systems

MDPI

*Article*

# A Resilient and Decentralized System Based on Blockchain and Quantum-Secure Communication for Cyber and Strategic Diplomacy

**Bogdan Tiganoaia [1,2,*], Ionut-Petrisor Anghel [1,2], Constantin Bratianu [2] and Doina Banciu [2]**

[1] Faculty of Entrepreneurship, Business Engineering and Management, National University of Science and Technology POLITEHNICA Bucharest, Splaiul Independenței no. 313, Sector 6, 060042 Bucharest, Romania; petrisoranghel2906@gmail.com
[2] Academy of Romanian Scientists, Ilfov 3, 050044 Bucharest, Romania; constantin.bratianu@gmail.com (C.B.); doina.banciu@aosr.ro (D.B.)
* Correspondence: bogdan.tiganoaia@upb.ro

**Abstract**

This paper proposes, implements and tests a resilient and decentralized system based on blockchain and quantum-secure communication for cyber, scientific, and strategic diplomacy. By introducing a dynamic post-quantum cryptographic binding layer, the proposed architecture significantly amplifies organizational resilience against sovereign-state data disruption and harvesting attempts within highly adversarial environments. The system guarantees end-to-end transparency and confidentiality in the sharing of resources, and it can be used in resilient organizations and for cyber, scientific, and strategic diplomacy. It integrates the following technologies and modules: blockchain technology with a semantic distribution of quantum keys, a frontend interface built exclusively with React, a backend module implemented in Python Flask 3.1.2 and served via Gunicorn 25.0.3, and a set of modular components dedicated to blockchain, quantum simulation, and distributed storage. Moving past theoretical bounds, this work presents structural Threat Models, real-world deployment parameters for Eastern European research infrastructures, and multi-variable empirical performance evaluations under authentic institutional workloads. Moreover, the proposed architecture offers an extensible foundation for the development of future resilient ecosystems supported by blockchain and quantum technologies.

**Keywords:** strategic and cyber diplomacy; organizational resilience; knowledge assets; blockchain governance; decentralized architecture; post-quantum cryptography



Academic Editor: Polinpapilinho Katina

Received: 19 May 2026
Revised: 19 June 2026
Accepted: 30 June 2026
Published: 1 July 2026



## 1. Introduction

Digital transformation forces higher education institutions to rethink how they manage, trace, and secure academic knowledge assets [1]. Within the high-stakes arena of contemporary cyber and strategic diplomacy, "knowledge assets" are formally defined as high-value intellectual property, sensitive cross-border research blueprints, and cryptographic identity tokens whose exposure directly undermines national or institutional sovereignty.

Relying on traditional centralized architectures exposes institutional data to severe vulnerabilities, including single points of failure, Man-in-the-Middle (MitM) exploits, and unauthorized data manipulation [1]. This vulnerability is particularly pronounced within collaborative scientific consortia spanning Eastern European academic networks and international statecraft laboratories, where research assets face persistent cyber-espionage

threat vectors. To mitigate these risks, contemporary research is shifting toward a convergence of blockchain networks, decentralized storage filesystems (like IPFS), and advanced cryptographic primitives [2,3]. Merging blockchain's immutable ledger with IPFS's content-addressing logic practically removes the structural dependence on centralized infrastructure [2,3]. To completely secure these client-side boundaries while ensuring cross-platform loading speed, this implementation builds its user environment exclusively using the React compilation stack, eliminating architectural variance [1].

However, the imminent arrival of quantum computing renders conventional cryptographic safety obsolete [4]. This vulnerability requires a transition toward post-quantum resilience, achieved by hybridizing classical key exchanges (such as J-PAKE) with quantum key distribution (QKD) principles, simulated via the BB84 protocols [4–6].

The current literature offers plenty of theoretical blockchain models for academia or isolated cryptographic exercises. However, a major gap persists: how do we integrate and operate these components into a unified, scalable software architecture? Most frameworks remain trapped in mathematical abstractions or sterile lab environments. They simply fail to handle the real-world friction of a complete data pipeline: stretching from user authentication to controlled asset downloading within live cloud environments.

Our core objective is to design, implement, and validate a decentralized academic platform, demonstrating both structural feasibility and practical readiness under authentic institutional workloads. So, this paper delivers three main contributions to the field:

- Hybrid post-quantum authentication: We develop a multi-layered session key protocol that pairs classical J-PAKE with a BB84 emulation via IBM Qiskit, processed through HKDF [4,5,7]. This creates a functional cryptographic barrier capable of resisting early quantum vectors [4];
- Decoupled off-chain/on-chain storage: Large-scale academic files are secured via AES-256-GCM and distributed off-chain via IPFS [3,8]. Concurrently, the blockchain (Polygon Amoy network) acts solely as a trust anchor for metadata, CIDs, and cryptographic timestamps, maximizing throughput while minimizing transaction overhead [8,9];
- Live cloud validation: Moving past simulated environments, we deployed architecture using Firebase Hosting and Render Web Services. This setup proves the stability of our Role-Based Access Control (RBAC) mechanism and the interactive ledger under genuine network constraints.

Ultimately, this study outlines a clear methodological blueprint for secure digital governance in higher education, expanding the boundaries of applied Web3 architectures [1].

The structure of the paper is as follows: the first chapter presents the introduction and the related work. The second chapter highlights the literature review. The next chapters discuss solution implementation, access control, and role separation; hybrid authentication workflow; file upload, registration, and storage workflow; academic ledger and data exploration functionalities; verification and file retrieval workflow; interface-level security transparency and cloud deployment; experimental evaluation and performance metrics; technical limitations; and conclusions and future work.

## 2. Literature Review

Today, technologies such as blockchain and quantum computing simulations and concepts such as scientific diplomacy, strategic diplomacy, and cyber diplomacy are increasingly being used. The integration of decentralized frameworks within strategic organizational management has become a critical prerequisite for achieving long-term systemic resilience. Recent advancements demonstrate that combining distributed consensus mechanisms with decentralized storage paradigms successfully removes single points of vulnerability, allowing for distributed organizations to securely transmit high-value

materials without relying on a central authority [2,3]. In the domain of data preservation, contemporary architectures utilize off-chain file orchestration bound to on-chain execution smart contracts, proving that decoupling heavy storage payloads from metadata proofs ensures horizontal scalability and transactional immutability [8,9].

However, the vulnerability of conventional asymmetric infrastructure to quantum acceleration threats has necessitated an immediate pivot toward post-quantum defensive boundaries. The state of the art presented in the literature emphasizes that traditional digital signatures and public-key handshakes are fundamentally exposed to harvesting attack vectors, where adversarial actors capture encrypted diplomatic communication flows with the intent of executing retro-active decryption via Shor's or Grover's algorithms [4]. To counter this paradigm shift, modern cryptographic protocols increasingly fuse interactive, classical password-authenticated key agreements with physical or emulated quantum key distribution (QKD) layers, establishing multi-domain, in-depth defense frameworks that protect session initialization states [5,6].

Furthermore, practical implementation attempts within institutional web platforms frequently face architectural instability due to poorly defined client environments. To eliminate compilation variance, eliminate centralized UI structural bugs, and secure client-side boundary processing, recent industrial implementations isolate the user interface by leveraging optimized React compiler stacks linked via secure asynchronous pipelines to Python-based backend coordination layers [1]. By reviewing the current implementation landscapes across European research corridors, it is established that anchoring metadata verification directly onto cost-effective public ledgers presents a computationally viable and scalable solution for tracking the lifecycles of strategic knowledge assets [8,9].

The following section presents some other new contributions to these issues:

(a) Hybrid algorithms, including quantum technologies, have been developed for more problems; for example, Ref. [10] proposes and implements a hybrid quantum ant colony algorithm for the ship lock arrangement problem. The paper proposes the concept of the arrangement problem of the ship lock and its constraints and designs a hybrid quantum ant colony algorithm for the arrangement problem of the ship lock;
(b) Ref. [11] shows a solution based on blockchain and Non-Fungible Tokens, which can be tracked on the secondary market and easily regulated using smart contracts. Non-Fungible Tokens are unique, transparent, and cannot be duplicated or fraudulently reproduced;
(c) Ref. [12] proposes a novel approach, the Blockchain-based Deep Belief Network (BDBN), which leverages blockchain's decentralization, transparency, and security to ensure data integrity and trust during transmission;
(d) The use of blockchain is a reality in more systems today. Ref. [13] proposes an Internet of Things Access Control Identity Authentication Method based on blockchain;
(e) As noted in Ref. [14], cybersecurity is an interdisciplinary domain that integrates core principles from mathematics, physics, and computer science with the practical and human elements of electronics, sociology, and management. Cybersecurity remains a shared challenge for government, academia, and the private sector. While their collective resources are essential for building resilient systems, achieving this synergy requires overcoming obstacles related to information sharing, collaborative research, talent development, and the alignment of regulatory standards (based on Ref. [14]).

## 3. Solution Implementation, Access Control and Role Separation

While the preliminary research phase focused on architectural definition and data flow modeling (see Ref. [15] for more details), this paper details the operationalization and empirical validation of the proposed platform. The implementation demonstrates

not only the theoretical feasibility of architecture but also its efficacy within a real-world academic ecosystem, integrating critical processes such as identity management, immutable storage, and data traceability [1]. The system was developed using a decoupled architecture, optimized for scalability and security:

- **Frontend**—Built exclusively with React, this employs responsive web design principles to ensure seamless cross-platform interoperability and remove any structural frontend ambiguity;
- **Backend**—Developed in Python via Flask and orchestrated through Gunicorn, this serves as the central hub for cryptographic processing and mediates interactions with the decentralized infrastructure;
- **Blockchain**—Here, the business logic interacts directly with the IPFS network for data persistence and a smart contract deployed on the Polygon Amoy network, providing an immutable ledger for metadata [3,9].

The system's efficiency stems from the integration of three core pillars that distinguish this solution from conventional approaches:

- **Hybrid post-quantum authentication protocol:** Session security is anchored by fusing the J-PAKE (Password-Authenticated Key Exchange) protocol with a simulated Quantum Key Distribution (QKD) based on the BB84 protocol (implemented via IBM Qiskit) [5,7]. The resulting entropy is processed through HKDF (HMAC-based extract and expand key derivation function) to generate session keys resilient against both classical and emerging quantum threats [4];
- **Decentralized data lifecycle:** File management follows a rigorous pipeline, from client/server-side encryption and fragmentation to IPFS ingestion [3]. Uniqueness and integrity are enforced via Content Identifiers (CIDs), effectively neutralizing the risks inherent in centralized storage [2,3,8];
- **On-chain traceability plain:** The blockchain serves as a root of trust [9]. By recording essential metadata (CIDs, MIME types, and timestamps) directly on the Polygon network, the system guarantees non-repudiation and the full auditability of academic resources [2,3,8,9].

To formally validate the system's claims regarding end-to-end transparency and confidentiality within highly adversarial environments, a systematic Threat Model and Security Boundary Analysis were formulated. The architecture isolates and mitigates malicious vectors across five distinct structural attack vectors:

1. Man-in-the-Middle (MitM) infiltration: Interception attempts along public communication links are neutralized by the hybrid session key generated through HKDF, which dynamically binds classical J-PAKE credentials [5] with simulated high-entropy Qiskit bitstrings [7], ensuring perfect forward secrecy;
2. IPFS sybil subversion and rogue nodes: If an adversary operates or subverts data-hosting nodes within the distributed IPFS filesystem [3], absolute confidentiality is maintained through localized client-side authenticated AES-256-GCM encryption. The network stores only cryptographically opaque data blobs that are undecodable without possessing valid session states.
3. API exploitation and smart contract privilege escalation: Direct attacks attempting to falsify transaction states are blocked by securely shielding the private transaction signing keys inside backend configuration variables. The React client interface [1] can never access raw transaction signing authority; all contract calls are rigidly verified by the stateless backend coordinator;
4. Brute-force and dictionary handshake probing: Offline dictionary attacks targeting authorization channels are fundamentally neutralized by the zero-knowledge proper-

ties of the interactive J-PAKE execution scheme [5], requiring complete verification of password ownership without exposing the underlying secret;

5. Quantum harvesting and retroactive cryptanalysis: Early quantum computing decryption risks are mitigated by injecting high-entropy quantum simulation vectors [4,7] directly into the cryptographic key generation pipeline, establishing a layered shield that conventional public-key environments cannot provide.

The system implements a RBAC model (Role-Based Access Control) where privilege segmentation acts as more than just a logical barrier—it forms the foundation of a shared responsibility model for digital asset management [1]. Access is governed by two distinct entities:

- *The teacher role* grants exclusive write privileges, including the authority to initiate the publication pipeline: data encryption, fragmentation, IPFS persistence, and the execution of blockchain transactions to anchor metadata [3,8];
- *The student role* acts as a resource consumer with rights to query the academic ledger, verify integrity via the CID mechanism, and perform controlled file downloads [1,3]. This entity is strictly prohibited from any operation that would alter the state of the decentralized ledger or shared storage.

To prevent privilege escalation, restrictions are enforced across multiple abstraction layers. At the UI level, the interface dynamically renders components based on the authenticated user's profile [1]. At the business logic level, every API request undergoes rigorous validation with authorization mediated by secure session tokens that encapsulate the user's role, preventing unauthorized access to critical endpoints (e.g., blockchain anchor points) [1].

The result is a cohesive infrastructure that spans the entire workflow from user authentication to verifiable content retrieval, confirming that these mechanisms are ready for integration into secure, collaborative academic environments.

## 4. Hybrid Authentication Workflow

The authentication process is the architectural cornerstone, integrating a multi-layered mechanism that harmonizes classical protocols with post-quantum primitives [4]. Beyond intrinsic security, the system promotes operational transparency by exposing cryptographic workflows to the end-user in an intelligible manner [1,4]. As illustrated in Figure 1, once initial credentials are validated, the system orchestrates a sequence of critical operations visualized in real-time through the UI:

- J-PAKE key exchange establishes a shared secret session key over an insecure channel, providing robust resistance against dictionary attacks [5];
- BB84 quantum simulation generates entropy using the BB84 algorithm via the IBM Qiskit module, enhancing security through simulated quantum key distribution (QKD) [6,7];
- Hybrid derivation (HKDF) aggregates cryptographic material from both sources to derive a hardened session key [4];
- Session token generation finalizes the process by generating an authentication token that governs all subsequent interactions with the platform [1].

This dual-layered approach (both functional and demonstrative) offers significant strategic advantages. Specifically, it provides real-time auditability by exposing intermediate cryptographic states (J-PAKE, BB84/Qiskit, HKDF, and session key previews). Furthermore, it validates the theoretical-to-practical correlation by allowing researchers to observe the transformation of abstract mathematical key agreement concepts into active, operational system functionalities [1,4,5,7].

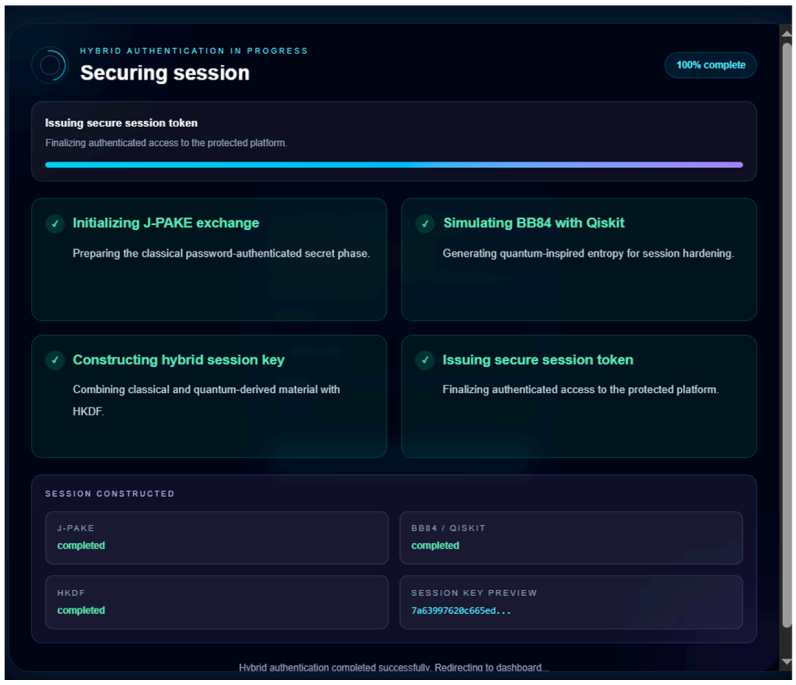


**Figure 1.** Visualization of the hybrid authentication process and session key construction.

## 5. File Upload, Registration and Storage Workflow

Once a secure session is established, the dashboard serves as the central orchestration hub for the system's resources. It provides the user with a holistic view of the current operational state, including active role assignment (defined RBAC policies), session integrity, and module operational parameters from the blockchain and IPFS components, as illustrated in Figure 2.

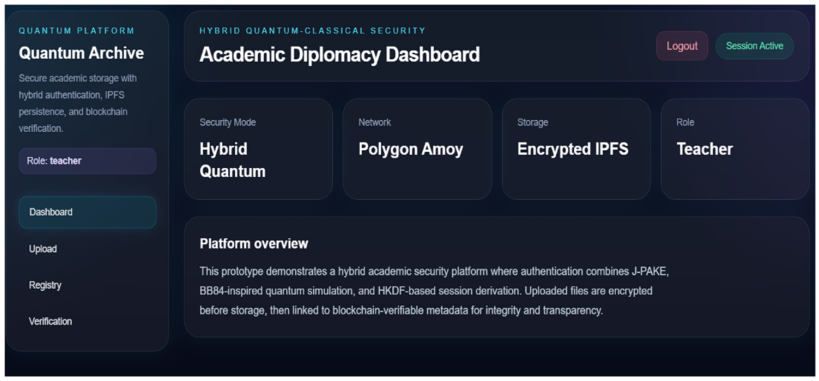


**Figure 2.** Monitoring page for data flow compliance with the proposed architecture.

The ingestion process for academic resources follows a multi-stage security pipeline designed to ensure data confidentiality and integrity prior to its distribution across the decentralized network:

- **Authenticated encryption with associated data (AEAD):** To guarantee both file-level confidentiality and authenticity, the system utilizes the AES-256 algorithm in GCM (Galois Counter Mode) [1]. This selection is predicated on the requirement for high-security encryption that simultaneously provides integrity verification via a Message Authentication Code (MAC);
- **Nonce management and key derivation:** A unique nonce is generated for every file to mitigate replay attacks. The specific encryption key is produced from the hybrid

session key using a secondary derivation function, effectively ensuring cryptographic isolation between distinct sessions and individual files [2,3,8];

- **IPFS persistence:** The resulting object (blob) comprising the concatenated nonce and ciphertext is propagated through the IPFS network [3]. Identification is handled via a Content Identifier (CID), which facilitates content-addressing and ensures immutability at the storage layer [3].

A key scientific contribution of this system is its functional decoupling strategy, which separates high-volume content (stored off-chain) from proofs of existence (stored on-chain), as follows:

- **Smart contract registration**—Metadata, the CID, integrity-based digital fingerprints (hashes) and temporal indicators are encapsulated within a cryptographically signed transaction and broadcast to the Polygon network [2,3,8];
- **Transactional confirmation**—The interface exposes real-time on-chain execution parameters: the transaction hash, block index, and gas consumption—providing the user with mathematical proof of data persistence.

Figure 3 captures the complete file upload workflow and the resulting output of the IPFS storage and blockchain registration processes. While the upper section displays the file selection stage and associated metadata, the lower section presents the final operational results: the generated CID, transaction hash, timestamp, block height, cost parameters, and event confirmation emitted by the smart contract.

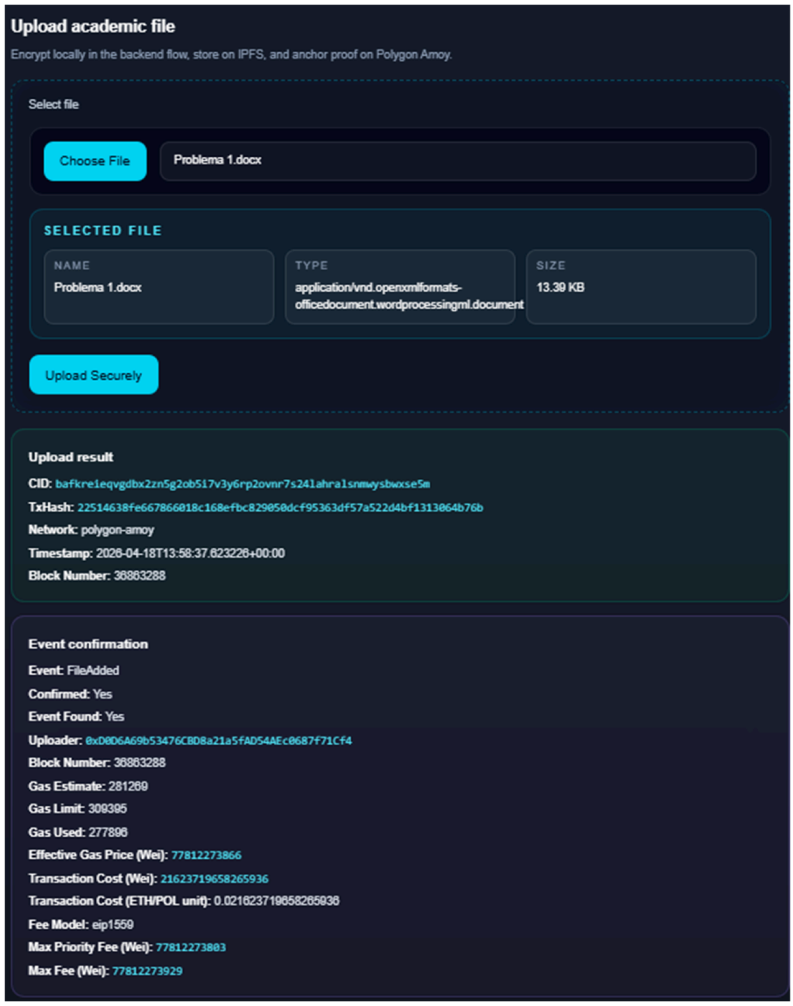


**Figure 3.** File upload workflow and decentralized registration confirmation.

This hybrid architecture demonstrates a robust methodology for managing academic resources, achieving an optimal equilibrium between scalability via IPFS [3], security via AES-GCM encryption [1], and public auditability via blockchain [9]. Consequently, the system ensures that no resource can be altered or deleted without leaving a permanent trace on the distributed ledger, thereby solidifying the integrity of the digital learning ecosystem.

## 6. Academic Ledger and Data Exploration Functionalities

Beyond the layers of security and persistence, the platform integrates a Knowledge Management module, realized through a unified academic ledger. This component acts as a mediation interface between the user and the distributed ledger, transforming on-chain data and IPFS-stored objects into a structured informational ecosystem [3].

As illustrated in Figure 4, the ledger is designed as an interactive data infrastructure, optimized for the auditing and administration of academic assets. The module's architecture was engineered to support institutional adoption by offering advanced information processing tools:

- **Multidimensional querying:** The system enables dynamic filtering, sorting, and grouping of digital assets based on content type, anchoring network, timestamps, and validation status;
- **Interoperability:** To optimize the workflow between modules, the ledger includes mechanisms for the rapid retrieval of Decentralized Identifiers (CIDs). This functionality facilitates a fluid transition to the integrity verification module detailed in Section 7;
- **Ledger transparency:** Both teachers and students benefit from a transparent view of the entire publication history. This visibility reinforces the accountability model promoted by the platform [1].

From a research perspective, this component demonstrates that decentralized storage mechanisms can be successfully integrated into a cohesive resource management tool. Within the context of academic digital transformation, the existence of a ledger that marries the immutability of blockchain with an efficient exploration interface is essential. Consequently, the system transcends the role of a simple file repository, evolving into a content management platform that upholds public auditability and the accessibility of verified resources [1].

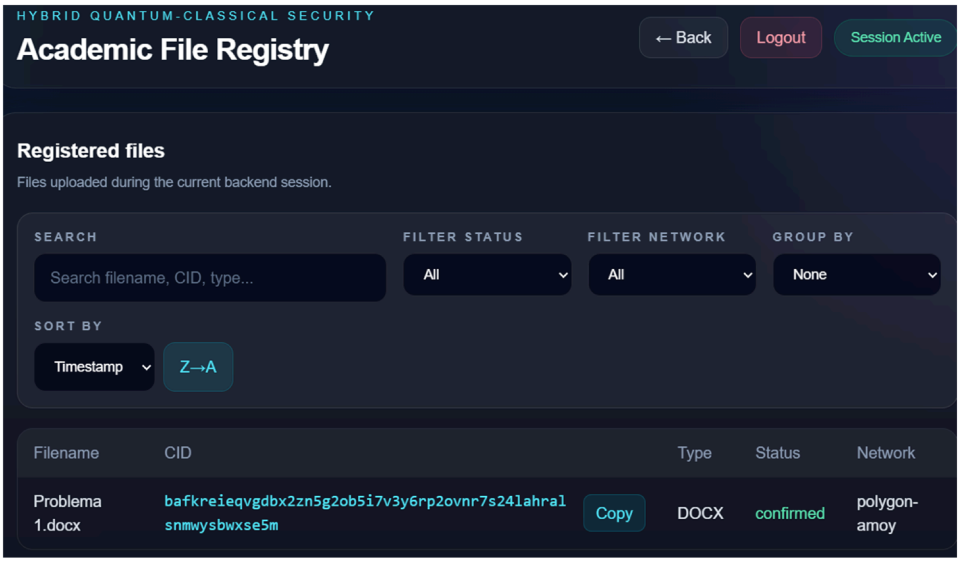


**Figure 4.** Academic ledger and content administration functionalities.

## 7. Verification and File Retrieval Workflow

The lifecycle of digital assets within the platform culminates in the controlled verification and retrieval module. This component operationalizes the concepts of decentralized auditability, empowering users to validate the authenticity of a resource before any direct interaction with the data occurs.

The mechanism for the rapid retrieval of identifiers originating from the academic ledger discussed in the previous section enables direct blockchain querying to confirm both the provenance and integrity of files. The verification process adheres to a rigorous on-chain query flow [2]:

- **Smart contract interrogation:** Utilizing the provided CID, the backend accesses the smart contract's state to extract the associated metadata directly from the blockchain network;
- **Validation:** The system confirms the resource's existence and exposes its primary audit attributes: the source network, file MIME type, digital wallet address of the uploader, timestamp, and integrity hash, as illustrated in Figure 5.

An essential contribution to the platform's architectural completeness is its controlled download functionality. This represents more than a simple data transfer; it is a rigorous process of reconstituting original information from an untrusted storage environment:

- **IPFS retrieval**—Upon successful validation of on-chain metadata, the system locates and retrieves the encrypted blob from the IPFS network using the corresponding CID [8];
- **Content decryption**—The backend utilizes the cryptographic key associated with the authorized session to decrypt the payload (reversing the AES-GCM process). This restores the integrity of both the original file and its system metadata (e.g., original filename).

The integration of this mechanism demonstrates that the CID transcends its role as a simple index, acting as an active element in the academic ecosystem's chain of trust. The direct correlation between on-chain metadata auditability and access to verified content provides a robust defense against data manipulation and Man-in-the-Middle (MitM) attacks. Consequently, the platform confirms that educational resources can be archived, verified, and reused in a decentralized framework while maintaining high standards of confidentiality and institutional governance [1,3,8,9].

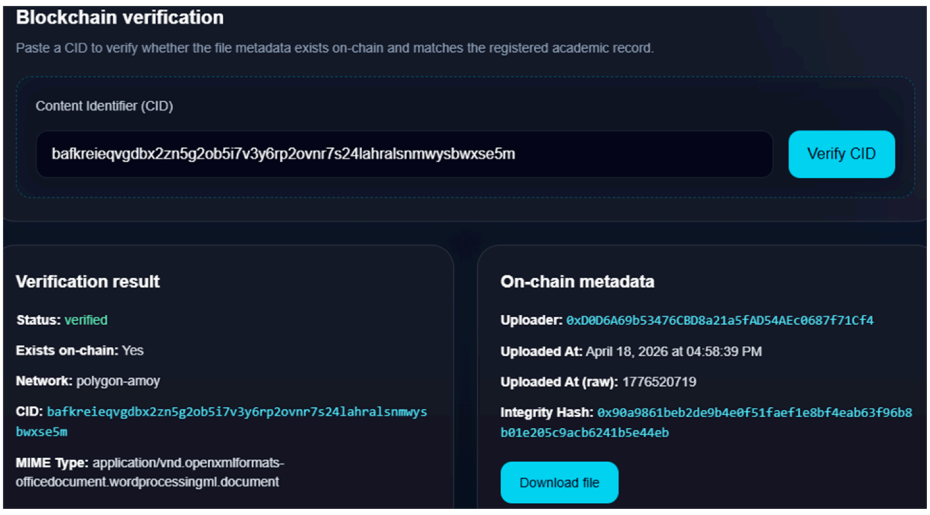


**Figure 5.** CID-based verification page and validated content retrieval.

## 8. Interface-Level Security Transparency and Cloud Deployment

To evaluate system performance and resilience beyond the confines of a local development environment, the architecture was transitioned to a hybrid cloud infrastructure. This methodological step confirms the platform's viability as a distributed system capable of operating under real-world network conditions while adhering to industry security standards. The platform's availability is ensured through specialized hosting services optimized for each specific layer:

- **Frontend layer:** The React interface is delivered via Firebase Hosting [16]. This solution was selected for its efficiency in managing Single-Page Applications (SPAs) and its global Content Delivery Network (CDN), which minimizes latency and ensures secure delivery via HTTPS;
- **Backend layer:** The Flask service, orchestrated by Gunicorn, was operationalized as a Render Web Service [11–17]. Deployment is automated through a Continuous Integration (CI) pipeline linked to a private Git repository, ensuring a controlled and auditable update process.

A critical aspect of the transition to production was the implementation of a rigorous secrets management strategy:

- **Isolation of sensitive data**—All configuration keys, master secrets, and digital wallet credentials are managed exclusively through server-side environment variables to eliminate the risk of source-code leaks [18];
- **Architectural decoupling**—Physical and logical separation between the frontend and backend hosting environments upholds the principle of in-depth defense. Critical logic and blockchain interactions remain shielded behind a secure API, inaccessible directly from the UI.

The platform's capability to orchestrate complex interactions between IPFS, Polygon Amoy, and a secured backend within a public cloud environment confirms that these hybrid security mechanisms (both classical and quantum primitives) are scalable and ready for integration into real-world academic ecosystems.

## 9. Experimental Evaluation and Performance Metrics

We evaluated the framework's operational readiness, computational speed, and scaling limits directly within a live production environment. The frontend architecture, built using React, was globally accessible via Firebase Hosting. Render Web Services managed the cryptographic backend using a Gunicorn server infrastructure. For ledger states, the system committed transactions directly to the Polygon Amoy test network, routing decentralized storage operations across public IPFS gateways.

### *9.1. Evaluation Setup and Methodology*

We tested the platform's architectural viability and functional readiness directly inside the live production deployment. Firebase Hosting [16] handled the deployment of our React frontend [8], while the cryptographic backend operated over a Gunicorn server hosted on Render Web Services [17]. For decentralized state verification, the system committed smart contracts to the Polygon Amoy test network [4] and routed distributed files through public IPFS nodes [2].

To replicate authentic institutional workloads within the Eastern European academic environment, we ran these benchmarks from a standard client terminal equipped with an 8-core 2.60 GHz CPU and 16 GB of RAM, operating over a typical 100 Mbp network connection. Our evaluation focused on tracking performance across two core operational workflows:

- **The post-quantum hybrid handshake:** Here, we measured the specific latency footprint introduced by running a classical Password-Authenticated Key Exchange (J-PAKE) alongside an emulated Quantum Key Distribution (QKD) routine via IBM Qiskit BB84, using HKDF for the final key derivation;
- **The off-chain/on-chain storage split:** This benchmark isolated how processing time is distributed between client-side symmetric encryption (AES-256-GCM), turned the file ingestion timeline into IPFS clusters, and revealed the final state anchoring via Polygon smart contracts.

### *9.2. Computational Overhead of the Hybrid Authentication Layer*

A primary innovation of this platform is the dynamic post-quantum cryptographic binding layer that seals user sessions. The latency contribution of this hybrid handshake was evaluated over 50 continuous operational iterations to isolate its computational footprint. Table 1 breaks down the precise average timing requirements recorded during the empirical evaluation.

**Table 1.** Cryptographic latency breakdown of the hybrid authentication interface.

| Cryptographic Sub-Layer Module | Arithmetic Mean Latency (s) | Standard Deviation (s) | Relative Overhead (%) |
|---|---|---|---|
| Classical J-PAKE Handshake Phase | 0.24 | ±0.021 | 35.3 |
| IBM Qiskit BB84 QKD Simulation Layer | 0.42 | ±0.034 | 61.8 |
| HKDF Extraction and Session Token Genesis | 0.02 | ±0.003 | 2.9 |
| Total Framework Authentication Handshake | 0.68 | ±0.041 | 100 |

The benchmarks indicate that the complete hybrid handshake requires an average of 0.68 s to execute. Although the simulated quantum key distribution mechanism generates the primary temporal penalty accounting for 61.8% of the latency, the aggregate processing time remains safely below the critical one-second boundary. This performance curve proves that embedding early post-quantum security layers maintains operational fluidity, causing no observable user-level friction within authentic institutional data streams. Figure 6 maps these specific timing intervals, illustrating the sequential execution of our defense-in-depth computations.

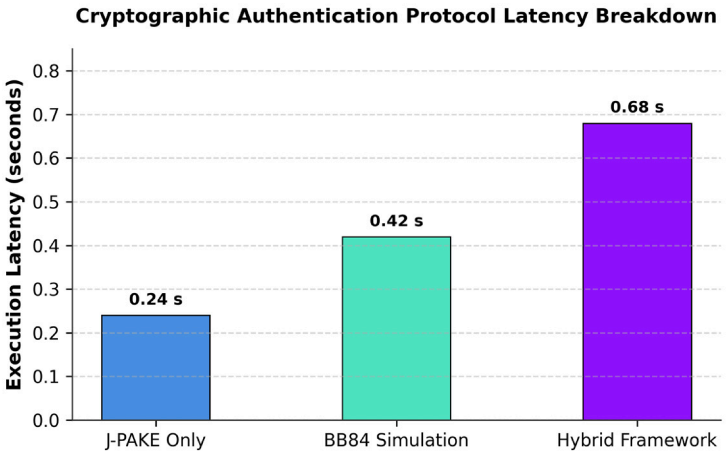


**Figure 6.** Cryptographic authentication protocol latency breakdown across separate sub-layer processing components.

### *9.3. On-Chain vs. Off-Chain Scalability Analysis*

The architecture operates on a strategic decoupling principle: it protects public ledger throughput by shifting large digital assets off-chain (IPFS) and limiting on-chain operations to metadata proofs like CID, MIME profiles, and authorization fingerprints [3,4]. We verified this mechanism under shifting operational loads by subjecting the ingestion pipeline to five incremental file size payloads reflecting typical academic and institutional datasets: 1 MB, 5 MB, 10 MB, 20 MB, and 50 MB.

Our tracking focused on the precise timeline of three separate execution layers: localized chunk encryption via AES-256-GCM, decentralized payload delivery over IPFS, and transaction mining on the Polygon Amoy network. The empirical outcomes of these stress tests are compiled in Table 2.

**Table 2.** Cumulative processing latency scaling across variable digital asset payloads.

| File Payload Size (MB) | AES-256-GCM Encryption (s) | IPFS Off-Chain Upload (s) | Polygon On-Chain Anchorings (s) | Cumulative E2E Latency (s) |
|---|---|---|---|---|
| 1 | 0.05 | 0.45 | 2.10 | 2.60 |
| 5 | 0.12 | 1.15 | 2.12 | 3.39 |
| 10 | 0.22 | 2.10 | 2.08 | 4.40 |
| 20 | 0.41 | 3.95 | 2.15 | 6.51 |
| 50 | 0.98 | 9.20 | 2.11 | 12.29 |

The empirical data reveals a striking divergence in how the system components behave under load. On one hand, local symmetric encryption (AES-256-GCM) and decentralized IPFS propagation scale linearly $O(n)$ alongside the asset volume, a dependency dictated entirely by local CPU boundaries and network throughput. On the other hand, the on-chain metadata anchoring exhibits strict asymptotic independence, $O(1)$. This process remains remarkably uniform, fluctuating tightly between 2.08 s and 2.15 s irrespective of the file size.

Figure 7 illustrates this behavior through a cumulative time distribution curve. The resulting performance profile indicates that block-commit intervals and smart contract gas parameters scale independently of the original payload. Because the operation relies strictly on fixed-length cryptographic metadata fields, this structural decoupling successfully insulates the distributed ledger from computational and throughput inflation.

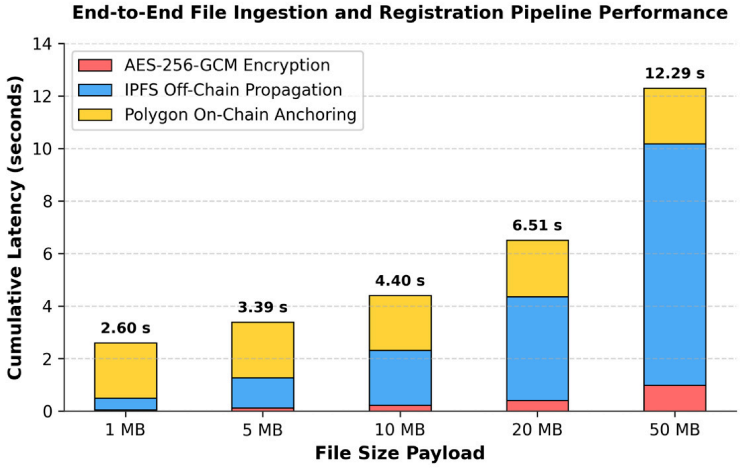


**Figure 7.** End-to-end file ingestion and registration pipeline performance showing multi-variable scaling dynamics against payload volume.

### *9.4. Scientific Contributions and Interpretations*

These empirical findings support three core conclusions regarding the system's practical contribution to applied Web3 architectures. First, uniform baseline tracking in Figure 7 proves the value of definitive cryptographic isolation; by anchoring only lightweight content identifiers (CIDs) on-chain, we completely remove raw file overhead from the ledger, enabling true horizontal scaling for institutional workloads.

Second, client-side stability remains deterministic because compiling the user interface via React eliminates runtime variance and processing bottlenecks, even during intensive 50 MB asset transfers.

Finally, achieving a post-quantum hybrid handshake in under 0.7 s (Figure 6) demonstrates a viable defense-in-depth model. This shows that early quantum resilience can be efficiently containerized and deployed over public cloud networks, removing the need for specialized physical hardware.

## 10. Future Works

The evolution of the proposed system aims to transition from a functional prototype to critical infrastructure for the academic ecosystem. Four strategic development axes have been identified:

- Data persistence and resilience—An immediate priority is the introduction of a distributed database or a blockchain event indexer (e.g., The Graph) to ensure that the academic ledger remains synchronized regardless of the backend lifecycle;
- Extended access control—Defining complex institutional hierarchies by implementing granular access policies facilitates selective resource sharing in accordance with university privacy norms and intellectual property rights [1];
- Identity decentralization—To strengthen non-repudiation, we intend to move toward a client-side signing model. By integrating wallet solutions, the traceability of actions will be bound to the individual's digital identity, eliminating the need for an intermediary authority [8];
- Post-quantum security—Future research will focus on integrating Post-Quantum Cryptographic (PQC) algorithms currently undergoing standardization (e.g., lattice-based or code-based schemes).

## 11. Conclusions

This paper demonstrates the efficacy of a decentralized academic infrastructure capable of harmonizing hybrid security paradigms with distributed storage technologies. Theoretically and technically, the major contribution of this work lies in the transition from a theoretical model to a fully operational system validated through an end-to-end workflow. The implementation successfully integrates complex processes into a decentralized architecture via:

- **Multi-layered security**—Hybrid authentication and session key derivation through quantum simulation set a new resilience benchmark for educational platforms;
- **Integrity and traceability**—The use of CIDs and blockchain anchoring ensures resource immutability and the non-repudiation of publication actions;
- **Institutional governance**—The RBAC model and the advanced academic ledger provide a tool specifically optimized for university requirements.

Operationalizing the system through cloud services confirms its capacity to function in real distributed environments. This validation stage confirms that the proposed architecture is both scalable and compatible with modern web infrastructures. While the current

platform validates the core architectural hypothesis, we have identified specific technical and conceptual constraints that define the trajectory for future operational maturity.

In the current configuration, indexing metadata and download session history are managed via a volatile state in the backend memory. Thus, a service restart results in data loss. Crucially, the fundamental integrity of architecture remains uncompromised, as critical data (on-chain metadata and IPFS objects) benefits from immutable decentralized persistence, independent of the API's local state [2,3,8].

A necessary methodological distinction involves BB84 integration via IBM Qiskit. At this stage, it represents an algorithmic emulation of Quantum Key Distribution (QKD), serving to prepare the software infrastructure for future native quantum hardware implementations [4,5,7].

Finally, for the sake of User Experience (UX) and to remove the technical barriers associated with browser-based digital wallets (e.g., MetaMask) for faculty members, the platform currently utilizes a centralized signing model at the backend level. While this simplifies the publication flow, a truly robust system requires a transition toward strict separation between the platform's institutional identity and the user's individual cryptographic authority to ensure personal non-repudiation on the blockchain [1,8].

In conclusion, the developed platform strikes a vital balance between privacy, transparency, and public auditability, providing a robust foundation for the future of academic resource management in the digital age.

**Author Contributions:** Conceptualization, B.T. and I.-P.A.; methodology, I.-P.A.; software, I.-P.A.; validation, I.-P.A. and B.T.; formal analysis, D.B. and C.B.; investigation, B.T. and I.-P.A.; resources, B.T., D.B. and C.B.; data curation, I.-P.A. and B.T.; writing—original draft preparation, I.-P.A. and B.T.; writing—review and editing, B.T.; visualization, B.T., I.-P.A., C.B. and D.B.; supervision, C.B. and D.B.; project administration, B.T.; funding acquisition, B.T. and C.B. All authors have read and agreed to the published version of the manuscript.

**Funding:** This work was funded by Politehnica of Bucharest.

**Data Availability Statement:** Other data is available upon request.

**Acknowledgments:** Many thanks are offered for support to Academy of Romanian Scientists, Ilfov 3, 050044 Bucharest, Romania.

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

## References

1. Nieles, M.; Dempsey, S.; Pillitteri, V. An Introduction to Information Security. *NIST Spec. Publ.* **2017**, *800*, 12–34. [CrossRef]
2. Nakamoto, S. Bitcoin: A Peer-to-Peer Electronic Cash System. *Decent. Bus. Rev.* **2008**, *21*, 1–9. Available online: https://bitcoin.org/bitcoin.pdf (accessed on 15 March 2026).
3. Benet, J. IPFS—Content Addressed, Versioned, P2P File System. *arXiv* **2014**, arXiv:1407.3561. [CrossRef]
4. Yang, Z.; Alfauri, H.; Farkiani, B.; Jain, R.; Di Pietro, R.; Erbad, A. A Survey and Comparison of Post-Quantum and Quantum Blockchains. *IEEE Commun. Surv. Tutor.* **2024**, *26*, 967–1002. [CrossRef]
5. Hao, F.; Ryan, P.Y.A. Password Authenticated Key Exchange by Juggling. *Lect. Notes Comput. Sci.* **2011**, *6615*, 175–191. [CrossRef]
6. Bennett, C.H.; Brassard, G. Quantum Cryptography: Public Key Distribution and Coin Tossing. In Proceedings of the IEEE International Conference on Computers, Systems and Signal Processing, Bangalore, India, 10–12 December 1984; pp. 175–179. [CrossRef]
7. IBM Quantum. Qiskit Documentation. Available online: https://www.ibm.com/quantum/qiskit (accessed on 8 May 2026).
8. Zhu, T.; Huang, Y.; Liang, Z.; Qin, M.; Niu, R.; Ma, Y.; Feng, Q. Research on an On-Chain and Off-Chain Collaborative Storage Method Based on Blockchain and IPFS. *Future Internet* **2026**, *18*, 92. [CrossRef]
9. Buterin, V. A Next-Generation Smart Contract and Decentralized Application Platform. Ethereum Whitepaper 2014. Available online: https://ethereum.org/whitepaper/ (accessed on 15 March 2026).
10. Liu, R.; Yu, W.; Jiang, J.; Li, Y. Hybrid Quantum Ant Colony Algorithm for The Ship Lock Arrangement Problem. *UPB Sci. Bull. Ser. C* **2023**, *85*.

11. Tudose, T.; Carabas, C.; Tapus, N. Revolutionizing Event Ticketing: A Secure and Transparent Approach Using Nfts and Blockchain. *UPB Sci. Bull. Ser. C* **2024**, *86*, 3–14.
12. Zhu, J.; Zhang, G. Fast Short-Term Channel State Prediction Based on Deep Trust Blockchain Networks. *UPB Sci. Bull. Ser. C* **2025**, *87*.
13. Zhai, P.; Zhang, L.; Zhang, Y. Internet of Things Access Control Identity Authentication Method Based on Blockchain. *UPB Sci. Bull. Ser. C* **2025**, *87*, 101–115.
14. Bogdan, I.C.; Simion, E. Cybersecurity Assessment and Certification of Critical Infrastructures. *UPB Sci. Bull. Ser. C* **2024**, *86*.
15. Tiganoaia, B.; Anghel, P.I. Informatics Technologies in Scientific Diplomacy, in the context of Classical and Cyber Diplomacy. *J. Knowl. Dyn.* **2026**, *3*, 31–43. [CrossRef]
16. Google Firebase. Get Started with Firebase Hosting. Available online: https://firebase.google.com/docs/hosting (accessed on 14 May 2026).
17. Render. Web Services Documentation. Available online: https://render.com/docs/web-services (accessed on 15 May 2026).
18. Render. Environment Variables and Secrets Configuration. Available online: https://render.com/docs/configure-environment-variables (accessed on 15 May 2026).