(19) OFICIUL DE STAT
PENTRU INVENŢII ŞI MĂRCI
Bucureşti

ROMÂNIA

(11) **RO 135681 A0**
(51) **Int.Cl.**
G16H 10/60 (2018.01).
G16H 15/00 (2018.01).
G06F 16/23 (2019.01).
G06F 21/64 (2013.01)

(12) # CERERE DE BREVET DE INVENŢIE

(21) Nr. cerere: **a 2021 00541**

(22) Data de depozit: **13/09/2021**

(41) Data publicării cererii:
29/04/2022 BOPI nr. **4/2022**

(71) Solicitant:
• **UNIVERSITATEA DE ŞTIINŢE AGRICOLE ŞI MEDICINĂ VETERINARĂ A BANATULUI "REGELE MIHAI I AL ROMÂNIEI" - DIN TIMIŞOARA**, *CALEA ARADULUI NR. 119, TIMIŞOARA, TM, RO;*
• **UNIVERSITATEA DE VEST DIN TIMIŞOARA**, *BD.VASILE PÂRVAN NR.4, TIMIŞOARA, TM, RO*

(72) Inventatori:
• **SPĂTARU ALEXE LUCA**, *STR. MIRCEA-DIMITRIE RAŢIU, NR.3, ET.2, AP.7, TIMIŞOARA, TM, RO;*
• **PUNGILĂ CIPRIAN-PETRIŞOR**, *BD.DÎMBOVIŢA, NR.8, ET.3, AP.8, TIMIŞOARA, TM, RO;*
• **GALIŞ DARIUS**, *STR.MĂRĂŞEŞTI, NR.49, CURTICI, AR, RO;*
• **ZAHARIE DANIELA**, *STR.NICOLAE TABLE, NR.2, BL.B, SC.2, AP.8, TIMIŞOARA, TM, RO;*
• **MIRCU CĂLIN**, *STR.PRAGA, NR.37, DUMBRĂVIŢA, TM, RO;*
• **HUŢU IOAN**, *STR.GH.LAZĂR, NR.34, ET.VIII, AP.69, TIMIŞOARA, TM, RO*

(74) Mandatar:
CABINET DE PROPRIETATE INDUSTRIALĂ TUDOR ICLĂNZAN, *PIAŢA VICTORIEI NR.5, SC.D, AP.2, TIMIŞOARA, TM*

(54) # METODĂ ŞI SISTEM BAZATE PE TEHNOLOGIA BLOCKCHAIN PENTRU RAPORTAREA REZISTENŢEI LA PREPARATELE ANTIMICROBIENE

(57) **Rezumat:**

Invenţia se referă la o metodă şi la un sistem de raportare a rezistenţei la preparatele antimicrobiene, bazate pe tehnologia blockchain. Metoda cuprinde o primă etapă de iniţializare (**302**), în care un nod al sistemului de raportare porneşte un subsistem de procesare şi îl configurează şi, de asemenea, porneşte un subsistem blockchain local de tip privat sau se conectează la un subsistem blockchain extern de tip public, urmată de etapele de aşteptare (**303**), în care se aşteaptă apariţia unui mesaj de la utilizator sau apariţia unei tranzacţii într-un jurnal blockchain al subsistemului blockchain extern public, de recepţie (**304**) a unei cereri de operaţie în care subsistemul de procesare recepţionează un mesaj, de decriptare (**305**), în care sunt decriptate părţile criptate ale mesajului recepţionat şi o etapă de validare (**306**) a operaţiei în care sunt verificate identificatorul şi versiunea operaţiei, precum şi structura corpului mesajului, iar dacă sunt valide se trece la etapa de discriminare (**307**) care diferenţiază tratarea operaţiilor după tipul lor, care poate fi de interogare, care nu schimbă starea sistemului, sau acţiuni care schimbă starea sistemului şi, dacă operaţia este de interogare, este urmată de un pas de interogare (**308**) în care una sau mai multe operaţii salvate ca tranzacţii sunt citite şi agregate conform cererii, iar dacă operaţia este o acţiune, este urmată de paşii de creare/restaurare (**310**) a contextului, executare a operaţiei (**311**) şi înregistrare a tranzacţiei (**312**), şi, indiferent de tipul operaţiei, pasul de integrogare sau pasul de înregistrare se continuă cu un răspuns (**309**) în care rezultatul operaţiei este calculat, în pasul de execuţie (**311**), sau răspunsul interogaţiei este transmis înapoi la utilizator. Sistemul este format dintr-un număr de noduri (**101**) independente care permit unor utilizatori (**110**) conectaţi printr-o reţea (**104**) de acces să comunice mesaje (**105**) către un nod din sistem care efectuează metoda conform invenţiei.

Revendicări: 18
Figuri: 9

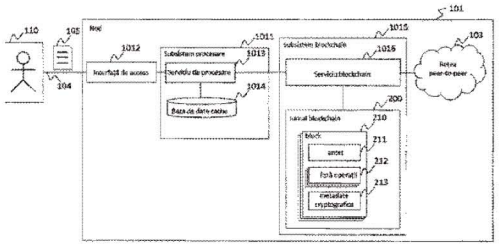

Fig. 2

RO 135681 A0

107

METODĂ ŞI SISTEM BAZATE PE TEHNOLOGIA BLOCKCHAIN PENTRU RAPORTAREA REZISTENŢEI LA PREPARATELE ANTIMICROBIENE

Domeniul invenţiei este cel al farmaco-vigilenţei şi anume al monitorizării şi raportării rezistenţei la un preparat antimicrobian.

Rezistenţa la preparate antimicrobiene (AMR) este un fenomen întâlnit atunci când un medicament nu mai prezintă eficienţă în tratarea unui anumit microorganism (bacterii, viruşi, paraziţi etc.), fenomen ce se formează în timp prin schimbări genetice datorită suprautilizării, utilizării inadecvate sau utilizării incorecte ale unui antibiotic. Începând cu 2020, AMR a ajuns să fie considerată una dintre cele mai semnificative zece pericole cu care omenirea se confruntă la nivel global, conform Organizaţiei Mondiale a Sănătăţii [1], ajungând să fie un factor de impact major asupra economiei şi sănătăţii publice. AMR se răspândeşte la nivel genetic prin mutaţia, respectiv replicarea genei ce conţine codificarea rezistenţei la un anumit antibiotic/antiviral sau până şi prin însăşi răspândirea bacteriei ce are deja dezvoltată gena în cauză. Amplificarea fenomenului de răspândire a genelor rezistente ridică problematici importante exprimate prin creşterea ineficienţei medicamentelor, prin nevoia de dezvoltare continuă a altor tipuri de medicamente capabile de a combate mitridatizarea microorganismelor, prin creşterea costurilor asociate cercetării şi nu în ultimul rând prin răspândirea tot mai acerbă a efectelor nefaste produse atât de bacterii, cât şi de efectele secundare provocate de remediile utilizate. Prin prisma motivelor enumerate mai sus, se consideră imperativă necesitatea existenţei unor metode de detectare şi raportare rapidă a fenomenului AMR. Fenomenul este detectabil prin maniere cunoscute cum ar fi analiza genetică a

microorganismelor într-un laborator sau prin urmărirea efectelor adverse produse de un anumit antibiotic.

Din punct de vedere legal, conform Legii nr. 95/2006, publicată în Monitorul Oficial al României, Agenția Națională a Medicamentului și a Dispozitivelor Medicale (ANMDM) are responsabilitatea de a autoriza sau retrage de pe piață anumite tipuri de medicamente (art. 704) și de a menține un sistem de farmacovigilență ce presupune colectarea informațiilor asupra riscurilor de utilizare a anumitor medicamente (art. 827). De asemenea, conform aceleiași legi, ANMDM adoptă măsuri pentru a motiva pacienții și/sau profesioniștii în domeniu să raporteze efectele adverse cu date exacte şi verificabile pentru efectuarea unei evaluări științifice a eficienței respectivului medicament (art. 828). Pe lângă acestea, ANMDM este obligată prin lege să distribuie la timp informații referitoare la aspectele de farmacovigilență, în ceea ce privește utilizarea unui medicament (art. 828).

ANMDM furnizează un portal web ce conține informații relevante farmacovigilenței, precum ar fi rapoarte de evaluare, rezumate ale caracteristicilor produselor sau planul de management al riscului pentru un medicament autorizat (art. 833). Acest portal permite pacienților și medicilor sa raporteze și să obțină informații precum rezistența antimicrobiană la un anumit medicament.

Dacă în baza notificărilor și rapoartelor obținute, medicamentul s-a dovedit a fi nociv, lipsit de eficacitate terapeutică sau cu o rată de risc-beneficiu nefavorabilă, ANMDM poate implementa diferite grade de intervenție asupra autorizației medicamentului. De asemenea, deținătorul autorizației este responsabil să mențină un sistem de farmacovigilență intern (art. 830), asemănător celui ANMDM, prin care se efectuează o evaluare științifică a informațiilor colectate și ia măsuri pentru a minimiza riscul unei reacții adverse

în utilizarea unui medicament. Fiecare deținător al autorizației este responsabil să fie în permanență în contact cu o persoană fizică/juridică ce prezintă calificarea necesară pentru a putea fi responsabilă de farmacovigilență, capabilă de a opera un sistem de management al riscului pentru fiecare medicament și care să poată sa transmită datele obținute la ANMDM sub formă de rapoarte. De asemenea, deținătorul autorizației trebuie să transmită rapoarte periodice la Agenția Europeană a Medicamentelor (EMA) cu date actualizate ce țin de rezultatele tuturor studiilor efectuate pentru identificarea riscurilor și beneficiilor, o evaluare științifică a raportului de risc-beneficiu și toate datele ce cuprind volumul vânzărilor medicamentului.

Așa cum este cunoscut din stadiul actual al tehnicii, tehnologia blockchain a apărut în 2009 și a fost popularizată odată cu extinderea conceptului Bitcoin care până în prezent, a influențat modul prin care economia modernă poate fi schimbată. Conceptual, "blockchain" este un registru de tranzacții distribuit într-o rețea, care nu poate fi modificat odată ce e validat și stabilit de un anumit număr, considerat relevant, de participanți din rețea. Autenticitatea tranzacțiilor este, în general, garantată de o semnătură digitală a expeditorului, de obicei creată prin utilizarea unei perechi de chei criptografice ce asigură securitatea informațiilor transmise. Pe lângă aspectele enumerate, ce ar putea fi implementate într-o anumită măsură și în bazele de date tradiționale, tehnologia blockchain aduce multiple avantaje: transparența parțială sau integrală a datelor, imutabilitatea informațiilor, descentralizarea (acolo unde se dorește acest lucru), eliminarea intermediarilor din efectuarea tranzacțiilor.

Tot din stadiul actual al tehnicii este cunoscut faptul că tehnologia blockchain mai permite și implementarea unor așa zise contracte inteligente care sunt verificabile formal și care nu sunt altceva decât programe sau proceduri automate de procesare a datelor (i.e. automate cu stări finite) ce sunt stocate ca înregistrări în blockchain și care sunt executate conform unui protocol de către

un utilizator sau automat de către un nod autorizat atunci când anumite condiții logice dinamice legate de datele prezente în tranzacțiile înregistrate în blockchain sunt valide. Ca urmare a execuției unui contract inteligent sunt produse noi operații în jurnalul blockchain ce pot fi validate pentru verificarea autenticității de către orice parte terță. Astfel, tranzacțiile din registru reprezintă o schimbare de stare a contractului și vor fi semnate de inițiatorul tranzacției. De asemenea, la nivel de contract se pot implementa permisiuni pentru a permite doar unor agenți, deținători ai cheii, să efectueze anumite tranzacții. Astfel, avantajele tehnologiei se pot aplica acum la mai multe situații și domenii de specialitate, unul din ele fiind în sistemele de sănătate. Printre soluțiile propuse pentru tratarea cazurilor de rezistență antimicrobiană, regăsim și utilizarea tehnologiei blockchain în acest domeniu, tehnologie a cărei integrare este tot mai proeminentă în sistemele moderne de sănătate datorită proprietăților esențiale de transparență, accesibilitate și integritate a datelor.

Aplicabilitatea tehnologiei blockchain în domeniul medical poate fi remarcată prin următoarele invenții:

Se cunoaște invenția AU2021100430A4 care asigură stocarea și distribuirea sigură a datelor pacienților. Invenția este o platforma interoperabilă care permite schimbul de date privind asistența medicală și care leagă o multitudine de aplicații disparate, la distanță, reprezentând în general sisteme de furnizori care conțin fișe medicale electronice (EHR) pentru a permite colectarea, procesarea și stocarea centralizată a fișelor medicale în timp real într-un magazin de date, împreună cu accesul controlat și stocarea centralizată. Baza centrală de date cu evidențele medicale primește, în timp real, date de intrare electronice completate de furnizori multipli din diferite surse de evidență medicală. Platforma permite normalizarea semantică a informațiilor prin convertirea datelor din evidențele medicale în formate de mesaje standardizate utilizând un

motor de conversie a datelor şi maparea datelor convertite în terminologii standard utilizând produse de cartografiere.

Este cunoscută invenţia US20170039330A1 care descrie crearea unei platforme descentralizate şi autonome pentru economia din domeniu medical. Sunt furnizate un sistem şi o metodă pentru o platformă autonomă descentralizată. Sistemul şi metoda agregă toate datele privind asistenţa medicală într-o topologie globală teoretică a graficelor şi procesează datele de o manieră hibridă federativă după arhitecturi de procesare distribuite de tipul peer-to-peer.

De asemenea, se cunoaşte invenţia US10340038B2 care presupune încorporarea în blockchain a tranzacţiilor dintr-un sistem medical. Sunt prezentate sistemele şi metodele de validare a tranzacţiilor medicale. Tranzacţiile privind asistenţa medicală unei părţi interesate sunt procesate într-un lanţ de blocuri de tranzacţii de asistenţă medicală. Lanţul poate fi considerat o cronică a istoricului medical al pacientului. Când se efectuează o tranzacţie, parametrii medicali corespunzători (de exemplu, internări, externări, dovezi clinice, rezultate etc.) sunt trimise către unul sau mai multe dispozitive de validare. Dispozitivele stabilesc valabilitatea tranzacţiei şi generează un bloc nou prin intermediul unui principiu al dovezii de lucru. Odată ce noul bloc a fost calculat, acesta poate fi ataşat la blockchain-ul de îngrijire a sănătăţii părţii interesate.

Tot din stadiul actual al tehnicii, sunt cunoscute metodele de utilizare a tehnologiei blockchain pentru trasabilitatea şi managementul stocării, transportului şi distribuţiei de medicamente şi vaccinuri şi pentru eliminarea riscurilor de contrafacere a acestora.

În ceea ce priveşte rezistenţa la preparatele antimicrobiene, aşa cum este cunoscut din stadiul actual al tehnicii, ANMDM oferă un sistem electronic de raportare centralizat expus printr-un portal Web pentru raportare şi

monitorizare. Sunt cunoscute mai multe inconveniente ale acestui sistem printre care:

- *Toleranță scăzută* la defecte datorită arhitecturii centralizate și a lipsei redundanței și a paralelismului, un simplu defect sau atac cibernetic efectuat cu succes poate să blocheze nu doar publicarea de noi raportări de farmacovigilență din partea pacienților și personalului medical autorizat, dar și restricționează accesul la rapoartele deja existente.
- *Scalabilitate redusă*. Trasabilitatea și monitorizarea manipulării medicamentelor poate presupune un număr mare de raportări ce ar fi greu de procesat și stocat de către un astfel de sistem centralizat.
- *Lipsa transparenței deciziilor* și a istoricului notificărilor și raportărilor. Raportările și notificările pacienților și medicilor nu sunt făcute publice cu precădere datorită confidențialității și a legislației GDPR care nu permite acest lucru. Aceste raportări sunt vizibile doar pentru ANMDM care întocmește și publică eventual decizii și rapoarte sintetice pe baza acestora. Pacienții și medicii nu văd mesajele și raportările din sistem și în consecință anumite detalii precum și studii ulterioare de corelare a datelor de către laboratoare și organisme externe nu sunt posibile. Din păcate, autoritatea ANMDM fiind singura ce poate accesa și procesa notificările și raportările poate întocmi sau nu rapoarte. Acest fapt este lipsit de transparență deoarece permite pe de o parte corupția și trucarea adevărului din teren și, pe de o altă parte face imposibilă elaborarea oricărui studiu ulterior care ar putea beneficia de agregarea și consolidarea datelor istorice.
- *Securitate scăzută*. Datele fiind centralizate și aflate sub umbrela unei autorități unice centrale ele pot fii compromise.
- *Lipsa garanției autenticității rapoartelor*. Rapoartele ANMDM publice nu pot fi verificate atâta timp cât nu se poate verifica legătura dintre

rapoartele ANMDM şi sursele utilizate la întocmirea lor care, deşi pot fi semnate electronic şi deci avea o garanţie de autenticitate asupra originii lor, nu sunt publicate şi relaţionate cu rapoartele. Nu există garanţii procedurale formale asupra autenticităţii surselor utilizate pentru generarea de raportări şi decizii. Este deci imposibilă verificarea în timp real şi formal a autenticităţii şi a respectării procedurilor şi a legislaţiei.

- *Lipsa raportării în timp real*. Întrucât datele comunicate către ANMDM nu sunt publice este imposibil de verificat de către o parte terţă dacă constrângerile de timp sau dacă procedurile de procesare sunt respectate cu strictețe. Există un conflict de rol, ANMDM nu se poate verifica pe ea însăşi, ea are obligaţia principală de a elabora rapoarte şi reguli aplicative de farmacovigilenţă în conformitate cu legislaţia şi de a monitoriza si sancţiona pe cei care nu le respectă. Însăşi faptul că datele sunt stocate şi accesibile doar de către ANMDM face imposibilă monitorizarea şi controlul în timp real iar pacienţii si medicii nu au garanţii asupra timpului de procesare şi nici a rezultatului procesării conform procedurilor fixate prin legislaţie. Spre exemplu, să presupunem că este raportat decesul mai multor persoane datorită unui medicament X administrat într-un context de utilizare farmaco-complex nou şi necunoscut în prealabil sau în contextul unui lot de medicamente contaminat cu substanţe toxice letale. În acest caz, întrucât medicii deşi raportează notificările de farmacovigilenţă acestea sunt necunoscute altor medici până la procesarea lor de către ANMDM iar această lentoare poate costa vieţi. Mai mult, ANMDM poate reacţiona întârziat aşteptând studii alternative, timp în care alţi bolnavi pot deceda sau rămâne cu sechele datorate tratamentelor necorespunzătoare.
- *Imposibilitatea implementării de contracte inteligente şi de proceduri automate de control*. Deşi ANMDM elaborează rapoarte decizionale, implementarea acestora nu este nici imediată şi nici obligatorie în sensul

că între momentul publicării deciziei și aplicarea efectivă pot apărea întârzieri deoarece nu există nici un mecanism care să poată bloca spre exemplu comercializarea chiar și temporară a unor medicamente sau a unor loturi precise. Spre exemplu, deși informațiile prezente în codul de bare al unei rețete electronice conțin datele de identificare a medicamentelor și ale pacienților, nu există nici un mecanism de control automat care să invalideze vânzarea unui lot proaspăt retras. Spre un alt exemplu, pot apărea conflicte atunci când deținătorul autorizației acționează în interes economic personal pentru a continua vânzarea produsului autorizat. Chiar dacă există metode de penalizare în aceste situații, fiind imprevizibile, până în momentul când s-au implementat grade de intervenție, sănătatea publică poate suferi. De asemenea și spre exemplu, la primirea rapoartelor, ANMDM trebuie să se consulte cu EMA pentru a identifica rapoartele duplicate (art. 835), lucru ce ar impune timp în plus de procesare, ce poate fi economisit dacă există un mecanism inerent de detectare a rapoartelor duplicat.

Observăm că datorită mecanismelor încorporate, a gradului de securitate și ale avantajelor tehnologice aduse, exemplele prezentate relevă faptul că tehnologia blockchain are potențial major cu un impact considerabil în domeniul medical și farmaceutic. Cu toate acestea, raportându-ne la contextul actual, nu se poate discuta despre existența unui brevet sau studiu care ar considera problematica rezistenței la preparate antimicrobiene (AMR) în contextul tehnologiei blockchain, ce să fie conceput special pentru a rezolva problema detectării rezistenței, astfel încât să poată evita răspândirea acesteia și care să implementeze metode bine-definite de protejare a sănătății publice și de minimalizare a pierderilor economice în cazul manifestării fenomenului AMR.

Problema tehnică ce se dorește a fi soluționată este găsirea unei sistem și a unei metode adecvate pentru raportarea fenomenului de rezistență la

preparatele antimicrobiene care să fie sigure, verificabile formal și în timp real și care garantează autenticitatea și integritatea raportărilor și a deciziilor publicate prin rapoarte într-un mod transparent și direct în conformitate cu cerințele de confidențialitate și conform legislației GDPR.

Mai sunt căutate și alte detalii și avantaje de implementare care vor deveni evidente pentru o persoană antrenată în domeniul farmacovigilenței și al tehnologiei blockchain.

Metoda şi sistemul conform invenţiei înlătură dezavantajele de mai sus prin aceea că utilizează un sistem și o metodă de raportare al rezistenței la preparatele antimicrobiene de către un utilizator către un sistem de raportare distribuit prin intermediul unor mesaje de raportare ce conţin un antet, un corp, şi preferabil o semnătură criptografică şi care este executată de oricare din nodurile sistemului de raportare, metoda cuprinzând etapele de inițializare în care nodul pornește un subsistem de procesare și îl configurează și în care pornește un subsistem blockchain local de tip privat sau se conectează la un subsistem blockchain extern de tip public și, o etapă de așteptare în care așteaptă apariția unui mesaj de la un utilizator printr-o interfață conectată la o rețea de acces sau, așteaptă apariția unei tranzacții într-un jurnal blockchain al unui subsistem blockchain extern public, tranzacția fiind un mesaj primit de către subsistemul blockchain de la un utilizator extern prin intermediul unei rețele și al unei interfețe de acces și o etapă de recepție a unei cereri de operație în care, ca urmare a apariției unui mesaj atunci când subsistemul blockchain este privat sau,ca urmare a apariției unei tranzacții cuprinzând un mesaj atunci când subsistemul blockchain este extern şi public şi în care subsistemul de procesare recepționează mesajul și o etapă de decriptare în care, părțile criptate cu cheia publică a ANMDM ale mesajului recepționat sunt decriptate și, o etapă de validare operație în care sunt verificate identificatorul și versiunea operației care trebuie să fie valide și, în care sunt verificate structura corpului mesajului

care trebuie să conțină toate câmpurile conform unei definiții a formatului mesajului cunoscută intern de către subsistemul de procesare și, în care sunt verificate valorile câmpurilor mesajului folosind o listă de predicate de verificare care garantează că mesajul este bine definit și, în care sunt verificate semnăturile mesajului care trebuie să fie autentice, iar suma de control să indice integritatea mesajului și, în care sunt verificate tipul operației care, pentru nodurile configurate ca noduri de stocare, este restricționată la operații de tip interogare și, daca sunt invalide atunci ignoră mesajul și revine în pasul de așteptare sau dacă sunt valide atunci trece la etapa următoare de discriminare care diferențiază tratarea operațiilor după tipul lor și care pot fii operații de interogare care nu schimbă starea sistemului sau operații care sunt acțiuni și au un contract de execuție ce schimbă starea sistemului și,dacă operația este o interogare, este urmată de un pas de interogare în care una sau mai multe operații salvate ca tranzacții în jurnalul blockchain sau dintr-o bază de date cache local sunt citite și agregate conform cererii de operație iar,dacă operația este o acțiune care presupune schimbări ale stării sistemului, este urmată de pașii de Creare/Restaurare context în care dacă operația este prima dintr-un contract identificat printr-un număr de secvență unic atunci creează un context de execuție format dintr-un tabel asociativ de chei și valori asociate și care inițial este gol sau,dacă operația este o operație următoare dintr-un contract identificat prin numărul de secvență unic atunci citește lista de operații de reîmprospătare a contextului de execuție din jurnalul blockchain sau dintr-o bază de date cache locală, operații care sunt asociate contractului în desfășurare și care au fost salvate în prealabil când au fost executate operațiile precedente din contract și care au același număr de secvență și care prin execuția lor restaurează contextul de execuție pentru a fi identic cu cel precedent permițând executarea contractului din punctul rămas și pasul de execuție operație în care o funcție ce are identificatorul identic cu identificatorul operației și aceeași versiune este invocată de subsistemul de procesare folosind parametrii din

102

corpul mesajului şi contextul de execuţie din pasul de creare/restaurare context şi care produce un răspuns şi o listă de operaţii de împrospătare care, dacă sunt prezente, modifică starea contractului aflat în desfăşurare şi care trebuie scrise în jurnalul blockchain şi pasul de înregistrare tranzacţie care, în cazul în care starea contractului s-a schimbat prin execuţia operaţiei şi contractul mai presupune şi alte operaţii viitoare nefiind finalizat, salvează lista de operaţii de împrospătare în jurnalul blockchain şi,pentru orice tip de operaţie pasul de interogare sau pasul de înregistrare continuă cu un pas de răspuns operaţie în care rezultatul operaţiei calculat în pasul de execuţie sau răspunsul interogaţiei este transmis înapoi utilizatorului.

Conform unui aspect al acestei invenţii, subsistemul blockchain deşi necesar este unul existent diferenţa fiind dată doar de conţinutul tranzacţiilor care sunt cereri şi operaţii de farmacovigilenţă înregistrate în jurnalul blockchain.

Conform unui aspect al acestei invenţii, sistemul este scalabil şi are o toleranţă crescută la defecte el putând fi crescut prin adăugare de noi instanţe de noduri.

Conform unui aspect al acestei invenţii, metoda şi sistemul asigură transparenţa operaţiilor de raportare a deciziilor întregul istoric de acţiuni fiind salvat şi disponibil în jurnalul blockchain.

Conform unui aspect al acestei invenţii, metoda şi sistemul permit raportarea în timp real fără cenzură, ANMDM putând doar să acrediteze sau nu validitatea raportărilor fără a le putea bloca pentru alte cazuri decât cele în care cererile de operaţii nu sunt invalide din punct de vedere formal. Orice utilizator emiţând o cerere de operaţie validă va vedea în timp real că raportarea sa este introdusă automat în jurnalul blockchain.

Conform unui aspect al acestei invenţii, securitatea datelor şi a sistemului sunt crescute datorită tehnologiei blockchain. Toate operaţiile fiind imutabile, şi

autentificate prin semnături criptografice ce pot fi verificate de către orice utilizator fiind quasi-imposibilă falsificarea datelor.

Conform unui aspect major al acestei invenții, este posibilă implementarea cerințelor GDPR pentru asigurarea confidențialității datelor singurul aspect imposibil de implementat fiind ștergerea efectivă a datelor care, datorită arhitecturii blockchain este imposibilă. Totuși, este posibil controlul acreditărilor și a valabilității cheilor criptografice permițând spre exemplu repudierea dreptului de acces la date care este tot o formă limitată de implementare a cerinței de ștergere. Pentru a implementa ștergerea efectivă este necesar ca ANMDM să genereze periodic un nou jurnal în care să fie copiate doar acele operații care sunt încă permise spre citire. Totuși acest mecanism este contrar ideii de blockchain și este descurajat deși este posibil.

Conform unui aspect major al acestei invenții, pot fi implementate contracte inteligente oricât de complexe atâta timp cât ele pot fi descrise sub forma unor automate cu stări finite FSM reactive în care o cerere de operație reprezintă un eveniment declasator al unei tranziții, iar tranziția este implementată printr-o funcție atașată tipului de operație ce consumă parametrii transmiși în cererea de operație și care mai face referință la contextul contractului care este scris în jurnalul blockchain. Pentru claritate, ca urmare a execuției unei operații dintr-un contract, starea acesteia este scrisă sub forma unor operații în jurnalul blockchain urmând ca, atunci când apare o nouă cerere, starea de execuție să fie refăcută din jurnalul blockchain, execuția contractului putând continua cu un pas și tot așa mai departe până la terminarea lui. Spre exemplu, un contract inteligent poate implementa eliminarea operațiilor duble. Spre un alt exemplu, un contract inteligent poate asigura că părțile protejate ale unei raportări printr-o operație nu sunt disponibile publicului, dar pot fi obținute de o parte terță ca urmare a unei runde de schimburi de mesaje în care datele sunt criptate și dezvăluite progresiv.

Conform unui aspect al acestei invenţii, baza de date asociativă utilizată de un nod al sistemului are un rol de cache pentru optimizarea performanţei fiind evitate parcurgerea repetată şi decriptările inutile ale operaţiunilor din jurnalul blockchain.

Conform unui aspect al acestei invenţii, tranzacţiile din jurnalul blockchain pot cuprinde orice raportări sau operaţie de farmacovigilenţă printre care cele mai importante sunt:

- operaţii declarative care permit definirea structurii cererilor de operaţii acceptabile de către sistem şi a versiunilor de implementare ce pot fi consultate şi/sau,
- mesaje din partea clienţilor ce cuprind cereri de operaţii complexe şi/sau,
- operaţii de stare care salvează starea de execuţie curentă după execuţia şi/sau,
- operaţii declarative de noi utilizatori (i.e. medici, Deţinători de licenţă, Farmacii etc.) ce conţin identităţile lor şi care pot fi publicate în întregime sau parţial criptate etc.

Alte avantaje sunt prezentate şi vor deveni evidente din descrierea detailată a invenţiei.

În continuare oferim o descriere literară a funcţionării unei implementări posibile ce trebuie să fie înţeleasă larg, ca un exemplu în care opţiunile de implementare alese nu sunt limitări ci exemple.

Metoda enunţată este bazată pe tehnologia blockchain şi permite raportarea şi analiza stării rezistenţei la preparatele antimicrobiene de către orice client implicat în utilizarea şi controlul eficienţei preparatelor antimicrobiene cu scopul analizei eficienţei, detectării fenomenului AMR şi reacţiei la apariţia fenomenului AMR indiferent de natura, structura şi anvergura membrilor

rețelei. Conform studiului actual al invenției, se pot identifica 4 actori implicați în raportarea fenomenului AMR:

- Pacient
- Profesionist în domeniul sănătății (Medic, Veterinar, Farmacist)
- Deținător autorizație (Companii farmaceutice din România, UE, țări terțe)
- Agenție națională (e.g. ANMDM, Agenția Europeană pentru Medicamente)

În sistemul propus, una sau mai multe agenții naționale activează ca o autoritate supremă de încredere, respectiv precum creatorul arhitecturii și a cărei chei publice este certificată și cunoscută de toți participanții. O agenție națională trebuie să se ocupe de menținerea rețelei, primirea și procesarea rapoartelor, iar ceilalți actori doar înregistrează rapoartele în blockchain, cu datele personale criptate pe baza permisiunilor oferite de deținătorul sau deținătoarea datelor. Acest lucru este posibil datorită mecanismelor criptografice intrinseci tehnologiei blockchain folosite, unde identitatea unei entități este asigurată de o pereche de chei, una privată (care nu trebuie divulgată nimănui) și una publică (derivată de la cheia privată într-un mod sigur, și care este expusă public). Cererile de operații în sistem sunt semnate criptografic fapt care asigură validarea fiecărei operații. Fiecare adresă în blockchain este asociată unei chei publice, respectiv, fiecare operație este validată cu ajutorul cheii private, oferind certificarea că doar deținătorul original al cheii a efectuat acea operație (ca singur posesor al cheii private asociate cheii publice). Sunt acceptate și operații de către utilizatori anonimi atât timp cât aceștia fac dovada rezolvării unui puzzle criptografic dificil și care limitează atacurile malițioase.

De asemenea, pentru fiecare raport va fi generat un șir de biți unic (cu ajutorul sumelor de control hash și al semnăturilor criptografice), asemănător unei semnături, pentru evitarea publicării și introducerii în baza de date a rapoartelor

duplicate sau neautentice. Mai exact, pentru verificarea dublurilor anumite date dintr-un mesaj care au un caracter unic precum CNP-ul unei persoane vor fi trecute printr-un algoritm de hash generând o sumă de control ce poate fi verificată în alte rapoarte şi operaţii pentru a elimina dublurile. Acest aspect este bine-cunoscut din tehnicile de indexare a bazelor de date. Este esenţial de menţionat că aceste date nu sunt vizibile, ele fiind salvate local de un nod într-o bază de date asociativă şi nu pot fi derivate în niciun mod de la semnătura generată. Pe lângă acestea, un Pacient sau un Profesionist în domeniu nu trebuie să aibă iniţial un cont (adică o cheie) în blockchain, ci poate comunica direct cu noduri menţinute de Agenţia naţională sau un Deţinător de autorizaţie, care la rândul lor sunt responsabili de a procesa rapoartele şi de a acţiona corespunzător conform legilor în vigoare.

În cazul rapoartelor transmise din partea Deţinătorului autorizaţiei, se vor publica în registru toate rapoartele specifice utilizate pentru descrierea eficienţei sistemului de farmacovigilenţă intern, a sistemului de management de risc al medicamentelor sau ce conţin orice actualizări efectuate de acesta. Înainte de aceasta cheia publică sau mai precis certificatul Deţinătorului autorizaţiei trebuie să fie validat şi adăugat de Agenţia naţională într-o listă cu toţi participanţii şi care apare tot în jurnalul blockchain. O problemă ar putea apărea atunci când cheia privată a unui Deţinător de autorizaţie este pierdută sau divulgată unui actor maliţios. Pentru a remedia situaţia, deţinătorul original al cheii poate contacta Agenţia naţională pentru a invalida cheia pierdută care repudiază certificatul printr-o operaţie ce apare de asemenea în jurnalul blockchain şi pentru a valida o cheie nouă.

Deoarece rapoartele sunt vizibile tuturor, Deţinătorul autorizaţiei nu poate ignora un raport de rezistenţă antimicrobiană şi ar fi motivat să acţioneze rapid la îmbunătăţirea metodelor de farmacovigilenţă, deoarece lipsa adoptării unor măsuri de îmbunătăţire va fi imediat detectabilă. Totodată la primirea unui

raport ce detaliază efectele adverse ale unui medicament, Agenția națională poate solicita deținătorului autorizației un nou raport ce ar exprima metodele de intervenție folosite pentru a minimaliza riscurile utilizării respectivului medicament. În acest caz, Agenția națională poate detecta momentul de timp exact în care Deținătorul autorizației a luat cunoștință de efectele adverse și va trebui să acționeze conform intervalelor de timp stabilite de legi, i.e. la 15 zile în cazul efectelor adverse de natură gravă și 90 de zile în cazul efectelor adverse considerate mai puțin grave. Astfel se pot lua măsuri asupra modificării autorizației medicamentului mai rapid decât de obicei, iar sănătatea publică nu va suferi din cauza procesării îndelungate, a rapoartelor întârziate, evitând astfel și acele situații în care Deținătorul autorizației nu recunoaște momentul de timp când a luat cunoștință de efectul advers. Pe lângă acestea, fiecare participant al arhitecturii are acces la istoricul de operații efectuate și poate obține istoricul complet care a dus la starea curentă, deci un deținător de autorizație poate identifica ușor cauzele ce au adus la ineficacitatea medicamentului și poate efectua o evaluare științifică mai exactă. De asemenea, se vor evita cazurile de falsificare în contextul raporturilor de farmacovigilență din cauza transparenței și integrității datelor, inerente funcționalității blockchain – aspecte care susțin supravegherea distribuirii rapoartelor de eficiență a medicamentelor dar și de asigurarea integrității și imutabilității datelor.

Toate datele și operațiile într-un blockchain sunt încorporate în secvențe de blocuri de date. Un bloc reprezintă o structură de date ce conține un antet care are o referință criptografică (e.g. o funcție de hash) la blocul anterior. Prin urmare, odată ce s-a stabilit un consens asupra ultimului bloc ce reprezintă starea actuală, nu se mai pot modifica operațiile și datele din trecut fără a se restabili un consens asupra unei noi stări – aspect care asigură non-repudierea. În acest caz, algoritmul de consens ar trebui să garanteze dificultatea practică de a efectua aceste modificări nejustificate care în majoritatea cazurilor sunt de

natură malițioasă. Pentru invenția în cauză, s-a implementat un sistem de consens bazat pe autoritate, unde fiecare bloc este validat de autoritatea supremă de încredere, i.e. Agenția națională, prin furnizarea unei semnături digitale generată de la cheia privată a entității. Participanții în acest consens sunt nodurile dispuse de Agenția națională, cu resurse disponibile pentru mentenanța și întreținerea unui sistem/server ce rulează permanent, capabil de a primi operațiile de la ceilalți participanți din rețea. După stabilirea consensului, starea fiecărui participant este actualizată conform tranzacțiilor incluse în ultimul bloc validat. Pentru a economisi spațiu, se dedică noduri speciale cu rol de stocare, i.e. nodurile deținute de Agenția națională sau de către orice deținător de autorizație, ce sunt interogate în momentul în care un participant ar dori să acceseze unele date sau informații din trecut. De exemplu, un Specialist în domeniul sănătății poate să consulte baza de date din blockchain pentru a afla reacțiile adverse ale unui anumit medicament înainte de a prescrie o rețetă unui anumit pacient. La fel poate acționa și un pacient înainte de a procura un medicament ce nu necesită o rețetă. În acest caz sunt accesibile doar informațiile publice dintr-un raport, cum ar fi reacțiile adverse, tipul de medicament sau orice alt tip de date fără caracter personal sau care nu descriu o identitate.

Se dă în continuare un exemplu de realizare a invenției în legătură cu figurile care reprezintă:

Figura 1prezintă sistemul de raportare la rezistența antimicrobiană (100).

Figura 2 ilustrează structura unui nod (101) al sistemului de raportare (100), fie el de consens (101a) sau stocare (101b) (vezi figura 1).

Figura 3 detaliază structura unui jurnal blockchain (200), pentru o implementare preferabilă,și care este compus din blocuri de date (210a-210b).

Figura 4 ilustrează două exemple de mesaje (105a-b) ce sunt cereri de operații care pot fi recepționate de sistemul de raportare (100) (vezi figura 1).

Figura 5 exemplifică un mesaj (105c) care este o cererea de operație specială care definește cerere de operație ce poate fi recepționată de sistemul de raportare (100) (vezi figura 1), cererea specială poate fi consultată de utilizatori pentru a afla structura unei operații.

Figura 6 ilustrează pentru o implementare preferabilă o listă de funcții de validare Java Script care trebuie respectate de un client pentru a crea o cerere de operație (105) validă.

Figura 7 prezintă un exemplu de criptare al unei operații și care restricționează accesul la toate datele criptate conform unei cerințe GDPR.

Figura 8 ilustrează în continuarea figurii 7 printr-un exemplu preferabil, două operații de dezvăluire a unei părți criptate și care permite unui utilizator terț să își dezvăluie identitatea și să ceară accesul la un mesaj de raportare prealabil criptat de un utilizator inițial care dezvăluie conținutul raportării.

Figura 9 descrie pașii unei metode de raportare a rezistenței la preparatele antimicrobiene ce poate fi executată de un nod (101) al unui sistem de raportare la preparatele antimicrobiene (100).

Este de la sine înțeles că desenele și descrierea detailată ce urmează a fi prezentate sunt oferite ca exemple preferabile ele nelimitând spiritul invenției. De asemenea este evident că, pentru o persoană antrenată în domeniul rezistenței la preparatele antimicrobiene și al tehnologiei blockchain,alte exemple și variante de implementări alternative ar fi evidente și sunt ușor de identificat și extrapolat în spiritul invenției.

In cele ce urmează se da descriere detaliată a unor implementări preferabile. Aceleași referințe alfanumerice sunt utilizate pentru identificarea aceluiași element în diversele ilustrații. Referințele având același prefix numeric

urmat de un caracter sunt variante ale aceleiași entități sau exprimă o secvență având ca referință prefixul numeric al unei aceleiași entități.

Figura 1 prezintă un sistem de raportare la rezistența antimicrobiană (100) de tip descentralizat care constă dintr-un număr de unul sau mai multe noduri de consens (101a) și din unul sau mai multe noduri de stocare (101b) ce sunt legate între ele și pot comunica printr-o rețea de tip peer-to-peer (103). Oricare din nodurile sistemului (101a-b) sunt accesibile de către utilizatori (110a-e) printr-o rețea publică (104). Utilizatorii externi (110a-e) pot trimite sistemului de raportare (100) mesaje (105) ce conțin cereri de operații și primesc răspunsuri **cu rezultate**. Fiecare utilizator (110a-e) are un rol definit: Medic (110a), Pacient (110b), Distribuitor Licențiat de Medicamente sau Farmacie (110c), Producător sau deținător de licență (110e) pentru un medicament sau operator ANMDM (110e) al Agenției Naționale a Medicamentelor și a Dispozitivelor Medicale.

Conform unui aspect al acestei invenții, fiecare utilizator are o identitate digitală preferabil semnată printr-un certificat digital semnat ierarhic de o autoritate autentificată și poate interoga sistemul de raportare (100) emițând mesaje (105) cu cereri de operații.

Conform unui aspect al acestei invenții, sistemul de raportare (100) acceptă spre procesare cererile de operații (105) în funcție de parametrii mesajului și de rolul utilizatorului (110a-e) care l-a emis. Spre exemplu, pentru anumite medicamente ANMDM poate restricționa raportarea de evenimente medicale permițând doar medicilor (110a) să raporteze contraindicațiile grave, iar pentru alte medicamente ea poate să permită raportarea oricărui pacient (110b) cu condiția ca acesta să nu fie spre exemplu anonim, ci să aibă declarată identitatea sa digitală.

Conform unui aspect al acestei invenții, cererile de operații din mesajele (105) pot fi interogări de informații ce nu schimbă starea sistemului de raportare (100) sau operații care schimbă starea sistemului prin modificarea unui jurnal de

operații local care reprezintă starea scrisă a sistemului. Distincția între nodurile de consens (101a) și cele de stocare (101b) este legată de acest aspect și anume, nodurile de stocare (101b) pot primi doar cereri de interogare, iar nodurile de consens (101a) pot executa și operațiuni care schimbă starea sistemului.

Figura 2 detaliază pentru o implementare preferabilă structura logică a unui nod (101) sistemului de raportare (100), fie el de consens (101a) sau stocare (101b) (vezi figura 1). Așa cum este evident pentru o persoană antrenată în domeniul sistemelor informatice, nodurile (101) ale sistemului de raportare (100) sunt aplicații software ce rulează fiecare pe un computer având cel puțin:

- unitate centrală de procesare CPU capabilă să încarce și să execute programul aplicației preferabil scrisă sub forma unuia sau mai multor fișiere executabile și,
- o memorie cu acces aleator în care instrucțiunile ce descriu aplicația sunt încărcate și din care sunt citite de unitatea centrală pentru a fi executate și care mai stochează și starea aplicației pe perioada execuției și,
- un mediu de stocare permanent care stochează codul aplicației și starea persistentă a acesteia chiar și când nodul nu este alimentat cu energie electrică sau când aplicația nu rulează și,
- un periferic pentru comunicațiile în rețea, preferabil de tipul Ethernet, și care permite nodurilor (101) să comunice între ele și cu utilizatorii externi (110).

Conform figurii 2 și cu referire la pașii metodei ilustrate în figura 9, fiecare nod (101) conține o interfață care preia dintr-o rețea de comunicații (104) mesaje (105) cu cereri de operații.

Într-o implementare preferabilă ilustrată în figura 2, interfața (1012) transmite mesajul (105) către un subsistem de procesare (1011) ce conține un serviciu de procesare (1013) configurat pentru a executa pașii (302-320) ai metodei menționate și să colaboreze cu un subsistem blockchain (1015) configurat și

care este conectat prin rețeaua de tip peer-to-peer (103) și care colaborează cu serviciile blockchain (1016) ale altor instanțe de noduri (101), serviciul blockchain (1016) fiind configurat să execute pași (331-337) ai metodei și să mențină local un jurnal blockchain (200) compus dintr-un număr de blocuri (210) fiecare având un antet (211), o listă de operații sau tranzacții (212) și niște metadate criptografice(213) care atestă validitatea și autenticitatea blocului și apartenența acestuia la jurnal (200).

Într-o implementare alternativă neilustrată, interfața (1012) preia mesaje (105) și le transmite direct subsistemului blockchain (1015), iar subsistemul de procesare (1011) care monitorizează schimbările din jurnalul blockchain (200) reacționează la apariția unui mesaj (105) și produce rezultate pe care le înregistrează tot prin subsistemul blockchain (1015) în jurnalul blockchain (200) și eventual notifică prin aceiași interfață (1012) clienții. Această variantă de implementare este preferabilă în cazul în care subsistemul blockchain (1015) este unul public, iar ANMDM nu deține monopolul asupra acestuia ci este doar un utilizator.

Conform unui aspect al acestei invenții, serviciul de procesare (1013) utilizează o bază de date locală (1014) de tip cache indexat care îi permite procesarea mesajelor (105) fără a interoga și decripta și parcurge în mod repetat și inutil jurnalul (200),accelerând execuția pentru operație ce ar fi costisitoare din punct de vedere al performanței. Baza de date (1014) permite deci accelerarea execuției aceasta neavând un alt rol funcțional.

Conform unui aspect al acestei invenții, subsistemul blockchain este preferabil de tip privat, implementarea lui fiind bine-cunoscută din stadiul artei diferența fiind aceea că tranzacțiile înregistrate în jurnalul blockchain (200) sunt operații specifice sistemului de raportare (100), ele fiind structuri de date parțial criptate și codificate într-un format scris precum formatul JSON sau XML.

Conform unui aspect al acestei invenții, întrucât operațiile sunt scrise și publicate în jurnalul blockchain (200) ele sunt accesibile oricărui utilizator (110) cu mențiunea că, părțile din operații care sunt criptate nu pot fii interpretate de utilizatorii neautorizați care nu dispun de o cheie de decriptare.

Conform unui aspect al acestei invenții, sistemul de raportare (100) este distribuit și beneficiază de toate avantajele tehnologiei blockchain și anume:

- Transparență - fiecare operație înregistrată în jurnalul blockchain (200) este vizibilă.
- Integritate, validitate și imutabilitate a datelor - datorită mecanismelor intrinseci de securitate criptografice, respectiv a structurilor de date specifice tehnologiei blockchain datele sunt imutabile și semnate deci nu pot fi șterse sau alterate, iar integritatea lor poate fi verificată.
- Reziliență și rezistență la defecte –nodurile (101) sunt distribuite și independente, iar datorită subsistemului blockchain (1015) ele cooperează prin rețeaua peer-to-peer (103) pentru asigurarea coerenței jurnalului blockchain (200) local. Nodurile fiind independente toleranța la defecte este crescută.
- Disponibilitate înaltă –adăugarea de noi noduri (101) permite creșterea capacității sistemului pentru a suporta un număr sporit de utilizatori și tranzacții.
- Non-repudiere - operațiile prezente în blockchain nu pot fi negate sau oprite sau șterse de o entitate. În același mod, o entitate care inițiază o operație va putea fi identificată ulterior la orice moment de timp prin mecanisme criptografice.
- Securitate sporită - datorită multitudinii de noduri participante în rețea, sistemul nu are un punct central de vulnerabilitate și poate să opereze în continuare la deconectarea unui nod.

- Lipsa întârzierilor de raportare – operaţiile publicate în jurnalul blockchain (200) sunt vizibile şi disponibile imediat nefiind necesară o aprobare şi nu pot fi şterse. Orice utilizator poate verifica dacă cererea sa este înregistrată în timp real.
- Posibilitatea eliminării cenzurii – într-o implementare avansată în care subsistemul blockchain este unul public, nodurile aparţinând mai multor utilizatori, distribuitori de medicamente şi ONG-uri şi autorităţi de control şi care utilizează, aşa cum este cunoscut din cazul sistemului Bitcoin, o schemă de autorizare a rundelor de tipul "proof-of-work" şi nu de tipul "proof-of-authority" cum este cazul pentru un sistem blockchain privat, este posibil ca cenzura să fie eliminată în condiţiile în care nici una din părţile participante nu deţine mai mult de jumătate plus unul din numărul de noduri.
- Trasabilitate şi corelaţie – datorită semnării criptografice a operaţiilor şi respectiv a blocurilor şi datorită tehnologiei blockchain, toate operaţiile şi raportările sintetice pot fii urmarite, sursa informaţiilor lor fiind identificabilă ele putând fii corelate unele cu altele. Astfel, nu pot fi inventate rapoarte de sinteză false fără ca sursa evenimentelor lor sa nu disponibilă.

Figura 3 ilustrează pentru o implementare preferabilă structura unui jurnalul blockchain (200). Acesta cuprinde o listă de blocuri (210a-201b) din care primul bloc (210a) este rădăcina, iar următoarele sunt blocuri înlănţuite (210b) ce fac fiecare referinţă la blocul precedent printr-o sumă de control hash. Fiecare nod conţine un antet (211), o listă de operaţii (212) şi o semnătură criptografică (213).

Antetul (211) unui bloc înlănţuit cuprinde mai multe câmpuri de date din care:

- "*previous_hash*" este un câmp obligatoriu și are ca valoare suma de control hash a blocului precedent din listă. Într-o implementare preferabilă această semnătură poate fii de exemplu printr-un algoritm precum MD5.
- "*timestamp*" este opțional dar preferabil și marchează data și ora când blocul a fost creat și scris. Într-o implementare preferabilă acest câmp este scrisîntr-un format UNIX-Epoch, UTC sau ISO-8601.
- "*body_length*" este preferabil dar opțional și reprezintă lungimea în octeți a corpului (212) ce conține lista de operații.
- "*block_ID*" este opțional și este un număr de index unic pentru fiecare bloc. Într-o implementare preferabilă indexul fiecărui bloc este incremental cu pasul unitar și pornește de la indexul blocului rădăcină (210a) care este ales prin convenție a fi zero sau unu.
- "*nonce*" este un câmp obligatoriu doar daca subsistemul blockchain (1015) este unul public iar schema de autorizare a rundelor este de tipul "*proof-of-work*" sau dacă subsistemul blockchain (1015) este privat și schema de autorizare a rundelor este de tipul "*proof-of-authority*" dar care acceptă și mesaje (105) de la utilizatori anonimi adică fără identitate digitală și care pentru a putea publica un mesaj trebuie să dovedească că nu sunt malițioși și să rezolve un puzzle de o dificultate și cu o valoare rezultat precizate în acest câmp. În acest ultim caz, acest câmp permite unui nod (101) să implementeze un mecanism reglator (i.e. termenul anglo-saxon original fiind acela de "throttling") care limitează eficacitatea atacurilor cibernetice prin inundarea cu mesaje neautorizate și în care, fiecare utilizator ce dorește să publice un mesaj trebuie să facă un efort computațional prealabil pentru rezolvarea puzzle-ului dat și care atestă prin răspunsul său că este bine intenționat făcând costisitoare atacurile cu mesaje false.

Corpul blocului (212) cuprinde o listă cu operaţiile recepţionate de nodul curent (101) într-o rundă de timp, operaţiile din listă fiind extrase din mesajele (105) sau produse de subsistemul de procesare (1011) ca urmare a execuţiei unei cereri de operaţii.

Semnătura criptografică (213) atestă că, conţinutul blocului este nemodificat şi autentic conform unei autorităţi digitale. În cazul preferabil semnătura (213) este o funcţie hash MD5 semnată cu un algoritm criptografic "RSAES-OAE". Alte scheme şi algoritmi echivalenţi sunt posibile.

Conform unui aspect al acestei invenţii şi într-un caz preferabil, subsistemul blockchain (200) este privat şi se află sub o singură autoritate, semnătura criptografică a blocurilor fiind realizată de ANMDM prin nodurile (101).

Conform unui aspect al acestei invenţii, un bloc (210) este preferabil scris în formatul JSON.

Figura 4 şi cu referinţe la figurile precedente ilustrează două exemple de mesaje (105) reprezentând două operaţii ce au ca rezultat modificarea stării sistemului de raportare (100). Astfel, nodul de consens (101a) ce primeşte un astfel de mesaj (105a) îl introduce într-o listă de aşteptare, iar atunci când runda curentă de procesare periodică expiră scrie operaţia din corpul mesajului (1052a) în lista de operaţii (212) a unui bloc (210b) nou creat ce este inserat în jurnalul blockchain (200) şi semnat şi care va fi distribuit celorlalte noduri (101) prin reţeaua peer-to-peer (103) folosind un protocol de coerenţă.

Conform figurii 4, mesajul (105a) din stânga este un mesaj ce declară un eveniment medical pentru un medicament. Antetul mesajului (1051a) şi semnătura (1053a) sunt create de utilizator doar pentru nodul (101) de recepţie şi ele nu sunt publicate în jurnalul blockchain (200).

Conform unui aspect al acestei invenţii, antetul mesajului (1051a-b) poate cuprinde mai multe câmpuri:

- "*id*" este un câmp obligatoriu și reprezintă identificatorul operației din corpul mesajului (1052a). Într-o implementare preferabilă el are o structură ierarhică similară unui nume de domeniu Web invers în care prefixul precizează autoritatea care a definit mesajul și tipul mesajului iar sufixul este numele operației. În exemplul din figura 4, autoritatea de definire a mesajului este agenția identificată ca fiind "*ro.anmdm*" unde "*ro*" este prefixul țării iar "*anmdm*" este acronimul instituției ANMDM. Tot conform aceluiași exemplu "*declaration*" este tipul mesajului acesta fiind o declarație iar "*medicalevent*" este numele operației. Evident alte codări și reprezentări sunt posibile singura cerință fiind unicitatea lor.
- "*version*" este un identificator de versiune. Este posibil ca sistemul să suporte mai multe versiuni ale unei operații, iar acest identificator permite discriminarea versiunii corecte ce trebuie executată.
- "*SID*" este opțional și este identificatorul sursei mesajului (105) ce conține două câmpuri. Câmpul "*protocol*" precizează cum trebuie interpretată identitatea a cărei valoare este scrisă în câmpul "*value*". Astfel, conform exemplului din figura 4 stânga, sursa mesajului (105) este un utilizator al cărui cheie publică conformă standardului RSA de 512biți este scrisă în câmpul "*value*" sub forma unui șir de caractere hexazecimal.

Conform unui aspect al acestei invenții, identificatorul sursei mesajului "*SID*" este un câmp opțional iar în cazul absenței lui mesajul are o sursă anonimă. Conform unui aspect al acestei invenții, nu este obligatoriu ca identificatorul "*SID*" să fie transmis în clar. Un exemplu de criptare fiind ilustrat în figura 7. Conform unui aspect al acestei invenții, similar câmpului "*SID*" este posibil să fie definit un câmp "*DID*" care este identificatorul destinației mesajului (105) și care are o structură identică în care valoarea câmpului "*value*"conține cheia publică a destinatarului.

Conform unui aspect al acestei invenții, în conformitate cu exemplul din figura 4 dreapta și pentru o implementare preferabilă, valoarea câmpului "*value*" poate fi și un certificat criptografic public spre exemplu într-un format "X509_PEM" sau altul așa cum este precizat prin câmpul "*protocol*" și care conține pe lângă cheia publică și alte informații fiind semnat și autentificat de o autoritate superioară.

Tot din Figura 4 stânga, corpul mesajului (1052a) conține o structură specifică operației de declarație pentru un eveniment medical având identificatorul definit în antet și care specifică valorile parametrilor specifici operației.

Conform unei implementări preferabile, câmpul "*source*" al mesajului precizează o sursă care este un pacient și care are diferite date de identificare precum CNP-ul, adresa ș.a.m.d.

Conform unei implementări preferabile conforme normelor GDPR, datele pot fi ascunse prin criptare, aspect ce este ilustrat în figura 7.

Tot din Figura 4 stânga, corpul mesajului (1052a) mai conține și mesajul declarației evenimentului și cuprinde câmpul:

- "*type*" – tipul evenimentului medical. Este de la sine înțeles că acest câmp are o valoare standardizată, iar valoarea "alergie" este dată doar ca titlu exemplificativ și pentru claritate.
- "*product*" – identificarea produsului. Ea conține
  - "*GTIN*" - identificatorul global al produsului
  - "*batch_id*" - identificatorul lotului medicamentului și,
  - "*SN*" – numărul serial al medicamentului și,
- "*symptoms*" - descriere a simptomelor observate preferabil folosind un standard precum ICD-10.

Tot din Figura 4 stânga, mesajul (105) poate conține și o semnătură criptografică (1053a) și care în acest caz este absentă mesajul fiind nesemnat.

Conform exemplului din figura 4 dreapta, mesajul (105b) este o declarație a unui producător de medicamente ce dorește să fie inclus pe lista producătorilor licențiați ai ANMDM.

Conform exemplului din figura 4 dreapta, corpul mesajului declară detaliile privind producătorul și anume:

- "*PID*" – este identificatorul unic de producător,
- "*name*" – este numele lizibil al producătorului,
- "*address*" – adresa sediului social al firmei,
- "*URL*" – link-ul paginii web al producătorului,
- "*SID*" – identificatorul sursă al producătorului. În cazul ilustrat acesta este precizat ca un certificat PEM X.509

Conform exemplului din figura 4 dreapta, mesajul (105b) este semnat printr-o succesiune de funcții hash producând valoarea finală din câmpul "*value*". Procedural, suma de control hash a mesajului este calculată inițial folosind algoritmul "MD5", iar apoi rezultatul este criptat conform protocolului "RSAES-OAEP" cu cheia privată a producătorului de medicamente, care nu este divulgată, dar care își face cunoscută cheia sa publică SIDsub forma unui certificat semnat digital de o autoritate superioară, și care permite ANMDM să decripteze în sens invers și să calculeze suma de control hash originală ce poate fii comparată cu cea a mesajului,iar în caz că acestea coincid să aibă certitudinea că într-adevăr producătorul având identificatorul sursa SID este cel ce a creat mesajul care este nealterat.

Conform unui aspect al acestei invenții un mesaj poate avea mai multe semnături alternative. În cazul exemplului din figura 4 dreapta, lista semnăturilor are doar o variantă.

Figura 5 și cu referințe la figurile precedente prezintă un mesaj (105c) special în sensul că el este un mesaj declarativ de operații posibile în sistem.

Conform unui aspect major al acestei invenţii, ANMDM poate defini sine-die noi operaţii posibile, versiuni de implementare şi să repudieze operaţiile existente,iar aceste definiţii sunt publicate în jurnalul blockchain (200) fiind direct disponibile utilizatorilor care astfel pot consulta în orice moment lista definiţiilor şi pot verifica dacă ANMDM respectă standardele de raportare. Este astfel posibilă modificarea dinamică şi transparentă a operaţiilor din sistemul (100) fără a necesita o altă infrastructură specială, sistemul de raportare (100) fiind deci reflexiv şi dinamic.

Astfel, conform exemplului ilustrat în figura 5, ANMDM are prefixul de domeniu de identificare "*ro.anmdm.declarations*" rezervat declaraţiilor ce descriu capabilităţile sistemului (100) şi prin el poate modifica comportamentul sistemului. Mai precis, prin sub domeniul "*ro.anmdm.declarations.operations*", ANMDM poate modifica lista de operaţii acceptabile de către sistemul de raportare (100) şi a versiunilor de implementare ale acestora neavând nevoie de o altă infrastructură de implementare decât acelaşi jurnal blockchain (200).

Conform exemplului ilustrat în figura 5, ANMDM declară prin mesajul ilustrat o nouă versiune "2.0" pentru operaţia de raportare "*ro.anmdm.declarations.medicalevent*" a cărei utilizare, dar cu versiunea "2.0" este ilustrată în figura 4 stânga.

Conform exemplului ilustrat în figura 5, câmpul "*operation*" defineşte structura operaţiei şi a câmpurilor sale în care valorile sunt iniţializate cu valori implicite nenule sau valori goale.

Conform unui aspect major al acestei invenţii, câmpul "*validations*" conţine o listă de predicate care pot fi verificate de un client ce doreşte să emită o cerere de operaţie printr-un mesaj. Fiecare din predicate verifică structura mesajului şi valorile câmpurilor. Clienţii pot astfel verifica dacă o operaţie este validă sau nu înainte de a emite mesajul (105) cu cererea de operaţie. Aspectul de validare ilustrat în figura 6.

Figura 6 prezintă un exemplu de implementare preferabilă în care predicatele de validare din figura 5 sunt implementate ca funcții JavaScript și care, în cazul unei erori returnează un mesaj de eroare. Aceste funcții sunt scrise în format JSON sub forma unei liste de scripturi executabile preferabil fără alte dependențe externe decât cele precizate de ANMDM.

Conform unui aspect al acestei invenții, prezența predicatelor de validare nu constituie un punct de risc de securitate pentru sistemul de raportare (100) întrucât acestea nu sunt executate de către nodurile (101) și întrucât utilizatorii nu sunt obligați să le ruleze, iar codul sursă este semnat și controlat în prealabil de ANMDM.

Conform unui aspect de implementare al acestei invenții, utilizarea funcțiilor JavaScript ca predicate este un avantaj care facilitează implementarea aplicațiilor client de tip Web.

Figura 7 ilustrează printr-o modalitate de criptare parțială a unei cereri de operații (1052) și care poate fi utilizată pentru ascunderea selectivă a oricăror date și expunerea lor conformă cu un protocol de tipul unui automat cu stări finite FSM.

Conform exemplului din figura 7, corpul unui mesaj (1052d) conține în parte date cu caracter privat care trebuie să fie vizibile ANMDM sau, spre exemplu, oricărui utilizator care primește explicit dreptul de acces dar care trebuie ascunse publicului datorită cerințelor legislației GDPR.

Conform exemplului din figura 7, corpul mesajului în clar (1052d) poate fii înlocuit cu un corp de mesaj parțial criptat (1052e) echivalent și care permite accesul la datele protejate doar de către ANMDM sau unui utilizator terț care face o cerere de acces utilizatorului posesor.

Conform exemplului din figura 7, corpul mesajului clar (1052d) este separat în două obiecte, un obiect public (401) și un obiect privat (402) ce urmează a fi

criptat şi care conţine acele câmpuri ale corpului mesajului (1052d) care sunt private şi trebuie ascunse prin criptare. Precum se observă, corpul mesajului (1052d) poate fi obţinut prin reuniunea obiectelor (401-402). Obiectul privat (402) ce trebuie criptat este scris şi criptat folosind două scheme de criptare şi anume o primă criptare folosind cheia publică DID a destinatarului care este ANMDM şi o a doua criptare cu o cheie privată ad-hoc PEID (i.e. termenul în limba engleză fiind "Private encription key ID") care nu este ilustrată în figură deoarece nu este divulgată în mesajul (1052e) iar cheia publică EID (i.e. termenul în limba engleză fiind "Encription key ID") conjugată ei care este publicată în corpul mesajului criptat (1052e) împreună cu valoarea criptată a obiectului (402). Astfel, ANMDM poate decripta mesajul (1052e) deoarece dispune de cheia sa privată şi nici un alt utilizator din sistem nu poate decripta partea ascunsă a mesajului (1052e) deoarece nu dispune de cheia PEID. Mai mult, identitatea sursei nu este cunoscută de nici un utilizator altul decât cel ce a emis mesajul cu corpul (1052e) şi de ANMDM cerinţele GDPR cerute fiind respectate.

Conform unui aspect al acestei invenţii, un utilizator care dispune de una din cheile private PEID, necunoscută încă,ar putea decripta câmpul "_merge_encrypted1" şi obţine obiectul privat (402) pe care l-ar putea injecta printr-o reuniune cu mesajul (1052e) din care câmpul"_merge_encrypted1" a fost în prealabil şters pentru a obţine corpul mesajului în clar (1052d).

Conform unui aspect al acestei invenţii, exemplul din figura 7 este unul simplificat pentru claritate, în realitate într-o implementare preferabilă, pentru a menţine ordinea câmpurilor neschimbată obiectul privat (402) este reprezentat printr-o secvenţă de comenzi DIFF care aplicate obiectului public (401) produc corpul mesajului (1052d), aceste comenzi fiind criptate.

Figura 8 continuă exemplul din figura 7 şi exemplifică cum un utilizator terţ poate obţine de la utilizatorul iniţial dreptul de a accesa datele private din

mesajul criptat (1052e). Astfel, prin mesajul (105f) utilizatorul terț emite o operație de tipul "*ro.anmdm.declaration.medicalevent.onrequest.issued*"în care atât corpul (1052f) cât și semnătura (1053f) conțin părți criptate cu cheia publică ad-hoc EID și care pot fi decriptate doar de către utilizatorul inițial. Pentru a evita atacurile, mesajul mai conține și date criptate ce sunt accesibile doar de către ANMDM prin cheia privată conjugată cheii publice DID și care poate conține identitatea SID a utilizatorului terț sau, dacă sistemul este configurat pentru a accepta mesaje de la utilizatori anonimi să conțină soluția unui puzzle "*proof-of-work*". Utilizatorul inițial află de existența mesajului (105f) fie prin monitorizare directă fie de la ANMDM care cunoaște atât indicatorul de secvență cât și identitatea utilizatorului inițial și care notifică utilizatorul inițial atunci când mesajul (105e) este recepționat.

Conform exemplului din figura 8, doar utilizatorul inițial poate decripta partea mesajului criptată cu cheia EID și prin decriptare poate afla conținutul obiectului dezvăluit (403) de utilizatorul terț care conține numărul de secvență și identitatea lui.

Conform exemplului din figura 8 și ca urmare a decriptării parțiale a mesajului (105f) prin aflarea obiectului dezvălui (403) ce conține identitatea utilizatorului terț, utilizatorul inițial care cunoaște acum identitatea utilizatorului terț și cererea sa, poate dacă dorește să răspundă printru ultim mesaj (1052g) care este adresat utilizatorului terț și doar lui.

Conform exemplului din figura 7 și în conformitate cu un aspect al acestei invenții cheia unică PEID este dezvăluită utilizatorului terț prin mesajul criptat din corpul mesajului final (1052g).

Conform unui aspect al acestei invenții ce reiese din figurile 7 și 8, observăm că toate mesajele dintre utilizatorul inițial și cel terț sunt criptate și pot fi accesate doar de aceștia neexistând nici o corelație între publicarea raportului inițial criptat (1052e) și cererea de divulgare (1052f) și răspunsul final (1052g).Totuși,

rolul ANMDM nu este eliminat complet şi pentru simplitate se preferă ca aceste operaţii să fie verificate pentru autenticitate şi coerenţă deşi aceasta este mai degrabă o alegere de implementare.

Conform unui aspect major al acestei invenţii, orice contract complex, poate fi descris printr-un automat cu stări finite în care mesajele sunt evenimente ce declanşează tranziţii adică operaţiile şi care schimbă starea sistemului adică a jurnalului blockchain (200). Astfel operaţiile active (i.e. care nu sunt simple interogări ce nu schimă starea sistemului) sunt tranziţiile din automate şi sunt scrise în jurnalul blockchain (200) care poate fi văzut ca o trasă de execuţie parţial criptată, operaţiile fiind descifrabile doar de către cei autorizaţi ce dispun de cheile de decriptare.

Figura 9 prezintă o implementare preferabilă a unei metode de raportare a rezistenţei la preparatele antimicrobiene ce poate fi executată de un nod (101) al unui sistem de raportare la rezistenţa antimicrobiană (100) şi care cuprinde etapele de:

- Iniţializare(302) în care:
  - nodul (101) porneşte şi configurează un subsistem de procesare (1011) şi,
  - nodul (101) porneşte şi configurează un subsistem blockchain (1015) local de tip privat sau se conectează la un subsistem blockchain extern de tip public şi,
- Aşteptare (303) în care aşteaptă:
  - apariţia unui mesaj (105) de la un utilizator (110) printr-o interfaţă (1012) conectată la o reţea (104) sau,
  - apariţia unei tranzacţii într-un jurnal blockchain (200) al unui subsistem de blockchain (1015) extern public, tranzacţia fiind un mesaj (105) primit de către subsistemul blockchain (1015) de la un

utilizator extern (110) prin intermediul unei rețele (104) și al unei interfețe de acces (1012) și,

- Recepție cerere operație (304) în care:
  - ca urmare a apariției unui mesaj (105) atunci când subsistemul blockchain este privat sau,
  - ca urmare a apariției unei tranzacții cuprinzând un mesaj (105) atunci când subsistemul blockchain (1015) este extern și public și,

subsistemul de procesare (1011) recepționează mesajul (105) și,

- Decriptare(305) în care, părțile criptate ale mesajul (105) recepționat criptate cu cheia publică al ANMDM sunt decriptate și,
- Validare operație (306) în care sunt verificate:
  - identificatorul și versiunea operației care trebuie să fie valide și,
  - structura corpului mesajului care trebuie să conțină toate câmpurile conform unei definiții a formatului mesajului cunoscută intern de către subsistemul de procesare și,
  - valorile câmpurilor mesajului folosind o listă de predicate de verificare care garantează că mesajul este bine definit și,
  - semnăturile mesajului care trebuie să fie autentice,iar suma de control să indice integritatea mesajului și,
  - tipul operației care, pentru nodurile configurate ca noduri de stocare, este restricționată la operații de tip interogare și,
- Discriminare tip operație (307) care separă tratare a operațiilor de interogare care nu schimbă starea sistemului (100) de operațiile care sunt acțiuni și au un contract de execuție ce schimbă starea sistemului și,

dacă operația este o interogare, este urmată de pasul de:

- Interogare (308) în care una sau mai multe operații salvate ca tranzacții în jurnalul blockchain (200) sau dintr-o bază de date cache local (1014) sunt citite și agregate și conform cererii de operație și,dacă operația este o

acțiune care presupune schimbări ale stării sistemului, este urmată de pașii de:

- Creare/Restaurare context (310) în care:
  - dacă operația este prima dintr-un contract identificat printr-un număr de secvență unic atunci creează un context de execuție format dintr-un tabel asociativ de chei și valori asociate sau,
  - dacă operația este o operație consecutivă dintr-un contract și care este identificat prin numărul de secvență unic atunci citește din jurnalul blockchain (200) lista de operații de reîmprospătarea stării și care sunt asociate contractului în desfășurare și care au fost salvate în prealabil când au fost executate operațiile precedente din contract și care au același număr de secvență și care prin execuția lor restaurează contextul de execuție pentru a fi identic cu cel precedent permițând executarea contractului din punctul rămas și,
- Execuție operație (311) în care o funcție ce are identificatorul identic cu identificatorul operației și aceeași versiune este invocată de subsistemul de procesare (1011) folosind parametrii din corpul mesajului și contextul de execuție din pasul precedent și care produce un răspuns și o listă de operații de împrospătare care, dacă sunt prezente, modifică starea contractului aflat în desfășurare și care trebuie scrise în jurnalul blockchain (200) și,
- Înregistrare tranzacție (312) care, în cazul în care starea contractului s-a schimbat prin execuția operației și contractul mai presupune și alte operații viitoare nefiind finalizat, salvează lista de operații de împrospătare în jurnalul blockchain (200) și,
- Răspuns operație (309) în care rezultatul operației calculat în pasul de execuție (311) este transmis utilizatorului.

GLOSAR de TERMENI

AMR	rezistența la preparate antimicrobiene
ANMDM	Agenția Națională a Medicamentului și Dispozitivelor Medicale
Bitcoin	Monedă și sistem de tranzacționare și creare a monedei bazat pe tehnologia blockchain.
Blockchain	Jurnal sau listă înlănțuită de blocuri de date sau înregistrări rezistentă la modificări, a cărei integritate și autenticitate pot fi verificate prin algoritmi criptografici de semnare și verificare ce fac quasi imposibilă falsificarea datelor.
DIFF	Protocol de comparare a versiunilor și pentru aplicarea de transformări de versiune pentru fișiere
FSM	Automat cu stări finite
GDPR	legislația europeană pentru protecția datelor cu caracter personal
GMT	Timpul conform meridianului zero Greenwitch
GTIN	”Global Trade Identification Number” identificator global al unui produs
Hash	funcție greu inversabilă rezistentă la coliziuni ce transformă un șir de date într-o sumă de control Hash criptografic
	Funcție hash ce folosește și o cheie si care permite calculul unei semnături digitale
ICD-10	Standardul internațional pentru clasificarea statistică a bolilor si simptomelor revizia a 10-a
JSON	Java Script Object Notation – formatul de scriere a obiectelor JavaScript
MD5	Algoritmul de hash “Message-Digest No. 5”

ONG	Organizație Non-Guvernamentală
P2P, Peer-to-peer	rețea de comunicații descentralizată, distribuită
PEM	Format folosind norma de codare BASE64 pentru stocarea certificatelor criptografice conform standardului RFC-1422
	proof-of-authority metodă prin care o acțiune este autorizată ca urmare a dovezii dispunerii unei autorizații sau autorității ce poate fi verificată și care este autentică și sigură din punct de vedere criptografic.
	proof-of-work metodă prin care o acțiune este autorizată ca urmare a rezolvării unei probleme dificile de tip puzzle fără cunoștințe a priori prin încercări repetate și a cărei soluție o dată găsită este ușor de validat.
RSA	standardul criptografic Rivest–Shamir–Adleman
UTC	Timp Universal Coordinat
UNIX-Epoch	Timpul actual exprimat numeric în format Unix
ISO-8601	Standardul internațional pentru formatul de timp
Client Web	Portal de aplicații conținând pagini și aplicații de tipul HTML/JavaScrit/CSS.

REVENDICĂRI

1. O metodă de raportare a rezistenței la preparatele antimicrobiene de către un utilizator (110) către un sistem de raportare (100) prin intermediul unor mesaje de raportare (105) ce conțin un antet (1051) un corp (1052) și preferabil o semnătură criptografică (1053) și care este executată de oricare din nodurile (101) ale unui sistem de raportare (100), **caracterizată prin aceea că** metoda cuprinde etapele de:

- **Inițializare** (302) în care:
  - nodul (101) pornește și configurează un subsistem de procesare (1011) și,
  - nodul (101):
    - pornește și configurează un subsistem blockchain (1015) local de tip privat sau,
    - se conectează la un subsistem blockchain extern de tip public și,
- **Așteptare** (303) în care așteaptă:
  - apariția unui mesaj (105) de la un utilizator (110) printr-o interfață (1012) conectată la o rețea (104) sau,
  - apariția unei tranzacții într-un jurnal blockchain (200) al unui subsistem blockchain (1015) extern public, tranzacția fiind un mesaj (105) primit de către subsistemul blockchain (1015) de la un utilizator extern (110) prin intermediul unei rețele (104) și al unei interfețe de acces (1012) și,
- **Recepție** cerere operație (304) în care:
  - ca urmare a apariției unui mesaj (105) atunci când subsistemul blockchain este privat sau,
  - ca urmare a apariției unei tranzacții cuprinzând un mesaj (105) atunci când subsistemul blockchain (1015) este extern și public și,

subsistemul de procesare (1011) recepționează mesajul (105) și,

- **Decriptare** (305) în care, părțile criptate cu cheia publică a ANMDM ale mesajului (105) recepționat sunt decriptate și,
- **Validare** operație (306) în care sunt verificate:
    - identificatorul și versiunea operației care trebuie să fie valide și,
    - structura corpului mesajului care trebuie să conțină toate câmpurile conform unei definiții a formatului mesajului cunoscută intern de către subsistemul de procesare și,
    - valorile câmpurilor mesajului folosind o listă de predicate de verificare care garantează că mesajul este bine definit și,
    - semnăturile mesajului care trebuie să fie autentice iar suma de control să indice integritatea mesajului și,
    - tipul operației care, pentru nodurile configurate ca noduri de stocare, este restricționată la operații de tip interogare și,

  dacă predicatele sunt invalide atunci ignoră mesajul și revine în pasul de așteptare sau dacă sunt valide atunci trece la etapa următoare și,

- **Discriminare** tip operație (307) care diferențiază tratarea operațiilor după tipul lor și care pot fi operații de interogare care nu schimbă starea sistemului (100) sau operații care sunt acțiuni și au un contract de execuție ce schimbă stare sistemului și,

dacă operația este o interogare, este urmată de pasul de:

- **Interogare** (308) în care una sau mai multe operații salvate ca tranzacții în jurnalul blockchain (200) sau dintr-o bază de date cache local (1014) sunt citite și agregate și conform cererii de operație și,

dacă operația este o acțiune care presupune schimbări ale stării sistemului, este urmată de pașii de:

- **Creare/Restaurare context** (310) în care:
    - o dacă operația este prima dintr-un contract identificat printr-un număr de secvență unic atunci creează un context de execuție format dintr-un tabel asociativ de chei și valori asociate și care inițial este gol sau,
    - o dacă operația este o operație următoare dintr-un contract identificat prin numărul de secvență unic atunci citește lista de operații de reîmprospătare a contextului de execuție din jurnalul blockchain (200) sau dintr-o bază de date cache locală (1014), operații care sunt asociate contractului în desfășurare și care au fost salvate în prealabil când au fost executate operațiile precedente din contract și care au același număr de secvență și care prin execuția lor restaurează contextul de execuție pentru a fi identic cu cel precedent permițând executarea contractului din punctul rămas și,
- **Execuție operație** (311) în care o funcție ce are identificatorul identic cu identificatorul operației și aceeași versiune este invocată de subsistemul de procesare (1011) folosind parametrii din corpul mesajului și contextul de execuție din pasul precedent și care produce un răspuns și o listă de operații de împrospătare care, dacă sunt prezente, modifică starea contractului aflat în desfășurare și care trebuie scrise în jurnalul blockchain (200) și,
- **Înregistrare tranzacție** (312) care, în cazul în care starea contractului s-a schimbat prin execuția operației și contractul mai presupune și alte operații viitoare nefiind finalizat, salvează lista de operații de împrospătare în jurnalul blockchain (200) și,

pentru orice tip de operație pasul de interogare sau pasul de înregistrare continuă cu un pas de:

- **Răspuns operație** (309) în care rezultatul operației calculat în pasul de execuție (311) sau răspunsul interogației (308) este transmis înapoi utilizatorului.

2. Metoda conform revendicării 1, **caracterizată prin aceea că** pasul de validare verifică și acceptă mesaje (105) ce cuprind un antet (1051) ce conține cel puțin un identificator unic și care identifică numele operației solicitate și un identificator de versiune care identifică ce variantă de implementare a operației este cerută spre a fi executată și care mai cuprinde un corp (1052) ce are un conținut specific metodei identificate și care cuprinde parametrii de execuție ai metodei conform unui format scris.
3. Metoda conform revendicării 2, **caracterizată prin aceea că** mesajul (105) mai cuprinde metadate criptografice (1053) ce cuprind o listă de semnături criptografice în care fiecare semnătură este formată dintr-o listă de funcții hash sau funcții hash criptografice și care sunt calculate înlănțuit una după cealaltă prima folosind ca valoare de intrare antetul (1051) concatenat cu corpul (1052) iar fiecare din următoarele folosind rezultatul funcției hash precedente din listă și în care fiecare funcție hash este identificată printr-un protocol care determină tipul funcției hash folosit și care mai cuprinde și o valoare care este rezultatul funcției hash.
4. O metodă conform revendicării 2, **caracterizată prin aceea că** identificatorul operației din antet (1051) este un identificator de definiție operație și care permite definirea de operații și în care corpul mesajului (1052) conține definiția operației definite ce poate fi cerută de un utilizator (110).
5. O metodă conform revendicării 4, **caracterizată prin aceea că** definiția operației din corpul mesajului (1052) cuprinde și o listă de predicate ce pot fi executate de un utilizator pentru a valida structura și valorile câmpurilor unui mesaj ce cuprinde o cerere de operație conformă cu definiția precizată.

6. O metodă conform revendicării 4, **caracterizată prin aceea că** definiția operației din corpul mesajului (1052) cuprinde o funcție script sau codul binar care este implementarea operației și care poate fi executat de un utilizator pentru verificarea rezultatului operației atunci când un nod execută operația și care permite utilizatorului să verifice că nodurile sistemului au executat ce trebuiau să execute conform operației.
7. Metoda conform revendicării 1, **caracterizată prin aceea că** sunt definite operații de:
   - creare/înregistrare și/sau,
   - acreditare și/sau,
   - repudiere,

   de către un utilizator a unui alt utilizator, medicament, studiu medical sau a altei entități de farmacovigilență.
8. Metoda conform revendicării 7, **caracterizată prin aceea că** în pasul de validare se verifică și dacă utilizatorul și/sau medicamentul și/sau studiul medical și/sau altă entitate de farmacovigilență din cererea de operație sunt valide și nerepudiate.
9. Metoda conform revendicării 1, **caracterizată prin aceea că** rezultatul unei operații este o tranzacție de raport cu referințe la alte operații înregistrate în jurnalul blockchain (200) și care precizează sursele de informații folosite la sintetizarea rezultatului.
10. Un sistem de raportare a rezistenței la preparatele antimicrobiene (100) distribuit format dintr-un număr de noduri (101) independente și care permite unor utilizatori (110) conectați printr-o rețea de acces (104) să comunice mesaje (105) către un nod din sistemul (100) ce cuprinde cereri de operații de farmacovigilență **caracterizat prin aceea că** fiecare nod:
    - conține sau se poate conecta la un subsistem blockchain (1015) distribuit ce acceptă cereri de tranzacții care sunt operații de farmacovigilență și

care sunt scrise într-un jurnal blockchain (200) de către un serviciu blockchain (1016) şi replicate printr-un protocol de consens printr-o reţea peer-to-peer (103) ce leagă instanţele distribuite ale serviciilor blockchain (1016) şi,

- conţine un subsistem de procesare (1011) ce cuprinde un serviciu de procesare (1013) şi o bază de date asociative cache locală (1014), serviciul de procesare fiind configurat să:
  - **fie iniţializat** şi configurat/autoconfigurat la pornire şi care:
    - porneşte şi configurează un subsistem blockchain (1015) local de tip privat sau,
    - se conectează la un subsistem blockchain extern de tip public şi să,
  - **aştepte**:
    - apariţia unui mesaj (105) de la un utilizator (110) primit prin intermediul interfeţei (1012) conectată la o reţeaua (104) sau,
    - apariţia unei tranzacţii în jurnal blockchain (200) al unui subsistem blockchain (1015) extern public, tranzacţia fiind un mesaj (105) primit de către subsistemul blockchain (1015) de la un utilizator extern (110) prin intermediul unei reţele (104) şi al unei interfeţe de acces (1012) şi să,
  - **recepţioneze** o cerere de operaţie ca urmare a:
    - apariţiei unui mesaj (105) prin interfaţa (1012) atunci când subsistemul blockchain este privat sau,
    - apariţiei unei tranzacţii în subsistemul blockchain (1015) extern public şi care cuprinde corpul unui mesaj (105) de farmacovigilenţă şi să,
  - **decripteze** părţile criptate ale corpului (1052) ale mesajului (105) şi care constituie o cerere de operaţie de farmacovigilenţă parţial

criptată folosind cheia privată a ANMDM cu care a fost configurat în etapa de inițializare și să,

- **valideze** cererea de operație decriptată verificând:
  - identificatorul și versiunea operației care trebuie să fie valide și,
  - structura corpului mesajului care trebuie să conțină toate câmpurile conform unei definiții a formatului mesajului cunoscută intern de către subsistemul de procesare și,
  - valorile câmpurilor mesajului folosind o listă de predicate de verificare care garantează că mesajul este bine definit și,
  - semnăturile mesajului care trebuie să fie autentice iar suma de control să indice integritatea mesajului și,
  - tipul operației care, pentru nodurile configurate ca noduri de stocare, este restricționată la operații de tip interogare și,

și dacă acestea sunt invalide atunci să ignore mesajul iar dacă sunt valide atunci să:

- **Discrimineze** execuția în funcție de tipul operației și dacă operația este o interogare atunci să:
  - **Interogheze** jurnalul blockchain (200), și/sau baza de date locală (1014) și să agrege conform cererii datele citite într-un răspuns sau,

dacă operația este o acțiune care presupune schimbări ale stării sistemului să:

- **Creeze/Restaureze** contextul de execuție al contractului corespunzător cererii de operație în care:
  - dacă operația cerută este prima dintr-un contract identificat printr-un număr de secvență unic atunci creează un context de execuție format dintr-un tabel asociativ de chei și valori asociate și care inițial este gol sau să,

- dacă operația este o operație următoare dintr-un contract identificat prin numărul de secvență unic atunci citește lista de operații de reîmprospătare a contextului de execuție din jurnalul blockchain (200) sau din baza de date cache locală (1014), operații care sunt asociate contractului în desfășurare și care au fost salvate în prealabil când au fost executate operațiile precedente din contract și care au același număr de secvență și care prin execuția lor restaurează contextul de execuție pentru a fi identic cu cel precedent permițând executarea contractului din punctul rămas și să,

- **Execute operația** cerută prin invocarea unei funcții ce are identificatorul identic cu identificatorul operației și aceeași versiune și care primește ca parametrii corpul mesajului și care utilizează contextul de execuție din pasul precedent și care produce un răspuns și o listă de operații de împrospătare care, dacă sunt prezente, modifică starea contractului aflat în desfășurare și care trebuie scrise în jurnalul blockchain (200) și să,
- **Înregistreze tranzacții** în jurnalul blockchain (200) pentru operațiile de reîmprospătare produse în cazul când starea contractului s-a schimbat prin execuția operației și contractul mai presupune și alte operații viitoare nefiind finalizat și,

pentru orice tip de operație în urma interogării sau a înregistrării tranzacțiilor să:

- **Răspundă** utilizatorului cu rezultatul obținut în urma execuției sau cu răspunsul interogării. Răspunsul fiind:
  - Direct atunci când cererea de operație este realizată prin intermediu interfeței (1014) sau,

- Indirect printr-o tranzacție de tip răspuns înregistrată în jurnalul blockchain (200) atunci când cererea de operație este indirectă și este obținută dintr-o tranzacție din jurnalul blockchain (200).

11. Sistem conform revendicării 10, **caracterizat prin aceea că** validează, verifică și acceptă mesaje (105) ce cuprind un antet (1051) ce conține cel puțin un identificator unic și care identifică numele operației solicitate și, un identificator de versiune care identifică ce variantă de implementare a operației este cerută spre a fi executată și, care mai cuprinde un corp (1052) ce are un conținut specific metodei identificate și care cuprinde parametrii de execuție ai metodei conform unui format scris.
12. Sistem conform revendicării 10, **caracterizat prin aceea că** mesajul (105) mai cuprinde și metadate criptografice (1053) ce cuprind o listă de semnături criptografice în care fiecare semnătură este formată dintr-o listă de funcții hash sau funcții hash criptografice și, care sunt calculate înlănțuit una după cealaltă prima folosind ca valoare de intrare antetul (1051) concatenat cu corpul (1052) iar fiecare din următoarele folosind rezultatul funcției hash precedente din listă și în care fiecare funcție hash este identificată printr-un protocol care determină tipul funcției hash folosit și care mai cuprinde și o valoare care este rezultatul funcției hash.
13. Sistem conform revendicării 11, **caracterizat prin aceea că** identificatorul operației din antet (1051) este un identificator de definiție operație și care permite definirea de operații și în care corpul mesajului (1052) conține definiția operației definite ce poate fi cerută de un utilizator (110).
14. Sistem conform revendicării 13, **caracterizat prin aceea că** definiția operației din corpul mesajului (1052) cuprinde și o listă de predicate ce pot fi executate de un utilizator pentru a valida structura și valorile câmpurilor unui mesaj ce cuprinde o cerere de operație conformă cu definiția precizată.

15. Sistem conform revendicării 13, **caracterizat prin aceea că** definiția operației din corpul mesajului (1052) cuprinde o funcție script sau codul binar care este implementarea operației și care poate fi executat de un utilizator pentru verificarea rezultatului operației atunci când un nod execută operația și care permite utilizatorului să verifice că nodurile sistemului au executat ce trebuiau să execute conform operației.
16. Sistem conform revendicării 10, **caracterizat prin aceea că** sunt definite operații de:
    - creare/înregistrare și/sau,
    - acreditare și/sau,
    - repudiere,

    de către un utilizator a unui alt utilizator, medicament, studiu medical sau a altei entități de farmacovigilență.
17. Sistem conform revendicării 16, **caracterizat prin aceea că** sistemul verifică și validează dacă utilizatorul și/sau medicamentul și/sau studiul medical și/sau altă entitate de farmacovigilență din cererea de operație sunt valide și nerepudiate.
18. Sistem conform revendicării 10, **caracterizat prin aceea că** rezultatul unei operații este o tranzacție de raport cu referințe la alte operații înregistrate în jurnalul blockchain (200) și care precizează sursele de informații folosite la sintetizarea rezultatului.

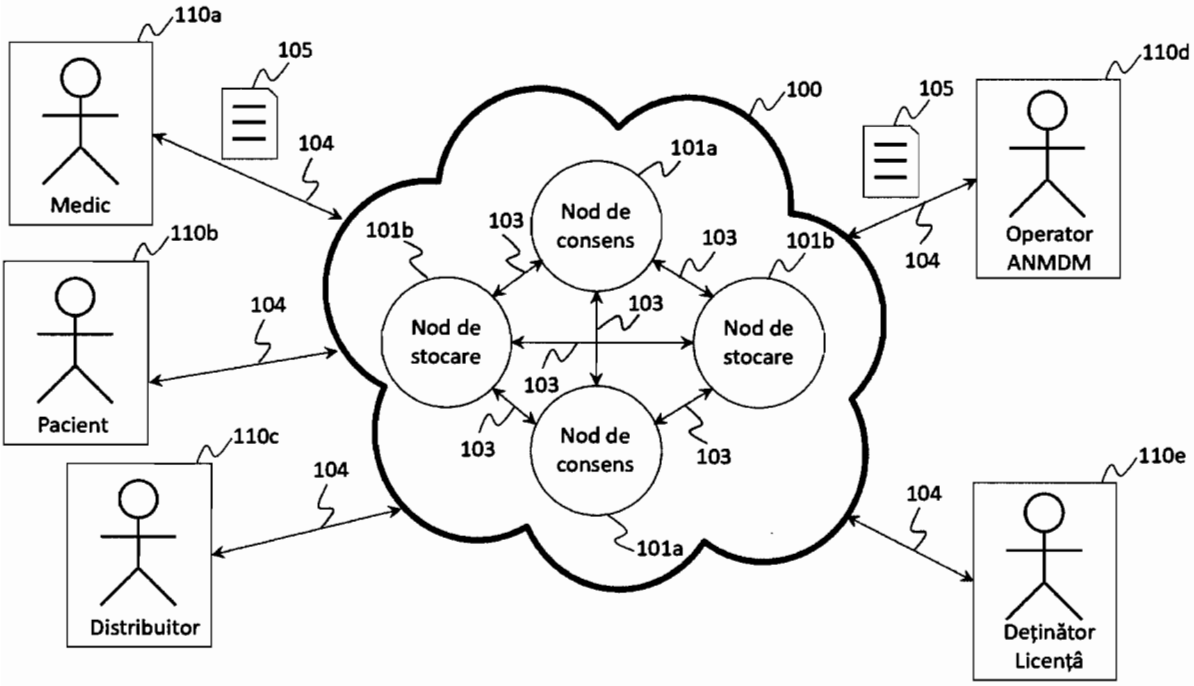

Figura 1:

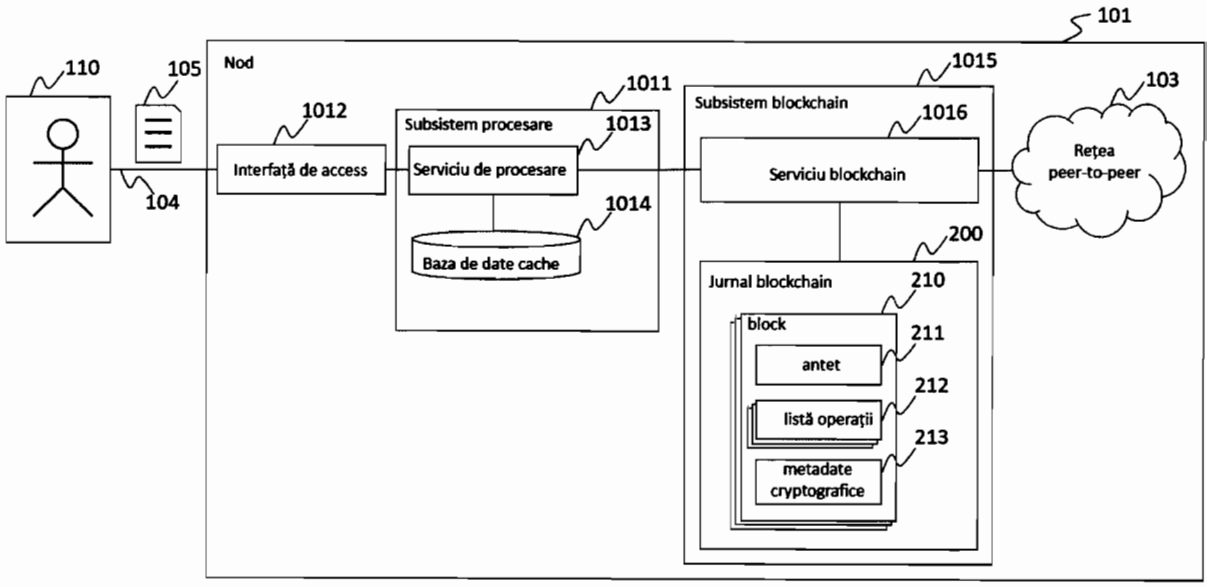

Figura 2: .

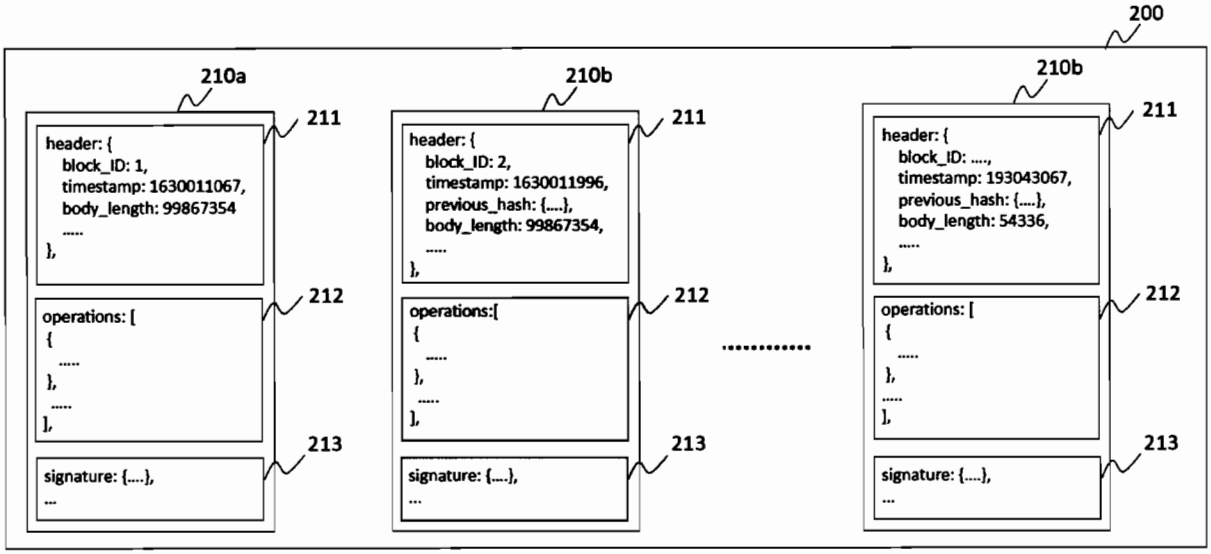

Figura 3:

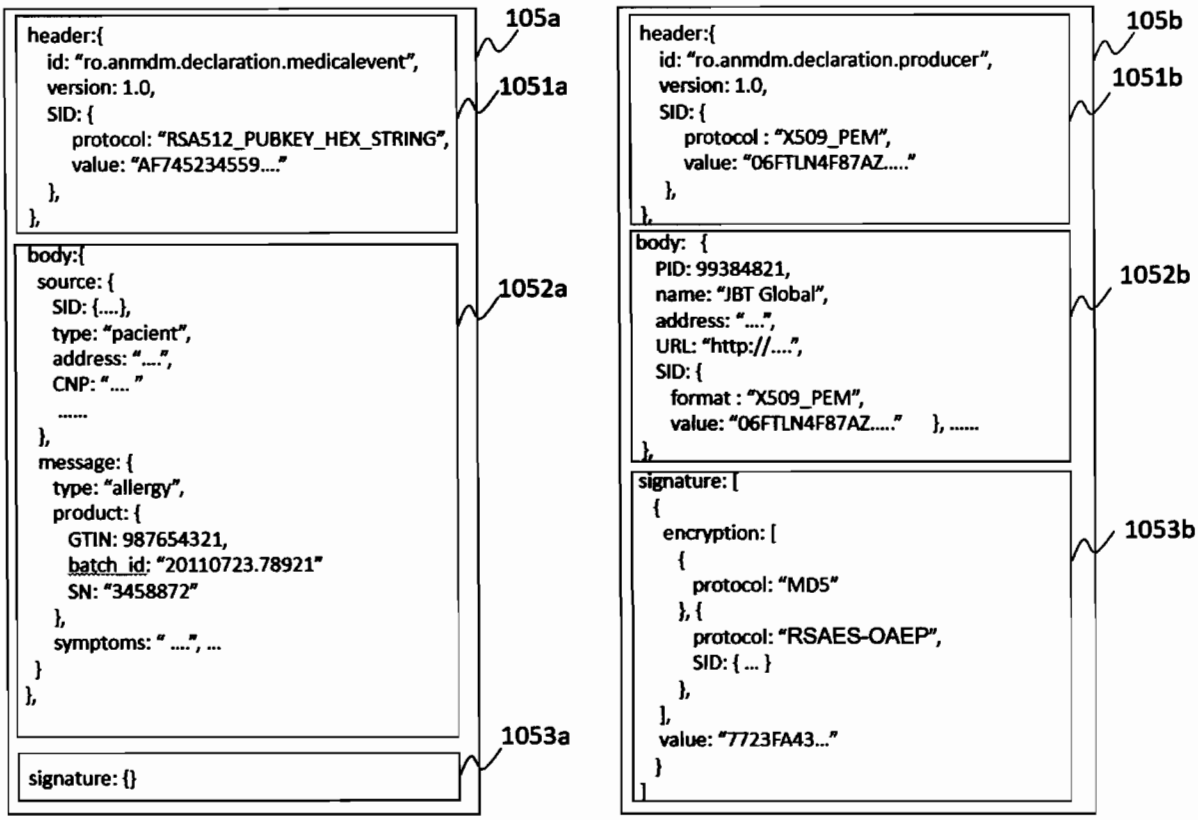

Figura 4:

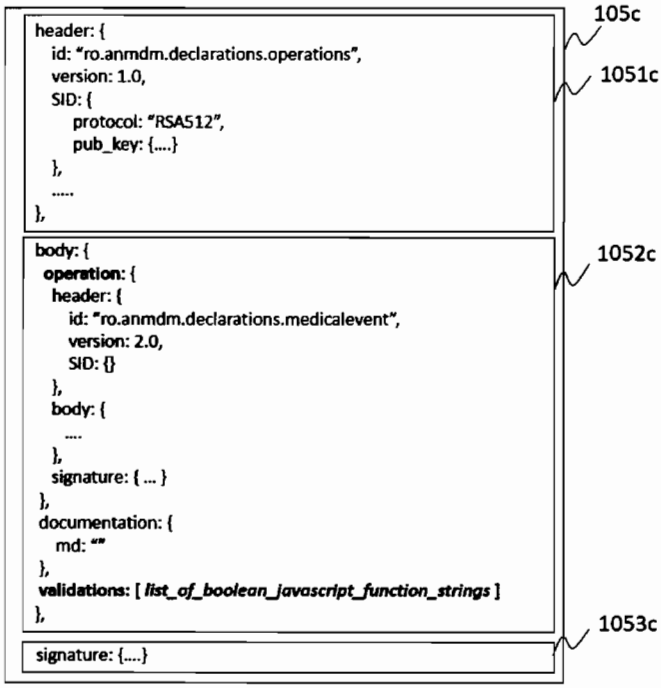

Figura 5: .

```
[
  function () {
      if(operation.header.id != "ro.anmdm.declaration.medicalevent")) {
          return "Error: Unknown event type!";
      }
  },
  function() {
      if(operation.header.SID == null || !(operation.header.SID  instanceof Object))) {
          return "Error: SID must be an object!";
      }
  },
  function() {
      if(operation.header.SID.protocol == null || !["RSA512_PUBKEY_HEX_STRING", "X509_PEM"].includes(operation.header.SID.protocol)) {
          return "Error: Unknown SID protocol! Must be one of [RSA512_PUBKEY_HEX_STRING, X509_PEM]";
      }
  },
  function() {
      if(operation.header.SID.value == null || !SID.protocol[operation.header.SID.protocol].IsValid(operation.header.SID.value)) {
          return "Error: Invalid SID value!";
      }
  }
]
```

Figura 6: .

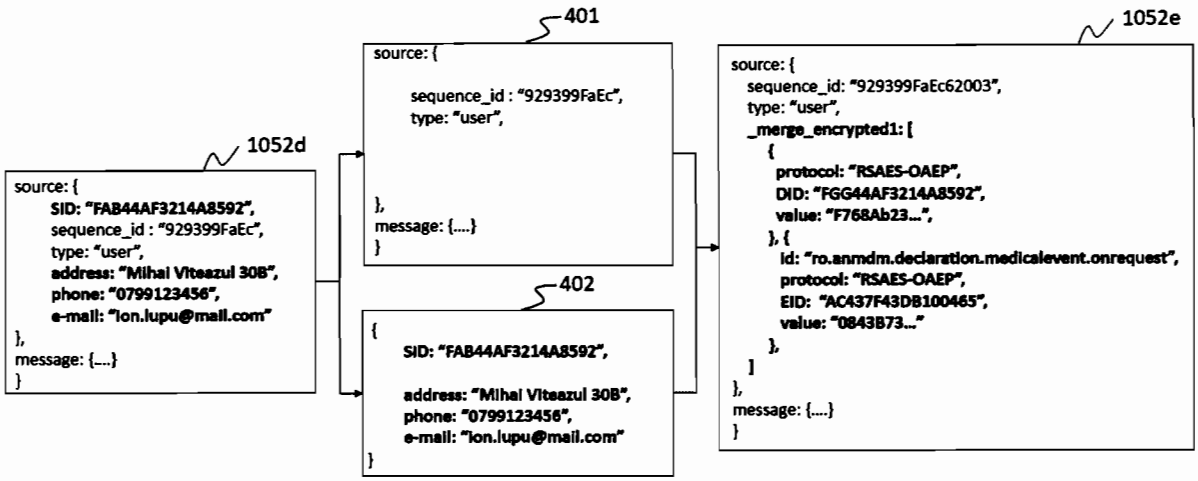

Figura 7: .

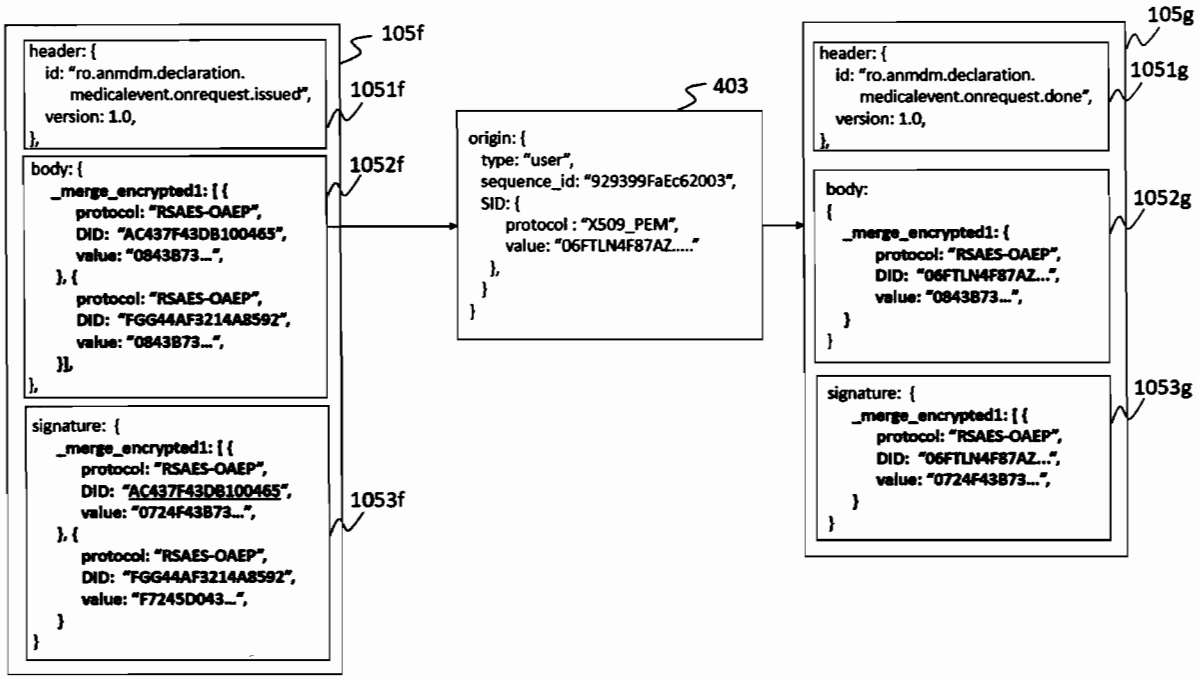

Figura 8: .

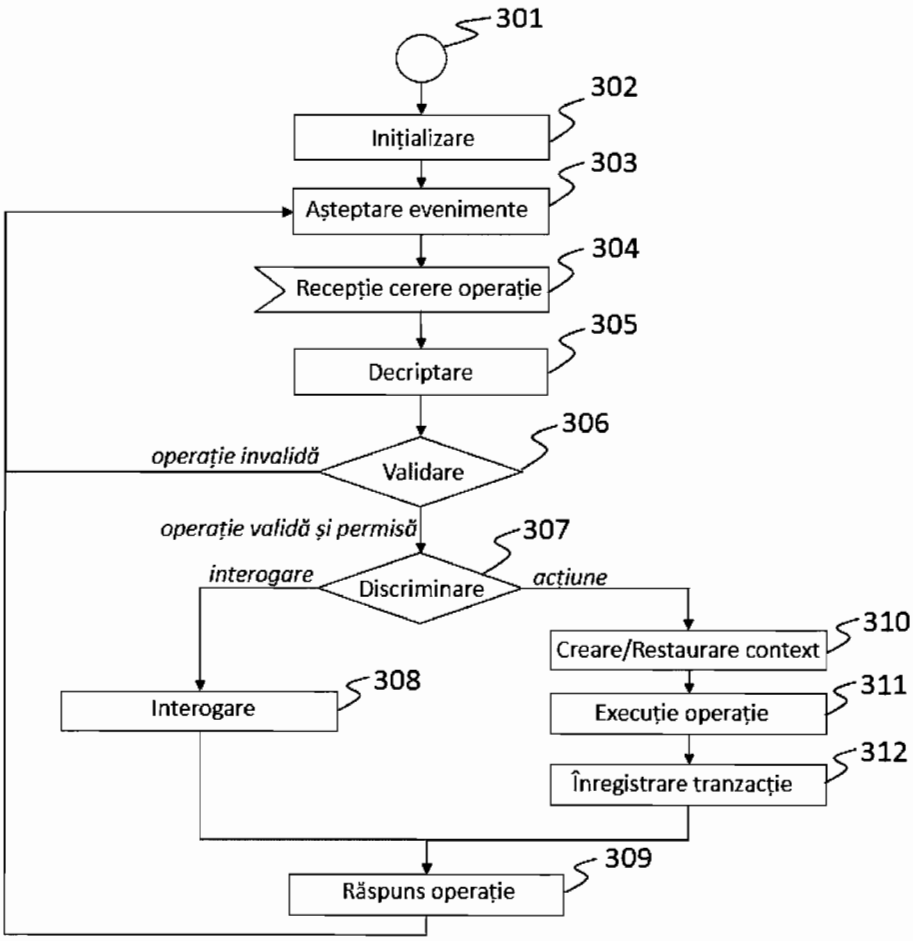
301
302
Inițializare
303
Așteptare evenimente
304
Recepție cerere operație
305
Decriptare
306
operație invalidă
Validare
operație validă și permisă
307
interogare
Discriminare
acțiune
310
Creare/Restaurare context
308
Interogare
311
Execuție operație
312
Înregistrare tranzacție
309
Răspuns operație

Figura 9: .