

## Informatics Technologies in Scientific Diplomacy, in the Context of Classical and Cyber Diplomacy

Bogdan TIGANOAIA<sup>1</sup>, Petrisor-Ionut ANGHEL<sup>2</sup>

<sup>1</sup> National University of Science and Technology POLITEHNICA Bucharest;  
Academy of Romanian Scientists, Ilfov 3, 050044 Bucharest, Romania;  
[bogdan.tiganoaia@upb.ro](mailto:bogdan.tiganoaia@upb.ro) (corresponding author)

<sup>2</sup> National University of Science and Technology POLITEHNICA Bucharest;  
Academy of Romanian Scientists, Ilfov 3, 050044 Bucharest, Romania;  
[petrisoranghel2906@gmail.com](mailto:petrisoranghel2906@gmail.com)

Received: March 17, 2026

Revised: April 10, 2026

Accepted: May 25, 2026

Published: June 30, 2026

**Abstract:** The paper presents the results of the authors' research for 14 months within a project funded by the Romanian Academy of Scientists. The design, implementation and testing of a decentralized web3 platform, based on Blockchain technologies – including smart contracts and Quantum, useful for education and diplomacy, is presented. The platform can also be used for knowledge management - for explicit knowledge flows. Our architecture allows quantum-enhanced authentication – offering an experimental, but future-oriented alternative to completely classical systems. It consists of a modular, layered structure, which includes the components: frontend, backend, quantum service integration, decentralized storage (IPFS) and blockchain registry. The platform is implemented and tested using several work scenarios. The 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.

**Keywords:** science, diplomacy, cyber, blockchain, technology.

### Introduction

*Diplomacy (classical)* is the art, science, and means by which nations, groups, or individuals conduct their affairs so as to protect their interests and promote their political, economic, cultural, or scientific relations, while maintaining peaceful relations (<https://www.cyber-diplomacy-toolbox.com/Diplomacy.html>, accessed in 2025). The word *diplomacy* originally comes from the Ancient Greek term δίπλωμα (a double-folded paper, a license, a map), referring to a document that allows someone to travel or have privileges. From the term δίπλωμα comes the later Latin term diploma (a state document, an official document). The *Vienna Convention on Diplomatic Relations (1961)* establishes the rules for the exchange and treatment of representatives between states and facilitates the development of good governance and friendly relations between nations, regardless of constitutional and social systems (obviously different, with substantial differences) - adapted from (<https://www.cyber-diplomacy-toolbox.com/Diplomacy.html>, accessed in 2025). Among the essential points of the Convention we can mention:

1. rules on the appointment of foreign representatives / states;
2. rules on the expulsion of diplomats, as the main sanction;
3. the right of diplomatic communication;
4. protection of diplomats;
5. protection of diplomats' families;
6. immunity from civil and administrative jurisdiction;

### How to cite

Tiganoaia, B. & Anghel, P.I. (2026). Informatics Technologies in Scientific Diplomacy, in the context of Classical and Cyber Diplomacy. *Journal of Knowledge Dynamics*, Vol. 3, No.1, pp. 31-43.  
<https://doi.org/10.56082/jkd.2026.1.31> ISSN ONLINE 3061-2640

7. the obligation of diplomats to respect the laws of the host state, etc.

Diplomacy has some distinctive characteristics that differentiate it from other types of communication and negotiation. Diplomacy can be (adapted from O. P. Jindal Global University, accessed in 2025):

- Bilateral: as is usually the case, which means that it involves two actors or parties. The aim is to establish and maintain mutually beneficial relations.
- Multilateral: there are situations of such diplomacy, which means that it involves more than two actors or parties. The aim is to create and maintain a collective and cooperative relationship between the parties.
- Continuous: this actually involves a process, not an event. The process is a long-term one whose goal is the constant and consistent involvement and interaction between the parties.
- Flexible: diplomacy is adaptable, it is not rigid or fixed, but rather adjustable – this implies that methods and tools can be modified over time, depending on the situation the parties are facing.

The four fundamental principles / stages of effective diplomacy:

1. negotiation,
2. communication,
3. relationship building,
4. promotion of interests.

These principles are interconnected and work in harmony to facilitate successful diplomatic engagements. Diplomacy is based on a long-term vision and strategic thinking (Bratianu & Lefter, 2001).

### **The main types of diplomacy**

The next part of the paper explains the main types of diplomacy (selection, of the most important):

1. **Public diplomacy** – often confused with classical diplomacy, being the oldest.

2. **Scientific diplomacy**

Scientific diplomacy eludes an agreed definition, but is generally understood to include three aspects – see ([https://www.eeas.europa.eu/eeas/what-science-diplomacy\\_en](https://www.eeas.europa.eu/eeas/what-science-diplomacy_en), accessed in 2025):

1. **Diplomacy for science** – the use of diplomatic action to facilitate international scientific collaboration, for example, by negotiating research and development agreements and exchange programs or by enabling the establishment of international research infrastructures;

2. **Science for diplomacy** – the use of science as a power to promote diplomatic objectives, for example, to build bridges between nations and create goodwill on which diplomatic relations can be built;

3. **Science in diplomacy** – the direct support of diplomatic processes through science, for example, by providing scientific advice and evidence to inform and support decision-making in foreign and security policies.

In the European Union / Europe there are many examples of institutions established with both scientific and science diplomacy motivation:

1. The European Organization for Nuclear Research (CERN), established in 1954.
2. The Joint Research Centre (JRC) of the European Commission, established in 1957.
3. The International Institute for Applied Systems Analysis (IIASA), established in 1972.
4. The International Thermonuclear Experimental Reactor (ITER), under construction in the south of France – operational by 2035.
5. The Synchrotron System for Experimental Science and Applications in the Middle East (SESAME) – with financial support also from the EU, an international centre

of excellence for Israel, the Palestinian Territories, Egypt, Jordan, Iran, Pakistan, Turkey and Cyprus – inaugurated in 2017.

6. New institutional actors have emerged, such as the International Council for Science, created in 2018.

### **3. Cyber diplomacy**

**Cyberspace** is a complex and (still) unexplored and evolving territory. States use common and accepted rules, protocols, and behaviours to facilitate interactions between global actors in the public and private sectors. Due to **the nature of cyberspace**, it is important to engage in cyber diplomacy rather than relying solely on cyber defence (adapted from **Error! Hyperlink reference not valid.**, accessed in 2025).

**Cyber diplomacy** is the art, science, and means by which nations, groups, or individuals operate in cyberspace to protect their interests and advance their political, economic, cultural, or scientific relationships, while maintaining peaceful relations (adapted from **Error! Hyperlink reference not valid.**, accessed in 2025). Cyber diplomacy should minimize the consequences of (adapted from **Error! Hyperlink reference not valid.**, accessed in 2025):

1. cyber aggression,
2. cyber attacks on critical infrastructure,
3. data breaches, cybercrime,
4. cyber espionage,
5. online theft
6. offensive cyber operations by state or non-state actors.

The Paris Call for Trust and Security in Cyberspace, launched on 12 November 2018 at the Paris Peace Forum, addresses emerging and under-regulated cyber challenges. States, companies (including Microsoft, Kaspersky, Siemens, Google, Facebook), professional associations and civil society organizations are discussing solutions for the regulation of cyberspace, the enforceability of international law and responsible behaviour of states (adapted from **Error! Hyperlink reference not valid.**, accessed in 2025). **The 9 Principles - The Paris Call for Trust and Security in Cyberspace**

1. Protecting People and Infrastructure
2. Protecting the Internet
3. Defending Electoral Processes
4. Defending Intellectual Property
5. Non Proliferation
6. Lifecycle Security
7. Cyber Hygiene
8. No Private Cyberattacks
9. International Norms

### **4. Energy Diplomacy**

Energy diplomacy refers to the way in which states and international actors manage and negotiate their energy resources, trade relations and energy-related interests; this is essential for the energy security of any country, energy being the vital factor for the functioning of modern economies (Apostol, 2023).

### **5. Cultural Diplomacy**

Cultural diplomacy can be defined as the exchange of ideas, information, art and other aspects of culture between nations and their populations, with the aim of promoting mutual understanding with direct implications for improving bilateral relations.

### **6. Educational Diplomacy**

Educational diplomacy uses initiatives to achieve educational objectives in order to build international relations. We can include student exchange programs, joint study programs

between universities in different countries and initiatives that promote global educational objectives, such as Sustainable Development Goal 4 - quality education for all.

## 7. Economic Diplomacy

Economic diplomacy ensures an efficient framework for institutional cooperation in order to carry out concerted efforts to promote Romania's economic objectives abroad and, respectively, to support the attraction of foreign investment in Romania (Romanian Foreign Ministry, Economic diplomacy, accessed in 07.07.2025, <https://www.mae.ro/node/1418/1>).

## Informatics Technologies

### 1. Blockchain

Blockchain technology is based on Distributed Ledger Technology (DLT), which allows direct transactions between users without the need for intermediaries or a centralized authority to oversee them. Transactions are validated with a consensus mechanism within an interconnected network of computers. What is a blockchain? In 1991, Stuart Haber and W. S. Stornetta published a paper titled *How to Apply a Time Stamp to a Digital Document*, in which they proposed a method for digitally time stamping documents using hash functions, digital signatures, and data stored in blocks. This paper is considered to be the first description of the blockchain concept. Today, we refer to the term "blockchain" as a distributed database or ledger that is shared among the nodes of a computer network and stores data in blocks that are linked together using various consensus algorithms. Being open and distributed, blockchain offers immutability, security, and transparency. In 2008, Satoshi Nakamoto published a paper titled *Bitcoin: A Peer-to-Peer Electronic Cash System*, in which he proposed a decentralized financial instrument using a digital currency called Bitcoin. It proposes a *peer-to-peer network that uses proof-of-work to record a public history of transactions*.

There are several organizations with connections to blockchain development, such as:

- IBM is the most involved and a major investor.
- Mastercard is another organization that has over 100 blockchain patents filed. This company uses the technology to increase fraud protection and reduce transaction costs (Investopedia accessed in 2025). According to Investopedia, the three largest blockchain companies are:
  - Coinbase Global Inc. (San Francisco, CA, USA)—COIN;
  - Canaan Inc. (Beijing, China)—CAN;
  - Galaxy Digital Holdings Ltd. (New York, NY, USA)—BRPHF.

### 2. Quantum Technologies

Quantum technologies use the principles of quantum mechanics – for example, superposition and inseparability – to develop new capabilities in the fields of computation, communication and detection. These technologies are in their infancy, opening up new research directions, but have the potential to revolutionize various fields: data security, healthcare, finance, national security, etc. Key areas to explore in the field of quantum technologies:

1. Quantum Computing - This field aims to create computers that can perform calculations far beyond the capabilities of classical computers, using qubits, which can exist in multiple states simultaneously due to superposition. Companies such as IBM are leaders in the development of quantum hardware with qubit processors.
2. Quantum Communication: Quantum Key Distribution (QKD) uses quantum mechanics to enable secure communication by detecting eavesdropping attempts. Nokia is researching quantum-resistant cryptography and quantum key distribution to enhance security.
3. Quantum networks: aim to connect quantum computers and sensors.

4. Quantum Sensing: Quantum sensors are characterized by very good sensitivity and precision in measuring physical quantities such as time, magnetic fields and gravity. Applications in the field can be in areas such as: health, environmental monitoring, navigation, etc. Cold atom interferometry is being explored for applications in space and defence.

*Advantages of using quantum technologies:*

1. Economic potential – by 2035, trillions of dollars
2. Changes in society – by using quantum technologies, challenges in areas such as: climate change, new materials, new medicines are considered.
3. National security – quantum technologies, especially quantum computing and communications, have implications for national security, including cryptography and surveillance.
4. Public Policy - Governments and policy makers are actively involved in developing strategies to encourage the development of quantum technologies, address potential risks and ensure responsible development.

*Challenges / Opportunities in the field of Quantum computing and technologies:*

1. Building and scaling quantum computers and networks remains a significant challenge.
2. Ethical considerations: The development and implementation of quantum technologies raises ethical questions regarding privacy, security and potential misuse.
3. International collaboration: International collaboration is crucial for sharing knowledge, resources and best practices in the field.

The topic is obviously not completely exhausted / covered, we can find more details about Quantum Technologies here - <https://www.nokia.com/quantum/quantum-technologies-explained/>

### **3. Cloud, Edge and Fog Computing**

Cloud computing, edge computing and fog computing are all methods of providing computing services, but they differ in their approach to where data processing and storage take place.

**Cloud computing** is a centralized model in which data is processed and stored on remote servers:

- Centralized: Data is processed and stored on remote servers accessed via the internet.
- Scalable: Resources can be easily scaled up or down, depending on demand.
- Examples: Websites, online applications, large-scale data analysis.
- Advantages: Cost-effective for many applications, easy to manage, scalable and accessible from anywhere.
- Disadvantages: Latency can be an issue for real-time applications, security issues when transmitting sensitive data.

**Edge computing** brings processing closer to the data source, often directly on devices:

- Decentralized: Processing occurs closer to the data source, often on or near the device.
- Low latency: Ideal for real-time applications where fast response times are crucial.
- Examples: Autonomous vehicles, industrial automation, video surveillance.
- Advantages: Low latency, improved security, bandwidth savings.
- Disadvantages: Limited processing power on edge devices, more complex to manage than the cloud.

**Fog computing** acts as a bridge between the two, distributing processing between edge devices and the cloud:

- Hybrid: Extends cloud computing capabilities to the edge of the network, acting as an intermediate layer between edge devices and the cloud.

- **Distributed processing:** Data can be processed at various points along the network, from edge devices to fog nodes and the cloud.

Examples: Smart cities, industrial IoT, content delivery networks.

- **Advantages:** Reduces latency compared to cloud-only solutions, handles more complex processing than edge solutions alone, manages data flow between edge and cloud.

- **Disadvantages:** More complex to implement than edge or cloud, requires careful network design.

#### **4. IoT and BigData**

**IoT devices** collect data from the environment, such as temperature data from a smart thermostat or machine health data from industrial equipment. The devices continuously send information over the internet, often in real time (Pritesh Patel, 2024).

**Big Data platforms** store and process this data. Because IoT devices can generate large volumes of data, managing them becomes difficult with traditional databases. Big Data technologies such as Hadoop and Spark can process and store data in distributed systems, which can allow companies to work more efficiently with large data sets (Pritesh Patel, 2024).

**5. Artificial Intelligence (AI) and Machine Learning (ML)** - represent the pinnacle of contemporary technological innovation. These revolutionary fields are the basis of many transformative changes in modern society, redefining industrial processes, business models and human-technology interaction (Bittnet Report - *AI and ML: The technologies that are transforming the future*, accessed in 2025)

**6. Augmented reality (AR) and virtual reality (VR)** - virtual reality involves the experience in a virtual environment without sensory contact with the environment around you, while augmented reality superimposes 3D objects on the real world, precisely to create the sensation that everything is *real*. Augmented reality is not a fully immersive experience like virtual reality (VR), the latter requiring the use of a special headset (Soft Tehnica Report, 2025)

#### **7. Business information systems – ERP, CRM, WMS, SFA, BI**

ERP – Enterprise Resource Planning

CRM – Customer Relationship Management

WMS - Warehouse Management System

SFA - Sales Force Automation

BI – Business Intelligence

#### **Objectives and Methodology of Our Research**

The objective of the research is the development of a decentralized web3 platform, based on Blockchain technologies - for details see (Tiganoaia et Alexandru, 2026) and (Tiganoaia et Anghel, 2026) – including smart contracts and Quantum, useful for education and diplomacy. Regarding the research methodology, the research used scientific research tools and methods, as follows:

- software modelling and simulation.
- bibliographic research.
- case study.

These scientific research tools and methods are integrated into the research plan, which contains activities, along with the implementation period.

## Activities / results / what is next ?

1. Designing a decentralized platform useful for science diplomacy courses - where assistants and teachers can securely upload and manage course materials, training or assignments. This stage has been completed.
2. Implementing the decentralized platform - we are at the beta version of the platform, for which we have tested several performance indicators / metrics. This is the second step after the alpha version.
3. Next comes the final version of the application and its analysis in terms of performance indicators (times, scalability, etc.) - details in the next 2026 report.

The approach is a hybrid one:

1. classic authentication using J. PAKE and
2. simulated **quantum key exchange** (via IBM Qiskit Runtime) for increased session security.

The content is stored off-chain via IPFS (Interplanetary File System - <https://docs.ipfs.tech/>), with metadata and CIDs stored on a blockchain using smart contracts (Solidity). The goal is to **simulate quantum-enhanced security** within a scalable and decentralized storage architecture - Hybrid (classical - quantum) architecture for decentralized educational platform. **Our architecture enables quantum-enhanced authentication** - providing an experimental but future-oriented alternative to fully classical systems.

### 1. Architecture Description

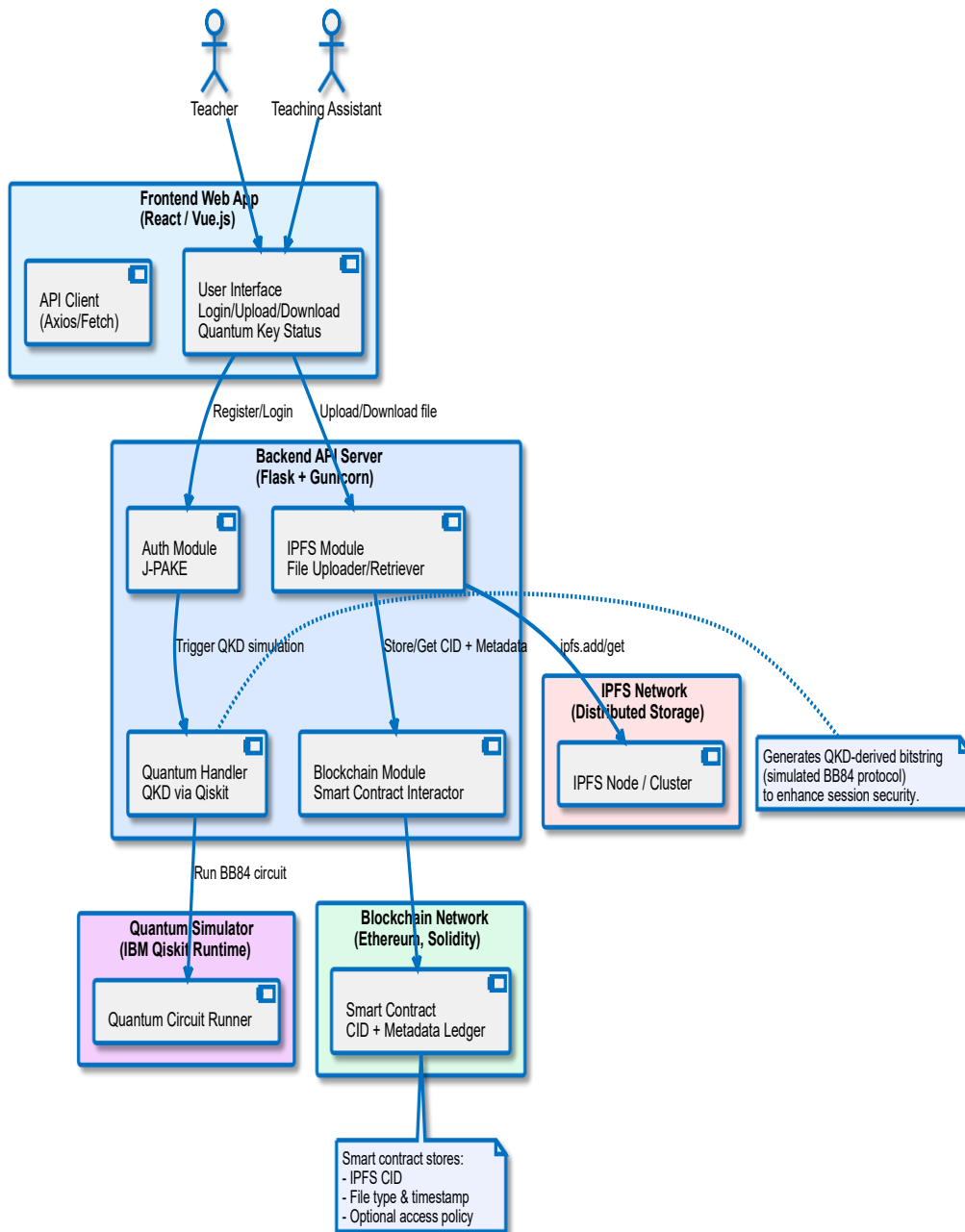
The architecture – see Figure 1, consists of a modular, layered structure, comprising the components:

- frontend - in the world of web and software development, the frontend is everything that a user sees, clicks, and interacts with directly on a website or app. It is often referred to as the **client-side** because it runs right inside the user's web browser.
- backend - the back end is the **behind-the-scenes machinery of a website or application**. It consists of the server, the application logic, and the database. Users never see it directly, but it is responsible for processing data, handling user authentication, power-housing business logic, and making sure the front end has the information it needs to function.
- quantum service integration,
- decentralized storage (IPFS), and
- blockchain ledger.

The decentralized storage (IPFS) stands for **Inter Planetary File System**. IPFS is a very real, groundbreaking technology designed to change how data is stored and shared across the internet. IPFS is a decentralized, peer-to-peer (P 2 P) network for storing and sharing files. To understand the differences it is helpful to compare IPFS to the traditional web. The standard internet we use every day relies on **HTTP** (Hypertext Transfer Protocol). IPFS approaches data completely differently.

- HTTP is Location-Based - When a user looks for a file using HTTP, the client uses a URL ( like <https://name.com/> ). This tells the browser **where** the file is (on a specific server owned by a specific company). **The Problem:** If that server crashes, gets hacked, or the company goes out of business, the file vanishes. If millions of people try to access it at once, the server crashes.
- IPFS is Content-Based - Instead of asking **where** a file is, IPFS asks **what** the file is. Every file uploaded to IPFS gets a unique cryptographic fingerprint called a **CID ( Content Identifier )**. **The Solution:** When a user looks for a file, the client requests its CID. The IPFS network finds any computer (node) nearby that has a copy of that file and pulls it from them.

The backend orchestrates secure communication between layers, ensuring that user actions (such as logging in and uploading files) pass through both classical authentication and simulated quantum key phases before interacting with the storage or blockchain subsystems. This architecture intentionally balances performance (classical primitives) and research experimentation (quantum simulation), providing a platform for future quantum enhancements once hardware QKD becomes practical.



**Figure 1. The overall architecture of the Decentralized Platform (DP) system – our proposal**

**2. Sequential workflow for authentication, file upload, and file retrieval:**

The focus is on authentication, quantum simulation and the content/file lifecycle (upload, storage, retrieval) – see Figure 2a and Figure 2b. Users – teachers/assistants/students are classically authenticated using the J. PAKE protocol (ensures mutual authentication and Man in the Middle attack resistance), followed by a

simulation of a quantum key exchange process (BB84) via IBM's Qiskit Runtime. This quantum generated bit string hash is used to enhance session-level cryptographic tokens.

### 3. The platform's end-to-end workflow

Content files are uploaded via the frontend, stored in IPFS, and linked to metadata stored in a blockchain ledger via smart contracts – see Figure 4. Access to files is governed by retrieving CIDs from the blockchain and resolving them through the IPFS network. Metadata (file type, user, timestamp, CID) is stored on the blockchain, ensuring file auditability and tamper resistance. This flow is particularly relevant in academic environments where data authenticity, decentralized integrity, and future-proof quantum readiness are essential.

Users are provided with real-time visual feedback on their authentication status, upload progress, quantum key simulation status, and blockchain-related actions.

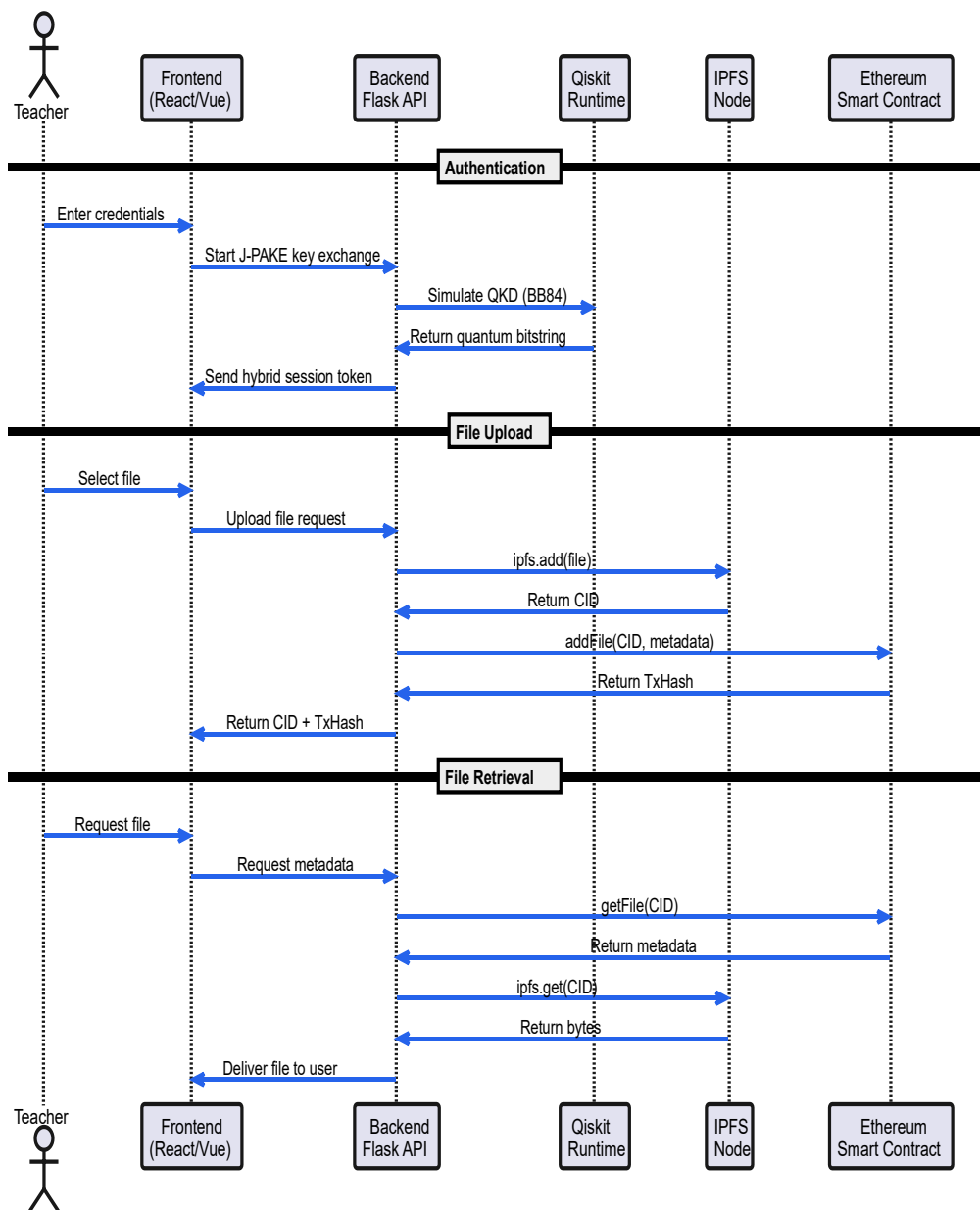


Figure 2a. Sequential flow for authentication, file upload and retrieval – our proposal

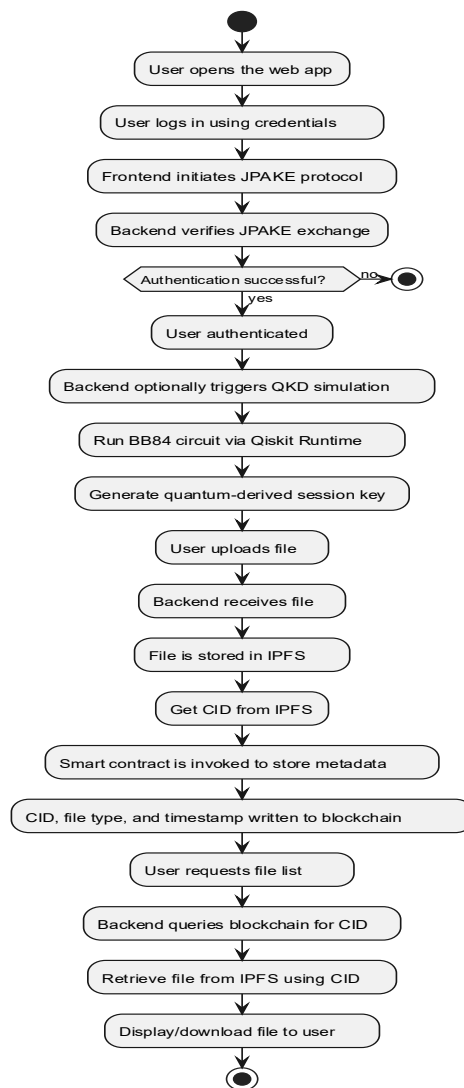


Figure 2b. Sequential flow for authentication, file upload and retrieval - our proposal

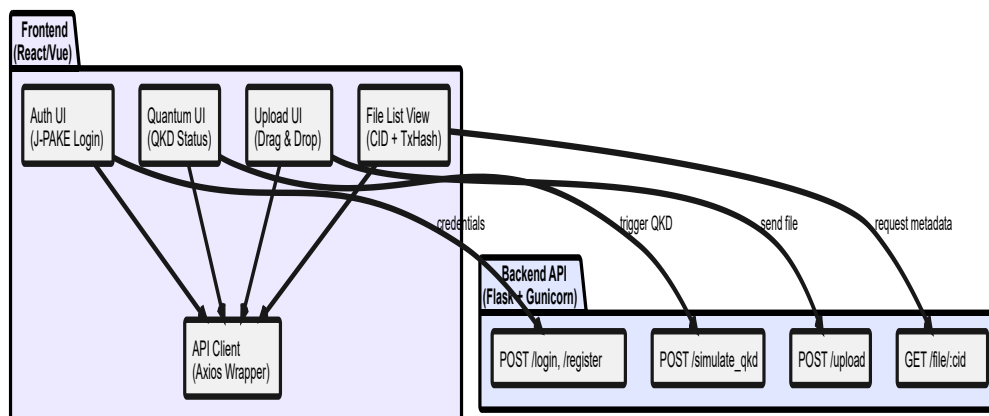


Figure 3. Frontend-Backend component diagram and REST API interaction - our proposal

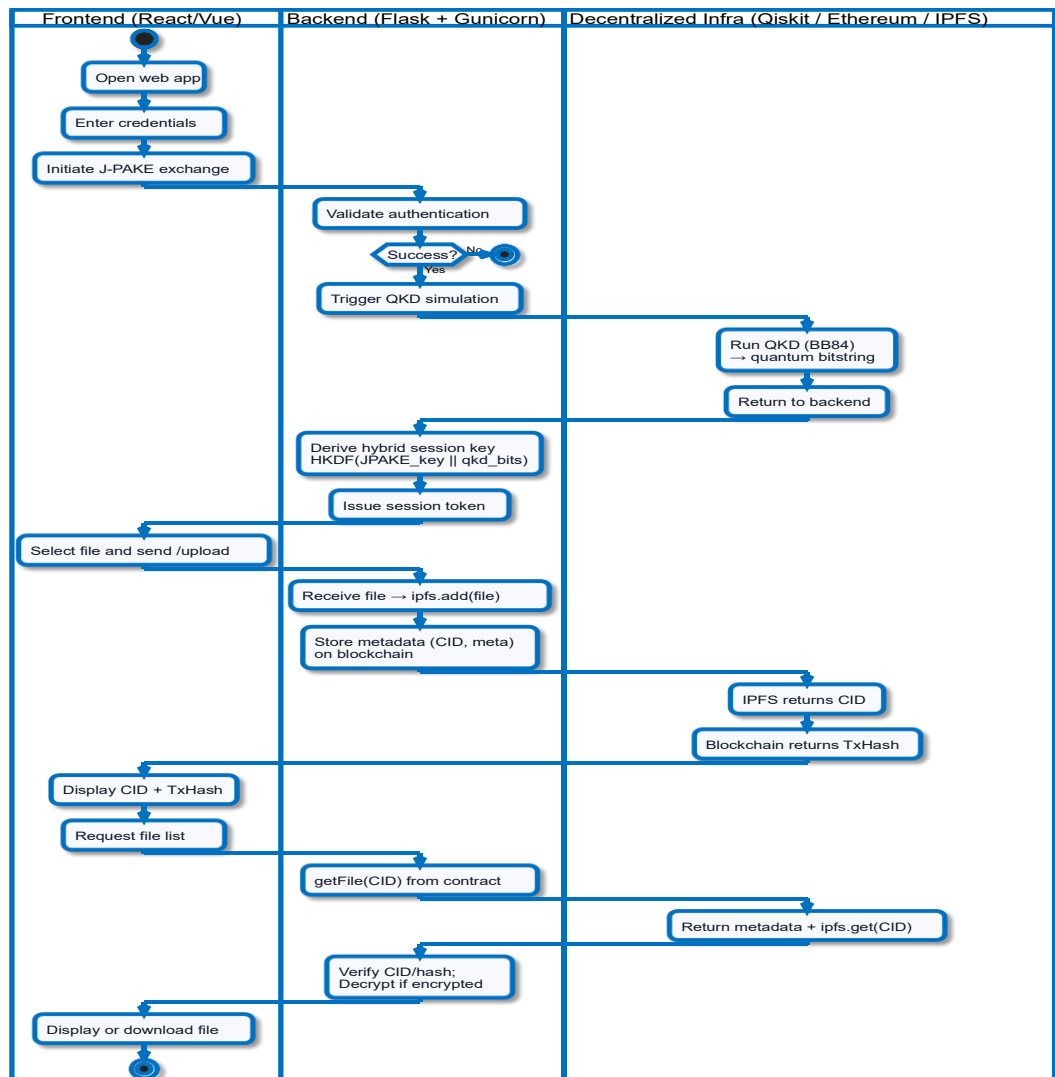


Figure 4. The platform's end-to-end workflow - our proposal

#### 4. Frontend-Backend component diagram and REST API interaction

The frontend communicates securely with the backend API using authenticated REST calls (secured with HTTPS and session tokens derived partially from simulated quantum keys). The frontend-backend component diagram and REST API interaction are our proposals and they can be found in the Figure 3.

A **REST API interaction** is the way two different computers or software applications talk to each other over the internet. When the client uses an app on a phone, he does not hold all the world's data inside it. Instead, it / he interacts with a remote server using a set of rules called **REST (REpresentational State Transfer)**. The core concept is a request and response model. Every REST API interaction is a conversation based on a strict **client-server model**:

- **the client** (e.g., the mobile app or browser of the client) asks for something.
- **the server** (the remote computer) processes the request and sends a response back.

When the client initiates an interaction, it sends a package of information to the server containing four main things: the URL (endpoint) - this is the digital address of the specific data or service the client wants to interact with; the HTTP method (get, post, put, patch, delete); the headers - these are like the metadata on an envelope and they contain extra

information, such as authentication keys or the format of the data being sent (usually application/json); the body - this contains the actual data the client wants to send to the server. The server's response - after receiving the request, the server processes it and sends back a response containing two critical things: a status code (a three-digit number telling the client how the request went); the payload (the data). Most modern REST APIs return data in a lightweight format called **JSON** (JavaScript Object Notation), which looks like a structured list of key-value pairs.

The proposed hybrid architecture is operational in the alpha simulation phase, achieving a ~95% file upload success rate and nearly 100% for downloads on a sample of 50 files with sizes in the 10-1024KB range. The lower upload success rate can be attributed to occasional instability in the cryptographic pipeline for larger files, as well as IPFS latency during decentralized storage.

### **5. Platform implementation – beta version**

To evaluate the preliminary performance of the proposed hybrid web application, we implemented a Python simulation that generates approximate values for the main system operations. So, the decentralized platform was implemented and we are at the beta version of the platform, for which we have tested several performance indicators / metrics. The final version is proposed for the end of the year (2026) – with an analysis in terms of performance indicators (times, scalability, etc.). The performance metrics for the implemented version can be viewed in the paper written by (Tiganoaia et Anghel, 2026) and consist of:

1. Authentication Latency - Comparative distribution for J. PAKE, QKD and HKDF - authentication latency comes from the quantum key distribution phase, which requires approximately 0.6 to 1.5 seconds per session, while the additional cost introduced by deriving the session key through HKDF is negligible. Therefore, for small files, the hybrid authentication process remains under 2 seconds, demonstrating the feasibility of this method in a decentralized educational context.

2. Upload latency components by file size - Impact of encryption, IPFS and Blockchain operations - for file uploads, the total latency increases proportionally to the file size due to the linear scaling of the encryption process.

3. Download latency components by file size - IPFS retrieval and decryption time - the dominant factor is the latency for retrieving data from IPFS, which varies between 0.5 and 1.9 seconds, while file downloads require only minimal decryption time, with values below 1 second, confirming the efficiency of the AEAD encryption scheme used.

4. Upload Throughput vs. File Size - The transfer rate varies depending on the file size, reaching up to approximately 300KB/s for uploads.

5. Download Throughput vs. File Size - The transfer rate varies depending on the file size, reaching up to approximately 600KB/s for downloads.

6. Upload and Download Success Rates - Platform Stability in Simulation.\

### **Conclusions**

1. Classical authentication is secured by the J. PAKE protocol, which uses zero-knowledge proofs to allow two parties to establish a shared secret over an insecure channel without revealing the password or its hash. This choice provides robustness against offline dictionary attacks and guarantees mutual authentication without centralized password storage.

2. To extend this fundamental security, the system incorporates a simulated quantum key distribution mechanism using IBM's Qiskit Runtime. Scalability considerations were addressed by offloading large data (such as video lectures or training modules) to IPFS. Only the content identifiers (CIDs) and metadata are stored on the blockchain. This separation between the data payload and metadata allows for availability without overloading the blockchain or incurring high transaction costs.

3. A list of all the technologies and frameworks that will be used in our hybrid decentralized authentication and storage platform, enhanced with quantum technology: React, Vue, Flask, Gunicorn, IBM Qiskit SDK, Solidity, Infura, Ethereum, IPFS.

**Artificial intelligence instruments Declaration:** The authors do not use Artificial intelligence instruments for this research. All images and paragraphs are original.

**Acknowledgments:** Part of this paper was presented at the AOSR Spring National Conference in May 2026 – but without any publication. The research is part of a project carried out by the authors through Academy of Romanian Scientists.

## References

- Apostol Daniel, *Romania's Energy Diplomacy: between assets and challenges*, 2023, <https://www.economistul.ro/lumea-energiei/diplomatia-energetica-a-romaniei-intre-atuuri-si-provocari-62944/>
- Bittnet Report, *AI and ML: The technologies that are transforming the future* [https://www.bittnet.ro/noutati/ai-si-ml-tehnologiile-care-transforma-viitorul/#:~:text=Inteligen%C8%9Ba%20Artificial%C4%83%20\(AI\)%20%C8%99i%20%C3%8Env%C4%83%C8%9Barea,afaceri%20%C8%99i%20interac%C8%9Biunea%20uman%2Dtehnologie](https://www.bittnet.ro/noutati/ai-si-ml-tehnologiile-care-transforma-viitorul/#:~:text=Inteligen%C8%9Ba%20Artificial%C4%83%20(AI)%20%C8%99i%20%C3%8Env%C4%83%C8%9Barea,afaceri%20%C8%99i%20interac%C8%9Biunea%20uman%2Dtehnologie), accessed at 07.07.2025
- Bratianu, C. & Lefter, V. (2001). *Management strategic universitar*. Editura RAO, Bucharest.
- Cyber Risk GmbH, *What is diplomacy?* <https://www.cyber-diplomacy-toolbox.com/Diplomacy.html>, accessed at 30.06.2025.
- Cyber Risk GmbH, *What is cyber diplomacy?* [https://www.cyber-diplomacy-toolbox.com/Cyber\\_Diplomacy.html](https://www.cyber-diplomacy-toolbox.com/Cyber_Diplomacy.html), accessed at 30.06.2025
- Investopedia, *The 6 Biggest Blockchain Companies*. Available online <https://www.investopedia.com/10-biggest-blockchain-companies-5213784> (accessed on 2 May 2023).
- O. P. Jindal Global University, *What is diplomacy? Definition, scope, importance & more*, <https://jgu.edu.in/blog/2024/02/24/what-is-diplomacy/>, 2024, accessed at 30.06.2025.
- Pritesh Patel, *What Happens When IoT Meets AI and Big Data?*, <https://www.iotforall.com/iot-meets-big-data-ai>, 2024.
- Romanian Foreign Ministry, *Economic diplomacy*, accessed in 07.07.2025, <https://www.mae.ro/node/1418/1>
- Soft Tehnica Report, *What is Augmented Reality. How does it differ from Virtual Reality?* <https://soft-tehnica.com/ro/ce-este-realitatea-augmentata-prin-ce-se-diferentiaza-de-realitatea-virtuala/#:~:text=Cele%20dou%C4%83%20no%C8%9Biuni%20au%20la,c%C4%83%20total%20este%20%E2%80%9Creal%E2%80%9D>, accessed at 07.07.2025.
- Tiganoaia Bogdan, Petrisor-Ionut Anghel, Doina Banciu - coauthors, *A Decentralized Platform Leveraging Blockchain and Quantum-Secure Communication for Scientific Diplomacy and Trusted Resource Sharing*, sent for publishing at one Clarivate Analytics, 2026.
- Tiganoaia Bogdan; Alexandru, George Madalin. *Building a Blockchain-Based Decentralized Crowdfunding Platform for Social and Educational Causes in the Context of Sustainable Development*. Sustainability 2023, 15, 16205. <https://doi.org/10.3390/su152316205>
- The Diplomatic Service of the European Union, *What is science diplomacy*, [https://www.eeas.europa.eu/eeas/what-science-diplomacy\\_en](https://www.eeas.europa.eu/eeas/what-science-diplomacy_en), accessed la 30.06.2025