



Academia de Studii Economice din București

Facultatea de Cibernetică, Statistică și Informatică Economică

Specializarea Informatică Economică

**LUCRARE DE LICENȚĂ**

Conducător ştiințific:

Conf. Univ. Dr. Cristian Valeriu TOMA

Autor:

Marin RUSU

BUCUREȘTI

2019

ACADEMIA DE STUDII ECONOMICE DIN BUCUREŞTI

Facultatea de Cibernetică, Statistică și Informatică Economică

Specializarea Informatică Economică

**Partajarea securizată a înregistrărilor medicale electronice folosind tehnologia blockchain**

Conducător ştiinţific:

Conf. Univ. Dr. Cristian Valeriu TOMA

Autor:

Marin RUSU

BUCUREȘTI

2019

Cuprins

[*1.* *Introducere* 5](#_Toc13167674)

[*2.* *Aplicarea tehnologiei blockchain* 8](#_Toc13167675)

[2.1 Prezentarea generală a mediului actual 8](#_Toc13167676)

[2.2 Stocarea și partajarea datelor EHR folosind tehnologia blockchain 9](#_Toc13167677)

[2.3 Registru imutabil al tranzacțiilor 10](#_Toc13167678)

[2.4 Rețea distribuită 10](#_Toc13167679)

[2.5 Criptarea puternică 11](#_Toc13167680)

[2.6 Tipuri de blockchain 11](#_Toc13167681)

[2.7 EOSIO Blockchain 12](#_Toc13167682)

[2.8 IPFS 13](#_Toc13167683)

[2.9 Aplicații posibile ale tehnologiei blockchain în domeniul asistenței medicale 13](#_Toc13167684)

[2.10 Implementări posibile 15](#_Toc13167685)

[*3.* *Implementarea soluției* 18](#_Toc13167686)

[3.1 Funcționalitățile aplicației 18](#_Toc13167687)

[3.2 Arhitectura sistemului 19](#_Toc13167688)

[3.3 Contractul inteligent 20](#_Toc13167689)

[3.4 Politica de acces 22](#_Toc13167690)

[3.5 Meta-datele înregistrărilor medicale 27](#_Toc13167691)

[3.6 Proiectarea bazelor de date 30](#_Toc13167692)

[3.7 Înregistrarea utilizatorilor 30](#_Toc13167693)

[3.8 Managementul permisiunilor 33](#_Toc13167694)

[3.9 Adăugarea înregistrării medicale 34](#_Toc13167695)

[3.10 Consultarea înregistrărilor medicale 36](#_Toc13167696)

[3.11 Experiența utilizatorului 37](#_Toc13167697)

[3.12 Transparența dosarului medical 38](#_Toc13167698)

[*4.* *Concluzii / Alte considerente* 40](#_Toc13167699)

[4.1 Conformitatea cu cerințele stabilite 40](#_Toc13167700)

[4.2 Limitări și direcții de dezvoltare 40](#_Toc13167701)

[4.3 Alternative pe piață 41](#_Toc13167702)

[4.4 Migrația de la soluția centralizată la cea bazată pe blockchain 41](#_Toc13167703)

[4.5 Alte considerente 42](#_Toc13167704)

[*Bibliografie* 44](#_Toc13167705)

[*Anexă* 46](#_Toc13167706)

[Lista figurilor 46](#_Toc13167707)

# *Introducere*

**Abstract.** *Protecția datelor personale se referă la asigurarea faptului că utilizatorul păstrează controlul asupra accesului la informație, în timp ce accesibilitatea datelor se referă la asigurarea faptului că accesul la informație este nelimitat. Conflictele dintre confidențialitatea și accesibilitatea datelor sunt naturale să apară, iar asistența medicală este un domeniu în care acestea sunt deosebit de relevante. În prezenta lucrare, voi discuta despre modul în care tehnologia blockchain și contractele inteligente (“smart contracts”) ar putea soluționa unele scenarii tipice legate de accesul, gestiunea și interoperabilitatea datelor din domeniul de sănătate. Apoi voi propune implementarea unei arhitecturi informaționale de scară largă pentru accesul la înregistrările electronice medicale, bazată pe contracte inteligente. Principala mea contribuție va consta în încadrarea aspectelor legate de viața privată și accesibilitatea datelor în domeniul asistenței medicale și propunerea unei arhitecturi bazate pe tehnologia blockchain, precum și a unui plan pentru trecerea progresivă de la tehnologia actuală la o soluție de tip blockchain.*

Înregistrările medicale electronice (*“Electronic Health Records” EHR)* sunt informații critice și foarte sensibile folosite pentru diagnostic și tratament, care trebuie distribuite frecvent și partajate între *“actorii”* domeniului asistenței medicale, cum ar fi furnizorii de servicii medicale, companiile de asigurări, farmaciile, cercetătorii, familiile pacienților. Aceasta reprezintă o provocare majoră pentru actualizarea istoricului medical al pacientului. Stocarea și partajarea datelor între entități multiple, menținerea controlului accesului prin numeroasele consimțăminte complică doar procesul de tratament al unui pacient. Un pacient, care suferă de o afecțiune medicală gravă, cum ar fi cancerul sau HIV, trebuie să mențină un istoric lung al procesului de tratament, de reabilitare și de monitorizare ulterioară. Accesul la un istoric complet poate fi crucial pentru tratamentul său.

Un pacient poate vizita mai multe instituții medicale pentru o consultație sau poate fi transferat de la un spital la altul. În conformitate cu legislația [1, 2], pacientul are dreptul asupra informațiilor sale medicale și poate stabili reguli și limite privind cine poate consulta înregistrările sale de sănătate. Dacă un pacient trebuie să-și împărtășească datele clinice în scopuri de cercetare sau să le transfere de la un spital la altul, el poate fi obligat să semneze un consimțământ care specifică ce tip de date vor fi partajate, informațiile despre destinatar și perioada în care datele pot fi accesate de către acesta. Acest lucru poate fi extrem de dificil de realizat, mai ales atunci când un pacient se mută într-un alt oraș, regiune sau țară și poate nu știe în prealabil spitalul unde va primi îngrijire mai târziu.

Chiar dacă consimțământul este furnizat, procesul de transfer al datelor este de durată, mai ales dacă va avea loc prin poștă. Transferul datelor pacientului prin e-mail nu este luat în calcul de către majoritatea spitalelor, deoarece acest lucru ar putea impune riscuri de securitate în timp ce înregistrările sale sunt în tranzit. Ecosistemele actuale pentru schimbul de informații în domeniul sănătății, cum ar fi [***CommonWell Health Alliance***](https://www.commonwellalliance.org/), au ca scop asigurarea faptului că datele din dosarul electronic de sănătate al pacientului sunt partajate în mod sigur, eficient și precis la nivel național SUA. Însă odată ce furnizorii de servicii medicale au acces la informațiile de sănătate ale pacientului, este dificil de garantat că acesta ar putea primi opinii independente de la diferiți furnizori de asistență medicală. În plus, astfel de ecosisteme nu corespund cerințelor de transfer al datelor dintr-o țară în alta.

Agregarea datelor în scopuri de cercetare necesită, de asemenea, consimțământul pacientului, cu excepția cazului în care datele sunt anonimizate. Cu toate acestea, s-a demonstrat că eliberarea independentă de date medicale anonimizate la nivel local, care aparțin aceluiași pacient și care provin din diferite surse (de exemplu, mai multe instituții medicale vizitate de pacient) ar putea determina de-identificarea pacientului și, prin urmare, violarea confidențialității acestuia [3,4].

Bazându-ne pe o autoritate centrală care va stoca și gestiona datele pacienților, precum și politicile de acces asupra lor, vom avea un singur punct de eșec (*„single point of failure”*) și un *„bottleneck”* (un singur component care limitează puternic performanța sau capacitatea întregului sistem) al întregului *framework*. De asemenea, va fi necesară fie efectuarea tuturor operațiunilor (cum ar fi căutarea sau anonimizarea) asupra unor date criptate, fie alegerea unei entități cu adevărat de încredere care va avea acces la informații sensibile despre pacienți. Prima variantă mai necesită și gestionarea unei cantități mare de memorie [5] și nu este potrivită pentru mediul spitalicesc. A doua variantă s-a dovedit a fi foarte dificil de pus în practică. Portofelul *GoogleHealth* [6], care este un exemplu de asemenea autoritate centrală, a arătat că pacienții sunt preocupați de intimitatea lor și sunt conștienți de riscul potențial ca datele lor sensibile să fie utilizate în mod abuziv.

Accesul la un registru comun, imutabil și transparent care va conține un istoric al tuturor acțiunilor care s-au întâmplat cu toți participanții la rețea (cum ar fi modificarea permisiunilor de către pacient, un doctor care accesează sau încarcă noi înregistrări, sau partajarea datelor pentru cercetători) ar putea depăși toate problemele prezentate mai sus. Prin furnizarea unui instrument pentru obținerea unui consens între entitățile distribuite, fără a se baza pe o singură parte de încredere, tehnologia blockchain va garanta securitatea datelor, controlul asupra datelor sensibile și va facilita gestionarea datelor medicale pentru pacient și diferiți actori din domeniul medical. În contextul de asistență medicală putem defini o tranzacție ca un proces de încărcare sau transfer de date medicale între actorii conectați. Un set de tranzacții grupate la un moment dat este adăugat la registrul care înregistrează toate tranzacțiile și, prin urmare, reprezintă starea rețelei.

Interoperabilitatea datelor medicale este o problemă care rămâne deschisă până în prezent. Întrebarea principală sună în felul următor: *Cum să fie asigurat accesul liber la date sensibile (date medicale), păstrând confidențialitatea datelor cu caracter personal și anonimatul, evitând în același timp utilizarea incorectă a acestora?* Tehnologia blockchain și contractele inteligente par să ofere un mod interesant și inovator de a păstra referințele la înregistrările electronice medicale. Folosind această tehnologie, pacienții ar putea controla mai bine propriile date, iar cadrele și instituțiile medicale, cum ar fi spitalele, ar putea avea acces la datele pacienților adăugate de către alte instituții. Tehnologia blockchain oferă o istorie comună, imutabilă și transparentă a tuturor tranzacțiilor pentru a construi aplicații cu încredere, responsabilitate și transparență. Această tehnologie oferă o oportunitate unică de a dezvolta un sistem sigur și credibil de gestionare și partajare a datelor EHR.

Posibilitatea de a utiliza tehnologia blockchain pentru managementul datelor medicale a condus recent la o atenție atât în industrie, cât și în mediul academic [7, 8, 9]. Cu toate acestea, a fost propus un singur prototip funcțional al unui sistem care utilizează tehnologia blockchain pentru gestionarea datelor medicale [7].

Beneficiile cheie ale aplicării tehnologiei blockchain în domeniul asistenței medicale sunt următoarele:

* *Tranzacții verificabile și imutabile*
* *Rezistența la manipularea datelor*
* *Transparența*
* *Integritatea datelor medicale*

Acest lucru se realizează în principal prin utilizarea protocolului de consens și a primitivelor criptografice, cum ar fi ***hashing*** și ***semnătura digitală.***

În această lucrare voi prezenta unele concepte privind gestionarea datelor medicale folosind tehnologia blockchain, care vor sta la baza implementării unui sistem pentru gestiunea și partajarea acestor date, fiind posibilă ulterior integrarea acestuia în practica clinică. Scopul său va fi oferirea accesului securizat la datele pacientului, evitând accesul unei terțe părți la acestea fără permisiune.

Cerințele cheie adresate sistemului vor fi următoarele:

* *Asigurarea confidențialității datelor*
* *Stocarea și partajarea securizată a datelor*
* *Disponibilitatea datelor*
* *Controlul fin asupra drepturilor de acces asupra datelor*
* *Ușurința în folosință a sistemului*

Efectele folosirii acestui sistem vor fi următoarele:

* *Reducerea în mod semnificativ a timpului necesar partajării datelor EHR*
* *Îmbunătățirea luării deciziilor în ceea ce privește îngrijirea medicală, folosind un istoric actualizat, corect și transparent al pacientului*
* *Reducerea costurilor totale folosind noua infrastructură bazată pe tehnologia blockchain*
* *Oferirea unor noi oportunități de business în ceea ce privește stocarea dosarului medical al pacienților*

# *Aplicarea tehnologiei blockchain*

## Prezentarea generală a mediului actual

În paragraful ce urmează voi analiza sistemele de gestionare a înregistrărilor electronice medicale care au fost implementate în SUA până la momentul actual.

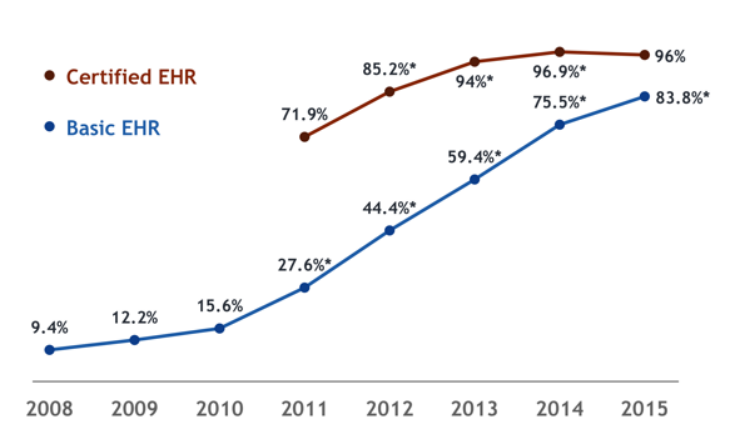


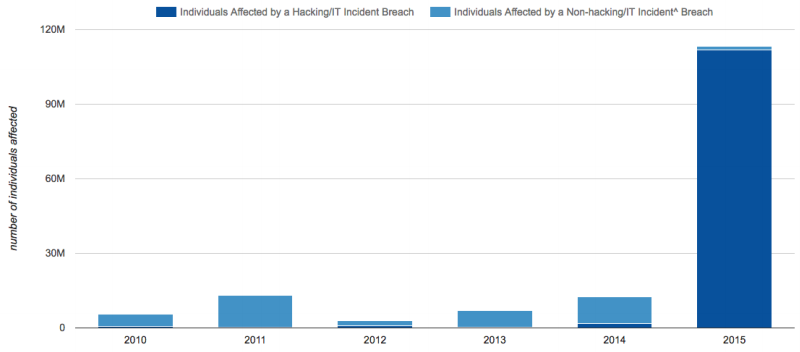
Figura . Adoptarea de înregistrări electronice de sănătate în spitalele federale de îngrijire acută din SUA

În 2008, mai puțin de 10% din înregistrările medicale erau stocate electronic (*Figura 1*) [10]. Înregistrările medicale stocate pe hârtie sunt dificil de mutat sau copiat din locația lor inițială în alte locuri de deservire (de exemplu, spitale) sau direct la pacient. Astăzi, aproape toate înregistrările medicale sunt stocate în registrul electronic de sănătate (*„Electronic Health Record System” EHR*), însă datele rămân în mare parte non-portabile.

Mai mulți factori contribuie la dificultatea furnizării și controlului accesului la datele medicale. Mulți furnizori de asistență medicală interpretează greșit cerințele HIPPA („*Health Insurance Portability and Accountability Act”)* [11], partajând datele numai când acestea sunt absolut necesare. De asemenea, accesul la datele despre sănătate este restricționat pentru pacient și persoanele care pot lua decizii legate de domeniul medical cu acordul pacientului. Unele instituții percep gestionarea acestor date ca fiind un avantaj competitiv. Deținerea înregistrării medicale a pacientului contribuie la „*lipirea”* acestuia de instituția medicală, în timp ce partajarea acesteia permite pacientului să caute îngrijire la o altă instituție. Furnizorii de asistență medicală percep înregistrarea medicală a pacientului ca fiind proprietatea lor decât a pacientului. În timp ce acest lucru este corect din punct de vedere legal, el creează obstacole inutile și uneori costisitoare pentru pacienți care au nevoie sau vor să își mute datele lor medicale într-o altă locație.

Programul responsabil pentru adoptarea rapidă a EHR în ultimii 7 ani necesită ca furnizorii să permită pacienților posibilitatea de a vizualiza, descărca și transmite înregistrările lor în alte locații. Majoritatea furnizorilor partajează cel puțin unele date cu alte sisteme externe [12], indicând progrese limitate în acest domeniu; cu toate acestea, *status quo* este că informațiile rămân, cel mai des, în sistemul care le-a generat. Dificultatea de a muta în siguranță și de a împărtăși datele de sănătate în timp util are un impact negativ asupra îngrijirii pacienților.

În eseul său din 2008 [13], *„The Patient as the Platform”,* Doc Searls relatează un banc personal care descrie tipul de impact pe care îl poate avea partajarea slabă a înregistrărilor medicale asupra tratamentului pacientului. Concluzia lui este că pacienții trebuie să aibă control asupra asistenței lor medicale și aceasta include controlul asupra înregistrărilor medicale. După spusele sale, pacientul trebuie să devină platforma pentru asistența medicală, dar „pentru ca pacienții să devină platforme, avem nevoie de mai multe instrumente și capabilități care sunt native pentru pacient”. Searls merge dincolo de a afirma că datele electronice de sănătate ar trebui să fie ușor de partajat; el pledează pentru a face pacienții custozi ai propriilor date de asistență medicală, astfel încât aceștia pot controla definitiv unde și cum pot fi folosite acestea.

Odată cu adoptarea înregistrărilor electronice de sănătate, faptul că nu se execută promisiunea de a partaja datele de sănătate nu este unica problemă cu care se confruntă sistemele EHR. Adoptarea mai largă a fișelor medicale electronice a activat nivele de breșe în securitate mai înainte necunoscute (*Figura 2*). Majoritatea pacienților sunt îngrijorați referitor la confidențialitatea și securitatea dosarelor medicale, unii pacienți reținând informații de la furnizorul lor de servicii medicale din cauza acestor preocupări.

*Figura 2.* *Numărul de persoane afectate de breșele de securitate în sistemele EHR din SUA [14]*

Adoptarea pe scară largă a înregistrărilor electronice de sănătate trebuie să fie o soluție sigură, eficientă și de încredere la problema incapacității de a partaja date între furnizori, pacienți și cercetători. Cu toate acestea, silozurile de informații sunt aproape la fel de impenetrabile ca și în cazul în care erau în zilele înregistrărilor pe hârtie, cu riscul suplimentar de breșe de securitate care au loc frecvent și cu un impact foarte puternic.

## Stocarea și partajarea datelor EHR folosind tehnologia blockchain

O posibilă soluție pentru aceste (și multe alte) probleme este implementarea unui sistem controlat de pacient pentru stocarea și partajarea datelor EHR bazat pe tehnologia blockchain. Pentru a înțelege cum tehnologia blockchain poate îmbunătăți securitatea și eficiența stocării și partajării datelor medicale, este mai întâi necesar să se ofere o imagine de ansamblu asupra tehnologiei blockchain și beneficiilor sale.

Blockchain este o tehnologie de tip *peer-to-peer*  ce conține un registru (*„ledger”)* distribuit care a fost inițial utilizată în industria financiară. Ea se bazează pe 3 principii fundamentale. În primul rând, datele sunt stocate într-un registru de tranzacții care e public și imutabil, oricine putând să îl citească. Din cauza că tranzacțiile nu pot fi niciodată șterse sau modificate, există întotdeauna o înregistrare completă și incontestabilă a tuturor tranzacțiilor. În al doilea rând, blockchain-urile sunt implementate prin intermediul unei rețele descentralizate de noduri cu putere de calcul, ceea ce le face robuste împotriva erorilor și atacurilor. Descentralizarea înseamnă, de asemenea, că nici o entitate nu deține sau controlează blockchain-ul. În al treilea rând, metadatele care descriu fiecare tranzacție sunt disponibile pentru toți cei din sistem, dar asta nu înseamnă că datele stocate în blockchain sunt ușor de citit. Blockchain-ul se bazează pe pseudoanonimitatea (înlocuirea numelor cu identificatori) și infrastructura cheilor publice (PKI), care permite ca conținutul blockchain-ului să fie criptat într-un mod care este prohibitiv costisitor de a fi spart. Atunci când tehnologia blockchain se folosește pentru stocarea și partajarea metadatelor medicale, fiecare dintre aceste trei principii se aplică.

## Registru imutabil al tranzacțiilor

Blockchain a fost inițial conceput ca o componentă a infrastructurii pentru crypto monede (*„cryptocurrency”),* cum ar fi **Bitcoin**. Tranzacțiile din blockchain-ul Bitcoin reprezintă tranzacții financiare: transferul de sume specifice de bitcoins de la un cont la altul. Oricine poate verifica cărui cont îi aparține unui anumit bitcoin utilizând instrumente software adecvate pentru a examina tranzacțiile în blockchain-ul public. În contextul asistenței medicale, tranzacțiile ar consta în documentarea unor episoade specifice din serviciile de asistență medicală furnizate pacientului. Furnizorii de servicii medicale și pacienții ar contribui cu date și o politică de acces asupra acestora, care vor fi atașate la un ID al pacientului. Aceste date vor putea revendica istoria și lacunele în îngrijirea pacienților. Deoarece registrul este imutabil, nimeni nu poate șterge sau modifica înregistrarea. Actualizările vor include metadate cu referire la data, ora, hash-ul înregistrării medicale, precum și entitatea care a adăugat-o. În acest mod, pe baza sistemului EHR implementat pe baza tehnologiei blockchain se va putea face audit în orice moment de timp asupra tuturor acțiunilor întreprinse de către participanți.

## Rețea distribuită

Serviciile financiare, juridice, de sănătate și alte tipuri de tranzacții au anumite cerințe comune. Este necesar să se stabilească identitatea părților implicate în tranzacție, să se mențină încrederea, să se garanteze că tranzacțiile sunt înregistrate în mod corespunzător și nu pot fi modificate și că infrastructura în care se desfășoară tranzacțiile este stabilă. Înainte de a apărea tehnologia blockchain, singura modalitate de a atinge aceste obiective a fost crearea unei autorități centrale puternice pentru a furniza aceste servicii, de exemplu bănci, guverne și case de compensare. În domeniul dosarelor medicale, fiecare spital sau sistemul de sănătate servește ca autoritate centrală pentru a furniza servicii de evidență și transmitere a datelor.

Infrastructura tradițională centralizată a tranzacțiilor pare a fi o soluție naturală a problemei. Deși are multe avantaje, există și dezavantaje. O infrastructură centralizată este vulnerabilă la erori, corupție și atacuri. Această arhitectură provoacă silozurile informaționale care sunt predominante în domeniul asistenței medicale de astăzi. Tehnologia blockchain înlocuiește infrastructura centralizată cu una *distribuită*. Software-ul acestei tehnologii rulează pe mii de noduri distribuite într-o întreagă rețea. Pentru a procesa o tranzacție, aceasta este distribuită tuturor nodurilor din rețea, iar tranzacția este rezolvată atunci când nodurile au ajuns la un consens pentru a accepta noua tranzacție în registrul comun. Procesul este sofisticat din punct de vedere tehnologic, însă înlocuiește întreaga instituție de păstrare a înregistrărilor și de procesare a tranzacțiilor. Aceasta reduce costurile generale ale tranzacțiilor în ceea ce privește prețul și timpul de execuție. De asemenea, aceasta înseamnă că nu există un singur punct de eșec, oferind o infrastructură mai robustă și mai sigură.

## Criptarea puternică

Criptografia cu chei publice este un sistem de criptare care utilizează 2 perechi de chei: o cheie „*publică*” disponibilă tuturor și o cheie „*privată*” cunoscută numai titularului acesteia. Fiecare cheie poate fi utilizată pentru a cripta un mesaj, dar cealaltă cheie trebuie să decripteze mesajul. Practic vorbind, există 2 cazuri de utilizare care implică chei publice și private. Mai întâi, un expeditor poate codifica un mesaj cu o cheie publică și să se asigure că numai deținătorul cheii private îl poate decripta. În al doilea rând, un mesaj sau un document poate fi criptat cu o cheie privată. Dacă mesajul are sens atunci când e decriptat utilizând cheia publică corespunzătoare, este garantat că titularul cheii private este partea care a criptat mesajul. Aceasta este uneori numită „*semnarea*” unui mesaj (mai exact, hash-ul, ci nu întreg mesajul, este semnat cu cheia privată), deoarece este analog celui care își pune semnătura unică pe un document.

Blockchain suportă, de asemenea, un concept numit „*M-of-N”* semnături sau „*multisig”,* ceea ce înseamnă că există un total de chei criptografice N și cel puțin M dintre ele trebuie să fie prezente pentru a decripta datele. În acest fel, pacientul poate furniza cheile îngrijitorilor autorizați, medicilor și altora pentru a acorda acces fără cheia specifică a pacientului [15]. De exemplu, acest lucru este util atunci când pacientul este inconștient sau incapabil și nu poate oferi consimțământul de a accesa datele sale.

Criptografia cu cheie publică este un concept important pentru tehnologia blockchain. Toate tranzacțiile sunt semnate cu chei private ca modalitate de stabilire a identităților participanților.

## Tipuri de blockchain

Pe baza modului în care este definită identitatea unui utilizator în rețea, se pot distinge 2 tipuri de sisteme blockchain: cu permisiuni (*„permissioned”*) și fără permisiuni (*„permissionless”*). Un sistem de tip permissionless este unul în care identitatea participanților este fie pseudonimă, fie chiar anonimă și fiecare utilizator poate adăuga un nou bloc în registru sau să participe la validarea rețelei [16]. În esență, oricine este liber să devină un nod și oricine (teoretic) poate deveni un miner care să deservească rețeaua în căutarea unei recompense. Pe măsură ce oricine poate participa la validarea blockchain-ului, acest tip de blockchain este rezistent la cenzură, deoarece nodurile de validare sunt descentralizate și, prin urmare, depășesc controlul oricărei entități. Cu cât numărul de noduri este mai mare, cu atât rezistența blockchain-ului e mai mare. În schimb, în cazul unui sistem de tip *permissioned*, identitatea unui utilizator este controlată de un furnizor de identitate.

Furnizorul de identitate este încredințat în menținerea controlului accesului la rețea și drepturile utilizatorului de a participa la consens sau de a valida un nou bloc. Acest blockchain restricționează părțile care pot participa la obținerea consensului sau validării lanțului. Prin urmare, într-un blockchain de tip *permissioned* (privat), numai un grup de utilizatori restricționat și preselectat are dreptul de a valida tranzacțiile incluse în blocuri. Un avantaj major al acestui tip este că el poate fi securizat fără o activitate minieră costisitoare și consumatoare de energie, ca dovadă a muncii (*„Proof of Work”*), deoarece capitalul *„Proof of Stake”* poate fi atribuit pur și simplu acelor actori cunoscuți și de încredere care sunt aprobați pentru a valida tranzacțiile rețelei. Modelele de consens de tip *„Proof of Stake”* se scalează cu mult mai ușor, deoarece nu necesită cicluri computaționale tot mai mari (*hashpower)*, facilitând mai multe tranzacții pe secundă și ajungând la un consens mai rapid decât modelele miniere actuale. Multe blockchain-uri private ale corporațiilor și instituțiilor financiare urmează acest model.

## EOSIO Blockchain

EOSIO este un software care introduce o arhitectură de blockchain concepută pentru a permite scalarea verticală și orizontală a aplicațiilor descentralizate [18]. Acest lucru se realizează printr-o construcție asemănătoare sistemului de operare pe care pot fi construite aplicații. Software-ul oferă conturi, autentificare, baze de date, comunicare asincronă și programarea aplicațiilor pe mai multe nuclee și/sau grupuri de CPU-uri. Tehnologia rezultată este o arhitectură de blockchain care are potențialul de a scala la milioane de tranzacții pe secundă, elimină taxele de utilizare și permite implementarea rapidă și ușoară a aplicațiilor descentralizate, în contextul unui blockchain guvernat. Software-ul EOSIO poate fi folosit pentru a crea atât blockchain-uri private, cât și publice. Rămâne la discreția părților care lansează blockchain-ul pentru a determina permisiunile și regulile de participare la rețea.

Software-ul EOS.IO utilizează singurul cunoscut algoritm de consens decentralizat, dovedit a fi capabil să îndeplinească cerințele de performanță ale aplicațiilor, ***Delegated Proof of Stake (DPOS)***. În cadrul acestui algoritm, cei care dețin tokenuri pe un blockchain care adoptă software-ul EOSIO pot selecta producătorii de blocuri printr-un sistem de votare cu aprobare continuă. Oricine poate alege să participe la producția de blocuri și va avea ocazia să producă blocuri, cu condiția să-i convingă pe deținătorii de tokenuri să voteze pentru ei.

Toleranța bizantină la erori (*Byzantine Fault Tolerance)* este adăugată la algoritmul DPOS, permițând tuturor producătorilor să semneze toate blocurile atâta timp cât niciun producător nu semnează două blocuri cu același *timestamp* sau aceeași înălțime a blocului. Odată ce 15 producători din 21 total au semnat un bloc, acesta este considerat ireversibil. Orice producător bizantin ar fi trebuit să genereze dovezi criptografice ale trădării lor prin semnarea a două blocuri cu același *timestamp* sau cu același vârf. Conform acestui model, un consens ireversibil ar trebui să fie atins în decurs de o secundă.

Aceste proprietăți sunt extrem de utile pentru a implementa viitorul sistem EHR. În primul rând, aprobarea unei tranzacții va avea loc foarte rapid, ceea ce este crucial în domeniul medical, permițând personalului medical să acceseze instant dosarul medical și să se concentreze asupra lecuirii pacientului, în același timp îmbunătățind experiența utilizatorilor sistemului. În al doilea rând, aceasta va stimula instituțiile medicale care vor rula nodurile de blockchain să ofere servicii tehnice cât mai calitative pentru ca ulterior să fie votate ca producători de blocuri de către pacienți. Ele vor fi motivate de interesul economic, deoarece fiecare producător de blocuri este remunerat de către sistem cu un comision pentru fiecare tranzacție procesată și aprobată.

## IPFS

Implementarea sistemului de fișiere distribuit care urmează a fi folosită este cea pusă la dispoziție de către IPFS. Sistemul de fișiere interplanetar (*The InterPlanetary File System IPFS)* este un sistem de fișiere distribuit *peer-to-peer* care caută să conecteze toate dispozitivele de calcul cu același sistem de fișiere [19]. În unele moduri, IPFS este similar cu Web-ul, dar IPFS ar putea fi văzut ca un singur *roi* BitTorrent, schimbând obiecte într-un depozit Git. Cu alte cuvinte, IPFS furnizează un model de stocare bazat pe blocuri care sunt adresate în funcție de conținutul acestora cu o capacitate de transfer foarte înaltă, cu legături hypertext adresate în funcție de conținut. Aceasta formează un arbore hash generalizat (*Merkle DAG*), o structură de date pe care se pot construi sisteme de fișiere care oferă suport pentru versionare, tehnologii blockchain, sau chiar un Web Permanent. IPFS combină o tabelă de dispersie distribuită, un schimb de blocuri stimulat și un spațiu de nume auto-certificat. IPFS nu are un singur punct de eșec și toate nodurile nu trebuie să aibă încredere reciproc.

Toate aceste proprietăți ale sistemului IPFS sunt foarte utile în contextul implementării unui sistem EHR bazat pe tehnologia blockchain din următoarele considerente:

* Stocând doar *hash-ul* înregistrării medicale în blockchain, se va economisi spațiul de memorie ocupat de *state-ul* contractului inteligent
* *Hash-ul* ne dă garanția următoare: în caz că conținutul înregistrării a fost modificat intenționat de către un răufăcător, putem depista cu ușurință acest lucru
* Replicarea înregistrărilor doar pe unele noduri, și anume celor care vor utiliza cel mai frecvent o înregistrare specifică, va reduce spațiul de stocare per ansamblu, păstrând totuși proprietatea ca înregistrarea să poată fi regăsită de la mai multe noduri

Neavând un singur punct de eșec, acest sistem corespunde cerințelor formulate inițial față de sistemul EHR, și anume de a fi accesibil și tolerant la erori.

## Aplicații posibile ale tehnologiei blockchain în domeniul asistenței medicale

În această secțiune, voi propune 3 scenarii: îngrijirea primară a pacienților, cercetarea medicală și sănătatea conexă.

**Scenariul 1. Îngrijirea primară a pacienților.** Utilizarea tehnologiei blockchain pentru îngrijirea primară a pacienților poate contribui la rezolvarea următoarelor probleme ale sistemelor actuale de asistență medicală:

* Un pacient vizitează frecvent mai multe spitale deconectate. El trebuie să păstreze un istoric al tuturor datelor medicale și să mențină actualizările. Acest lucru duce la situația în care este posibil ca informațiile solicitate să nu fie disponibile
* Datorită indisponibilității datelor, este posibil ca pacientul să fie nevoit să repete câteva teste pentru rezultate de laborator. Acest lucru este obișnuit când rezultatele sunt stocate într-un alt spital și nu pot fi accesate imediat.
* Datele privind asistența medicală sunt sensibile, iar gestionarea lor este greoaie. Cu toate acestea, în practica clinică nu există niciun sistem care ia în calcul viața privată, care să permită pacienților să mențină politica de control a accesului într-o manieră eficientă.
* Schimbul de date între diferiți furnizori de asistență medicală poate necesita eforturi majore și poate dura mult timp

În continuare, propun două abordări care pot fi implementate separat sau combinate pentru îmbunătățirea îngrijirii pacienților.

* *Abordarea bazată pe instituții:* Rețeaua va fi formată de către părți de încredere: instituțiile de îngrijire medicală sau medici generaliști (îngrijitori). Părțile vor rula protocolul de consens și vor menține registrul distribuit. Pacientul (sau rudele acestuia) va putea accesa și gestiona permisiunile și înregistrările medicale printr-o aplicație de la orice nod unde acestea sunt stocate. Dosarul medical existent va putea fi accesat de la nodurile unde acesta este replicat. Dacă un nod este offline, pacientul va putea accesa aceste date prin orice alt nod online. Procesul de gestionare a cheilor și politicii de control al accesului vor fi codificate în „*chaincode”,* asigurând astfel securitatea datelor și confidențialitatea pacientului.
* *Caz specific (condiții medicale grave, examinare, îngrijire vârstnică):* În timpul spitalizării pacientului pentru tratament, reabilitare, examinare sau intervenție chirurgicală, ar putea fi creat un registru specific cazului. Rețeaua va conecta medici, asistente medicale și familia pentru a obține un tratament eficient și transparent. Acest lucru va ajuta la eliminarea greșelilor făcute de om, pentru a asigura un consens în cazul unei dezbateri despre anumite etape ale tratamentului.

**Scenariul 2. Agregarea datelor pentru scopuri de cercetare.** Este foarte important să se asigure că sursele datelor sunt instituții medicale de încredere și, prin urmare, datele sunt autentice. Folosirea unui registru distribuit va asigura trasabilitatea și va garanta confidențialitatea pacienților, precum și transparența procesului de agregare a datelor. Datorită lipsei actuale a mecanismelor adecvate, pacienții nu sunt adesea dispuși să participe la schimbul de date. Folosind tehnologia blockchain în cadrul unei rețele de cercetători, bio-bănci și instituții de asistență medicală se va facilita procesul de colectare a datelor pacienților în scopuri de cercetare.

**Scenariul 3. Conectarea diferiților „jucători” de asistență medicală pentru o mai bună îngrijire a pacienților.** Sănătatea conectată este un model socio-tehnic pentru gestionarea și furnizarea asistenței medicale, prin utilizarea tehnologiei pentru furnizarea serviciilor de asistență medicală de la distanță [17]. Împărțirea registrului (folosind abordarea bazată pe permisiuni) între entități (cum ar fi companiile de asigurări și farmacii) va facilita administrarea medicamentelor și a costurilor pentru un pacient, în special în cazul gestionării bolilor cronice. Furnizarea pentru farmacii a datelor despre prescripții, actualizate cu exactitate, va îmbunătăți logistica. Accesul la un registru comun ar permite transparența în întregul proces al tratamentului, de la monitorizarea dacă pacientul urmează corect tratamentul prescris, pentru a facilita comunicarea cu societatea de asigurări cu privire la costurile tratamentului și medicamentelor.

**Implementarea scenariilor.** Pentru a implementa cele trei scenarii de asistență medicală prezentate mai sus, trebuie să alegem între cele două tipuri de blockchain-uri. Mai jos, voi prezenta argumentele în favoarea folosirii blockchain-ului cu permisiuni („*permissioned*”).

1. Anonimitatea utilizatorilor și imposibilitatea de a verifica identitatea deținătorilor de conturi (ca în cazul blockchain-urilor fără permisiuni) ar putea cauza impersonalizarea și utilizarea necorespunzătoare a datelor.
2. Datele privind sănătatea pacienților sunt de natură foarte sensibilă. Chiar monitorizarea comunicării între un pacient și un anumit clinician poate dezvălui anumite date sensibile despre pacient, încălcând astfel viața privată.
3. Este necesar un răspuns rapid al unui sistem, deoarece orice actualizare a informațiilor despre tratamentul unui pacient ar putea fi crucială pentru pacient.
4. Necesitatea de a plăti pentru executarea tranzacțiilor, de exemplu, actualizarea permisiunilor unui medic pentru a accesa o informație despre sănătate sau pentru a împărtăși unele date pentru cercetare ar putea limita gradul de utilizare al sistemului.

## Implementări posibile

Pentru a implementa un sistem de înregistrări medicale bazate pe tehnologia blockchain, EHR-urile și alte sisteme de evidență ar cripta și trimite o tranzacție care conține documentele de îngrijire a pacientului – note de întâlnire, rețete, istorii familiale etc. – folosindu-se 4 moduri posibile de stocare ale acestor date. Tranzacția ar include o semnătură digitală de la contribuitor pentru a identifica proveniența și contul pacientului din blockchain ca destinatar ar tranzacției.

Primul tip de stocare ar fi stocarea directă în blockchain-ul medical public. Avantajele acestuia ar fi faptul că datele vor putea fi accesibile din orice nod al rețelei, însă ca neajuns ar fi faptul că fiecare instituție care va rula un nod va avea nevoie de un spațiu de stocare foarte mare pentru a putea stoca local datele tuturor pacienților, acestea făcând parte din „*state-ul”* blockchain-ului. Mai mult, în implementarea tehnologiei blockchain care urmează a fi folosită, și anume ***EOSIO*** fiecare octet de memorie ocupat în RAM trebuie plătit de către contul care îl folosește, iar aceasta ar putea servi drept o piedică pentru adopția implementării folosind tehnologia blockchain de către pacienți.

Al doilea tip de stocare ar fi unul de tip hibrid, adică stocarea datelor are loc „*offchain”* în următoarele baze de date: în primul rând o bază de date locală în care fiecare spital va salva local datele generate de el, iar în al doilea rând o platformă în „*cloud*” care va stoca datele pacientului organizate în funcție de categoria datelor (spre exemplu, în funcție de nivelul de senzitivitate al datelor, sau semantica lor) și criptate cu cheia simetrică AES a pacientului. Un medic înregistrat în sistem ar putea accesa sau încărca datele în „*cloud repository*” în funcție de politica de control definită de pacient care e implementară în logica din „*chaincode*” și stocată ca state al contractului inteligent al fiecărui nod. Avantajele acestui tip sunt următoarele: în primul rând se reduce volumul de date stocat local stocat în fiecare nod al blockchain-ului până la stocarea chaincodului, permisiunilor și metadatelor despre înregistrări, iar în bazele de date locale se vor stoca ca „*back-up”* doar datele generate de către acel spital, iar în al doilea rând se reduce încărcarea sistemului („*system load*”) prin stocarea datelor efective off-chain. Neajunsurile sale sunt următoarele: arhitectura sistemului care va urma a fi implementat va fi una foarte complexă și există un risc foarte mare ca unele lacune în securitate să nu poată fi observate, punând în pericol securitatea datelor pacienților. De asemenea în caz că cloud repository și baza de date locală cad, datele acelui pacient rămân indisponibile, ceea ce ar putea crea erori în menținerea unui dosar electronic medical complet și ar putea face mai grea punerea unui diagnostic pacientului.

Al treilea tip de stocare ar putea fi ales de către pacient și s-ar afla în afara sistemului. Pacientul va putea stoca dosarul medical criptat cu cheia sa simetrică local (pe laptop, telefon, tabletă etc.), într-o bază de date sau în cloud la un furnizor ales de către pacient, iar partajarea va avea loc printr-o zonă de buffer din contractul inteligent din blockchain, în care înregistrările se vor afla un timp limitat, mai bine spus, atât timp cât durează permisiunea de adăugare sau citire. Avantajele acestui tip sunt următoarele: în primul rând, datele vor fi stocate off-chain, ceea ce va reduce încărcarea sistemului; în al doilea rând, nu va mai fi nevoie de baze de date pentru stocarea centralizată a datelor sau stocarea lor locală în nodurile care rulează blockchain software; în al treilea rând, dat fiind faptul că pacientul poate alege unde vor fi stocate datele sale, apar noi oportunități de business pentru furnizorii de servicii de stocare a datelor în cloud; în al patrulea rând arhitectura sistemului va fi destul de simplă, ceea ce va permite observarea majorităților breșelor de securitate care pot apărea. Neajunsurile sunt următoarele: cu toate ca datele se stochează off-chain, din cauza că se află în afara sistemului, e necesară o zonă de buffer în contractul inteligent, dimensiunea spațiului căreia va trebui să o aibă local orice nod din blockchain. De asemenea odată ce datele se stochează în afara sistemului este posibil ca pacientul să își piardă dosarul medical. Acesta totuși va putea fi restabilit, în cazul în care furnizorii de asistență medicală vor păstra o copie a înregistrărilor partajate de către pacient. Acest mod de stocare poate afecta *user experience* al pacientului, deoarece în acest caz sistemul de permisiuni nu va mai putea automatiza în întregime procesul de partajare și stocare a înregistrărilor, la fiecare adăugare sau citire fiind nevoie de consimțământul pacientului și de preluarea sau stocarea manuală a înregistrărilor în zona de buffer a contractului inteligent.

Al patrulea tip de stocare este folosirea unui sistem de fișiere distribuit și stocarea efectivă a datelor *off chain* în cadrul acestuia, iar metadatele despre înregistrare (cel mai important câmp fiind hash-ul înregistrării), politica de acces definită de pacient și cheile publice ale participanților să fie stocate în blockchain ca *state* al contractului inteligent. Avantajele acestui tip sunt următoarele: datele se vor stoca *off chain,* ceea ce va reduce încărcarea sistemului; folosirea unui sistem de fișiere distribuit va conduce la faptul că datele vor putea fi disponibile din mai multe noduri; sistemul de permisiuni va putea automatiza procesul de stocare și partajare a înregistrărilor medicale; arhitectura sistemului rezultat nu va fi foarte complicată, ceea ce va permite observarea majorităților breșelor de securitate care pot apărea. Neajunsurile sunt următoarele: nodurile sistemului de fișiere vor trebui să fie rulate de către fiecare spital, companie de asigurări și alți participanți ai sistemului, aceștia trebuind să ofere un spațiu de stocare semnificativ. Mai mult, din cauza politicii de stocare a fișierelor, după o perioadă prestabilită, aceste se vor șterge de către nod. Aceasta implică faptul ca participanții vor trebui să ofere un timp de stocare cât mai mare. Problema poate fi soluționată din punct de vedere economic cu ajutorul unui sistem de recompensă pentru acei participanți care vor pune la dispoziție un spațiu și timp de stocare mai mare. Această recompensă va fi de forma unei cryptomonede a sistemului care va avea o contravaloare în valutele non crypto.

Luând în calcul ca în sistemul proiectat accentul se va pune pe securitate, accesibilitate și o experiență a utilizatorului cât mai înaltă pentru a spori gradul de adopție, al patrulea tip de stocare este cea mai optimă alegere. Indiferent de modul de stocare ales, pacienții și medicii ar folosi o aplicație web sau mobilă pentru a vedea conținutul dosarului medical, pacienții fiind în stare să acorde și drepturi de acces la dosarul lor.

Acest tip de sistem are o serie de avantaje față de metodele actuale de păstrare a evidenței dosarelor medicale:

* Pacienții devin platforma, deținând și controlând accesul la datele lor de sănătate. Acest lucru elimină toate obstacolele în calea pacienților care achiziționează copii ale dosarelor lor de sănătate sau le transferă altui furnizor de asistență medicală
* Deoarece datele sunt stocate într-un sistem de fișiere distribuit, nu există o singură instituție care poate fi jefuită sau spartă pentru a obține un număr mare de înregistrări ale pacienților
* Datele sunt criptate și pot fi decriptate numai cu cheia privată a pacientului. Chiar dacă rețeaua este infiltrată de un nod rău intenționat, nu există o modalitate practică de citire a datelor acestuia
* Infrastructura însăși oferă capabilități de audit și non-repudiere. Metodele folosite de adăugare a datelor și a metadatelor includ, de asemenea, contul pacientului, marcaje de timp și hash-ul înregistrării pentru a determina dacă conținutul acesteia nu a fost modificat.

Metoda bazată pe blockchain pentru stocarea și partajarea înregistrărilor medicale include toate criteriile așteptate de la un sistem de păstrare și partajare a înregistrărilor medicale și depășește ceea ce poate face un sistem centralizat tradițional, deoarece îmbunătățește accesul pacienților la evidențele lor și întărește securitatea împotriva atacurilor asupra datelor senzitive.

# *Implementarea soluției*

## Funcționalitățile aplicației

Aplicația avută în vedere în lucrarea de față, denumită *EOS Medical*, are obiectivul de a oferi pacienților o platformă pentru stocarea dosarului medical împreună cu toate modificările făcute asupra acestuia, precum și partajarea lui cu personalul medical, iar medicilor un suport pentru consultarea dosarului pacientului, pentru monitorizarea stării de sănătate a acestuia și punerea unui diagnostic potrivit. Acest paragraf are rolul de a detalia cerințele funcționale pe care trebuie să le îndeplinească această platformă pentru a atinge obiectivele principale amintite în capitolul anterior.

Cerințele funcționale se vor identifica și modela prin intermediul diagramelor cazurilor de utilizare. Aplicația presupune 2 tipuri de actori: medic și pacient, fiecare dintre aceștia având cazuri de utilizare diferite (*Figura 3* și *Figura 4*).

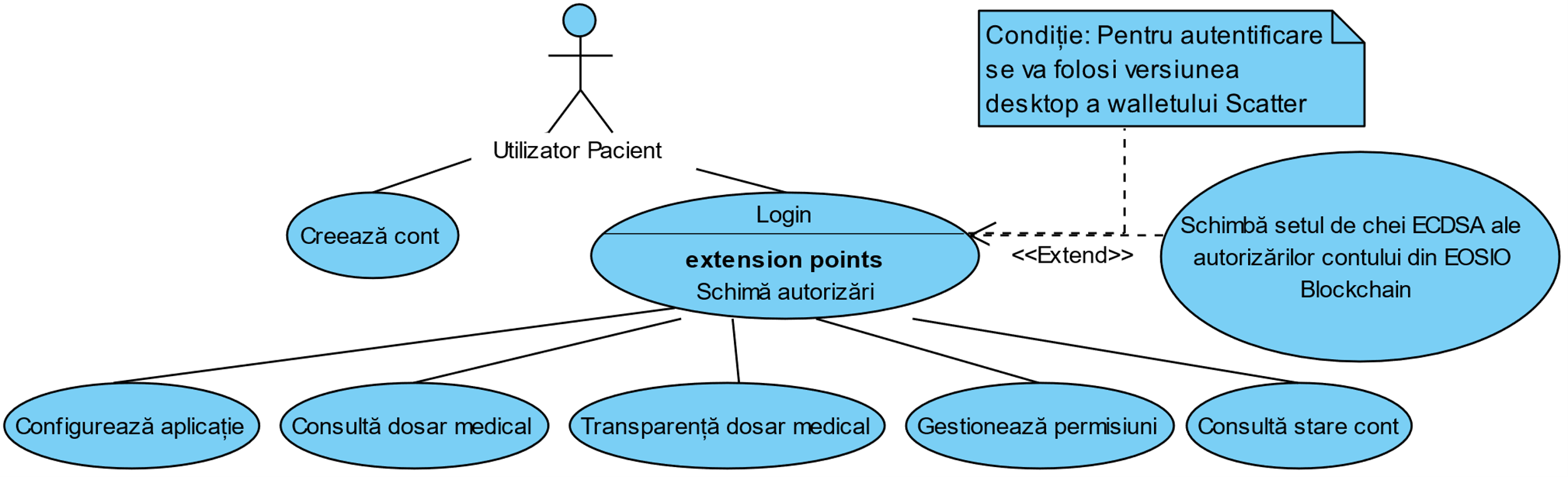


Figura . Diagrama cazurilor de utilizare pentru pacient

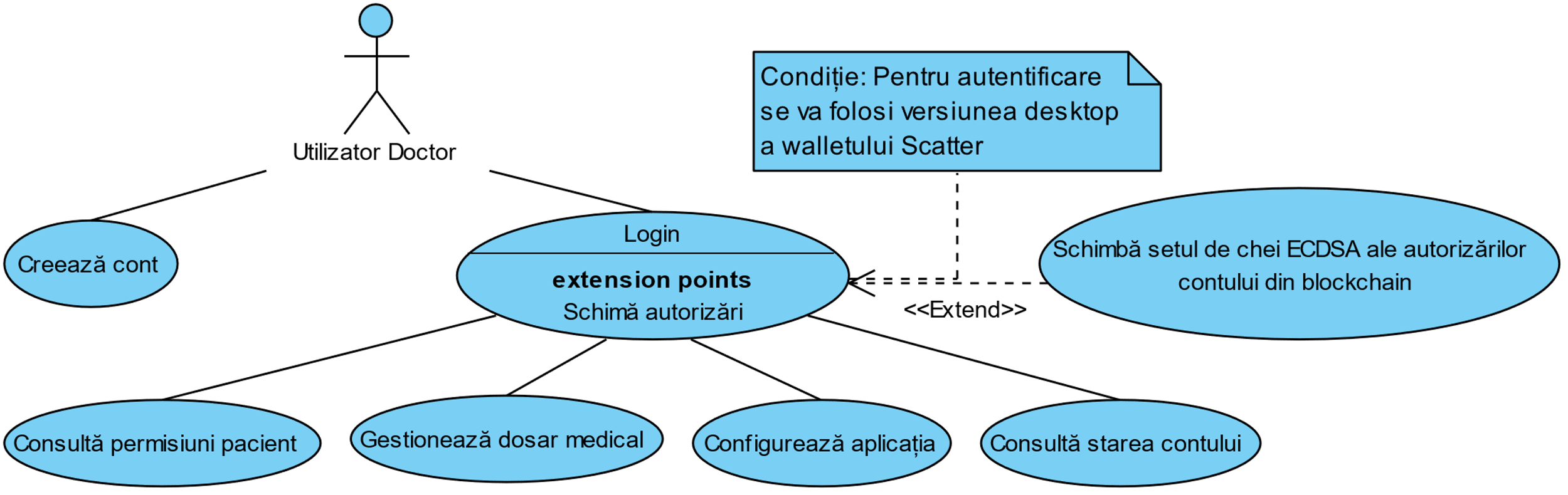


Figura . Diagrama cazurilor de utilizare pentru doctor

## Arhitectura sistemului

Pentru a putea satisface cazurile de utilizare specificate în paragraful anterior, este necesară construirea unei infrastructuri a sistemului, care va respecta toate specificațiile enunțate în capitolul anterior. Aceasta va avea următoarele componente: aplicația web dezvoltată în cadrul framework-ului React, blockchain-ul EOSIO, sistemul de fișiere distribuit IPFS, serviciul de identificare, wallet-ul Scatter care va stoca cheile private ECDSA asociate contului din bockchain și wallet-ul dezvoltat în NodeJS care va stoca cheile private de partajare (RSA pe 1024 biți) și de criptare a înregistrărilor medicale (AES). În continuare este prezentată diagrama de desfășurare, unde se observă cum are loc interacțiunea dintre acestea (*Figura 5*).

O imagine care conține text, hartă

Descriere generată automat

Figura . Diagrama de desfășurare a arhitecturii aplicației

Analizând această diagramă, se observă clar că această arhitectură satisface criteriile cheie specificate în capitolul precedent, cum ar fi **accesibilitatea datelor** (sistemul e decentralizat), **stocarea și partajarea securizată** (înregistrările sunt stocate criptat în IPFS, toate tranzacțiile se semnează cu ajutorul wallet-ului, comunicarea cu serviciul de identificare se va face prin intermediul protocolului HTTPS), **rețeaua de încredere** (identitatea fiecărui utilizator nou este validată de către serviciul de identificare).   
 Serviciul de identificare este unul centralizat, ceea ce la prima vedere contravine cu concepția sistemului decentralizat. Această alegere nu a fost făcută în zadar. În primul rând, ea asigură compatibilitatea noului sistem cu tehnologiile și sistemele implementate până la momentul actual, în special baza de date a tuturor cetățenilor deținută de către Guvern și baza de date a medicilor deținută de către Ministerul Sănătății, care reprezintă servicii centralizate. De asemenea, stocarea distribuită a acestor baze de date ar fi ineficientă, deoarece s-ar consuma foarte mult spațiu de stocare în zadar. În al doilea rând, folosirea acestui serviciu va avea loc foarte rar, în condiții limitate. Acesta va fi folosit doar la înregistrarea noilor utilizatori și la solicitarea numelui contului din blockchain pe baza numelui complet al pacientului/doctorului. Astfel, în momentul în care majoritatea utilizatorilor vor fi identificați și înregistrați, necesitatea acestuia va fi minimă, iar în cazul în care acesta va fi indisponibil, sistemul va putea funcționa în continuare fără nici o problemă, punând la dispoziție serviciile de bază.

Logica care va controla activitatea sistemului se va afla în contractul inteligent medical stocat în fiecare nod al blockchain-ului, invocarea acesteia fiind posibilă din fiecare dintre acestea. Astfel sistemul va fi robust în fața atacurilor (este imposibilă modificarea logicii în unul dintre noduri, celelalte vor observa acest lucru), precum și în cazul în care unul dintre noduri va cădea. Se observă că contractul cooperează cu serviciul de identificare pentru a fi posibilă înregistrarea de utilizatori noi și cu aplicația web, căreia îi furnizează funcționalitățile de bază pentru manipularea permisiunilor și înregistrărilor medicale.

Stocarea efectivă a înregistrărilor medicale va avea loc în sistemul de fișiere distribuit IPFS sub formă *compresată* și *criptată.* În urma acestei separări în blockchain se vor stoca doar meta-datele înregistrărilor. Această separare s-a făcut din următoarele considerente: pentru a reduce spațiul de stocare (în blockchain înregistrarea va fi replicată pe toate nodurile, în IPFS selectiv pe unele noduri); pentru a introduce componenta economică (instituțiile medicale care dețin resurse hardware limitate, în special memorie, vor putea rula noduri de blockchain și de IPFS însă cu o politică de cache restrânsă, iar cele cu resurse de stocare semnificative vor putea rula atât noduri de blockchain, cât și de IPFS cu politică de cache extinsă, fiind remunerate de către sistem).

Aplicația web va interacționa cu toate componentele sistemului, agregând toate funcționalitățile acestuia și punându-i-le la dispoziție utilizatorului într-o interfață grafică intuitivă și ușor de folosit. Trebuie de menționat faptul că stocarea acesteia nu va avea loc în maniera tradițională folosind un web server, deoarece aceasta ar putea afecta puternic scalabilitatea sistemului. În acest caz, chiar dacă blockchain-ul și sistemul de stocare sunt decentralizate, interacțiunea cu acestea se va face dintr-un singur punct, aplicația web devenind de fapt un *bottleneck* și un *single point of failure* în cadrul sistemului. De aceea, aceasta va fi stocată de asemenea în IPFS, putând fi accesată din orice nod al acesteia de către browser-ul web.

## Contractul inteligent

Blockchain-ul EOSIO execută codul din cadrul aplicațiilor folosind *WebAssembly (WASM).* La momentul actual, instrumentul cel mai matur pentru construirea de aplicații care se compilează în WASM este *clang / llvm* cu compilatorul de C/C++. Din această cauză, contractele inteligente din cadrul blockchain-ului EOSIO se scriu în limbajul C++, fiind de fapt niște clase obișnuite, care conțin o stare internă, iar metodele publice sunt acțiunile care pot fi invocate de către tranzacțiile transmise nodurilor din blockchain (în cadrul unei tranzacții se pot invoca mai multe acțiuni).

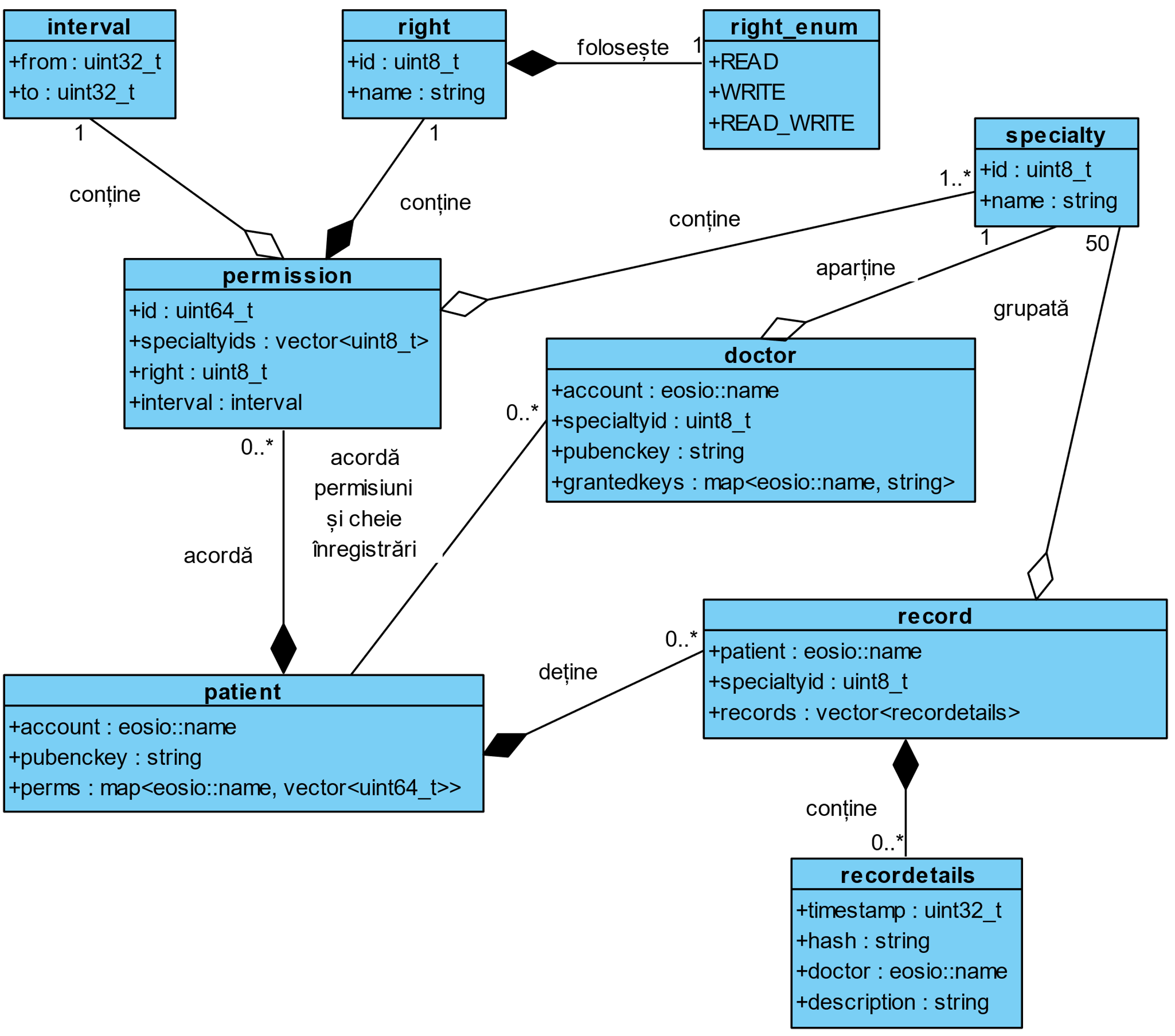


Figura . Diagrama de clase pentru starea interna a contractului inteligent

Starea internă a contractului este persistentă de-a lungul timpului în urma invocării acțiunilor contractului prin intermediul *tabelelor multi-indexate,* care o stochează într-un *cache* din EOSIO RAM pentru acces rapid.O tabelă este modelată printr-o structură din limbajul C/C++. Fiecare contract rezervă o partiție din RAM-ul acestui cache, accesul partiției fiind făcut pe baza numelui tabelei, codul contractului și unui domeniu. Cu ajutorul acestor tabele vom modela structura permisiunilor și meta-datelor despre dosarul medical al pacientului. Această structură este reflectată de către *Figura 6*.

În acest context, trebuie menționată tabela *record*. Această tabelă nu este expusă în *ABI* aferent fiecărui contract, astfel aflarea conținutului acesteia de către oricine este imposibilă prin intermediul apelurilor *RPC* către un nod din blockchain. Aceasta este o măsură de securitate pentru a preveni situația în care atacatorul a obținut cheia de decriptare a pacientului. Neavând acces la hash-ul înregistrărilor din blockchain, acesta nu va putea să găsească conținutul criptat al acestora din IPFS, și respectiv să vadă conținutul lor. Unica modalitate de a obține aceste meta-date este de a rula o tranzacție cu acțiunea de citire a acestora ce aparține contractului, acesta din urmă fiind unica entitate care are acces la ele și le oferă conform politicii de acces definite de către pacient.

## Politica de acces

Pacientul are acces nerestricționat asupra înregistrărilor din dosarul său medical. Totuși, pentru a putea partaja dosarul său medical cu personalul medical, este nevoie de folosirea unei politici de acces bazată pe permisiuni acordate de către pacient. Permisiunile vor permite partajarea selectivă a înregistrărilor cu un grad de flexibilitate foarte înalt. Astfel, este posibilă acordarea unui medic a unei permisiuni cu un anumit tip de drept, care poate fi de *CONSULTARE, ADĂUGARE* sau *CONSULTARE* și *ADĂUGARE* concomitent, pentru înregistrări ce fac parte din una sau mai multe specialități medicale, pentru un anumit interval, care poate fi *LIMITAT* sau *NELIMITAT.* Pacientul poate să folosească toate operațiile *CRUD* (creare, citire, modificare, ștergere) asupra permisiunilor. Unica restricție care este impusă, este ca aceste permisiuni să nu se suprapună.

Algoritmul care verifică dacă două permisiuni acordate aceluiași medic nu se suprapun constă în următorii pași, toate verificările trebuind să fie îndeplinite:

* Verifică dacă drepturile sunt diferite
* Verifică dacă vectorii cu id-uri de specialități sunt distincți
* Verifică dacă intervalele de timp nu se suprapun

Algoritmii folosiți pentru definirea politicii de acces asupra înregistrărilor se regăsesc în *Figura 7*, *Figura 8* și *Figura 9*. În acest context, trebuie detaliat mecanismul prin care are loc auto-ștergerea permisiunilor. Acesta se aplică doar permisiunilor cu drept de adăugare, deoarece odată ce acestea expiră, devin inutile și ocupă spațiu în zadar în cache-ul contractului. Auto-ștergerea funcționează prin invocarea amânată a acțiunii de ștergere a unei permisiuni. Tranzacțiile amânate poartă autoritatea contractului care le trimite. Astfel, fiind planificată din cadrul acțiunii de adăugare sau modificare, această tranzacție poartă autoritatea pacientului care a invocat ultimele 2 acțiuni, făcând posibilă executarea automată a acțiunii de ștergere care necesită semnătura digitală a pacientului. În cadrul blockchain-ului EOSIO acțiunile amânate sunt programate să ruleze, în cel mai bun caz, într-o perioadă ulterioară, la discreția producătorului. Nu există nici o garanție că acțiunea amânată va fi executată. Soluția acestei probleme este ștergerea manuală a permisiunii de către utilizator.

Pentru a facilita managementul acestor permisiuni se va folosi o mașină de stări virtuală. Stările nu vor fi stocate efectiv, ci se vor calcula la *run-time*, în momentul încărcării permisiunilor în cadrul aplicației. Tranzițiile se vor face pe baza unor predicate, iar tranziția în faza finală unde permisiunea va fi ștearsă se va face pe baza mecanismului de auto-ștergere sau prin ștergerea manuală de către utilizator. Logica conform căreia au loc tranzițiile este prezentată în *Figura 10*. Trebuie de notat faptul că permisiunea poate fi ștearsă de către pacient indiferent de starea în care se află, auto ștergerea funcționând doar pentru starea *Expired.*

O imagine care conține text, hartă

Descriere generată automat

Figura . Diagrama de activitate pentru adăugarea unei permisiuni

O imagine care conține text

Descriere generată automat

Figura . Diagrama de activitate pentru modificarea unei permisiuni

O imagine care conține text

Descriere generată automat

Figura . Diagrama de activitate pentru ștergerea unei permisiuni

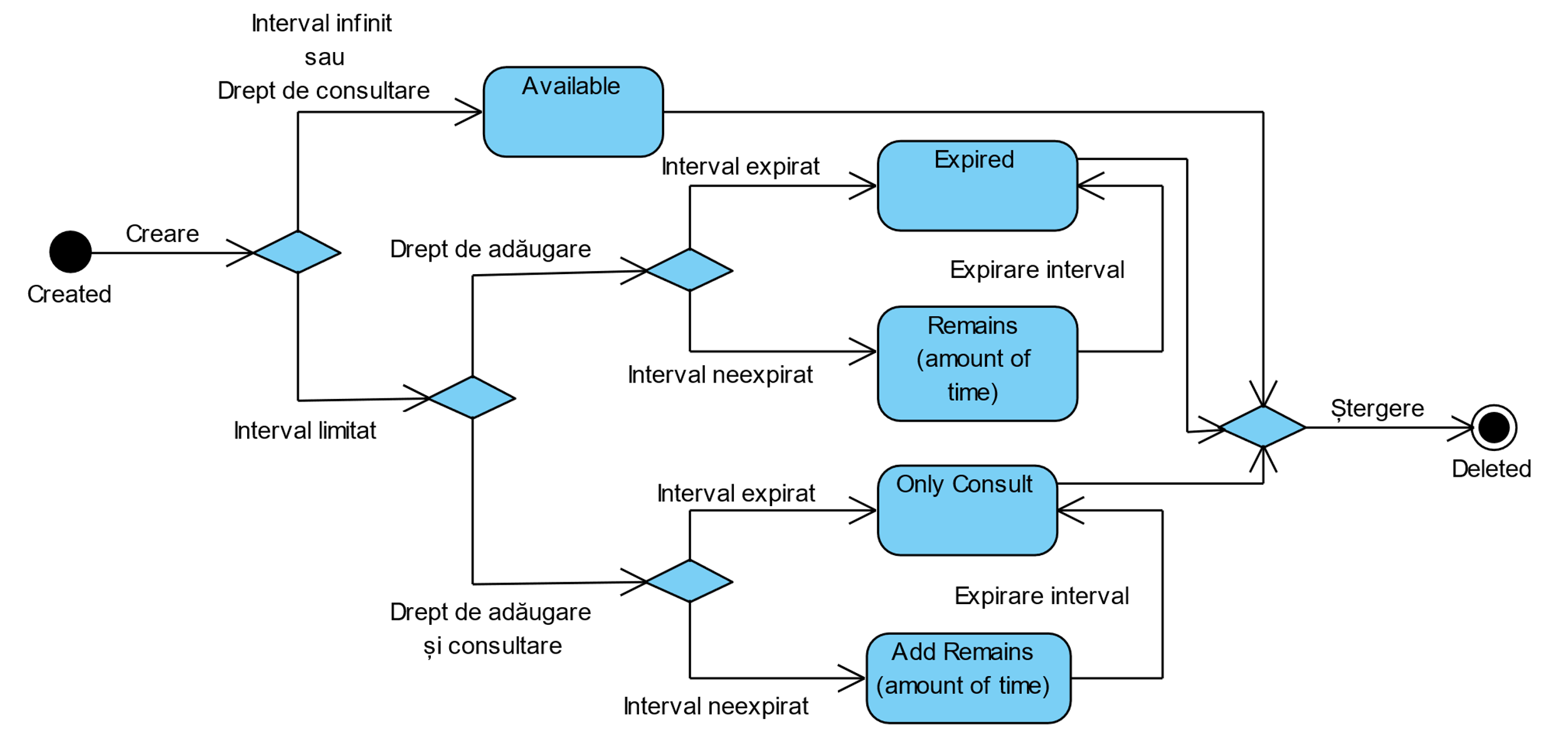


Figura . Diagrama de stări pentru permisiune

## Meta-datele înregistrărilor medicale

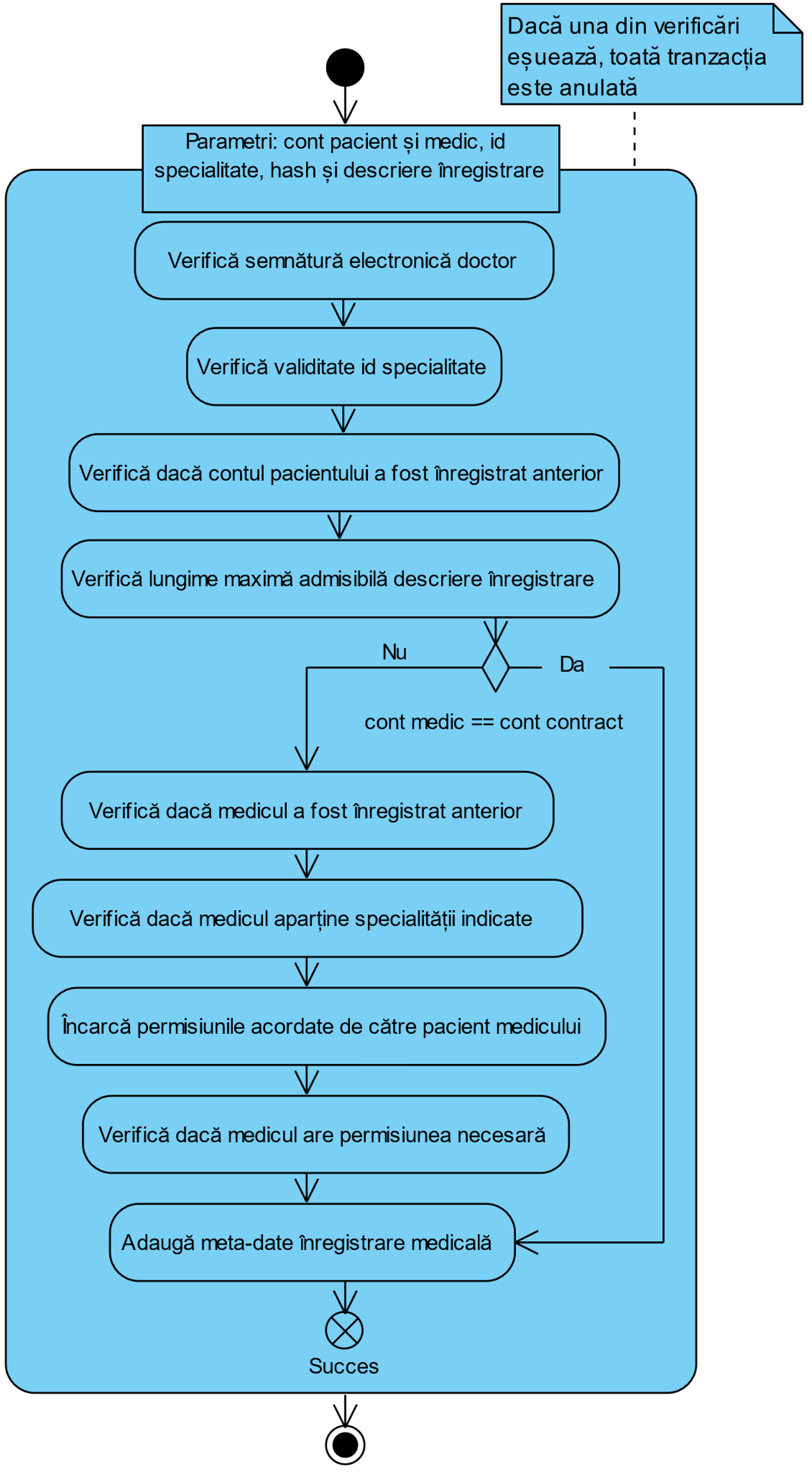


Figura . Diagrama de activitate adăugare meta-date înregistrare medicală

După cum a fost menționat în capitolul precedent, este necesară implementarea unui mecanism de rezervă pentru gestionarea dosarului medical în cazul care pacientul este inconștient sau inapt. Acest lucru se realizează prin intermediul verificării dacă contul medicului specificat în parametrii acțiunii este echivalent cu cel al contului unde a fost încărcat contractul, caz în care sistemul de permisiuni este ocolit. Această verificare are loc după ce a fost verificată semnătura electronică a contului medicului, astfel încât să nu existe nici o șansă de a exploata acest mecanism (*break the glass mechanism)*.

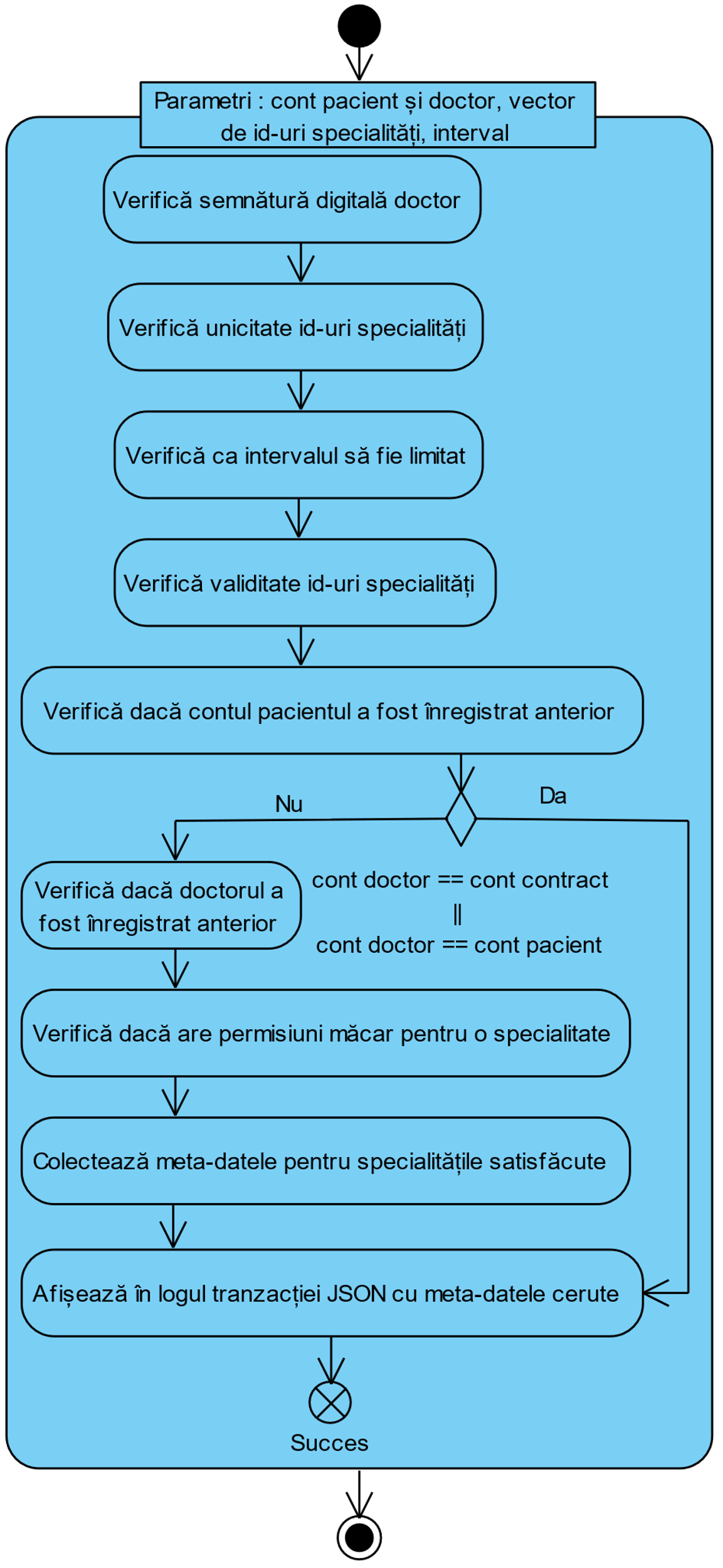


Figura . Diagrama de activitate consultare meta-date înregistrări medicale

Asemănător cazului de adăugare a înregistrării, pentru a consulta înregistrări se va folosi *break the glass mechanism*. Totuși, în cazul consultării, se face o verificare suplimentară, contului doctorului cu cel al pacientului. Astfel în cazul în care cele două coincid, atunci pacientului i se dă accesul deplin la dosarul său. Acest lucru este posibil verificării în prealabil a semnăturii electronice a pacientului, precum și a faptului că se verifică în prealabil dacă contul specificat pentru pacient face parte din tabela pacienților, iar doctorul nu poate fi pacient în același timp pacient, aceștia mereu se află în tabele diferite.

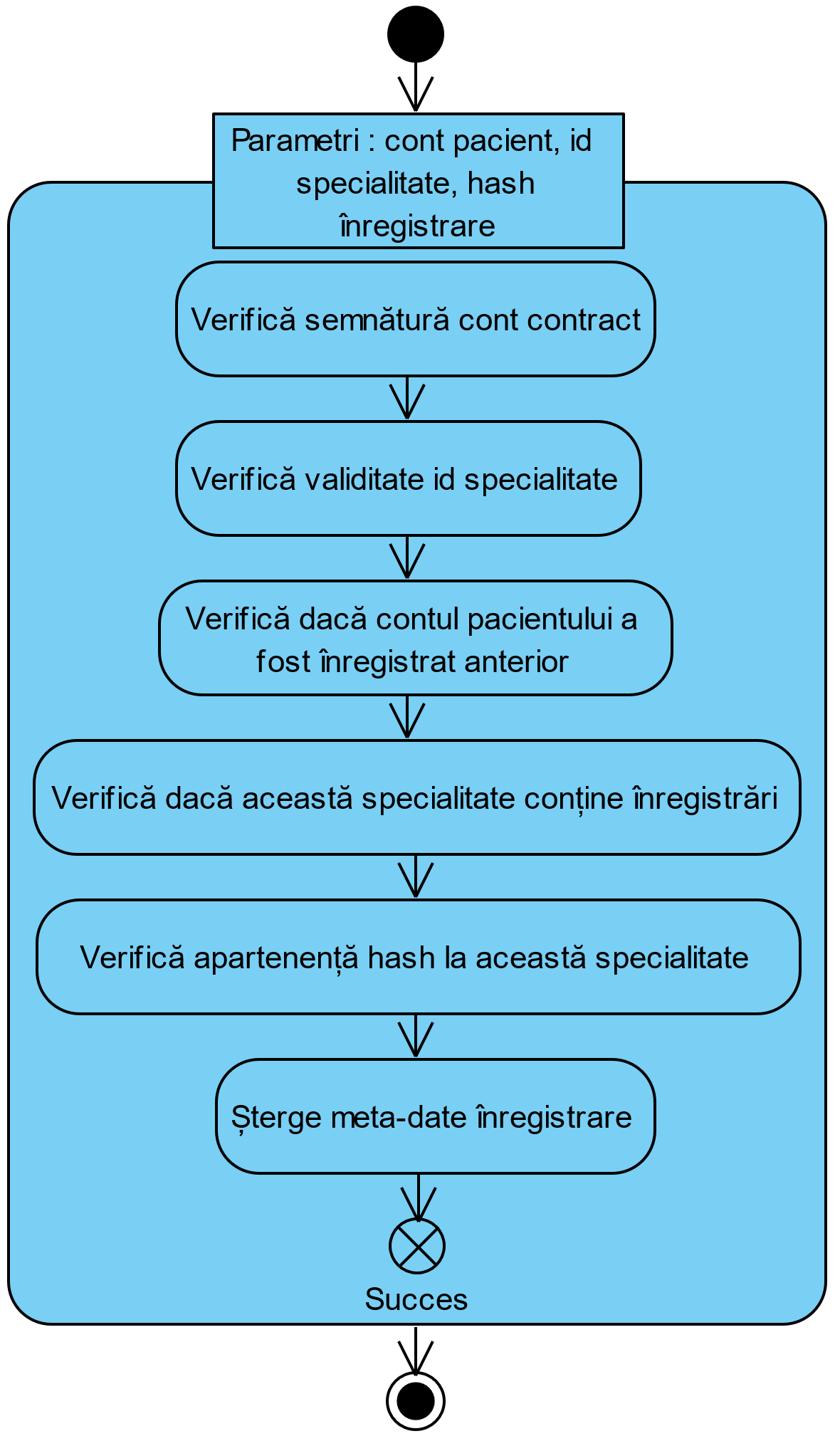


Figura . Diagrama de activitate ștergere meta-date înregistrare

Analizând diagramele din *Figura 11, Figura 12* și *Figura 13* se observă clar rolurile cu care pot fi invocate acțiunile contractului inteligent pentru manipularea meta-datelor despre înregistrările din dosarul medical:

* Adăugare: această acțiune poate fi invocată doar de către medicul calificat în specialitatea cărei aparține înregistrarea sau administratorul contractului inteligent, pentru a preveni introducerea unor date eronate de către persoanele necalificate, cum ar fi pacientul
* Consultare: această acțiune poate fi invocată de către medic în limita politicii de acces impusă de pacient; pacientul și administratorul contractului inteligent au acces nerestricționat
* Ștergere: această acțiune poate fi invocată doar de către administratorul contractului inteligent, pentru a asigura consistența și integritatea dosarului medical, această acțiune fiind folosită doar în cazuri excepționale în urma producerii unei erori umane de către doctor în momentul adăugării înregistrării (spre exemplu, dacă din greșeală a fost adăugată o înregistrare greșită)

## Proiectarea bazelor de date

Serviciul de identificare folosește două baze de date pentru a putea furniza cele 2 servicii de bază aplicațiilor ce comunică cu acesta: înregistrare de noi utilizatori și furnizare cont blockchain pe baza numelui complet sau vice-versa. Prima bază de date conține identitățile actorilor, adică datele lor personale, iar a doua utilizatorii ce dețin cont în blockchain și au fost înregistrați în cadrul contractului inteligent. Dat fiind faptul că funcționalitățile oferite sunt reduse și majoritatea logicii e incapsulată în contract, schema acestor baze de date este simplă, aceasta urmând principiul de proiectare *KISS(Keep It Simple and Short).* În *Figura 14* și *Figura 15* sunt prezentate schemele acestor baze de date. Trebuie de menționat că tabela *Specialty* este pre-populată cu date din contractul inteligent, pentru a menține sincronizarea dintre cele două, aceasta urmând principiul *DRY (Don’t Repeat Yourself).*

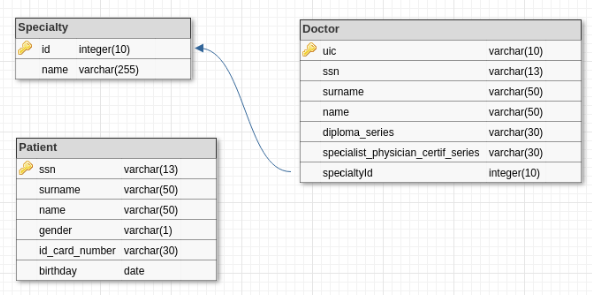


Figura . Schema bazei de date identități pacienți și medici

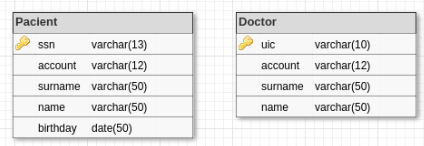


Figura . Schema bazei de date utilizatori înregistrați

## Înregistrarea utilizatorilor

Înregistrarea s-ar fi putut face pe baza unui sistem de invitații, ceea ce presupune verificarea identității utilizatorului manual de către o persoană specializată, crearea contului de către aceasta și înmânarea credențialelor către utilizator. Acest tip de înregistrare este ineficient și creează incomodități atât pentru administratori, cât și pentru utilizatori. Pentru a automatiza acest proces în cadrul sistemului a fost introdus serviciul de identificare, acesta cooperând cu aplicația web și cu blockchain-ul pentru a realiza acest lucru. Înregistrarea are loc în următoarele etape:

1. Preluare date din aplicația web
2. Verificare identitate utilizator de către serviciul de identificare
3. Creare cont în blockchain și înregistrare în cadrul contractului inteligent
4. Înregistrare în cadrul serviciului de identificare
5. Oferire chei private pacientului
6. Importarea cheilor private în wallet-uri

Algoritmul complet este prezentat în diagrama de activitate din *Figura 16*. Acest algoritm este protejat în fața atacurilor de tipul ***man in the middle****,* deoarece cheile private sunt generate local în cadrul aplicației web, în tranzit aflându-se doar cheile publice aferente autorizațiilor contului din blockchain, 2 chei ECDSA pentru autoritatea *owner* și *active* folosite la semnarea tranzacțiilor*,* transmise printr-un canal securizat oferit de protocolul HTTPS, iar în răspunsul de la server se află doar rezultatul creării contului. Mai mult, acest algoritm oferă garanția că nimeni nu va putea crea un cont de sine stătător în blockchain ***ocolind serviciul de identificare***, folosindu-se de următoarele două proprietăți: în cadrul blockchainului EOSIO pentru a crea un cont nou e nevoie de un cont deja existent; în momentul înregistrării contului în cadrul contractului inteligent se verifică semnătura electronică a contului contractului inteligent, semnătură ce este deținută doar de către serviciul de identificare. Odată importate în wallet-uri, cheile private generate în RAM se distrug.

O imagine care conține captură de ecran

Descriere generată automat

Figura . Diagramă de activitate înregistrare utilizator

## Managementul permisiunilor

Folosind interfața intuitivă oferită de către aplicația web, pacientul va putea gestiona politica de acces asupra dosarului medical. Pentru realizarea acestui lucru este necesară conlucrarea a trei componente din cadrul sistemului: aplicația web, wallet-ul Scatter ce conține cheile necesare pentru semnarea tranzacțiilor și unul din nodurile din blockchain. Toate operațiile efectuate asupra permisiunilor (creare, modificare, ștergere) au loc după același algoritm, care este prezentat în diagrama de interacțiune din *Figura 17*.

O imagine care conține captură de ecran

Descriere generată automat

Figura . Diagrama de interacțiune pentru operațiile cu permisiuni

După cum se observă în cadrul diagramei de mai sus, interacțiunea dintre aplicație și wallet are loc prin intermediul *WebSockets,* conexiune ce este stabilită în momentul în care utilizatorul se loghează în aplicație prin intermediul wallet-ului, iar interacțiunea dintre aplicație și nodurile din blockchain prin intermediul apelurilor *RPC* folosind protocolul HTTP/HTTPS. Trebuie de menționat faptul că utilizatorul, în cazul dat pacientul, trebuie să aibă instalat local, pe calculator wallet-ul Scatter, indiferent de tipul de aplicație folosit (web, mobile sau desktop).

## Adăugarea înregistrării medicale

Adăugarea unei înregistrări medicale poate fi făcută doar de către medicul specialist în limita politicii de acces impuse de către pacient, folosind interfața grafică din cadrul aplicației web. Pentru a adăuga o înregistrare este necesară conlucrarea următoarelor componente din cadrul platformei: aplicația web, Scatter wallet, un nod IPFS, un nod EOSIO și opțional walletul ce conține cheile private de partajare și criptare a înregistrărilor. Diagrama BPMN care ilustrează cum are loc acest proces este prezentată în *Figura 18*.

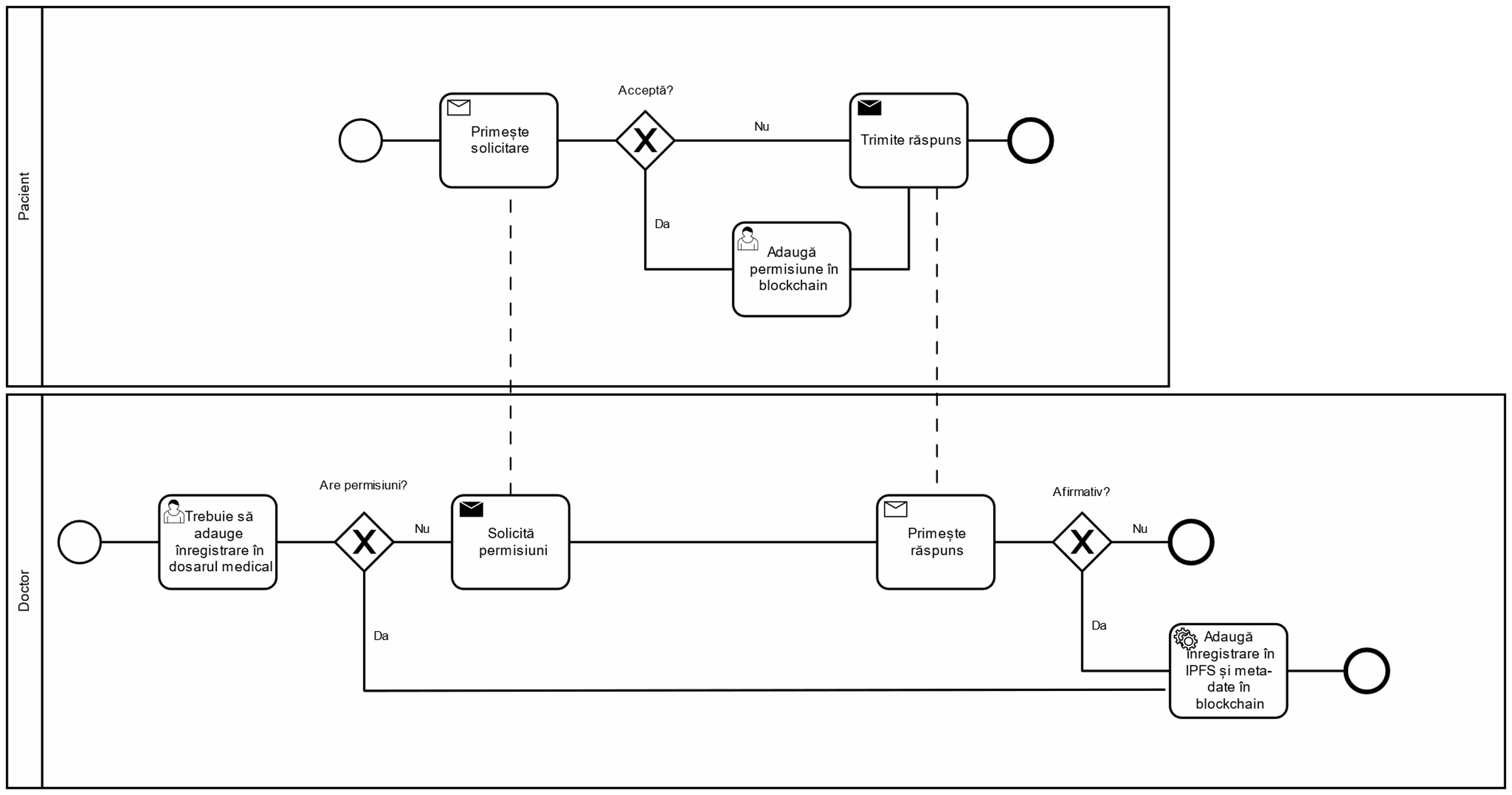


Figura . Diagrama de colaborare BPMN pentru adăugare înregistrare medicală

Algoritmul detaliat care reprezintă cum are loc interacțiunea dintre aceste componente este prezentat în *Figura 19*.

O imagine care conține captură de ecran

Descriere generată automat

Figura . Diagrama de interacțiune pentru adăugare înregistrare medicală

În urma pasului 1 este obținută cheia privată RSA a doctorului care în combinație cu cheia publică asociată este folosită pentru partajarea cheii private AES a pacientului folosită la criptarea înregistrărilor medicale. În starea internă a contractului inteligent, în tabela medici, fiecare doctor are un câmp în care sunt enumerate toate cheile private AES acordate de către pacienți lui, criptate cu cheia publică de partajare a acestuia. La pasul 2 are loc regăsirea acestei chei a pacientului căruia urmează să i se adauge înregistrarea. În caz că pacientul nu i-a acordat anterior nici o permisiune cu drept de adăugare, această cheie va lipsi și procedeul se va încheia. Între pasul 2 și 3 are loc procesarea înregistrării medicale. Mai întâi se decriptează cheia pacientului folosind cheia privată a doctorului, apoi fișierul .xml ce conține înregistrarea medicală în format *C-CDA (Consolidated Clinical Document Architecture)* este comprimat folosind tipul de compresie lossless *LZMA (Lempel-Ziv-Markov),* pentru ca ulterior să fie criptat cu cheia simetrică a pacientului, apoi ambele chei private din RAM sunt distruse. La pasul 3 are loc stocarea acestei înregistrări în cadrul IPFS folosind *REST API* pus la dispoziție de către acesta. O precondiție este ca în browserul medicului să fie instalată extensia *IPFS Companion.* Nodul IPFS necesar pentru stocarea înregistrării poate fi rulat *embedded* în cadrul browserului sau poate specificată adresa HTTP a unui nod care rulează pe altă mașină. În urma stocării, aplicației îi este returnat un obiect ce conține detaliile aferente operației de stocare, însă câmpul cel mai importat este *root hash* cu ajutorul căruia această înregistrare poate fi regăsită (IPFS folosește *content addressing*). Apoi este creat obiectul de tranzacție ce conține toate meta-datele aferente acestei înregistrări, inclusiv hash-ul acesteia și semnat cu cheia privată ECDSA a medicului stocată în wallet-ul Scatter. Tranzacția este ulterior trimisă unui nod din blockchain, unde va fi rulată acțiunea de adăugare a metadatelor. În caz că aceasta eșuează (doctorul nu are permisiune sau a fost depășit timpul de execuție al tranzacției), înregistrarea adăugată anterior în IPFS se va afla într-o stare *atârnată*, hash necesar acesteia va fi pierdut, ea ocupând un spațiu de stocare în zadar. Aceasta nu este o problemă majoră, deoarece odată ce este hash-ul ei este pierdut ea nu va mai putea fi adresată și nici partajată între noduri, astfel că în funcție de politica de cache setată, aceasta va fi ștearsă automat de pe nodurile unde a fost stocată inițial. În cazul în care tranzacția a fost rulată cu succes, ea este adăugată în registrul comun, meta-datele sunt salvate în starea internă a contractului, iar aplicației îi este întors un obiect JSON ce conține detaliile rulării tranzacției.

## Consultarea înregistrărilor medicale

Consultarea înregistrărilor medicale este posibilă datorită conlucrării dintre următoarele componente ale sistemului: aplicația web, Scatter wallet, un nod IPFS, un nod EOSIO și opțional walletul ce conține cheile private de partajare și criptare a înregistrărilor. Ea are loc în 2 etape: în prima etapă se obține lista înregistrărilor medicale din blockchain în funcție de criteriile specificate, iar în a doua etapă are loc vizualizarea conținutului înregistrării stocate în IPFS.

Prima etapă este prezentată în *Figura 20*. În cazul în care tranzacția a rulat cu succes, aplicației îi este returnat un obiect JSON ce conține lista cu toate meta-datele înregistrărilor ce satisfac criteriile specificate în funcție de politica de acces (în caz că doctorul nu are permisiuni pentru toate specialitățile medicale indicate, acestuia îi vor fi puse la dispoziție doar înregistrările pentru specialitățile unde are).

În mod implicit doctorului i se afișează contul medicului care a adăugat înregistrarea. În caz că acesta a specificat afișarea numelui complet al acestuia în loc de cont, va fi nevoie de-l regăsit în cadrul serviciul de identificare. Pentru a minimiza numărul de interacțiuni cu acest serviciu, respectiv cu rețeaua, luând în calcul ca aceasta mapare este permanentă, se poate folosi o optimizare, și anume folosirea unui cache local în care se salvează aceste mapări, astfel interacțiunea cu serviciul are loc doar în cazul în care numele medicului nu a fost încărcat anterior.

O imagine care conține captură de ecran

Descriere generată automat

Figura . Diagrama de interacțiune pentru citire listă înregistrări medicale

A doua etapă este prezentată în *Figura 21*. Acest algoritm este similar celui folosit la adăugare, doar că este în ordine inversă. La pasul 1 aplicația îi cere doctorului cheia sa privată de partajare sau parola de la wallet. În cazul în care acesta furnizează parola, la pasul 2 această cheie este solicitată de la wallet, apoi decriptată cu parola furnizată (cheile stocate în cadrul walletului sunt criptate simetric cu parola aleasă de utilizator în momentul înregistrării), altfel se va folosi cheia privată introdusă de acesta. La pasul 3 are loc regăsirea cheii de decriptare a înregistrării medicale care i-a fost furnizată anterior de către pacient, aceasta fiind decriptată cu cheia privată de partajare a medicului. La pasul 4 folosind hash-ul înregistrării, conținutul acesteia este regăsit din IPFS, se decompresează și decriptatează, ulterior cheile private din RAM fiind distruse. Pentru a îmbunătăți experiența utilizatorului, aplicația copiază conținutul înregistrării pe clipboard, deschide un nou tab în browser cu un *viewer* pentru documente C-CDA, medicului rămânându-i să dea paste în cadrul zonei destinate indroducerii conținutului documentului și ulterior să analizeze înregistrarea.

O imagine care conține captură de ecran

Descriere generată automat

Figura . Diagrama de interacțiune pentru consultare conținut înregistrare

## Experiența utilizatorului

Majoritatea aplicațiilor care sunt construite pe baza tehnologiei blockchain și folosesc criptografia bazată pe chei publice și private necesită un nivel semnificativ de cunoștințe tehnice în acest domeniu din partea utilizatorilor. Aceasta ar putea fi o piedică în adopția noului sistem de către medici și pacienți și ar influența negativ experiența folosirii aplicației. Pentru a soluția această problemă este necesară abstractizarea pe cât este posibil a detaliilor tehnice, precum și oferirea unei interfețe grafice foarte intuitive. Totuși aceștia vor trebui să fie informați despre riscurile asociate coruperii cheilor lor private.

Elementele care contribuie la abstractizarea detaliilor legate de criptografia bazată pe cheile public sunt wallet-urile. Acestea au rolul de a stoca securizat cheile private și a asigura faptul că acestea nu vor putea fi corupte (doar pe durata aflării în wallet, în cazul aflării în tranzit aceasta este responsabilitatea altor părți ale sistemului). Mai mult, acestea oferă un mecanism simplu de acces la chei, cerând utilizatorului o parolă care poate fi ușor memorată, lucru ce nu poate fi spus despre cheile private, care sunt destul de lungi și au o înșiruire *random* de caractere, făcând foarte grea memorarea acestora. Unica manipulare pe care utilizatorul o face cu cheile private din blockchain este importarea lor manuală în wallet-ul Scatter, odată făcut acest lucru acesta se poate loga cu o parolă în wallet și să folosească aplicația, toate detaliile aferente semnării tranzacțiilor, furnizării identității utilizatorului, folosirii cheilor private sunt abstractizate și ascunse de către conlucrarea dintre aplicația web și wallet. Stocarea cheilor private de partajare și criptare a fișierelor are loc automat într-un alt wallet, care poate stoca chei din formate diferite, nu doar ECDSA. Aceste chei sunt mai întâi criptate cu parola aleasă de utilizator în momentul înregistrării, apoi trimise walletului spre stocare. Totuși este recomandată stocarea cheilor în alte locuri alternative, aplicația permițând acest lucru. În momentul efectuării operațiilor cu înregistrările medicale tot ce se cere de la utilizator este introducerea parolei acestuia de la wallet sau introducerea directă a cheii private, restul operațiilor au loc automat. Acest lucru influențează foarte pozitiv asupra experienței utilizatorului, acesta fiind nevoit sa memoreze doar 2 parole (acestea pot fi și identice, dar nu este recomandat).

## Transparența dosarului medical

Una din proprietățile de bază ale tehnologiei blockchain este imutabilitatea, orice tranzacție care a avut loc în cadrul sistemului este înregistrată în registrul comun, fiind practic imposibilă alterarea acesteia (sunt necesare resurse de calcul enorme pentru a modifica hash-ul de legătură dintre blocuri). Această proprietate oferă o trasabilitate excelentă asupra tuturor acțiunilor întreprinse de către personalul medical, fiind o sursă credibilă de istoric al dosarului medical. Aplicația web pune la dispoziție pacientului rapoarte detaliate sub formă de diagrame și tabele, în funcție de contul doctorului și intervalului selectat, bazându-se pe istoricul tranzacțiilor efectuate de către medic asupra dosarului său medical furnizat de către nodurile din blockchain.

În *Figura 22* este prezentată activitatea unui doctor asupra dosarului medical sub formă de grafic. În *Figura 23* este prezentat un raport detaliat asupra acțiunilor de adăugare a înregistrărilor medicale întreprinse de către un doctor, ce conține informații despre autoritatea sub care a fost rulată tranzacția (în cazul dat autoritatea ce are permisiunea *active* și actorul *docvasileion),* hash-ul înregistrării, specialitatea medicală pentru care a fost adăugată, timestampul nodului din blockchain în momentul adăugării, numărul blocului unde se află tranzacția, precum și id-ul acesteia.

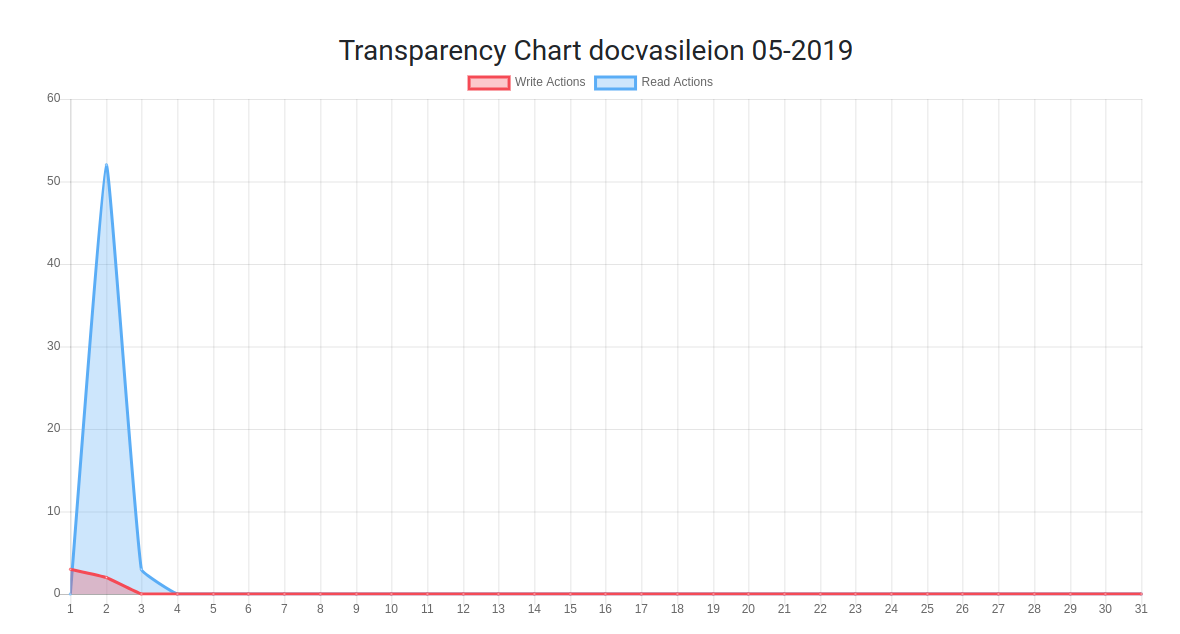
******

Figura . Raport grafic activitate doctor asupra dosarului medical

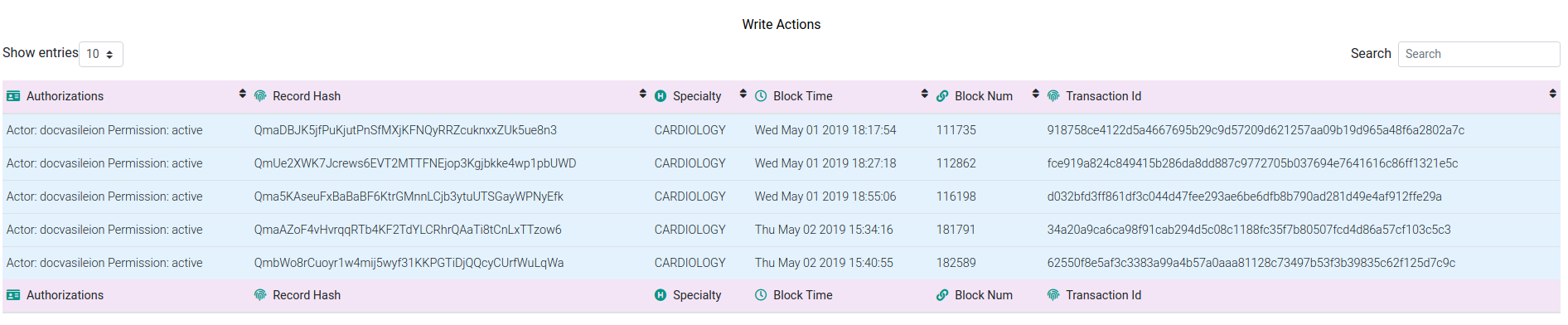


Figura . Raport grafic activitate doctor asupra dosarului medical

# *Concluzii / Alte considerente*

## Conformitatea cu cerințele stabilite

Analizând atent arhitectura sistemului prezentat în capitolul anterior, se poate de afirmat că respectă în întregime cerințele formulate la începutul lucrării:

* *Asigurarea confidențialității datelor:* toate înregistrările medicale sunt criptate cu o cheie simetrică deținută doar de către pacient, nimeni nu poate vizualiza conținutul acestora fără ea
* *Stocarea și partajarea securizată a datelor:* toate înregistrările medicale sunt stocate în formă compresată și criptată, iar partajarea lor are loc folosind o pereche de chei asimetrice prin intermediul căreia pacientul îi poate transmite medicului în care are încredere cheia de criptare a înregistrărilor pentru ca acesta să poate vizualiza conținutul lor
* *Disponibilitatea datelor:* sistemul este distribuit, nu există un singur punct de eșec, meta-datele, permisiunile și logica contractului inteligent fiind disponibile din orice nod al blockchainului, iar conținutul înregistrărilor și aplicația web este disponibilă din orice nod al sistemului de fișiere IPFS. Dacă ne referim la disponibilitate, *călcâiul lui Ahile* al sistemului este serviciul de identificare, care este unul centralizat, totuși în momentul în care majoritatea utilizatorilor vor fi înregistrați, folosirea acestuia va fi nesemnificativă
* *Controlul fin asupra drepturilor de acces asupra datelor:* politica de acces bazată pe permisiuni este foarte flexibilă, permițând pacientului să seteze permisiuni granulare asupra înregistrărilor dosarului medical pentru diferiți doctori, în funcție de specialitatea medicală, dreptul de acces și tipul de interval
* *Ușurința în folosința sistemului:* toate detaliile de ce țin de securitate, precum și complexitatea sistemului sunt ascunse de către aplicația web, care pune la dispoziție o interfață grafică intuitivă și necesită de la utilizator memorarea a două parole de la wallet

## Limitări și direcții de dezvoltare

Cu toate că sistemul întrunește cerințele impuse inițial, implementarea acestuia are unele limitări. Acesta ia în calcul doar două tipuri de utilizatori: medic și pacient, implementând doar primul scenariu din cele trei expuse inițial, și anume ***îngrijirea primară a pacientului***. Acest lucru nu satisface în întregime principiul sănătății conexe, neluând în calcul alte entități medicale precum spitalele, farmaciile, companiile de asigurări în medicină, bio-băncile. Prin introducerea în sistem a bio-băncilor va fi posibilă implementarea scenariului de ***agregare a datelor pentru scopuri de cercetare***, aceasta necesitând adăugarea posibilității de partajare a înregistrărilor sub formă anonimă. Prin introducerea în sistem a farmaciilor și companiilor de asigurări va fi posibilă implementarea scenariului trei de ***conectare a diferiților jucători de pe piața serviciilor medicale***. În acest context, un nouă direcție de dezvoltare ar fi adăugarea facilității de eliberare și folosire în cadrul sistemului a rețetelor medicale compensate, făcând transparent acest proces și împiedicând fraudele legate de acestea. De asemenea la momentul actual pacienții și medicii se află în două categorii strict separate, cu toate că un medic poate fi în același timp și pacient. Introducerea acestei facilități va necesita modificări doar în cadrul logicii contractul inteligent, neafectând restul sistemului. Datorită proiectării modulare a sistemului, extinderea acestuia nu va fi atât de costisitoare, cum ar fi fost cazul în cazul în care acesta ar fi fost un monolit.

## Alternative pe piață

La momentul scrierii acestei lucrări, pe piața din România nu există alternative ale acestui sistem decentralizat pentru stocarea și partajarea dosarelor medicale. Există un prototip pus la dispoziție de **CNAS** ce implementează dosarul electronic medical, care folosește în mare parte în implementare aceleași concepte enunțate în lucrarea prezentă, și anume stocarea dosarului medical sub formă electronică și accesul la acesta cu consimțământul pacientului, precum și folosirea unui mecanism de acces la acesta în situații de urgență. Ambele aplicații conțin module asemănătoare, cum ar fi *Istoric Medical, Documente Medicale, Date Personale.* Diferența dintre aceste sisteme este că cel pus la dispoziție de CNAS este o soluție **centralizată**, minusurile căreia au fost expuse în capitolul 2 al lucrării.

În prezent, se dorește introducerea în Legea 95/2006 care ține de reforma în domeniul sănătății a unui nou articol, numit ***Dosarul electronic al pacientului***. Soluția decentralizată s-ar potrivi cel mai bine pentru medicina privată și companiile de asigurare, care sunt interesate să aibă acces la dosarul complet și actualizat al pacientului, ea contribuind și la conectarea celor două entități.

## Migrația de la soluția centralizată la cea bazată pe blockchain

Este naiv să credem că industria de asistență medicală va elimina soluțiile de astăzi și va reimplementa sistemele de evidență a înregistrărilor electronice medicale bazate pe arhitectura de tip blockchain. Îngrijirea medicală este o industrie reticentă în a-și asuma riscuri, puțin probabil să accepte cu ușurință timpul și costul necesar pentru trecerea la o tehnologie nouă și nedovedită. În plus, există o mare inerție și investiții în *status quo*.

Pentru a obține rate ridicate de adoptare a EHR în SUA, Centrele pentru Medicare și Servicii de Îngrijire Medicală (CMS) au cheltuit peste 30 de miliarde de dolari începând cu 2011. O nouă abordare a evidenței va trebui să respecte această investiție și să lucreze împreună cu infrastructura EHR existentă, nu să o înlocuiască. Instituțiile care mențin date privind asistența medicală în sistemele centralizate percep datele pacientului ca un bun valoros și va fi dificil să-și schimbe modul de gândire.

În timp ce o soluție bazată pe blockchain poate fi o opțiune la un moment dat în viitor, în prezent se necesită o soluție de punte. Următoarele soluții propuse includ crearea unei noi facilități pentru stocarea datelor clinice care se bazează pe tehnologia blockchain, continuând să utilizeze sistemele EHR (și altele) de astăzi pentru captarea și stocarea datelor pacientului. Acest lucru oferă multe dintre avantajele soluției de tip blockchain, în timp ce utilizează investițiile actuale în IT din domeniul sănătății. Standardele și politicile existente oferă cadrul pentru copierea datelor din sistemele tradiționale în noul sistem bazat pe blockchain. Noul sistem va fi în mod eficient o înregistrare electronică medicală personală bazată pe blockchain ( „*Personal Health Record” PHR).*

Soluția propusă începe cu sistemele informatice de sănătate din ziua de astăzi, în special EHR-urile, dar, de asemenea, include potențial și sistemele de informații de laborator, sistemele de radiologie, bazele de date ale plătitorilor, dispozitivele medicale și dispozitivele pentru consumatori. Aceste sisteme vor continua să funcționeze așa cum o fac astăzi, stocând date în bazele de date proprietare. În plus față de stocarea propriei copii a datelor, fiecare sistem va transmite, de asemenea, o copie către sistemul PHR bazat pe blockchain.

Toate sistemele EHR trebuie să ofere posibilitatea ca pacienții să vizualizeze, să descarce și să transmită informațiile despre sănătate în format citit de om, precum și în format citit de mașină. Formatul documentului este **C-CDA**, un format XML care poate fi citit de mașină. Aplicând CSS stiluri pe un document C-CDA, acesta devine un fișier HTML care poate fi citit de un om folosind un browser web. Multe sisteme electronice de sănătate satisfac criteriul de vizualizare / descărcare / transmitere prin punerea la dispoziția pacientului a documentelor C-CDA pe un portal destinat pacienților. De acolo, pacientul poate descărca sau transmite documentul la destinația aleasă. Unele sisteme EHR oferă și alte metode de transmisie care nu necesită un portal destinat pacienților.

Există 3 opțiuni pentru conectarea funcției de vizualizare / descărcare / transmitere a sistemelor EHR la un sistem PHR bazat pe blockchain:

1. Furnizorii de sisteme EHR implementează un client în cadrul software-ului EHR care comunică direct și automat informațiile de sănătate către PHR bazat pe blockchain. Aceasta ar fi opțiunea preferată, dar necesită efort și cooperare din partea furnizorilor EHR și este puțin probabil să apară fără reglementare sau stimulare.
2. Distribuitorii de sisteme EHR utilizează protocoale existente, cum ar fi REST, SOAP sau Direct Messaging, pentru a trimite informații de sănătate unui PHR bazat pe blockchain, care este echipat pentru a primi date în conformitate cu aceste standarde. Aceasta ar însemna că sistemul PHR bazat pe blockchain ar trebui să poată gestiona aceste protocoale de comunicare și să fie configurat să primească documente din diferite surse. Această funcționalitate este oarecum grea pentru un asemenea sistem, care este conceput ca un simplu registru electronic de tranzacții.
3. Pacienții continuă să primească informațiile despre sănătate prin portalurile existente ale pacienților și să încarce documentele la PHR bazat pe blockchain. Această metodă cu cel mai mic numitor comun va funcționa în toate cazurile, dar se bazează pe pasul suplimentar, manual al pacientului care acționează ca intermediar. În cel mai rău scenariu, acest lucru va conduce la înregistrări incomplete dacă pacientul nu completează pasul manual.

Opțiunea 3 este cel mai simplu scenariu și este cel mai ușor de implementat. Fiabilitatea celorlalte două opțiuni depinde de disponibilitatea furnizorilor de sisteme EHR.

Pentru alte sisteme decât EHR, situația este oarecum mai puțin clară. În mod conceptual, există modalități de împărțire a fluxului de date care iese din aceste sisteme și transmiterea unei copii către sistemul PHR bazat pe blockchain; cu toate acestea, aspectele economice și de reglementare implicate pot complica și întârzia implementarea acestor eforturi.

## Alte considerente

Un sistem de evidență a datelor privind sănătatea care se bazează în întregime pe tehnologia blockchain este posibil, dar nu este practicabil în viitorul apropiat. Strategia de punte a unui sistem PHR bazat pe blockchain alături de infrastructura actuală a datelor privind asistența medicală este mai realistă, totuși există obstacole și provocări semnificative care trebuie depășite.

Prima provocare este că în prezent nu există o infrastructură adecvată de blockchain pentru asistența medicală. Mai important, nu există un grup interesat care pare motivat să creeze unul. Pentru a stabili și menține o rețea de noduri, este necesar ca indivizii și organizațiile să-și dedice puterea de calcul. Nodurile care mențin blockchain-ul Bitcoin sunt recompensate prin faptul că sunt capabile să „*mineze*” noi bitcoins care sunt depozitați în contul proprietarului nodului.

*Ce i-ar motiva pe proprietarii de calculatoare să-și folosească puterea de procesare pentru a menține un blockchain de îngrijire medicală?*

O sugestie [20] ar fi ca nodurile care contribuie cu date în sistem ar furniza, de asemenea, puterea de calcul pentru a menține blockchain-ul de îngrijire a sănătății. Acest lucru este fezabil, dar dacă contribuabilii sunt spitalele și alte sisteme de sănătate, numărul total de noduri din rețea poate fi destul de mic. Un blockchain robust se bazează pe un număr mare de noduri independente. Acest lucru înseamnă, de asemenea, că autoritățile centrale care controlează în prezent silozurile de date ar rămâne responsabile de infrastructură, făcând să deraieze conceptul de încredere în rețea, existând un număr redus de autorități centrale care păstrează datele în siguranță. În cazul în care se va folosi arhitectura blockchain propusă de EOSIO, în care tranzacțiile sunt validare de către 21 *block producers* aleși prin vot, această problemă ar putea fi soluționată. Totuși va apărea o nouă problemă, și anume implicarea tuturor participanților sistemului în monitorizarea acestuia și alegerea unor block producers onești și eliminarea celor care au un comportament ilicit.

Un alt considerent este că infrastructura de tip blockchain care stochează datele trebuie să fie invizibilă pentru utilizatorii finali – atât pacienți, cât și furnizori de asistență medicală. Tehnologia de stocare trebuie să fie abstractizată de instrumentele pe care le folosește utilizatorul. Dacă un utilizator trebuie să ia pași suplimentari care consumă timp pentru a lucra cu datele și permisiunile din blockchain, adoptarea pe scară largă ar putea fi în pericol. Soluția acestei probleme a fost propusă în implementarea din capitolul precedent.

Performanța este o considerație tehnică majoră pentru orice soluție bazată pe blockchain. În funcție de detaliile implementării, efectuarea unui număr mare de tranzacții pe un blockchain poate fi foarte costisitoare în ceea ce privește timpul și puterea de procesare. Acest lucru înseamnă că performanța și scalabilitatea trebuie proiectate în soluția proiectată încă de la început.

# *Bibliografie*

1. Legislația privind confidențialitatea datelor medicale și a secretului medical <https://www.legmed.ro/doc/legislatie-confidentialitate.pdf>
2. Directiva UE. 95/46 / CE a Parlamentului European și a Consiliului din 24 octombrie 1995 privind protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal și libera circulație a acestor date. Jurnalul Oficial al CE. 1995; 23 (6) <https://papyrus.bib.umontreal.ca/xmlui/bitstream/handle/1866/9411/articles_198.html>
3. Baig MM, Li J, Liu J, Wang H. Clonarea pentru protecția vieții private în mai multe publicații de date independente. Lucrările celei de-a 20-a conferințe internaționale ACM privind managementul informațiilor și cunoștințelor - CIKM'11. 2011: 885. <https://dl.acm.org/citation.cfm?id=2063705>
4. Dubovitskaya A, Urovi V, Vasirani M, Aberer K, Schumacher MI. Progresele IFIP în tehnologia informației și comunicațiilor, SEC 2015. Springer Science and Business Media; 2015. O arhitectură e-health bazată pe cloud technology pentru protejarea confidențialității datelor. <https://ieeexplore.ieee.org/abstract/document/7163220>
5. Moore C, O'Neill M, O'Sullivan E, Doroz Y, Sunar B. Criptarea homomorfă practică: Un sondaj. 2014 Simpozionul Internațional IEEE pentru Circuite și Sisteme (ISCAS): 2792-2795. <https://ieeexplore.ieee.org/abstract/document/6865753>
6. O actualizare pe blogul oficial Google Health and Google PowerMeter [Internet] Google. 2017. [citat la 9 martie 2017]. <https://googleblog.blogspot.com/2011/06/update-on-google-health-and-google.html>
7. Azaria A, Ekblaw A, Vieira T, Lippman A. Medrec: Utilizarea tehnologiei blockchain pentru accesul la date medicale și gestionarea permisiunilor. A doua Conferință Internațională privind datele deschise și mari (*Open and Big Data*) 2016 Aug; 25-30. <https://ieeexplore.ieee.org/abstract/document/7573685>
8. Yue X, Wang H, Jin D, Li M, Jiang W. Healthcare data gateways: Found healthcare intelligence on blockchain with novel privacy risk control. Journal of Medical Systems. 2016;40(10):218. <https://www.ncbi.nlm.nih.gov/pubmed/27565509>
9. Beninger P, Ibara MA. Pharmacovigilance and biomedical informatics: a model for future development. Clinical Therapeutics. 2016 <https://www.ncbi.nlm.nih.gov/pubmed/27913029>
10. Adoptarea sistemelor electronice de înregistrare a sănătății în spitalele de îngrijire acută non-federală din SUA: 2008-2015 <https://dashboard.healthit.gov/evaluations/data-briefs/non-federal-acute-care-hospital-ehr-adoption-2008-2015.php>
11. Health Insurance Portability and Accountability Act <https://www.nytimes.com/2015/07/21/health/hipaas-use-as-code-of-silence-often-misinterprets-the-law.html?_r=0>
12. Interoperabilitatea între spitalele de îngrijire acută non-federală din SUA în 2015 <https://dashboard.healthit.gov/evaluations/data-briefs/non-federal-acute-care-hospital-interoperability-2015.php>
13. Doc Searls *“The Patient as the Platform”* 24 iunie 2008 <https://www.linuxjournal.com/content/patient-platform>
14. Breșe de securitate în sistemul EHR din SUA care au dus la scurgerea informațiilor de sănătate ale pacienților <https://dashboard.healthit.gov/quickstats/pages/breaches-protected-health-information.php>
15. Blockchain Technology: The Solution for Healthcare Interoperability <https://www.linkedin.com/pulse/blockchain-technology-solution-healthcare-peter-b-nichol>
16. Swanson T. Consensus-as-a-service: un scurt raport privind apariția sistemelor de registre autorizate și distribuite. 2015 <https://allquantor.at/blockchainbib/pdf/swanson2015consensus.pdf>
17. Sănătatea conectată <https://en.wikipedia.org/wiki/Connected_health>
18. EOS.IO Technical White Paper <https://github.com/EOSIO/Documentation/blob/master/TechnicalWhitePaper.md#actions--handlers>
19. IPFS Technical White Paper <https://github.com/ipfs/papers/raw/master/ipfs-cap2pfs/ipfs-p2p-file-system.pdf>
20. Evaluarea blockchain-ului pentru schimbul de informații privind sănătatea <http://geekdoctor.blogspot.com/2016/03/evaluating-blockchain-for-health.html>

# *Anexă*

## Lista figurilor

[Figura 1. Adoptarea de înregistrări electronice de sănătate în spitalele federale de îngrijire acută din SUA 7](file:///C:\Users\marin\Downloads\Licenta%20Final.docx#_Toc12566505)

[Figura 2. Numărul de persoane afectate de breșele de securitate în sistemele EHR din SUA [14] 8](file:///C:\Users\marin\Downloads\Licenta%20Final.docx#_Toc12566506)

[Figura 3. Diagrama cazurilor de utilizare pentru pacient 17](#_Toc12566507)

[Figura 4. Diagrama cazurilor de utilizare pentru doctor 17](#_Toc12566508)

[Figura 5. Diagrama de desfășurare a arhitecturii aplicației 18](#_Toc12566509)

[Figura 6. Diagrama de clase pentru starea interna a contractului inteligent 20](#_Toc12566510)

[Figura 7. Diagrama de activitate pentru adăugarea unei permisiuni 22](#_Toc12566511)

[Figura 8. Diagrama de activitate pentru modificarea unei permisiuni 23](#_Toc12566512)

[Figura 9. Diagrama de activitate pentru ștergerea unei permisiuni 24](#_Toc12566513)

[Figura 10. Diagrama de stări pentru permisiune 25](#_Toc12566514)

[Figura 11. Diagrama de activitate adăugare meta-date înregistrare medicală 26](#_Toc12566515)

[Figura 12. Diagrama de activitate consultare meta-date înregistrări medicale 27](#_Toc12566516)

[Figura 13. Diagrama de activitate ștergere meta-date înregistrare 28](#_Toc12566517)

[Figura 14. Schema bazei de date identități pacienți și medici 29](#_Toc12566518)

[Figura 15. Schema bazei de date utilizatori înregistrați 29](#_Toc12566519)

[Figura 16. Diagramă de activitate înregistrare utilizator 31](#_Toc12566520)

[Figura 17. Diagrama de interacțiune pentru operațiile cu permisiuni 32](#_Toc12566521)

[Figura 18. Diagrama de colaborare BPMN pentru adăugare înregistrare medicală 33](#_Toc12566522)

[Figura 19. Diagrama de interacțiune pentru adăugare înregistrare medicală 34](#_Toc12566523)

[Figura 20. Diagrama de interacțiune pentru citire listă înregistrări medicale 35](#_Toc12566524)

[Figura 21. Diagrama de interacțiune pentru consultare conținut înregistrare 36](#_Toc12566525)

[Figura 22. Raport grafic activitate doctor asupra dosarului medical 38](file:///C:\Users\marin\Downloads\Licenta%20Final.docx#_Toc12566526)

[Figura 23. Raport grafic activitate doctor asupra dosarului medical 38](file:///C:\Users\marin\Downloads\Licenta%20Final.docx#_Toc12566527)