118.
32. Razaque, A.; Amanzholova, S.; Mutanov, G.; Ussatova, O.; Farhad, M.A.; Kistaubayev, Y.; Kamilla, S.; Adilzhan, K. An anti-corruption system for academic achievement verification using blockchain. *Front. Blockchain* **2025**, *8*, 1683522. [CrossRef]

https://doi.org/10.3390/su18073547