Blockchain-Enabled Learning Management Systems: Redefining Trust and Security in Digital Education

Nemanja Zdravković[0000-0002-2631-6308]

Faculty of Information Technology, Belgrade Metropolitan University

Tadeuša Košušća 63, 11000 Belgrade, Serbia

nemanja.zdravkovic@metropolitan.ac.rs

Abstract. The widespread adoption of Learning Management Systems (LMSs) as mission-critical digital infrastructures in higher education has introduced significant security and trust challenges. While centralized LMS architectures provide operational efficiency, they remain structurally vulnerable to insider threats, silent database compromise, mutable audit logs, and credential forgery. Existing blockchain-based research in education has largely focused on certificate authentication and transcript portability, leaving internal LMS integrity and enterprise-grade threat mitigation insufficiently addressed.

This paper proposes a blockchain-enabled audit extension architecture for LMS environments, designed to enhance assessment integrity, traceability, and institutional trust without replacing existing platforms. Building upon a formal threat model tailored to LMS infrastructures, we derive security requirements including immutability, non-repudiation, auditability, confidentiality, and trust separation. To satisfy these requirements, we introduce a permissioned distributed ledger layer based on Hyperledger Fabric, operating alongside the institutional Information System. The architecture employs event-based transaction modeling, identity-bound cryptographic signatures, distributed endorsement policies, and minimal on-chain storage through hash anchoring of sensitive data.

A proof-of-concept implementation within a controlled institutional test network demonstrates the feasibility of recording grade submission and modification events as append-only ledger transactions. The prototype validates distributed validation, identity attribution via Certification Authority infrastructure, and tamper-evident audit logging using a Raft-based ordering service and CouchDB world state management.

The results indicate that integrating a permissioned blockchain layer can significantly strengthen enterprise security posture by mitigating structural weaknesses inherent in centralized LMS systems. Although the current deployment remains limited in scale, the proposed model establishes a scalable foundation for secure, verifiable digital education infrastructures and future large-scale institutional integration.

Keywords: blockchain · learning management systems · Hyperledger Fabric · enterprise security · digital education · permissioned distributed ledger

Research Paper - Invited Paper
DOI: https://doi.org/10.46793/BISEC25.009Z
Part of ISBN: 978-86-89755-40-4

1 Introduction

The digital transformation of higher education has fundamentally reshaped the way teaching, assessment, and credentialing are conducted. Learning Management Systems (LMSs) have become critical digital infrastructures supporting course delivery, assessment submission, grade management, certification issuance, and communication between learners on one side and faculty on the other. Particularly after the global shift toward online and hybrid learning models accelerated by the COVID-19 pandemic, LMS platforms have transitioned from supplementary tools to mission-critical enterprise systems within Higher Education Institutions (HEIs) [1–3].

While LMS platforms provide scalability and operational efficiency, their centralized architectures introduce significant security and trust challenges [4]. Most commercially available LMS solutions rely on traditional client-server architectures and centralized database management systems. In such environments, administrators maintain privileged access, assessment records are mutable, and audit mechanisms depend heavily on institutional oversight rather than cryptographic guarantees [5]. From a business information security perspective, this architecture creates exposure to several risk categories: unauthorized grade manipulation, credential fraud, insider misuse, insufficient auditability, and reputational damage resulting from compromised academic integrity [6].

The importance of secure credentialing and academic data protection has already been highlighted in prior research. Earlier work has explored blockchain-based models for secure handling of education information and learner-centric transcript systems, emphasizing immutability and transparency as key security properties [7]. Similarly, secure credentialing mechanisms using blockchain have been proposed to address the vulnerability of PDF-based certificates and centralized validation mechanisms [8]. More recently, lightweight permissioned distributed ledger models based on Hyperledger have been examined to improve scalability and reduce computational overhead in HEI credentialing networks [9].

These studies demonstrate that blockchain technology can enhance the issuance and verification of academic credentials. However, the majority of existing work in blockchain-enabled education focuses primarily on certificate authentication and transcript validation. Broader LMS security concerns, particularly those related to assessment workflows, grade modification events, and enterprise audit mechanisms still remain insufficiently addressed.

Blockchain technology, originally introduced through Bitcoin [10], has evolved into a broader class of distributed ledger technologies (DLTs) capable of supporting enterprise applications beyond cryptocurrencies. Surveys such as Zheng et al. [11] and Underwood [12] describe blockchain as a decentralized, append-only ledger secured through cryptographic mechanisms and distributed consensus. The core security properties of blockchain systems which are immutability, transparency, non-repudiation, and distributed fault tolerance make these technologies attractive for environments requiring tamper-resistant record keeping.

In the educational domain, several studies have explored blockchain for lifelong learning passports, credit transfer systems, and credential verification [13,

14]. These works primarily focus on external verification of academic achievements and interoperability across institutions. While they recognize blockchain's capacity to provide immutable certification records, they do not systematically address internal LMS integrity, event logging of assessment modifications, or enterprise-grade threat modeling.

From a business information security standpoint, LMS platforms face several distinct threats:

- Insider threats, where privileged administrators may modify grades without traceability.
- Centralized database compromise, enabling unauthorized alterations of assessment records.
- Opaque audit trails, making forensic investigation difficult in case of disputes.
- Credential forgery, particularly when validation mechanisms rely on downloadable files.

Traditional database logging mechanisms can record changes, but these logs remain alterable by high-privilege actors and do not inherently provide cryptographic immutability. Consequently, trust in LMS systems often depends on institutional authority rather than verifiable technical guarantees.

Permissioned blockchain platforms such as Hyperledger Fabric offer a different trust model. Unlike public blockchains that rely on Proof-of-Work or Proof-of-Stake mechanisms, Hyperledger Fabric is designed for enterprise environments with known participants and identity management through Certification Authorities [15]. Fabric supports modular consensus (e.g., Raft), private channels, and smart contracts (chaincode), making it suitable for institutional networks requiring controlled access, performance efficiency, and regulatory compliance.

This paper builds upon previous credentialing research and extends it toward a broader security extension architecture for Learning Management Systems. Rather than replacing existing LMS platforms, we propose a blockchain-based audit and integrity layer that operates alongside an HEI's Information System. The objective is to introduce cryptographically verifiable event logging for credential issuance and assessment-related transactions, thereby enhancing transparency and mitigating enterprise security risks.

Unlike prior work that focused primarily on credential issuance and validation, this paper explicitly frames blockchain integration as an enterprise risk mitigation strategy for LMS infrastructures. By mapping security objectives such as integrity, non-repudiation, auditability, confidentiality, and availability to specific architectural components of a permissioned blockchain network, we demonstrate how distributed ledger technologies can redefine trust models in digital education.

The remainder of this paper is structured as follows. Section 2 reviews related work in blockchain-enabled education and LMS security. Section 3 defines the threat model for LMS environments. Section 4 discusses the rationale for adopting Hyperledger Fabric. Section 5 presents the proposed architecture. Section 6 describes the proof-of-concept implementation. Section 7 analyzes security

properties and enterprise implications. Finally, Section 8 concludes with future directions toward full institutional deployment and extended evaluation.

2 Background and Related Work

Blockchain technology has evolved significantly from its original application in cryptocurrencies to broader enterprise and institutional use cases. Introduced by Nakamoto in 2008) [10], blockchain established the concept of a distributed, append-only ledger secured by cryptographic hashing and consensus protocols. Subsequent surveys have formalized blockchain's architectural properties and consensus models, highlighting its potential beyond financial systems [11, 12].

Within education, blockchain adoption has primarily focused on credential verification and lifelong learning records. Grech and Camilleri provided one of the earliest European Commission reports examining blockchain in education, emphasizing transparency and credential portability [14]. Chen et al. explored blockchain's potential applications in online education and smart learning environments, arguing that decentralized ledgers could improve trust in digital certification systems [16], while the authors of [17] examined blockchain's role in digital learning credential management, highlighting automation of verification processes and learner ownership of credentials.

A top-down model for secure online studies was introduced in [7] with the use of blockchain to protect education information and support learner-centric eTranscript systems. Afterwards, a blockchain-based credential issuance and validation model was introduced to mitigate vulnerabilities in PDF-based certificate distribution [8]. This work was later extended through a lightweight permissioned distributed ledger architecture using Hyperledger technologies to improve scalability and reduce computational complexity in HEI environments [9].

Despite these advancements, most research regarding blockchain technologies in education remains centered on credential authentication, credit portability, or lifelong learning passports. The broader integration of blockchain as a security extension layer for internal LMS processes, particularly assessment workflows and grade integrity mechanisms, remains underexplored.

Learning Management Systems have become central to higher education operations, handling course materials, submissions, grade calculation, and communication. Studies on online learning systems have long recognized the importance of information security and privacy protection [18–20]. Data privacy in LMSs was discussed in [21] and pointed out that different LMS users (students, faculty members and staff) had diverse and sometimes contradicting opinions about who has access to what data, whether student data is protected by different parties, and how often the data was used for different purposes.

Regading modern and widely adopted LMS platforms such as Moodle, Blackboard, and Canvas, all of them rely on centralized database architectures. While these systems implement role-based access control and logging mechanisms, they remain susceptible to several security risks such as centralized database compromise, insider modification of assessment results, insufficiently protected ap-

plication programming interface (API) endpoints, as well as log tampering by privileged users and limited cross-institution audit interoperability.

Research in the field of educational cybersecurity has increasingly recognized insider threats as a significant concern in digital academic environments [22], where the authors argue that centralized logging mechanisms can record modifications, but they do not inherently prevent alteration of historical records by users with sufficient privileges [4].

From an enterprise risk management perspective, unauthorized grade changes or credential manipulation can have substantial legal and reputational consequences for HEIs. However, literature addressing LMS security tends to focus on network-level attacks, authentication mechanisms, or student privacy compliance (GDPR), rather than cryptographically verifiable immutability of academic records [23, 24].

This gap becomes particularly relevant when LMS platforms are extended with custom modules or in-house developed systems, which are common in STEM-focused institutions and where rapid feature deployment may overshadow security architecture considerations.

While public blockchains such as Ethereum have been widely studied for decentralized applications, enterprise environments often require permissioned models with known participants [25, 26]. Hyperledger Fabric, developed under the Linux Foundation, provides a modular and permissioned blockchain framework tailored for business applications [15].

Unlike Proof-of-Work (PoW) systems, Hyperledger Fabric separates transaction endorsement from ordering, enabling lightweight consensus mechanisms such as Raft. It also incorporates identity management through Certification Authorities, private channels for restricted data visibility, and pluggable smart contract execution (chaincode). These properties make Fabric particularly suitable for institutional networks with predefined trust relationships [27].

Permissioned distributed ledger technologies have already demonstrated effectiveness in healthcare record management [28, 29] and supply chain systems [30, 31]. In the educational domain, however, their application has predominantly remained within credential issuance use cases rather than full LMS integration.

While the author's prior work demonstrated the feasibility for secure issuance and validation transactions within a private HEI network, it did not extend to event-based logging of assessment modifications or enterprise-grade threat modeling for LMS infrastructures, which this paper tends to incorporate. Moreover, existing blockchain-in-education models often remain conceptual or certificate-centric without addressing integration with institutional Information Systems.

Therefore, there is a clear need for a security-driven architecture that extends existing LMS platforms with a permissioned blockchain layer, explicitly designed to enhance assessment integrity, transaction traceability, and enterprise auditability.

This paper addresses that gap through a proof-of-concept Hyperledger Fabric-based extension model, coupled with a formal threat analysis tailored to LMS environments.

3 Threat Model for LMS Environments

Most LMSs systems operate as centralized digital platforms responsible for managing course content, student submissions, grading workflows, and academic documentation. From an information security perspective, LMS platforms handle highly sensitive institutional assets whose integrity and confidentiality are critical to maintaining academic credibility and regulatory compliance.

Traditional LMS architectures rely on centralized database management systems, role-based access control mechanisms, and application-layer logging. While these mechanisms provide operational functionality, they assume trust in privileged actors and in the integrity of system logs. In enterprise contexts, such assumptions may be insufficient.

To justify the introduction of a permissioned blockchain layer, a formal threat model must first identify which assets to protect, what are the possible adversaries and attack surfaces, summarized with attack scenarios.

3.1 Critical Assets in LMS Environments

The most critical asset class consists of assessment records, including assignment grades, examination scores, and continuous assessment components. These records represent academic decisions and directly influence student progression, graduation eligibility, and count toward students' professional opportunities. Unauthorized modification of such records constitutes a direct breach of academic integrity.

Secondly, assessment modification events, which include grade adjustments, late submission approvals, reassessments, and administrative overrides are of note as well. While legitimate grade modifications may occur, their transparency and traceability are very important. In traditional centralized LMS architectures, such changes are typically logged within application-layer or database logs, which remain under the control of privileged system users such as system administrators.

A third asset class involves credential data, including diploma supplements, transcripts, and certificates of completion. These artifacts often exist both in database form, and often also as binary files such as PDF documents. Since such documents are used externally (employment opportunities, accreditation procedures, transfer purposes etc.), their authenticity must be verifiable.

Additional assets include submission metadata, such as timestamps of submission, evaluator identity, and grading timestamps. These elements are particularly important in dispute resolution scenarios. Metadata can also include audit trails.

In centralized systems, all these assets reside within a single administrative trust domain. The concentration of control creates inherent exposure to tampering, accidental modification, or insider misuse.

3.2 Adversary categories

In order to assess the security posture of LMS environments, it is necessary to define realistic adversary categories and their capabilities.

The first and most significant adversary category is the so-called malicious insider, typically a privileged administrator or faculty member with legitimate access to LMS administrative controls. Such users may possess database-level permissions or elevated application privileges. In centralized architectures, these individuals may alter grades or assessment records and potentially modify or delete associated log entries. The insider threat is particularly challenging because it originates from within the institutional trust boundary.

A second adversary category consists of an external attacker exploiting LMS vulnerabilities. Through misconfigured APIs, credential compromise, or unpatched application flaws, an attacker may gain unauthorized access to the LMS server or underlying database. Once access is obtained, database records may be altered or exfiltrated. Traditional logging mechanisms may not provide sufficient guarantees against post-compromise tampering.

A third adversary type is the credential forger, typically external to the institution, who modifies a downloaded certificate or fabricates academic documentation. Since many institutions rely on visual inspection or manual verification procedures, altered files may pass superficial scrutiny unless robust validation mechanisms are implemented.

Finally, there exists a category of integrity-eroding administrative practices. These may not stem from malicious intent but rather from operational inefficiencies, undocumented grade corrections, or retroactive adjustments made without transparent documentation. While not strictly adversarial in nature, such practices degrade trust and increase institutional risk exposure.

These adversary categories demonstrate that LMS security challenges are not limited to network-level attacks but include governance and insider threat dimensions.

3.3 Attack Surfaces

Traditional LMS architectures expose several structural attack surfaces due to their centralized design. The primary attack surface is the centralized database layer, where assessment records and credential data are stored. Any actor with sufficient privileges can modify records directly at the database level. While database systems maintain logs, these logs are mutable and typically reside within the same administrative domain.

The administrative control interface represents another significant attack surface. Elevated privileges allow authorized users to perform modifications that may not require multi-party validation. In many LMS implementations, grade adjustments do not require cryptographic confirmation or distributed approval mechanisms.

The API layer also introduces vulnerabilities. LMS platforms often expose REST APIs for integration with external systems. Improper authentication, token mismanagement, or insufficient rate limiting may allow unauthorized access

Table 1: Summary of LMS Threat Model

Category	Description	Security Risk	Implication
Critical Assets	Grades, assessment events, credentials, submission metadata, and audit logs stored within the LMS infrastructure.	Unauthorized modification, deletion, or falsification of academic records.	Compromised academic integrity and institutional credibility.
Malicious Insider	Privileged administrative or teaching staff member with legitimate system access.	Grade tampering and alteration of audit logs without detection.	Loss of trust and potential legal consequences.
External Attacker	Compromise of LMS server or API endpoints via vulnerabilities or credential theft.	Silent modification of database records or data exfiltration.	Integrity breach at institutional scale.
Credential Forger	External manipulation or fabrication of certificate documents.	Fraudulent validation of altered academic documents.	Reputational damage and administrative overhead.
Centralized Database	Mutable centralized storage of academic records within a single trust domain.	Absence of cryptographic immutability and tamper evidence.	Inability to guarantee historical integrity.
Logging Systems	Application-layer or database logs stored within the same administrative boundary.	Log deletion or rewriting by privileged actors.	Weak forensic and audit capabilities.

or data manipulation. Additionally, server-side logging systems represent a structural weakness. Since logs are usually stored locally within the application server or database infrastructure, they remain vulnerable to deletion or alteration by privileged actors or attackers who compromise the server.

Finally, file-based credential storage mechanisms introduce risks when certificates are generated as downloadable documents without cryptographic anchoring to an immutable record. Modified files may appear legitimate unless verified against a trusted external source.

Collectively, these vulnerabilities stem from a single architectural characteristic which states that all core components operate within a unified trust boundary. As a result, the integrity of assessment and credential records ultimately depends on administrative control rather than cryptographic guarantees. Table 1 gives a summary of the LMS threat model.

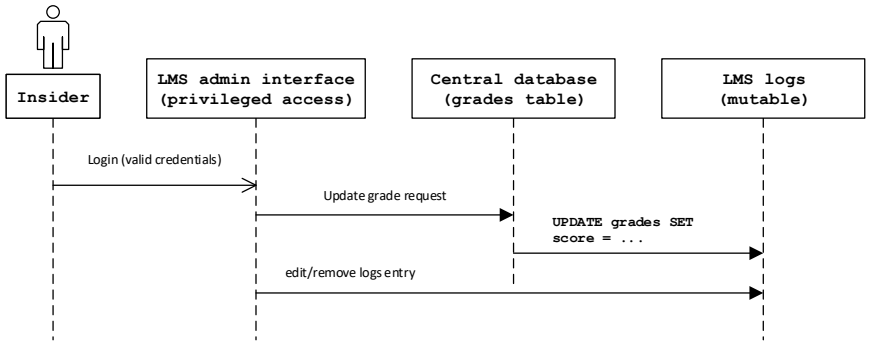


Fig. 1: Sequence diagram for unauthorized grade modification.

3.4 Possible Attack Scenarios

To illustrate the practical implications of the defined threat model, three representative attack scenarios are described below. These scenarios reflect realistic risks observed in centralized LMS environments and directly motivate the architectural decisions proposed in this work.

Unauthorized Grade Modification
In a centralized LMS architecture, a privileged administrator or faculty member may alter a student's grade directly within the system interface or underlying database. While such modifications may sometimes be legitimate (e.g., error correction), the absence of immutable logging mechanisms allows unauthorized changes to occur without verifiable traceability. In extreme cases, associated log entries may be modified or deleted, either intentionally or through administrative oversight, as shown in Fig. 1. The resulting lack of tamper-evident audit trails undermines academic integrity and exposes the institution to legal and reputational risk.

Silent Database Compromise
An external attacker exploiting vulnerabilities in the LMS application layer, authentication mechanisms, or exposed API endpoints may gain unauthorized access to the underlying database. Once access is achieved, assessment records, submission timestamps, or credential data may be altered or deleted, as shown in Fig. 2. Because traditional logging systems reside within the same trust domain as the database, a sophisticated attacker may modify or purge log records to conceal malicious activity. This scenario represents a systemic integrity failure, potentially affecting large volumes of academic data.

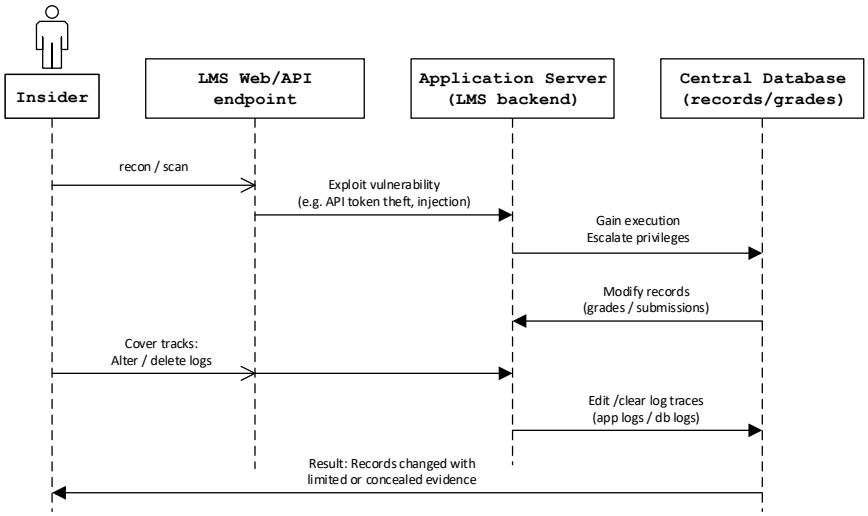


Fig. 2: Sequence diagram for silent database compromise.

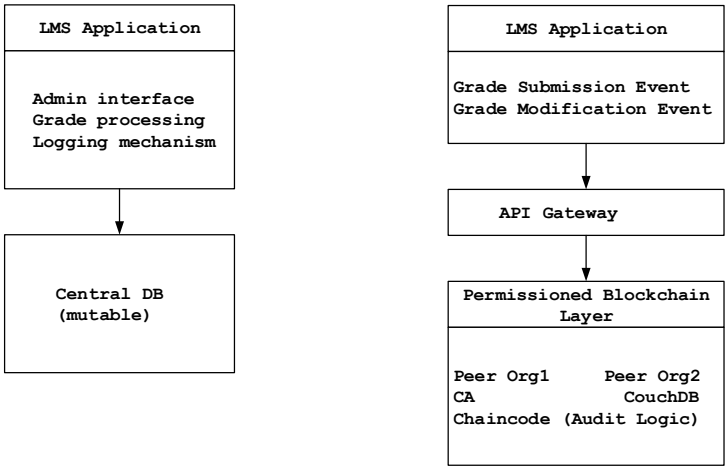
Credential Tampering and Fraudulent Validation
Academic certificates and transcripts are frequently generated as downloadable digital documents. A student or external actor may modify such a document using standard editing tools while preserving visual elements such as logos and signatures. If validation mechanisms rely solely on manual verification or email-based confirmation with the issuing institution, forged documents may evade detection. The lack of cryptographically verifiable anchoring between issued credentials and an immutable record increases the risk of credential fraud and administrative burden for institutions.

Because both the database and logging systems are in the same administrative trust domain, a privileged insider can modify grades and potentially tamper with logs, reducing audit reliability.

3.5 Security Requirements

Based on the identified assets, adversary profiles, and structural vulnerabilities of traditional LMS architectures, a set of core security requirements can be derived to guide the design of a blockchain-enabled extension model, as shown in Fig. 3. The key differences withing the tow models are that the event logging moved outside LMS trust domain, with the blockchain layer acting as an append-only ledger with distributed validation secured with cryptographic signatures.

First, immutability of critical academic events must be ensured, meaning that assessment submissions, grade assignments, and subsequent modifications



(a) Traditional LMS model. (b) LMS with Blockchain Layer.

Fig. 3: Conceptual Security Improvement with Blockchain Layer.

must be recorded in a tamper-evident, append-only manner. Second, the system must provide non-repudiation, such that every recorded action is cryptographically linked to a verified institutional identity, preventing actors from denying their involvement in a transaction. Third, auditability and traceability must be strengthened by maintaining a verifiable chronological record of events that cannot be altered retroactively. Fourth, the architecture must preserve confidentiality, ensuring that sensitive academic data are accessible only to authorized participants, particularly in permissioned institutional networks. Finally, the system must introduce trust separation, meaning that the logging and verification mechanisms operate outside the primary LMS administrative domain, thereby reducing reliance on centralized authority and mitigating insider threats. These requirements collectively motivate the integration of a permissioned blockchain layer as a cryptographic integrity extension rather than a replacement of existing LMS platforms.

The key differences withing the tow models in Fig. 3 are that the event logging moved outside LMS trust domain, with the blockchain layer acting as an append-only ledger with distributed validation secured with cryptographic signatures.

4 Hyperledger Fabric in Enterprise LMS Environments

The threat model defined in Section 3 established several core security requirements for LMS operating in enterprise higher education environments. These included immutable event logging, non-repudiation, tamper-evident auditabil-

ity, confidentiality of academic records, and separation of trust domains. The selection of an appropriate blockchain platform must therefore be driven by these requirements rather than by technological popularity.

Public Ethereum-based blockchains rely on open participation, energy-intensive consensus mechanisms such as PoW, and transparent transaction visibility. Such properties conflict with enterprise requirements for controlled access, regulatory compliance, predictable performance, and data confidentiality.

Unlike public blockchains, Hyperledger Fabric separates transaction execution, endorsement, and ordering phases, enabling flexible consensus configurations and improved performance scalability [32]. This architecture makes it particularly suitable for environments where participant identities are authenticated and controlled.

Firstly, Hyperledger Fabric incorporates a Membership Service Provider (MSP) and Certification Authority (CA) infrastructure that binds transactions to verified institutional identities. Each peer and client application must possess cryptographic credentials issued by a trusted authority. This mechanism supports strong identity assurance and enables non-repudiation of grade submissions and modification events.

Regarding consensus protocols, Hyperledger Fabric supports protocols such as Raft, which provide crash fault tolerance without computationally expensive mining processes [33]. In an HEI network composed of known peer organizations (e.g., multiple faculties or administrative units), Raft consensus ensures distributed agreement while maintaining low latency. This characteristic enables the blockchain layer to function as an audit extension without degrading LMS performance [34].

Fabric also supports chaincode, a smart contract mechanism which allows the implementation of application-specific transaction logic. For LMS integration, chaincode can define structured transaction types such as grade submission and modification events, as well as credential issuance events and validation requests.

This programmable layer allows the blockchain network to enforce schema validation and ensure consistent transaction formatting. By encoding audit logic at the ledger level, integrity verification becomes independent of LMS application-layer controls.

The platform also enables the creation of so-called private channels, restricting data visibility to designated peer organizations. this will enable off-chain storage of sensitive payloadswith only cryptographic hashes recorded on the ledger. This design supports confidentiality while preserving immutability guarantees, which aligns with institutional governance requirements and reduces regulatory exposure such as GDPR.

5 Proposed Blockchain-Enabled LMS Architecture

This Section presents a blockchain-enabled LMS security extension architecture designed for enterprise higher education environments. The proposed approach does not aim to replace existing LMS platforms; instead, it introduces a permissioned blockchain layer that provides tamper-evident auditability and cryptographic integrity for high-value LMS events, primarily those related to assessment and credentialing.

This solution integrates via APIs and event triggers without requiring major modifications to the LMS core. In addition, the system prioritizes immutable logging of assessment and credentialing events over storage of full academic content on-chain. Sensitive academic data should remain within institutional systems whenever possible. For instance, on-chain records should store minimal metadata and cryptographic hashes. Participation is restricted to known institutional entities and organizational units. Finally, this design supports gradual rollout, starting with a proof-of-concept and expanding toward production deployment in future work.

The proposed architecture shown in Fig. 4 adopts a layered model to separate operational LMS workflows from trust and audit mechanisms. At a high level, the LMS/HEI Information System remains the system of record for learning content, while the blockchain network functions as an external integrity and accountability layer.

The operational domain includes the LMS application, database, and existing administrative interfaces. It performs standard functions such as assignment publication, submission collection, and grade management. In the proposed architecture, Layer 0 additionally emits security-relevant events (e.g., grade entry, grade change) to the integration layer.

The gateway serves as the boundary component that transforms LMS events into blockchain transactions. It performs event normalization (consistent data schema) hashing of sensitive payloads, identity binding (signing under institutional credentials), and submission to Fabric via SDK/Gateway APIs. Importantly, this component allows the blockchain layer to remain decoupled from LMS implementation details.

The Fabric network is composed of peers belonging to organizational units (e.g., faculty and/or department), a CA for identity issuance, and an ordering service. Chaincode defines transaction formats and validation logic for LMS audit events. The ledger stores immutable event entries to support forensic traceability and accountability.

5.1 Event-to-Transaction Model

A key architectural decision is to treat LMS security-relevant actions as events, each mapped to a well-defined blockchain transaction type. This approach ensures consistent audit representation regardless of LMS platform differences.

To preserve privacy and reduce ledger bloat, the system stores only minimal metadata on-chain and anchors sensitive content through cryptographic hashes.

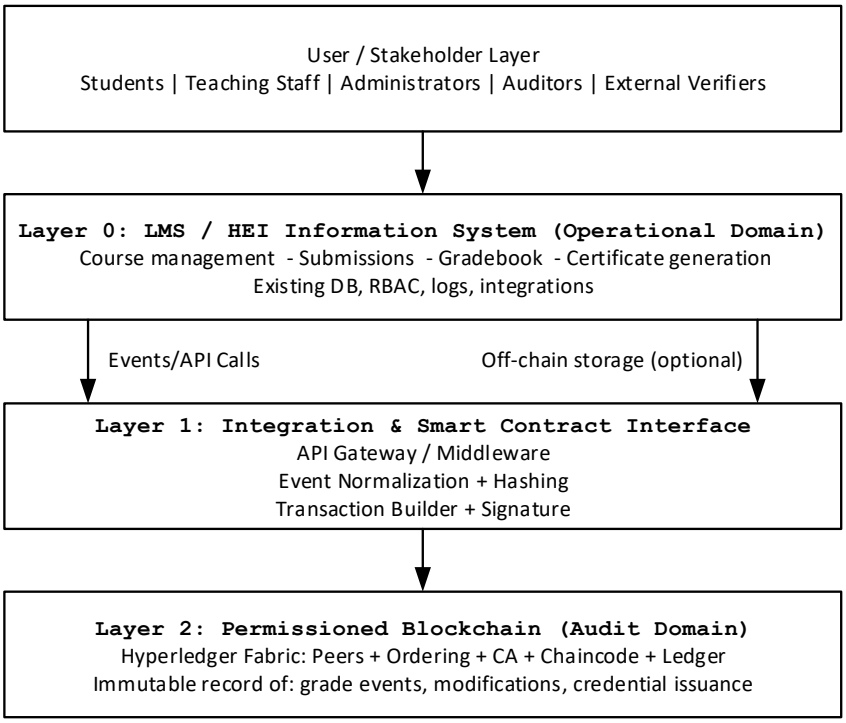


Fig. 4: Layered LMS Architecture.

The proposed model currently supports five transaction types:

- `GradeSubmissionTx`: initial grade entry for an assessment item;
- `GradeModificationTx`: any change to an existing grade record;
- `CredentialIssuanceTx`: issuance of diploma supplement/certificate metadata;
- `CredentialValidationTx`: validation request referencing credential hash;
- `AuditQueryTx` (logical operation): retrieval of historical events (read-only).

At this stage, the implementation focuses on the audit-layer integration and transaction lifecycle rather than full LMS deployment. Events can be generated via a mock LMS connector or a minimal integration stub, demonstrating feasibility of event normalization,hashing and signing, chaincode invocation, and immutable ledger storage. An audit record structure can be implemented as the following snippet.

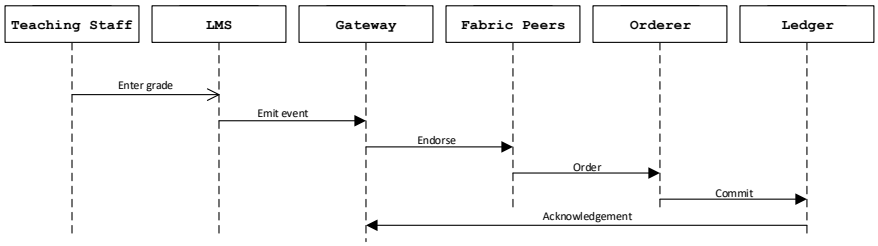


Fig. 5: Grade Submission Sequence.

```
AuditRecord {
  recordId:         string        // unique ID
  eventType:        enum {GRADE_SUBMIT, GRADE_MODIFY, CRED_ISSUE, CRED_VALIDATE}
  studentRef:       string        // pseudonym or student ID (policy-dependent)
  courseRef:        string
  assessmentRef:    string?       // null for credential events
  actorRef:         string        // identity-bound (via Fabric CA/MSP)
  actorRole:        enum {STAFF, ADMIN, SYSTEM}
  timestamp:        int64
  payloadHash:      string        // SHA-256/other hash of off-chain payload
  prevRecordId:     string?       // links modifications to earlier events
  metadata:         map<string,string>
}
```

This structure supports auditability and traceability: modifications link to previous records and cannot overwrite history.

5.2 Workflows

When a grade is entered, the LMS triggers an event containing grade details, as shown in Fig. 5. The gateway builds the transaction, hashes the payload, signs it under an institutional identity, and submits it to Fabric. Fabric commits the record after endorsement and ordering.

For modifications, the gateway can include a previous record ID and a reason code (if available). This ensures every adjustment becomes an immutable append-only record, enabling transparent reconstruction of grade histories.

6 Proof-of-Concept implementation

To evaluate the feasibility of the proposed blockchain-enabled LMS architecture, a controlled proof-of-concept (PoC) deployment was established using a minimal but representative Hyperledger Fabric network configuration within the

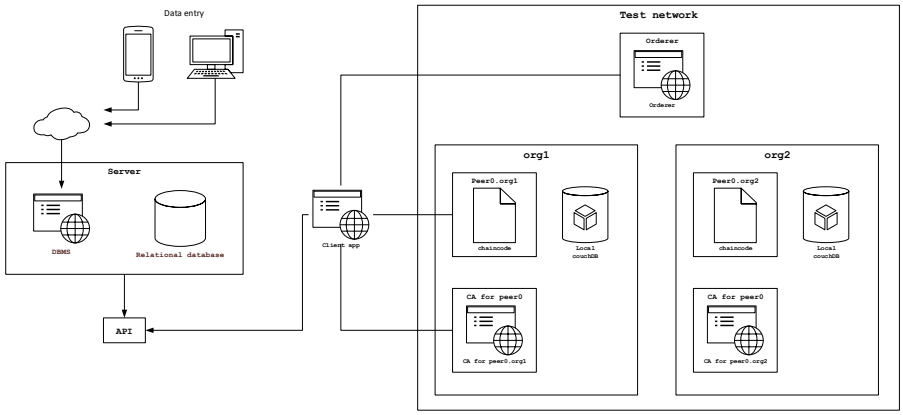


Fig. 6: PoC network topology.

Blockchain Technology Laboratory at Belgrade Metropolitan University. The main goal of the PoC was to demonstrate distributed endorsement, identity-bound transaction recording, and tamper-evident ledger maintenance in an institutional context.

The PoC deployment consists of two logical organizations, denoted as `Org1` and `Org2`, connected through a shared ordering service, as shown in Fig. 6. These organizations may represent distinct faculties, departments, or administrative units within the same HEI. Each organization hosts a Fabric peer node and maintains its own state database. This topology enforces distributed validation of transactions while preserving institutional governance boundaries.

Each organization operates a Fabric peer node, with chaincode execution executing smart contract logic for transaction validation. Furthermore, each node has transaction endorsement for verifying proposed transactions against endorsement policies. Note that the PoC has two storage layers. The first one is the blockchain ledger, which contains the ordered, append-only sequence of committed transactions. This ledger ensures immutability through cryptographic hash chaining. The second one is the world state database, which stores the latest values of ledger key–value pairs in queryable JSON format. For the world state, CouchDB was selected as this database has native support for structured JSON documents, rich query capabilities suitable for audit and reporting scenarios.

Even in the event of world state corruption, the ledger can reconstruct the world state deterministically, reinforcing data integrity guarantees.

The PoC network also incorporates a Hyperledger Fabric CA to manage identities and enforce membership policies. The CA issues X.509 certificates to the two peer nodes, ordering service nodes, client applications (e.g., the LMS integration gateway). By utilizing CA, cryptographic binding of transactions to verified institutional entities and role-based permissions through the MSP are enforced. Unlike public blockchains that rely on pseudonymous addresses, this

Fig. 7: Simulated transaction testing.

permissioned identity model aligns with enterprise governance requirements in HEIs.

The network employs a Raft-based ordering service, providing crash fault tolerance without computationally intensive mining processes. The ordering service collects endorsed transactions from peer nodes, establishes deterministic transaction ordering, packages transactions into blocks, and finally distributes committed blocks to all peers.

Currently, the PoC remains limited in scope and scale. It was deployed in a controlled test network rather than a production LMS environment. LMS integration was simulated via gateway application rather than embedded directly in a live LMS platform, as shown in Fig. 7.

7 Security analysis and enterprise implications

The central architectural contribution of the proposed model is the separation of operational LMS functionality from a distributed audit domain. In traditional LMS deployments, assessment records, administrative controls, and logging systems reside within the same centralized trust boundary. As a result, privileged actors or compromised servers may modify grades and associated logs without generating tamper-evident traces.

The integration of a permissioned blockchain layer fundamentally alters this trust model. By recording grade submission and modification events as append-only ledger transactions, the system ensures that changes cannot overwrite historical records. Instead, modifications generate new entries cryptographically linked to previous events. Because ledger blocks are hash-chained and distributed across multiple peers, retroactive alteration becomes computationally and organizationally infeasible without detection.

Furthermore, Hyperledger Fabric's identity management infrastructure binds each transaction to a cryptographically verifiable institutional identity. This provides non-repudiation: actors cannot deny authorship of submitted or modified records. In contrast to conventional username-based logging, blockchain records include digital signatures validated by a CA, strengthening accountability in academic dispute scenarios.

The distributed endorsement model additionally mitigates insider threats. Transactions require validation according to predefined endorsement policies, reducing reliance on a single administrative authority. Even if the LMS database is compromised, discrepancies between centralized data and the blockchain audit trail become detectable through reconciliation queries.

Confidentiality is preserved by storing only minimal metadata and cryptographic hashes on-chain. Sensitive academic content may remain off-chain within institutional systems, while the ledger provides integrity anchoring. Combined with permissioned network participation and optional private channels, this design aligns with enterprise data protection requirements.

Collectively, these mechanisms address the security requirements defined in Section 3: immutability, tamper-evident auditing, non-repudiation, confidentiality, distributed validation, and trust separation.

Beyond technical security properties, the proposed architecture has meaningful implications for institutional governance and enterprise risk management. Academic record manipulation and credential fraud represent high-impact risks for HEIs, potentially affecting accreditation status, legal liability, and public reputation. By introducing cryptographically verifiable audit trails, the architecture reduces the likelihood of undetected grade tampering and strengthens institutional defensibility in dispute scenarios.

The present evaluation remains architectural and proof-of-concept in nature. The deployment was conducted in a controlled test network rather than within a production LMS environment. Performance benchmarking under high transaction volumes was not performed, and adversarial penetration testing was outside the scope of this study. Additionally, governance policies for multi-institution endorsement were not fully explored.

Nevertheless, the structural properties introduced by the permissioned ledger demonstrably mitigate core integrity weaknesses inherent in centralized LMS systems. The PoC confirms technical feasibility and establishes a foundation for future large-scale deployment, performance evaluation, and formal security verification.

8 Conclusion

The increasing reliance on digital Learning Management Systems in higher education has amplified the importance of ensuring the integrity, transparency, and accountability of academic records. Traditional LMS architectures, while operationally efficient, remain structurally centralized and therefore vulnerable to insider threats, silent database compromise, and mutable audit logs. As digital education becomes foundational to institutional operations, the integrity of assessment and credentialing processes must be reinforced through stronger technical guarantees.

This paper proposed a blockchain-enabled audit extension architecture for LMS environments, designed specifically for enterprise higher education institutions. Rather than replacing existing LMS platforms, the approach introduces a permissioned blockchain layer based on Hyperledger Fabric to provide tamper-evident logging, identity-bound transactions, and distributed validation of critical academic events. The architecture separates operational workflows from the audit domain, thereby mitigating structural weaknesses inherent in centralized trust models.

A proof-of-concept deployment demonstrated the feasibility of recording grade submission and modification events as append-only ledger transactions within a controlled institutional network. The implementation validated immutability, non-repudiation, distributed endorsement, and integrity anchoring of assessment records while preserving data confidentiality through minimal on-chain storage.

From an enterprise perspective, the proposed model strengthens institutional trust, enhances auditability, and reduces the risk exposure associated with academic record manipulation. While the prototype remains limited in scale and does not yet represent a production-level LMS integration, it establishes a practical and extensible foundation for secure, verifiable digital education infrastructures.

Future work will focus on performance evaluation under realistic workloads, deeper LMS integration through standardized APIs, formal security verification, and governance modeling for multi-institution federated networks. Such extensions will enable comprehensive evaluation of scalability, interoperability, and regulatory compliance in large-scale deployments.

By introducing cryptographic trust separation into LMS ecosystems, this work contributes toward redefining how integrity and accountability can be achieved in digital education environments.

Appendix

The Appendix gives exmaple code snippets for a transaction builder, chaincode record creation, and example JSON audit record, respectively.

This pseudocode illustrates the core logic executed by the integration gateway that connects the LMS to the blockchain network.

```
function handleLmsEvent(event):
    canonical = normalize(event)
    payloadHash = HASH(canonical.payload)
    tx = {
        eventType: canonical.type,
        studentRef: canonical.studentRef,
        courseRef: canonical.courseRef,
        assessmentRef: canonical.assessmentRef,
        actorRef: canonical.actorRef,
        actorRole: canonical.actorRole,
        timestamp: canonical.timestamp,
        payloadHash: payloadHash,
        prevRecordId: canonical.prevRecordId,
        metadata: canonical.metadata
    }
    signature = SIGN(tx, gatewayPrivateKey)
    submitToFabric(tx, signature)
```

This chaincode skeleton demonstrates the ledger-level logic for creating a new audit record within the permissioned blockchain. The smart contract first checks whether a record with the same identifier already exists to prevent overwriting, reinforcing the append-only property of the ledger.

```
func (s *SmartContract) CreateAuditRecord(ctx contractapi.TransactionContextInterface,
    recordId string, jsonRecord string) error {

    exists, err := s.RecordExists(ctx, recordId)
    if err != nil { return err }
    if exists { return fmt.Errorf("record %s already exists", recordId) }

    // Optional: validate schema, enforce eventType enum, require payloadHash, etc.
    // Optional: enforce that GradeModificationTx includes prevRecordId.

    return ctx.GetStub().PutState(recordId, []byte(jsonRecord))
}
```

The example JSON object illustrates the structure of a blockchain audit record for a grade modification event. It includes references to the student, course, assessment item, and actor identity, all bound to a precise timestamp.

```
{
  "recordId": "GRD-2026-000183",
  "eventType": "GRADE_MODIFY",
  "studentRef": "STU-92a1f1",
  "courseRef": "CS401",
  "assessmentRef": "A3",
  "actorRef": "msp:org1:staff:ta-014",
  "actorRole": "STAFF",
  "timestamp": 1771286400,
  "payloadHash": "sha256:4d7c...9a2f",
  "prevRecordId": "GRD-2025-000112",
  "metadata": {
    "reason": "manual_correction",
    "policy": "two_person_review_pending"
  }
}
```

Acknowledgment

This paper was supported by the Blockchain Technology Laboratory at Belgrade Metropolitan University, Serbia.

References

1. Dhawan, S.: Online learning: A panacea in the time of covid-19 crisis. Journal of educational technology systems **49**(1), 5–22 (2020)
2. Alturki, U., Aldraiweesh, A.: Application of learning management system (lms) during the covid-19 pandemic: A sustainable acceptance model of the expansion technology approach. Sustainability **13**(19), 10991 (2021)
3. Adedoyin, O.B., Soykan, E.: Covid-19 pandemic and online learning: the challenges and opportunities. Interactive learning environments **31**(2), 863–875 (2023)
4. Alexei, L.A., Alexei, A.: Cyber security threat analysis in higher education institutions as a result of distance learning. International Journal of Scientific and Technology Research (3), 128–133 (2021)
5. Afolalu, O., Tsoeu, M.S.: Cybersecurity in higher education institutions: A systematic review of emerging trends, challenges and solutions. Future Internet **17**(12), 575 (2025)
6. Kepuska, K., Tomasevic, M.: A lightweight framework for cyber risk management in western balkan higher education institutions. PeerJ Computer Science **10**, e1958 (2024)
7. Damnjanović, M., Grković, V., Zdravković, N.: Towards secure online studies: Applying blockchain to e-learning. In: Proceedings of the 11th International Conference on e-Learning, Belgrade, Serbia. pp. 10–12 (2020)
8. Zdravković, N., Jović, J., Damnjanović, M.: Secure credentialing in e-learning using blockchain. In: Proceedings of the 11th International Conference on e-Learning, Belgrade, Serbia. pp. 39–43 (2020)
9. Zdravkovic, N., Dimitrijevic, N., Simjanovic, D.J., Ponnusamy, V.: A lightweight permissioned distributed ledger for credentialing in higher education institutions. In: Proceedings of the 13th International Conference on e-Learning, Belgrade, Serbia. pp. 40–45 (2022)
10. Nakamoto, S.: Bitcoin: A peer-to-peer electronic cash system (2008)
11. Zheng, Z., Xie, S., Dai, H., Chen, X., Wang, H.: An overview of blockchain technology: Architecture, consensus, and future trends. In: 2017 IEEE international congress on big data (BigData congress). pp. 557–564. Ieee (2017)
12. Underwood, S.: Blockchain beyond bitcoin. Communications of the ACM **59**(11), 15–17 (2016)
13. Turkanović, M., Hölbl, M., Košič, K., Heričko, M., Kamišalić, A.: Eductx: A blockchain-based higher education credit platform. IEEE access **6**, 5112–5127 (2018)
14. Grech, A., Camilleri, A.F.: Blockchain in education. Publications Office of the European Union (2017)
15. Androulaki, E., Barger, A., Bortnikov, V., Cachin, C., Christidis, K., De Caro, A., Enyeart, D., Ferris, C., Laventman, G., Manevich, Y., et al.: Hyperledger fabric: a distributed operating system for permissioned blockchains. In: Proceedings of the thirteenth EuroSys conference. pp. 1–15 (2018)
16. Chen, Y., Bellavitis, C.: Blockchain disruption and decentralized finance: The rise of decentralized business models. Journal of Business Venturing Insights **13**, e00151 (2020)
17. Jirgensons, M., Kapenieks, J.: Blockchain and the future of digital learning credential assessment and management. Journal of teacher education for sustainability **20**(1), 145–156 (2018)

18. Alwi, N.H.M., Fan, I.S.: E-learning and information security management. International Journal of Digital Society (IJDS) **1**(2), 148–156 (2010)
19. Chen, Y., He, W.: Security risks and protection in online learning: A survey. International Review of Research in Open and Distributed Learning **14**(5), 108–127 (2013)
20. Sadiqzade, Z., Alisoy, H.: Cybersecurity and online education–risks and solutions. Luminis Applied Science and Engineering **2**(1), 4–12 (2025)
21. Jiang, J.A., Robledo Yamamoto, F., Nagy, V., Zander, M., Barker, L.: Data privacy in learning management systems: perceptions of students, faculty, and administrative staff. In: International Conference on Human-Computer Interaction. pp. 100–115. Springer (2023)
22. Georgiadou, A., Mouzakitis, S., Askounis, D.: Detecting insider threat via a cybersecurity culture framework. Journal of Computer Information Systems **62**(4), 706–716 (2022)
23. Aleksieva-Petrova, A., Chenchev, I., Petrov, M.: Lms data collection, processing and compliance with eu gdpr. In: EDULEARN19 Proceedings. pp. 6494–6501. IATED (2019)
24. Amo, D., Alier, M., García-Peñalvo, F.J., Fonseca, D., Casany, M.J.: Gdpr security and confidentiality compliance in lms'a problem analysis and engineering solution proposal. In: Proceedings of the Seventh International Conference on Technological Ecosystems for Enhancing Multiculturality. pp. 253–259 (2019)
25. Buterin, V., et al.: Ethereum white paper. GitHub repository **1**(22-23), 5–7 (2013)
26. Dannen, C., et al.: Introducing Ethereum and solidity, vol. 1. Springer (2017)
27. Milicevic, V., Jovic, J., Zdravkovic, N.: An overview of hyperledger blockchain technologies and their uses (2021)
28. Azaria, A., Ekblaw, A., Vieira, T., Lippman, A.: Medrec: Using blockchain for medical data access and permission management. In: 2016 2nd international conference on open and big data (OBD). pp. 25–30. IEEE (2016)
29. Grković, V., Jović, J., Zdravković, N., Trajanović, M., Domazet, D., Ponnusamy, V.: Usage of blockchain technology for sensitive data protection-medical records use case. Proc. ICIST **2020**, 216–221 (2020)
30. Saberi, S., Kouhizadeh, M., Sarkis, J., Shen, L.: Blockchain technology and its relationships to sustainable supply chain management. International journal of production research **57**(7), 2117–2135 (2019)
31. Queiroz, M.M., Telles, R., Bonilla, S.H.: Blockchain and supply chain management integration: a systematic review of the literature. Supply chain management: An international journal **25**(2), 241–254 (2020)
32. Nikolić, S., Zdravković, N., Franc, I., Arivazhagan, N.: A comparison on hyperledger consensus mechanism security and their applications. In: Proceedings of the 13th International Conference on Business Information Security (BISEC-2022), Belgrade, Serbia. pp. 34—-41 (2023)
33. Piao, X., Li, M., Meng, F., Song, H.: Latency analysis for raft consensus on hyperledger fabric. In: International Conference on Blockchain and Trustworthy Systems. pp. 165–176. Springer (2022)
34. Battisti, J.H., Batista, V.E., Koslovski, G.P., Pillon, M.A., Miers, C.C., Marques, M.A., Simplício, M., Kreutz, D.: Performance analysis of the raft consensus algorithm on hyperledger fabric and ethereum on cloud. In: 2023 IEEE International Conference on Cloud Computing Technology and Science (CloudCom). pp. 155–160. IEEE (2023)