Noi tehnologii informatice - de la provocări actuale către Blockchain în diplomaţia ştiinţifică, în contextul diplomaţiei clasice si cibernetice – NEWTECH BLOCKCHAIN – SCIENCE, CYBER, DIPLOMACY

Domeniul stiintific: *RO-SCUD - Știință-Cultură-Diplomație pentru România*

Cuvinte cheie: *stiinta, diplomatie, cyber, blockchain, tehnologie.*

Raportul 2 – R2

Decembrie 2025

Prezentat de:
Bogdan TIGANOAIA

A. DIPLOMATIE CLASICA-DIPLOMATIE STIINTIFICA-DIPLOMATIE CIBERNETICA

Diplomația (clasica) este arta, știința și mijloacele prin care națiunile, grupurile sau indivizii își conduc afacerile, astfel încât să își protejeze interesele și să își promoveze relațiile politice, economice, culturale sau științifice, menținând în același timp relații pașnice [1].

Cuvântul **diplomație** provine inițial din termenul grecesc antic δίπλωμα (o hârtie împăturită dublu, o licență, o hartă), referindu-se la un document care permite cuiva să călătorească sau să aibă privilegii. Din termenul δίπλωμα provene mai tarziu termenul latin diplomă (un document de stat, un document oficial). ***Convenția de la Viena privind relațiile diplomatice (1961)*** stabileste regulile pentru schimbul și tratamentul reprezentantilor între state și facilitează dezvoltarea relațiilor de buna guvernanta si prietenie între națiuni, indiferent de sisteme constituționale și sociale (evident diferite, cu diferente substantiale) - adaptat dupa [1].

Tipuri de diplomatie (selectie, dintre cele mai importante):

1. **Diplomatia publica** – adesea se confunda cu diplomatia clasica, fiind cea mai veche.

2. **Diplomatia stiintifica**

Diplomația științifică scapă unei definiții convenite, dar este în general înțeleasă ca incluzând trei aspecte – vezi [4]:

1. ***Diplomația pentru știință*** – utilizarea acțiunii diplomatice pentru a facilita colaborarea științifică internațională, de exemplu, prin negocierea acordurilor de cercetare și dezvoltare și a programelor de schimb sau prin permiterea înființării de infrastructuri de cercetare internaționale;
2. ***Știința pentru diplomație*** – utilizarea științei ca putere pentru a promova obiective diplomatice, de exemplu, pentru construirea de punți între națiuni și crearea de bunăvoință pe care se pot construi relații diplomatice;
3. ***Știința în diplomație*** – sprijinul direct al proceselor diplomatice prin știință, de exemplu, prin furnizarea de consultanță științifică și dovezi pentru a informa și sprijini procesul decizional în politicile externe și de securitate.

In Uniunea Europeana / Europa exista multe exemple de instituții înființate cu o motivație atât științifică, cât și de diplomație științifică:

1. Organizația Europeană pentru Cercetare Nucleară (CERN), înființată în 1954
2. Centrul Comun de Cercetare (JRC) al Comisiei Europene, înființat în 1957
3. Institutul Internațional pentru Analiza Sistemelor Aplicate (IIASA), înființat în 1972
4. Reactorul Termonuclear Experimental Internațional (ITER), aflat în construcție în sudul Franței – operational pana in 2035.
5. Sistemului de Sincrotron pentru Știință Experimentală și Aplicații în Orientul Mijlociu (SESAME) – cu sprijin financiar si de la UE, centru international de excelenta a Israelului, Teritoriilor Palestiniene, Egiptului, Iordaniei, Iranului, Pakistanului, Turciei și Ciprului – inaugurat in 2017.

6. Au apărut noi actori instituționali, cum ar fi Consiliul Internațional pentru Știință, creat în 2018.

3. Diplomatia cibernetica

Spatiul cibernetic reprezinta un teritoriu complex și neexplorat (inca suficient), în continuă evoluție. Statele utilizează regulile, protocoalele și comportamentele comune și acceptate pentru a facilita interacțiunile dintre actorii globali din sectorul public și cel privat. Datorită naturii spațiului cibernetic, este important să ne angajăm în diplomația cibernetică, mai degrabă decât să ne bazăm exclusiv pe apărarea cibernetică [3].

Diplomația cibernetică este arta, știința și mijloacele prin care națiunile, grupurile sau indivizii își desfășoară activitatea în ***spațiul cibernetic***, astfel încât să își protejeze interesele și să își promoveze relațiile politice, economice, culturale sau științifice, menținând în același timp relații pașnice [3].

Diplomația cibernetică trebuie să minimizeze consecințele (adaptat dupa [3]):

1. agresiunii cibernetice,
2. atacurilor cibernetice asupra infrastructurii critice,
3. încălcărilor de date, ale criminalității cibernetice,
4. spionajului cibernetic,
5. furtului online
6. operațiunilor cibernetice ofensive efectuate de actori statali sau nestatali.

Apelul de la Paris pentru încredere și securitate în spațiul cibernetic, lansat pe 12 noiembrie 2018 în cadrul Forumului pentru Pace de la Paris, abordează provocările cibernetice emergente și insuficient reglementate. Statele, companiile (inclusiv Microsoft, Kaspersky, Siemens, Google, Facebook), asociațiile profesionale și organizațiile societății civile discută pentru a găsi soluții pentru reglementarea spațiului cibernetic, practicabilitatea dreptului internațional și comportamentul responsabil al statelor [3].

Cele 9 principii - Apelul de la Paris pentru încredere și securitate în spațiul cibernetic

1. Protejarea persoanelor și a infrastructurii
2. Protejarea internetului
3. Apărarea proceselor electorale
4. Apărarea proprietății intelectuale
5. Neproliferarea
6. Securitatea ciclului de viață
7. Igiena cibernetică
8. Fără atacuri cibernetice private
9. Norme internaționale

B. TEHNOLOGII INFORMATICE FOLOSITE

I. Blockchain

Ce este un blockchain? În 1991, Stuard Haber și W. S. Stornetta au publicat o lucrare intitulată „Cum se aplică o ștampilă temporală unui document digital", în care au propus o metodă de ștampilare temporală digitală a documentelor folosind funcții hash, semnături digitale și date stocate în blocuri. Această lucrare este considerată a fi prima descriere a conceptului de blockchain. În prezent, ne referim la termenul „blockchain" ca la o bază de date distribuită sau un registru care este partajat între nodurile unei rețele de calculatoare și stochează date în blocuri care sunt legate între ele folosind diferiți algoritmi de consens. Fiind deschis și distribuit, blockchain-ul oferă imutabilitate, securitate și transparență. În 2008, Satoshi Nakamoto a publicat o lucrare intitulată „Bitcoin: Un sistem electronic de numerar peer-to-peer", în care a propus un instrument financiar descentralizat folosind o monedă digitală numită Bitcoin. Aceasta propune o „rețea peer-to-peer care folosește proof-of-work pentru a înregistra un istoric public al tranzacțiilor" [5]. Tehnologia Blockchain se bazează pe Tehnologia Registrului Distribuit (DLT), care permite tranzacții directe între utilizatori fără a fi nevoie de intermediari sau o autoritate centralizată care să le supravegheze. Tranzacțiile sunt validate cu un mecanism de consens în cadrul unei rețele interconectate de computere.

Există mai multe organizații cu conexiuni în dezvoltarea unui blockchain, cum ar fi:

- IBM este cel mai implicat și un investitor principal.
- Mastercard este o altă organizație care are peste 100 de brevete blockchain depuse. Această companie folosește tehnologia pentru a crește protecția împotriva fraudei și pentru a reduce costurile tranzacțiilor [5].

Conform Investopedia [6], cele mai mari trei companii blockchain sunt

→ Coinbase Global Inc. (San Francisco, CA, SUA)—COIN;

→ Canaan Inc. (Beijing, China)—CAN;

→ Galaxy Digital Holdings Ltd. (New York, NY, SUA)—BRPHF.

II. Tehnologii Quantum

Tehnologiile cuantice utilizează principiile mecanicii cuantice – de exemplu superpoziția și inseparabilitatea, pentru a dezvolta noi capacități în domeniul calculului, comunicării și detectării. Aceste tehnologii sunt la inceput, deschid noi directii de cercetare, dar au potențialul de a revoluționa diverse domenii: seuritatea datelor, asistența medicală, finanțe, securitatea națională etc.

Arii (cheie) de explorat in domeniul tehnologiilor cuantince:

1. **Quantum Sensing**: Senzorii cuantici sunt caracterizati de sensibilitate și precizie foarte bune în măsurarea mărimilor fizice precum timpul, câmpurile magnetice și gravitația. Aplicatiile în domeniul pot fi in domenii precum: sănătate, monitorizarea mediului,

navigație etc. Interferometria cu atomi reci este explorată pentru aplicații în spațiu și apărare.

2. **Quantum Communication**: Distribuția cheilor cuantice (QKD) utilizează mecanica cuantică pentru a permite o comunicare securizată prin detectarea tentativelor de interceptare. Nokia cercetează criptografia rezistentă la procese cuantice și distribuția cheilor cuantice pentru a spori securitatea.
3. **Quantum Computing** - Acest domeniu își propune să creeze computere care pot efectua calcule mult dincolo de capacitățile computerelor clasice, utilizând qubiți, care pot exista în mai multe stări simultan datorită suprapunerii. Companii precum IBM sunt lideri în dezvoltarea de hardware cuantic cu procesoare de qubiți.
4. **Retele cuantice**: își propun să conecteze computerele cuantice și senzorii.

Avantaje ale folosirii tehnologiilor cuantice:

- Potential economic – pana in 2035, trilioane de dolari
- Schimbari in societate – prin utilizarea tehnologiilor cuantice se au in vedere provocari in domenii precum: schimbări ale climei, noi materiale, noi medicamente.
- Securitate nationala – tehnologiile cuantice, în special calculul și comunicațiile cuantice, au implicații pentru securitatea națională, inclusiv criptografia și supravegherea.
- Polici publice - guvernele și factorii de decizie politică sunt implicați activ în dezvoltarea de strategii pentru a încuraja dezvoltarea tehnologiilor cuantice, a aborda riscurile potențiale și a asigura o dezvoltare responsabilă.

Provocari / Oportunitati:

- Construirea și scalarea computerelor și rețelelor cuantice rămâne o provocare semnificativă.
- Considerații etice: dezvoltarea și implementarea tehnologiilor cuantice ridică întrebări etice privind confidențialitatea, securitatea și potențiala utilizare abuzivă.
- Colaborare internațională: colaborarea internațională este crucială pentru partajarea cunoștințelor, resurselor și celor mai bune practici în domeniu.

Subiectul evident nu este complet epuizat / tratat, putem gasim mai multe detalii despre Tehnologiile Quantum aici - https://www.nokia.com/quantum/quantum-technologies-explained/

C. OBIECTIVE / METODOLOGIE

OBIECTIVE:

- ***Dezvoltare platformă web3 descentralizată – proiectata si implementata, bazată pe tehnologiile Blockchain – inclusiv contracte inteligente (smart contracts) si Quantum, utila pentru educație si diplomatie.***

Cu privire la ***metodologia cercetării***, în cadrul proiectului se vor folosi ***instrumente şi metode de cercetare ştiinţifică***, astfel:

- *modelarea si simularea software.*
- *analiza comparativă.*
- *cercetarea bibliografică.*
- *chestionarul.*
- *studiul de caz.*
- *focus-grupul.*
- *cercetarea structurată (bazată pe metode cantitative) dar şi cercetarea nestructurată (bazată pe metode calitative);*

Aceste instrumente şi metode de cercetare ştiinţifică sunt integrate în planul de cercetare, care conţine activităţi, împreună cu perioada de realizare.

D. ACTIVITATI / REZULTATE / CE URMEAZA?

Proiectarea unei platforme descentralizate utile pentru cursuri de diplomatie stiintifica - unde asistenții si profesorii pot încărca și gestiona în siguranță materialele cursurilor, instruirilor sau temelor. ***Aceasta etapa a fost finalizata.***

Implementarea platformei descentralizate – suntem la versiunea alpha a platformei, pentru care am testat cativa indicatori / metrici de performanta.

Urmeaza versiunea beta si finala a aplictatiei si analiza ei din punct de vedere al indicatorilor de performanta (timpi, scalabilitate, etc) - detalii in urmatorul raport R3 – 2026.

Abordarea este una hibrida:

1. autentificare clasică folosind JPAKE și
2. schimb simulat de ***chei cuantice*** (prin intermediul IBM Qiskit Runtime) pentru o securitate sporită a sesiunii.

Conținutul este stocat în afara lanțului de date prin intermediul IPFS (Interplanetary File System - https://docs.ipfs.tech/), metadatele și CID-urile fiind stocate pe un blockchain folosind contracte inteligente (Solidity).

Scopul este de a simula securitatea îmbunătățită cuantic în cadrul unei arhitecturi de stocare scalabile și descentralizate - ***Arhitectură hibridă (clasică - cuantică) pentru platformă educațională descentralizată.***

Arhitectura noastră permite ***autentificarea îmbunătățită cuantic*** - oferind o alternativă experimentală, dar orientată spre viitor, la sistemele complet clasice.

1. ***Descrierea arhitecturii***

Arhitectura constă dintr-o structură ***modulară, stratificată***, care cuprinde componentele

- ***frontend,***
- ***backend,***
- ***integrarea serviciilor cuantice,***
- ***stocarea descentralizată (IPFS) și***
- ***registrul blockchain.***

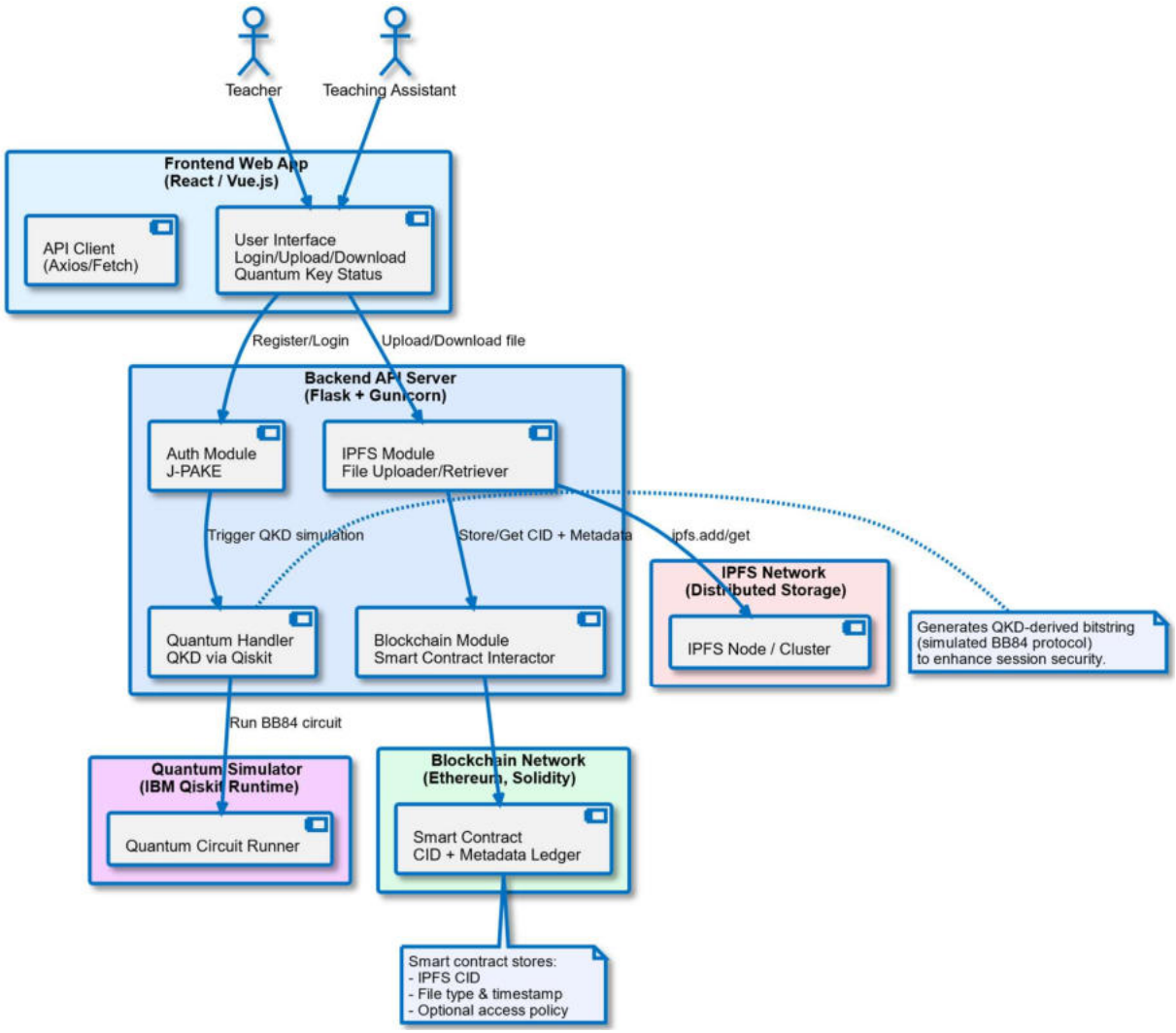

Figura 1 Arhitectura generală a sistemului Platformei Descentralizate (DP) – propunerea noastră

Backend-ul orchestrează comunicarea securizată între straturi, asigurându-se că acțiunile utilizatorilor (cum ar fi conectarea și încărcarea fișierelor) traversează atât fazele de autentificare clasică, cât și cele ale cheilor cuantice simulate înainte de a interacționa cu subsistemele de stocare sau blockchain. Această arhitectură echilibrează în mod intenționat performanța (primitive clasice) și experimentarea în cercetare (simulare cuantică), oferind o platformă pentru viitoare îmbunătățiri cuantice, odată ce QKD-ul hardware va deveni practic.

2. ***Fluxul de lucru secvențial pentru autentificare, încărcarea fișierelor și recuperarea acestora:***

Accentul este pe autentificare, simulare cuantică și ciclul de viață al continutului / fișierelor (încărcare, stocare, recuperare).

Utilizatorii – profesori / asistenti / studenti sunt autentificați clasic folosind protocolul JPAKE (asigură autentificarea reciprocă și rezistența la atacul Man in the Middle), urmat de simularea unui proces de schimb de chei cuantice (BB84) prin intermediul Qiskit Runtime de la IBM. Acest hash de șir de biți generat cuantic este utilizat pentru a îmbunătăți token-urile criptografice la nivel de sesiune.

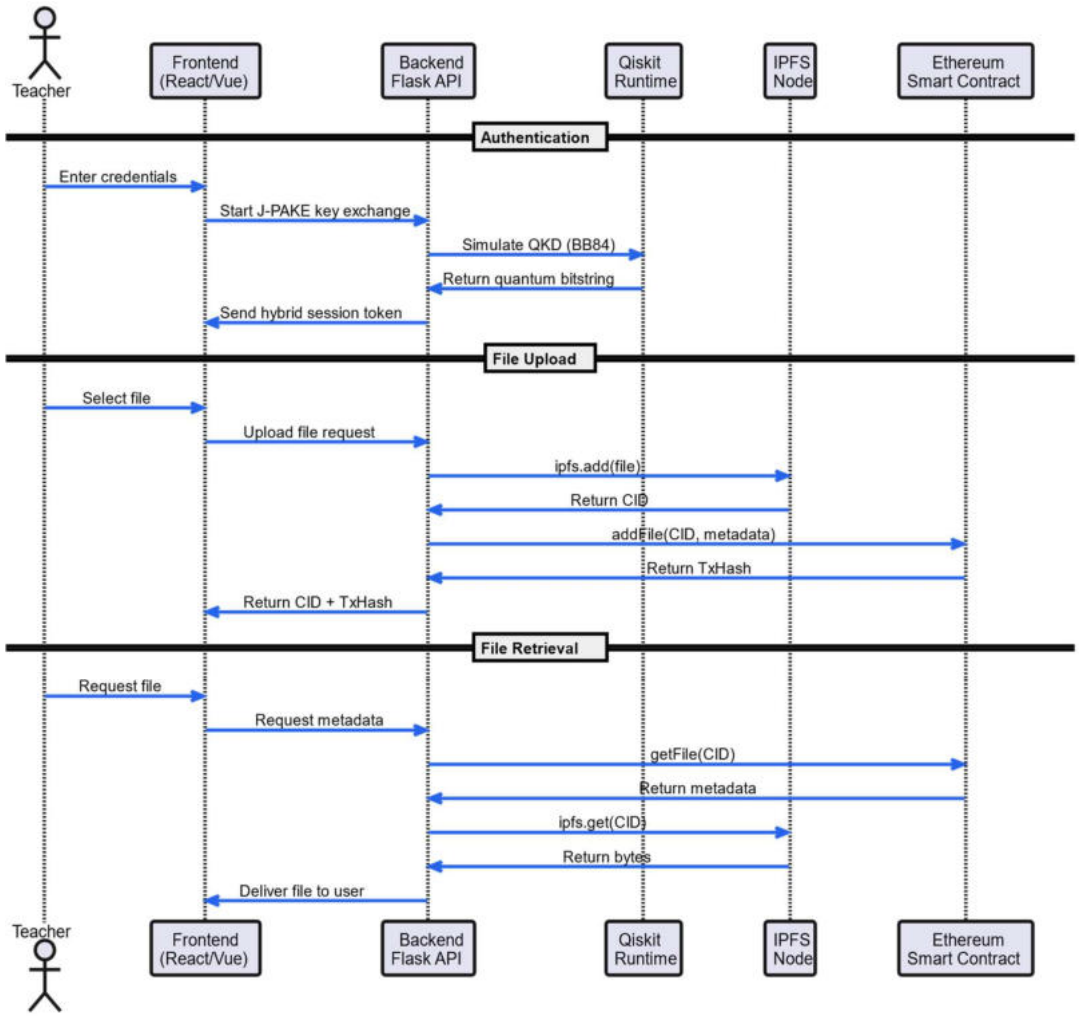

Figura 2 Fluxul secvențial pentru autentificare, încărcarea fișierelor și recuperarea acestora – propunerea noastră

3. *Fluxul de activități end-to-end al platformei*

Fișierele de continut sunt încărcate prin frontend, stocate în IPFS și legate de metadatele stocate într-un registru blockchain prin contracte inteligente. Accesul la fișiere este guvernat de recuperarea CID-urilor din blockchain și rezolvarea acestora prin rețeaua IPFS. Metadatele (tipul fișierului, utilizatorul, marcajul temporal, CID-ul) sunt stocate pe blockchain, asigurând auditabilitatea fișierelor și rezistența la manipulare. Acest flux este relevant în special în mediile academice unde autenticitatea datelor, integritatea descentralizată și pregătirea cuantică orientată spre viitor sunt esențiale.

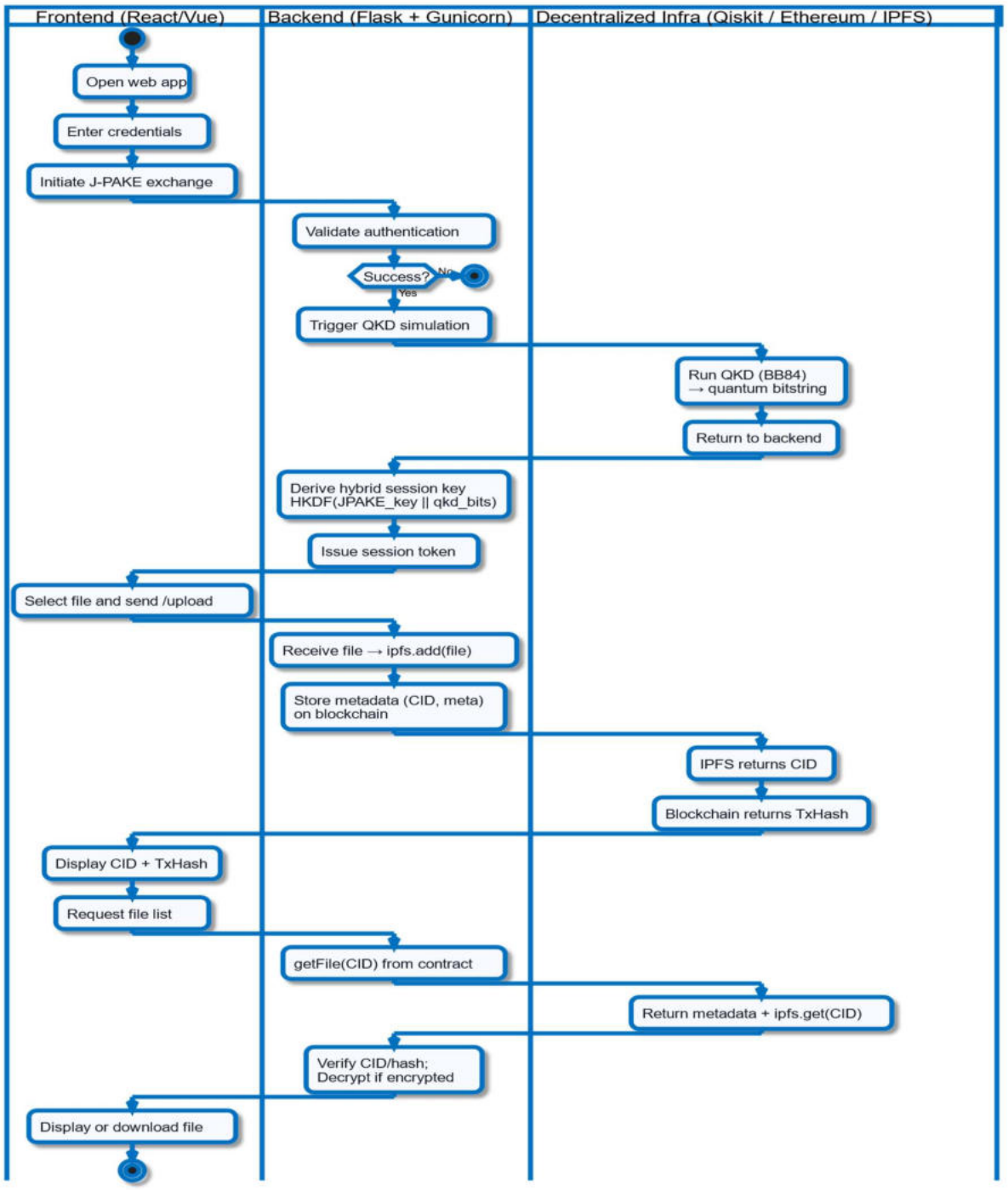

Figura 3 Fluxul de activități end-to-end al platformei – propunerea noastra

Utilizatorilor li se oferă feedback vizual în timp real cu privire la starea lor de autentificare, progresul încărcării, stadiul simulării cheii cuantice și acțiunile legate de blockchain.

4. *Diagrama componentelor Frontend-Backend și interacțiunea API-ului REST*

Frontend-ul comunică în siguranță cu API-ul backend folosind apeluri REST autentificate (securizate cu HTTPS și token-uri de sesiune derivate parțial din chei cuantice simulate).

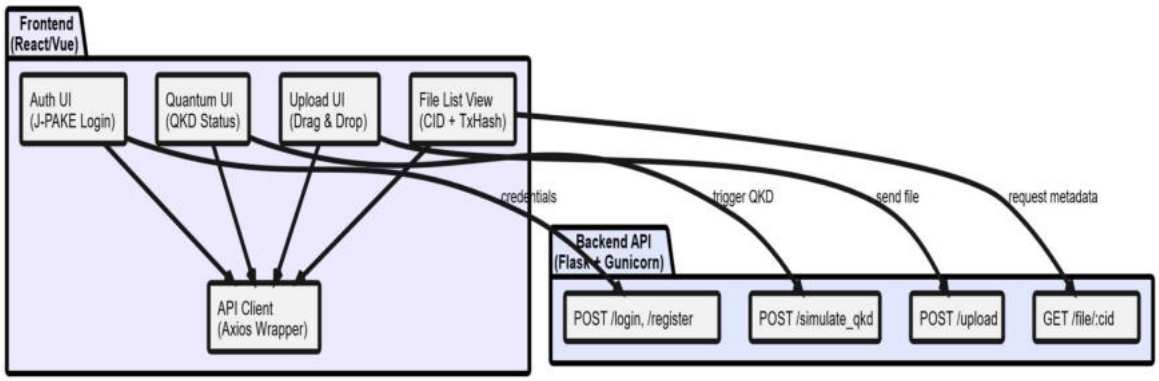

Figura 4 Diagrama componentelor Frontend-Backend și interacțiunea API-ului REST - propunerea noastră

5. *Implementarea platformei – versiunea Alpha*

Arhitectura propusă este implementată ca un prototip web hibrid modular ***Python-JavaScript,*** format din trei componente principale:

- interfața web,
- serverul API dezvoltat în Flask și deservit prin Gunicorn și
- infrastructura descentralizată bazată pe Ethereum și IPFS.

În ceea ce privește interfața web, am optat pentru React împreună cu Vue, în timp ce apelurile REST sunt gestionate prin Axios, care gestionează starea aplicației prin intermediul unor token-uri de sesiune temporare.

Backend-ul coordonează:

- autentificarea,
- criptarea fișierelor și
- interacțiunea cu stratul de stocare distribuit implementat prin IPFS, unde sunt stocate fișierele criptate, asigurând astfel integritatea prin CID-ul generat.

Un aspect important de evidențiat este faptul că ***se generează o cheie nouă pentru fiecare sesiune***, ceea ce înseamnă că compromiterea unui singur token nu acordă acces la nicio resursă.

Pentru a ilustra componenta de ***diplomație științifică si cibernetica digitală integrată în platformă***, am dezvoltat ***două scenarii*** de interacțiune reprezentative la nivel de interfață web, prezentate schematic în figurile 5 și 6.

Primul scenariu, prezentat în Fig. 5, are ca obiectiv nu doar ***securizarea procesului de autentificare***, ci și consolidarea încrederii utilizatorilor prin transparența etapelor interne (formarea cheii de sesiune hibride rezultată din combinarea protocoalelor J-PAKE și QKD).

Al doilea scenariu, prezentat în Fig. 6, descrie procesele de încărcare și validare a fișierelor academice prin transparență operațională, demonstrând ***un model de diplomație cibernetică-științifică*** în care securitatea și responsabilitatea academică devin proprietăți verificabile tehnologic.

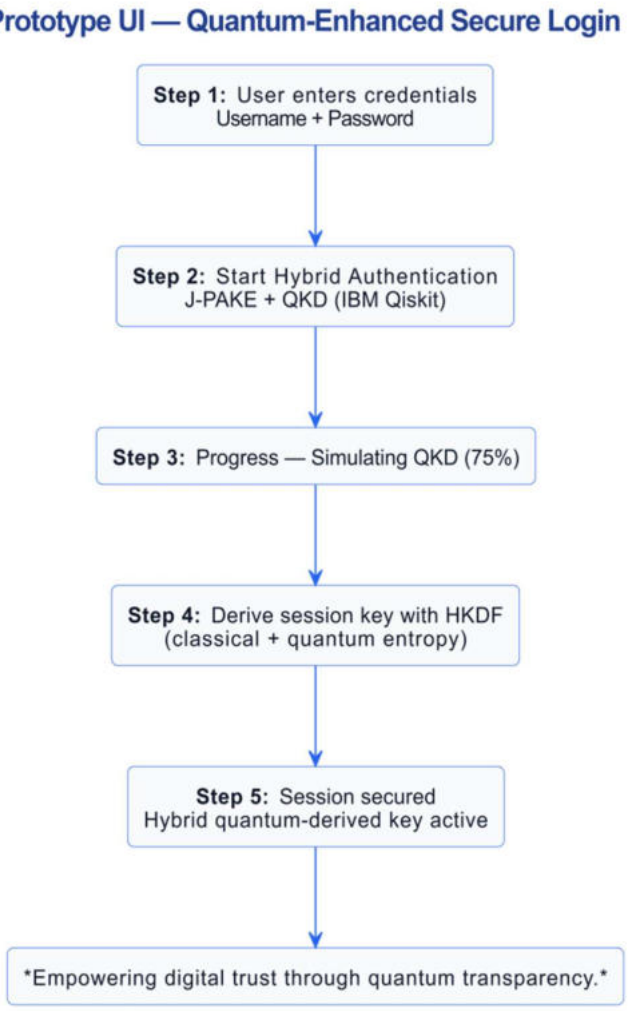

Figura 5 Autentificare securizată îmbunătățită cuantică: Autentificare transparentă prin schimb de chei hibrid clasic-cuantic

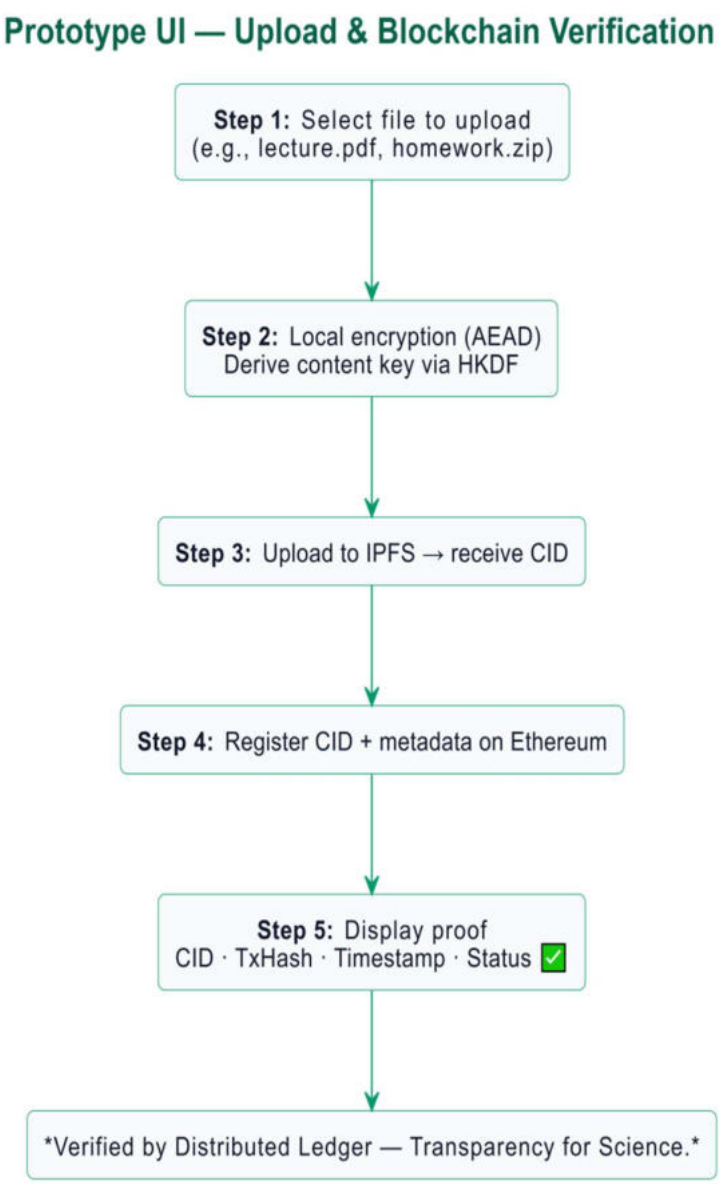

Figure 6 Încărcare descentralizată și verificare blockchain: Integritate academică prin încredere distribuită

6. *Metrici de performanta pentru varianta implementata – Alpha*

Pentru a evalua performanța preliminară a aplicației web hibride propuse, am implementat o simulare Python care generează valori aproximative pentru principalele operațiuni ale sistemului.

După cum se arată în Fig. 7, cea mai mare contribuție la ***latența autentificării provine din faza de distribuție a cheii cuantice, care necesită aproximativ 0,6 până la 1,5 secunde per sesiune***, în timp ce costul suplimentar introdus prin derivarea cheii de sesiune prin HKDF este neglijabil. Prin urmare, pentru fișiere mici, procesul de autentificare hibridă rămâne sub 2 secunde, demonstrând fezabilitatea acestei metode într-un context educațional descentralizat.

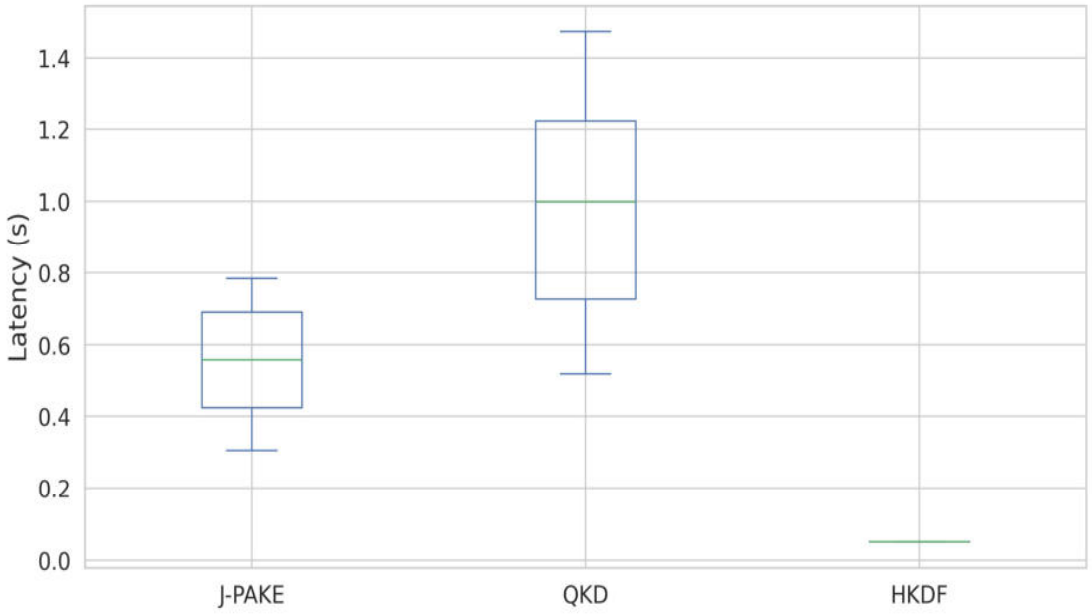

Figura 7 Latența de autentificare - Distribuție comparativă pentru J-PAKE, QKD și HKDF

În ceea ce privește încărcarea fișierelor, latența totală crește proporțional cu dimensiunea fișierului datorită scalării liniare a procesului de criptare. După cum se arată în Fig. 8, pentru fișiere mici, sub 100KB, timpul mediu necesar pentru criptare și înregistrare rămâne sub 2 secunde, în timp ce pentru fișiere de până la 1MB, latența de încărcare crește la aproximativ 4-5 secunde în principal, din cauza timpului de confirmare a tranzacțiilor Blockchain. Acest lucru sugerează un blocaj moderat introdus de natura descentralizată a operațiunilor de scriere.

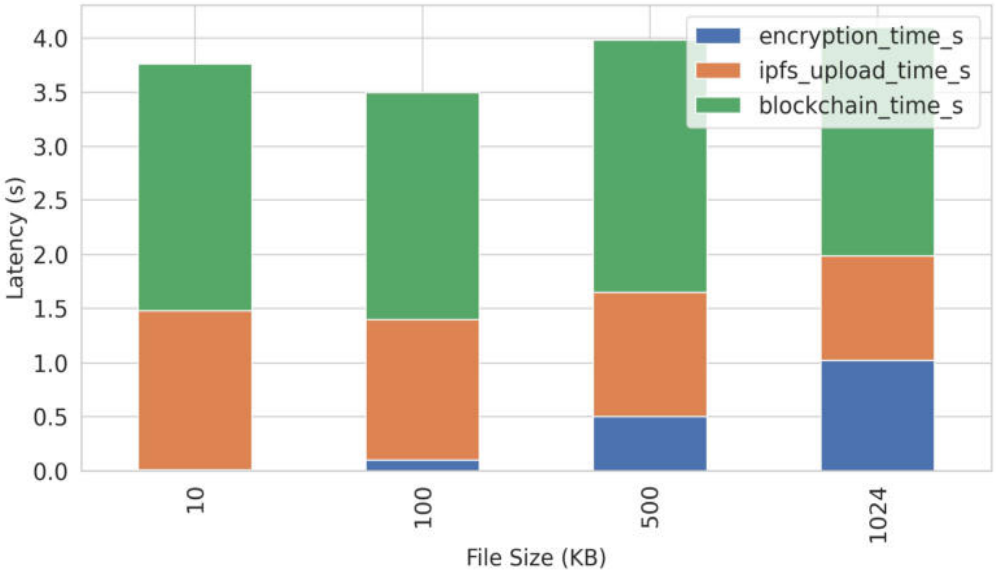

Figura 8 Componente de latență a încărcării în funcție de dimensiunea fișierului - Impactul criptării, IPFS și operațiunilor Blockchain

În schimb, în Fig. 9 observăm că factorul dominant este latența de recuperare a datelor din IPFS, care variază între 0,5 și 1,9 secunde, în timp ce descărcările de fișiere necesită doar un timp minim de decriptare, cu valori sub 1 secundă, confirmând eficiența schemei de criptare AEAD utilizată. Astfel, chiar și pentru fișiere de până la 1 MB, procesul complet de descărcare rămâne sub pragul de 2,5 secunde.

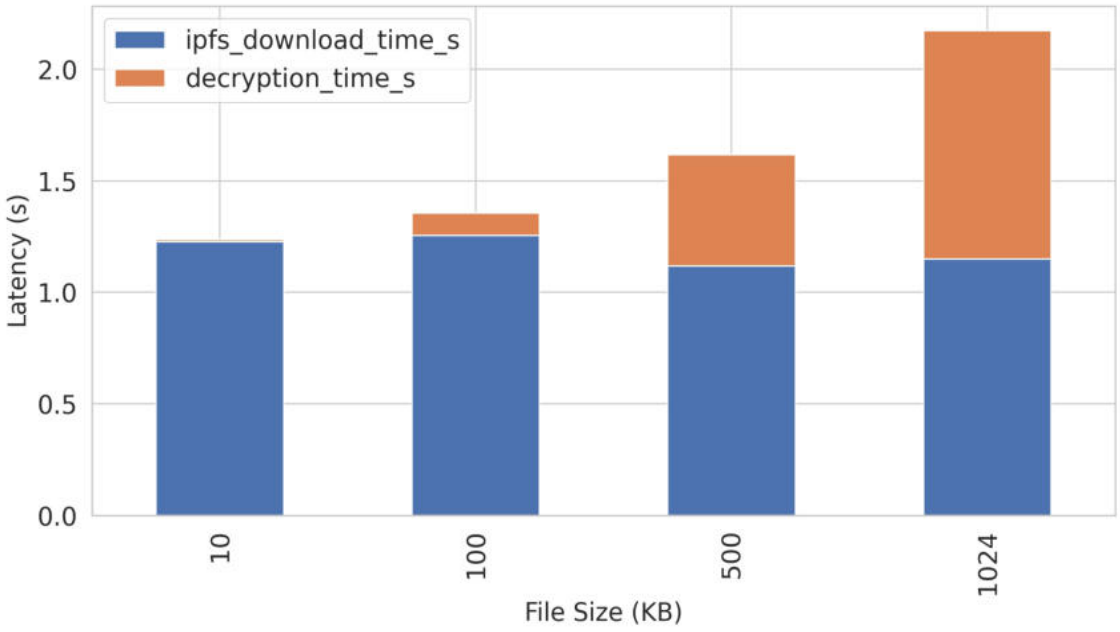

Figura 9 Componente de latență pentru descărcare după dimensiunea fișierului - Timp de recuperare și decriptare IPFS

Graficele din Fig. 10 și Fig. 11 arată că principalul factor care limitează performanța este rețeaua IPFS, în special în timpul încărcărilor de fișiere, unde sunt implicate interacțiuni cu Blockchain-ul. Debitul de transfer variază în funcție de dimensiunea fișierului, ajungând până la aproximativ 300KB/s pentru încărcări și 600KB/s pentru descărcări.

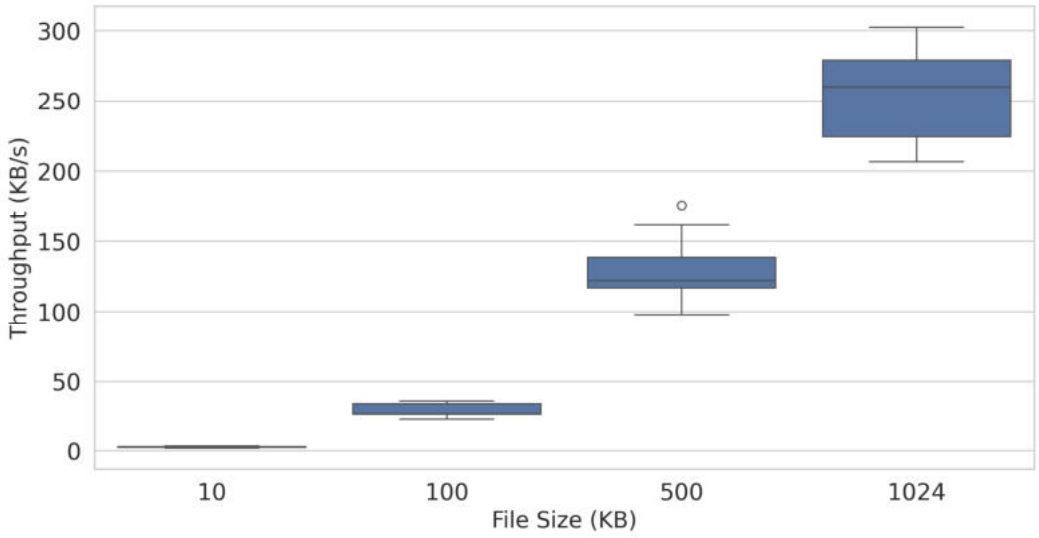

Figura 10 Upload Throughput in functie de dimensiunea fisierului

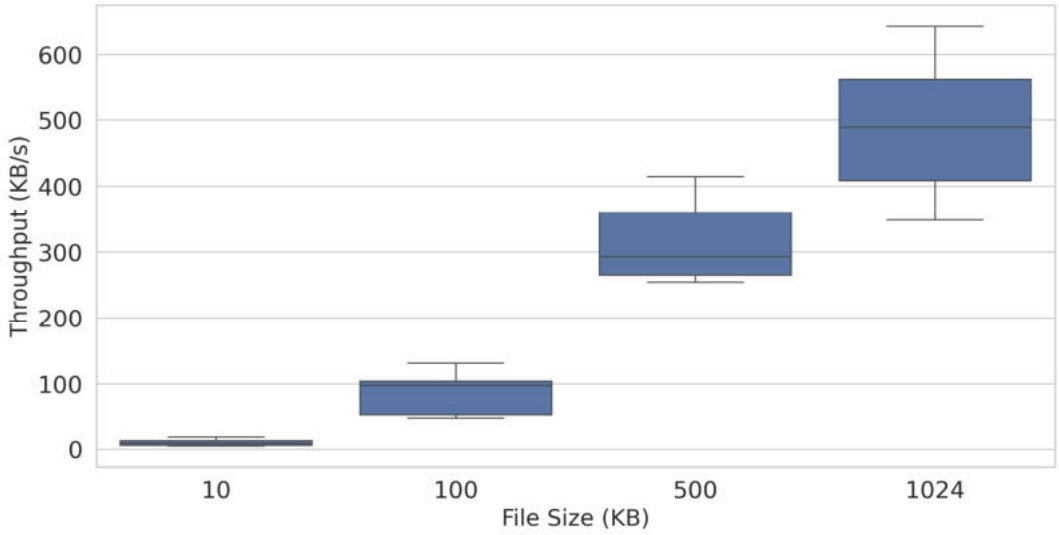

Figura 11 Download Throughput in functie de dimensiunea fisierului

Conform Fig. 12, arhitectura hibridă propusă este operațională în faza de simulare alfa, atingând o rată de succes a încărcării fișierelor de ~95% și aproape 100% pentru descărcări pe un eșantion de 50 de fișiere cu dimensiuni în intervalul 10-1024KB. Rata de succes a încărcării mai mică poate fi atribuită instabilității ocazionale din pipeline-ul criptografic pentru fișierele mai mari, precum și latenței IPFS în timpul stocării descentralizate.

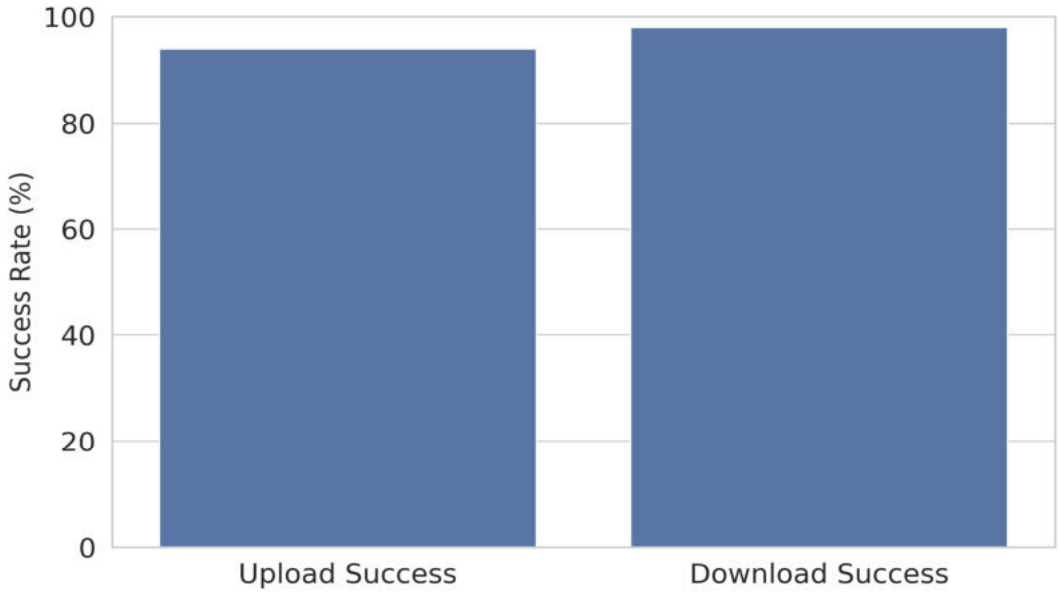

Figure 12 Ratele de succes ale încărcării și descărcării - Stabilitatea platformei în simularea Alpha

Concluzii:

1. Autentificarea clasică este securizată prin protocolul JPAKE, care utilizează dovezi zero-knowledge pentru a permite celor două părți să stabilească un secret partajat pe un canal nesigur,

fără a dezvălui parola sau hash-ul acesteia. Această alegere asigură robustețe împotriva atacurilor de dicționar offline și garantează autentificarea reciprocă fără stocarea centralizată a parolelor.

2. Pentru a extinde această securitate fundamentală, sistemul încorporează un mecanism simulat de distribuție a cheilor cuantice folosind mediul Qiskit Runtime de la IBM.

Considerațiile de scalabilitate au fost abordate prin descărcarea datelor voluminoase (cum ar fi prelegerile video sau modulele de instruire) către IPFS. Doar identificatorii de conținut (CID) și metadatele sunt stocate pe blockchain. Această separare între sarcina utilă a datelor și metadate permite disponibilitatea fără a suprasolicita blockchain-ul sau a genera costuri ridicate ale tranzacțiilor.

3. O listă cu toate tehnologiile și framework-urile care vor fi utilizate în platforma noastră hibridă descentralizată de autentificare și stocare, îmbunătățită cu ajutorul tehnologiei cuantice: **React, Vue, Flask, Gunicorn, IBM Qiskit SDK, Solidity, Infura, Ethereum, IPFS.**

CE URMEAZA?

- Lucram la implementarea platformei in varianta descrisa mai sus - versiunea Beta.

- Analiza oportunităţii realizarii unui workshop / mesa rotunda / focus-grup în scopul creșterii nivelului de instruire şi conştientizare asupra noilor tehnologii, inclusiv asupra tehnologiilor de tip Blockchain pentru diplomatie. Se doreste promovarea dar și consolidărea notiunilor de diplomatie stiintifica, clasica si cibernetica.

E. INDICATORI - ARTICOLE

Articole PUBLICATE – conferinte ISI

1. Maria-Elena ENACHE, ***Bogdan Dumitru ȚIGĂNOAIA***, Alexandru PETRISOR, Georgiana MOICEANU, Andrei NICULESCU, *IoT Integration in Educational Institutions for a Green and Digital Transition Case Study at POLITEHNICA University of Bucharest*, The 12th International Conference of Management and Industrial Engineering – ICMIE 2025, https://icmie-faima-upb.ro/, ISI indexed (***past editions were indexed***) in the Clarivate Analytics, indexed in the ProQuest international database, Bucharest, Romania, 6-7 of November, 2025.

2. Maria-Elena ENACHE, ***Bogdan Dumitru ȚIGĂNOAIA***, Alexandru PETRISOR, Georgiana MOICEANU, Olivia Doina NEGOITA, *Research Instrument for Assessing the Integration Level of IoT Technologies for the Green and Digital Transition in Organizations*, The 12th International Conference of Management and Industrial Engineering – ICMIE 2025, https://icmie-faima-upb.ro/, ISI indexed (***past editions were indexed***) in the Clarivate Analytics, indexed in the ProQuest international database, Bucharest, Romania, 6-7 of November, 2025.

Articole (trimise spre evaluare – in curs de recenzie) – revistă cotata ISI

1. **Bogdan TIGANOAIA**, Petrisor-Ionut ANGHEL, **Doina BANCIU** – coautori, *A Decentralized Platform Leveraging Blockchain and Quantum-Secure Communication for Scientific Diplomacy and Trusted Resource Sharing, trimis spre recenzie la* revista cotata Clarivate Analytics**.**

F. BIBLIOGRAFIE

[1] What is diplomacy?, https://www.cyber-diplomacy-toolbox.com/Diplomacy.html, accesat la 30.06.2025.

[2] What is cyber diplomacy?, https://www.cyber-diplomacy toolbox.com/Cyber_Diplomacy.html, accesat la 30.06.2025

[3] **Bogdan TIGANOAIA**, Petrisor-Ionut ANGHEL, **Doina BANCIU -** coautori, *A Decentralized Platform Leveraging Blockchain and Quantum-Secure Communication for Scientific Diplomacy and Trusted Resource Sharing, trimis spre recenzie la* revista cotata Clarivate Analytics**.**

[4] What is science diplomacy, https://www.eeas.europa.eu/eeas/what-science-diplomacy_en, accesat la 30.06.2025

[5] **TIGANOAIA, B.**; Alexandru, G.-M. 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

[6] 6 Biggest Blockchain Companies. Available online: https://www.investopedia.com/10-biggest-blockchain-companies-5213784 (accessed on 2 May 2023).