ROMÂNIA

(19) OFICIUL DE STAT
PENTRU INVENŢII ŞI MĂRCI
Bucureşti

(11) **RO 138235 A0**

(51) Int.Cl.
H04L 9/32 (2006.01);
G06F 21/31 (2013.01);
G06F 21/34 (2013.01);
G06F 21/62 (2013.01);
G06Q 20/40 (2012.01)

(12) # CERERE DE BREVET DE INVENŢIE

(21) Nr. cerere: **a 2023 00447**

(22) Data de depozit: **10/08/2023**

(41) Data publicării cererii:
30/05/2024 BOPI nr. **5/2024**

(71) Solicitant:
• **CRYPTODATA TECH S.R.L.**, *BD.PIPERA 1/II, VOLUNTARI, IF, RO*

(72) Inventatori:
• **BARLIGA SEBASTIAN**, *STR.REPUBLICII, NR.36, AP.1, BRAŞOV, BV, RO;*
• **COCORU DUMITRU**, *SPLAIUL UNIRII, NR.33, BL.M4, SC.2, ET.1, AP.41, SECTOR 3, BUCUREŞTI, B, RO;*
• **VAJAIALA-TOMICI CĂTĂLIN- MIHAI**, *STR.DUNĂRII, BL.L4, SC.1, ET.2, AP.10, ALEXANDRIA, TR, RO*

(54) # SISTEM ŞI METODĂ DE GESTIONARE A IDENTITĂŢILOR DIGITALE DESCENTRALIZATE

(57) **Rezumat:**

Invenţia se referă la un sistem şi la o metodă pentru gestionarea identităţilor digitale descentralizate, utilizate într-un mediu distribuit, pentru a realiza, într-un mod sigur şi integru, tranzacţii virtuale, transfer de documente şi comunicare criptată. Sistemul funcţionează pe baza tehnologiei de tip blockchain şi include: un dispozitiv (**DH**) hardware de tip token capabil să genereze şi să stocheze chei de criptare asociate unor identităţi (**ID**) descentralizate, un modul (**MAP**) de mapare pentru corespondenţa dintre adrese de e-mail şi identităţile (**ID**) digitale descentralizate, un modul (**MC**) de comunicare pentru e-mail şi chat criptat prin blockchain, un modul (**MConf**) de conformitate pentru recunoaşterea identităţilor în cadrul UE, un modul (**MID**) de identitate descentralizată pentru managementul identităţilor prin blockchain şi un modul (**AUT**) de autentificare care combină o autentificare în doi paşi cu o autentificare unică. Metoda conform invenţiei implică înrolarea utilizatorilor, generarea identităţilor descentralizate, autentificarea prin blockchain şi realizarea de tranzacţii virtuale utilizând identităţi descentralizate într-un sistem distribuit.

Revendicări: 16
Figuri: 5

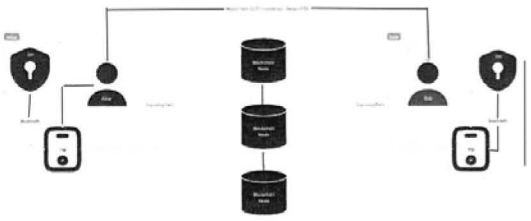

Fig. 1

RO 138235 A0

90

SISTEM ȘI METODĂ DE GESTIONARE A IDENTITĂȚILOR DIGITALE DESCENTRALIZATE

Invenția se referă la un sistem și o metodă de gestionare a identităților digitale descentralizate, destinate interconectării utilizatorilor într-un sistem distribuit, în scopul realizării de tranzacții virtuale, transfer de documente și comunicare internă prin intermediul unor servicii de e-mail și chat criptate.

În era digitală, securitatea și verificarea identității sunt esențiale, dar sistemele actuale se confruntă cu vulnerabilități semnificative. De la frauda de identitate și cenzură până la riscurile asociate cu gestionarea parolelor și securitatea portofelelor de criptomonede, există o nevoie urgentă de inovație în acest domeniu.

Se cunoaște din stadiul tehnicii soluția prezentată în cererea de brevet **WO 2022/248404A1**, publicată la data de 01.12.2022 - "A method for managing a digital identity". Cererea de brevet prezintă o metodă de gestionare unei identități digitale a unei entități într-un mod descentralizat. Pentru aceasta, se utilizează un domeniu pentru entitate, însoțit de un certificat securizat și direcționat către unul sau mai multe servere. Se definesc reguli de acces pentru identități digitale, iar accesul la datele stocate se realizează prin conexiuni peer-to-peer sigure într-o rețea globală distribuită. Sistemul rezultat este o rețea distribuită de entități, fiecare având cel puțin o identitate digitală asociată. Metoda și sistemul rezultate pot fi utilizate într-un mediu social, într-o rețea de mesagerie sau chiar într-un sistem de criptomonedă distribuit. De asemenea, acestea facilitează schimbul de date între utilizatori, sporind confidențialitatea și controlul asupra informațiilor.

Mai este cunoscută din stadiul tehnicii soluția prezentată în cererea de brevet **WO 2022/148765A1**, publicată la data de 14.07.2022 – "Method and system for managing digital, electronic communication". Cererea de brevet dezvăluie o metodă de gestionare a comunicării electronice într-un mod descentralizat, bazat pe tehnologia blockchain. Un utilizator creează un cont pe un serviciu de comunicare, iar acțiunile sale de comunicare sunt înregistrate ca tranzacții pe un blockchain asociat cu un token specific. Serverul central poate citi aceste tranzacții și oferi informații de prioritate bazate pe ele. Sistemul și metoda prezentate oferă o gestionare și monitorizare sigură și transparentă a comunicării digitale între utilizatori.

Soluţiile cunoscute din stadiul tehnicii prezintă două dezavantaje importante. Pe de o parte, fără implementarea unei măsuri de securitate suplimentară, cheile private utilizate în sistemele blockchain sau în metodele de gestionare a identităţilor pot fi vulnerabile la atacuri şi furt de date. Pe de altă parte, fără utilizarea unei soluţii tehnice de conformitate, scalabilitatea soluţiilor prezentate în stadiul tehnicii este limitată şi dependentă de aria geografică în care sunt implementate.

În general, sistemele de comunicare centralizate tradiţionale, inclusiv VoIP (Voice over IP) şi email, cunoscute în stadiul tehnicii, prezintă următoarele dezavantaje:

- creează un singur punct de eşec: dacă serverul central se opreşte, întregul sistem poate fi perturbat;

- ridică probleme de confidenţialitate: serverul central are acces la toate datele care trec prin el;

- serverul central este o ţintă pentru hackeri şi actori rău intenţionaţi care doresc să intercepteze sau să manipuleze datele;

- serverele centrale pot fi supuse supravegherii şi cenzurii, limitând libertatea de exprimare şi accesul la informaţii. Sistemele de comunicare bazate pe WebRTC, precum WhatsApp, Signal şi altele, pot fi uşor blocate de către autorităţi;

- probleme de performanţă: în cazul în care un număr mare de utilizatori încearcă să acceseze serverul în acelaşi timp, acesta poate deveni supraîncărcat generând întârzieri sau pierderi de date sau, în funcţie de distanţa geografică dintre server şi client, la latenţe ridicate;

- furtul de identitate şi atacurile de tip phising au mai multe şanse de succes deoarece verificarea identităţii se realizează prin metode tradiţionale de autentificare, precum utilizarea parolelor. În plus, serverul are acces la datele de autentificare ale utilizatorilor, ceea ce reprezintă o vulnerabilitate majoră pentru confidenţialitatea şi securitatea datelor;

- este dificilă verificarea faptului că un mesaj provine de la persoana care pretinde că l-a trimis. Acest lucru poate duce la probleme de încredere şi poate permite atacuri de tip "man-in-the-middle";

- fără un mod sigur de a verifica că datele nu au fost alterate, utilizatorii nu pot fi siguri că informaţiile pe care le primesc sunt exacte şi de încredere;

- sunt vulnerabile la atacuri de tip "Denial of Service" (DoS) care poate inunda serverul cu trafic inutil ce poate duce la întreruperi ale serviciului şi poate împiedica utilizatorii să comunice.

Pentru a depăşi deficienţele soluţiilor identificate în stadiul tehnicii, invenţia de faţă introduce un protocol descentralizat pentru comunicare şi autentificare, care utilizează tehnologia blockchain pentru securizarea şi verificarea identităţii. Prin eliminarea dependenţei de sisteme centralizate şi puncte unice de eşec, protocolul propus oferă o soluţie robustă şi rezistentă la atacuri. Integrând soluţii avansate pentru stocarea în portofel rece şi autentificarea descentralizată, acest protocol oferă utilizatorilor control deplin şi suveranitate asupra propriilor date şi active.

Invenţia de faţă oferă o alternativă viabilă la metodele centralizate care domină în prezent peisajul tehnologic. Cu potenţialul său de a revoluţiona modul în care comunicăm şi ne protejăm datele, protocolul descentralizat deschide calea către un viitor digital mai sigur şi mai liber.

Prezenta invenţie rezolvă problema tehnică a securizării cheilor private utilizate în sistemele blockchain simultan cu gestionarea identităţilor digitale într-un mod descentralizat şi global, într-un mod eficient şi scalabil.

Sistemul de gestionare a identităţilor digitale descentralizate, conform prezentei invenţii, înlătură dezavantajele menţionate mai sus prin aceea că funcţionează în baza tehnologiei blockchain şi este alcătuit din următoarele module funcţionale:

- un dispozitiv hardware reprezentat de un dispozitiv fizic de tip token, capabil să genereze şi să stocheze chei publice şi private asociate cu identitatea digitală a cel puţin unui utilizator, dispozitiv hardware care se conectează la terminalul mobil personal al utilizatorului care doreşte să genereze o identitate digitală descentralizată;

- un modul de mapare care are rolul de a are rolul de a realiza corespondenţa între adresele de e-mail ale utilizatorilor cu identităţile digitale descentralizate / identificatorii descentralizaţi;

- un modul de comunicare dedicat gestionării creării, trimiterii şi primirii de e-mailuri şi chat-uri criptate prin intermediul reţelei blockchain şi în baza criptării realizate utilizând cheile publice şi private stocate pe dispozitivul hardware de tip token;

- un modul de conformitate prevăzut cu eIDAS ce asigură recunoaşterea identităţilor digitale create şi gestionate, conform invenţiei, de către serviciile publice din alte state membre ale Uniunii Europene;

- un modul de identitate descentralizată care gestionează crearea, actualizarea şi ştergerea identităţilor descentralizate utilizând tehnologia blockchain prin asocierea unui document tip DID cu o adresă did:com, document ce conţine informaţii legate de identitatea utilizatorului şi utilizat pentru verificarea autenticităţii şi acreditărilor acestuia şi

- un modul de autentificare ce combină autentificarea în doi paşi şi autentificarea unică ce permite gestionarea securizată a identităţilor descentralizate şi comunicarea criptată.

Într-un exemplu preferat de realizare, dispozitivul hardware al sistemului permite efectuarea de operaţiuni criptografice fără a dezvălui valoarea cheii de criptare în sine, asigurând astfel un nivel suplimentar de protecţie.

Într-un alt exemplu preferat de realizare, fiecare dintre identităţile digitale ale utilizatorilor, gestionate de sistemul conform invenţiei, este legată de o pereche de chei criptografice, constând dintr-o cheie privată, păstrată în siguranţă în cadrul cheii de securitate certificată FIPS 140-02, folosită pentru semnarea cererilor de tranzacţie, şi o cheie publică, utilizată de nodurile reţelei blockchain, pentru verificarea semnăturii digitale.

Într-un alt exemplu preferat de realizare, adresa portofelului blockchain din cadrul modulului de identitate descentralizată este utilizată ca identificator did:com.

În mod avantajos, documentul care conţine informaţii legate de o identitate descentralizată este stocat pe blockchain şi poate fi accesat şi verificat de orice utilizator al reţelei.

Într-un exemplu alternativ de realizare, modulul de autentificare foloseşte o cheie de securitate prin WebAuthn şi verifică identitatea unui utilizator cu ajutorul documentului ce conţine informaţiile legate de o identitate descentralizată stocat pe blockchain.

În mod avantajos, stocarea cheilor de securitate se face într-un mediu fizic, izolat de Internet şi de alte reţele potenţial compromise iar operaţiunile criptografice realizate nu dezvăluie valoarea cheii în sine.

Într-un exemplu preferat de realizare, dispozitivul hardware este compatibil cu o varietate de dispozitive şi platforme şi, prin intermediul unei conexiuni de tip Bluetooth criptate, poate comunica cu telefoane mobile, tablete, calculatoare şi alte dispozitive compatibile.

Metoda de gestionare a identităţilor digitale descentralizate, conform invenţiei, înlătură dezavantajele menţionate anterior prin aceea că implică realizarea următorilor paşi operaţionali:

- se realizează înrolarea utilizatorului şi generarea de identităţi descentralizate prin utilizarea dispozitivului hardware şi instalarea unei aplicaţii mobile tip portofel electronic care reprezintă punctul de acces la utilizatorilor la o reţea de tip blockchain şi la sistemul de gestionare a identităţilor;

- se realizează autentificarea şi autorizarea utilizatorului, utilizând cheia publică stocată în registrul blockchain şi asociată identităţii descentralizate create la pasul anterior pentru verificarea semnăturii digitale;

- se realizează interacţiunea cu reţeaua blockchain prin intermediul aplicaţiei mobile ce permite utilizatorului să trimită şi să primească tranzacţii, să gestioneze identităţi descentralizate şi să efectueze alte operaţiuni specifice blockchain-ului;

- se realizează tranzacţionări virtuale ale utilizatorilor autentificaţi la pasul anterior, inclusiv utilizarea de servicii de e-mail şi/sau de chat, transfer de documente, tranzacţionare de monede virtuale, toate fiind realizate cu asigurarea integrităţii şi a confidenţialităţii acestora;

- se realizează semnarea tranzacţiilor prin utilizarea aplicaţiei mobile care trimite datele către portofelul rece, fie prin conexiune fizică fie prin conexiune wireless tip Bluetooth; portofelul rece semnează tranzacţia folosind cheia privată stocată în mod sigur şi trimite semnătura înapoi aplicaţiei mobile;

- se transmit tranzacţiile semnate către reţeaua blockchain unde fiecare tranzacţie este verificată şi înregistrată în nodurile reţelei;

- se realizează sincronizarea periodică a aplicaţiei mobile cu reţeaua blockchain pentru a reflecta starea actuală a contului, tranzacţiilor şi identităţilor descentralizate ale utilizatorilor;

- se realizează închiderea în siguranţă a conexiunii cu portofelul *rece*, după finalizarea tranzacţiilor.

Într-un alt exemplu preferat de realizare, utilizatorii sistemului, conform metodei din prezenta invenţie, pot asigna una sau mai multe adrese de e-mail pentru identitatea descentralizată proprie şi pot căuta identităţi descentralizate ale altor utilizatori prin introducerea a cel puţin unei adrese de e-mail utilizând modulul de mapare.

În mod avantajos, aplicaţia mobilă, conform metodei din prezenta invenţie, permite utilizatorilor să gestioneze identităţile descentralizate şi să iniţieze şi să primească comunicaţii de tip WebRTC prin protocolul VOBP, folosind nodurile reţelei blockchain ca servere TURN.

Într-un exemplu alternativ de realizare, aplicaţia mobilă, conform metodei din prezenta invenţie, poate solicita portofelului *rece* să genereze şi să gestioneze chei, să furnizeze un număr aleatoriu securizat şi să efectueze alte operaţiuni criptografice, toate în conformitate cu standardele relevante.

Într-un exemplu preferat de realizare a invenţiei, generarea unei identităţi descentralizate conform metodei implică parcurgerea următoarelor etape:

- se generează un mnemonic conform algoritmului standardizat BIP-39 folosind capabilităţile cheii de securitate pentru a genera numere aleatorii;

- mnemonicul este transformat într-o sămânță criptografică folosind o funcție de hash și, eventual, o parolă suplimentară;

- sămânța este folosită pentru a deriva o cheie principală (master key) folosind algoritmul BIP-32; cheia principală va fi rădăcina ierarhiei de chei pentru portofelul de identități descentralizate;

- utilizând cheia principală și structura specifică blockchain-ului Cosmos SDK, se generează o adresă DID unică;

- se creează un document DID care conține informații legate de identitatea utilizatorului, inclusiv cheile publice, serviciile asociate și alte metadate;

- documentul DID este semnat digital cu cheia privată asociată și trimis către blockchain; blockchain-ul va funcționa ca un registru pentru toate documentele DID;

- nodurile blockchain verifică semnătura și integritatea documentului DID și în înregistrează în blockchain pentru a se asigura imutabilitatea și transparența identităților descentralizate;

- utilizatorul poate gestionare și actualiza documentul DID prin intermediul portofelului care gestionează identitățile descentralizate, folosind cheia de securitate și protocolul propus pentru autentificare și operațiuni criptografice.

În mod avantajos, integrarea tehnologiei WebRTC cu cea a tehnologiei blockchain se realizează, conform prezentei metode, prin intermediul a două componente esențiale: semnalizarea, pentru a stabili conexiunile între perechi în WebRTC și colectarea candidaților ICE, pentru a îmbunătăți traversarea NAT și a face rețeaua mai rezistentă la blocări și cenzură.

Într-un exemplu preferat de realizare a invenției, metoda utilizează pentru implementarea aplicației mobile tip portofel o componentă hardware specifică, o cheie de securitate care implementează un TPM dintr-un chip SoC aprobat de FIPS 140-02.

Într-un alt exemplu preferat de realizare, integrarea tehnologiei WebRTC, conform prezentei metode, se face urmând următorii pași operaționali:

- un utilizator inițiază o cerere de comunicare, de exemplu, un apel video, către un alt utilizator prin intermediul aplicației care implementează protocolul VOBP;

- fiecare nod blockchain acționează ca un server TURN, înlocuind serverele TURN tradiționale;

- utilizatorul inițiator generează o ofertă SDP și o trimite destinatarului prin intermediul blockchain-ului, folosind identificatorul did:com: specific;

- ambii utilizatori se autentifică reciproc folosind metoda de autentificare descentralizată, implicând cheia de securitate şi modulul de identitate descentralizată;

- utilizatorul destinatar generează un răspuns SDP şi îl trimite înapoi iniţiatorului prin blockchain;

- ambii utilizatori colectează candidaţii ICE prin nodurile blockchain, care acţionează ca servere STUN şi TURN.

- utilizatorii stabilesc o conexiune peer-to-peer, traversând NAT şi evitând cenzura, datorită naturii descentralizate a blockchain-ului;

- comunicaţia este securizată folosind criptarea şi cheia de securitate, care oferă un nivel suplimentar de protecţie;

- utilizatorii sunt împerecheaţi şi pot comunica prin WebRTC, beneficiind de toate avantajele VOBP, inclusiv lupta împotriva cenzurii şi securitatea îmbunătăţită.

- procesul de conexiune WebRTC este integrat cu aplicaţia mobilă de portofel şi cu modulul de identitate descentralizată, permiţând gestionarea securizată a identităţilor şi comunicarea criptată.

Sistemul şi metoda, conform invenţiei, prezintă următoarele avantaje:

- oferă comunicare descentralizată prin intermediul e-mailurilor şi chat-urilor blockchain, menţinând în acelaşi timp imutabilitatea şi încrederea inerente tehnologiei blockchain;

- cheile private sunt protejate prin tehnologii avansate de criptare şi de protecţie a datelor

- operaţiunile criptografice se realizează fără a se dezvălui valoarea cheii în sine, asigurându-se astfel un nivel suplimentar de securitate;

- face posibil ca doar utilizatorii legitimi să aibă acces la serviciile de e-mail şi chat criptate, datele personale ale acestora fiind protejate împotriva accesului neautorizat sau a falsificării;

- elimină necesitatea unei entităţi centrale de gestionare a identităţilor, ceea ce conduce la o autonomie mai mare şi o securitate îmbunătăţită a datelor utilizatorilor;

- asigură conformitatea cu standardele eIDAS ceea ce demonstrează utilizatorilor că soluţia propusă spre brevetare respectă standardele şi regulile impuse de Uniunea Europeană în domeniul identităţii digitale şi al securităţii cibernetice;

- toate tranzacţiile şi datele sunt înregistrate în mod transparent, oferind o pistă de audit clară şi verificabilă. Flexibilitatea şi extensibilitatea blockchain-ului permite adaptarea şi extinderea sistemului cu diverse aplicaţii şi cerinţe, inclusiv integrarea cu WebRTC pentru a îmbunătăţu comunicarea peer-to-peer şi a combate cenzura.

Se dă, în continuare, un exemplu de realizare a invenției, în raport cu figurile 1-5, care reprezintă:

- figura 1 – conexiunea VOBP (Voice Over Blockchain Protocol) între două persoane;
- figura 2 – conținutul unei identități descentralizate;
- figura 3 – conținutul tipic al unui document de identitate descentralizată;
- figura 4 – procesul de autentificare SSO;
- figura 5 – ierarhia cheilor deterministe BIP44.

Sistemul, conform invenției, funcționează în baza tehnologiei blockchain și este destinat gestionării identităților digitale descentralizate, a comunicării securizate și a conformității cu standardele eIDAS din Uniunea Europeană.

În sistemele tradiționale de comunicare peer-to-peer, cum ar fi WebRTC, una dintre provocări este traversarea NAT (Network Address Translation). Când un dispozitiv se află în spatele unui NAT, poate fi dificil pentru alte dispozitive să stabilească o conexiune directă cu acesta. Deși protocoale precum STUN (Session Traversal Utilities for NAT) și TURN (Traversal Using Relays around NAT) pot ajuta, acestea se bazează încă pe servere centralizate și nu rezolvă complet problema.

Sistemul și metoda de gestionare a identităților virtuale descentralizate, conform invenției, înlătură această problemă prin utilizarea unui protocol descentralizat conceput pentru a înlocui sistemele tradiționale de comunicarea VoIP (Voice over IP) cu un nou standard, denumit VOBP (Voice Over Blockchain Protocol), conform figurii 1.

Sistemul, conform invenției, este alcătuit din următoarele blocuri funcționale:

** un dispozitiv hardware **DH** care reprezintă componenta fizică a sistemului. Acesta este reprezentat de un dispozitiv fizic de tip token, capabil să genereze și să stocheze chei publice și private asociate cu identitatea digitală a cel puțin unui utilizator. Dispozitivul hardware **DH** se conectează la terminalul mobil personal al utilizatorului care dorește să genereze o identitate digitală descentralizată. Dispozitivul hardware **DH** utilizează tehnologii avansate de criptare și de protecție a datelor pentru a asigura faptul că nicio persoană neautorizată nu poate accesa sau extrage cheile private de criptare stocate pe acesta. Dispozitivul **DH** permite efectuarea de operațiuni criptografice fără a dezvălui valoarea cheii de criptare în sine, asigurând astfel un nivel suplimentar de securitate. Cheile publice și private asociate identităților digitale sunt esențiale în criptografia asimetrică, unde cheia publică este folosită pentru criptarea mesajelor și verificarea semnăturilor digitale, iar cheia privată este folosită pentru decriptare și semnarea mesajelor.

82

Identitatea fiecărui utilizator este legată de o pereche de chei criptografice, constând dintr-o cheie privată şi una publică. Cheia privată, păstrată în siguranţă în cadrul cheii de securitate certificată FIPS 140-02, este folosită pentru a semna cererile de tranzacţie, în timp ce cheia publică este utilizată de nodurile reţelei blockchain pentru a verifica semnătura digitală. Această metodă de autentificare descentralizată permite utilizatorilor să îşi controleze şi să îşi recupereze identitatea, fără a depinde de servicii centralizate.

** un modul de mapare **MAP** (ledger descentralizat). Acest modul are rolul de a realiza corespondenţa dintre adresele de e-mail ale utilizatorilor cu identităţile digitale descentralizate / identificatorii descentralizaţi **ID**. Un utilizator poate avea una sau mai multe adrese de e-mail însă doar o singură identitate descentralizată **ID**. Modulul de mapare **MAP** pune la dispoziţia utilizatorilor sistemului, conform invenţiei, un mijloc de accesare şi identificare a identităţilor descentralizate în cadrul reţelei blockchain. Fiecare utilizator îşi poate conecta una sau mai multe adrese de e-mail la identitatea sa digitală descentralizată **ID**. Modul în care funcţionează modulul de mapare **MAP** este similar cu sistemul DNS (Domain Name System) care asociază numele de domenii cu adresele IP (Internet Protocol) corespunzătoare. Aşa cum DNS-ul "traduce" numele de domenii în adrese IP, modulul de mapare **MAP** realizează conversia între adresele de e-mail şi identificatorii descentralizaţi **ID**.

Modulul de mapare **MAP** este integrat în cadrul blockchain-ului şi funcţionează similar cu un serviciu de nume de domeniu (DNS) sau cu serviciul de nume Ethereum (ENS), având rolul de a facilita procesul de descoperire a utilizatorilor în etapa iniţială a semnalizării VOBP. Pentru a înţelege mai bine funcţionarea modulului de mapare **MAP** se descrie mai jos principalele operaţiuni realizate de acesta:

1. Funcţionarea DNS: Un serviciu de nume de domeniu (DNS) este un sistem descentralizat care traduce numele de domeniu uşor de reţinut, cum ar fi "www.exemplu.com", în adrese IP numerice, care sunt utilizate de computere pentru a identifica serverele. Aceasta permite utilizatorilor să acceseze site-uri web folosind nume familiare, în loc să introducă adrese IP complexe. DNS-ul funcţionează ca o agendă telefonică pentru Internet, făcând legătura între numele de domeniu şi adresele IP corespunzătoare.

2. Aplicarea Principiilor DNS în Blockchain: Modulul de mapare **MAP** aplică principiile DNS în contextul blockchain, permiţând asocierea identităţilor descentralizate **ID** cu identificatori online precum adrese de e-mail sau conturi de social media. Acest lucru face ca **ID**-urile şi adresele

de portofel, care sunt greu de partajat şi de reţinut, să fie accesibile prin identificatori mai familiari şi mai uşor de utilizat.

3. Beneficiile Integrării cu Blockchain: Integrarea modulului de mapare **MAP** cu blockchain-ul aduce avantajele descentralizării, securităţii şi transparenţei. Utilizatorii au control deplin asupra informaţiilor pe care le partajează, iar datele sunt stocate într-un mod care previne manipularea neautorizată. Acest sistem de descoperire adaptat pentru blockchain facilitează comunicarea peer-to-peer şi promovează adoptarea tehnologiei VOBP.

4. Integrare cu Alte Module: Modulul de mapare **MAP** interacţionează cu alte module ale sistemului, inclusiv cu modulul de identitate descentralizată **MID** şi cu aplicaţia mobilă, oferind o experienţă de utilizare coerentă şi eficientă.

5. Facilitarea Comunicării Peer-to-Peer: Prin simplificarea procesului de mapare a utilizatorilor, modulul de mapare **MAP** contribuie la facilitarea comunicării peer-to-peer şi la promovarea adoptării tehnologiei VOBP.

** un modul de comunicare **MC** dedicat gestionării creării, trimiterii şi primirii de e-mailuri şi chat-uri criptate pe blockchain. Criptarea este realizată utilizând cheile publice şi private stocate pe dispozitivul hardware **DH** de tip token şi asigură confidenţialitatea şi autenticitatea mesajelor transmise între utilizatori. Prin implementarea comunicării pe blockchain, se asigură un grad ridicat de siguranţă şi integritate a informaţiilor. Modulul de comunicare **MC** este dotat cu tehnologii de criptare pentru a asigura confidenţialitatea şi integritatea comunicărilor, protejând utilizatorii împotriva interceptărilor şi a altor tipuri de atacuri. Modulul de comunicare **MC** poate utiliza IPFS (InterPlanetary File System), prin care fişierele pot fi accesate şi partajate fără a depinde de servere centralizate. Utilizarea IPFS permite stocarea conţinutului de e-mail, asigurând disponibilitatea acestuia chiar şi în cazul în care furnizorul de e-mail nu este disponibil.

** un modul de conformitate **MConf** prevăzut cu eIDAS (Electronic Identification, Authentication, and Trust Services) ce realizează compatibilitatea cu standardele eIDAS din Uniunea Europeană. Integrarea eIDAS asigură că soluţia respectă standardele şi regulile impuse de Uniunea Europeană în domeniul identităţii digitale şi al securităţii cibernetice. Modulul de conformitate **Mconf** asigură recunoaşterea identităţilor digitale create şi gestionate de sistemul conform prezentei invenţii de către serviciile publice din alte state membre ale Uniunii Europene, ceea ce asigură posibilitatea implementării pe scară largă şi interoperabilitate.

** un modul de identitate descentralizată **MID** care gestionează crearea, actualizarea şi ştergerea identităţilor descentralizate utilizând tehnologia blockchain. Modulul de identitate

descentralizată **MID** asociază un document de tip **DID** (Decentralized Identifier) cu o adresă did:com permițând gestionarea identităților și istoricizarea acestora. Documentul **DID** asociat cu adresa did:com conține informații legate de identitatea utilizatorului și se folosește pentru a verifica autenticitatea și acreditările acestuia.

Modulul de identitate descentralizată **MID** este esențial pentru gestionarea identităților în rețeaua blockchain. O identitate descentralizată **ID**, conform figurii 2, este un șir de text simplu, compus din trei părți: 1) identificatorul schemeil URL did, 2) identificatorul pentru metoda DID și 3) identificatorul specific metodei DID. În contextul prezentei invenții, adresa portofelului blockchain este utilizată ca identificator did:com:, având în vedere că implementarea de față se bazează pe Cosmos SDK și include un prefix specific.

Modulul de identitate descentralizată **MID** gestionează crearea, actualizarea și ștergerea identităților descentralizate pe blockchain, asociind un document **DID** cu o adresă de tip did:com:12345678asdasdads. Documentul **DID**, stocat pe blockchain, conține informații esențiale legate de identitatea utilizatorului, care sunt folosite pentru a verifica acreditările DID. Această abordare permite gestionarea transparentă și securizată a identităților, istoricizarea și urmărirea schimbărilor.

Un document **DID**, conform figurii 3, este o structură de date standardizată care conține informații legate de un identificator descentralizat **ID**. Acesta servește ca o legătură între DID și modul în care ID-ul poate fi utilizat. Documentul **DID** este stocat pe blockchain și poate fi accesat și verificat de oricine are acces la rețea.

Iată ce conține în mod tipic un document **DID**, conform figurii 3:

1. Identificatorul **ID**: Un șir unic care identifică subiectul **ID** (de obicei, utilizatorul sau entitatea asociată cu **ID**).

2. Chei Publice: Documentul **DID** include una sau mai multe chei publice, care pot fi utilizate pentru a verifica semnături digitale și a cripta comunicațiile.

3. Endpoint-uri de Serviciu: Acestea sunt URL-uri sau alte descriptori care indică modul în care se poate comunica cu subiectul **ID**. De exemplu, acestea pot include adrese pentru mesagerie, servicii web sau alte canale de comunicare.

4. Metadate și Atribute: Documentul **DID** poate conține și alte metadate sau atribute legate de subiectul **ID**, cum ar fi nume, adrese de e-mail, afilieri organizaționale sau orice altă informație relevantă pentru identitate.

5. Controlul de Acces şi Permisiuni: Documentul **DID** poate defini şi reguli şi permisiuni pentru cine poate accesa sau modifica documentul, oferind un control granular asupra gestionării identităţii.

6. Istoric şi Versiuni: În unele implementări, documentul **DID** poate include şi un istoric al modificărilor şi versiunilor anterioare, permiţând urmărirea şi auditarea schimbărilor.

** un modul de autentificare **AUT** de tip Single Sign-On / Two-Factor Authentication ce combină autentificarea în doi paşi (2FA) şi autentificarea Single Sign-On (SSO). Prin autentificarea în doi paşi, utilizatorii trebuie să furnizeze două elemente de autentificare diferite pentru a dovedi identitatea lor. Aceste elemente pot fi: ceva ce utilizatorul cunoaşte (parolă, pin), ceva ce utilizatorul deţine (token, dispozitiv mobil, cheie de securitate fizică) sau ceva ce utilizatorul este (amprentă proprie, retină).

Modulul de autentificare **AUT**, conform figurii 4, foloseşte o cheie de securitate prin WebAuthn şi implică realizarea următorilor paşi operaţionali:

a) Iniţierea Autentificării: Utilizatorul accesează o aplicaţie sau un serviciu care necesită autentificare. Aplicaţia solicită autentificare prin SSO şi redirecţionează utilizatorul către serviciul de autentificare centralizat, care utilizează protocolul propus în prezenta invenţie.
b) Solicitarea Cheii de Securitate: Serviciul de autentificare solicită utilizatorului să introducă cheia de securitate, care este echipată cu un TPM conform cu FIPS 140-02 şi comunică prin canalul criptat Bluetooth proprietar.
c) Generarea şi Verificarea Cererii: Modulul de identitate descentralizată **MID** generează o cerere de autentificare, folosind identificatorul did:com: specific blockchain-ului Cosmos SDK. Cheia de securitate semnează cererea, iar serviciul de autentificare verifică semnătura folosind cheia publică asociată cu identitatea descentralizată **ID**.
d) Verificarea Identităţii cu Blockchain: Serviciul de autentificare verifică identitatea utilizatorului cu documentul **DID** stocat pe blockchain, asigurând că informaţiile sunt corecte şi actualizate.
e) Generarea Token-ului SSO: După verificarea cu succes, serviciul de autentificare generează un token SSO, care este semnat digital pentru a asigura integritatea.
f) Redirecţionarea către Aplicaţie: Utilizatorul este redirecţionat înapoi către aplicaţia iniţială, cu token-ul SSO inclus. Aplicaţia verifică token-ul şi acordă accesul.
g) Accesul la Alte Servicii: Token-ul SSO permite utilizatorului să acceseze şi alte servicii şi aplicaţii asociate, fără a necesita autentificare repetată.

h) Integrarea cu Portofelul şi Modulul MID: Procesul de SSO este integrat cu aplicaţia mobilă de portofel şi cu modulul MID din prezenta cerere de brevet, permiţând gestionarea securizată a identităţilor şi comunicarea criptată.

i) Securitate Adiţională cu Cheia de Securitate: Cheia de securitate oferă un nivel suplimentar de securitate, protejând împotriva furtului de identitate şi a atacurilor de tip phishing.

Soluţia de stocare rece a cheilor de securitate, utilizată de prezenta invenţie, constă în păstrarea cheilor private într-un mediu fizic izolat de Internet şi de alte reţele potenţial compromise. Cheia de securitate, certificată FIPS 140-02, implementează această soluţie, oferind un dispozitiv hardware dedicat care stochează cheile într-un mod care le izolează de atacurile cibernetice.

Dispozitivul hardware **DH**, conform invenţiei, stochează în siguranţă cheile private asociate cu identitatea digitală a unui utilizator. Cheile private nu pot fi accesate sau extrase de persoane neautorizate. Operaţiunile criptografice sunt realizate fără a se dezvălui valoarea cheii în sine. Abordarea combină avantajele unui dispozitiv fizic securizat cu flexibilitatea şi accesibilitatea unei aplicaţii mobile, creând o soluţie robustă şi inovatoare pentru viitorul securizat al comunicării digitale.

Dispozitivul hardware **DH**, conform invenţiei, este compatibil cu o varietate de dispozitive şi platforme. Prin intermediul unei conexiuni de tip Bluetooth criptate, dispozitivul hardware **DH** poate comunica cu telefoane mobile, tablete, calculatoare şi alte dispozitive compatibile, oferind autentificare puternică şi operaţiuni criptografice într-o varietate de contexte.

În cadrul sistemului descentralizat, conform invenţiei, cheia de securitate poate fi utilizată ca element de autentificare în cadrul celui de-al doilea pas al autentificării. Utilizatorul introduce parola sa şi, apoi, trebuie să furnizeze cheia de securitate, care poate fi reprezentată de un dispozitiv hardware sau o aplicaţie mobilă specială (credenţiale), pentru a finaliza procesul de autentificare.

Autentificarea Single Sign-On (SSO) permite utilizatorilor să se autentifice o singură dată şi apoi să acceseze multiple aplicaţii sau servicii fără a fi nevoie să reintroducă credenţialele de autentificare pentru fiecare dintre ele.

În cadrul sistemului descentralizat, conform invenţiei, utilizatorii pot folosi cheia de securitate pentru a se autentifica o singură dată, ulterior având acces automat la diverse aplicaţii şi servicii, gestionate în mediul virtual descentralizat.

Sistemul conform invenţiei este construit pe baza unei reţele de tip blockchain care are capacitatea intrinsecă de a oferi confidenţialitate, robusteţe şi securitate. Fiecare tranzacţie este

validată şi înregistrată în multiple noduri din reţea, creând un istoric imutabil şi transparent, care face dificilă orice încercare de fraudă sau manipulare a datelor.

Prin utilizarea criptării şi a autentificării descentralizate, blockchain-ul permite utilizatorilor să îşi controleze şi să îşi protejeze datele, fără a depinde de o autoritate centrală, ceea ce reduce semnificativ riscul de compromitere sau abuz.

Toate tranzacţiile şi datele sunt înregistrate în mod transparent, oferind o pistă de audit clară şi verificabilă. Flexibilitatea şi extensibilitatea blockchain-ului permit adaptarea şi extinderea acestuia pentru a se potrivi cu diverse aplicaţii şi cerinţe, inclusiv integrarea cu WebRTC pentru a îmbunătăţi comunicarea peer-to-peer şi a combate cenzura.

Diferenţa dintre utilizarea unui ledger descentralizat, registru descentralizat, şi unul centralizat este că se elimină existenţa unui punct central de control care să deţină şi să administreze întregul sistem. În cazul sistemului de faţă, datele şi tranzacţiile sunt distribuite şi stocate pe mai multe noduri independente care lucrează în colaborare pentru a menţine integritatea şi securitatea reţelei.

Integrarea modulelor menţionate anterior într-un sistem integrat, conform invenţiei, conduce la realizarea unei platforme securizate, descentralizate şi compatibile cu reglementările UE pentru gestionarea identităţilor digitale şi comunicarea criptată.

Metoda de gestionare a identităţilor descentralizate, conform invenţiei, elimină punctele unice de eşec şi contribuie la crearea unui sistem distribuit mai sigur şi cu o rezilienţă mai bună la atacurile cibernetice.

Metoda, conform invenţiei, prezintă următorii paşi operaţionali:

- pasul 1: înrolarea şi generarea de identităţi descentralizate - utilizatorul intră în posesia tokenului şi instalează o aplicaţie mobilă dedicată sistemului, conform invenţiei. Prin intermediul aplicaţiei mobile, utilizatorul este instruit să se înroleze şi, în urma parcurgerii acestui proces, se creează o identitate descentralizată utilizând tehnologia blockchain. Aceasta implică crearea de chei publice şi private, care sunt salvate automat pe token. Specific prezentei invenţii, tokenul nu permite extragerea cheilor private.

Pe tot parcursul utilizării sistemului şi a metodei, conform invenţiei, tokenul se află conectat la terminalul mobil al utilizatorului. Cheia publică este înregistrată în ledger-ul blockchain.

- pasul 2: autentificare şi autorizare – pentru a efectua tranzacţii sau pentru a accesa mediul virtual dedicat, prin intermediul aplicaţiei software specifice prezentei invenţii, utilizatorul trebuie

să se autentifice. Folosind tokenul conectat la teminalul mobil pe care se află instalată aplicaţia mobilă, utilizatorul dovedeşte că deţine cheia privată asociată cu identitatea descentralizată prin furnizarea unei semnături digitale valide. Sistemul va verifica semnătura digitală utilizând cheia publică stocată în ledger-ul blockchain şi autorizează utilizatorul pentru a efectua tranzacţiile dorite în mediul virtual.

Tokenul poate fi conectat la terminalul mobil al dispozitivului fie wireless, prin tehnologie Bluetooth, fie fizic utilizând portul USB al terminalului.

Autentificarea descentralizată se bazează pe tehnologia blockchain, care permite validarea şi verificarea identităţii fără a depinde de o autoritate centrală. Fiecare utilizator îşi controlează propriile credenţiale şi date, iar procesul de autentificare este realizat prin intermediul nodurilor din reţea. Aceasta înseamnă că niciun terţ nu deţine sau controlează informaţiile sensibile, reducând astfel riscul de abuz sau furt.

- pasul 3: utilizarea de identităţi virtuale descentralizate – utilizatorii sistemului pot asigna una sau mai multe adrese de e-mail pentru identitatea descentralizată proprie. Utilizatorii pot căuta identităţi descentralizate ale altor utilizatori prin introducerea a cel puţin unei adrese de e-mail utilizând modulul de mapare **MAP** ce face corespondenţa dintre adresele de e-mail ale utilizatorilor şi identităţile lor descentralizate, opţiune de căutare disponibilă tuturor utilizatorilor sistemului.

Fiecare utilizator este administratorul propriu al datelor personale introduse în sistem.

- pasul 4: tranzacţionare virtuală – utilizatorii autentificaţi în mediul virtual dedicat utilizează identitatea descentralizată în locul unui username tradiţional. Tranzacţiile realizate de aceştia sunt înregistrate în ledger-ul blockchain, asigurând transparenţa şi imutabilitatea datelor.

Metoda, conform invenţiei, permite utilizarea serviciilor de e-mail şi / sau de chat, transferul de documente, tranzacţionarea de monede virtuale utilizând identităţi descentralizate într-un sistem în care cheile publice sunt salvate în ledger-ul unui blockchain iar cheile private într-un dispozitiv de tip token ce asigură integritatea şi confidenţialitatea acestora.

Procesul de generare a unei identităţi descentralizate **ID** (Decentralized Identifier) dintr-un mnemonic, transformându-l într-o sămânţă, apoi într-o cheie principală, creând un portofel pentru gestionarea identităţilor descentralizate şi trimiterea unui document DID către registrul blockchain poate fi descris astfel:

a) generarea mnemonicului: utilizatorul foloseşte capabilităţile cheii de securitate pentru a genera numere aleatorii, care sunt apoi utilizate pentru a crea un mnemonic conform

algoritmului standardizat BIP-39. Acest mnemonic este o frază secretă care va fi folosită pentru a deriva cheia privată;

b) transformarea în sămânță: mnemonicul este transformat într-o sămânță criptografică folosind o funcție de hash și, eventual, o parolă suplimentară. Acest proces este conform cu standardul BIP-39;

c) derivarea cheii principale: sămânța este folosită pentru a deriva o cheie principală (master key) folosing algoritmul BIP-32. Această cheie principală va fi rădăcina ierarhiei de chei pentru portofelul care gestionează identitățile descentralizate;

d) crearea portofelului care va gestiona identitățile descentralizate: cheia principală este folosită pentru a crea un portofel pentru gestionarea identităților descentralizate, care va gestiona cheile și identitățile descentralizate ale utilizatorului. Portofelul poate fi stocat într-o cheie de securitate cu un TPM conform cu FIPS 140-02, pentru securitate suplimentară;

e) generarea adresei DID: utilizând cheia principală și structura specifică blockchain-ului Cosmos SDK, se generează o adresă DID unică cu prefixul did:com:.

f) crearea documentului DID: se creează un document DID care conține informații legate de identitatea utilizatorului, inclusiv cheile publice, serviciile asociate și alte metadate. Documentul DID este formatat conform standardului stabilit de https://www.w3.org/TR/did-core/

g) trimiterea documentului DID către blockchain: documentul DID este semnat digital cu cheia privată asociată și trimis către blockchain. Blockchain-ul va funcționa ca un registru (ledger) pentru toate documentele DID.

h) verificarea și înregistrarea pe blockchain: nodurile blockchain verifică semnătura și integritatea documentului DID și în înregistrează în blockchain. Acest proces asigură imutabilitatea și transparența identităților descentralizate.

i) gestionarea și actualizarea documentelor DID: utilizatorul poate gestionare și actualiza documentul DID prin intermediul portofelului DID, folosind cheia de securitate și protocolul propus pentru autentificare și operațiuni criptografice.

Metoda, conform invenției, permite stocarea credențialelor într-o formă criptată și securizată pe blockchain. Utilizatorii își pot verifica identitatea prin semnarea digitală a cererilor, iar nodurile din rețea validează aceste semnături. Acest proces asigură confidențialitatea și integritatea datelor și permite autentificarea rapidă și eficientă.

Un alt avantaj al metodei de autentificare descentralizată este rezistența la cenzură și interferențe. Fără o autoritate centrală care să poată fi atacată sau compromisă, sistemul rămâne funcțional chiar și în condiții de atac sau restricții guvernamentale. Aceasta îmbunătățește disponibilitatea și accesibilitatea serviciilor, promovând libertatea și autonomia digitală.

Un aspect esențial al metodei de autentificare descentralizată propuse este utilizarea standardelor blockchain, cum ar fi BIP32 și mnemonics, pentru a permite utilizatorului să își recupereze și să își controleze identitatea. Implementarea portofelului HD (Hierarchical Deterministic) este un subprodus al mai multor Propuneri de Îmbunătățire Bitcoin (BIP), în special BIP32 pentru criptografia de bază și generarea de chei, BIP39 pentru fraza de inițiere și recuperare, și BIP44 pentru ierarhia de conturi multi-protocol, a se vedea figura 5. Spre deosebire de serviciile centralizate, unde accesul la un număr de telefon, o adresă de e-mail sau alte date poate fi restricționat sau întrerupt, în acest sistem, utilizatorul este adevăratul proprietar al identității sale.

Metoda, conform invenției, realizează integrarea tehnologiei WebRTC cu cea a tehnologiei blockchain prin intermediul a două componente esențiale: semnalizarea și colectarea candidaților ICE (Interactive Connectivity Establishment), după cum se poate vedea în figura 1.

Semnalizarea este procesul prin care se stabilesc conexiunile între perechi în WebRTC.

Se utilizează blockchain pentru semnalizare, deoarece acesta realizează deja această funcție prin conectarea și descoperirea nodurilor în rețea. Aceasta înseamnă că semnalizarea devine mai robustă și descentralizată, eliminând dependența de servere centrale și reducând vulnerabilitățile.

Colectarea candidaților ICE joacă un rol crucial în rețea, deoarece nodurile vor implementa serverele STUN și TURN. Fiecare nod va funcționa și va acționa ca un server TURN, facilitând descoperirea și conexiunea între perechi. Aceasta îmbunătățește semnificativ traversarea NAT și face rețeaua mai rezistentă la blocări și cenzură.

Prin aceste modificări, protocolul WebRTC este îmbunătățit pentru a se potrivi cu cerințele actuale de securitate, confidențialitate și libertate de comunicare. Integrarea cu blockchain transformă semnalizarea și colectarea candidaților ICE, păstrând în același timp restul protocolului neschimbat. Rezultatul este o soluție inovatoare care îmbunătățește WebRTC, oferind o platformă de comunicare mai sigură, mai liberă și mai rezistentă la interferențe și cenzură.

Procesul de stabilire a unei conexiuni WebRTC și împerechere poate fi descris astfel, referindu-se la modulele și componentele specifice prezentei invenții, conform figurii 1:

1. Iniţierea Conexiunii: Un utilizator iniţiază o cerere de comunicare (de exemplu, un apel video) către un alt utilizator prin intermediul aplicaţiei care implementează protocolul VOBP (Voice Over Blockchain Protocol) propus.

2. Descoperirea şi Conectarea la Noduri Blockchain: Aplicaţia utilizează modulul blockchain pentru a descoperi şi a se conecta la nodurile blockchain relevante. Fiecare nod blockchain acţionează ca un server TURN, înlocuind serverele TURN tradiţionale.

3. Generarea şi Trimiterea Ofertei SDP: Utilizatorul iniţiator generează o ofertă SDP (Session Description Protocol) şi o trimite destinatarului prin intermediul blockchain-ului, folosind identificatorul did:com: specific.

4. Autentificarea şi Verificarea Identităţii: Ambii utilizatori se autentifică reciproc folosind metoda de autentificare descentralizată din prezenta invenţie, implicând cheia de securitate şi modulul de identitate descentralizată MID.

5. Generarea şi Trimiterea Răspunsului SDP: Utilizatorul destinatar generează un răspuns SDP şi îl trimite înapoi iniţiatorului prin blockchain.

6. Colectarea Candidaţilor ICE: Ambii utilizatori colectează candidaţii ICE (Interactive Connectivity Establishment) prin nodurile blockchain, care acţionează ca servere STUN şi TURN.

7. Stabilirea Conexiunii Peer-to-Peer: Utilizatorii stabilesc o conexiune peer-to-peer, traversând NAT şi evitând cenzura, datorită naturii descentralizate a blockchain-ului.

8. Securizarea Comunicaţiei cu Cheia de Securitate: Comunicaţia este securizată folosind criptarea şi cheia de securitate, care oferă un nivel suplimentar de protecţie.

9. Împerecherea şi Comunicarea: Utilizatorii sunt împerecheaţi şi pot comunica prin WebRTC, beneficiind de toate avantajele VOBP, inclusiv lupta împotriva cenzurii şi securitatea îmbunătăţită.

10. Integrarea cu Portofelul şi Modulul de identitate descentralizată MID: Procesul de conexiune WebRTC este integrat cu aplicaţia mobilă de portofel şi cu modulul de identitate descentralizată MID, permiţând gestionarea securizată a identităţilor şi comunicarea criptată.

Sistemul şi metoda de gestionare a identităţilor digitale descentralizate, conform invenţiei, utilizează o aplicaţie mobilă tip portofel electronic care reprezintă punctul de acces al utilizatorilor la reţeaua blockchain şi la sistemul de gestionare a identităţilor.

Aceasta permite utilizatorilor să creeze şi să gestioneze identităţi descentralizate, să comunice în siguranţă prin e-mailuri şi chat-uri criptate, şi să interacţioneze cu blockchain-ul pentru a efectua diverse operaţiuni.

Pentru implementarea aplicației mobile este necesară utilizarea unei componente hardware specifice, o cheie de securitate care implementează un TPM dintr-un chip SoC aprobat de FIPS 140-02. Acest TPM este un microcontroler care stochează chei criptografice specifice unui gazde, asigurând integritatea hardware-ului și software-ului unui sistem și protejând cheile criptografice. Poate genera, stoca și limita utilizarea cheilor criptografice, detectând și protejând împotriva încercărilor de modificare a software-ului sau a hardware-ului.

Aplicația tip portofel trebuie să fie proiectată special pentru protocolul dezvăluit în prezenta invenție pentru a comunica cu cheia de securitate prin Bluetooth. Aceasta permite o integrare fluidă și securizată între componentele software și hardware, oferind o soluție completă pentru gestionarea identității și comunicarea descentralizată.

Standardul FIPS 140-02 (Federal Information Processing Standard) este un standard guvernamental pentru validarea modulelor criptografice și este recunoscut pentru cerințele sale stricte în ceea ce privește securitatea și integritatea datelor. Implementarea unui TPM (modul de platformă de încredere) care este conform cu FIPS 140-02 în cadrul soluției noastre hardware aduce un nivel înalt de securitate și încredere.

Un TPM conform cu FIPS 140-02 este proiectat pentru a oferi o protecție robustă cheilor criptografice. Cheile private nu pot fi extrase din TPM, ci pot fi utilizate doar în interiorul acestuia pentru a semna sau verifica semnături digitale. Aceasta înseamnă că, chiar și în cazul unui atac reușit asupra sistemului, un atacator nu ar putea extrage cheile private pentru a le utiliza în mod fraudulos.

TPM-ul stochează cheile într-o formă criptată și securizată, și le utilizează în operațiuni criptografice fără a le expune în afara chipului. Acest lucru îl face extrem de rezistent la atacuri fizice și software, inclusiv la încercările de a inspecta sau modifica hardware-ul sau software-ul.

De asemenea, TPM-ul poate genera chei criptografice în interiorul chipului, asigurând că acestea nu sunt expuse în niciun moment al procesului de generare.

Acesta poate, de asemenea, să efectueze operațiuni de autentificare, criptare și decriptare, și să gestioneze certificatele și credențialele într-un mod care îndeplinește cerințele stricte de securitate ale standardului FIPS 140-02.

Procesul de funcționare al aplicației mobile, care servește ca punte între portofelul *rece* (*cold wallet*) prin Bluetooth și soluția blockchain, poate fi descris astfel:

1. Iniţierea Conexiunii Bluetooth: Utilizatorul deschide aplicaţia mobilă, care iniţiază o conexiune Bluetooth cu portofelul rece. Această conexiune este securizată printr-un canal criptat proprietar.

2. Autentificarea cu Cheia de Securitate: Utilizatorul se autentifică în aplicaţie folosind cheia de securitate din portofelul rece, care conţine un TPM conform cu FIPS 140-02. Acest proces asigură că doar utilizatorul autorizat poate accesa portofelul.

3. Interacţiunea cu Blockchain-ul: Aplicaţia mobilă permite utilizatorului să interacţioneze cu blockchain-ul, inclusiv să trimită şi să primească tranzacţii, să gestioneze identităţi descentralizate **ID** şi să efectueze alte operaţiuni specifice blockchain-ului.

4. Semnarea Tranzacţiilor cu Portofelul Rece: Pentru orice tranzacţie care necesită semnarea digitală, aplicaţia mobilă trimite datele către portofelul rece prin Bluetooth. Portofelul rece semnează tranzacţia folosind cheia privată stocată în mod sigur şi trimite semnătura înapoi aplicaţiei mobile.

5. Transmiterea Tranzacţiilor Semnate către Blockchain: Aplicaţia mobilă transmite tranzacţia semnată către reţeaua blockchain, unde este verificată şi înregistrată de nodurile reţelei.

6. Gestionarea identităţilor descentralizate: Aplicaţia mobilă permite utilizatorului să gestioneze identităţile descentralizate şi să iniţieze şi să primească comunicaţii WebRTC prin protocolul VOBP, folosind nodurile blockchain ca servere TURN. (doar partea de hand-shaking)

7. Generarea şi Gestionarea Cheilor: Aplicaţia mobilă poate solicita portofelului rece să genereze şi să gestioneze chei, să furnizeze un număr aleatoriu securizat şi să efectueze alte operaţiuni criptografice, toate în conformitate cu standardele relevante.

8. Actualizări şi Sincronizare cu Blockchain-ul: Aplicaţia mobilă se sincronizează regulat cu blockchain-ul pentru a reflecta starea actuală a contului, tranzacţiilor şi identităţilor descentralizate ale utilizatorului.

9. Închiderea Conexiunii Bluetooth: După finalizarea operaţiunilor, conexiunea Bluetooth cu portofelul *rece* este închisă în mod sigur.

REVENDICĂRI

1. Sistem de gestionare a identităţilor digitale descentralizate **caracterizat prin aceea că** funcţionează în baza tehnologiei blockchain şi este alcătuit din următoarele module funcţionale:

- un dispozitiv hardware (**DH**) reprezentat de un dispozitiv fizic de tip token, capabil să genereze şi să stocheze chei publice şi private asociate cu identitatea digitală a cel puţin unui utilizator, dispozitiv hardware (**DH**) care se conectează la terminalul mobil (**TM**) personal al utilizatorului care doreşte să genereze o identitate digitală descentralizată;

- un modul de mapare (**MAP**) care are rolul de a are rolul de a realiza corespondenţa între adresele de e-mail ale utilizatorilor cu identităţile digitale descentralizate / identificatorii descentralizaţi (**DID**);

- un modul de comunicare (**MC**) dedicat gestionării creării, trimiterii şi primirii de e-mailuri şi chat-uri criptate prin intermediul reţelei blockchain şi în baza criptării realizate utilizând cheile publice şi private stocate pe dispozitivul hardware (**DH**) de tip token;

- un modul de conformitate (**MConf**) prevăzut cu eIDAS ce asigură recunoaşterea identităţilor digitale create şi gestionate, conform invetiei, de către serviciile publice din alte state membre ale Uniunii Europene;

- un modul de identitate descentralizată (**MID**) care gestionează crearea, actualizarea şi ştergerea identităţilor descentralizate utilizând tehnologia blockchain prin asocierea unui document tip DID cu o adresă did:com, document ce conţine informaţii legate de identitatea utilizatorului şi utilizat pentru verificarea autenticităţii şi acreditărilor acestuia şi

- un modul de autentificare (**AUT**) ce combină autentificarea în doi paşi şi autentificarea unică ce permite gestionarea securizată a identităţilor descentralizate şi comunicarea criptată.

2. Sistem, conform revendicării independente 1, **caracterizat prin aceea că** dispozitivul hardware (**DH**) permite efectuarea de operaţiuni criptografice fără a dezvălui valoarea cheii de criptare în sine, asigurând astfel un nivel suplimentar de protecţie.

3. Sistem, conform revendicării 1, **caracterizat prin aceea că** identitatea fiecărui utilizator este legată de o pereche de chei criptografice, constând dintr-o cheie privată, păstrată în siguranță în cadrul cheii de securitate certificată FIPS 140-02, folosită pentru semnarea cererilor de tranzacție, și o cheie publică, utilizată de nodurile rețelei blockchain, pentru verificarea semnăturii digitale.

4. Sistem, conform revendicării 1, **caracterizat prin aceea că** adresa portofelului blockchain din cadrul modulului de identitate descentralizată (**MID**) este utilizată ca identificator did:com.

5. Sistem, conform revendicării 1, **caracterizat prin aceea că** un documentul care conține informații legate de o identitate descentralizată (**DID**) este stocat pe blockchain și poate fi accesat și verificat de orice utilizator al rețelei.

6. Sistem, conform revendicării 1, **caracterizat prin aceea că** modulul de autentificare (**AUT**) folosește o cheie de securitate prin WebAuthn și verifică identitatea unui utilizator cu ajutorul documentului ce conține informațiile legate de o identitate descentralizată (**ID**) stocat pe blockchain.

7. Sistem, conform revendicării 1, **caracterizat prin aceea că** stocarea cheilor de securitate se face într-un mediu fizic, izolat de Internet și de alte rețele potențial compromise iar operațiunile criptografice realizate nu dezvăluie valoarea cheii în sine.

8. Sistem, conform revendicării 2, **caracterizat prin aceea că** dispozitivul hardware (**DH**) este compatibil cu o varietate de dispozitive și platforme și, prin intermediul unei conexiuni de tip Bluetooth criptate, poate comunica cu telefoane mobile, tablete, calculatoare și alte dispozitive compatibile.

9. Metodă de gestionare a identităților digitale descentralizate **caracterizată prin aceea că** implică realizarea următorilor pași operaționali:

   - se realizează înrolarea utilizatorului și generarea de identități descentralizate prin utilizarea dispozitivului hardware (**DH**) și instalarea unei aplicații mobile tip portofel

electronic care reprezintă punctul de acces la utilizatorilor la o rețea de tip blockchain și la sistemul de gestionare a identităților;

- se realizează autentificarea și autorizarea utilizatorului, utilizând cheia publică stocată în registrul blockchain și asociată identității descentralizate create la pasul anterior pentru verificarea semnăturii digitale;

- se realizează interacțiunea cu rețeaua blockchain prin intermediul aplicației mobile ce permite utilizatorului să trimită și să primească tranzacții, să gestioneze identități descentralizate (**ID**) și să efectueze alte operațiuni specifice blockchain-ului;

- se realizează tranzacționări virtuale ale utilizatorilor autentificați la pasul anterior, inclusiv utilizarea de servicii de e-mail și/sau de chat, transfer de documente, tranzacționare de monede virtuale, toate fiind realizate cu asigurarea integrității și a confidențialității acestora;

- se realizează semnarea tranzacțiilor prin utilizarea aplicației mobile care trimite datele către portofelul rece, fie prin conexiune fizică fie prin conexiune wireless tip Bluetooth; portofelul rece semnează tranzacția folosind cheia privată stocată în mod sigur și trimite semnătura înapoi aplicației mobile;

- se transmit tranzacțiile semnate către rețeaua blockchain unde fiecare tranzacție este verificată și înregistrată în nodurile rețelei;

- se realizează sincronizarea periodică a aplicației mobile cu rețeaua blockchain pentru a reflecta starea actuală a contului, tranzacțiilor și identităților descentralizate ale utilizatorilor;

- se realizează închiderea în siguranță a conexiunii cu portofelul *rece*, după finalizarea tranzacțiilor.

10. Metodă, conform revendicării 9, **caracterizată prin aceea că** utilizatorii sistemului pot asigna una sau mai multe adrese de e-mail pentru identitatea descentralizată proprie și pot căuta identități descentralizate ale altor utilizatori prin introducerea a cel puțin unei adrese de e-mail utilizând modulul de mapare (**MAP**).

11. Metodă, conform revendicării 9, **caracterizată prin aceea că** aplicația mobilă poate permite utilizatorilor să gestioneze identitățile descentralizate (**ID**) și să inițieze și să

67

primească comunicații de tip WebRTC prin protocolul VOBP, folosind nodurile rețelei blockchain ca servere TURN.

12. Metodă, conform revendicării 9, **caracterizată prin aceea că** aplicația mobilă poate solicita portofelului *rece* să genereze și să gestioneze chei, să furnizeze un număr aleatoriu securizat și să efectueze alte operațiuni criptografice, toate în conformitate cu standardele relevante.

13. Metodă, conform revendicării 9, **caracterizată prin aceea că** generarea unei identități descentralizate (**ID**) implică următoarele etape:

- se generează un mnemonic conform algoritmului standardizat BIP-39 folosind capabilitățile cheii de securitate pentru a genera numere aleatorii;
- mnemonicul este transformat într-o sămânță criptografică folosind o funcție de hash și, eventual, o parolă suplimentară;
- sămânța este folosită pentru a deriva o cheie principală (master key) folosind algoritmul BIP-32; cheia principală va fi rădăcina ierarhiei de chei pentru portofelul de identități descentralizate;
- utilizând cheia principală și structura specifică blockchain-ului Cosmos SDK, se generează o adresă DID unică;
- se creează un document DID care conține informații legate de identitatea utilizatorului, inclusiv cheile publice, serviciile asociate și alte metadate;
- documentul DID este semnat digital cu cheia privată asociată și trimis către blockchain; blockchain-ul va funcționa ca un registru pentru toate documentele DID;
- nodurile blockchain verifică semnătura și integritatea documentului DID și în înregistrează în blockchain pentru a se asigura imutabilitatea și transparența identităților descentralizate;
- utilizatorul poate gestiona și actualiza documentul DID prin intermediul portofelului care gestionează identitățile descentralizate, folosind cheia de securitate și protocolul propus pentru autentificare și operațiuni criptografice.

14. Metodă, conform revendicării 9, **caracterizată prin aceea că**, realizează integrarea tehnologiei WebRTC cu cea a tehnologiei blockchain prin intermediul a două componente

esențiale: semnalizarea, pentru a stabili conexiunile între perechi în WebRTC şi colectarea candidaților ICE, pentru a îmbunătăți traversarea NAT şi a face rețeaua mai rezistentă la blocări şi cenzură.

15. Metodă, conform revendicării 9, **caracterizată prin aceea că**, pentru implementarea aplicației mobile tip portofel, este necesară utilizarea unei componente hardware specifice, o cheie de securitate care implementează un TPM dintr-un chip SoC aprobat de FIPS 140-02.

16. Metodă, conform revendicării 12, **caracterizată prin aceea că**, integrarea tehnologiei WebRTC se face urmând următorii paşi operaționali:

- un utilizator inițiază o cerere de comunicare, de exemplu, un apel video, către un alt utilizator prin intermediul aplicației care implementează protocolul VOBP;

- fiecare nod blockchain acționează ca un server TURN, înlocuind serverele TURN tradiționale;

- utilizatorul inițiator generează o ofertă SDP şi o trimite destinatarului prin intermediul blockchain-ului, folosind identificatorul did:com: specific;

- ambii utilizatori se autentifică reciproc folosind metoda de autentificare descentralizată, implicând cheia de securitate şi modulul de identitate descentralizată (**MID**);

- utilizatorul destinatar generează un răspuns SDP şi îl trimite înapoi inițiatorului prin blockchain;

- ambii utilizatori colectează candidații ICE prin nodurile blockchain, care acționează ca servere STUN şi TURN.

- utilizatorii stabilesc o conexiune peer-to-peer, traversând NAT şi evitând cenzura, datorită naturii descentralizate a blockchain-ului;

- comunicația este securizată folosind criptarea şi cheia de securitate, care oferă un nivel suplimentar de protecție;

- utilizatorii sunt împerecheați şi pot comunica prin WebRTC, beneficiind de toate avantajele VOBP, inclusiv lupta împotriva cenzurii şi securitatea îmbunătățită.

65

- procesul de conexiune WebRTC este integrat cu aplicația mobilă de portofel și cu modulul de identitate descentralizată (**MID**), permițând gestionarea securizată a identităților și comunicarea criptată.

64

FIGURI

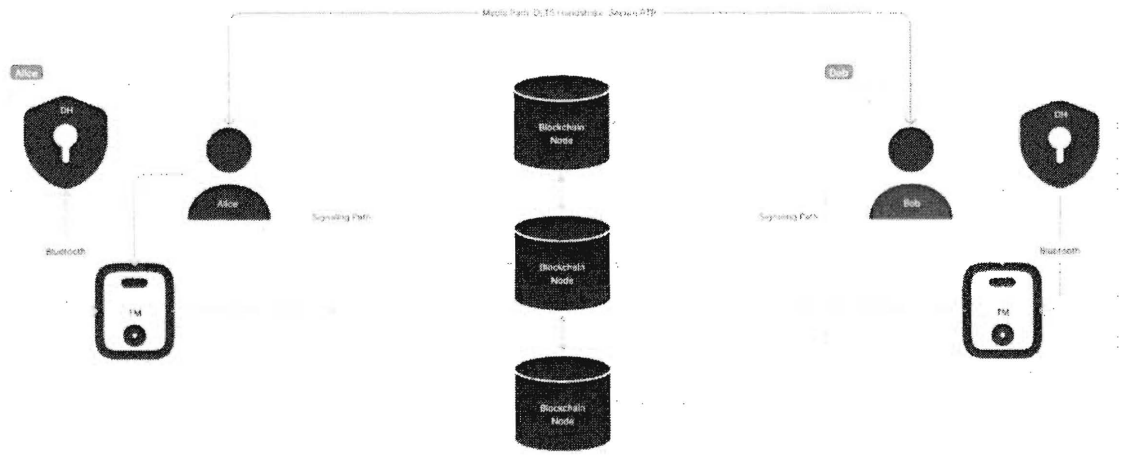

Figura 1

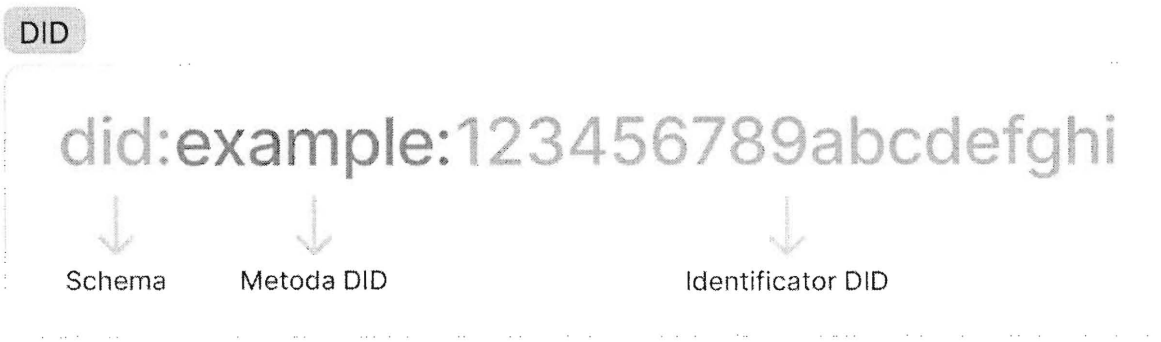

Figura 2

63

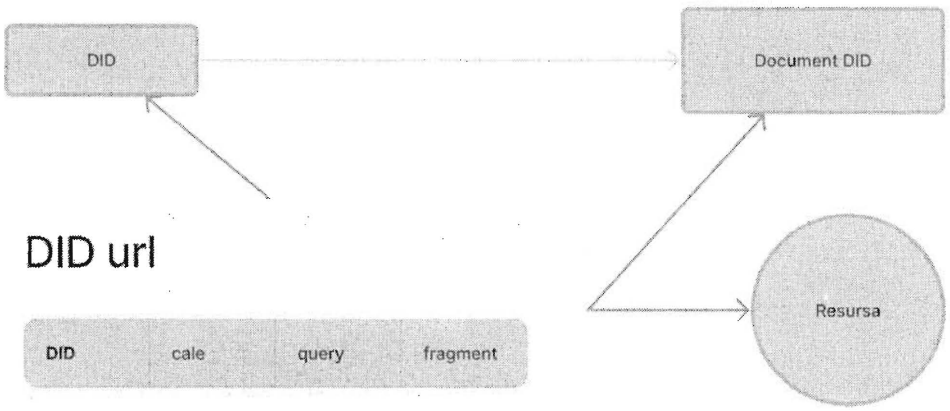

Figura 3

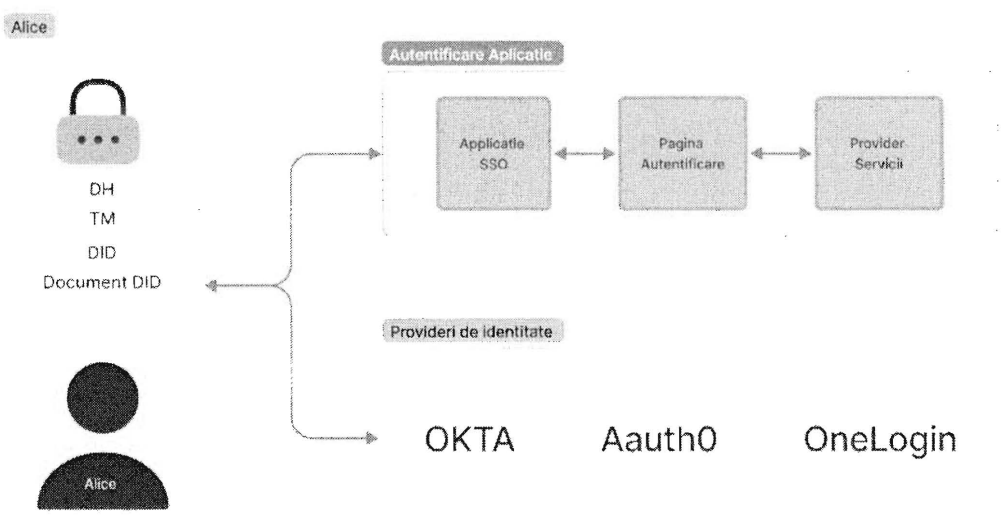

Figura 4

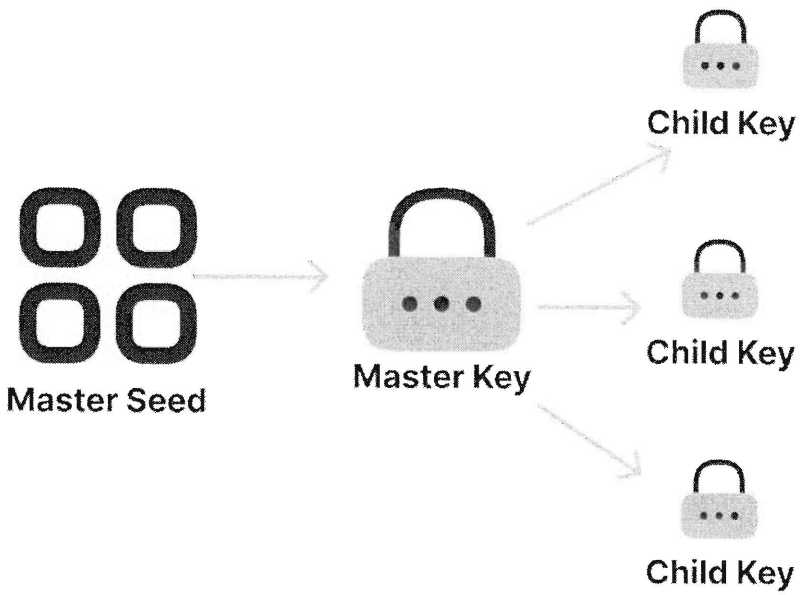

Figura 5