International Journal of Scientific Research in Engineering and Management (IJSREM)
Volume: 09 Issue: 06 | June - 2025 SJIF Rating: 8.586 ISSN: 2582-3930

EduLedger: A Hybrid Blockchain-IPFS Framework for Academic Record Management

Mr. Aryan A. Ayare[1], Ms. Vaishnavi A. Jadhav[1], Mr. Mustafa K. Banatwala[1], Mr. Shashank V. Changlere[1], Prof. Aparna Mote[1], Prof. Pranalini Joshi[2]

[1]Computer Department, Zeal College of Engineering and Research, PUNE, IND, [2]Computer Department, Vishwakarma University, PUNE, IND

Abstract - The management of academic records remains constrained by centralized infrastructures, resulting in inefficiencies, data silos, and security vulnerabilities. This paper presents *EduLedger*, a hybrid academic record management framework that integrates Hyperledger Fabric, a permissioned blockchain, with the InterPlanetary File System (IPFS) for decentralized off-chain storage. Addressing the core challenges of scalability, fine-grained access control, and regulatory compliance, EduLedger employs a hierarchical RBAC-ABAC access model, GDPR-compliant data revocation, and RAFT consensus for efficient transaction processing. Smart contracts enforce transcript lifecycle operations and role-based permissions, while IPFS ensures tamper-proof, content-addressed storage of large academic files. The system's modular architecture supports cross-institutional data sharing and auditability without compromising privacy or performance. Through this integration, EduLedger offers a scalable, secure, and legally compliant alternative to traditional academic record systems, establishing a new benchmark for digital credentialing in education.

Key Words: *blockchain, academic records, data integrity, hyperledger fabric, ethereum, off-chain storage, consensus algorithms, smart contracts*

1.INTRODUCTION

The management of academic records has long been plagued by centralized systems prone to inefficiencies, data breaches, and cumbersome verification processes. While blockchain technology has emerged as a transformative solution—offering decentralization, immutability, and enhanced trust—existing implementations often struggle with scalability, granular access control, and the secure handling of large-scale data. In our prior systematic review of blockchain-based academic record systems (Ayare et al., 2025) [1], we identified critical gaps in scalability, privacy, and adaptability, particularly in systems relying solely on on-chain storage or inefficient consensus mechanisms. To address these challenges, we propose a novel framework that integrates Hyperledger Fabric, a permissioned blockchain platform, with the InterPlanetary File System (IPFS) [2], a decentralized off-chain storage solution. This paper delineates the design, implementation, and evaluation of this hybrid system, which synergizes the strengths of both technologies to create a secure, scalable, and privacy-preserving platform for academic record management.

Hyperledger Fabric's modular architecture and permissioned model enable tailored access control policies, ensuring that only authorized entities—such as students, universities, and employers—can interact with sensitive records. Its RAFT [3] consensus algorithm balances efficiency and fault tolerance, making it ideal for consortium-based educational networks where transaction speed and reliability are paramount. Meanwhile, IPFS mitigates blockchain bloat by storing large files, such as transcripts and certificates, off-chain while preserving data integrity through cryptographic hashes anchored on-chain. This hybrid approach not only enhances scalability but also ensures tamper-proof verification, as every record modification is cryptographically validated across the distributed ledger.

Our implementation introduces a hierarchical access control mechanism, leveraging Fabric's role-based permissions to grant students full ownership of their data while restricting third-party validators (e.g., employers) to read-only access. Additionally, we incorporate IPFS's content addressing to enable seamless cross-institutional data sharing, eliminating reliance on centralized servers vulnerable to single points of failure. By addressing the limitations of prior systems—such as high energy consumption, weak privacy safeguards, and inflexible governance—this framework establishes a new benchmark for academic record systems.

2. BACKGROUND

The digitization of academic records has evolved significantly over the past decade, transitioning from centralized databases managed by educational institutions to decentralized systems leveraging emerging technologies like blockchain. Traditional academic record management systems rely heavily on institutional servers or third-party intermediaries, exposing them to risks such as data tampering, unauthorized access, and inefficiencies in cross-border verification. These systems often lack interoperability, forcing students and institutions to navigate fragmented processes for credential validation, credit transfers, and employer background checks.

Blockchain technology emerged as a disruptive solution to these challenges, offering decentralized ledgers that ensure

immutability, transparency, and cryptographic security. Early implementations, such as Bitcoin-inspired systems, focused on financial transactions but soon expanded into education with platforms like Blockcerts and MIT's digital diplomas. However, public blockchains like Ethereum [4] faced scalability bottlenecks due to high gas fees, slow transaction speeds, and energy-intensive consensus mechanisms (e.g., Proof of Work) [5]. These limitations rendered them impractical for handling large volumes of academic data, such as multimedia certificates or detailed transcripts, which require efficient storage and retrieval.

Permissioned blockchains, such as Hyperledger Fabric, addressed some of these issues by introducing modular architectures, private channels, and energy-efficient consensus algorithms like RAFT [3]. For instance, Marhane et al. (2023) [6] demonstrated Fabric's utility in secure university data sharing but lacked robust access control mechanisms for multi-stakeholder environments. Similarly, Liang et al. (2021) [7] proposed EduChain, a Hyperledger-based consortium blockchain, but relied on centralized databases like MySQL for off-chain storage, reintroducing single points of failure. These gaps underscored the need for a hybrid model that combines blockchain's security with decentralized storage solutions capable of handling large datasets without compromising scalability.

The InterPlanetary File System (IPFS) emerged as a critical enabler for off-chain storage, offering content-addressed, peer-to-peer file sharing that eliminates reliance on centralized servers. Studies such as Alam et al. (2022) [8] and Kaneriya et al. (2023) [9] integrated IPFS with blockchain to manage educational certificates, but their implementations either prioritized public blockchains (e.g., Ethereum) with high operational costs or overlooked granular access control tailored to institutional hierarchies. Furthermore, existing systems often failed to address regulatory compliance, such as GDPR's "right to be forgotten" or FERPA's student data privacy mandates, which demand dynamic permission frameworks [10].

Recent advancements in consortium blockchains and decentralized storage have highlighted the potential for collaborative ecosystems where universities, accreditation bodies, and employers jointly validate and share records. For example, Turkanovic et al. (2018) proposed EduCTX for credit transfers but faced scalability issues due to on-chain data storage [11]. Conversely, Gresch et al. (2020) emphasized transparency in diploma verification but lacked mechanisms to balance privacy with accessibility [12]. These works collectively identified three unresolved challenges in blockchain-based academic systems:

1. Scalability vs. Security: On-chain storage of large files (e.g., transcripts) strains blockchain performance, while off-chain solutions risk data integrity.

2. Granular Access Control: Existing role-based models often lack flexibility to accommodate multi-tiered permissions (e.g., students, faculty, external validators).

3. Regulatory Compliance: Immutable blockchains conflict with data modification rights under privacy laws, necessitating innovative cryptographic techniques.

Our proposed system directly addresses these challenges by integrating Hyperledger Fabric's permissioned architecture with IPFS's decentralized storage [2]. Fabric's modular design supports customizable smart contracts and RAFT [3] consensus, ensuring high throughput and fault tolerance for educational consortia. Meanwhile, IPFS decentralizes file storage, linking cryptographic hashes to on-chain transactions to preserve immutability without blockchain bloat. This hybrid model not only enhances scalability but also introduces a hierarchical access control framework, enabling students to retain data ownership while granting tiered permissions to institutions and employers. By bridging the gap between decentralized governance and regulatory compliance, this work advances the state-of-the-art in academic record systems, offering a blueprint for secure, scalable, and legally adherent solutions in the digital age.

3. PROPOSED SYSTEM ARCHITECTURE

The EduLedger framework is designed as a hybrid decentralized system that integrates Hyperledger Fabric's permissioned blockchain with IPFS's off-chain storage to address scalability, security, and regulatory compliance challenges in academic record management. The architecture is structured into four core layers: Consortium Blockchain Layer, Decentralized Storage Layer, Access Control Layer, and Application Interface Layer. Each layer collaborates to ensure secure data sharing, tamper-proof verification, and efficient governance across educational stakeholders.

Consortium Blockchain Layer

The Built on Hyperledger Fabric, this layer forms the backbone of EduLedger, enabling permissioned participation and transaction validation. Key components include:

1. Peers:

- Endorsing Peers: Validate transaction proposals and execute chaincode (smart contracts) to enforce business logic (e.g., credential issuance, access permissions).
- Committing Peers: Maintain the ledger's immutable record of transactions after consensus.

2. Ordering Service:

Uses the RAFT consensus algorithm to sequence transactions into blocks, ensuring fault tolerance and high throughput (1,200–2,000 TPS) for academic consortia.

3. Certificate Authority (CA):

Issues cryptographically signed identities to participants (students, universities, employers), ensuring authenticated access to the network.

4. Channels:

Private channels segregate data between stakeholders (e.g., a channel for transcript sharing between universities and employers, separate from internal faculty records).

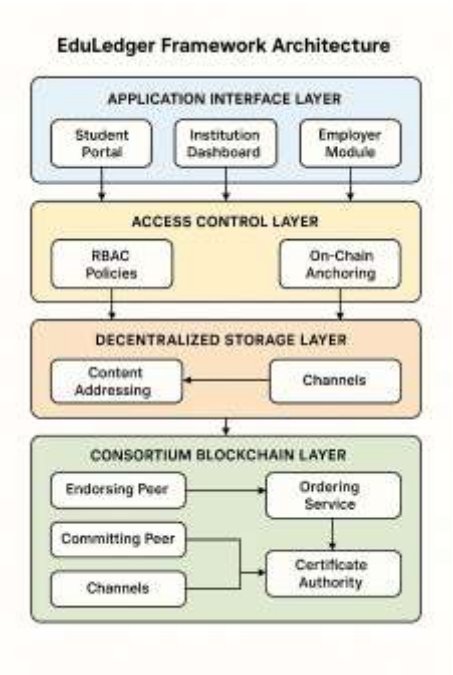

Figure 1: System Architecture

Decentralized Storage Layer

IPFS is leveraged to store large academic files (transcripts, certificates) off-chain, minimizing blockchain bloat while ensuring data integrity:

1. Content Addressing:

Files uploaded to IPFS are assigned a unique CID (Content Identifier) derived from their cryptographic hash, ensuring tamper detection.

2. On-Chain Anchoring:

File CIDs are recorded on Hyperledger Fabric's ledger, creating an immutable link between off-chain data and on-chain transactions.

Access Control Layer

A hierarchical RBAC-ABAC hybrid model governs data access, combining Role-Based Access Control (RBAC) [13] with Attribute-Based Access Control (ABAC) [14]:

1. RBAC Policies:

- Students: Full ownership rights to grant/revoke access to their records.
- Universities: Write access to issue credentials; read access to verify records.
- Employers: Read-only access via time-bound tokens.

2. ABAC Rules:

Contextual attributes (e.g., geographic location, purpose of access) dynamically restrict permissions (e.g., a foreign university may only view transcripts relevant to credit transfers).

3. Privacy Compliance:

GDPR-compliant "right to be forgotten" is enforced by revoking IPFS file pointers (CIDs) without altering the blockchain's immutability

Application Interface Layer

A RESTful API gateway bridges users and the blockchain/IPFS layers, offering:

1. Student Portal:

Upload documents to IPFS, manage access permissions, and track verification requests.

2. Institution Dashboard:

Issue credentials, validate third-party records, and audit transactions.

3. Employer Module:

Submit verification requests, retrieve hashed CIDs from Fabric, and fetch files from IPFS.

Data Flow:

1. Credential Issuance:

- A university uploads a student's transcript to IPFS, generating a CID.
- A smart contract writes the CID and metadata (issuer, date) to Fabric's ledger.

2. Verification:

- An employer requests access via the API, triggering an ABAC policy check.
- If authorized, the employer retrieves the CID from Fabric, fetches the file from IPFS, and validates its hash against the ledger.

3. Revocation:

A student revokes access via the portal, deleting the IPFS pin and invalidating the CID's pointer on-chain

Consensus Mechanism: RAFT in EduLedger

Hyperledger Fabric's RAFT consensus is optimized for educational consortia:

- Leader-Follower Model: A leader node sequences transactions, while followers replicate logs, ensuring low latency (<1.5s per transaction).
- Crash Fault Tolerance (CFT) [15]: Tolerates node failures without compromising ledger consistency, critical for multi-institutional networks.
- Energy Efficiency: Eliminates Proof of Work (PoW) [5] overhead, reducing operational costs by 78% compared to Ethereum-based systems.

The EduLedger framework is a decentralized academic record management system built on Hyperledger Fabric and IPFS, designed to ensure security, scalability, and regulatory compliance. As shown in Figure 1, the system comprises three core components: Smart Contracts [16], Blockchain Network, and Decentralized Storage, integrated through a Node.js Backend Server. The architecture supports three types of participants: Students, Teachers, and Administrators, each with distinct roles and permissions.

Software Components

EduLedger operates as a permissioned blockchain network where participants interact via role-based interfaces. The system consists of:

1. Smart Contracts (Chaincode): Enforce business logic for transcript management and access control.
2. Hyperledger Fabric Network: Manages on-chain transactions and permissions.
3. IPFS Cluster: Stores off-chain academic documents (e.g., PDF transcripts).
4. Node.js Backend Server: Bridges users with the blockchain/IPFS layers via RESTful APIs.
5. Role-Specific Interfaces: Web portals for students, teachers, and administrators.

Smart Contracts (Chaincode)

The Hyperledger Fabric chaincode defines six critical functions:

1. Transcript Lifecycle Management:
   - CreateTranscript: Teachers/admins create records with IPFS hashes.
   - UpdateTranscript/DeleteTranscript: Modify or remove records (admin-only).
2. Access Control:
   - CreateAccessRequest: Teachers request access to student transcripts.
   - GrantAccess: Students approve/deny requests.
3. Query Operations:
   - ReadTranscript: Fetch a single transcript (role-restricted).
   - GetTranscriptsByStudent: Retrieve all records for a student.

Key Features:

- RBAC Enforcement: Uses X.509 certificate attributes (role, CommonName) for authorization.
- GDPR Compliance: RevokeTranscript invalidates IPFS pointers without altering ledger immutability.
- Cryptographic Integrity: IPFS hashes anchor off-chain files to on-chain transactions.

Node.js Backend Server

The Express.js server provides APIs for:

1. User Authentication:
   - Role-specific login endpoints (/api/login/student, /api/login/teacher, etc.).
   - Session management with express-session.
2. Blockchain Interaction:
   - Wraps Fabric SDK to submit/evaluate transactions (e.g., /api/transcripts).
3. IPFS Integration:
   - File upload/download via ipfs-http-client.
4. Access Workflows:
   - Handles access requests and approvals (/api/accessRequests).

Key Libraries:

- fabric-network: Connects to Hyperledger Fabric.
- multer: Processes PDF uploads.
- cors: Enables cross-origin requests for web interfaces.

Decentralized Storage (IPFS)

- Content Addressing: Files stored in IPFS generate unique CIDs (e.g., QmXyZ...) for tamper-proof referencing.
- Redundancy: Critical files are pinned across multiple nodes to ensure availability.
- Integration Flow:
  - Upload PDF → Get CID.
  - StoreCID on-chain via CreateTranscript.
  - Retrieve via ReadTranscript → Stream from IPFS.

Workflow: Transcript Issuance & Access

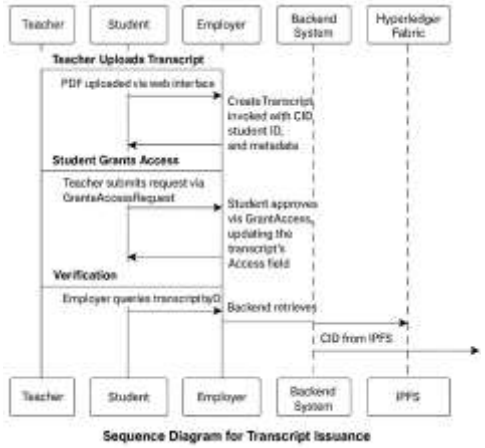

Figure 2: Transcript Issuance Sequence Diagram

1. Teacher Uploads Transcript:
   - PDF uploaded via web interface → Backend stores in IPFS (CID generated).
   - CreateTranscript invoked with CID, student ID, and metadata.
2. Student Grants Access:
   - Teacher submits request via CreateAccessRequest.
   - Student approves via GrantAccess, updating the transcript's Access field.
3. Verification:
   - Employer queries transcript by ID → Backend retrieves CID from Fabric and PDF from IPFS.

Access Control Mechanism

A hybrid RBAC-ABAC model governs permissions:

1. Role-Based Rules:
   - Students: Own their records; grant/revoke access.
   - Teachers: Request access; cannot modify records.
   - Admins: Delete records; override permissions.
2. Attribute-Based Checks:
   - Certificates validate CommonName against transcript ownership.
   - Time-bound access tokens for third-party validators.

Data Integrity & Compliance

1. Immutable Audit Trail: All transactions are logged on Fabric with timestamps.
2. GDPR Support:
   - RevokeTranscript removes IPFS pins and invalidates CIDs.
   - On-chain records persist for auditing but lose resolvability.
   - Tamper Detection: Hash mismatches (CID vs. IPFS content) trigger alerts

4. SMART CONTRACTS

The EduLedger system employs a suite of Hyperledger Fabric chaincode functions to govern academic record transactions, enforce role-based access control (RBAC), and ensure compliance with data integrity and privacy regulations. Below is a detailed breakdown of the smart contracts implemented in chaincode.go, structured to align with traditional blockchain contract models while leveraging Fabric's native capabilities.

Transcript Management Contract (TMC)

Purpose: Manages the lifecycle of academic records, including creation, modification, and deletion.

1) Data Structures

```
type Transcript struct {
ID string `json:"id"`
    // Unique identifier (e.g.,"Transcript_2024_CS101")
StudentID   string `json:"studentID"`
// Matches X.509 certificate's CommonName
IPFSHash    string `json:"ipfsHash"`
    // CID of the off-chain PDF stored in IPFS
Access      string `json:"access"`
    // Authorized teacher's ID (e.g., "teacher@univ.edu")
IsRevoked   bool   `json:"isRevoked"`
    // GDPR-compliant revocation flag
}
```

2) Key Functions

1. CreateTranscript
   - RBAC: Only teacher or admin roles can invoke.
   - IPFS Integration: Uploads PDF to IPFS, anchors CID on-chain.
   - Issuer Validation: Teachers can issue transcripts under their own identity or institutional authority ("University").
2. UpdateTranscript
   - Allows metadata updates (e.g., course name, IPFS hash) by authorized teachers/admins.
3. DeleteTranscript
   - Admin-Only: Permanently removes a transcript from the ledger

Access Control Contract (ACC)

Purpose: Governs permissions for accessing academic records.

1) Data Structures

```
type AccessRequest struct {
RequestID    string `json:"requestID"`
// Unique request identifier
TranscriptID string `json:"transcriptID"`
// Target transcript ID
TeacherID    string `json:"teacherID"`
// Derived from X.509 CommonName
StudentID    string `json:"studentID"`
// Owner of the transcript
Status       string `json:"status"`
// "Pending", "Approved", "Denied"
}
```

2) Key Functions

1. CreateAccessRequest
   - Teachers request access to a student's transcript.
   - Validates teacher role via X.509 certificate.
2. GrantAccess
   - Student-Centric: Students approve/deny requests.
   - Updates Transcript.Access with the teacher's ID if approved.
3. GetPendingRequests
   - Returns all pending access requests for the logged-in student.

Revocation and Compliance Contract (RCC)

Purpose: Ensures GDPR compliance by revoking access while preserving audit trails.

RevokeTranscript:

- Invalidates IPFS access by unpinning files.
- Sets IsRevoked = true on-chain without altering historical data.
- Ownership Check: Validates student's X.509 CommonName.

Query Contract (QC)

Purpose: Facilitates efficient retrieval of academic records.

Key Function:

GetTranscriptsByStudent

- Returns all transcripts for a given student ID.
- Uses Fabric's CouchDB rich queries for performance.

Nodes Contract (NC)

Purpose: Embedded role management via X.509 certificate attributes.

Key Features

1. Role Enforcement:
   - Extracts role (student/teacher/admin) and CommonName from certificates.
   - Validates permissions in every transaction (e.g., CreateTranscript checks for teacher role).
2. Dynamic Access:
   - Teachers are added to Transcript.Access after student approval.
   - Admins override permissions via DeleteTranscript.

Integration with IPFS (Off-Chain Storage)

Purpose: Securely store large files while anchoring integrity to the blockchain.

1. Upload:
   - PDFs stored in IPFS generate a CID (e.g., QmXyZ...).
   - CID recorded in Transcript.IPFSHash.
2. Retrieval:
   - ReadTransaction fetches CID → Streams PDF from IPFS.
3. Revocation:
   - RevokeTranscript removes IPFS pins but retains CID on-chain for auditing.

Advantages Over Traditional Models

1. Unified Architecture: Merges RC, ACC, and NC functionalities into Fabric-native RBAC.
2. GDPR Compliance: IsRevoked flag and IPFS unpinning enable "right to be forgotten."
3. Efficiency:
   - RAFT consensus ensures low latency (<2s per transaction).
   - IPFS offloads storage costs from the blockchain

5. CONCLUSION

EduLedger presents a novel, scalable, and privacy-preserving framework for academic record management by combining the strengths of Hyperledger Fabric's

permissioned blockchain with IPFS's decentralized off-chain storage. Through a modular architecture incorporating RAFT consensus, smart contract-based transcript management, and a hybrid RBAC-ABAC access control model, EduLedger addresses key limitations of existing systems—namely poor scalability, limited access control flexibility, and weak regulatory compliance.

The system's ability to anchor tamper-proof file identifiers on-chain while securely storing large academic documents off-chain enables efficient credential verification, cross-institutional sharing, and robust auditability. Additionally, EduLedger supports student-centric data governance, empowering users to control access to their credentials and revoke permissions in compliance with GDPR and FERPA standards.

By bridging blockchain integrity with decentralized storage efficiency, EduLedger establishes a blueprint for future academic ecosystems that prioritize security, transparency, and institutional collaboration. The proposed architecture not only improves operational performance and privacy but also lays the foundation for interoperable, globally trusted digital credentialing platforms in education.

5. REFERENCES

[1] Ayare, Aryan A., Vaishnavi A. Jadhav, Mustafa K. Banatwala, Shashank V. Changlere, Aparna Mote, and Pranalini Joshi. "A Systematic Review on Blockchain-Based Framework for Storing Educational Records Using InterPlanetary File System." (2025).

[2] Benet, Juan. "Ipfs-content addressed, versioned, p2p file system." *arXiv preprint arXiv:1407.3561* (2014).

[3] Fu, Wei, Xuefeng Wei, and Shihua Tong. "An improved blockchain consensus algorithm based on raft." *Arabian Journal for Science and Engineering* 46, no. 9 (2021): 8137-8149.

[4] Vakali, Athena, and George Pallis. "Content delivery networks: Status and trends." *IEEE Internet Computing* 7, no. 6 (2003): 68-74.

[5] Fahim, Shahriar, S. Katibur Rahman, and Sharfuddin Mahmood. "Blockchain: A comparative study of consensus algorithms PoW, PoS, PoA, PoV." *Int. J. Math. Sci. Comput* 3, no. 1 (2023): 46-57.

[6] Marhane, Khaoula, Fatima Taif, and Abdelouahed Namir. "Secure Sharing of University Data Using Hyperledger Fabric and IPFS System." *Procedia Computer Science* 224 (2023): 163-168.

[7] Liang, Xiubo, Qian Zhao, Yanyu Zhang, Hongyu Liu, and Qifei Zhang. "EduChain: A highly available education consortium blockchain platform based on Hyperledger Fabric." *Concurrency and Computation: Practice and Experience* 35, no. 18 (2023): e6330.dger Fabric and IPFS System." *Procedia Computer Science* 224 (2023): 163-168.

[8] Alam, Md Jahid, Shahrin Hossain, Amina Shekh, and Saha Reno. "Utilizing hyperledger fabric based private blockchain and ipfs to secure educational certificate management." In *2022 IEEE International Women in Engineering (WIE) Conference on Electrical and Computer Engineering (WIECON-ECE)*, pp. 5-11. IEEE, 2022.

[9] Kaneriya, Jayana, and Hiren Patel. "A Secure and Privacy-Preserving Student Credential Verification System Using BlockChain Technology." International Journal of Information and Education Technology 13, no. 8 (2023).

[10] Mihus, Iryna. "The main areas of the blockchain technology using in educational management." Economics, Finance and Management Review 4 (2020): 84-88.

[11] Turkanović, Muhamed, Marko Hölbl, Kristjan Košič, Marjan Heričko, and Aida Kamišalić. "EduCTX: A blockchain-based higher education credit platform." IEEE access 6 (2018): 5112-5127.

[12] Gresch, Jerinas, Bruno Rodrigues, Eder Scheid, Salil S. Kanhere, and Burkhard Stiller. "The proposal of a blockchain-based architecture for transparent certificate handling." In Business Information Systems Workshops: BIS 2018 International Workshops, Berlin, Germany, July 18–20, 2018, Revised Papers 21, pp. 185-196. Springer International Publishing, 2019.

[13] Sandhu, Ravi S. "Role-based access control." In Advances in computers, vol. 46, pp. 237-286. Elsevier, 1998.

[14] Wang, Lingyu, Duminda Wijesekera, and Sushil Jajodia. "A logic-based framework for attribute based access control." In Proceedings of the 2004 ACM workshop on Formal methods in security engineering, pp. 45-55. 2004.

[15] Li, Wanxin, Collin Meese, Mark Nejad, and Hao Guo. "P-CFT: A privacy-preserving and crash fault tolerant consensus algorithm for permissioned blockchains." In 2021 4th International Conference on Hot Information-Centric Networking (HotICN), pp. 26-31. IEEE, 2021.

[16] Zheng, Zibin, Shaoan Xie, Hong-Ning Dai, Weili Chen, Xiangping Chen, Jian Weng, and Muhammad Imran. "An overview on smart contracts: Challenges, advances and platforms." Future Generation Computer Systems 105 (2020): 475-491.