

UNIVERSITATEA NAȚIONALĂ DE ȘTIINȚĂ ȘI TEHNOLOGIE
POLITEHNICA BUCUREȘTI
FACULTATEA DE AUTOMATICĂ ȘI CALCULATOARE
DEPARTAMENTUL DE CALCULATOARE



LUCRARE DE DISERTAȚIE

Sistem Descentralizat de Verificare
a Identității Digitale

Angelo-Gabriel BARBU

Coordonator științific:

Lect. Dr. Dumitru-Clementin CERCEL

BUCUREȘTI

2025

NATIONAL UNIVERSITY OF SCIENCE AND TECHNOLOGY
POLITEHNICA BUCHAREST
FACULTY OF AUTOMATIC CONTROL AND COMPUTER
SCIENCE
COMPUTER SCIENCE AND ENGINEERING DEPARTMENT



DISSERTATION THESIS

Decentralised Digital Identity
Verification System

Angelo-Gabriel BARBU

Thesis advisor:

Lect. Dr. Dumitru-Clementin CERCEL

BUCHAREST

2025

CUPRINS

1	Introducere	1
1.1	Identitatea Digitală în Contextul Actual	1
1.2	Tendința Ascendentă a Soluțiilor Descentralizate	1
1.3	Motivație	1
1.4	Obiective	2
2	State of the Art	3
2.1	Evoluția Sistemelor de Identitate Digitală	3
2.2	Tehnologia Blockchain ca un Fundament pentru Identitatea Digitală	3
2.3	Principii de Identitate Autosuverană	3
2.4	Experiența Utilizatorului și Adoptia Portofelelor Digitale de Identitate	4
2.5	Standarde W3C pentru Identitatea Descentralizată	4
2.6	Protocoale de Interoperabilitate – DIDComm și Hyperledger Aries	4
2.7	Mecanisme de Revocare și Status al Credențialelor	5
2.8	Interoperabilitatea Inter-Chain și Straturile de Identitate Agnostice	5
2.9	Verificarea cu Divulgare Zero – zk-SNARK/zk-STARK în SSI	5
2.10	Identitatea Digitală în Contextul European: eIDAS 2.0, EBSI și ESSIF	6
2.11	Guvernare, Cadre de Încredere și Reglementare	6
2.12	Identitatea Mobilă și Standardul ISO 18013-5	6
2.13	Platforme și Inițiative de Referință	7
2.14	Securitatea și Confidențialitatea în Sisteme de Identitate Descentralizate	7
2.15	Lacune și Oportunități	7
3	Modelul proiectului	8
3.1	Stiva de tehnologii	9

3.1.1	Sistem Blockchain și Contractul Inteligent	9
3.1.2	Contractul Inteligent	10
3.1.3	Criptare și semnături	11
3.1.4	Zero-Knowledge Proofs (ZKPs)	11
3.2	Software as a Service (SaaS)	12
3.2.1	Middleware/API	12
3.2.2	Componenta Vizuală	12
4	Workflow-ul sistemului și Experiența Utilizatorului	13
4.1	Workflow-ul Sistemului de Identități Digitale	13
4.2	Scenarii de funcționare	14
4.3	Proprietăți cheie ale workflow-ului	21
5	Metricile de Analiză a Performanțelor și Analiza Rezultatelor	22
5.1	Metricile de Analiză a Performanțelor	22
5.2	Ecosistemului Ethereum ca Blockchain pentru Soluția Propusă	22
5.3	Analiza Rezultatelor	26
5.3.1	Testarea Securității	26
5.3.2	Evaluarea Confidențialității	27
5.3.3	Testarea Scalabilității	28
5.3.4	Testarea Utilizării - Proof of Concept	28
6	Metodologia de Cercetare și Contribuții Personale	33
6.1	Metodologia de Cercetare	33
6.2	Contribuțiile Personale	33
6.2.1	Contribuțiile Teoretice	33
6.2.2	Contribuțiile Practice	34
7	Concluzii, Rezultate și Plan de Cercetare Viitor	35
7.1	Concluzii	35
7.2	Rezultate	35

7.3 Plan de Cercetare Viitor	35
--	----

SINOPSIS

În contextul digitalizării, managementul identității digitale prezintă diverse provocări, în special cu privire la confidențialitatea, securitatea și autonomia fiecărui individ asupra datelor sale personale. Această lucrare de cercetare își dorește să introducă un Sistem Descentralizat de Verificare a Identității Digitale, cu ajutorul avantajelor tehnologiei **blockchain** pentru a aborda provocările enumerate anterior. Prin adoptarea unor principii de tip **Self-Sovereign Identity (SSI)**, acest sistem oferă posibilitatea fiecărei persoane de a-și crea, administra și distribui datele sale de identitate, fără a necesita o autoritate centralizată, oferind un grad ridicat de control și confidențialitate.

Lucrarea de cercetare abordează o metodologie de cercetare mixtă, combinând articolele multiple din domeniu, design și dezvoltare de sisteme și teste empirice pentru a evalua sistemul propus. Platforma de dezvoltare blockchain **Ethereum** a fost aleasă datorită ecosistemului său stabil și a suportului pentru contracte inteligente, esențiale pentru managementul identității digitale într-un context descentralizat.

Planul de cercetare viitor constă în continuarea cercetării pentru a analiza într-o manieră mai detaliată scalabilitatea soluțiilor, mecanisme avansate de protecție a confidențialității și principii de design centrate pe utilizator, având ca scop obținerea unui sistem rafinat și încurajarea adopției la scară largă. Lucrarea de față își dorește atât să crească interesul cu privire la managementul descentralizat al identității digitale, cât și să stabilească fundația pentru inovații viitoare ce au ca prioritate drepturile și nevoile indivizilor în mediul digital.

Lucrarea va urmări implementarea unui prototip ce are la bază un sistem descentralizat de verificare a identității digitale, cu scopul testării și analizei unui astfel de sistem.

Mai mult, în cadrul lucrării se va demonstra validitatea prototipului ca potențială soluție în ceea ce privește problema identității digitale prin implementarea unui **Proof of Concept (PoC)** simplist, demonstrând, astfel, aplicabilitatea sistemului într-un mediu real.

Prototipul prezentat în lucrare poate fi găsit în acest repository [GitHub](#).

ABSTRACT

In the context of digitalization, managing digital identities presents multiple challenges, especially regarding the confidentiality, security and the autonomy of individuals over their personal data. This dissertation aims to introduce a Decentralised Digital Identity Verification System, by employing the advantages of **blockchain** technology to address the challenges mentioned before. By adopting **Self-Sovereign Identity (SSI)** principles, this system allows each

person to create, manage and share their identity data, removing the need of a centralised authority, providing a high degree of control and confidentiality.

The research paper adopts a mixed research methodology, combining multiple domain articles, system design and development and empirical testing to evaluate the proposed system. The **Ethereum** blockchain development platform was chosen based on its stable ecosystem and support for smart contracts, which are essential for managing digital identities in a decentralised context.

Further research is recommended for a thorough analysis of the solution's scalability, advanced privacy preserving mechanisms and user-centered design principles, aiming to achieve a refined system and encourage large-scale adoption. This dissertation aims not only to increase interest in decentralized digital identity management but also to establish the foundation for future innovations that prioritize individuals' rights and needs in the digital environment.

The research paper will pursue the implementation of a prototype based on a decentralized digital identity verification system, with the goal of testing and analyzing such a system.

Furthermore, the dissertation will demonstrate the validity of the presented propotype as a viable solution to the digital identity problem by implementing a simplistic **Proof of Concept (PoC)**, proving the application of such a system in a real world environment.

The presented prototype can be found in this GitHub repository.

1 INTRODUCERE

1.1 Identitatea Digitală în Contextul Actual

În era digitală în care ne aflăm, identitatea joacă un rol esențial cu privire la modul în care interacționăm cu serviciile online. De la banking la social media, o identitate digitală verificabilă reprezintă fundamentul încrederii și al securității. Cu toate acestea, sistemele tradiționale de management al identității digitale sunt centralizate, oferind un control sporit asupra datelor personale unui grup restrâns de corporații și entități guvernamentale. Această centralizare duce la probleme multiple, precum breșe de confidențialitate, furturi de identitate și lipsa autonomiei utilizatorului asupra datelor sale personale.

1.2 Tendința Ascendentă a Soluțiilor Descentralizate

Limitările cauzate de sistemele de management a identității digitale au condus la un interes sporit asupra soluțiilor descentralizate. Tehnologia blockchain, recunoscută pentru rolul său esențial în piața de criptomonede, reprezintă o soluție viabilă pentru rezolvarea problemei identității digitale. Aceasta introduce conceptul de Identitate Autosuverană (Self-Sovereign Identity/SSI), o paradigmă în care indivizii au control asupra propriei lor identități, fără a fi legați de supravegherea unei autorități centrale. O astfel de abordare îmbunătățește atât confidențialitatea și securitatea, dar oferă și o schimbare în dinamica puterii asupra datelor, oferind utilizatorului control.

1.3 Motivație

Motivația acestui proiect este dată în primul rând de problemele cu privire la breșe de securitate asupra datelor și a furtului identității, evidențiind vulnerabilitatea sistemelor actuale de identitate digitală. Doar în anul 2021, lumea digitală a întâmpinat o creștere de 17% în breșe de securitate, afectând milioane de utilizatori la nivel mondial.

În al doilea rând, tendința ascendentă de a întări confidențialitatea individului ca un drept uman fundamental face apel la un sistem ce are ca prioritate controlul utilizatorului asupra datelor sale personale. Aceste probleme subliniază urgența de a obține o abordare mult mai sigură și centrată asupra confidențialității în contextul management-ului identității digitale.

1.4 Obiective

Lucrarea de disertatie are ca scop cercetarea **State-of-the-Art (SotA)** a sistemelor de identitate digitală și a integrării Blockchain în cadrul acestora, conturarea unei arhitecturi și a unei implementări pentru un Sistem Descentralizat de Verificare a Identității Digitale folosind tehnologia blockchain, dar si testarea și demonstrarea aplicabilității unui astfel de sistem. Obiectivele specifice sunt următoarele:

1. Utilizarea tehnologiei blockchain pentru a dezvolta un sistem sigur, de neatinș pentru managementul identității digitale;
2. Incorporarea principiilor de identitate autosuverană, oferind utilizatorilor posibilitatea de a crea, administra și distribui informațiile cu privire la identitatea lor într-o manieră anonimă.
3. Implementarea unor mecanisme de conservare a confidențialității ce oferă distribuie selectivă a datelor personale.
4. Integrarea sistemului descentralizat și a mecanismelor și principiilor incorporate într-o platformă de tip **Software as a Service (SaaS)** pentru demonstrarea aplicabilității sistemului într-o manieră practică, relevantă contextului tehnologic actual;
5. Demonstrarea aplicabilității unui astfel de sistem prin implementarea unui **Proof of Concept**;
6. Testarea robusteții și a performanței sistemului;
7. Crearea unui plan de cercetare viitor și a posibilelor îmbunătățiri ce pot fi aduse sistemului prezentat în cadrul acestei lucrări.

2 STATE OF THE ART

2.1 Evoluția Sistemelor de Identitate Digitală

Sistemele de identitate digitală au evoluat semnificativ pe parcursul ultimelor decenii, plecând de la o colecție de scheme simpliste de tip nume utilizator-parolă, ajungând, astfel, la modele mult mai complexe și centralizate controlate de corporații și guverne. În lucrarea [15] această evoluție este analizată și se evidențiază creșterea complexității tacticilor de furt al identității și necesitatea de a avea soluții mult mai sigure de management al identității. Cu toate acestea, astfel de sisteme centralizate sacrifică deseori confidențialitatea și gradul de control al utilizatorului, ducând la o problemă răspândită cu privire la folosirea eronată a datelor personale.

2.2 Tehnologia Blockchain ca un Fundament pentru Identitatea Digitală

Evoluția accelerată a **tehnologiei blockchain** a dus la apariția unei paradigme noi cu privire la managementul identităților digitale. Proprietăți cheie ale blockchain, precum imutabilitatea datelor, descentralizarea și transparența validează această tehnologie ca fiind soluția ideală pentru a obține sisteme de identitate sigure, cu un grad de confidențialitate ridicat.

În mod indirect, celebra lucrare a lui Satoshi Nakamoto [23] a pus bazele unei potențiale aplicații a tehnologiei blockchain în diverse domenii, nu doar în criptomonede. Mai mult, în lucrarea [28] este demonstrată în mod practic utilizarea blockchain în implementarea unor sisteme de identitate digitală sigure cu grad mare de confidențialitate, eliminând nevoia unei autorități centralizate.

2.3 Principii de Identitate Autosuverană

Paradigma de **Identitate Autosuverană** (Self-Sovereign Identity/SSI) a dus la migrarea funcționalităților și proprietăților modelelor de identitate digitală spre avantajul utilizatorului. În articolul [10] este prezentat conceptul de SSI ca fiind o abordare în care persoanele dețin și își controlează propriile lor date fără a fi necesară prezența unui intermediar. Acest model are la bază mai multe principii, cum ar fi consimțământul utilizatorului, grad de confidențialitate ridicat și portabilitate.

Cercetarea [11] evidențiază potențialul principiilor SSI de a spori controlul utilizatorului asupra propriilor date, subliniind implicațiile sale cu privire la confidențialitate și securitate, în special integrate într-o soluție ce are la bază tehnologia blockchain. Cu toate acestea, [15] prezintă și motivează existența problemelor ce țin de adopția la scară largă și interoperabilitatea modelelor ce se bazează pe acest principiu.

2.4 Experiența Utilizatorului și Adopția Portofelelor Digitale de Identitate

Deși fundamentele tehnice ale SSI sunt bine definite, adoptarea pe scară largă depinde în mare măsură de experiența de utilizare a portofelelor. Un studiu **ICICM 2024** evidențiază deficiențe critice de înțelegere și modele mentale eronate ale utilizatorilor atunci când folosesc portofele de identitate digitală, având impact direct asupra siguranței datelor. [25]

Analiza **IFIP AICT 2023** confirmă aceste constatări printr-un cognitive walk-through pe patru wallet-uri (Trinsic, Connect.me, esatus, Jolocom) și propune ghiduri de orientare pentru utilizare și design pentru onboarding, backup și selective-disclosure. [24] Rezultatele subliniază nevoia de interfețe explicite, fluxuri de permisiuni gradual-dezvăluite și suport multi-lingvistic înainte ca SSI să poată fi adoptat la scară largă.

2.5 Standarde W3C pentru Identitatea Descentralizată

Standardul **Decentralized Identifiers (DID) v1.0** stabilește un model de identificator persistent, agnostic față de registru, ce permite rezoluția metadatelor criptografice direct din blockchain-uri, DLT-uri sau chiar baze de date offline. [31]

Mai mult, **Verifiable Credentials Data Model 1.1** extinde conceptul de credențiale semnate criptografic, introducând mecanisme de extensibilitate și profiluri de prezentare selective, esențiale pentru protecția datelor cu caracter personal. [32]

Împreună, DID-urile și VC-urile formează fundamentul tehnic al majorității sistemelor SSI contemporane.

2.6 Protocoale de Interoperabilitate – DIDComm și Hyperledger Aries

Realizarea tranzacțiilor sigure între portofele și entități necesită protocoale de transport și negociere interoperabile. **Hyperledger Aries RFC 0003** descrie un set de protocoale peer-to-peer (issue-credential, present-proof, connection etc.) având ca fundament tehnologic DID-urile și VC-urile. [19]

La nivel de transport, **DIDComm v2.0** definește un canal criptat end-to-end, cu suport pentru rutare multi-hop și criptare by-recipient, făcând posibilă portabilitatea credențialelor între rețele eterogene. [14]

2.7 Mecanisme de Revocare și Status al Credențialelor

Un sistem SSI cu grad ridicat de maturitate trebuie să rezolve nu doar emiterea și prezentarea credențialelor, ci și revocarea lor rapidă, scalabilă și fără pierderea confidențialității. Noua specificație funcțională **W3C Bitstring Status List v1.0** propune un registru compact (bit-string comprimat) care poate însuma milioane de înregistrări într-un singur VC, reducând traficul de rețea și eliminând corelarea dintre titular și punctul de verificare. [33]

La nivel de cercetare, Schumm et al. demonstrează un protocol de **revocare pe bază de acumuloare criptografice**, ce obține timp sub-liniar pentru verificare și actualizare, făcând fezabilă revocarea anonimă în lanțuri publice. [27]

Astfel, aceste lucrări trasează direcția către registre de status distribuite, eficiente și privacy-preserving.

2.8 Interoperabilitatea Inter-Chain și Straturile de Identitate Agnostice

Fragmentarea ecosistemului DLT impune soluții care să transpună DID-uri și credențiale peste mai multe rețele. Un sondaj publicat în 2025 propune o arhitectură ierarhică de gateway-uri cross-chain și contracte inteligente de ancorare pentru sincronizarea statutului credențialelor între lanțuri eterogene. În paralel, Grupul de lucru EEA Cross-Chain Interoperability elaborează profile comune de verificare și scheme de semnătură compatibile, având ca scop evitarea unui grad ridicat de dependență față de diverse puncte centralizate. [21]

2.9 Verificarea cu Divulgare Zero – zk-SNARK/zk-STARK în SSI

Descoperirile recente arată o migrare accelerată de la schemele clasice de anonimizare la **Politicele cu Zero Cunoaștere** (Zero-Knowledge Policies/ZKP) pentru demonstrarea proprietății atributelor fără expunerea lor. [26] Un sondaj extins evidențiază integrarea zk-SNARK-urilor în fluxurile de emitere și prezentare a credențialelor, reducând supraîncărcarea de date și costurile on-chain. [9]

Propuneri experimentale, precum prototipul SSI bazat pe ZKP și blockchain prezentat în [9] demonstrează obținerea unui echilibru între confidențialitate și trasabilitate prin mecanisme de dezanonimizare controlată.

2.10 Identitatea Digitală în Contextul European: eIDAS 2.0, EBSI și ESSIF

Regulamentul (UE) **2024/1183** (cunoscut drept **eIDAS 2.0**) definește *European Digital Identity Wallet*, solicitând interoperabilitate cu DID-uri, VC-uri și mecanisme de dezvăluire minimală. [8]

Pentru implementare, **European Blockchain Services Infrastructure (EBSI)** rulează o rețea de noduri publice care oferă servicii de rezoluție DID (metoda *did:ebis*), depozitare de credențiale și registru de revocare, integrate cu **European Self-Sovereign Identity Framework (ESSIF)**. [17] Această infrastructură reprezintă, de fapt, un fundament inițial pentru diploma EUROPASS, titlul de rezidență digitală și, în viitor, portofelul european de identitate.

2.11 Guvernare, Cadre de Încredere și Reglementare

Pe lângă aspectele tehnice, identitatea descentralizată necesită cadre de guvernare capabile să alinieze părțile interesate și să asigure conformitatea juridică.

Trust Over IP (ToIP) Stack propune o arhitectură în patru straturi care separă asigurarea criptografică (layer 1–2) de guvernare legală și socio-economică (layer 3–4), oferind modele de registre de încredere și medii de lucru reutilizabile pentru guvernare. [5] Mai mult, **Good Health Pass Blueprint v1.0** integrează aceste principii într-un set de nouă recomandări de interoperabilitate (UX consecvent, registru de încredere, politici de confidențialitate), validându-le în scenarii de călătorie trans-frontalieră [4]

Uniunea Europeană implementează conceptele ToIP prin **EU Digital Identity Wallet – Architecture & Reference Framework (ARF)**, care definește roluri, cicluri de viață și procese de evaluare a conformității pentru furnizorii de portofele ce urmează regulamentul *eIDAS 2.0*. [7] Din perspectivă academică, Gans et al. analizează impactul social al SSI și arată că un model mixt de guvernare (centralizat-descentralizat) este esențial pentru a evita dezechilibre de putere și a garanta beneficiile promise. [18]

2.12 Identitatea Mobilă și Standardul ISO 18013-5

Standardul **ISO/IEC 18013-5:2021** definește formatul și protocoalele de schimb pentru *Mobile Driving Licence* (mDL), permițând prezentarea selectivă a atributelor prin NFC, BLE sau online-DL-Router. Cercetările recente arată că aceeași structură poate găzdui orice tip de set de credențiale verificabil, facilitând convergența dintre portofelele SSI și identitățile guvernamentale mobile. [6]

2.13 Platforme și Inițiative de Referință

În prezent, există inițiative de referință și încercări de implementare a unei platforme de identități digitale:

1. **Sovrin Network** a introdus prima implementare globală de registru public bazat pe permisi, fiind dedicat identității autoguvernată, implementând paradigme tehnologice precum Plenum BFT și model trust-anchor. [29]
2. **Hyperledger Indy** furnizează un set de componente (ledger, pluggable consensus, portofel criptat) optimizate pentru operațiuni de anonimitate și revocare eficientă. [3]

Aceste platforme demonstrează fezabilitatea tehnică, însă ridică probleme de guvernare distribuită și sustenabilitate economică, aspecte pe care cercetarea de față își propune să le abordeze.

2.14 Securitatea și Confidențialitatea în Sisteme de Identitate Descentralizate

Proprietățile de securitatea și confidențialitatea datelor sunt esențiale în design-ul sistemelor de identitate descentralizate. Tehnici precum criptare și calcul securizat multi-party sunt doar câteva din cele necesare pentru a obține o protecție a datelor cât mai mare.

În articolul de cercetare [12] sunt analizate multiple tehnici de criptografie pentru a obține o verificare a datelor confidențială, fără a dezvălui date sensibile. Însă, asigurarea scalabilității pentru aceste mecanisme ce oferă un factor sporit de confidențialitate fără a face compromisuri cu privire la securitate rămâne o problemă validă.

2.15 Lacune și Oportunități

Cu toate că s-au făcut progrese majore în implementarea sistemelor de identitate bazate pe blockchain, încă există multiple lacune și zone ce pot fi îmbunătățite. În urma analizei State of the Art, se menționează deseori probleme cu privire la experiența utilizatorului, interoperabilitatea dintre mai multe platforme blockchain și echilibrul dintre confidențialitate și reglementări. Mai mult, lipsește un cadru de cercetare detaliat cu privire la performanțele și adopția într-un scenariu real a sistemelor SSI. Acest proiect are ca scop abordarea acestor lacune, având în prim plan confidențialitatea și analiza empirică a performanțelor sistemului.

3 MODELUL PROIECTULUI

Sistemul Descentralizat de Verificare a Identității Digitale are la bază tehnologia blockchain, ce oferă suport pentru contractele inteligente, esențiale în automatizarea emiterii, verificării și managementului identităților digitale. În cadrul acestui proiect, se va folosi Ethereum ca platforma blockchain optimă, datorită adopției pe scară largă, suportului regăsit în comunitate și a uneltelor de dezvoltare software robuste. Blockchain-ul local Ethereum va fi lansat și găzduit de o rețea locală de test cu ajutorul **Ganache** și a suitei **Truffle**, dedicate pentru testarea aplicațiilor Web3 dezvoltate pe **Mașina Virtuală Ethereum**.

Mai mult, Sistemul Descentralizat va fi incorporat într-o soluție **Software as a Service (SaaS)** pentru a demonstra funcționalitatea și aplicabilitatea sa într-un caz de utilizare practic și relevant.

Arhitectura întregului sistemului și modul de comunicare a componentelor sunt descrise în Figura 1, regăsită mai jos:

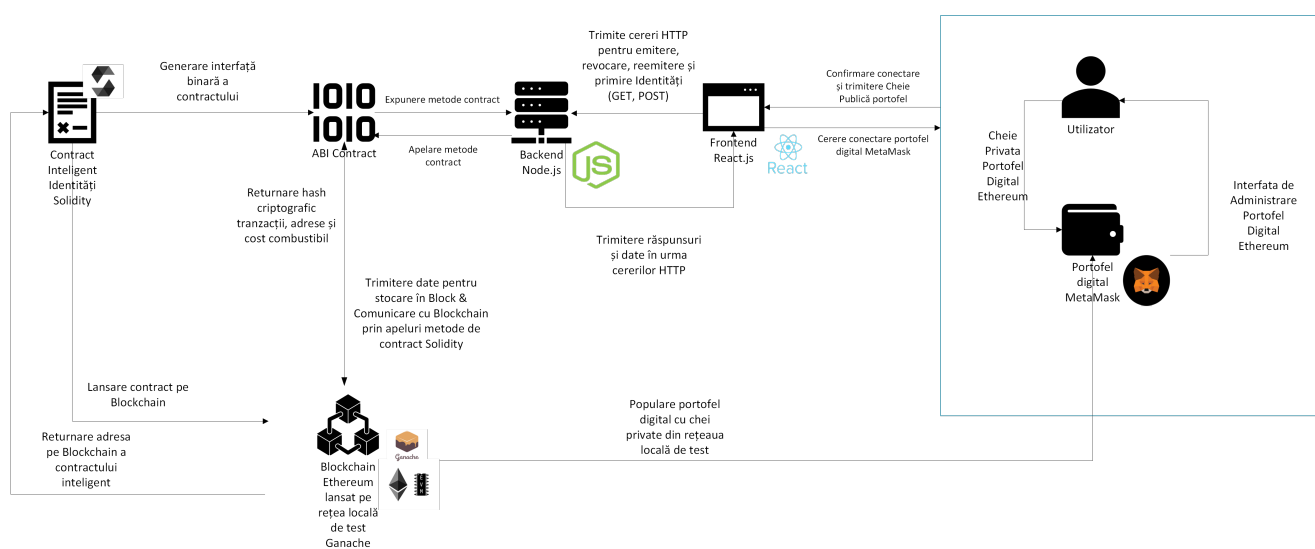


Figura 1: Arhitectura sistemului

3.1 Stiva de tehnologii

3.1.1 Sistem Blockchain și Contractul Inteligent

Componentele arhitecturii de sistem regăsite în Figura 1 sunt descrise după cum urmează:

1. Sistem Blockchain (Ethereum VM, Ganache):

- sistemul descentralizat Blockchain ce are la bază **Mașina Virtuală Ethereum (EVM)** în cadrul căreia sunt stocate identitățile digitale, oferind un mediu valabil la nivel global, cu unelte și mediu de dezvoltare cu un grad ridicat de maturitate.
- sistemul Blockchain este lansat ca o rețea locală de testare dedicată cu ajutorul **Ganache**, oferind unelte software populare, precum implementarea de teste funcționale și de integrare pentru dezvoltarea aplicațiilor descentralizate Web3 ce au ca fundament platforma Ethereum;

2. Contracte inteligente (Solidity, Truffle):

- contractele inteligente gestionează emiterea, verificarea, citirea și revocarea credențialelor; ele interacționează direct cu rețeaua blockchain pentru a înregistra tranzacțiile și a menține integritatea;
- contractele inteligente sunt compilate și lansate cu ajutorul **Truffle**, astfel fiind generată **interfața binară a contractului (ABI)**, iar contractul fiind lansat pe Blockchain;
- ele primesc și apeluri ale metodelor contractului inteligent din componenta de Backend (Business Logic) a întregului sistem;
- contractele inteligente Solidity sunt lansate pe Blockchain la o adresă fixă, oferind fiecărei identități digitale o sursă de veridicitate verificabilă și imutabilă.

3. Application Binary Interface(ABI) al contractului:

- încorporează datele contractului inteligent și metodele implementate în acesta cu ajutorul unei interfețe binare într-o reprezentare **JSON** obținută în urma compilării contractului inteligent, astfel este posibilă accesarea contractului inteligent în componenta de Business Logic;
- decuplează contractul inteligent de restul stivei de tehnologii (Node.js și React.js), fiind necesară doar interfața binară a contractului pentru a codifica și decodifica datele tranzacțiilor.

3.1.2 Contractul Intelligent

Contract Identitate
<code>address issuer;</code> <code>string credentialId - keccak256 (SHA-3)</code> <code>string dataHash - criptare AES</code> <code>bool valid</code>
<code>Credentials[] getCredentials</code> <code>(address user)</code> <code>Credentials[] getValidCredentials</code> <code>(address user)</code> <code>void issueCredential(address user, string</code> <code>credentialId, string dataHash, bool</code> <code>revalidate)</code> <code>bool verifyCredential(address user, string</code> <code>credentialId)</code> <code>void revokeCredential(address user, string</code> <code>credentialId)</code>

Figura 2: Contractul de identități al sistemului

Contractul inteligent de identități a fost implementat folosind limbajul de programare Solidity, nativ platformei blockchain Ethereum pentru a scrie cod executabil și distributiv, urmând principiile **Self-Sovereign Identity**, întrucât datele cu privire la identitatea digitală pot fi accesate, revocate și emise doar de utilizatorul emitent ce deține cheia privată a portofelului digital proprietar al identității respective. Aceste date nu pot fi copiate, mutate, citite, accesate sau șterse datorită proprietăților funcționale ale structurii de date Blockchain și a modului de funcționare al contractelor inteligente dezvoltate folosind **Mașina Virtuală Ethereum**.

Contractul inteligent de identități are o implementare necesară și suficientă, iar fiecare identitate conține membrii și metodele de mai jos:

1. **Adresa portofelului digital Ethereum emitent:** Emitentul este reprezentat de adresa publică a portofelului digital Ethereum deținut de utilizatorul ce a emis identitatea digitală și doar el poate accesa și administra acea identitate;
2. **Id Identitate:** Fiecare identitate are un identificator unic, generat cu ajutorul algoritmului de criptare **keccak256 (SHA-3)**, ce implică generarea unui **hash criptografic**,

imposibil de decriptat în contextul tehnologic actual, ce are la bază o combinație de date ale identității criptate și a adresei utilizatorului;

3. **Hash date identitate:** Datele sunt stocate în Block-uri pe Blockchain într-o formă criptată, reprezentate de un hash criptografic, generat folosind **criptarea AES**, ce are la bază setul de date de identitate și o cheie secretă, stocată într-un mediu sigur, în absența căreia datele identităților utilizatorului nu pot fi vizualizate sau revocate;
4. **Valid:** Există posibilitatea revocării identităților emise, însă odata stocate într-un block de rețea, acel block nu poate fi șters, ceea ce face ca datele de pe Blockchain să nu poată fi alterate în niciun mod. De aceea, se optează pentru un validator, prin care se pot revoca și revalida identități deja stocate, iar cele invalide să devină înaccesibile;
5. **Metodele contractului:** Metodele **getCredentials**, **getValidCredentials**, **issueCredential**, **verifyCredential** și **revokeCredential** sunt utilizate în cadrul componentei de backend pentru stocarea, vizualizarea și revocarea identităților de pe blockchain.

3.1.3 Criptare și semnături

Setul de chei publică-privată oferă un grad de securitate ridicat pentru tranzacții și garantează faptul că utilizatorii pot dovedi statutul de proprietari asupra credențialelor fără a dezvălui cheile private. Sistemul folosește algoritmul **Elliptic Curve Digital Signature Algorithm (ECDSA)** pentru generarea cheilor criptografice și semnarea tranzacțiilor, oferind un factor sporit de securitate și dimensiuni reduse ale cheilor criptografice.

În cadrul sistemului se utilizează **criptarea AES** pentru a stoca în mod sigur și criptat datele de identitate ale utilizatorului. **AES** este un algoritm de criptare simetric, ce folosește aceeași cheie secretă atât pentru criptare, cât și decriptare. Este folosit la scară largă pentru stocare și transmitere de date într-o manieră sigură.

Se regăsește și algoritmul de hasurare criptografică **Keccak256**, ce are la bază **Secure Hash Algorithm 3 (SHA-3)**. Este folosit în special în contractele inteligente dezvoltate pe platforma Ethereum și oferă un grad ridicat de integritate a datelor, identificatori unici și semnături digitale, având aceeași aplicabilitate și în cadrul sistemului nostru. Spre deosebire de AES, Keccak256 este un algoritm unilateral, iar decriptarea este imposibilă.

3.1.4 Zero-Knowledge Proofs (ZKPs)

Pentru a mări gradul de confidențialitate, sistemul integrează ZPK-uri pentru a permite utilizatorilor să dovedească faptul că dețin anumite caracteristici sau credențiale ale identității fără a dezvălui informații critice. Acest mecanism este esențial pentru a menține confidențialitatea în timpul interacțiunii cu părțile verificatoare.

3.2 Software as a Service (SaaS)

3.2.1 Middleware/API

Componenta de backend este implementată utilizând mediul de rulare **Node.js**, oferind o soluție necesară și suficientă pentru a găzdui și rula logica din spatele sistemului. Aceasta funcționează ca o punte între **componenta de frontend dezvoltată folosind React.js** și **contractele inteligente Solidity**. Este structurată folosind concepte de **design pattern** specifice unui **Model-View Controller (MVC)** și asigură un factor de mentenanță stabil și o separare logică a sistemului.

1. **Rute:** Se definesc puncte finale pentru primirea cererilor de la componenta vizuală;
2. **Controllere:** Asigură procesarea cererilor de la componenta vizuală și apelează metodele din cadrul serviciilor;
3. **Servicii:** Implementează logica de procesare a datelor dintre componenta de frontend și contractele inteligente, apelează metodele de contract și returnează rezultatele primite de pe blockchain;
4. **Configurări:** Se regăsesc configurări bazate pe variabile de mediu, în special în cazul definirii interacțiunii cu blockchain-ul Ethereum.

3.2.2 Componenta Vizuală

Componenta vizuală este reprezentată de conectarea portofelului digital de identități la portofelul Ethereum al utilizatorului cu ajutorul MetaMask.

Implementarea sa a fost dezvoltată folosind framework-ul **React.js**, o soluție populară în industrie pentru dezvoltarea interfețelor vizuale ale aplicațiilor.

Prin interfața vizuală sunt apelate metodele din API și este conectată în mod direct la extensia de browser MetaMask, oferind o punte între backend și MetaMask. Astfel, utilizatorul poate comunica cu Blockchain pentru a emite, gestiona și revoca identitățile digitale.

4 WORKFLOW-UL SISTEMULUI ȘI EXPERIENȚA UTILIZATORULUI

4.1 Workflow-ul Sistemului de Identități Digitale

Diagrama descriptivă a fluxului de lucru al sistemului și al scenariilor de funcționare este dată de figura de mai jos:

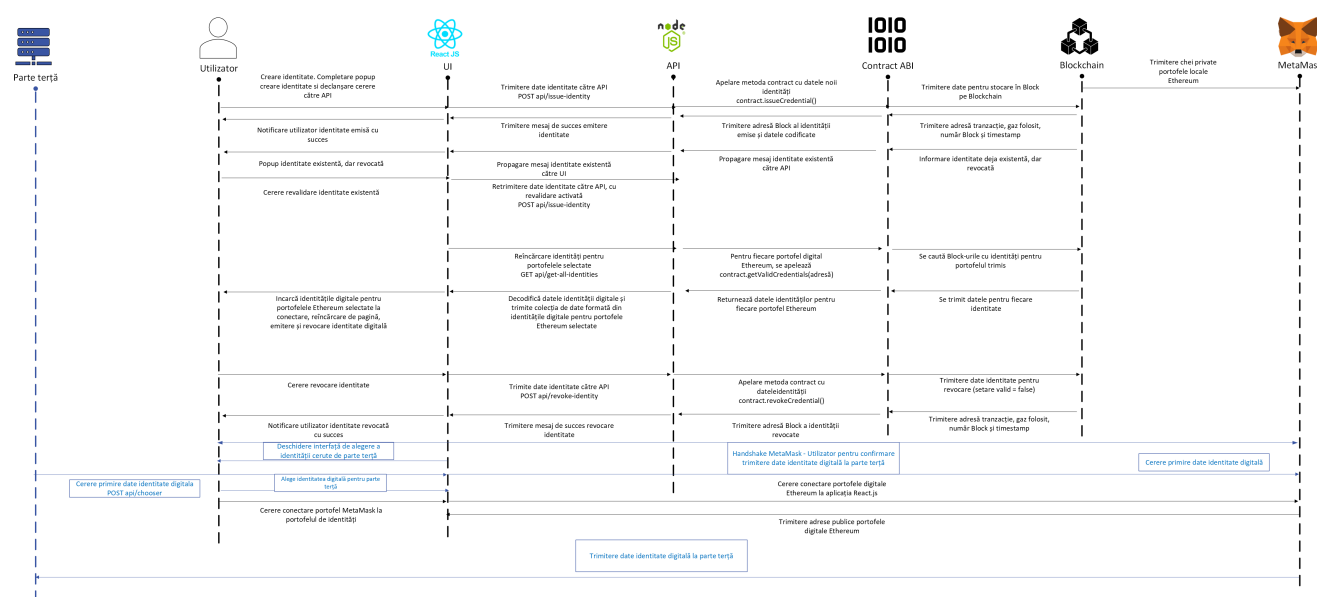


Figura 3: Diagrama workflow a scenariilor de funcționare ale sistemului

În cadrul diagramei workflow, se regăsesc următorii actori:

- **Utilizator:** utilizatorul uman al unuia sau mai multor portofele digitale Ethereum - poate iniția operații, precum emisie, revocare, revalidare și confirmare trimitere date digitale.
- **React.js UI:** aplicație web vizibilă pentru utilizator - declanșează popup-uri, trimite notificări către utilizator și apelează metodele REST API.
- **Node.js API:** codifică, decodifică și trimite datele de la UI către ABI-ul contractului inteligent.
- **Contract ABI:** interfață binară sigură pe care API-ul o folosește pentru a apela contractul inteligent Solidity lansat pe Blockchain.
- **Blockchain:** layer-ul de execuție pentru Ethereum Virtual Machine - stochează identitățile digitale și emite datele de tranzacție.

- **MetaMask:** extensie de browser pentru portofele digitale Ethereum - reține cheile private ale portofelelor utilizatorului, semnează tranzacțiile pe Blockchain și aprobă trimiterea datelor de identități digitale.

4.2 Scenarii de funcționare

În Figura 3 se regăsesc următoarele scenarii de funcționare:

1. **Încărcarea tuturor credențialelor/Sincronizarea portofelului de identități:** Acest workflow este declanșat automat de fiecare dată când utilizatorul conectează extensia de browser MetaMask, emite identitate, revocă identitate sau reîmprospătează pagina.
 - UI trimite portofelele digitale Ethereum selectate către API [GET /api/get-all-identities];
 - API apelează, pentru fiecare portofel digital Ethereum, metoda contractului cu ajutorul interfeței binare (ABI) pentru a prelua identitățile digitale corespunzătoare fiecărui portofel [getValidCredentials(addr)];
 - pentru fiecare apel, ABI caută Block-ul corespunzător fiecărei identități;
 - Blockchain-ul trimite către ABI datele codificate pentru fiecare identitate;
 - ABI trimite mai departe la API datele identităților;
 - API le decodifică și le formatează în format JSON, trimițându-le ca un vector de identități mai departe către UI (Figura 5);
 - UI încarcă identitățile în dashboard-ul portofelului de identități digitale (Figura 4.

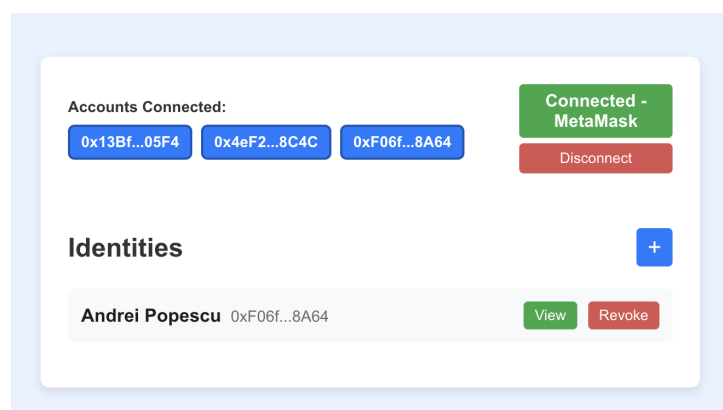


Figura 4: Dashboard portofel identități digitale

```

Received request to get all identities for accounts: [
  '0x13Bf03088AFC2f526bEf6727f8d852fd2FF05F4',
  '0x4eF20D4684D2a97194ADBa0d80C9eFA7b8668C4C',
  '0xF06f8786fF5E9Eb853091D12f3adaD7C7FaF8A64'
]
Fetched credentials for 0x13Bf03088AFC2f526bEf6727f8d852fd2FF05F4: []
Fetched credentials for 0x4eF20D4684D2a97194ADBa0d80C9eFA7b8668C4C: []
Fetched credentials for 0xF06f8786fF5E9Eb853091D12f3adaD7C7FaF8A64: [
  [
    '0xF06f8786fF5E9Eb853091D12f3adaD7C7FaF8A64',
    '0x76f59587825b5264aa90ad603104e5e25e086f7364594856a74a699cb099a9a5',
    'U2FsdGVkX18bdrG5dgaeLKBmvpCsi4Hh68pHEB5H3Ri0hi2vMT3361YQ3KjDV6rB1UrmVPbazuAa0V0vsuYkgj7JIG19+QGnsuW8RUPHM8U7JPMNzcAia6XHy9itxeLsHOP1Gk6ocH/ljysoRIFWK4MnMX1c0VTXUkgSANctmI=',
    true,
    issuer: '0xF06f8786fF5E9Eb853091D12f3adaD7C7FaF8A64',
    credentialId: '0x76f59587825b5264aa90ad603104e5e25e086f7364594856a74a699cb099a9a5',
    dataHash: 'U2FsdGVkX18bdrG5dgaeLKBmvpCsi4Hh68pHEB5H3Ri0hi2vMT3361YQ3KjDV6rB1UrmVPbazuAa0V0vsuYkgj7JIG19+QGnsuW8RUPHM8U7JPMNzcAia6XHy9itxeLsHOP1Gk6ocH/ljysoRIFWK4MnMX1c0VTXUkgSANctmI=',
    valid: true
  ]
]

```

Figura 5: Log-uri API la încărcarea identităților

2. Emiterea credențialelor:

- Utilizatorul completează un formular popup de emisie a identității (Figura 6);
- UI trimite datele pentru noua identitate către API [POST /api/issue-identity];
- API apelează metoda contractului cu ajutorul interfeței binare (ABI) pentru a emite și semna noua identitate digitală [issueCredential(data)] (Figura 7);
- ABI trimite tranzacția spre Blockchain, iar datele pentru noua identitate emisă sunt stocate pe un nou Block;
- Blockchain-ul trimite către ABI datele standard ale tranzacției: hash-ul tranzacției, gazul folosit, numărul de Block și timestamp-ul (Figura 8);
- ABI trimite la API datele tranzacției și adresa tranzacției;
- API trimite către UI un mesaj de succes;
- UI notifică Utilizatorul că tranzacția a fost emisă cu succes și porneste workflow-ul de încărcare a identităților digitale pentru portofelele selectate.

Figura 6: Popup emisie identitate nouă

```

Received request to issue identity for user: 0x4eF20D4684D2a97194ADBa0d80C9eFA7b8668C4C Angelo Barbu 2000-04-18 Romania 12345678 false
Issuing identity: 0x4eF20D4684D2a97194ADBa0d80C9eFA7b8668C4C Angelo Barbu 2000-04-18 Romania 12345678 false
Estimated Gas to Issue: 368579
Identity issued successfully: 0x7c39abb3c78e0629057f7f15afae2232b883e99383a3480dd77926abfe0dd62e
Data: U2FsdGVkX1+po70hCqIucZF0WEIRnc5mEnjq0PHIDfQL6V1vF/ZPTEQYHS3I7fGAE4QsrJrTTksjch8/tBDfi8eyuKy0P7ZBK97x06ahuxY0Nu20/myETRii4H1hgIYX9zgrQWu6K/vxMvP3sp0b2X9RT9D1Qi/GDXMLJ2Pw+7c=
Received request to get all identities for accounts: [
  '0x13Bf03088AFfc2f526bEf6727f8d852fd2FF05F4',
  '0x4eF20D4684D2a97194ADBa0d80C9eFA7b8668C4C',
  '0xF06f8786fF5E9Eb853091D12f3adaD7C7FaF8A64'
]
Fetched credentials for 0x13Bf03088AFfc2f526bEf6727f8d852fd2FF05F4: []
Fetched credentials for 0x4eF20D4684D2a97194ADBa0d80C9eFA7b8668C4C: [
  [
    '0x4eF20D4684D2a97194ADBa0d80C9eFA7b8668C4C',
    '0x7c39abb3c78e0629057f7f15afae2232b883e99383a3480dd77926abfe0dd62e',
    'U2FsdGVkX1+po70hCqIucZF0WEIRnc5mEnjq0PHIDfQL6V1vF/ZPTEQYHS3I7fGAE4QsrJrTTksjch8/tBDfi8eyuKy0P7ZBK97x06ahuxY0Nu20/myETRii4H1hgIYX9zgrQWu6K/vxMvP3sp0b2X9RT9D1Qi/GDXMLJ2Pw+7c=',
    true,
    issuer: '0x4eF20D4684D2a97194ADBa0d80C9eFA7b8668C4C',
    credentialId: '0x7c39abb3c78e0629057f7f15afae2232b883e99383a3480dd77926abfe0dd62e',
    dataHash: 'U2FsdGVkX1+po70hCqIucZF0WEIRnc5mEnjq0PHIDfQL6V1vF/ZPTEQYHS3I7fGAE4QsrJrTTksjch8/tBDfi8eyuKy0P7ZBK97x06ahuxY0Nu20/myETRii4H1hgIYX9zgrQWu6K/vxMvP3sp0b2X9RT9D1Qi/GDXMLJ2Pw+7c=',
    valid: true
  ]
]
Fetched credentials for 0xF06f8786fF5E9Eb853091D12f3adaD7C7FaF8A64: [
  [
    '0xF06f8786fF5E9Eb853091D12f3adaD7C7FaF8A64',
    '0x76f59587825b5264aa90ad603104e5e25e086f7364594856a74a699cb099a9a5',
    'U2FsdGVkX18bdrG5dgaekLBmvpCsi4Hh68pHEB5H3Ri0hi2vMT3361YQ3KjDV6rB1UrmVPbazuAa0V0vsuYkgj7JIG19+QGnsuW8RUPHM8U7JPMNzcAiai6XHy9itxelsh0PLGk6ocH/ljysoRIFWK4MnMX1c0VTXUkgSANctmI=',
    true,
    issuer: '0xF06f8786fF5E9Eb853091D12f3adaD7C7FaF8A64',
    credentialId: '0x76f59587825b5264aa90ad603104e5e25e086f7364594856a74a699cb099a9a5',
    dataHash: 'U2FsdGVkX18bdrG5dgaekLBmvpCsi4Hh68pHEB5H3Ri0hi2vMT3361YQ3KjDV6rB1UrmVPbazuAa0V0vsuYkgj7JIG19+QGnsuW8RUPHM8U7JPMNzcAiai6XHy9itxelsh0PLGk6ocH/ljysoRIFWK4MnMX1c0VTXUkgSANctmI=',
    valid: true
  ]
]

```

Figura 7: Log-uri API emite identitate

```

eth_estimateGas
eth_getBlockByNumber
eth_gasPrice
eth_sendTransaction

Transaction: 0x04246be5d67b7187041c495b8bac9f5658dd1e329e3760cd2362b38bdcc0f942
Gas usage: 336728
Block number: 236
Block time: Fri Feb 07 2025 15:41:09 GMT+0200 (Eastern European Standard Time)

eth_getTransactionReceipt
eth_call

```

Figura 8: Output Blockchain local la emite identitate

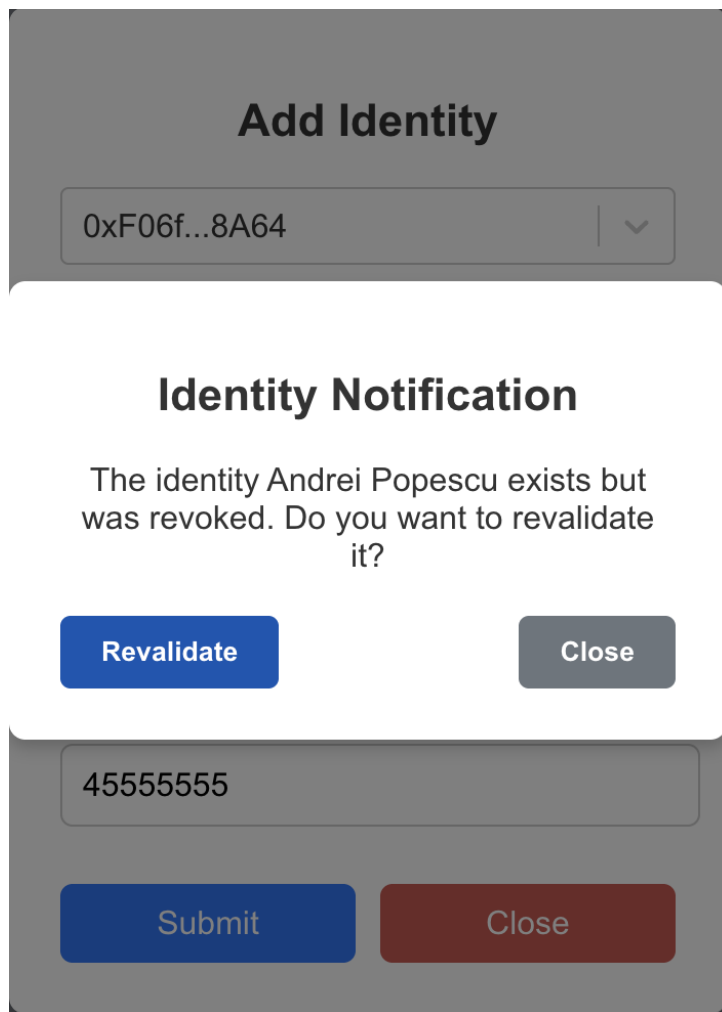


Figura 9: Pop-up revalidare identitate revocată anterior

3. Revalidarea unei identități revocate anterior:

- Utilizatorul apasă pe butonul *Revalidate*, declanșând workflow-ul (Figura 9);
- UI trimite din nou datele identității către API, dar cu flag-ul *revalidate=true* [POST `/api/issue-identity`] (Figura 10);
- Urmează workflow-ul pentru **emiterea credențialelor**, însă cu flag-ul *revalidate=true* (Figura 11).

```

Received request to issue identity for user: 0xF06f8786fF5E9Eb853091D12f3adaD7C7FaF8A64 Andrei Popescu 1999-03-13 Romania 45555555 false
Issuing identity: 0xF06f8786fF5E9Eb853091D12f3adaD7C7FaF8A64 Andrei Popescu 1999-03-13 Romania 45555555 false
Received request to issue identity for user: 0xF06f8786fF5E9Eb853091D12f3adaD7C7FaF8A64 Andrei Popescu 1999-03-13 Romania 45555555 true
Issuing identity: 0xF06f8786fF5E9Eb853091D12f3adaD7C7FaF8A64 Andrei Popescu 1999-03-13 Romania 45555555 true
Estimated Gas to Issue: 109380
Identity issued successfully: 0x76f59587825b5264aa90ad603104e5e25e086f7364594856a74a699cb099a9a5
Data: U2FsdGVkX1+PgWPrm2vLeS8HAK7hrCX55fJVCsb1Fb3V0FMbj7UG0dh37pvd+PXqz27ajfWLC5KmTFdPiRiKxx0kUGhfbImUWAacFB6j8abbw0gH06o8w7Wa0VG0UFzp
0hKrJ/vfms3Ml4UsvTiP/Mh2suRR+B/C16bw8Tqk5c=
Received request to get all identities for accounts: [
  '0x13Bf03088AFfc2f526bEf6727f8d852fd2FF05F4',
  '0x4eF20D4684D2a97194ADBa0d80C9eFA7b8668C4C',
  '0xF06f8786fF5E9Eb853091D12f3adaD7C7FaF8A64'
]
Fetched credentials for 0x13Bf03088AFfc2f526bEf6727f8d852fd2FF05F4: []
Fetched credentials for 0x4eF20D4684D2a97194ADBa0d80C9eFA7b8668C4C: []
Fetched credentials for 0xF06f8786fF5E9Eb853091D12f3adaD7C7FaF8A64: [
  {
    '0xF06f8786fF5E9Eb853091D12f3adaD7C7FaF8A64',
    '0x76f59587825b5264aa90ad603104e5e25e086f7364594856a74a699cb099a9a5',
    'U2FsdGVkX18bdrG5dgaekKBmvpCsi4Hh68pHEB5H3Ri0hi2vMT3361YQ3KjDV6rB1UrmVPbazuAa0V0vsuYkgj7JIG19+QGnsuW8RUPHM8U7JPMNzcAiai6XHy9itxeIsH
0PlGk6ocH/ljysoRIFWK4MnMX1c0VTXUkgSANctmI=',
    true,
    issuer: '0xF06f8786fF5E9Eb853091D12f3adaD7C7FaF8A64',
    credentialId: '0x76f59587825b5264aa90ad603104e5e25e086f7364594856a74a699cb099a9a5',
    dataHash: 'U2FsdGVkX18bdrG5dgaekKBmvpCsi4Hh68pHEB5H3Ri0hi2vMT3361YQ3KjDV6rB1UrmVPbazuAa0V0vsuYkgj7JIG19+QGnsuW8RUPHM8U7JPMNzcAiai6X
Hy9itxeIsH0PlGk6ocH/ljysoRIFWK4MnMX1c0VTXUkgSANctmI=',
    valid: true
  },
  {
    '0xF06f8786fF5E9Eb853091D12f3adaD7C7FaF8A64',
    '0xc76ea90e1aa1ed0208448c286e82c96f1399730fbf56d4daa7a385979a3b32fa',
    'U2FsdGVkX1/PJ2vQEGfLCQIKS0ziRML/ZG2fJBwumqP2r0n6x4jfyvmwlnRNzETqLBKyK+VMXoX6LEVazLHH64vnjuydN04aKX0S+k0Irw3o6KHsf6TiK7QDV1Z57qk5VH
nDv6Vf01S3vYzDZwsMsw2WiA/qR9ktz0zrYHBI08x/uLvH1PDo2Gr4hkUhm4Zk',
    true,
    issuer: '0xF06f8786fF5E9Eb853091D12f3adaD7C7FaF8A64',
    credentialId: '0xc76ea90e1aa1ed0208448c286e82c96f1399730fbf56d4daa7a385979a3b32fa',
    dataHash: 'U2FsdGVkX1/PJ2vQEGfLCQIKS0ziRML/ZG2fJBwumqP2r0n6x4jfyvmwlnRNzETqLBKyK+VMXoX6LEVazLHH64vnjuydN04aKX0S+k0Irw3o6KHsf6TiK7QD
V1Z57qk5VHnDv6Vf01S3vYzDZwsMsw2WiA/qR9ktz0zrYHBI08x/uLvH1PDo2Gr4hkUhm4Zk',
    valid: true
  }
]

```

Figura 10: Log-uri API la revalidare identitare revocată anterior

```

eth_estimateGas
eth_getBlockByNumber
eth_gasPrice
eth_sendTransaction

Transaction: 0x608c1cbb2d7941cf23eb023b7d52392bc674eba6be7f1dbfa5d72ca185a8e7b8
Gas usage: 109380
Block number: 258
Block time: Sun Jun 08 2025 17:28:17 GMT+0300 (Eastern European Summer Time)

eth_getTransactionReceipt

```

Figura 11: Output Blockchain local la revalidare identitate revocată anterior

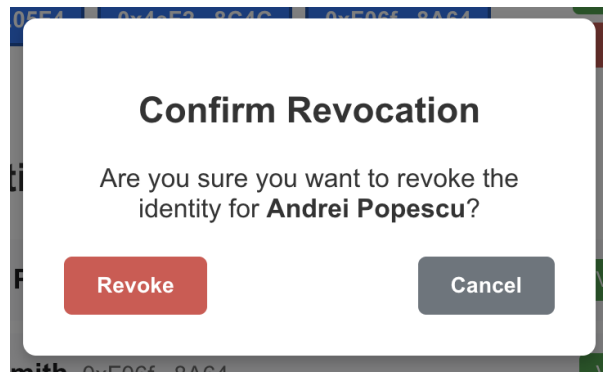


Figura 12: Popup revocare identitate existentă

4. Revocarea unei identități:

- Utilizatorul confirmă revocarea identității apăsând pe butonul *Revoke* (Figura 12);
- UI trimite către API ID-ul identității ce urmează să fie revocată; [POST /api/revoke-identity];
- API apelează metoda contractului cu ajutorul interfeței binare (ABI) pentru a seta validitatea identității digitale ca falsă *valid=false* [revokeCredential(id)] (Figura 13);
- ABI trimite tranzacția spre Blockchain, iar noul status de validitate este actualizat pentru identitatea respectivă;
- Blockchain-ul trimite către ABI datele standard ale tranzacției: hash-ul tranzacției, gazul folosit, numărul de Block și timestamp-ul (Figura 14);
- ABI trimite la API datele tranzacției și adresa tranzacției;
- API trimite către UI un mesaj de succes;
- UI notifică Utilizatorul că tranzacția a fost revocată cu succes și porneste workflow-ul de încărcare a identităților digitale pentru portofelele selectate.

```

Received request to revoke identity for user: 0xF06f8786fF5E9Eb853091D12f3adaD7C7FaF8A64 Andrei Popescu 1999-03-13 Romania 4555555
Revoking identity: 0xF06f8786fF5E9Eb853091D12f3adaD7C7FaF8A64 Andrei Popescu 1999-03-13 Romania 4555555
Estimated Gas to Revoke: 90677
Identity revoked successfully: 0x76f59587825b5264aa90ad603104e5e25e086f7364594856a74a699cb099a9a5
Received request to get all identities for accounts: [
  '0x13Bf03088AFfc2f526bEf6727f8d852fd2FF05F4',
  '0x4eF20D4684D2a97194ADBaa0d80C9eFA7b8668C4C',
  '0xF06f8786fF5E9Eb853091D12f3adaD7C7FaF8A64'
]
Fetched credentials for 0x13Bf03088AFfc2f526bEf6727f8d852fd2FF05F4: []
Fetched credentials for 0x4eF20D4684D2a97194ADBaa0d80C9eFA7b8668C4C: []
Fetched credentials for 0xF06f8786fF5E9Eb853091D12f3adaD7C7FaF8A64: [
  [
    '0xF06f8786fF5E9Eb853091D12f3adaD7C7FaF8A64',
    '0xc76ea90e1aa1ed0208448c286e82c96f1399730fbf56d4daa7a385979a3b32fa',
    'U2FsdGVkX1/PJ2vQEGfLCQIkS0ziRML/ZG2fJBwumqP2r0n6x4jYvmwLnRNzETqLBKyK+VMXoX6LEVazLHH64vnjuydN04aKX0S+k0Irw3o6KHs f6TiK7QDV1Z57qk5VHnDv6Vf01S3vYzDZwsMsw2WiA/qr9ktz0zrYHBI08x/ulvH1PDo2Gr4hkUhm4Zk',
    true,
    issuer: '0xF06f8786fF5E9Eb853091D12f3adaD7C7FaF8A64',
    credentialId: '0xc76ea90e1aa1ed0208448c286e82c96f1399730fbf56d4daa7a385979a3b32fa',
    dataHash: 'U2FsdGVkX1/PJ2vQEGfLCQIkS0ziRML/ZG2fJBwumqP2r0n6x4jYvmwLnRNzETqLBKyK+VMXoX6LEVazLHH64vnjuydN04aKX0S+k0Irw3o6KHs f6TiK7QDV1Z57qk5VHnDv6Vf01S3vYzDZwsMsw2WiA/qr9ktz0zrYHBI08x/ulvH1PDo2Gr4hkUhm4Zk',
    valid: true
  ]
]

```

Figura 13: Log-uri API pentru revocare identitate existentă

```

eth_estimateGas
eth_getBlockByNumber
eth_gasPrice
eth_sendTransaction

Transaction: 0xcabc12dc387b69eb13a8145128917fffd8420d7fbc9d22ef0067c78045728446be
Gas usage: 85877
Block number: 257
Block time: Sun Jun 08 2025 17:22:36 GMT+0300 (Eastern European Summer Time)

eth_getTransactionReceipt

```

Figura 14: Output Blockchain local la revocare identitate

5. Confirmarea selectivă a datelor unei identități digitale către o parte terță:

- Partea terță apelează componenta vizuală regăsită la *ui/chooser*;
- UI deschide pentru utilizator un selector din lista de identități digitale ale Utilizatorului;
- Utilizatorul alege identitatea pe care o va distribui către partea terță;
- UI - MetaMask: MetaMask trimite o cerere de confirmare către Utilizator pentru a conecta portofelul digital al identităților și a trimite datele identității digitale selectate;
- UI trimite datele identității selectate și semnătura din portofelul MetaMask (doar date publice, excluzând date sensibile, precum chei private);
- Partea terță primește datele identității digitale de la UI.

Demonstrarea acestui workflow poate fi regăsit la secțiunea **5.3.4 Testarea Utilizării - Proof of Concept**.

4.3 Proprietăți cheie ale workflow-ului

Conform diagramei din **Figura 3** și a analizei descriptive a scenariilor de funcționare, se remarcă următoarele proprietăți ale portofelului digital de identități:

- **Control centrat pe utilizator:** toate operațiile asupra portofelelor digitale, precum emiter, revalidare, revocare sau distribuie sunt efectuate în totalitate și exclusiv în urma cererii explicite a utilizatorului, urmată de semnătura MetaMask oferită tot de utilizator.
- **Componenta de Backend are rol strict de orchestrare:** API-ul se ocupă strict de orchestrarea apelurilor de metode de contract inteligent și decodificarea datelor, reprezentând o punte dintre UI și Blockchain. Stocarea, securitatea și autenticitatea datelor este dată în mod exclusiv de Blockchain.
- **Date on-chain, utilizare off-chain:** datele sunt stocate pe Blockchain-ul Ethereum, persistând cu ajutorul contractelor inteligente, dar sunt menținute în cache și decodate off-chain pentru performanțe ridicate ale sistemului.
- **Suport portofele multiple:** Portofelul de identități digitale poate fi conectat la orice număr de portofele digitale Ethereum, oferind, astfel, un suport extins.
- **Asigurarea unei piste de audit:** Fiecare acțiune ce schimbă starea portofelului de identități digitale este reprezentată de o tranzacție on-chain, ce are hash, timestamp și număr de Block.

5 METRICILE DE ANALIZĂ A PERFORMANTELOR ȘI ANALIZA REZULTATELOR

5.1 Metricile de Analiză a Performanțelor

Metricile de analiză a performanțelor includ:

1. **Analiză comparativă a Blockchain-ului Ethereum:** evaluarea ecosistemului Ethereum ca soluție Blockchain pentru sistemul de identități digitale, în comparație cu opțiunile disponibile în prezent;
2. **Securitate:** evaluarea securității sistemului la atacuri, precum furturi de identitate, breșe de date și acces neautorizat;
3. **Confidențialitate:** analiza eficienței mecanismelor de conservare a confidențialității, precum ZKP-urile și criptarea;
4. **Scalabilitate & Robustețe:** analiza abilității sistemului de a procesa un număr ridicat de utilizatori, tranzacții și cereri de verificare;
5. **Utilizare:** măsurarea ușurinței de utilizare și a satisfacției utilizatorilor cu privire la folosirea Portofelului de Identitate Digitală și a Interfeței de Verificare;
6. **Proof of Concept (PoC):** demonstrarea aplicabilității sistemului de identități digitale într-un scenariu ce simulează un caz de utilizare din viața reală.

5.2 Ecosistemului Ethereum ca Blockchain pentru Soluția Propusă

În urma unei analize cuprinzătoare a potențialelor soluții ca ecosistem Blockchain pentru portofelul de identități digitale, am constatat ca **Ethereum** este soluția optimă pentru sistemul de identități digitale prezentat în cadrul acestei lucrări. Această decizie a fost stabilită pe baza următoarelor criterii:

Criteriu	Relevanță pentru Sistemul de Identități Digitale
<i>Respectarea Standardelor</i>	Suport nativ pentru W3C DIDs, registre on-chain (ERC-1056, ERC-780, etc.)
<i>Experiența Utilizatorului</i>	Numărul de utilizatori ce pot folosi portofelul fără a necesita o instanță nouă
<i>Librării & Mediu de Dezvoltare</i>	Valabilitatea librăriilor de contracte inteligente testate, rețele de test, simulatoare, kit-uri de dezvoltare software, etc.
<i>Securitate & Descentralizare</i>	Seturi de validare diverse, audit, criptografie testată în timp, trasabilitatea erorilor, etc.
<i>Costuri & Scalabilitate</i>	Costuri pentru declanșarea tranzacțiilor și predictibilitatea acestora
<i>Adopție & Reglementări</i>	Dovadă că există o adopție largă a ecosistemului

Luând în considerare criteriile de evaluare de mai sus, am obținut următoarele concluzii:

Proprietăți	Dovadă	Impact
<i>Suport nativ pentru standarde DID (ERC-1056 / ethr-DID)</i>	Ethereum definește registrul <i>EthereumDIDRegistry</i> , un contract ce transformă fiecare pereche cheie-valoare într-o identitate digitală validă, în timp ce permite rotația cheilor identităților și delegarea acestora. [13]	Acces la un registru on-chain, open-source integrat cu majoritatea framework-urilor de identități digitale (SpruceID, Trinsic, etc.).
<i>Adopție largă a portofelului</i>	MetaMask raportează constant 30 M+ utilizatori activi lunar. [22]	Utilizatorii pot deține, semna și distribui chei ale identităților fără a instala nimic nou, oferind acces instant între browsere și mobil.
<i>Ecosistem de audit & Comunitate de dezvoltare</i>	Ecosistemul Ethereum ocupă primul loc în ceea ce privește numărul total de dezvoltatori activi pe fiecare continent. [16]	Suport extins și o bază mult mai mare de informații.
<i>Adopție pe scară largă</i>	Uniunea Europeană - EBSI, Brazilia - ICP Brasil PoC, Deloitte - KILT folosesc Ethereum Virtual Machine. [2]	Reglementare mai cuprinzătoare, în special pentru cercetare în mediul academic.

Cu toate acestea, în prezent există mai multe opțiuni pentru alegerea ecosistemului Blockchain,

precum **Solana ecosystem** și **Polkadot/KILT**. Astfel, în cadrul lucrării a fost efectuată o analiză comparativă asupra opțiunilor, întărind alegerea **Ethereum** ca ecosistem Blockchain pentru sistemul de identități digitale.

Criteriu	Ethereum/EVM	Solana	Polkadot/KILT
<i>Limbaj de Dezvoltare</i>	Solidity / Vyper - mii de contracte cu audit	Rust & C (Sealevel). Mai puține librării pentru Identități Digitale; o curbă de învățare mai abruptă	Librării bazate pe Rust
<i>Standarde de Identitate</i>	ERC-1056, ERC-725, EIP-712, etc.	Civic Pass & Solana Attestation Service (SAS) [1].	KILT parachain - credențiale W3C-VC
<i>Adopția Portofelului Digital</i>	MetaMask, Rabby, Coinbase Wallet, Rainbow, + orice portofel mobil Layer 2.	Phantom (10 M utilizatori activi lunar), Backpack, Solflare - adopție mai mică în afara ecosistemului Solana.	Polkadot.js, Talisman - nișă de piață.
<i>Validatori & Descentralizare</i>	aprox. 1 050 000 validatori (Proof-of-Stake) → coeficient Nakamoto ridicat. [30]	aprox. 4 500 validatori; cerințele hardware mai mari duc la un grad mai mare de centralizare.	Validare on-chain (aprox. 1 k) + parachainuri individuale; design eficient, însă necesită adopție și maturitate.
<i>Timp Istoric de Funcționare</i>	în funcțiune din 2015; regresii post-migrare mai mici de o oră.	cel puțin 7 întreruperi majore din 2020; cea mai recentă în februarie 2024 (aprox. 5 ore) [20].	Chain stabil.
<i>Performanțe & Costuri</i>	Layer 1 aprox. 15 Tranzacții Pe Secundă; L2s 1k–10k TPS, comisioane sub 0.10 dolari.	400–700 TPS, confirmări sub o secundă, comisioane sub un cent.	1k TPS per parachain; comisioane scăzute, însă necesită depuneri în criptomoneda specifică rețelei, DOT.
<i>Finanțările ecosistemului</i>	Finanțări de peste 20 de miliarde de dolari; Bitcoin, granturi ARB	injecții VC mult mai rapide, dar mai puțin consistente.	granturi de la Web3 Foundation; comunitate de dezvoltare mai restrânsă.
<i>Maturitate pentru cercetare academică</i>	Multiple lansări în producție (Microsoft Entra VC pilot, integrări SpruceID	Civic Pass - 2 milioane de verificări.	credențiale Deloitte KYC lansate pe KILT [2]; UX on-chain limitat.

În urma analizei comparative cuprinzătoare, putem deduce următoarele concluzii în ceea ce privește ecosistemul Ethereum:

1. **Standardele pe primul loc.** Ethereum este singurul Blockchain cu o metodă lansată pentru identități digitale W3C și suport masiv pentru portofele out-of-the-box.
2. **Robustețea rețelei în detrimentul tranzacțiilor pe secundă.** Sistemul de identități digitale are ca prioritate permanența și stabilitatea în favoarea performanțelor de viteză. Setul de validatori de peste un milion și timpul de offline al rețelei apropiat de zero oferă o garanție mai puternică, în comparație cu Solana, ce oferă mai multe tranzacții pe secundă, dar cu o perioadă și frecvență mult mai mare de întrerupere a rețelei.
3. **Interoperabilitate.** Aproape toate celelalte ecosisteme (Avalanche C-Chain, BNB Chain, Base, Polygon CDK) sunt sau urmează să fie compatibile cu Ethereum Virtual Machine, obținând un grad ridicat de knowledge-transfer între aceste rețele majore Blockchain.

5.3 Analiza Rezultatelor

5.3.1 Testarea Securității

Vom utiliza teste funcționale pentru a ne asigura că implementarea contractelor inteligente funcționează corespunzător în condiții normale. Testele implementate acoperă următoarele aspecte:

1. **Emiterea credențialelor:** se verifică emiterea credențialelor cu succes și faptul că nu pot fi emise duplicate;
2. **Verificarea credențialelor:** se verifică funcționalitatea de verificare a credențialelor și semnalarea credențialelor revocate ca fiind invalide;
3. **Revocarea credențialelor:** se verifică faptul că doar emitentul poate revoca credențialele, iar credențialele inexistente nu pot fi revocate.
4. **Afișarea credențialelor valide:** se verifică faptul că doar emitentul poate vizualiza credențialele, primindu-le doar pe cele valide.

Astfel, se utilizează testarea automată prin intermediul mediului de dezvoltare Truffle folosit pentru comunicarea cu rețeaua blockchain, implementarea contractelor inteligente și configurarea spațiului local de lucru blockchain și se obțin următoarele rezultate în urma testelor, conform Figurii 15.

```
Contract: Identity
  ✓ should return an empty array when no credentials exist
  ✓ should return credentials after issuance
  ✓ should return valid credentials only (84ms)
  ✓ should reflect revoked credentials as invalid (39ms)
  ✓ should handle multiple credentials for the same user (48ms)
  ✓ should issue a credential
  ✓ should revalidate an invalid credential (57ms)
  ✓ should not issue duplicate credentials if valid (97ms)
  ✓ should verify a credential
  ✓ should revoke a credential
  ✓ should not revoke a non-existent credential
  ✓ should not revoke a credential by a non-issuer

Number of Operations: 100
Load Test - Issue Credentials: 3.321s
Load Test - Verify Credentials: 828.927ms
Load Test - Revoke Credentials: 1.131s
Average Issue Time: 33.21 ms
Average Verify Time: 8.28 ms
Average Revoke Time: 11.3 ms
Results saved to test-results.json
  ✓ should handle load test for issuing, verifying, and revoking credentials (5284ms)
```

Figura 15: Rezultatul testelor functionale de securitate

Așadar, se poate observa robustețea sistemului în ceea ce privește atacuri în diferite scenarii de funcționare.

5.3.2 Evaluarea Confidențialității

Confidențialitatea datelor este respectată, atât la nivel de blockchain, cât și la nivel de contracte inteligente. Datele prelucrate și stocate în blockchain sunt mascate prin hash-ul acestora, astfel ele conțin doar identificatori necesari și hash-ul de date.

Atât în cazul tranzacțiilor de emitere și revocare, cât și în acela al evenimentelor de contract, date esențiale precum cheile private sau datele identității nu sunt dezvăluite, după cum se observă în Figura 16 și Figura 17:

[illegible]

Figura 16: Datele de tranzactie din mediul local de testare Ganache

[← BACK](#)

0xc624146ee77bb42faafce155b7ead7de88dcbce0ea7c169ba3e3eb011a1cb071 (0)

 To see rich event data [link a Truffle Project](#) containing the contract that emits this event.

TX HASH	LOG INDEX	BLOCK TIME
0xc624146ee77bb42faafce155b7ead7de88dcbce0ea7c169ba3e3eb011a1cb071	0	2024-05-23 15:09:25

CONTRACT

0x48D10d2fb62969c23DE57aC5D77790F74bd9a1dA

Figura 17: Eveniment de contract din mediul local de testare Ganache

5.3.3 Testarea Scalabilității

Se va executa un script ce simulează mai mulți utilizatori ce încearcă să emită și să verifice credențiale. Pentru cele trei operații de emiter, verificare și revocare s-au efectuat câte 100 de operații de verificare și s-au obținut următoarele rezultate, conform Figurii 18:

```
Number of Operations: 100
Load Test - Issue Credentials: 3.321s
Load Test - Verify Credentials: 828.927ms
Load Test - Revoke Credentials: 1.131s
Average Issue Time: 33.21 ms
Average Verify Time: 8.28 ms
Average Revoke Time: 11.3 ms
Results saved to test-results.json
```

Figura 18: Rezultatele testelor de scalabilitate

Se pot observa timpii totali de efectuare a celor 100 de operații și timpul mediu per operație, astfel atingând performanțe bune în ceea ce privește scalabilitate sistemului.

5.3.4 Testarea Utilizării - Proof of Concept

Testarea utilizării implică aplicabilitatea sistemului descentralizat de identități digitale într-un caz de utilizare real. Astfel, se va prezenta mai departe un **Proof of Concept**. Conceptul are la bază un modul de autentificare simplist, ce prezintă următoarele proprietăți:

- API dezvoltat aplicând modelul **MVC (Model View Controller)**, similar cu API-ul portofelului de identități digitale, cu ajutorul mediului de rulare **Node.js** și **Express**;
- UI dezvoltat în manieră similară, folosind **React.js**;

LOGIN

E-mail

Password

LOGIN

 Conectează-te cu Google

Connect with Digital Identity

Don't have an account? [Sign up](#)

Figura 19: Modul de autentificare

- bază de date **PostgreSQL**;
- prezintă mecanisme specifice unui modul de autentificare, precum RBAC (Role Based Access Control), token pentru sesiune, filtrare și limitare a fluxului de date, etc.
- este găzduit local, iar infrastructura de lansare a fost dezvoltată folosind **Docker**, **Kubernetes** și **Terraform**.

După cum reiese în Figura 19, se poate observa funcționalitatea de autentificare și înregistrare folosind un cont Google, o modalitate populară în modulele de autentificare ale diverselor platforme.

Așadar, acest Proof of Concept urmează a demonstra aplicabilitatea portofelului de identități digitale, prin oferirea unei funcționalități similare celei de *Conectează-te cu Google*. Scenariul de funcționare urmează fluxul de mai jos:

1. În urma apăsării butonului *Connect with Digital Identity*, butonul va redirecționa utilizatorul către componenta UI din cadrul portofelului de identități digitale(*ui/chooser*) ce listează toate identitățile valide asociate portofelelor Ethereum conectate, așa cum se observă în Figura 20.
2. MetaMask face o cerere către utilizator pentru a semna distribuția datelor identității digitale către partea terță, în cazul de față modulul de autentificare, conform Figurii 21.
3. Modulul de autentificare primește datele identității digitale și creează un cont pentru acesta, populând baza de date și precompletând informații, precum țara de reședință.

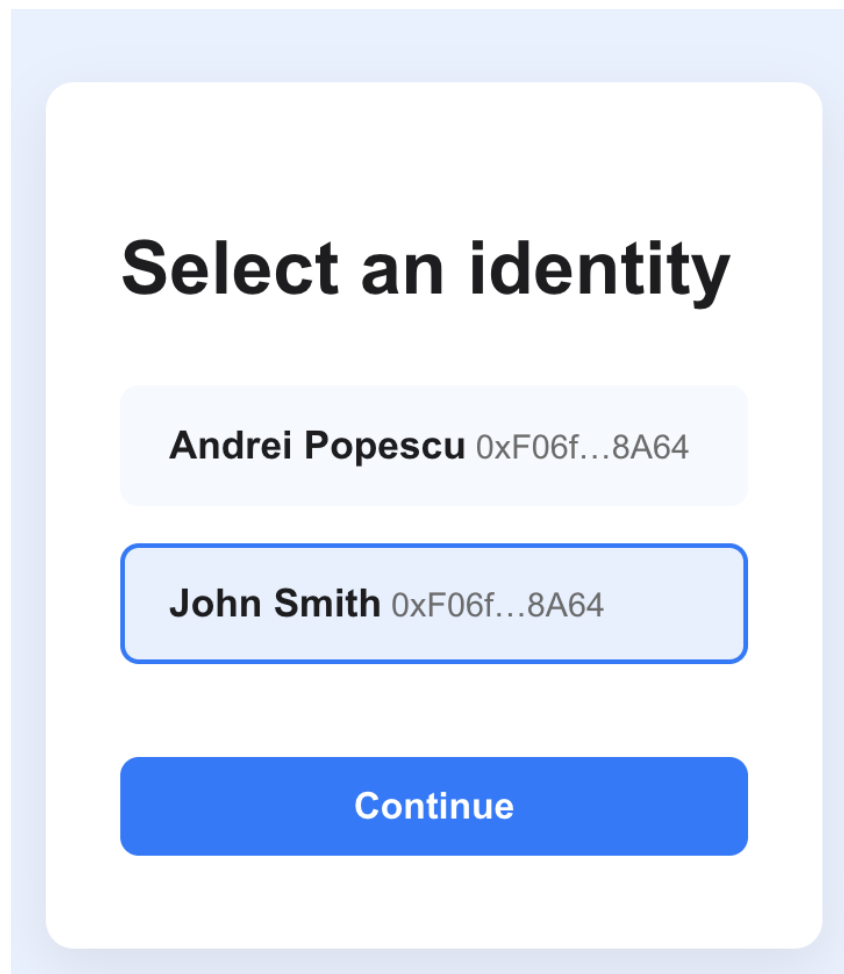


Figura 20: Alegere identitate digitală pentru înregistrare

Astfel, sistemul descentralizat de identități digitale este aplicat într-un scenariu de funcționare real și util, ce are potențialul de a fi adoptat la scară largă atât pentru scopul prezentat, cât și extins pentru mai multe tipuri de scenarii de funcționare.

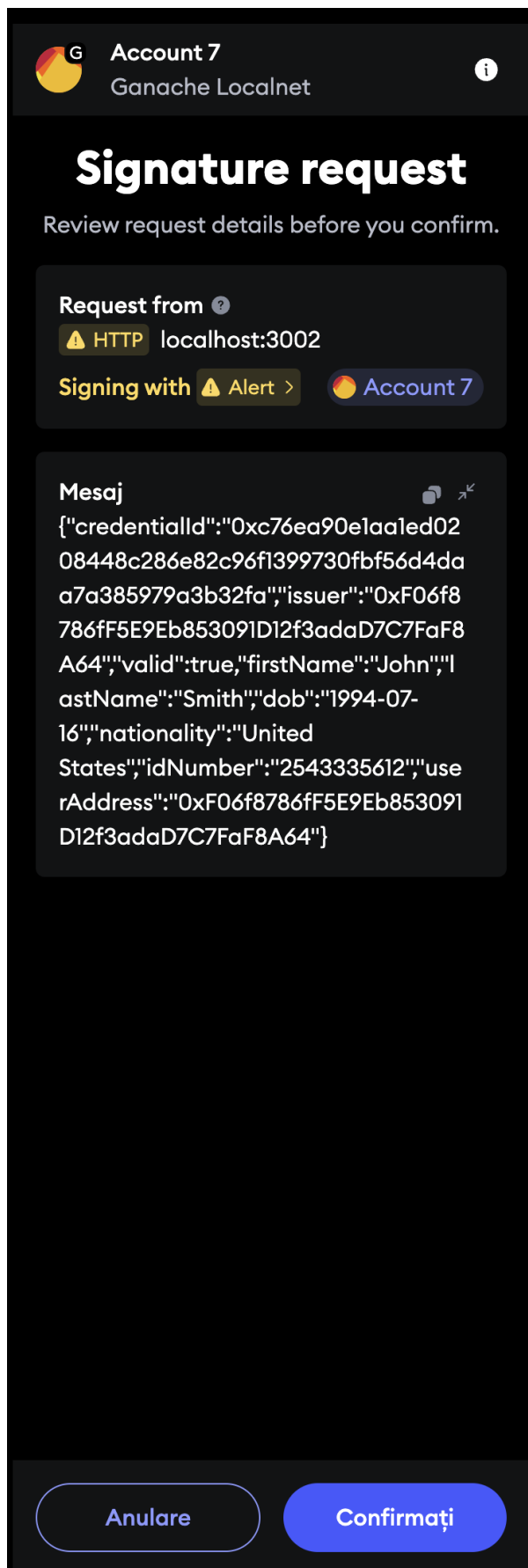


Figura 21: Cerere semnătură de la MetaMask

Hello, John Smith!

CancelLogout

Save Changes

Delete Account

Delete Account

Figura 22: Cont creat în modulul de autentificare

6 METODOLOGIA DE CERCETARE ȘI CONTRIBUȚII PERSONALE

6.1 Metodologia de Cercetare

Metodologia de cercetare îmbină cercetarea documentată, design-ul și dezvoltarea sistemului și testarea empirică a acestuia pentru a evalua sistemul propus. Metodologia implică:

1. **Analiza articolelor din domeniu:** Analiza articolelor științifice existente ce abordează astfel de sisteme și avansurile tehnologice în sistemele de identitate bazate pe blockchain și principii SSI;
2. **Design-ul sistemului:** Design-ul unei arhitecturi de sistem, a algoritmilor criptografici și a logicii de emitere, revocare și revalidare a identităților digitale bazate pe contracte inteligente, având ca fundament tehnologic principiile SSI și Blockchain;
3. **Dezvoltarea unei soluții complete:** Implementarea și dezvoltarea unui sistem complet, ce aplică într-un mod practic sistemul descentralizat, demonstrând, astfel, relevanța sa în contextul tehnologic actual;
4. **Testare empirică:** Implementarea unui set cuprinzător de teste funcționale și de integrare pentru a analiza metricile de securitate, confidențialitate și performanță;
5. **Analiză comparativă:** Analiză cuprinzătoare a posibilelor soluții Blockchain integrate în sistemul descentralizat de identități digitale;
6. **Dezvoltare și prezentare PoC:** Implementarea unui Proof of Concept cu scopul de a demonstra aplicabilitatea sistemului de identități digitale într-un caz de utilizare real;

6.2 Contribuțiile Personale

6.2.1 Contribuțiile Teoretice

Această lucrare de disertație contribuie la înțelegerea teoretică de a aplica tehnologia blockchain și principiile Self-Sovereign Identity (SSI) în administrarea identității digitale. Este analizat potențialul și limitările acestor tehnologii, adresând lacunele actuale în lucrările științifice existente legate de confidențialitate, securitate și controlul utilizatorului.

6.2.2 Contribuțiile Practice

Din punct de vedere practic, această lucrare prezintă o variantă incipientă a un sistem complet ce aplică sistemul descentralizat bazat pe structura blockchain, având scopul de a demonstra fezabilitatea unui sistem de verificare a identității descentralizat. Acest sistem include un portofel digital de identitate complet funcțional și contracte inteligente pentru administrarea credențialelor, oferind un fundament pentru viitoarele inovări în domeniul de sisteme de identități digitale.

Mai mult, în cadrul lucrării de cercetare a fost prezentat un Proof of Concept, cu scopul de a demonstra aplicabilitatea sistemului descentralizat de identități digitale într-un scenariu simulat de funcționare.

7 CONCLUZII, REZULTATE ȘI PLAN DE CERCETARE VIITOR

7.1 Concluzii

Sistemul descentralizat de verificare a identității digitale demonstrează aplicarea practică a tehnologiei blockchain și a principiilor SSI în îmbunătățirea management-ului de identitate digitală. Această lucrare de cercetare abordează provocările cu privire la sistemele de acest tip legate de confidențialitate, securitate și controlul utilizatorului, oferind o soluție sigură, centrată pe utilizator pentru verificarea identității digitale.

7.2 Rezultate

În cadrul disertației se dezvoltă cu succes un prototip demonstrativ, ce prezintă fezabilitatea și beneficiile unui sistem descentralizat de verificare a identității digitale. Rezultatele subliniază potențialul sistemului de a îmbunătăți administrarea identității digitale prin oferirea unei soluții sigure, ce protejează confidențialitatea utilizatorului și este centrat pe acesta.

7.3 Plan de Cercetare Viitor

Planul de Cercetare Viitor include cercetarea continuă și amănunțită pentru a atinge următoarele obiective:

1. Analiza într-un mod mai complex și detaliat scalabilitatea sistemului;
2. Identificarea și abordarea mecanisme de conservare a confidențialității mult mai avansate;
3. Cercetarea și aplicarea principii de design centrate pe utilizator pentru a îmbunătăți experiența utilizării;
4. Extinderea funcționalităților cu scopul obținerii unei soluții complete de gestiune a identităților digitale;
5. Încurajarea adopției pe scara largă a sistemelor de identitate descentralizate prin interoperabilitatea cu platformele existente;
6. Dezvoltarea unui formular de emitere al identității mult mai complex, având o procesare și validare mai amplă a identității, integrat cu mecanisme de analiză și validare a documentelor oficiale;
6. Dezvoltarea unei **strategii de integrare și dezvoltare continue (CI/CD pipeline)**

pentru crearea unor condiții optime lansării în producție a sistemului dezvoltat ca soluție asupra problemei.

BIBLIOGRAFIE

- [1] Civic (solana project). <https://solanacompass.com/projects/civic>. Accessed 2025-06-08.
- [2] Kilt (polkadot parachain) — parachains.info. https://parachains.info/details/kilt_polkadot. Accessed 2025-06-08.
- [3] Hyperledger Indy White Paper. Technical report, Hyperledger Foundation, 2019.
- [4] Good Health Pass Interoperability Blueprint. Technical report, Trust Over IP Foundation, 2021.
- [5] Introduction to Trust Over IP. Technical report, Trust Over IP Foundation, 2021.
- [6] ISO/IEC 18013-5:2021 – Personal identification – Mobile driver's licence (mDL). International Standard, 2021.
- [7] EU Digital Identity Wallet – Architecture and Reference Framework. GitHub Pages, 2023.
- [8] Regulation (EU) 2024/1183 establishing a European Digital Identity Framework. Official Journal of the European Union L 115, 2024.
- [9] Ismael Aguilera-López, Tiago M. Fernández-Caramés, and Paula Fraga-Lamas. Leveraging Zero-Knowledge Proofs for Blockchain-Based Identity Management: A Survey. *Journal of Information Security and Applications*, 80:103678, 2023.
- [10] Christopher Allen. The path to self-sovereign identity. 04 2016.
- [11] Eranga Bandara, Xueping Liang, Peter Foytik, Sachin Shetty, and Kasun De Zoysa. A blockchain and self-sovereign identity empowered digital identity platform. pages 1–7, 07 2021.
- [12] Jorge Bernal Bernabe, Jose Luis Canovas Sanchez, José Hernández-Ramos, Rafael Torres Moreno, and Antonio Skarmeta. Privacy-preserving solutions for blockchain: Review and challenges. *IEEE Access*, PP, 11 2019.
- [13] Pelle Braendgaard and Joel Torstensson. Eip-1056: Ethereum lightweight identity. <https://eips.ethereum.org/EIPS/eip-1056>, May 2018. Accessed on 2025-06-08.
- [14] Decentralized Identity Foundation. DIDComm Messaging Specification v2.0, 2023.

- [15] Omar Dib and Khalifa Toumi. Decentralized identity systems: Architecture, challenges, solutions and future directions. *Annals of Emerging Technologies in Computing (AETiC)*, 4(5):19–40, 2020.
- [16] Electric Capital Partners, LLC. 2024 crypto developer report. <https://www.developerreport.com/developer-report>, December 2024. Accessed 2025-06-08.
- [17] European Commission. European Blockchain Services Infrastructure (EBSI) – Overview, 2024. Web page.
- [18] Rachel Benchaya Gans, Jolien Ubacht, and Marijn Janssen. Governance and Societal Impact of Blockchain-Based Self-Sovereign Identities. *Policy and Society*, 41(3):402–415, 2022.
- [19] Daniel Hardman et al. Aries RFC 0003: Protocols. Hyperledger RFC, 2019.
- [20] Helius Dev. A complete history of solana outages: Causes and fixes. <https://www.helius.dev/blog/solana-outages-complete-history>, March 2025. Published approx. March 8 2025; accessed 2025-06-08.
- [21] Wenqing Li, Zhenguang Liu, Jianhai Chen, and Qinming He. Towards Blockchain Interoperability: A Comprehensive Survey on Cross-Chain Solutions. *Blockchain: Research and Applications*, 100:100286, 2025.
- [22] Luker. Metamask security monthly: February 2024. <https://metamask.io/news/security/metamask-security-monthly-february-2024>, March 2024. Accessed 2025-06-08.
- [23] Satoshi Nakamoto. Bitcoin: A peer-to-peer electronic cash system. *Cryptography Mailing list at https://metzdowd.com*, 03 2009.
- [24] Abylay Satybaldy. Usability Evaluation of SSI Digital Wallets. In *Privacy and Identity Management*, IFIP AICT, pages 101–117. 2023.
- [25] Max Sauer, Christoph Becker, Andreas Oberweis, Simon Pfeifer, Akim Stark, and Jan Sürmeli. User Experience and Information Security Implications of Digital Identity Wallets. In *Proc. ICICM 2024*, 2024.
- [26] Frederico Schardong and Ricardo Custódio. Self-Sovereign Identity: A Systematic Review, Mapping and Taxonomy. *Sensors*, 22(15):5641, 2022.
- [27] Daria Schumm, Rahma Mukta, and Hye-young Paik. Efficient Credential Revocation Using Cryptographic Accumulators. In *Proc. IEEE ICBC 2023*, 2023.
- [28] G Sreenath, Gowri T Sridhar, Aditya A Sannabhadti, Robin Mercy S J, and Manjunath R Kounte. Blockchain based digital identity solution. In *2024 2nd International Conference on Intelligent Data Communication Technologies and Internet of Things (IDCloT)*, pages 387–391, 2024.

- [29] Christopher Tobin and Daniel Reed. The Inevitable Rise of Self-Sovereign Identity. White paper, Sovrin Foundation, 2017.
- [30] Zoltan Vardai. Ethereum validators up 30% in a year, driven by institutional adoption. <https://cointelegraph.com/news/ethereum-validators-up-30-year-institutional-adoption>, October 2024. Accessed 2025-06-08.
- [31] World Wide Web Consortium. Decentralized Identifiers (DID) v1.0. W3C Recommendation, August 2021.
- [32] World Wide Web Consortium. Verifiable Credentials Data Model 1.1. W3C Recommendation, March 2022.
- [33] World Wide Web Consortium. Bitstring Status List v1.0. W3C Proposed Recommendation, March 2025.