

MINISTERUL EDUCAȚIEI NAȚIONALE



**UNIVERSITATEA TEHNICĂ**

DIN CLUJ-NAPOCA

**FACULTATEA DE AUTOMATICĂ ȘI CALCULATOARE**  
**DEPARTAMENTUL CALCULATOARE**

**Managementul studiilor clinice bazat pe tehnologia blockchain**

**LUCRARE DE LICENȚĂ**

Absolvent: **Alin Dan ȚANDEA**

Conducător științific: **asis. Ing. Cosmina Ivan**

**2018**

MINISTERUL EDUCAȚIEI NAȚIONALE



**UNIVERSITATEA TEHNICĂ**

DIN CLUJ-NAPOCA

**FACULTATEA DE AUTOMATICĂ ȘI CALCULATOARE  
DEPARTAMENTUL CALCULATOARE**

DECAN,  
Prof. dr. ing. Liviu MICLEA

DIRECTOR DEPARTAMENT,  
Prof. dr. ing. Rodica POTOLEA

Absolvent: **Alin Dan ȚANDEA**

**Managementul studiilor clinice bazat pe tehnologia blockchain**

1. **Enunțul temei:** *Scurtă descriere a temei lucrării de licență și datele inițiale*
2. **Conținutul lucrării:** *(enumerarea părților componente) Exemplu: Pagina de prezentare, aprecierile coordonatorului de lucrare, titlul capitolului 1, titlul capitolului 2, titlul capitolului n, bibliografie, anexe.*
3. **Locul documentării:** *Exemplu: Universitatea Tehnică din Cluj-Napoca, Departamentul Calculatoare*
4. **Consultanți:**
5. **Data emiterii temei:** 1 Noiembrie 2016
6. **Data predării:** 21 Februarie 2018 *(se va completa data predării)*

Absolvent: \_\_\_\_\_

Coordonator științific: \_\_\_\_\_





**UNIVERSITATEA TEHNICĂ**

DIN CLUJ-NAPOCA

**FACULTATEA DE AUTOMATICĂ ȘI CALCULATOARE  
DEPARTAMENTUL CALCULATOARE**

**Declarație pe proprie răspundere privind  
autenticitatea lucrării de licență**

Subsemnatul(a)

\_\_\_\_\_, legiti-  
mat(ă) cu \_\_\_\_\_ seria \_\_\_\_\_ nr. \_\_\_\_\_  
CNP \_\_\_\_\_, autorul lucrării \_\_\_\_\_

elaborată în vederea susținerii examenului de finalizare a studiilor de licență la Facul-  
tatea de Automatică și Calculatoare, Specializarea \_\_\_\_\_  
din cadrul Universității Tehnice din Cluj-Napoca, sesiunea \_\_\_\_\_ a an-  
ului universitar \_\_\_\_\_, declar pe proprie răspundere, că această lucrare este  
rezultatul propriei activități intelectuale, pe baza cercetărilor mele și pe baza informațiilor  
obținute din surse care au fost citate, în textul lucrării și în bibliografie.

Declar, că această lucrare nu conține porțiuni plagiate, iar sursele bibliografice au  
fost folosite cu respectarea legislației române și a convențiilor internaționale privind drep-  
turile de autor.

Declar, de asemenea, că această lucrare nu a mai fost prezentată în fața unei alte  
comisii de examen de licență.

În cazul constatării ulterioare a unor declarații false, voi suporta sancțiunile admin-  
istrative, respectiv, *anularea examenului de licență*.

Data

\_\_\_\_\_

Nume, Prenume

\_\_\_\_\_

Semnătura

**De citit înainte** (această pagină se va elimina din versiunea finală):

1. Cele trei pagini anterioare (foaie de capăt, foaie sumar, declarație) se vor lista pe foi separate (nu față-verso), fiind incluse în lucrarea listată. Foaia de sumar (a doua) necesită semnătura absolventului, respectiv a coordonatorului. Pe declarație se trece data când se predă lucrarea la secretarii de comisie.
2. Pe foaia de capăt, se va trece corect titulatura cadrului didactic îndrumător, în engleză (consultați pagina de unde ați descărcat acest document pentru lista cadrelor didactice cu titlaturile lor).
3. Documentul curent **nu** a fost creat în MS Office. E posibil să fie mici diferențe de formatare.
4. Cuprinsul începe pe pagina nouă, impară (dacă se face listare față-verso), prima pagină din capitolul Introducere tot așa, fiind numerotată cu 1.
5. Vizualizați (recomandabil și în timpul editării) acest document
6. Fiecare capitol începe pe pagină nouă.
7. Folosiți stilurile predefinite (Headings, Figure, Table, Normal, etc.)
8. Marginile la pagini nu se modifică.
9. Respectați restul instrucțiunilor din fiecare capitol.

# Cuprins

<b>Capitolul 1</b>	<b>Introducere - Contextul proiectului</b>	<b>11</b>
1.1	Contextul proiectului . . . . .	11
1.1.1	Subsection . . . . .	11
<b>Capitolul 2</b>	<b>Obiectivele Proiectului</b>	<b>13</b>
2.1	Titlu . . . . .	13
2.2	Alt titlu . . . . .	13
<b>Capitolul 3</b>	<b>Studiu Bibliografic</b>	<b>14</b>
3.1	Blockchain . . . . .	14
3.1.1	Structura de date . . . . .	14
3.1.2	Topologia rețelei . . . . .	15
3.1.3	Funcții de hash si criptografie . . . . .	16
3.1.4	Mecanism de consens . . . . .	16
3.1.5	Smart contract . . . . .	18
3.1.6	Implementari ale tehnologiei blockchain . . . . .	18
3.2	Scenarii de utilizare ale tehnologiei blockchain . . . . .	19
3.2.1	Determinarea identitatii digitale . . . . .	19
3.2.2	Trasarea provenientei produselor . . . . .	20
3.3	Tehnologia blockchain in studiile clinice . . . . .	20
3.3.1	Motivatie . . . . .	20
3.3.2	Modelarea cercetarii clinice sub forma unei retele de afaceri . . . . .	20
<b>Capitolul 4</b>	<b>Analiză și Fundamentare Teoretică</b>	<b>23</b>
4.1	Analiza sistem . . . . .	23
4.1.1	Cerinte functionale . . . . .	23
<b>Capitolul 5</b>	<b>Proiectare de Detaliu și Implementare</b>	<b>25</b>
<b>Capitolul 6</b>	<b>Testare și Validare</b>	<b>26</b>
6.1	Titlu . . . . .	26
6.2	Alt titlu . . . . .	26

<b>Capitolul 7</b>	<b>Manual de Instalare și Utilizare</b>	<b>27</b>
7.1	Titlu . . . . .	27
7.2	Alt titlu . . . . .	27
<b>Capitolul 8</b>	<b>Concluzii</b>	<b>28</b>
8.1	Titlu . . . . .	28
8.2	Alt titlu . . . . .	28
<b>Bibliografie</b>		<b>29</b>
<b>Anexa A</b>	<b>Secțiuni relevante din cod</b>	<b>30</b>
<b>Anexa B</b>	<b>Alte informații relevante (demonstrații etc.)</b>	<b>31</b>
<b>Anexa C</b>	<b>Lucrări publicate (dacă există)</b>	<b>32</b>

# Capitolul 1

## Introducere - Contextul proiectului

Titlul capitolului se bazează pe Heading 1 style, numerotat cu o cifra (x. Nume capitol), font Times New Roman de 14, Bold.

Ce se scrie aici:

- Contextul
- Conturarea domeniului exact al temei
- Reprezintă cca. 5% din lucrare

### 1.1 Contextul proiectului

Fontul folosit implicit în acest document este Times New Roman, dimensiune de 12, conform Normal style, cu spațiere la 1 rând (Paragraph, Line spacing de 1.0) și Justify. Pentru prima linie din fiecare paragraf se folosește indentare (implicit în Normal Style), iar între paragrafe succesive nu se lasă distanță suplimentară<sup>1</sup>.

#### 1.1.1 Subsection

Fiecare tabel introdus în lucrare este numerotat astfel: Tabel x.y, unde x reprezintă numărul capitolului iar y numărul tabelului din capitol. Se lasă un rând liber între tabel și paragraful anterior, respectiv posterior (table 1.1).

Fiecare figură introdusă în text este citată (de ex: în figura x.y este prezentată ...) și numerotată. Numerotarea se face astfel Figura x.y unde x reprezintă numărul capitolului iar y numărul figurii în acel capitol. E.g.: figure 1.1.

Fiecare capitol începe pe pagină nouă.

---

<sup>1</sup>Sunt rezolvate automat de Latex



Tabelul 1.1: Rezultate

Case	Method#1	Method#2	Method#3
1	50	837	970
2	47	877	230
3	31	25	415

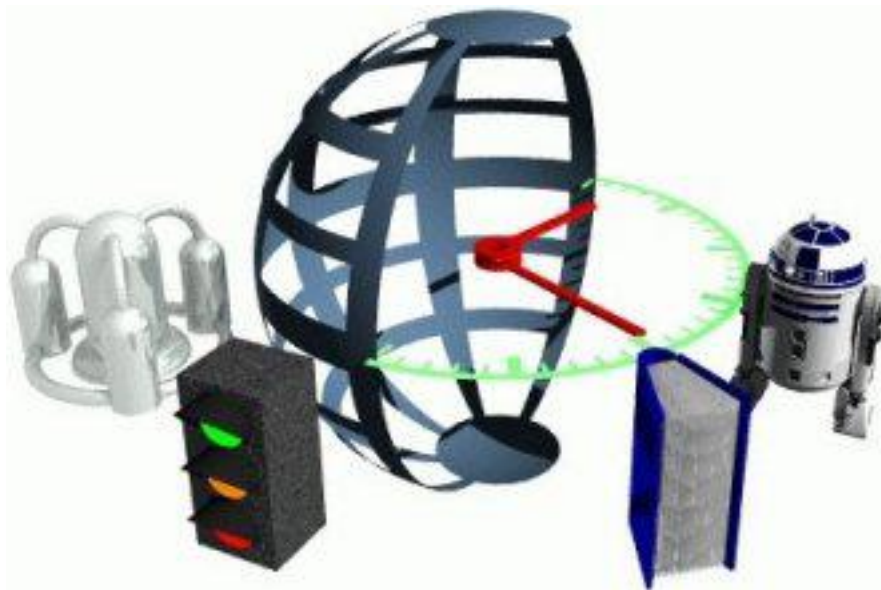


Figura 1.1: Numele figurii

# Capitolul 2

## Obiectivele Proiectului

În acest capitol se prezintă tema propriu-zisă (sub forma unei teme de proiectare sau cercetare, formulată exact, cu obiective clare - 2-3 pagini și eventuale figuri explicative).  
Reprezintă cca. 10% din lucrare.

**2.1 Titlu**

**2.2 Alt titlu**

# Capitolul 3

## Studiu Bibliografic

În acest capitol sunt prezentate o serie de concepte și tehnologii necesare pentru o mai bună înțelegere a temei alese și a modului în care au fost utilizate pentru implementarea acesteia. Capitolul continuă prin descrierea aplicării acestor concepte în anumite domenii precum și în domeniul studiilor clinice. Sunt prezentate unele beneficii aduse de aceste tehnologii, alături de o comparație a implementărilor existente ale acesteia.

### 3.1 Blockchain

Termenul de blockchain a devenit cunoscut odată cu creșterea în popularitate a monedelor virtuale, în special a monedei virtuale Bitcoin. O rețea blockchain poate fi definită ca fiind o bază de date distribuită, întreținută de o serie de participanți care validează înregistrările din cadrul rețelei folosind o comunicare de tip peer-to-peer. Înregistrările din cadrul rețelei sunt securizate prin metode criptografice care asigură imutabilitatea datelor. Rezolvarea conflictelor care pot apărea între înregistrările din rețea are loc prin utilizarea unor algoritmi de consens. Această secțiune analizează următoarele aspecte ale tehnologiei: structura de date, aspecte legate de criptografie, topologia rețelei, algoritmi de consens, smart contracts, permisiuni și implementări ale tehnologiei.

#### 3.1.1 Structura de date

Structura de date folosită reprezintă unul dintre mijloacele care asigură integritatea datelor din rețeaua blockchain. Documentația monedei virtuale Bitcoin descrie structura de date folosită ca fiind o listă invers înlantuită în care fiecare element, numit bloc, conține hash-ul blocului anterior, un timestamp și radacina Merkle a tranzacțiilor, folosită pentru a verifica integritatea acestora. Figura 3.1 prezintă structura de date folosită de Bitcoin[1].

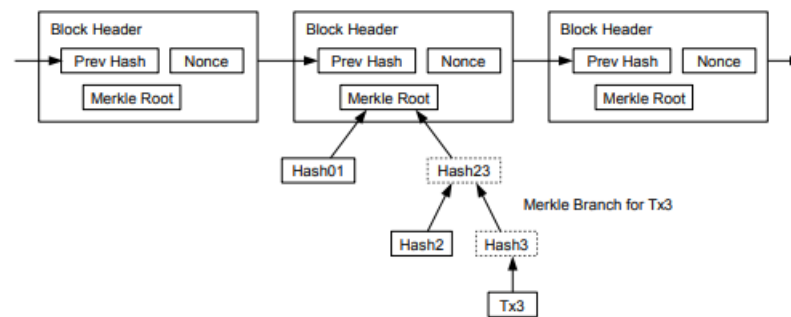


Figura 3.1: Cel mai lung lanț proof-of-work folosit de Bitcoin[1]

Fiecare bloc din structura de date este identificat prin funcția hash a header-ului blocului curent și a blocului anterior. Conceptul implementat de moneda virtuală Bitcoin este urmat de alte implementări care au adus unele modificări acestei structuri, dar păstrează unele concepte de bază introduse de Bitcoin.

### 3.1.2 Topologia rețelei

O caracteristică importantă a unei rețele blockchain este lipsa unei autorități centrale care să intermedieze tranzacțiile din cadrul rețelei. Pentru validarea și propagarea tranzacțiilor este folosită o rețea peer-to-peer de participanți[2]. În cadrul unei astfel de rețele fiecare participant are aceleași responsabilități și privilegii, spre deosebire de o topologie client-server unde rețeaua are un nod central cu capacități și responsabilități diferite față de clienții din rețea. Figura 3.2 ilustrează diferența dintre cele două topologii.

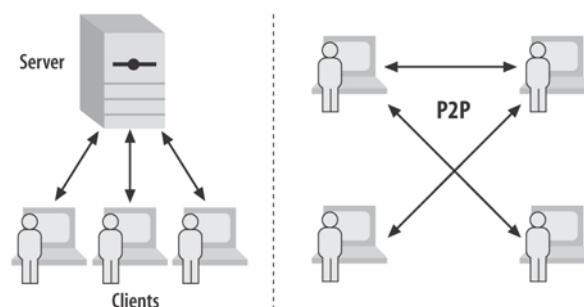


Figura 3.2: Rețea client-server vs peer-to-peer[3]

Fiecare peer deține o copie a informațiilor din rețea. Acest lucru face dificilă modificarea abuzivă a datelor, orice modificare fiind vizibilă pentru ceilalți participanți.

### 3.1.3 Funcții de hash si criptografie

O functie de hash reprezinta o metoda unidirectionala de mapare a unui sir de caractere de lungime arbitrara la un sir de caractere cu lungime fixa. Proprietatile necesare pentru o functie de hash sunt:

- Calcul rapid: efortul computational pentru calcularea rezultatului trebuie sa fie mic indiferent de sirul de intrare.
- Unidirectionala: obtinerea sirului original din hash nefezabila
- Determinista: rezultatul pentru un anumit sir de intrare este acelasi indiferent de cate ori este calculat.
- Rezistent la coliziuni: oricare ar fi sirurile de intrare  $a, b$  functia de hash  $h(a) = h(b)$  doar daca  $a = b$ . Cu alte cuvinte un sir de intrare produce intotdeauna un rezultat unic.
- Schimbarile mici din sirul de intrare produc schimbari majore in rezultatul functiei de hash

Printre algoritmi de hash folositi de diferitele implementari ale tehnologie blockchain se numara SHA256(Bitcoin) sau Keccak-256(Ethereum). Aceste functii sunt folosite si de catre algoritmi pentru stabilirea consensului.

Pentru controlarea accesului in retea blockchain este folosita metoda de criptografie cu cheie publica. Aceasta presupune folosirea unei perechi de chei formata dintr-o cheie privata si o cheie publica, derivata din cheia privata. Pentru autorizarea tranzactiilor este folosita partea privata a cheii. Identitatea unui utilizator este data de partea publica a cheii.

### 3.1.4 Mecanism de consens

O proprietate importanta a unei retele blockchain este lipsa unei autoritati centrale care sa valideze tranzactiile efectuate de participanti. Din aceasta cauza apare nevoia existentei unor mecanisme responsabile de rezolvarea conflictelor care apar in cadrul retelei intre inregistrarile detinute de participantii din retea. Algorimii de consens cei mai folositi sunt: Proof of Work(PoW) si Bizantine Fault Tolerance(BFT).

PoW este algoritmul aflat in spatele unor monede virtuale precum Bitcoin si Ethereum. Algoritmul este conceput sub forma unei competitii in care participantii din retea isi folosesc puterea de calcul pentru rezolvarea unei probleme. Primul participant care rezolva problema primeste dreptul de a crea urmatorul bloc din structura de date alaturi de o anumita recompensa. Rezolvarea problemei presupune efort masiv de calcul si din acest motiv este folosita drept masura de siguranta. Pentru a modifica intrarile deja salvate in blockchain un atacator are nevoie de mai mult de 50% din puterea de calcul a intregii retele,

un astfel de atac fiind nefezabil. In acest mod este asigurata corectitudinea informatiilor insa metoda folosita este ineficienta.

BFT asigura ajungerea la consens in cazul in care o parte din participantii sunt atacatori. Un algoritm pentru problema cunoscuta sub numele de "Problema generalilor bizantini" a fost implementat in anul 1999 Miguel Castro and Barbara Liskov sub numele de Practical Byzantine Fault Tolerance(PBFT). Algoritmul incearca ajungerea la un consens in cadrul sistemului, pastrand in acelasi timp o latenta scazuta si eficienta ridicata. Pasii algoritmului sunt urmatoarii:

- Un client trimite o cerere
- Cererea este transmisa celorlalti clienti
- Ceilalti clienti executa cererea si transmit raspunsul clientului care a initiat cererea
- Clientul asteapta pana cand primeste  $F + 1$  raspunsuri identice, unde  $F$  este numarul maxim de noduri malitioase tolerate

Conditia pentru functionarea corecta a sistemului este ca numarul de noduri malitioase din sistem sa fie mai mic decat  $1/3$  din numarul total de noduri din sistem.

O comparatie la nivel inalt a celor doua mecanisme de stabilire a consensului este prezentata in tabelul 3.1. Tabelul prezinta o comparatie a celor doi algoritmi luand in considerare unele proprietati importante ale unei retele blockchain: identitatea nodurilor, performanta, scalabilitatea, rezistenta la atacuri sau puterea consumata.

Tabelul 3.1: Comparatie la nivel inalt: PoW vs BFT

	Proof of Work	Byzantine Fault Tolerance
Managementul identitatii nodurilor	deschis, decentralizat	fiecare nod trebuie sa cunoasca informatii despre celelalte noduri
Scalabilitate	excelenta	limitata
Performanta(throuput)	limitata	excelenta(mii de tranzactii/sec)
Performanta(latenta)	latenta crescuta	excelenta(similara cu cea indusa de retea)
Putere consumata	Ridicata(PoW necesita putere de calcul ridicata)	Scazuta
Numar total de atacatori tolerati	<25% din puterea de calcul	<33% din numarul de noduri care voteaza

Se poate observa faptul ca algoritmi reprezinta doua abordari diferite in cadrul unei retele blockchain. PoW pune accent pe scalabilitate dar prezinta o performanta scazuta

in tim ce BFT asigura performanta ridicata dar cu o scalabilitate redusa. Decizia in ce priveste tipul de algoritm folosit depinde de nevoia sistemelor implementate.

### 3.1.5 Smart contract

Un smart contract reprezinta "un set de promisiuni in format digital in care partile implicate actioneaza conform acestor promisiuni". Altfel spus aceste contracte sunt o reprezentare digitala a unor clauze contractuale, integrate in software pentru a media actiuni prin operatii bazate pe reguli. Odata ce preconditionile pentru un smart contract sunt indeplinite si acesta este initiat actiunile din cadrul lui sunt executate, ele fiind irevocabile.

### 3.1.6 Implementari ale tehnologiei blockchain

Prima implementare cu succes a tehnologiei blockchain a fost realizata de moneda virtuala bitcoin. Odata cu cresterea acesteia in popularitate au aparut diverse implementari ale acestei tehnologii, fiecare avand unele particularitati si scopuri de utilizare diferite.

Tipuri de implementari. Exista 3 tipuri de implementari ale tehnologiei blockchain: public, privat si bazat pe permisiuni. Tabelul 3.2 prezinta o analiza la nivel inalt a celor 3 tipuri de implementari. Sunt luate in considerare aspecte precum drepturile de acces, performanta, costurile implicate, avantajele si dezavantajele fiecarei implementari precum si numarul de puncte de esec in cazul fiecareia.

Blockchain public. In cadrul unu blockchain public nu exista nevoia definirii unor drepturi de acces. Orice entitate are drepturi de acces egale in cadrul retelei si poate participa la procesul de validare a tranzactiilor. Din acest punct de vedere un blockchain public foloseste o topologie decentralizata nefiind prezenta o autoritate centrala care sa medieze tranzactiile din retea. O astfel de implementare este folosita de catre monedele virtuale Bitcoin sau Ethereum. In cadrul acestor retele participante efectueaza tranzactii fara a fi implicata a treia entitate in acest proces. Pentru a se ajunge la un consens, un mecanism de tip PoW este folosit, acesta avand un impact asupra performantei retelei si a consumului de enegie.

Blockchain privat. Spre deosebire de un blockchain public, cel privat foloseste o topologie centralizata. Accesul la retea este controlat de o autoritate centrala, aceasta avand dreptul de a lua decizii si de a implementa reguli in cadrul retelei. Un astfel de blockchain poate fi folosit in cazul in care este necesara restrictionarea accesului publicului larg la retea. O astfel de retea se bazeaza pe stabilirea unui nivel ridicat de incredere in autoritatea centrala responsabila de administrarea retelei. Deoarece doar o singura entitate este responsabila de procesul de validare a tranzactiilor, apare avantajul performantei crescute in comparatie cu un blockchain public.

Blockchain bazat pe permisiuni. Acesta abordare poate fi vazuta ca n hibrid intre un blockchai privat si unul public. Autoritatea in retea este detinuta de un set de entitati care pot face parte din organizatii diferite. Aceste entitati stabilesc drepturile de acces la retea si rparticipa la validarea tranzactiilor. Drepturile de acces depind de identitatile

Tabelul 3.2: Comparatie la nivel inalt a implementarilor tehnologiei blockchain

	Public	Privat	Bazat pe permisiuni
Topologie retea	decentralizata	partial decentralizata	partial decentralizata
Definire	Oricine are acces la datele din retea. Toate nodurile participa la validare	Permisunile de acces sunt controlate de o singura entitate de incredere din retea	Permisunile de acces sunt controlate de un numar prestabilit de noduri cu autoritate
Beneficii	- Sigur, deoarece toti participantii contribuie la validarea tranzactiilor - Transparent, toate tranzactiile fiind publice iar entitatile implicate anonime	- Verificare eficienta a tranzactiilor de catre autoritatea centrala - Autoritatea centrala decide entitatile care au acces la retea	- Eficient, deoarece un numar relativ mic de noduri verifica tranzactiile - Drepturile de acces sunt controlate de un set predeterminat de noduri - Controlul nu este detinut de catre o autoritate centrala
Provocari	Eficienta scazuta	Controlul este detinut de o singura entitate	
Cost	scazut	ridicat	mediu
Performanta	scazuta	excelenta	ridicata
Puncte de esec	n	1	* (nodurile cu autoritate)

participantilor, fiind nevoie de executarea unor smart contracts inainte de executarea unor tranzactii pentru validarea identitatii participantilor. Hyperledger Fabric si Corda sunt implementari ale unui astfel de blockchain. Ambele sunt solutii open-source care pot fi folosite pentru stocarea si partajarea datelor intre participantii retelei.

## 3.2 Scenarii de utilizare ale tehnologiei blockchain

Sectiunea curenta descrie unele sisteme existente care au la baza implementarii lor tehnologia blockchain. Capitolul prezinta motivatia alegerii tehnologiei blockchain precum si avantajele aduse de aceasta in sistemele implementate

### 3.2.1 Determinarea identitatii digitale

In lucrarea [cite here] autorul incearca obtinerea un sistem pentru managementul identitatii digitale a utilizatorilor care sa aiba urmatoarele proprietati:

- **Existenta** : entitatile trebuie sa existe independent, nu doar in mediul digital
- **Control**: o entitate are controlul absolut asupra identitatii proprii



- **Transparenta:** sistemele care mentin actualizata identitatea trebuie sa realizeze aceasta in mod transparent
- **Portabilitate :** identitatea trebuie sa fie transportabila
- **Consimtamant :** entitatile trebuie sa fie de acord cu partajarea informatiilor personale inainte de efectuarea acesteia.

Lucrarea propune un sistem decentralizat bazat pe tehnologia blockchain pentru managementul identitatii consumatorilor, fiind implicate institutiile care emit identitatea si cele care se folosesc de aceasta. Beneficiile aduse de utilizarea tehnologiei blockchain in acest sistem sunt: schimbul decentralizat de informatii legate de identitatea unei persoane, partajarea informatiilor doar cu acordul clientului care detine identitatea, independenta fata de entitatea care a emis o anumita informatie legata de identitatea unui client.

### 3.2.2 Trasarea provenientei produselor

Lucrarea [cite here] prezinta un sistem care are ca scop urmarirea distributiei, originii si a starii curente a produselor intr-un mediu complex care implica un numar ridicat de participanti din diferite organizatii. Solutia propusa foloseste framework-ul Hyperledger Fabric pentru implementarea unei retele decentralizate care sa faciliteze si sa imbunatateasca transparenta si posibilitatea de urmarire a originii produselor.

## 3.3 Tehnologia blockchain in studiile clinice

Tehnologia blockchain poate avea un impact global asupra cercetarii clinice deoarece permite urmarirea, partajarea si protectia informatiilor. Prin utilizarea unui sistem decentralizat folosit pentru urmarirea activitatilor din cadrul unui studiu clinic si a unei retele peer-to-peer pentru partajarea informatiilor sunt asigurate transparenta si protectia datelor personale ale pacientilor. Un sistem bazat pe aceasta tehnologie poate imbunatati metodologiile din cercetarea clinica si protectia datelor cu caracter sensibil.

### 3.3.1 Motivatie

### 3.3.2 Modelarea cercetarii clinice sub forma unei retele de afaceri

O **retea de afaceri** reprezintă o rețea complexă de companii ”unde scopul este de a susține cerintele informationale și operaționale ale afacerii cum ar fi cele de marketing, contabilitate ...”[4]. Un alt aspect important al unei retele de afaceri este ca aceasta nu inglobeaza doar afacerea in sine ci implică și unele entitati din exterior care susțin activitatea rețelei cum ar fi furnizorii sau distribuitorii.

În cazul studiilor clinice o rețea de afaceri poate fi formată din participanții direcți la activități(ex. centrele medicale în care se desfășoară studiile clinice), precum și partile care susțin activitatea studiilor clinice(ex. furnizori, instituții de reglementare...) Rețelele existente de afaceri folosesc în prezent metode similare pentru stocarea informațiilor. Entitățile implicate tranzacționează între ele, însă mențin înregistrări proprii referitoare la tranzacțiile efectuate. În cele mai multe cazuri o autoritate centrală în care toate partile implicate au încredere intermediază tranzacțiile și schimbul de informații din cadrul rețelei. Conceptul descris mai sus este ilustrat în figura 3.3.



Figura 3.3: Rețele de afaceri centralizate[3]

Această metodă prezintă o complexitate redusă dar produce în același timp unele dezavantaje. Partajarea informațiilor este efectuată indirect, responsabilă de acest lucru fiind autoritatea centrală. Din acest motiv procesul este încetinit, implicând costuri suplimentare. Stabilirea corectitudinii informațiilor devine dificilă în momentul în care partile implicate dețin înregistrări diferite referitoare la tranzacții. Printre sistemele care folosesc o astfel de abordare se numără Oracle Siebel Clinical Trial Management System[5]. Sistemul oferă posibilitatea cercetătorilor de a organiza și colecta date în cadrul unui studiu clinic, fiind astfel simplificată activitatea acestora. Datele sunt colectate într-o bază de date centrală. Partajarea datelor între participanți are loc fie prin implicarea unei autorități centrale, fie prin folosirea unor mijloace nesigure. Aceste mijloace sunt inefficiente și reprezintă un risc în ce privește protejarea datelor cu caracter sensibil.

**Rețele de afaceri decentralizate.** O altă abordare pentru realizarea unei rețele de afaceri reprezintă utilizarea unei rețele decentralizate. O astfel de metodă presupune folosirea unui registru comun, replicat de către fiecare participant din rețeaua de afaceri.

Procesul de salvare a tranzactiilor in cadrul registrului este de asemenea partajat, fiecare participant la retea participand la procesul de validare si memorare a tranzactiilor efectuate. Este eliminata astfel nevoia unei autoritati centrale, partile implicate avand incredere ca tranzactiile salvate in registrul comun sunt valide.

Figura 3.4 ilustreaza structura unei retele de afaceri decentralizate. O astfel de retea este similara cu o retea blockchain.

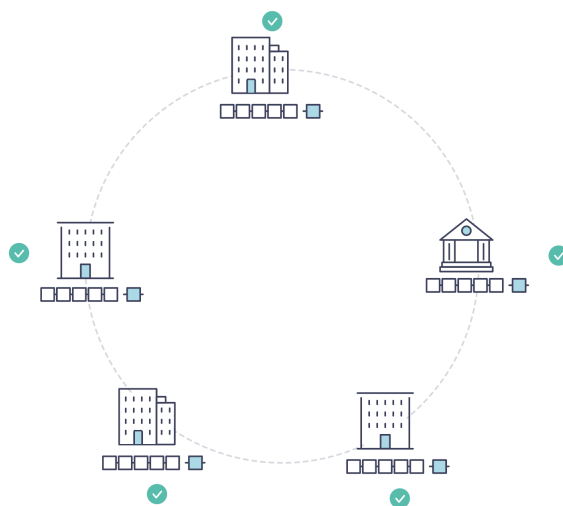


Figura 3.4: Rețele de afaceri decentralizate[3]

# Capitolul 4

## Analiză și Fundamentare Teoretică

Acest capitol prezintă tehnologiile folosite pentru realizarea unei aplicații decentralizate pentru managementul studiilor clinice.

### 4.1 Cerințe sistem

Secțiunea prezintă o analiză a sistemului pentru managementul studiilor clinice. Cerințele unui sistem pot fi clasificate în cerințe functionale și non-functionale. Cerințele functionale descriu comportamentul sistemului din punctul de vedere al utilizatorilor. Cerințele non-functionale

#### 4.1.1 Cerințe functionale

În continuare sunt prezentate cerințele functionale îndeplinite de modulul client al aplicației. Aceste functionalități sunt disponibile pentru utilizatorii sistemului:

1. **Autentificare:** Accesul la funcționalitățile aplicației este disponibil doar pentru utilizatorii autentificați. Identitatea utilizatorului are o importanță majoră în cadrul rețelei blockchain. În acest mod este asigurată posibilitatea urmăririi activității participanților și salvarea unui istoric a tuturor operațiilor efectuate de aceștia.
2. **Emitere identitate:** Utilizatorii autentificați au nevoie de o identitate emisă de organizația din care fac parte pentru a putea accesa rețeaua. Cu ajutorul acesteia utilizatorii sunt identificați în rețeaua blockchain și supuși regulilor de acces la resurse definite în sistem.
3. **Creare studiu clinic:** Utilizatorii au posibilitatea de a crea un nou studiu clinic folosind interfața utilizator după introducerea informațiilor necesare.
4. **Vizualizare studiu clinic:** Oferă posibilitatea utilizatorilor autentificați care au drepturile de acces necesare să acceseze informațiile despre un studiu clinic și datele legate de activitatea desfășurată în cadrul acestora.

5. **Inrolare pacienti:** Posibilitatea de a asocia un pacient la un studiu clinic.
6. **Definire formulare:** Cercetatorii pot defini in cadrul unui studiu clinic formulare de colectare a datelor de la pacienti. Aceste formulare ofera cercetatorului flexibilitatea de a defini campuri de text si intrebari cu variante de raspuns relevante pentru studiul clinic.
7. **Colectare date:** Folosind formularele definite, cercetatorii au posibilitatea de a colecta date de la un anumit pacient.
8. **Management drepturi de acces:** Administratorul unui studiu clinic defineste drepturile de citire sau scriere a utilizatorilor pentru studiul clinic de care este responsabil
9. **Management fisier protocol:** Protocolul unui studiu clinic descrie modul de desfasurare al unui studiu clinic. Utilizatorii care detin drepturile de acces necesare pot incarca un fisier de protocol si il pot descarca prin intermediul interfetei utilizator

# Capitolul 5

## Proiectare de Detaliu și Implementare

Împreună cu capitolul precedent reprezintă aproximativ 60% din total.

Scopul acestui capitol este de a documenta aplicația dezvoltată în așa fel încât dezvoltarea și întreținerea ulterioară să fie posibile. Cititorul trebuie să identifice funcțiile principale ale aplicației din ceea ce este scris aici. Capitolul ar trebui să conțină (nu se rezumă neapărat la):

- schema generală a aplicației
- descrierea fiecărei componente implementate, la nivel de modul
- diagrame de clase, clase importante și metode ale claselor importante.

# Capitolul 6

## Testare și Validare

Aproximativ 5% din total

**6.1 Titlu**

**6.2 Alt titlu**

# Capitolul 7

## Manual de Instalare și Utilizare

În secțiunea de Instalare trebuie să detaliați resursele software și hardware necesare pentru instalarea și rularea aplicației, precum și o descriere pas cu pas a procesului de instalare. Instalarea aplicației trebuie să fie posibilă pe baza a ceea ce se scrie aici.

În acest capitol trebuie să descrieți cum se utilizează aplicația din punct de vedere al utilizatorului, fără a menționa aspecte tehnice interne. Folosiți capturi ale ecranului și explicații pas cu pas ale interacțiunii. Folosind acest manual, o persoană ar trebui să poată utiliza produsul vostru.

### 7.1 Titlu

### 7.2 Alt titlu



# Capitolul 8

## Concluzii

Cca. 5% din total. Capitolul ar trebui sa conțină (nu se rezumă neapărat la):

- un rezumat al contribuțiilor voastre
- analiză critică a rezultatelor obținute
- descriere a posibilelor dezvoltări și îmbunătățiri ulterioare

### 8.1 Titlu

### 8.2 Alt titlu

# Bibliografie

- [1] S. Nakamoto, “Bitcoin: A peer-to-peer electronic cash system,” <http://bitcoin.org/bitcoin.pdf>.
- [2] A. Davison, *Killer Game Programming in Java*. Oeilly Media, Inc., 2005.
- [3] Hyperledger. (2018) Hyperledger Fabric documentation. [Online]. Available: <http://hyperledger-fabric.readthedocs.io/en/latest/>
- [4] L. Lewis, *Managing Business and Service Networks*. Norwell, MA, USA: Kluwer Academic Publishers, 2001.
- [5] G. W. Fegan and T. A. Lang, “Could an open-source clinical trial data-management system be what we have all been looking for?” *PLOS Medicine*, vol. 5, no. 3, pp. 1–3, 03 2008. [Online]. Available: <https://doi.org/10.1371/journal.pmed.0050006>

# Anexa A

## Secțiuni relevante din cod

```
/** Maps are easy to use in Scala. */
object Maps {
  val colors = Map("red" -> 0xFF0000,
                   "turquoise" -> 0x00FFFF,
                   "black" -> 0x000000,
                   "orange" -> 0xFF8040,
                   "brown" -> 0x804000)

  def main(args: Array[String]) {
    for (name <- args) println(
      colors.get(name) match {
        case Some(code) =>
          name + " has code: " + code
        case None =>
          "Unknown color: " + name
      }
    )
  }
}
```

## Anexa B

Alte informații relevante  
(demonstrații etc.)

## **Anexa C**

**Lucrări publicate (dacă există)**