



UNIVERSITATEA DIN  
BUCUREŞTI



FACULTATEA DE  
MATEMATICA ŞI  
INFORMATICA

PROGRAM DE STUDIU SISTEME DISTRIBUITE

Lucrare de disertație

TEHNOLOGIILE ETHEREUM,  
FLUTTER, SOLIDITY, WEB3DART  
ŞI FIREBASE CU APLICAȚII ÎN  
SISTEMELE DE VOT  
DECENTRALIZATE

Absolvent

Urmă Tudor-Irinel

Coordonator științific  
Conf.dr. Kevorchian Cristian

Bucureşti, iulie 2024

## **Rezumat**

Această lucrare de disertație are scopul de a prezenta potențialul pe care îl oferă tehnologia blockchain în integrarea unui sistem de vot securizat, accesibil, transparent și de încredere, și să propună, în urma investigațiilor, o proiectare, iar mai apoi o implementare, a unei aplicații mobile capabilă să îndeplinească cerințele unui astfel de sistem. Evoluția tehnologiei reușește să ofere accesibilitate pentru utilizatorii dornici să o folosescă, astfel, prin prisma internetului se pot desfășura procese electorale unde alegătorii pot vota indiferent de locația la care se află. Acest lucru vine cu anumite vulnerabilități cum ar fi securitatea, frauda, manipularea, indisponibilitatea și încrederea. Aici, tehnologia blockchain vine ca o extensie, datorită naturii sale imuabile, transperente și descentralizate. Aceste aspecte pot spori încrederea alegătorilor, fapt ce poate rezulta într-o creștere semnificativă în numărul participanților la vot. Viitoare cercetări sunt necesare pentru a găsi soluții scalabile în alegeri electorale de marimi ridicate.

## **Abstract**

This dissertation aims to present the potential of blockchain technology in implementing a secure, accessible, transparent, and reliable e-voting system, and to propose, after investigation, a design, followed by an implementation, for a mobile application capable of meeting the requirements for such a system. The technology advancement succeeds in providing accessibility for the user, thus, making e-voting systems possible where voters can cast their vote remotely. Multiple vulnerabilities come with these opportunities, like security, fraud, tampering, faulting, and reliability. Here, blockchain technology comes to the rescue using its immutable, transparent, and decentralized nature. This aspect can raise the voter's trust, which can lead to a substantial increase in vote participation. Future work is mandatory to find scalable solutions in large electoral contexts.

# Cuprins

<b>1 Motivație</b>	<b>7</b>
<b>2 Introducere</b>	<b>8</b>
2.1 Prezentare generală . . . . .	8
2.2 Contextul aplicației . . . . .	8
2.3 Obiective . . . . .	8
<b>3 Votul în ascensiunea lui</b>	<b>9</b>
3.1 Primele forme de votare . . . . .	9
3.2 Votul modern . . . . .	9
3.3 Era digitală și tehnologia blockchain . . . . .	10
<b>4 Blockchain</b>	<b>11</b>
4.1 Istorie . . . . .	11
4.2 Prezentare generală . . . . .	11
4.3 Tipuri de rețele . . . . .	13
4.4 Utilizări . . . . .	14
4.5 Contracte Inteligente . . . . .	14
4.6 Portofel . . . . .	14
<b>5 Sistemele de vot electronice</b>	<b>15</b>
5.1 Tipuri de sisteme . . . . .	15
5.2 Caracteristici . . . . .	16
5.3 Blockchain și Contractele Inteligente . . . . .	16
<b>6 Sistemele de vot bazate pe blockchain</b>	<b>18</b>
6.1 Implementări realizate și studii de caz . . . . .	18
6.1.1 Studii de caz . . . . .	18
6.1.2 Studii de caz cu implementări . . . . .	22
6.1.3 Implementări . . . . .	23
6.2 Analiză finală . . . . .	25
6.2.1 Tehnologii și terminologii . . . . .	25

6.2.2	Cerințe . . . . .	26
6.2.3	Contribuțiile sistemelor de vot bazate pe blockchain . . . . .	27
6.2.4	Provocări și Limitări . . . . .	28
<b>7</b>	<b>Sistem propus</b>	<b>29</b>
7.1	Structură . . . . .	29
7.2	Interfață . . . . .	29
7.3	Procesare a datelor . . . . .	30
7.4	Logică . . . . .	30
7.5	Integrarea secțiunilor . . . . .	31
7.6	Flux de date . . . . .	32
<b>8</b>	<b>Tehnologii Folosite</b>	<b>33</b>
8.1	Ethereum . . . . .	33
8.2	Sepolia . . . . .	33
8.3	Web3 . . . . .	33
8.4	Solidity . . . . .	34
8.5	Remix IDE . . . . .	34
8.6	MetaMask . . . . .	34
8.7	Infura . . . . .	35
8.8	Dart . . . . .	35
8.9	Flutter . . . . .	35
8.10	Firebase . . . . .	36
8.11	Microsoft Azure Face Api . . . . .	37
8.12	Google Cloud Secret Manager . . . . .	37
8.13	Web3Dart . . . . .	37
8.14	NewsApi . . . . .	37
8.15	Python . . . . .	37
8.16	Google Colab . . . . .	38
<b>9</b>	<b>Arhitectura aplicației</b>	<b>39</b>
9.1	Diagrame C4 . . . . .	40
9.1.1	Nivel 1 . . . . .	40
9.1.2	Nivel 2 . . . . .	41
9.1.3	Nivel 3 . . . . .	41
9.1.4	Nivel 4 . . . . .	42
9.2	Firebase Database . . . . .	50
9.3	Firebase Storage . . . . .	52
9.4	Firebase Authentication . . . . .	52
9.5	Google Cloud Secret Manager . . . . .	53

9.6	Flutter Application . . . . .	53
9.6.1	Model . . . . .	54
9.6.2	Service . . . . .	54
9.6.3	Screen . . . . .	55
9.6.4	Widget . . . . .	56
9.6.5	Utils . . . . .	57
9.7	Solidity . . . . .	58
9.8	Remix IDE . . . . .	60
9.9	Google Colab . . . . .	60
9.10	NewsApi . . . . .	61
9.11	Mențiuni ce țin de mediu . . . . .	61
9.11.1	Ethereum și Sepolia . . . . .	61
9.11.2	MetaMask . . . . .	61
9.11.3	Infura . . . . .	61
<b>10</b>	<b>Aplicația Mobilă</b>	<b>62</b>
10.1	On Boarding . . . . .	62
10.2	Login . . . . .	63
10.2.1	Reset Password . . . . .	63
10.3	Register . . . . .	64
10.4	Navigation . . . . .	64
10.5	Home . . . . .	65
10.6	Elections . . . . .	65
10.6.1	Election . . . . .	66
10.7	Search . . . . .	67
10.7.1	Election Statistics . . . . .	67
10.8	Card . . . . .	68
10.9	More . . . . .	68
10.9.1	Two Factor Authenticator . . . . .	69
10.9.2	Add/Change Id Card . . . . .	69
10.9.3	Set up Pin . . . . .	70
10.9.4	Change Password . . . . .	70
10.9.5	Account Details . . . . .	71
<b>11</b>	<b>Analiză asupra aplicației</b>	<b>72</b>
11.1	Analiză de cost . . . . .	72
11.2	Analiză de timp . . . . .	73
11.3	Avantaje . . . . .	73
11.4	Limitări . . . . .	74
11.5	Directii viitoare . . . . .	74

**12 Concluzii** **75**

**Bibliografie** **77**

# Capitolul 1

## Motivație

Sistemele de vot tradiționale prezintă dualitate dintr-o perspectivă negativă, a slabiciunilor. Din punct de vedere legal aceasta poate conduce ușor spre fraudă, falsificarea eventuală a voturilor, iar paralela se construiește și din punct de vedere social intervenind lipsa încrederii alegătorului în ceea ce privește validitatea voturilor. Deși, se remarcă un avans tehnologic semnificativ, încă nu s-au găsit metode sigure și de încredere pentru susținerea alegerilor politice folosind sisteme de vot prin internet. Astfel, un aspect important în democrație, și anume votul, afișează încă semne de vulnerabilitate. Se remarcă inițiative pornite de anumite țări ca Austria, Australia, Canada, Estonia, Franța, Germania, Japonia și Elveția, care, au reușit să adopte un astfel de sistem, pentru a oferi șanse egale persoanelor de pretutindeni. Blockchain, apare astfel, ca o soluție salvatoare care promite securitate, transparentă, imuabilitate și eficiență, calități care se potrivesc perfect stereotipului ideal al cerințelor alegerilor electorale. Utilizând avantajele pe care le oferă această tehnologie, și registrul său distribuit, putem aduce soluții problemelelor actuale a sistemelor de vot.

# **Capitolul 2**

## **Introducere**

### **2.1 Prezentare generală**

Tehnologia blockchain, a apărut inițial ca o fundație pentru criptomonede, dar a evoluat într-o unealtă puternică și versatilă. Caracteristicile cele mai importante de care aceasta tehnologie dă dovada sunt descentralizarea, imuabilitatea și transparența, trăsături care îl fac candidatul perfect pentru un astfel de mediu. Potențialul acestuia poate revoluționa sistemele de vot pe care le cunoaștem prin construirea unui spațiu securizat și transparent unde alegătorii își pot exercita voturile ce pot fi numărate fară existența manipularii sau fraudei electorale.

### **2.2 Contextul aplicației**

Adoptarea sistemelor de vot electronice este într-o continuă creștere datorită accesibilității sporite și reducerii costurilor, dar datorită stadiului lor încă incipient, acestea sunt deschise provocărilor legate de securitatea și încrederea alegătorului. Posibilitatea apariției atacurilor, manipularilor sau vulnerabilităților ridică semne de întrebare asupra integrității sistemului. Astfel, o tehnologie ca blockchain, poate să ajute în combaterea acestora prin asigurarea corectitudinii procedurii de evaluare a voturilor, inventariate în registrul distribuit, și a prevenției împotriva atacurilor cibernetice.

### **2.3 Obiective**

Obiectivele acestei disertații sunt prezentarea stadiului curent al tehnologiei blockchain în contextul sistemelor de vot, de a extrage informațiile necesare proiectării unui astfel de sistem, iar mai apoi să pună în aplicare toate cunoștințele rezultate în urma cercetărilor. Rezultatul se va regăsi într-o aplicație disponibilă pe dispozitivele mobile pentru a oferi accesibilitate și usurință de vot alegătorilor.

# **Capitolul 3**

## **Votul în ascensiunea lui**

Istoria votării o putem reprezenta drept o clădire construită, cărămidă cu cărămidă, pe parcursul secolelor de civilizație umană, aceasta cuprinde eforturile, adaptările și progresul prin care a trece natura unei societăți, împreună cu sfera ei politică. Înainte de a porni în aventura sistemelor de votare bazate pe blockchain, este esențial să cunoaștem rădăcinile acesteia și cum au influențat votul de astăzi.[47]

### **3.1 Primele forme de votare**

Prima punere în practică a unei forme de votare a fost observată în Grecia antică, mai exact în Atena, undeva în jurul secolului al V-lea î. Hr. Această formă de votare constă în strângerea cetățenilor, mai exact cetățenii liberi de sex masculin ce dețineau pământ, în grupuri ce își exprimau voturile folosind mâinile sau în scris, pe o bucată de oală spartă numită ostraka. Aceștia votau pentru exilarea, pentru o perioadă de 10 ani, liderului politic, care trebuia să obțină un număr de cel puțin 6.000 de voturi.

Mai târziu apare în Roma un sistem de vot mai complex în care participanții votau pentru direct pentru liderii lor, totuși, dreptul de vot a fost oferit doar anumitor persoane ce dețineau, la acel timp, o anumită postură și avere. Acest sistem a pus bazale pentru regimului politic democratic care a urmat.

În jurul secolului al XIII-lea, în Veneția a fost implementat un sistem de vot denumit "vot de aprobare" la care un participant vota toți candidații pe care acesta îi favoriza, iar la final, candidatul cu cele mai multe voturi câștiga.

### **3.2 Votul modern**

Votul modern se remarcă a fi într-o ascensiune continuă, datorită progresului în domeniul tehnologiei. Prima mașină mecanică folosită pentru votare a fost utilizată la începutul anilor 1900, aceasta având ca scop să reducă fraudele și erorile ce apăreau în

urma numararii voturilor.

La mijlocul secolului al XX-lea apar în lumina sistemele de vot cu carduri perforate și cele cu scanare optică care mai apoi sunt acaparate de mașinile electronice de vot ce apar la inceputul secolului al XXI-lea. Acest avans tehnologic vine astfel cu noi oportunități, dar și cu noi provocări în special asupra securității și integrității proceselor de votare.

### **3.3 Era digitală și tehnologia blockchain**

Creșterea exponențială a tehnologiei la care suntem martori vine cu numeroase șanse de schimbare a felului în care sunt desfășurate sistemele de votare. Apare conceptul de votare prin internet, dar și sistemele de vot bazate pe blockchain. Tehnologia blockchain, împreună cu natura sa descentralizată și invariabilă, promite astfel să rezolve problemele asociate sistemelor de vot deja cunoscute cum ar fi frauda, securitatea și transparenta.

# Capitolul 4

## Blockchain

### 4.1 Istorie

Istoria acestei tehnologie dateaza încă din anul 1982, când criptograful David Chaum propune un concept pentru un protocol asemanator unui blockchain in disertația sa reușind astfel să pună bazele securității digitale și protocolelor criptografice. În anul 1992 Stuart Haber și W. Scott Stornetta propun un sistem de marcarea temporală (timestamp) a documentelor digitale cu scopul de a asigura integritatea, astfel aceștia reușesc să introducă un lanț criptografic sigur de blocuri. [20]

Blockchain-ul a luat naștere prin prisma unei singure persoane, mai exact Satoshi Nakamoto, în anul 2008, acesta reușind să îmbunătățească design-ul inițial la nivel conceptual. Un an acest design este implementat, rețeaua Bitcoin este pornită, iar primul bloc, denumit și blocul genezei, este minat de însăși Satoshi Nakamoto.[40]

Urmează o perioada de dezvoltare și extindere ce rezultă în apariția Ethereum în anul 2015, prin intermediul caruia Vitalik Buterin, creatorul acestei platforme, introduce contractele inteligente și aplicațiile descentralizate prin mașina virtuală Ethereum.

### 4.2 Prezentare generală

Blockchain-ul este un registru de date descentralizate și distribuite într-un mod sigur. Acesta este creat de o secvență de blocuri, sau celule, legate între ele, iar fiecare bloc include hash-ul blocului anterior, marca temporală, nonce și rădăcina Merkle (vezi 4.1). Hash-ul blocului anterior are ca scop să mențină relația dintre blocul curent și cel precedent, marca temporală, sau timestamp în engleză, verifică datele curente și atribuie timpul sau data la care a fost creat documentul digital. Nonce reprezinta un număr folosit o singură dată, este particular mecanismului de consens PoW (proof of work sau dovada muncii), și este asignat blocului pe perioada minării. Rădăcina Merkle este un tip de structură de date cadru care stochează tranzacțiile într-un bloc prin fabricarea unei

amprente digitale a întregului set de tranzacții. Prin prisma acesteia ne este asigurată imutabilitatea și siguranța blockchain-ului întrucât datele înregistrate într-un bloc nu mai pot fi modificate pe viitor fără modificarea blocului precedent.[43]

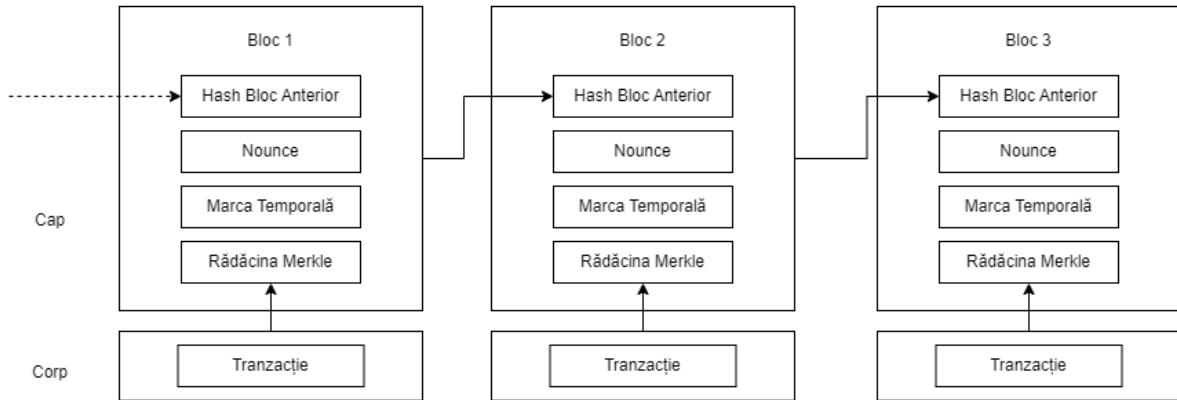


Figura 4.1: Versiune simplificată a unui lanț

Această tehnologie permite ca un grup colectiv participant să partajeze aceste date, ele fiind împărtite și duplicate în întreagă rețea. O astfel de metodă asigură diminuarea riscurilor de manipulare și a încercărilor frauduloase prin comunicarea și validarea noilor tranzacții cu toate registrele duplicate din rețeaua respectiva. Un registru blockchain poate astfel să fie partajat, dar nu modificat, întrucât aceasta modificare nu poate fi realizată fără ca celelalte părți să fie notificate. Fiecare părță joacă rolul unui nod dintr-o rețea, o nouă apariție pornește un întreg proces de copiere a tuturor blocurilor aflate în lanț, iar odată cu finalizarea acestui proces acesta va putea să primească blocuri noi.

Pentru a adăuga un bloc de tranzacții într-un astfel de registru este necesară găsirea unui sistem consensual, ce este inițiat între participanții rețelei (nodurile), care să se asigure că toate tranzacțiile sunt valide și autentice asupra tuturor nodurilor [58]. Pe parcurs au fost folosite o multitudine de astfel de algoritmi, dar cei mai cunoscuți au la bază modelele *Proof-of-Work* și *Proof-of-Stake*. PoW oferă tranzacției șansa să fie marcată drept unică și de incredere care trebuie să fie "minată" de catre unul din nodurile rețelei, care, după finalizare, va fi răsplătit cu o anumită sumă în monede. Acest rezultat poate fi foarte ușor verificat, dar greu de reproducere. Astfel, cel mai mare dezavantaj al PoW fiind faptul că este costisitor, consumă multă energie și timp [33]. PoS folosește "minatul" pentru a valida noi blocuri, acestea fiind generate și validate cu ajutorul mizei pe care utilizatorii o oferă, utilizatori care, nu mai trebuie să concureze pentru următorul bloc [35] [53]. Criptomonedele dintr-o astfel de rețea sunt pre-create și nu se remarcă un proces de "minat" cum întâlnim la PoW, fapt ce reduce costurile, iar procesarea tranzacțiilor este mult mai rapidă ca PoW.[58][53]

Raportându-ne la cele spuse anterior, componentele de bază într-o arhitectură blockchain sunt:

- Nod - reprezentat prin partile, sau utilizatorii, din rețeaua blockchain ce dispun de o copie a registrului distribuit, acesta fiind identic în întreaga rețea
- Tranzacție - caracterizată drept fundația blockchain-ului, acestea sunt înregistrate și verificate peste nodurile prezente.
- Bloc - acestea dețin informația care a fost adăugată în lanț, informație asupra careia nu se pot adăuga modificări sau eliminări.
- Lanț - reprezentat de o multitudine de astfel de blocuri, datorită faptului că blocul curent este în strânsă legătură cu cel precedent, prin reținerea hash-ului acestuia, un astfel de lanț nu poate fi manipulat.
- Miner - sunt nodurile care performă operații complexe, aceștia fiind responsabili să verifice dacă tranzacția este validă.
- Consens - reprezentat de acordul părților pentru participarea la tranzacții [52]

Caracteristicile ce pun în valoare această tehnologie sunt:

- Criptografie - părțile implicate oferă dovezi criptografice și computaționale fapt ce asigură autenticitatea și exactitatea tranzacțiilor
- Immutabilitate - menționat anterior, documentele aflate într-o rețea blockchain nu pot fi sterse sau modificate
- Proveniență - se poate cunoaște trecutul oricărei tranzacții într-un astfel de registru
- Descentralizare - remarcată prin distribuirea informației către nodurile participante, controlul acesteia fiind realizat sub algoritm consensual
- Anonimitate - fiecare nod, sau utilizator, are generată o adresă și nu poate fi identificat.
- Transparență - O rețea blockchain este aproape imposibil de șters deoarece un astfel de proces necesită o putere de calcul imensă[26]

### **4.3 Tipuri de rețele**

Rețele blockchain se împart, bazate pe intimitate, în trei categorii : public, privat sau consorțiu. O rețea publică permite interacțiune din partea oricărui individ, astă însemnând participare la înregistrarea informațiilor și/sau consensurilor și dețin acces la citirea tranzacțiilor[33]. Rețeaua privată pe de altă parte oferă aceste posibilități doar indivizilor autorizați, iar un consorțiu reprezintă o îmbinare între cele două anterior prezentate.

## 4.4 Utilizări

Datorită naturii sale, ce oferă soluții sigure, transparente și descentralizate, tehnologia blockchain poate fi, și este, integrată într-o gama largă de arii. Deși, aplicarea unui astfel de registru distribuit este perfect pentru sistemele bancare și de plată, această tehnologie nu se oprește aici gasind astfel implicare și în criptomonede, sănătate, contracte inteligente, finanțe descentralizate, donații, internetul lucrurilor și.a.m.d.[58]

## 4.5 Contracte Inteligente

Contractele inteligente datează din 1998, moment în care Nick Szabo a dezvoltat o monedă virtuală denumită "Bit Gold", acesta a reușit să prezică anumite aspecte pe care, în prezent, le catalogăm drept uzuale.[5]

Din punct de vedere analitic, denumirea lor arată implicit funcția autentică a contractelor de a crea o legătură între cele două părți aferente, acordurile acestora fiind scrise în linii de cod. Rularea acestora este proprie, un contract intelligent își efectuează funcțiile automat când anumite condiții sunt respectate, astfel reușind să eliminate necesitatea unei părți intermediare. Contractele inteligente oferă și beneficii ca reducerea riscurilor tranzacțiilor, reducerea costurilor de administrare și serviciu, și sporește eficiența proceselor la nivel de corporație. [57]

Un astfel de contract își face remarcată prezența în rețelele blockchain, reușind astfel să pună în lumină avantajele pe care le detine această tehnologie și să ofere o soluție superioară mecanismelor de tranzacții prezente. Aceste contracte sunt încărcate în rețea blockchain după ce trec printr-o serie de verificări și validări, loc în care, mai târziu, poate fi observat sau interogat, în anumite cazuri.

## 4.6 Portofel

O mențiune notabilă este portofelul din cadrul unei rețele blockchain. Acesta conține o colecție date ce identifică utilizatorul și îi permite acestuia să realizeze acțiuni în rețea.

# Capitolul 5

## Sistemele de vot electronice

Sistemele de vot electronic implică utilizarea unui sau mai multor hardware și software ce lucrează împreună cu scopul de a realiza un întreg proces de votare. Aici găsim multiple funcționalități pe care un astfel de sistem ar trebui să le dețină, acestea variind de la initializare până la strangerea și numărarea voturilor plasate. Desigur, un astfel de sistem necesită și un strict necesar, acesta fiind de înregistrare, autentificare, votare și numărare.[58]

Prima utilizare a acestui tip de voturi s-a marcat în anul 2000 în S.U.A. Aceasta a fost urmată de Franța, Marea Britanie, Spania, Irlanda, Estonia, Portugalia, Olanda, Paraguay, Finlanda, Austria, Germania și Norvegia. Estonia se remarcă ca fiind prima țară care permite votul de la distanță în anul 2007.[27]

### 5.1 Tipuri de sisteme

Voturile electronice se împart în cinci categorii : cartela perforată, DRE, sisteme de scanare optică, dispozitive de marcarea voturilor și votarea prin internet. Cartela perforată a apărut în anii 1960, acestea erau depozitate într-o cutie urmând a fi scanate folosind un cititor specific. DRE este un sistem de vot electronic ce prezintă buletinele de vot și înregistrările votantului direct pe un calculator, acesta interacționând folosind butoane fizice sau ecrane touch screen. Sistemele de scanare optică folosesc calculatoare ce conțin părți hardware și software specifice, alegătorii marchează votul pe un buletin de vot ce poate fi citit de un dispozitiv acestor voturi putând fi scanate pe loc sau la locația centrală. Dispozitivele de marcarea voturilor oferă alegătorului un buletin de vot electronic, iar după alegere acesta este printat fizic, acestea fiind专 pentru alegătorii cu dizabilități.[21]

Avansul tehnologic permite astfel introducerea votării folosind internetul, acesta fiind cel mai fezabil mod prin care se poate realiza o astfel de procedură. La rândul ei, acest tip de votare, se împarte în votarea la zone专izate, unde votanții au acces la un mod convenabil și eficient de vot, în votarea la cabine, care vor fi mult mai apropiate și

accesibile pentru votanți în locuri ca mall-uri, biblioteci și școli, și votarea remote, zonă care maximizează accesul votantului, dar vine și cu anumite dificultăți când vine vorba de securitate și alte probleme legate de cultura civică.[42]

## 5.2 Caracteristici

După mai multe cercetări s-a ajuns la concluzia că, un sistem de vot electronic necesită urmatoarele caracteristici:

- Fără bon - nu ar trebui să se emită un bon de dovadă a votării unui candidat [2]
- Corectitudine - inexistența unui rezultat preliminar este obligatorie, întrucât aceasta poate influența decizia alegătorilor [3] [16]
- Intimitate și anonimitate pentru alegator [66]
- Integritatea datelor - fiecare vot este unic și nu poate fi manipulat [29]
- De încredere - un astfel de sistem trebuie să prevină orice pierdere a voturilor sau erori [48]
- Unicitate - un candidat poate vota o singură dată [7] [55]
- Transparentă în verificare - alegătorii pot observa dacă votul lor a fost atribuit corect [34]

## 5.3 Blockchain și Contractele Inteligente

Acum, tehnologia blockchain, vine în sprijinul cerințelor necesare unui sistem de vot folosind internetul. O astfel de abordare poate face implementarea procesului de vot într-un mod simplu, accesibil și securizat. Acest sistem oferă caracteristici ca integritatea datelor, disponibile și toleranță la eșecuri, caracteristici care se mulează perfect asupra necesităților sistemelor de vot.

Aspecte cheie ce ies în evidență odată cu folosirea tehnologie blockchain sunt participarea de pretutindeni, asigurarea și motivarea alegătorului, prin oferirea unui sistem corect și de încredere, securitatea, eficiența, în special când discutăm de costuri, și precizia. Aici se mai adăugă și despărțirea de un element cheie prezent în sistemele de vot actuale, și anume, o entitate care are control asupra tuturor voturilor, și sub aripa căruia există acces asupra tot ce se întamplă în alegeri, fapt ce oferă posibilitatea manipulării sau înclinării rezultatelor cu scopuri neetice. Astfel, această despărțire poate asigura imuabilitate, lucru care se adună și în factorii de motivare ai alegatorului.

Acesta este locul unde, contractele inteligente își fac remarcată prezență. Cu ajutorul lor vom putea crea contracte ce se execută automat într-un blockchain. Fiecare contract intelligent va necesita reguli ca vor fi implementate în linii de cod împreună cu date de interes pentru alegător[56]. Menționat anterior, după ce aceste contracte sunt lansate în rețea, acestea nu mai pot alterate sau eliminate.

Există deja implementări propuse ce conțin design-ul unei astfel de infrastructuri, care, ar putea revoluționa votul, mai exact cel de la distanță, pe care îl cunoaștem. Discuția asupra acestora se va realiza la 6.

# Capitolul 6

## Sistemele de vot bazate pe blockchain

Sistemele de vot bazate pe blockchain reușesc să utilizeze eficient caracteristicile unice pe care tehnologia blockchain o oferă cu scopul de a rezolva, și pune în lumină, problemele generale ce apar în voturile electronice. Printre aceste probleme se numără securitatea, transparenta și integritatea, aspecte care vin ca o mănușă pentru un astfel de sistem.

### 6.1 Implementări realizate și studii de caz

Un lucru esențial în acest proces este familiarizarea cu literatura deja existentă, și care, a făcut posibilă deschiderea acestor drumuri. Aceste informații ne pot ajuta să înțelegem în detaliu potențialul pe care acest timp de sistem de vot, ce are la bază tehnologia blockchain, îl oferă în rezolvarea problemelor desfășurării unui proces electoral folosind internetul.

#### 6.1.1 Studii de caz

Potențialul aplicațiilor ce folosesc tehnologia blockchain în domeniul voturilor electronice a fost studiat pentru a prezenta și evalua securitatea, eficiența și posibilitatea unui mediu transparent și sigur de desfășurare a proceselor electorale.

#### A Systematic Review of Challenges and Opportunities of Blockchain for E-Voting

În anul 2020 Taş și Tanrıöver au publicat articolul numit "A Systematic Review of Challenges and Opportunities of Blockchain for E-Voting", la care au luat parte 63 de articole, ce avea ca scop să identifice lipsurile aflate în sistemele actual de vot electronice, să prezinte potențialul pe care îl detine conceptul de blockchain în direcția implementării

unui astfel de sistem, să ofere o imagine asupra soluțiilor deja existente și să propuna noi direcții de interes.[58]

Aceștia și-au bazat cercetarea pe 5 întrebări, pe care, aceștia le-au considerat ca fiind adecvate. Mai jos voi creea un tabel sub formă cheie-valoare , cheia reprezentând întrebarea, iar valoarea reprezentând raspunsul.

Întrebare	Răspuns
Care sunt lipsurile din votarea electronică?	Acestea sunt marcate de lipsa securității, în principal apărarea asupra diferitor atacuri cibernetice precum <i>DDoS</i> [7], TLS și/sau <i>man in the middle</i> [8] și atacuri asupra număratoarei voturilor [6] fapte ce duc la neîncrederea unui astfel de sistem.
Poate tehnologia blockchain să îmbunatățească votarea electronică?	Desigur, aceasta vine cu rezolvare la atacurile de tip <i>DDoS</i> , integritatea și încrederea, transparentă și intimitate, costuri reduse, rezultate instantanee și creștere de încredere a alegătorului.
Care sunt articolele și soluțiile existente?	Se remarcă existența multor astfel de articole, soluțiile principale constau în folosirea contractelor inteligente, asigurarea integrității datelor și adaptarea algoritmilor consensuali la cerințele unui sistem de vot electronic.
Ce platforme sau modele consensuale blockchain sunt folosite?	Platforma cea mai folosită se remarcă a fi Ethereum împreună cu contractele inteligente, iar modelele consensuale potrivite sunt cele de tip <i>DPoS</i> [31] [32] [35] ce sunt mai eficiente, când vine vorba de resurse și energie [53].
Care sunt direcțiile de viitor?	Cel mai important subiect este scalabilitatea întrucât eficiența unui astfel de sistem scade odată cu creșterea ratei de execuție, astfel modelele consensuale <i>DPoS</i> remarcându-se a fi potrivite [35] [62]. Se mai remarcă posibilitatea unor atacuri DDoS asupra contractelor inteligente ce pot duce la costuri monetare. [49]

Taş și Tanrıöver au concluzionat că, datorită dezavantajelor necunoscute încă a sistemelor de vot bazate pe blockchain fac punerea în practică la scară mare încă îndoiealnică. Aceștia propun aplicarea dezvoltărilor asupra unor mici regiuni pilot, iar mai apoi să le extindă. Aparent perfectă, această soluție încă prezintă anumite vulnerabilități ce merită documentate și tratate, dar deși aceste aspecte sunt descurajatoare, trebuie adus aminte faptul că acest sistem este încă la început și există o multitudine de oportunități.

## Blockchain for Electronic Voting System—Review and Open Research Challenges

Jafar, Aziz și Shukur au reușit să analizeze și să evaluateze articolele de cercetare prezente asupra sistemelor de vot bazate pe blockchain în "Blockchain for Electronic Voting System—Review and Open Research Challenges" [26]. Aceștia prezintă informațiile pe care le-au adunat în urma acestor cercetări.

Asemanator tabelului de la 6.1.1 voi contrui unul bazat pe secțiunile de interes din aceasta cercetare.

Secțiune	Rezumat
Secțiunea 4. Probleme și soluții în dezvoltarea sistemelor de vot prin internet	Sunt discutate principalele aspecte necesare pe care trebuie să le conțină un sistem de vot, și anume eligibilitate, unicitate, anonimitate, corectitudine, completitudine și soliditate. Aceștia adreseză problemele care pot apărea în aceste aspecte, iar, în prezent, implementarea unui astfel de sistem vin cu anumite compromisuri.
Secțiunea 5. Cerințe de securitate pentru sistemele de vot	Trebuie asigurată anonimitatea și unicitatea alegătorului, dar menținută precizia și integritatea rezultatelor. Este necesară prevenirea fraudei și corupției împreună cu asigurarea neprelucrarii datelor. Alegatorul trebuie să dispună de acces și siguranță, aspecte ce sporesc încrederea în sistem.
Secțiunea 6. Votarea electronică pe blockchain	Sunt prezentate calitățile blockchain-ului și de ce acesta este potrivit, cel puțin la nivel teoretic, pentru un sistem de vot electronic. Această idee ia apoi [22], dar este necesară o implementare amanunță.
Secțiunea 9. Propuneri de viitor	Sunt prezentate zonele de interes pentru viitoare cercetări, acestea fiind scalabilitatea, identitatea utilizatorilor, intimitatea tranzacțiilor, eficiența energetică, acceptarea sistemului, rezistența împotriva schimbării de către liderii politici și condiția de început la care se află acest concept.

Autorii prezintă cât de necesare sunt cercetările și rezolvările direcțiilor prezentate de către aceștia pentru a se reuși punerea în aplicare un sistem de vot baza pe blockchain.

## Blockchain-Based E-Voting Systems: A Technology Review

Mohammad et al. [43] au reușit să prezinte o vedere amplă asupra condiției la care se află sistemele de vot electronice bazate pe blockchain. Aceștia reușesc să treacă prin

toate aspectele ce țin de desfășurarea sistemelor electorale. Astfel, autorii discută despre potențialele beneficii, provocări, impact, aspecte legate de tehnologii și directii spre noi studii. Voi prezenta informațiile de interes într-un tabel similar prezentat anterior la 6.1.1.

Sectiune	Rezumat
Sectiunea 2. Sisteme de vot, tipuri și cerințe	Autorii împart sistemele în sisteme de vot tradiționale și electronice prezentând aspecte pentru fiecare. Zona de interes este țintită spre cerințele pe care le necesită un astfel de sistem, aceștia împărțindu-le în de securitate și non-securitate, care la rândul lor se dezbină în funcționale și nefuncționale. Cerințele de securitate sunt autenticitate și eligibilitate, anonimitate și discreție, asigurarea nemanipulării voturilor, integritate și încredere, detectie și monitorizare, corectitudine, verificabilitate și acuratețe, și disponibilitate. Cerințele non-securitate sunt flexibilitate, ușurință de înțelegere, accesibilitate, egalitate, interoperabilitate, eficiență de cost, transparentă și auditabilitate.
Sectiunea 5. Beneficii, provocări și impact	Sunt prezentate beneficiile, provocările și impactul pe care tehnologia blockchain o aduce în sistemele de vot. Beneficiile sunt securitate, transparentă, discreție, verificabilitate, auditabilitate, accesabilitate, descentralizare, eficiență, încredere, compatibilitate și imobilitate. Provocările pe care un astfel de sistem le aduce sunt similare cu beneficiile, întrucât implementarea sistemului stă la mâna dezvoltatorului care trebuie să folosească proprietățile acestuia.
Sectiunea 6. Tehnologii și implementarea sistemelor de vot bazate pe blockchain	Aceștia trec în revistă prin platformele blockchain, algoritmi consensuali, tehnici de securitate și intimitate, tehnici de autentificare și identificare, și alte tehnici criptografice, de dezvoltare și testare.
Sectiunea 7. Discuții și propuneri	Aceștia propun viitoare aspecte de interes ce țin de dezvoltarea sistemelor de vot bazate pe blockchain pe primele locuri aflându-se îmbunătățiri de scalabilitate și performanță, securitate și intimitate.

Autorii au ajuns la concluzia că tehnologia blockchain aduce în lumină caracteristici potrivite pentru înglobarea acestuia în procesele electorale, iar aspectele principale pe care trebuie pus accentul sunt securitatea și intimitatea. Se remarcă beneficiile indisputabile pe care această tehnologie le oferă, și anume trasparență și auditabilitate.

## 6.1.2 Studii de caz cu implementări

### On Secure E-Voting over Blockchain

Mccorry et al. [37] au publicat articolul "On Secure E-Voting over Blockchain" în care au propus un design de implementare a unui sistem de vot ce are la bază tehnologia blockchain. Autorii au luat în considerare abordarea protocolului *OV-net*, o schemă descentralizată în două runde [23], pe care, au implementat-o și asupra căreia au realizat experimente într-o rețea de test Ethereum. După cercetări aceștia au explicat că utilizarea unui astfel de protocol poate fi realizată doar la alegeri de nivel scăzut, și nu național, întrucât timpul de calcul este unul crescut, mai exact doisprezece secunde, astfel fiind posibile doar cinci voturi pe minut. Acest fapt este datorat interacțiunii dintre votanți pentru fiecare exprimare de vot, lucru imposibil de realizat când numărul alegătorilor este crescut. Datorită naturii unei alegeri electorale naționale de a fi centralizată, aplicarea unei soluții descentralizate folosind protocoale ca *OV-net* nu este posibilă. Autorii oferă un răspuns la această întrebare prin prezentarea a patru cercetări realizate în această direcție [24] [30] [51] [65] și printr-o propunere de implementare a unui sistem ce are la bază un protocol *E2E* (end-to-end), și anume *DRE-ip* (Direct Recording Electronic with Integrity and Enforced Privacy).

### Towards Secure E-Voting Using Ethereum Blockchain

Koç, Yavuz, Çabuk și Dalkılıç întorc spre a aduce un mediu securizat de vot și prin prezenta că este posibilă construirea unui sistem sigur de vot folosind blockchain [65]. Aceștia doresc să se focuseze pe implementarea soluției pe care o oferă într-un mediu de marime scăzută, de exemplu pentru procese electorale universitare. Autorii folosesc blockchain-ul Ethereum, loc unde, încarcă contractele inteligente, care permit verificarea și numărarea voturilor după ce alegerea este finalizată. Autentificarea alegătorilor lipsește, întrucât această este o problemă de sine stătătoare. Prin prisma implementării acestui sistem, autorii reușesc să avanzeze sistemele de vot electronice spre platforma blockchain.

### Blockchain-Based E-Voting System

Hjálmarsson și Hreiðarsson au propus și aplicat un design de sistem de vot electronic bazat pe blockchain, vezi [24], ce folosește contracte inteligente. Aceștia au definit rolurile de administrator, alegator, district și cabină, împreună cu desfășurarea unui astfel de proces electoral. Pentru fiecare procedură prezentă aceștia au creat un contract intelligent ce este inițializat de catre administratorul alegătorii. Aceștia au ales blockchain-ul *Geth* (Go-Ethereum) [13] întrucât oferă posibilitatea de dezvoltare spre extinderea protocolului original, a fost programat să nu exercite timp de nefuncționare, cenzură, fraudă sau interferențe, și rata tranzacțiilor este dependentă de timpul public sau privat al

rețelei. Autorii adresează cerințele unui sistem de vot care sunt respectate de design-ul propus. Discuta cum natura rețelei private alese împiedică atacurile de tip *DDoS* și *Sybil* (încercare de perturare a rețelei prin adăugare de noduri), și au grijă la vulnerabilitățile de autentificare printr-un ID Auðkenni [4] și un pin de șase cifre. Desigur, design-ul, respectă accesul la vot de prețutindeni, transparență și intimititatea alegătorului.

### **Decentralized Voting Platform Based on Ethereum Blockchain**

Khoury et. al [30] propun o platformă descentralizată de vot pe internet bazată pe tehnologia blockchain în Ethereum. Design-ul lor presupune ca fiecare alegere să fie reprezentată printr-un contract intelligent încarcat în rețeaua blockchain care va fi manageriat de o aplicație web. Astfel există două tipuri de contracte, unul de înregistrare, încarcat la fiecare eveniment, și unul pentru votare, acesta este scris o dată la început și încărcat cu diferite răspunsuri și întrebări specifice evenimentului. Aceștia folosesc o autentificare folosind SMS-urile, iar votarea va fi realizată printr-o aplicație mobilă. Contribuți principală a acestui articol este restricționarea apariției voturilor multiple folosind proprietățile dispozitivelor mobile.

### **Online Voting Application Using Ethereum Blockchain**

Shukla et. al [51] folosesc Ethereum, drept tehnologie blockchain, pentru a crea un sistem de vot prin internet. Aceștia construiesc propria lor rețea privată blockchain, loc unde, vor fi încărcate contractele inteligent. Scopul lor este de a eradică manipularea voturilor și indisponibilitățile ce țin de voturile fizice, și doresc să aducă transparență și autentificare în procedura lor de votare. Aceștia folosesc *OTP* (parole cu o singură utilizare) pentru autentificarea și validarea alegătorilor. Metoda acestora se diferențiază prin simplitate, scalabilitate și încredere deoarece implementarea propriei rețele nu necesită resurse externe pentru finanțare, aceștia obțin proprii ether prin proces de minare. Aplicația lor ia în seamă factorii de securitate, dar nu prezintă un mod puternic de administrare a autentificării.

#### **6.1.3 Implementări**

În aceasta secțiune vor fi prezentate proiecte implementate în direcția unor astfel de sisteme. Printre acestea se numără tipuri de proiecte care sunt deja dezvoltate sau într-un progres continuu.

#### **Polyas**

Polyas a suținut primul proces electoral în anul 1996 în Finlanda unde au participat 30.000 de alegători vorbind trei limbi diferite. Aceștia au fost certificați în anul 2016

de catre Oficiul Federal pentru Securitatea Informației. Compania folosește tehnologia blockchain pentru a oferi sisteme de vot electronice.[44]

## **Luxoft**

Luxoft este un furnizor global de servicii *IT*, iar din 2019, când Antony Welfare devine director general al practică blockchain, începe să dezvolte o infrastructură pentru sistemele de votare prin internet bazat pe blockchain. Aceștia oferă un prim astfel de sistem pus în folosință. Tot ei, anunță dorința de a oferi liberă utilizare a acestei platforme, lucru de promovează utilizarea în instituțiile publice.[36]

## **Voatz**

Compania Voatz utilizează dispozitivele mobile împreună cu tehnologia blockchain pentru a crea un sistem de votare prin internet. Aceștia se folosesc de caracteristicile pe care le oferă dispozitivele pentru autentificarea alegătorului cum ar fi scanarea amprentei sau retinei.[60]

## **Decentralized**

Decentralized Vote folosește o rețea publică blockchain Ethereum ce folosește un algoritm consensual bazat pe modelul *PoF* (Proof of Authority) cu noduri de validare autorizate. Sistemul utilizează o tehnică bazată pe *ZKP* denumită *zk-SNARK* pentru a oferi dovada, că utilizatorul este eligibil pentru vot, contractelor inteligente. Totuși aceștia nu asigură un sistem pentru desfășurarea alegerilor politice naționale. [10]

## **Agora**

Agora introduce o platformă digitală de vot al carui ecosistem rulează pe un blockchain personalizat proiectat și implementat pentru a îndeplini cerințele pe care le dispune un sistem de vot electronic. Aceștia oferă un mecanism consensual legitim și o tehnologie unică pentru securitate.[1]

## **Votem**

Votem reușește să creeze o platformă bazată pe tehnologia blockchain ce oferă imutabilitatea, acces bazat pe permisiuni, pista de audit și o bază de date distribuită. Aceștia oferă o soluție pentru sisteme de vot politice sau la nivel de asociație, reușind să pună în practică sistemul propriu în S.U.A și în alte zone din lume. De remarcat este faptul că securitatea, după ce aceștia au reușit să trateze un număr de peste 13 milioane de alegători, nu a permis frauda, compromisurile sau atacurile.[61]

## 6.2 Analiză finală

În această secțiune sunt prezentate aspectele cheie pe care le-am extras în urma cercetării asupra articolelor anterior menționate.

### 6.2.1 Tehnologii și terminologii

În acestă subsecțiune vom discuta despre tehnologii și terminologii cele mai des folosite în contextul sistemelor de vot electronic bazate pe blockchain.

#### Ethereum

Pe parcursul întregii cercetări se remarcă o concentrare asupra blockchain-ului Ethereum, care, oferă funcționalitatea contractelor inteligente ce permit crearea de protocoale de vot complexe reușind să sporească securitatea, transparenta și eficiența. Ethereum, datorită naturii sale *open-source*, prezintă oportunitatea de a dezvolta aplicații descentralizate către utilizatori. Această rețea reușeste să efectueze tranzacții la o viteză mai ridicată față de Bitcoin.

#### Contracte Inteligente

Contractele inteligente sunt evidențiate pe parcursul studiilor legate de implementări, vezi 6.1.2, drept soluția pentru eficientizarea costurilor și pentru limitările ce apar în scalabilitatea sistemelor de vot electronic. Acestea simplifică utilizarea blockchain-ului prin eliminarea necesității unei noi entități.

#### DPoS

Menționat anterior, în tabelul 6.1.1 , modelul consensual *DPoS*, introdus de Daniel Larimer, a fost demonstrat a fi cel mai potrivit pentru sistemele de vot electronice. Într-un astfel de model rețeaua funcționează pe baza unui proces electoral. Un nod din rețea este prezentat drept un candidat, care la rândului lui poate participa în alegere. Fiecare deține un anumit număr de jetoane, adică o anumită putere de vot (zece jetoane sunt egale cu 10 voturi), iar aceștia aleg pe cine doresc să voteze. Primele n noduri care au fost alese au acum dreptul de a adăuga noi blocuri în lanț, fiecare așteptându-și randul, iar dacă cineva își pierde rândul va aștepta următoarea lui apariție. Pentru acest proces fiecare nod din rețea este răsplătit cu noi jetoane, dar dacă aceștia își ratează randul sau adaugă tranzacții nevalide sunt penalizați. Comunitatea poate astfel să voteze anumite noduri care să dispară din rețea. Principalele avantaje ale unui astfel de sistem sunt eficiența, scalabilitatea și controlul, dar pot apărea probleme ca riscul monopolizării, îngălățării la vot sau încrederei. [11]

## ZKP

ZKP (Zero Knowledge Proof) este o metodă criptografică ce are ca scop prezentarea dovezei asupra cunoașterii datelor fără a le afișa. Ideea a apărut prima dată în anul 1989 datorită lui GoldWasser, Micali și Rackoff [17] aceștia reușind, utilând primitive criptografice, să facă posibilă demonstrarea stării de adevăr a unei afirmații asupra unor date secrete neoferind date suplimentare. Voi prezenta cum funcționează această metoda printr-un exemplu simplu, un joc în care îți este oferită o ilustrație cu diferite obiecte și imaginea obiectului pe care trebuie să îl găsești. Poți demonstra că acel obiect există în ilustrație fără a specifica locația exactă folosind o hârtie cu un spațiu exact în locul unde se află obiectul dorit [14]. Un astfel de model are un set de reguli pe care trebuie să le satisfacă, acestea fiind completitudinea, soliditate și zero cunoștințe. Completitudinea este satisfăcută dacă un verificator este total convins de afirmația doveditorului, soliditatea ține de o probabilitate mică de acceptare a declarației dacă aceasta este falsă și proprietatea *zero cunoștințe* are la bază conceptul că verificatorul nu știe nimic legat de informație, ci doar dacă aceasta este adevărată.

### 6.2.2 Cerințe

În urma studiilor de cercetare prezentate la secțiunea 6.1.1 și secțiunea 5.2 am extras cele mai vizate și importante cerințe necesare desfășurării unui proces electoral electronic. Voi împărți aceste tipuri de cerințe în securitate, legalitate și altele.

*Cerințe de securitate:*

1. Integritatea - garanția protecției datelor și a manipulărilor neautorizate împreună cu asigurarea împotriva vulnerabilităților și eșecurilor de securitate.
2. Soliditate - proprietatea unui sistem de a funcționa fără a pierde date și de a preveni erorile.
3. Eligibilitate - asigură că doar alegatorii eligibili pot vota, iar procesul de autentificare a acestuia trebuie să fie riguros.
4. Unicitate - un alegător are dreptul la un singur vot.
5. Corectitudine - mediul de votare trebuie să fie unul obiectiv fără a influența alegatorul.
6. Acuratețe - procesul de numărare a voturilor trebuie să fie corect, iar acestea nu pot fi alterate.
7. Verificabilitate - proprietate ce oferă accesul la verificarea corectitudinii desfășurării alegerilor

8. Disponibilitate - platforma trebuie să fie utilizabilă la orice moment indiferent de condiții
9. Anonimitate - nu trebuie să existe metode prin care să se poate construi o legătură între vot și alegător, astfel respectându-se intimitatea acestuia și nu oferă posibilitatea de dovedire a votării unui anumit candidat.

*Aspectele ce țin de legalitate:*

1. Egalitate - toți alegătorii au acces la portalul de vot indiferent de condiții, iar acesta trebuie să fie unul intuitiv pentru a asigura înțelegerea funcționării de către toți participanții
2. Disponibilitate - alegătorii trebuie să aibă acces, indiferent de locație sau circumstanțe, la procesul electoral
3. Caracter secret - votul alegătorului trebuie să ramână privat.
4. Integritate - trebuie luate măsuri împotriva fraudelor electorale
5. Democrație și singularitate - doar alegătorii eligibili au drept de vot, iar aceștia îl pot exercita o singură dată
6. Caracter liber exprimat - trebuie asigurată proprietatea că alegerea de vot a cetățeanului nu este influențată și nu este viciată în niciun alt fel.
7. Libertate - alegătorul are dreptul de a-și atrage în nulitate propriul vot.

*Alte cerințe:*

1. Eficiență de cost - se remarcă dorința construirii unui sistem accesibil, reutilizabil și care necesită costuri de menenanță scăzute
2. Interoperabilitate - integrare și compatibilitate crescută față de diferite componente și tehnologii

### **6.2.3 Contribuțiile sistemelor de vot bazate pe blockchain**

În această secțiune prezentăm calitățile pe care le are blockchain-ul în contextul alegerilor electorale.

1. Securitate - aici găsim proprietăți ca integritate, imuabilitate, durabilitate, stabilitate și nerepudiere.

2. Descentralizare - alegerile nu mai dispun de o singură entitate de control, toate atributiile acestei entități fiind distribuite în întreaga rețea .
3. Accesabilitate - oportunități egale de acces pentru alegătorii eligibili.
4. Anonimitate - sistemele bazate pe blockchain oferă alegătorilor un spațiu intim, protejându-se identitatea acestuia pe întreaga desfășurare.
5. Soliditate - blockchain reușește să ofere un mediu eligibil, corect, unic, preci, credibil și de încredere în care se poate desfășura un proces electoral .
6. Imuabilitate - oferă un scut împotriva manipulărilor și/sau eliminărilor voturilor.
7. Toleranță - tehnologie blockchain vine cu avantaje asupra combaterii atacurilor cibernetice ca DDoS și Sybil.
8. Transparentă - asigură o metodă fără eșec asupra verificării oricărui aspect ce ține de procesul electoral.
9. Eficiență - se remarcă eficiență asupra costurilor, timpului și performanței.
10. Încredere - un astfel de sistem poate oferi încredere alegătorilor astfel sporind numărul viitorilor participanți.
11. Compatibilitate - această tehnologie oferă adaptabilitate și flexibilitate în implementare sistemelor.

#### **6.2.4 Provocări și Limitări**

Deși o tehnologie aparent perfectă pentru un astfel de sistem de votare, blockchain-ul încă prezintă anumite provocări și limitări.

- Scalabilitate - performanța scade odată cu creșterea numărului de execuții.
- Identitatea utilizatorului - deși utilizatorii rețelei au asignate adrese, totuși aceste date pot duce la dezvaluirea identității acestuia
- Acceptare - sunt necesare desfășurări multiple pentru ca alegătorii să accepte și să aibă încredere într-o astfel de abordare
- Compromisuri - alegerea tipului de securitate a rețelei poate aduce anumite dezavantaje
- Împotrivire - datorită potențialului acestei tehnologii în combaterea fraudei electorale se pot remarca anumite împotriviri din partea liderilor politici coruși.
- Natură incipită

# Capitolul 7

## Sistem propus

În această secțiune este prezentat sistemul propus spre aplicare. Acest sistem cuprinde o încercare a abordării tuturor cerințelor necesare într-un proces electoral și a rezolvării problemelor ce apar în voturile electronice de la distanță.

### 7.1 Structură

Sistemul propus va fi format din trei module, interfață, logică și procesare a datelor, acesta fiind realizat pentru a fi disponibil pe dispozitivele mobile asigurând astfel **disponibilitate**. Pentru partea de interfață am ales framework-ul Flutter, logica aplicației va fi realizată folosind tehnologiile Ethereum, Sepolia, Web3, Solidity, MetaMask, Infura, Firebase, Microsoft Azure Face Api, Google Cloud Secret Manager și NewsApi, iar partea de procesare va fi realizată folosind Python. Toate aceste tehnologii vor fi prezentate în Capitolul 8.

### 7.2 Interfață

Menționat anterior, aceasta va fi realizată folosind limbajul dart, prin prisma acestuia doresc să ofer o interfață placută, intuitivă și simplificată pentru utilizatori. Astfel doresc să ating cerința ce ține de **egalitate**. Utilizatorul va dispune de o aplicație ce îi va oferi un mediu unde acesta va participa la procesul de autentificare, identificare, votare și, dacă dorește, informare. Prin prisma interfeței utilizatorului îi va fi oferită și **libertate**, el având și opțiunea de anulare, în sensul de nulitate, a votului. Această secțiune acoperă doar partea pe care o observă utilizatorul, care, după parerea mea, ar trebui să ofere acestuia impresia de siguranță și profesionalism.

## 7.3 Procesare a datelor

Procesarea datelor va consta într-o implementarea, folosind limbajul Python și mediu oferit de Google Colab, a unui mod simplu, rapid și sigur prin care vom putea asigura:

1. Securitate - se vor genera perechile unice pentru criptarea și decriptarea informațiilor, și se vor cripta informațiile portofelelor.
2. Eligibilitate - se vor sorta, verifica și asigna codurile de identificare a alegătorilor eligibili pentru vot.
3. Anonimitate și verificabilitate - eligibilitatea va fi verificată folosind o adresă din cadrul portofelelor, astfel, doar utilizatorul va săpe cine a votat, și se poate verifica validitatea voturilor fără a putea identifica persoana responsabilă.
4. Disponibilitate - vor fi încarcate contractele inteligente ce oferă cadrul unui proces electoral în rețeaua blockchain, loc în care vor fi accesibile indiferent de condiții.
5. Unicitate - alegătorii eligibili vor dispune de fondurile necesare pentru o singură tranzacție ce are ca scop exprimarea votului.

## 7.4 Logică

În această secțiune se remarcă partea fundamentală a acestui proiect, aici este zona de interes asupra careia se va îndrepta o porțiune semnificativă a eforturilor. Prin prisma acesteia doresc să ating cerințele de **securitate, transparentă, accesibilitate, anonimitate, integritate, democrație și singularitate, libertate, verificabilitate, eligibilitate, acuratețe, eficiență de cost și interoperabilitate**. Trebuie menționat faptul că **anonimitate** permite astfel combaterea **fraudei** print mituire sau constrangere a alegătorului spre o anumite decizie datorită naturii sistemului de a face indisponibilă identificarea indivizilor care au votat un anumit candidat. Vom împărți logica în 5 categorii astfel, securitate, identificare, desfășurare electorală, libertate și informare.

1. Securitate
  - (a) Google Cloud Secret Manager - vor fi salvate date secrete pentru criptarea și decriptarea informațiilor sensibile.
  - (b) Firebase - aici își vor avea locul datele, ce sunt într-un mediu sigur, iar pentru o dublă asigurare informațiile sensibile stocate vor fi criptate.
2. Identificare

- (a) Firebase Authentication - cu ajutorul acestei platforme vom autentifica utilizatorul și vom adăuga o secțiune de verificare folosind *2fa*.
- (b) Microsoft Azure Face Api - va fi folosită potrivirea facială pentru imaginea de pe cartea de identitate și poza realizată de utilizator, pentru a realiza încă un nivel de verificare

### 3. Desfășurare Electorală

- (a) Ethereum - după analiza desfășurata la 6.2 am ajuns la concluzia ca voi folosi blockchain-ul Ethereum pentru găzduirea alegerilor, și implicit a contractelor inteligente
- (b) Sepolia - vom folosi o rețea de test Ethereum, ce oferă finanțări gratuite, pentru a putea monitoriza și desfășura aspecte din cadrul alegerilor
- (c) Solidity - acest limbaj va fi folosit în crearea regulilor pe care un contract intelligent le va respecta
- (d) MetaMask - cu ajutorul acestui unelte vom crea portofele digitale și vom transfera jetoanele necesare pentru ca un alegător să poate lua parte la procesul electoral
- (e) Infura - vom folosi acest serviciu pentru a conecta aplicația de rețea la blockchain
- (f) Web3 - ne va oferi posibilitatea de a interacționa cu contractele inteligente încarcate pe blockchain
- (g) Firebase DB - vor fi salvate date legate de portofele și adrese ale alegerilor încărcate în rețea

- 4. Libertate - va fi oferită șansa utilizatorului de a înregistra un vot anulat, mai exact nul.
- 5. Informare - aici vom folosi NewsApi pentru a aduce informații relevante utilizatorului.

## 7.5 Integrarea secțiunilor

Integrarea secțiunilor va fi realizată folosind framework-ul Flutter, ce oferă o multitudine de pachete în acest sens. Astfel alegătorul va beneficia de toate funcționalitățile anterior prezentate respectându-se cerințele unui sistem de votare electronic.

## 7.6 Flux de date

Fluxul de date din cadrul unui sistem de votare electronic folosind blockchain este transparent, securizat, imutabil și cu toleranță la erori.

1. Înregistrare - utilizatorul este obligat să se înregistreze pentru a avea acces la sistem.
2. Verificare - pentru a avea acces la alegerile asignate, utilizatorul trebuie să își verifice contul folosind autentificarea în doi pași, încarcarea cărții de identitate și oferind necesarul pentru recunoașterea facilă.
3. Crearea alegerii - alegerile vor fi create folosind implementarea anterior menționată, alegătorul are acces doar dacă acesta a trecut prin toți pașii de verificare și este eligibil pentru participare.
4. Votare - după ce a trecut tot procesul, alegătorul își va putea exercita dreptul de vot la procesele electorale la care este eligibil, această acțiune fiind realizată printr-o tranzacție în rețeaua blockchain cu apel asupra metodei din cadrul contractului inteligent.
5. Verificarea votului - după finalizarea alegerii utilizatorul are acces la verificarea propriului vot, iar demonstrarea validității votului poate fi asigurată fără identificare.
6. Numărarea voturilor - pe tot parcursul desfășurării contractul deține valoarea totală a voturilor, date ce nu pot fi alterate datorită naturii imutabile a rețelei blockchain.

# Capitolul 8

## Tehnologii Folosite

### 8.1 Ethereum

Ethereum [12] este o platformă software globală decentralizată, ce a fost lansată în anul 2015, ce este întreținută folosind tehnologia blockchain. Fondatorii acestei platforme au fost printre primii care au văzut și exploatat adevaratul potentialul al blockchain. Ethereum oferă astfel criptomonedă sa nativa denumita ether(ETH) fapt pentru care este cunoscută în domeniul de investiții, iar pentru dezvoltatori, aceasta se oferă spre folosință în dezvoltarea blockchain și a aplicațiilor financiare decentralizate.

Ethereum folosește blockchain, un registru distribuit asemănător unei baze de date unde informațiile sunt stocate sub formă de blocuri în interiorul căruia găsim informații codificate despre blocul anterior și informația nouă pe care o aduce. Acest bloc, denumit și celulă, ajunge în blockchain după ce un validator verifică informația adusă și creează unul nou, sarcină pentru care acesta este rasplatit cu jetoane ether. Astfel se formează un întreg lanț codificat de informație ce nu poate fi modificat, întrucât acesta este raspândit în întreaga rețea blockchain.

### 8.2 Sepolia

Sepolia [50] este un testnet, rețea de testare din domeniul criptomonedelor, și are ca scop să ofere dezvoltatorilor un mediu de dezvoltare și testare a anumitor funcționalități sau aplicații pe blockchain-ul Ethereum.

Acesta este specializat în contracte inteligente și aplicații descentralizate.

### 8.3 Web3

Web3 [63] reprezintă o nouă generație a World Wide Web care se caracterizează prin decentralizare, tehnologii blockchain și îmbunătățirea controlului utilizatorului asupra da-

telor. Acesta este construit pe baza unei rețele decentralizate, ce folosesc tehnologia blockchain, astfel reduce dependența de un sigur punct de control datorită faptului că datele și aplicațiile sunt distribuite pe mai multe noduri. Aici găsim și contractele inteligente, contracte ce se executa singure folosind acordurile scrise direct în cod, ce rulează pe rețele blockchain executând condițiile proprii fapt ce reduce nevoia unui intermediar.

## 8.4 Solidity

Solidity [54] este un limbaj, ce folosește acolade, de nivel înalt, construit pe baza programării orientate obiect, proiecta pentru implementarea de contracte inteligente ce conduce comportamentul conturilor din cadrul statului Ethereum. A fost creat cu scopul de a viza mașina virtuală Ethereum. Acesta este influențat în mare parte de limbajul C++ pentru sintaxa de declarare a variabilelor, a buclelor, a conceptului de supraîncărcare a funcțiilor și implicit conversiile de tip, dar nu trebuie excluse și limbajele din care a împrumutat anumite concepte ca Python și JavaScript.

Cu ajutorul acestuia pot fi create contracte și date spre folosință în diferite domenii precum votarea, multifinanțarea, licitațiilor oarbe și a portofelelor cu semnături multiple.

## 8.5 Remix IDE

Remix IDE [46] este un mediu de dezvoltare ce este folosit pe întregul parcurs al dezvoltării unui contract intelligent. Acesta nu necesită configurare favorizând astfel un proces rapid de dezvoltare și oferă o versiune web, cât și una desktop. În cadrul găsim un set mare de plugin-uri, interfața este foarte intuitivă și putem testa contractele folosind medii Ethereum de test și conturile disponibile.

## 8.6 MetaMask

MetaMask [38] este o unealtă open source din cadrul Ethereum, mai exact un portofel digital, și are ca scop să stocheze informații referitoare la criptomonede din blockchain. Oferă utilizatorilor permisiunea de a interacționa cu medii web ce rulează aplicații decentralizate, contracte inteligente și multe altele din cadrul Ethereum.

Conceptul pe care se bazează portofelul MetaMask este unul simplu folosind două chei, publică și privată. Cu ajutorul cheii publice utilizatorul poate fi identificat, iar cea privată este oferită doar utilizatorului pentru a performa anumite acțiuni. De reținut faptul că MetaMask folosește tehnologia Infura.

## 8.7 Infura

Infura [25] este un serviciu ce oferă acces securizat și de încredere asupra unei varietăți de rețele blockchain. Aceasta reușește să elimine complexitățile ce stau la baza gestionării unei infrastructuri de tip blockchain, fapt ce ofera dezvoltatorilor șansa să se focuseze pe generarea aplicațiilor Web3.

Infura furnizează infrastructura și uneltele esențiale în construirea unei aplicații Web3 deservind astfel drept pod pentru conectarea aplicațiilor la rețelele blockchain, oferind dezvoltatorilor API-uri aferente interacțiunii cu acestea, lansarea și managerierea contractelor inteligente.

## 8.8 Dart

Dart [9] este un limbaj de programare creat de compania Google, a cărei sintaxă face familiarizarea cu acesta foarte ușoară. Acesta a fost proiectat pentru a dezvolta rapid aplicații disponibile pe mai multe platforme. Construit pentru dezvoltarea specializată spre client, acest limbaj reușește să ofere o multitudine de beneficii în generarea de produse de înaltă calitate pe aplicații web sau desktop și dispozitive mobile.

Aspecte cheie care fac limbajului Dart, în contextul dezvoltării aplicațiilor, o alegere oportună sunt:

- Ușurință în întegrelere, scriere și adaptare
- Concentrare pe client
- Verificabilitate imediată a modificărilor prin funcția *Hot-Reload*
- Disponibilitatea unei game mari de funcționalități și tipuri de date prin librăriile incluse pe care le oferă.

Limbajul Dart reușește să pună bazele *framework-ului* Flutter, ce devine o extensie populară pentru acest limbaj.

## 8.9 Flutter

Flutter [54] este un *framework* deschis, din punct de vedere al utilizării, creat de Google ce oferă dezvoltare de aplicații mobile, web și desktop folosind aceeași fundație. Astfel, prin prisma acestei tehnologii, se rezolvă problemele anterioare legate de eficiență în producerea de aplicații disponibile pe mai multe platforme fără a fi necesare implementări cu baze diferite.

Datorită mediului în care a fost creat, acest limbaj reușește să fie foarte ușor de utilizat împreună cu suitele de servicii oferite de Google.

Flutter oferă următoarele avantaje:

- Rapiditate - compilare rapidă și performanță crescută.
- Încredere - aceasta devine o unealtă de încredere datorită companiei Google, ce a creat acest *framework*, și a altor companii ce o utilizează.
- Calitate - se remarcă natura îmbunătățită a aplicațiilor pe care acest limbaj o aduce
- Facil în integrarea cu servicii Google

## 8.10 Firebase

Firebase [15] este o platformă dezvoltată de Google ce are ca scop să completeze necesitățile cerute de dezvoltatorii de aplicații mobile sau web, lucru ce le oferă acestora oportunitatea de a susține afacerile clienților într-un mod facil.

Prin prisma acestei platforme avem acces la baze de date, servicii, autentificare și integrare. Putem incorpora foarte ușor aplicația cu instrumente ca Google Ads, Google Play, Data Studio, Slack, Jira, Pager Duty, Android Studio, AdMob, Google Marketing Platform și BigQuery.

Firebase oferă o soluție intuitivă dată spre folosință cu scopul de a simplifica dezvoltarea prin punerea la dispoziție a mai multor unelte de care un programator se poate folosi pentru a livra, în timp optim, aplicații.

Astfel, firebase reușește să înglobeze o multitudine de servicii potrivite pentru un astfel de context, iar echipele ce au ca scop dezvoltarea se pot orienta asupra aspectelor ce țin de experiența clientului.

Cele mai cunoscute servicii oferite de firebase sunt:

- Firebase Authentication
- Firebase ML
- Firestore Database
- Firebase Storage
- Firebase Analytics
- RealTime Database

## 8.11 Microsoft Azure Face Api

Microsoft Azure Face Api [39] este un mecanism oferit de compania Microsoft, care utilizeaza algoritmi de detectare facială pentru recunoașterea și detectarea fețelor umane. Acest api oferă funcționalități ca recunoasterea, verificarea și gruparea facială.

## 8.12 Google Cloud Secret Manager

Google Cloud Secret Manager [18] reprezinta o unealta securizata pentru gestionarea informațiilor sensibile precum chei, parole și certificate. Aceasta garantează un mod protejat de stocare, acces și administrare a secretelor.

Secret Manager ofera avantaje ca :

- Securitatea - datele sunt criptate pe parcursul trecerii, dar și cand sunt stocate.
- Simplitate - efort scăzut în managerierea, updatarea și recuperarea secretelor
- Disponibilitate Globală - datele sunt stocate și duplicate pe multiple regiuni
- Scalabilitate - unealta este dezvoltată să scaleze împreună cu infrastructura utilizatorului, gestionând secretele pentru medii complexe

## 8.13 Web3Dart

Web3Dart [64] este o librărie ce dispune dezvoltatorului o metodă de interacționare cu blockchain-ul Ethereum din cadrul aplicațiilor Dart.

## 8.14 NewsApi

News API [41] este un instrument de căutare și oferire a articolelor încărcate pe internet. Acesta este un api de tip *HTTP REST*, astfel, accesul la aceste date se realizează prin interogări. Pentru a filtra datele este necesară modificarea parametrilor interogării, acest api oferă opțiuni ca țara, categoria, sursa, numărul de pagini sau interogări de text. pentru a folosi News API este necesara generarea unei chei ce permite accesul către aceasta.

## 8.15 Python

Python [45] este un limbaj de programare ai cărei apariție datează din 1989 când Guido van Rossum a venit cu ideea construirii unui limbaj simplu, intuitiv, disponibil și accesibil

indeferent de platforma de acces. Acest proiect a pornit ca un pasiune, denumirea căruia a provenit dintr-un serial denumit *Monty Python's Flying Circus*, și a ajuns să devină unul dintre cele mai puternice limbaje de programare.

În acest limbaj se pune accentul pe simplitate și ușurință de înțelegere, fapt pentru care este și cunoscut.

Python reușește să își facă prezența și în domeniul inteligenței artificiale datorită integrării cu o gamă largă de librării construite în acest sens. Astfel, prin prisma acestui limbaj putem antrena, monitoriza, modifica și utiliza modele ce țin de acest domeniu.

Punctele tari ale acestui limbaj de programare sunt:

- Ușurință în înțelegere și folosire.
- Disponibilitate prin natura sa *open source* și gratuitatea de folosință.
- Dezvoltare continuă permisă prin aspectul anterior prezentat, ce oferă acces dezvoltatorilor să aducă îmbunătățiri acestui limbaj
- Portabilitate datorită funcționalității pe mai multe platforme și/sau sisteme de operare .
- Puternic datorită formei de bază ce implementează conceptul de programare orientată obiect.

## 8.16 Google Colab

Google Colab [19] este o platformă bazată pe cloud oferită de Google, aceasta permite scrierea și execuția de cod scrisă în limbajul Python folosind o interfață web. Aceasta oferă un mediu asemănător *Jupyter Notebook*.

# Capitolul 9

## Arhitectura aplicației

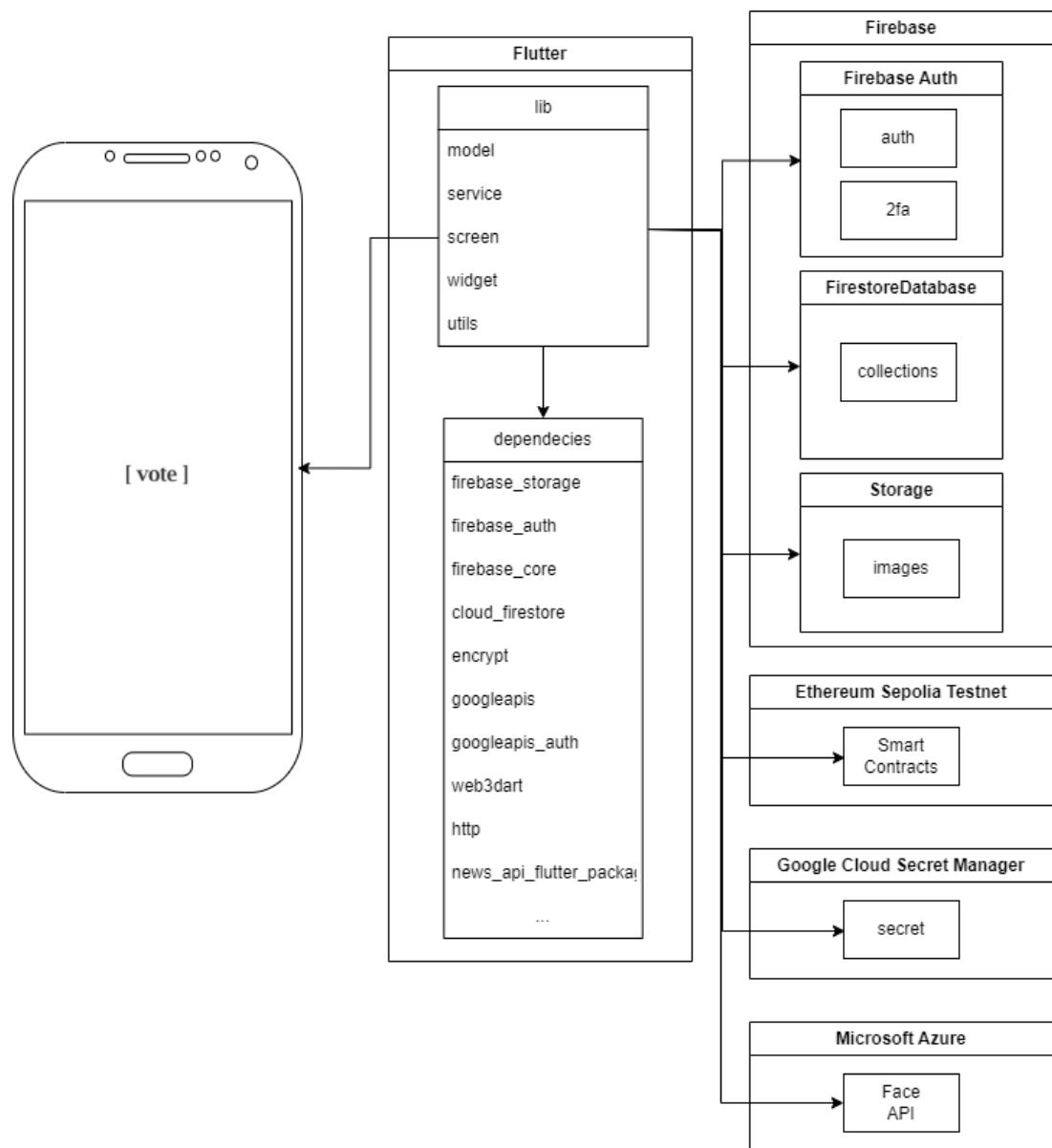


Figura 9.1: Arhitectura aplicației

## 9.1 Diagramme C4

Modelul C4 oferă o metodă simplă de generare și prezentare a arhitecturii software sub formă de diagramă.

### 9.1.1 Nivel 1

Vezi 9.2

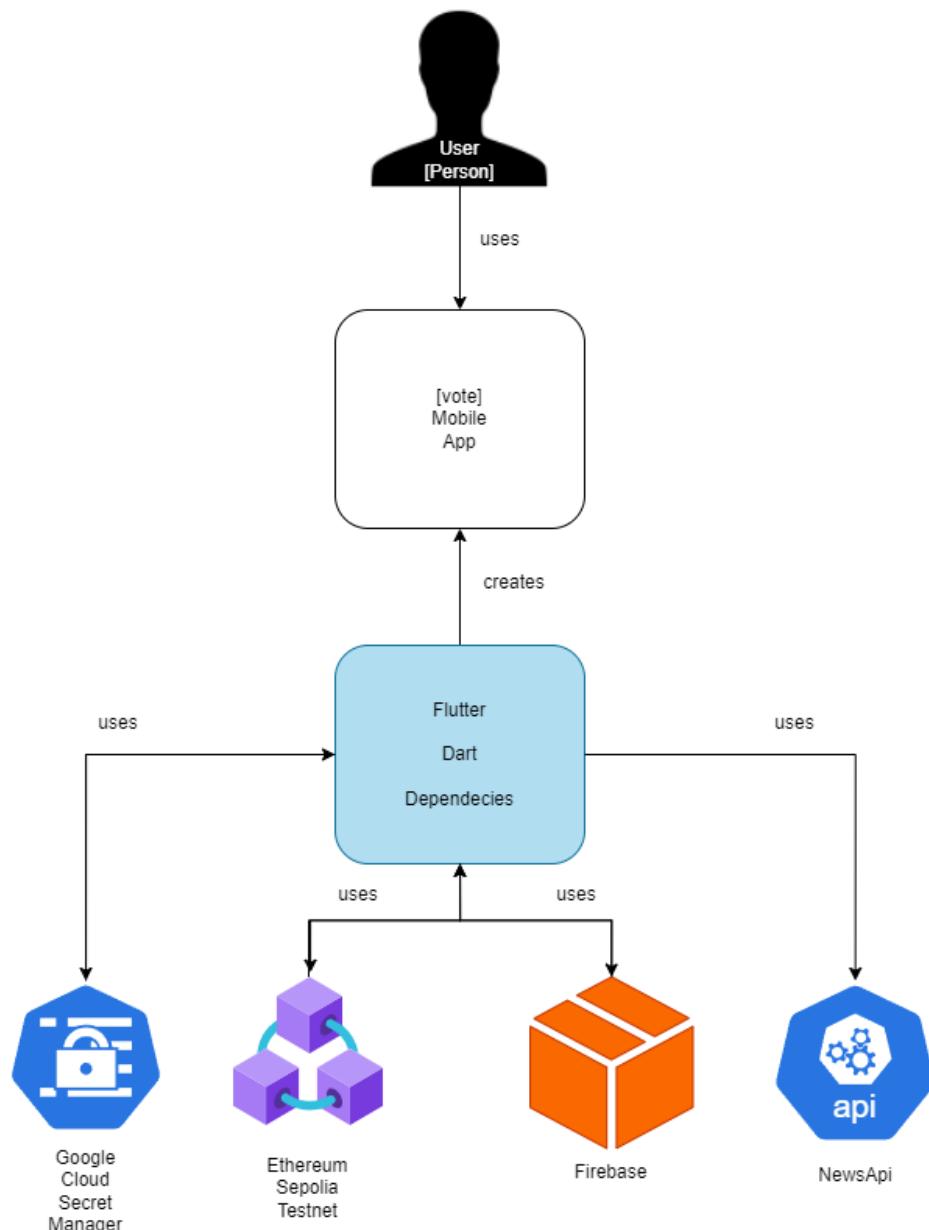


Figura 9.2: Diagrama C4 Nivel 1

### 9.1.2 Nivel 2

Vezi 9.3

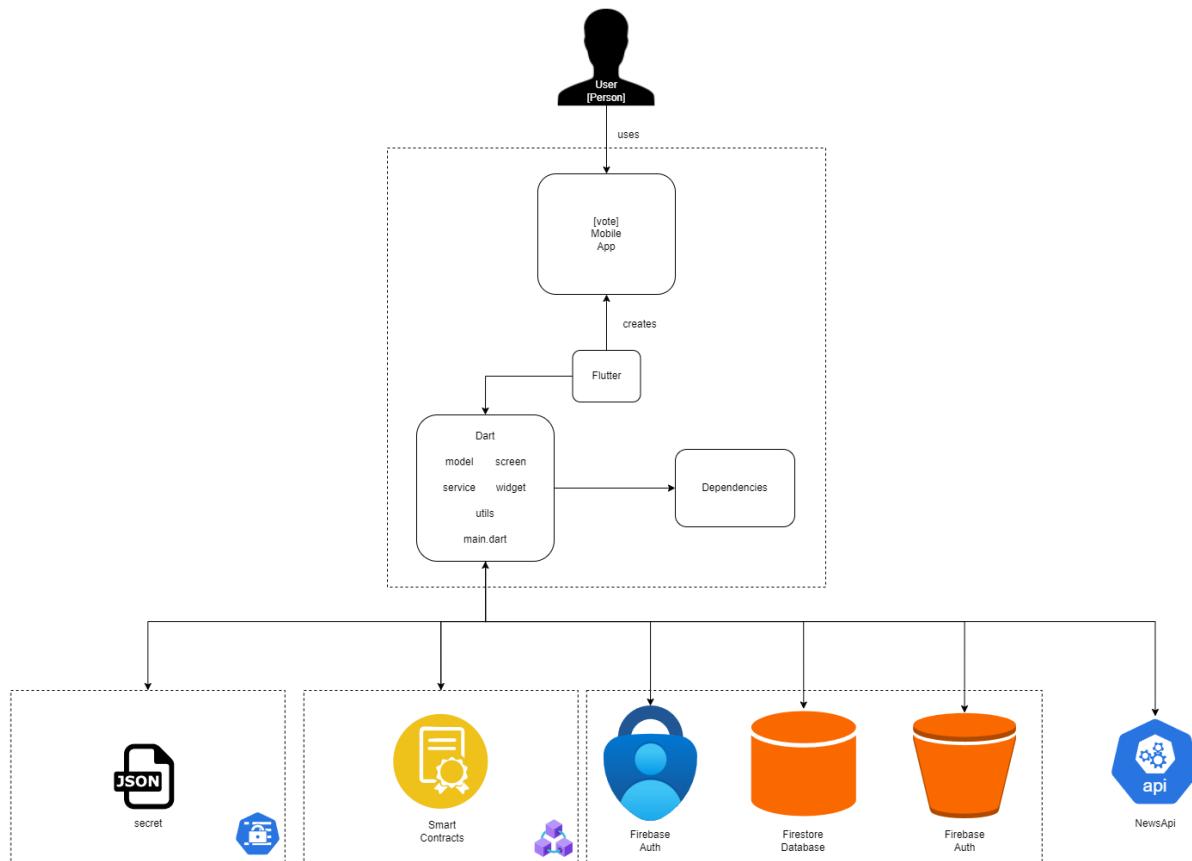


Figura 9.3: Diagrama C4 Nivel 2

### 9.1.3 Nivel 3

Vezi 9.4

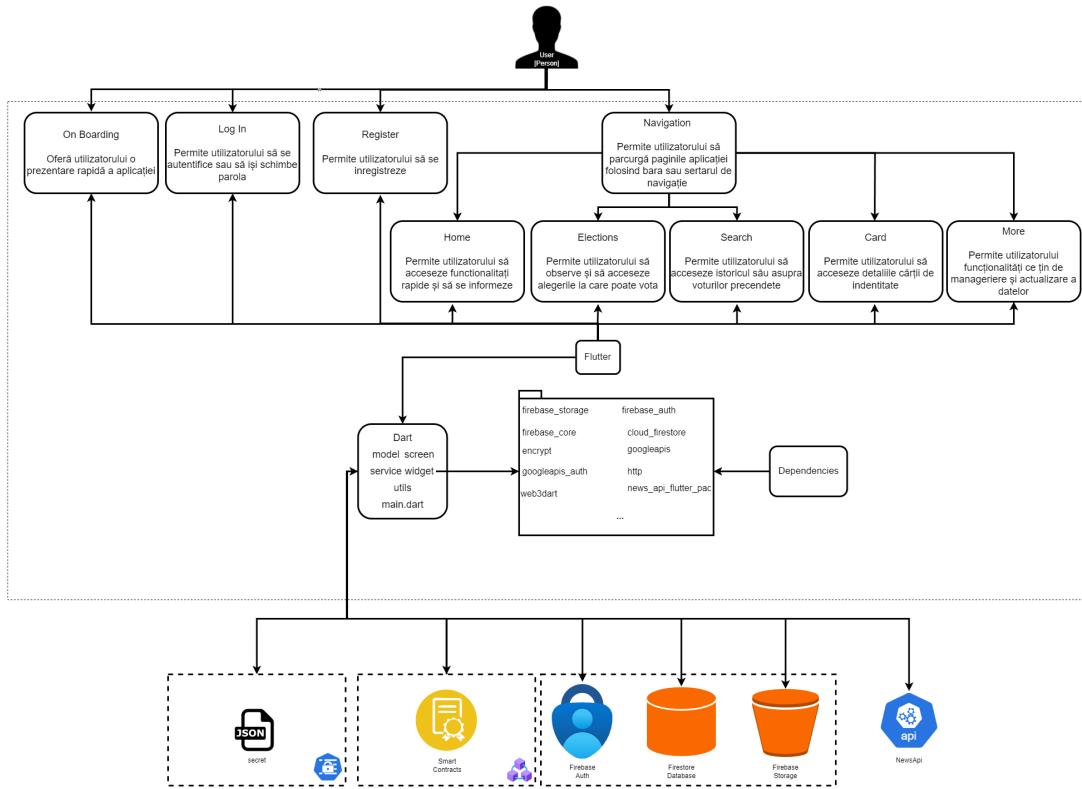


Figura 9.4: Diagrama C4 Nivel 3

#### 9.1.4 Nivel 4

##### Log In

Vezi 9.5

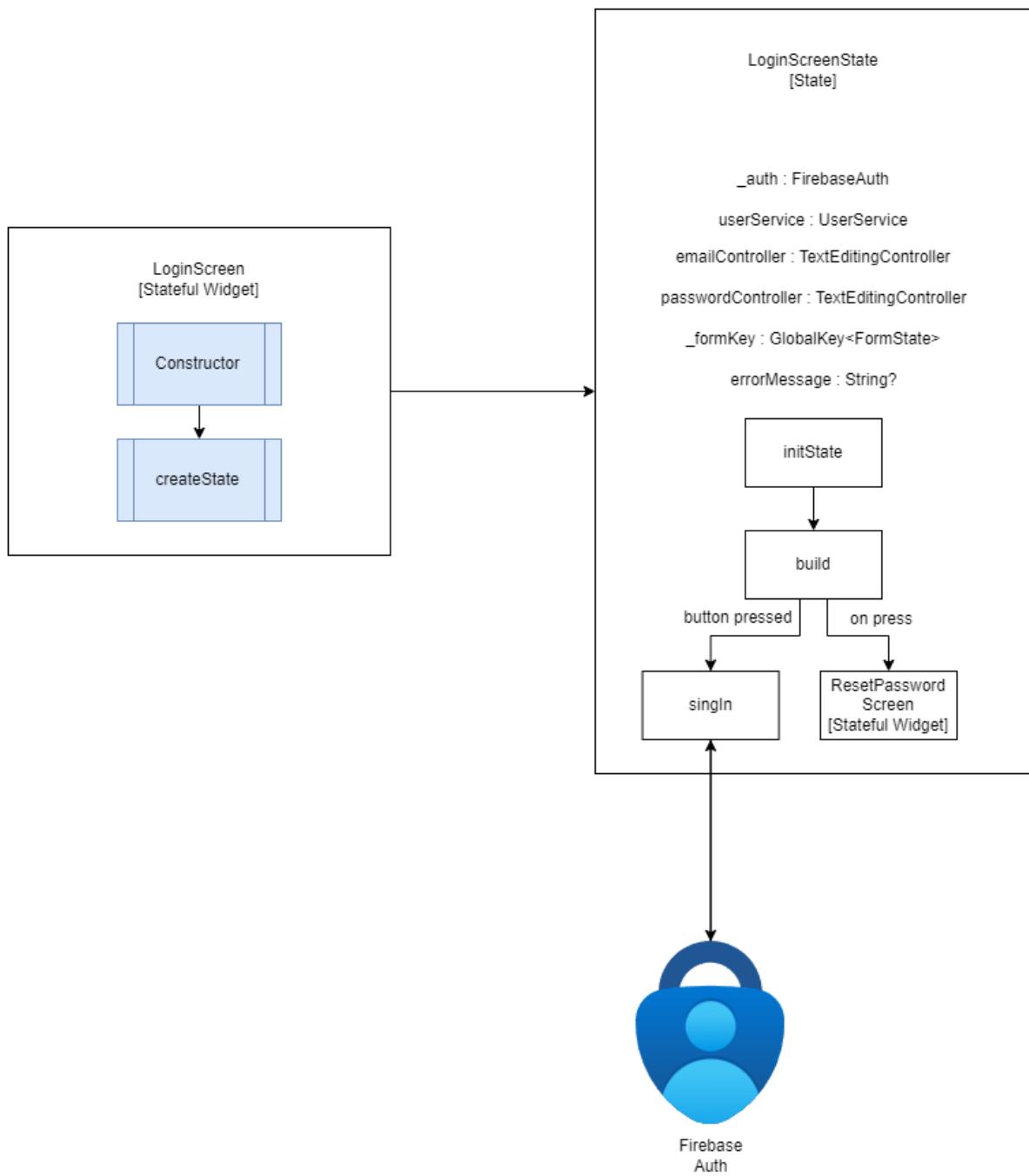


Figura 9.5: Diagrama C4 Nivel 4 Log in

## Register

Vezi 9.6

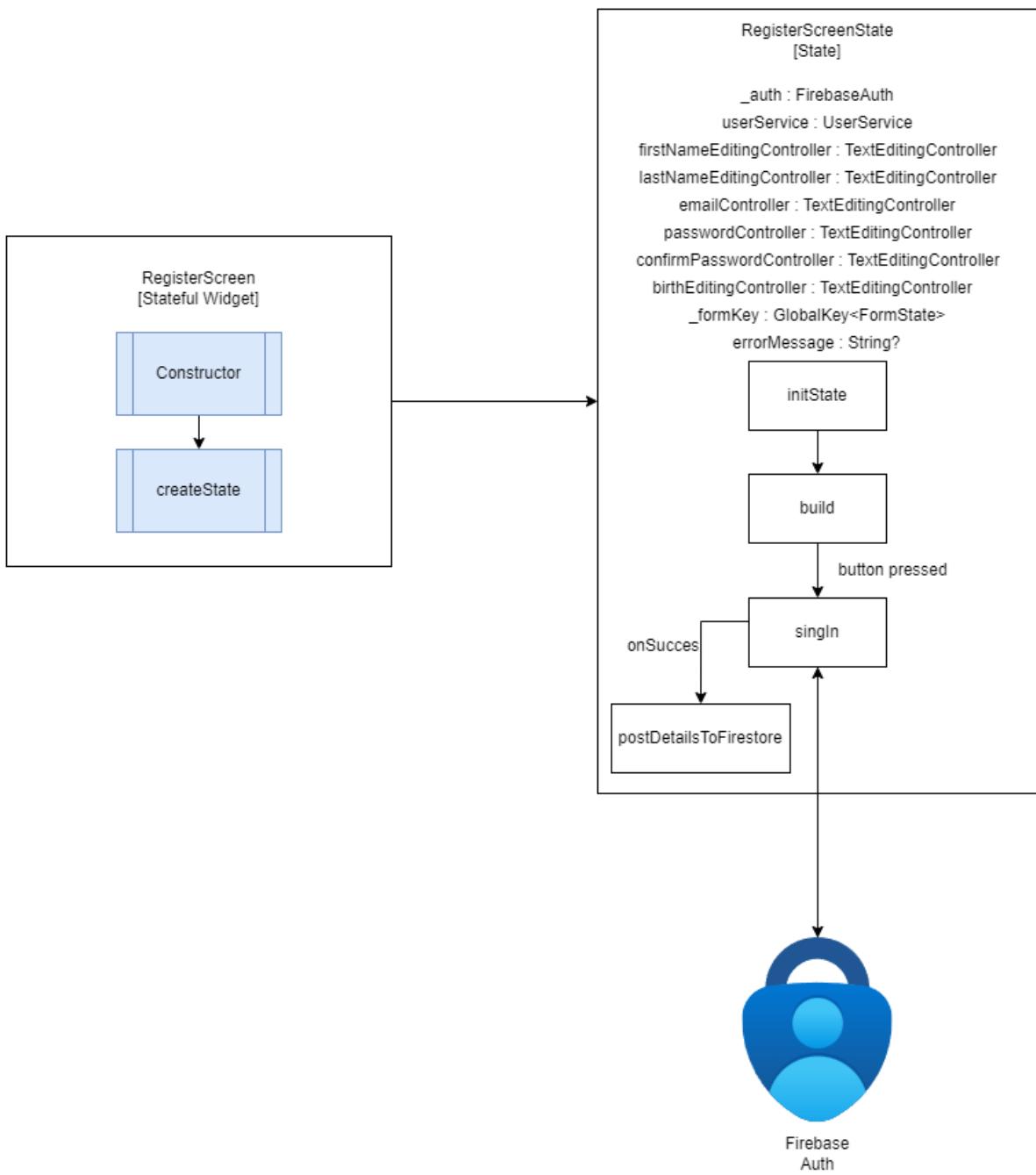


Figura 9.6: Diagrama C4 Nivel 4 Register

## Navigation

Vezi 9.7

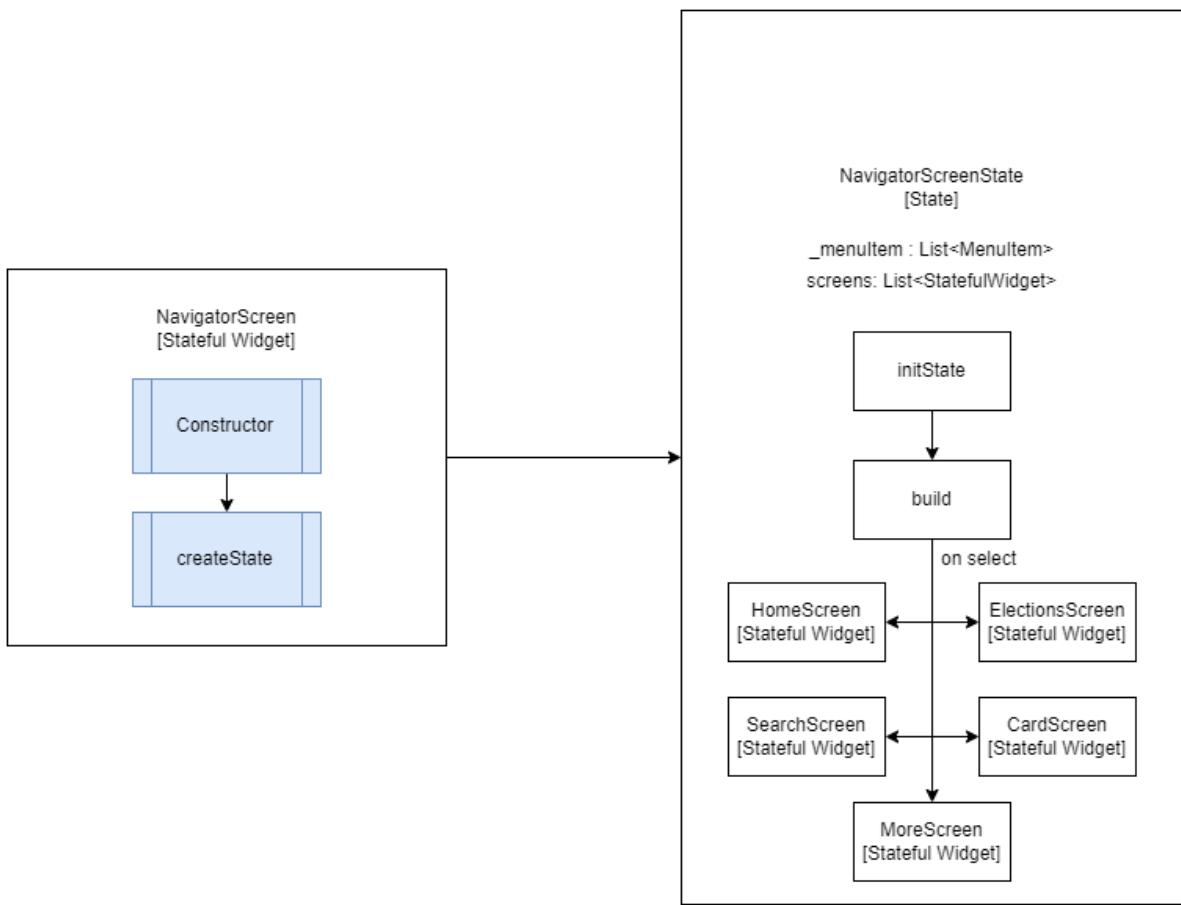


Figura 9.7: Diagrama C4 Nivel 4 Navigation

## Home

Vezi 9.8

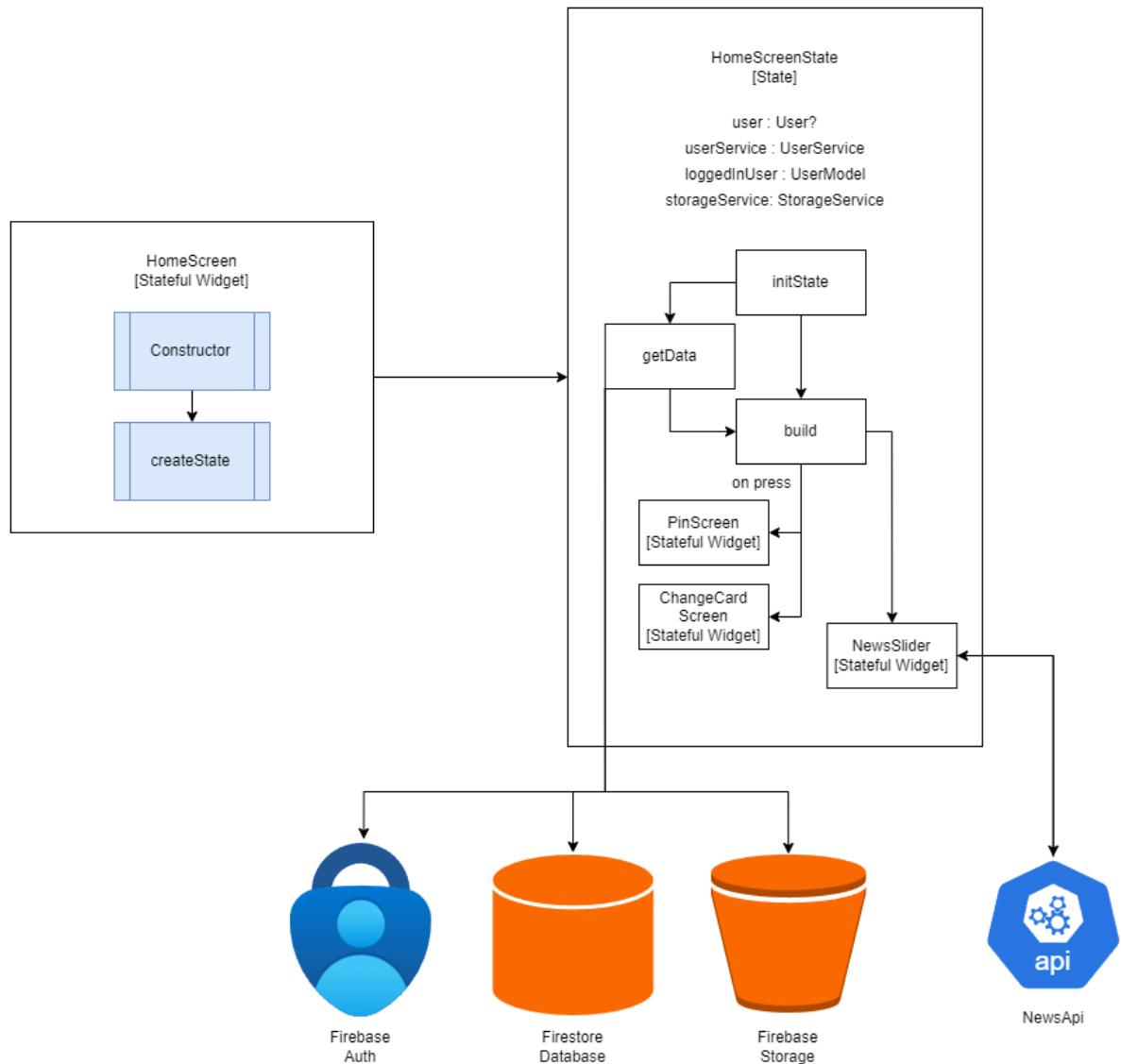


Figura 9.8: Diagrama C4 Nivel 4 Home

## Elections

Vezi 9.9

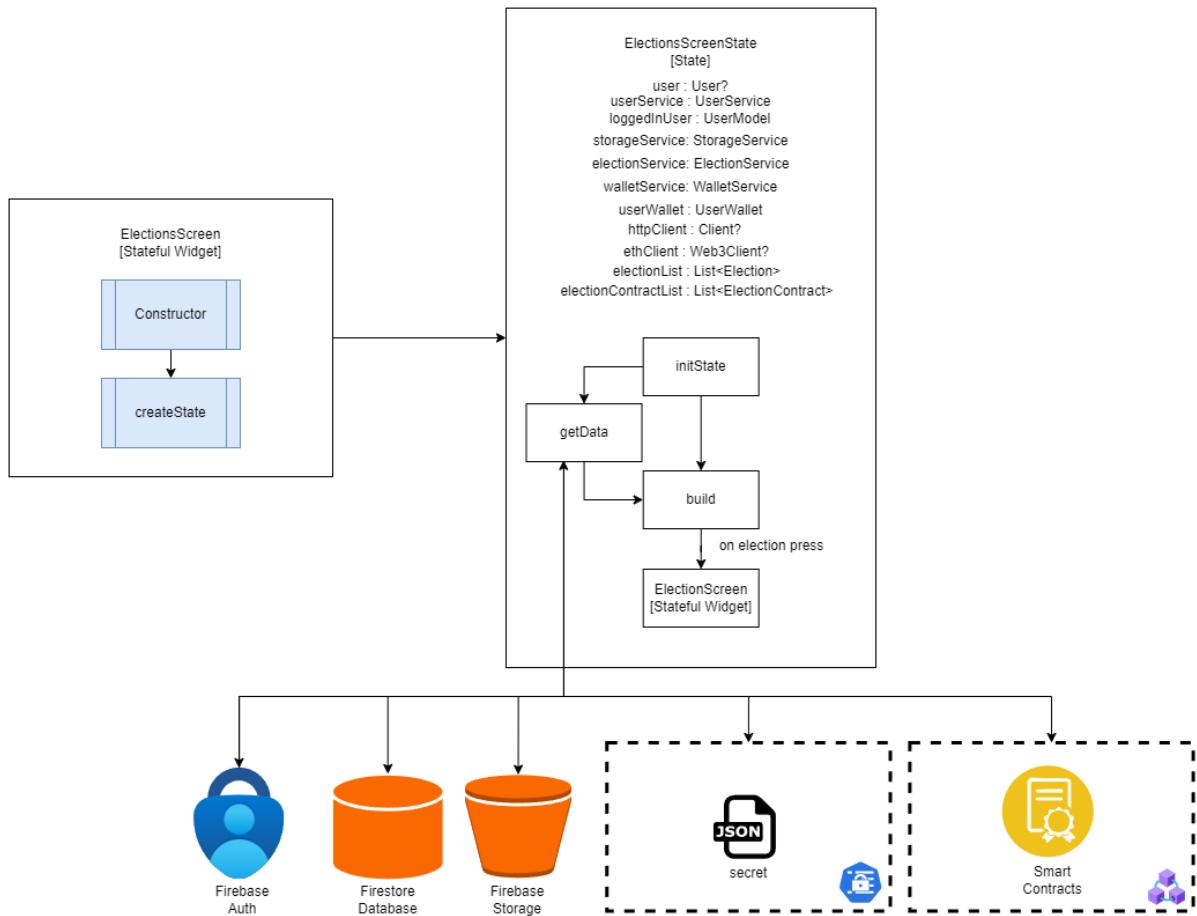


Figura 9.9: Diagrama C4 Nivel 4 Elections

## Search

Vezi 9.10

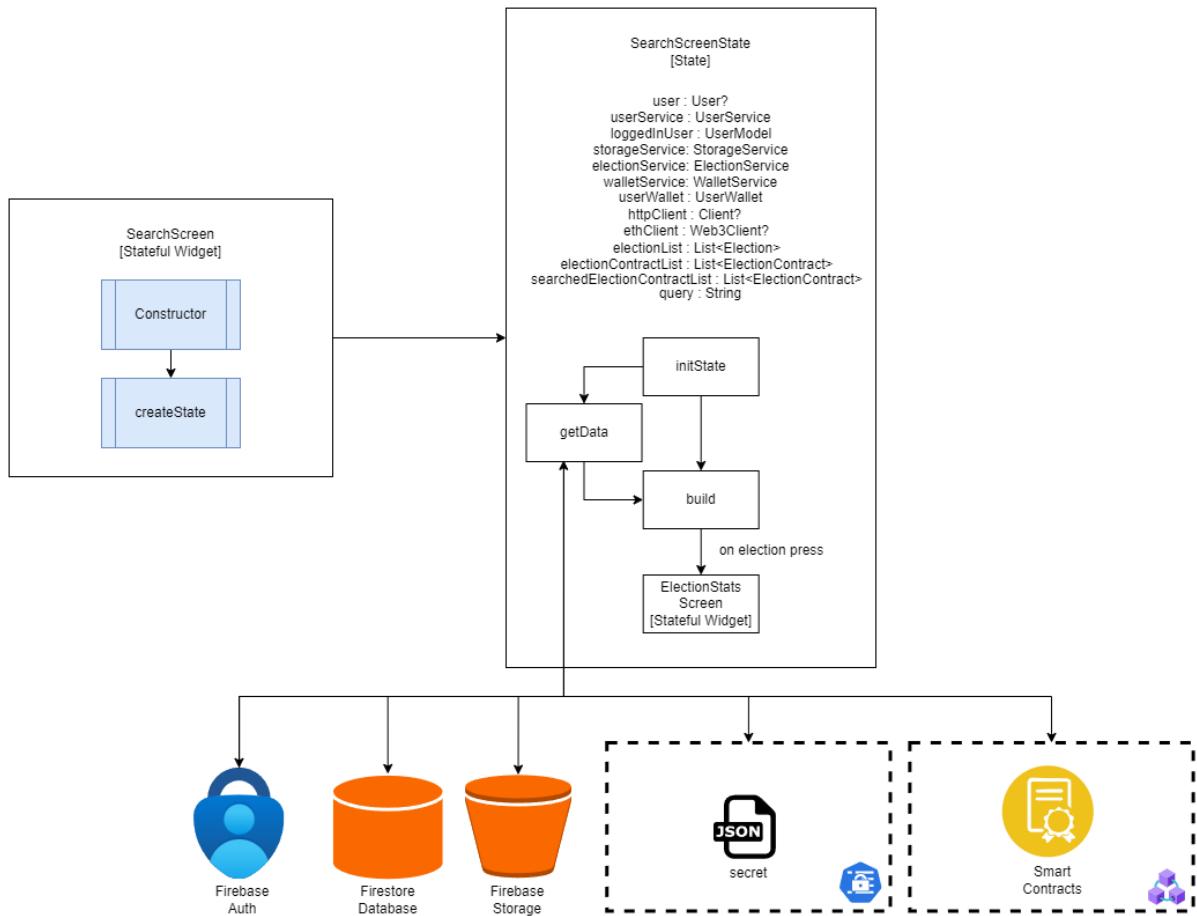


Figura 9.10: Diagrama C4 Nivel 4 Search

## Card

Vezi 9.11

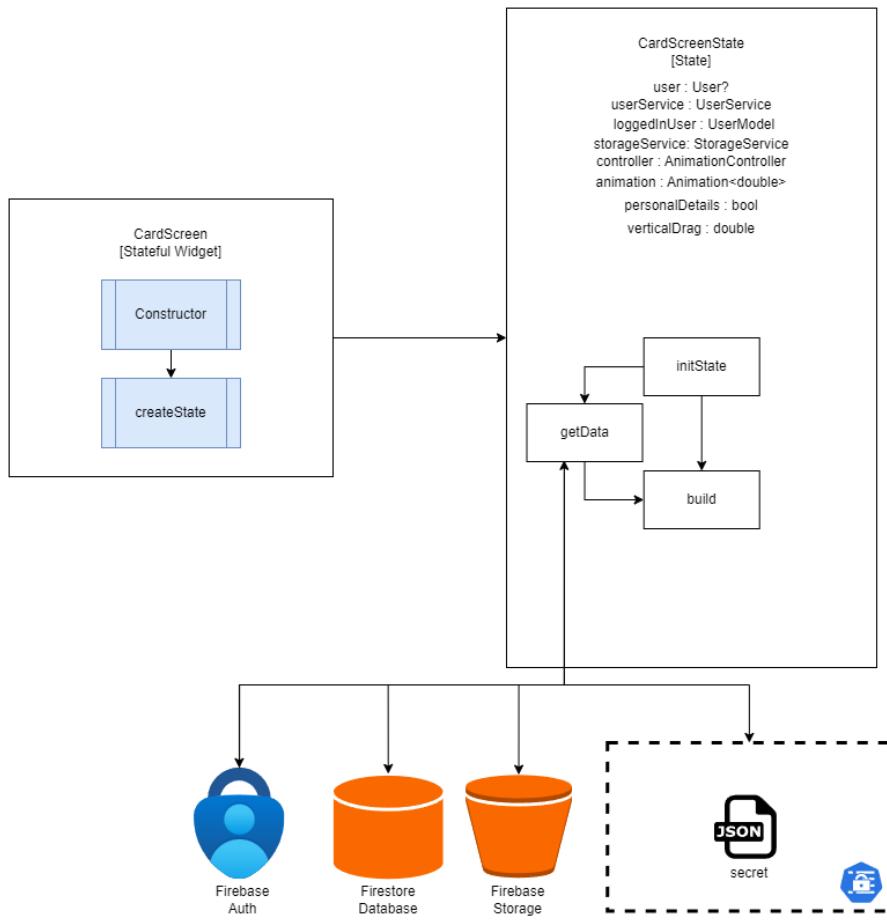


Figura 9.11: Diagrama C4 Nivel 4 Card

More

[Vezi 9.12](#)

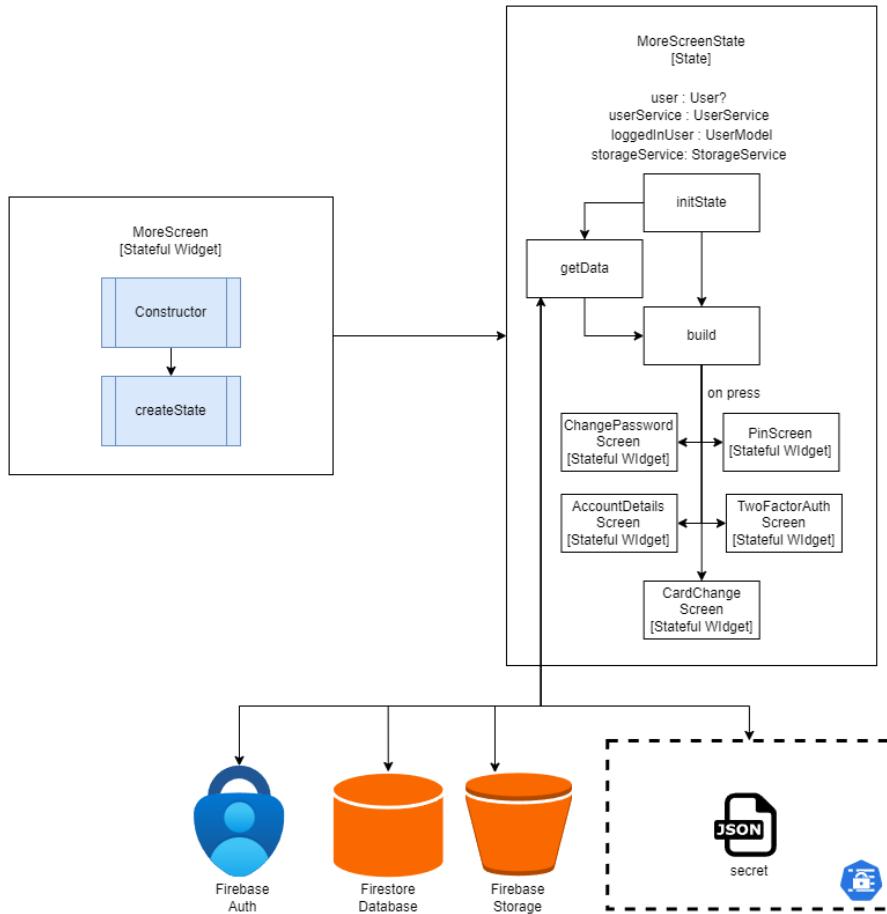


Figura 9.12: Diagrama C4 Nivel 4 More

## 9.2 Firestore Database

Firestore Database [15] reprezintă o bază de date, din cadrul platformei Firebase, ce conține documente de tip NoSQL și poate fi accesată prin intermediul SDK-urilor. Aceasta reușește să ofere notificări în timp real, iar datorită ecosistemului din care face parte prezintă potențial în simplificarea dezvoltării de aplicații.

Kesavan et al. [28] demonstrează cum folosirea acestui mijloc prezintă oportunități ce fac implementarea prototipizarea, iterarea și mentenanța aplicațiilor mai rapidă.

O bază de date își deservește scopul prin organizarea și stocarea informațiilor ce au un scop prestabilit. Aceste informații pot contribui în diferite moduri, de la simple date de prezentare până la imagini, modele sau alte elemente necesare.

Mentionat anterior, Firestore Database este o bază de date nerelațională, NoSQL, fapt ce implică anumite schimbări în modul de stocare. Acestea sunt des utilizate în aplicații web sau mobile și în domeniul Big Data deoarece natura sa oferă avantaje ca scalabilitate, disponibilitate, înțelegere ușoară și intuitivă.

Structura documentelor salvate folosind această unealtă este împărțină în 3 colecții:

user, election și wallet. Aspectul cel mai complex fiind stocarea detaliilor utilizatorului. Accesul unui document din cadrul unei astfel de colecții se realizează printr-un id aferent acestuia. Rezultatul fiind astfel informațiile de interes stocate.

Voi prezenta astfel în ordinea enumerării precedente colecțiile salvate folosind Firestore Database.

Colecția „user” reține detalii ce deservesc în identificarea utilizatorului. Putem accesa documentele folosind id-ul generat automat la înregistrare.

Câmpuri:

- dob - data de naștere a persoanei
- email - email-ul cu care persoane s-a înregistrat
- firstname - prenumele
- lastname - numele
- phoneNumber - numărul de telefon asignat în urma adăugării autenficării în doi pași
- pin - cod necesar pentru utilizarea anumitor funcționalități
- status - statusul cărții de identitate
- uid - id-ul asignat după autentificare
- idCard - colecție ce deține informațiile cardului de identificare (buletin) criptate
  - address - adresa domiciliului
  - city - orașul
  - country - țara
  - county - județul
  - dob - data de naștere
  - expireDate - data de expirare a cardului
  - firstname - prenumele
  - issueDate - data de emitere a cardului
  - lastname - numele
  - nationality - naționalitate
  - personalCode - codul numeri personal
  - sex - genul

Colecția „election” cuprinde alegerile, prezente cât și trecute, ce se află în rețeaua blockchain. Fiecare alegere este accesată folosind id-ul asignat.

Detalii prezente în fiecare document:

- contractAddress - adresa contractului inteligent la care se află alegerea, loc unde putem interoga spre aflarea informațiilor necesare despre aceasta (titlu, candidați și informații, data începerii) sau putem accesa anumite funcționalități
- testContract - o variabilă de tip boolean ce îmi ofer informația dacă acest contract este pentru testare, întrucât acestea au mici modificări aduse.
- img - calea la care se află imaginea alegerii, dacă nu este declarată se prezintă o imagine implicită

Colecția „wallet” deține detalii despre portofelele digitale ale utilizatorilor. Putem accesa un portofel folosind id-ul asignat. Un utilizator verificat are un portofel asignat pe baza codului numeric personal. Toate detalii afilate în cadrul acestui document sunt criptate.

Campuri:

- address - reprezintă adresa (sau cheia publică) prin care utilizatorul își face remarcată prezența
- owner - o variabilă ce ține codul numeric personal al deținătorului portofelului curent
- privateKey - cheia privată cu care utilizatorului poate performa anumite acțiuni

## 9.3 Firebase Storage

Firebase Storage face parte tot din suita oferită de platforma Firebase, aceasta are ca scop stocarea, organizarea și, mai apoi, accesarea datelor oferite de către client.

În cadrul aplicației, această unealtă ne permite stocarea imaginilor alegătorilor, alegătorilor și cele ale candidaților.

## 9.4 Firebase Authentication

Firebase Authentication este un instrument din cadrul Firebase ce oferă servicii, SDK-uri și librării de interfață specifice pentru procesele de înregistrare și autentificare. Aceasta oferă o multitudine de metode prin care utilizator se poate autentifica, de la utilizarea propriului email sau a numărului de telefon până la utilizarea furnizorul de identitate ca Google, Facebook și-md. Firebase Authentication susține și autentificarea în doi pași, acesta poate trimite sms-uri sau mesaje pe numarul de telefon sau email-ul asignat.

Integrarea cu acest instrument oferă aplicației noastre următoarele funcții de interes :

- Oferă posibilitatea înregistrării și autentificării
- Folosirea autentificării în doi pasi
- Oferirea opțiunii de "am uitat parola"

## 9.5 Google Cloud Secret Manager

Mentionat anterior în Capitolul 7, acesta este mediul unde avem salvate perechile de chei.

- cheie privată fernet - folosită în criptarea și decriptarea informațiilor sensibile, exemplu detaliu ale cărții de identitate.
- cheii private rsa - folosite pentru decriptarea datelor ce țin de portofelele asignate alegătorului, fiecare portofel este astfel criptat și decriptat folosind un set de chei diferit disponibil doar utilizatorului eligibil.

## 9.6 Flutter Application

În această secțiune discutăm despre arhitectura ce țin de partea interfeței grafice pe care utilizatorul o folosește cât și integrarea cu funcționalitățile aferent.

Prin prisma interfeței este oferit astfel un mod simplu, ușor de înțeles și intuitiv pentru utilizator de consumare a funcționalităților oferite.

Funcționalitățile implementate deservesc pentru :

- Crearea unei conexiuni cu platforma Firebase
- Utilizarea informațiilor primite în urma comunicării
- Contopirea cu interfața grafică
- Stocarea și managerierea datelor oferite de utilizator
- Realizarea fluxului de date ce trece prin toate procesele anterior menționate în Capitolul 7

Punerea în aplicare a fost realizată folosind Flutter și limbajul aferent Dart.

Structura implementării este împărțită astfel:

- Model
- Service

- Screen
- Widget
- Utils

### 9.6.1 Model

„Model” conține modelele, cu atributele aferente, specifice documentelor salvate în baza de date Firestore Database dar și necesare prezentării informațiilor unei alegeri ce vin din interogarea contractelor inteligente. Astfel, pentru fiecare element avem un obiect caracteristic ce detine informațiile acestuia.

Se remarcă urmatoarele modele:

- Article - articolele extrase cu ajutorul news api
- Candidate - candidații ce sunt extrași după interogarea contractului intelligent
- Election - alegerile extrase din Firebase DB
- ElectionContract - informațiile despre alegere extrase în urma tranzacțiilor cu funcții de interogare
- UserModel - informațiile campurilor asignate documentului user din cadrul Firebase DB
- WalletModel - informațiile campurilor asignate documentului wallet din cadrul Firebase DB

### 9.6.2 Service

„Service” conține serviciile din cadrul aplicației ce sunt folosite pe tot parcursul acesteia. Fiecare model anterior prezentat are asociat un serviciu care îi permite extragerea și manipularea informațiilor. Pe langă acestea există un serviciu specializat pentru contractele inteligente și pentru criptarea sau decriptarea informațiilor sensibile.

Arhitectura cuprinde urmatoarele servicii:

- ElectionService - extragem și manipulam informații legate de alegeri din Firebase DB
- ContractService - extragem informații legate de alegeri, interogam și performam anumite funcționalități asupra contractelor inteligente sub forma de tranzacții în rețeaua blockchain-ului

- UserService - extragem, manipulam și actualizam informații legate de alegeri din Firebase DB
- WalletService - extragem și manipulam informații legate de portofele din Firebase DB
- EncryptionService - criptam și decriptam datele ce sosesc sau părăsesc aplicația cu ajutorul cheilor oferite de secretul stocat în Storage Manager
- FaceRecognitionService - realizăm verificarea pozei cărtii de identitate cu cea a pozei oferite de utilizator

### 9.6.3 Screen

„Screen” conține toate fișierele necesare pentru interfața oferită utilizatorului. Un *ecran* pe care utilizatorul îl accesează are un astfel de fisier asignat. Prin intermediul lor putem astfel oferi informațiile, funcționalitățile și disponibilitatea pe care o are fiecare utilizator.

Aceasta este cea mai complexă parte și arată astfel:

- card
  - CardScreen
- elections
  - ElectionsScreen
  - ElectionScreen
- home
  - HomeScreen
- menu
  - MenuScreen
- more
  - AccountDetailsScreen
  - ChangePasswordScreen
  - MoreScreen
  - PinScreen
  - TwoFactorAuthScreen

- navigator
  - NavigatorScreen
- onboarding
  - OnBoardingScreen
  - Intro1Screen
  - Intro2Screen
  - Intro3Screen
  - Intro4Screen
- search
  - SearchScreen
  - ElectionStatsScreen
- singup/signin
  - ForgotPasswordScreen
  - RegistrationScreen
  - LoginScreen
- verify
  - CardChangeScreen
  - CardDetailsScreen
  - FacialRecognitionScreen
  - VerifyIntroScreen

#### **9.6.4 Widget**

„Widget” conține elemente de interfață grafice reutilizabile ce sunt folosite pe parcursul aplicației. Astfel de obiecte pot avea scop grafic și/sau funcțional.

Aplicația cuprinde următoarele widget-uri:

- CodeDialogBox
- CustomCardWidget
- CountryPickerWidget
- CustomDialogWidget

- DatePickerWidget
- MenuWidget
- NewsSliderItem
- NewsSlider
- PinDialogWidget
- RadialProgress
- SearchWidget
- TwoFactorCardWidget

### 9.6.5 Utils

„Utils” cuprinde tema asignată aplicației. Această tema conține valori pentru 2 tipuri de teme și anume: dark și light. Fiecare temă are la randul ei definite variabile specifice tipului.

Acesta este scheletul unei teme:

- font
- luminozitate
- culoare primara
- culoare fundalului schelei
- culoare fundalului dialogului
- tema pentru text
- tema pentru butoane
- tema pentru icoane
- tema pentru liste
- tema pentru pachete - spre exemplu logo

## 9.7 Solidity

În această secțiune vom prezenta folosirea limbajului Solidity în crearea contractelor inteligente. Acestea vor conține reguli pentru desfășurarea unui proces electoral. Toate caracteristicile acestui contract vor fi construite pe baza informațiilor ce au rezultat în urma cercetărilor realizate asupra sistemelor de vot bazate pe blockchain, dar vor respecta și cerințele pe care le impune stereotipul ideal al unei alegeri electorale.

Următoarea listă prezintă atributele pe care le deține un astfel de contract, toate acestea sunt declarate să fie private, dar le putem accesa folosind metodele din contract.

- `_candidates` - o listă a candidaților, fiecare candidat are un nume, o descriere și un număr de voturi
- `_eligibleVoters` - informații salvate sub formă cheie-valoare, cheia reprezentând adresa, iar valoare reprezentă o structură ce conține trei valori: alegerea votantului, dacă acesta a votat și dacă este eligibil.
- `_electionName` - numele alegerii
- `_country` - țara unde se desfășoară
- `_startDate` - data de începere a alegerii în secunde [59]
- `_duration` - durata de desfășurare în secunde
- `_totalVotes` - numărul total de voturi

Tabelul de mai jos va prezenta proprietățile contractului creat împreună cu funcția și cerințele sau aspectele pe care acestea reușesc să le asigure.

Proprietate	Cerințe Asigurate
getElectionInfo()	Aceasta este o metodă prin care putem extrage informațiile alegerii
getNumOfCandidates()	Metodă ce oferă numărul de candidați ai procesului electoral definit
getCandidateInfo(uint)	Putem extrage informații legate de candidați ca nume și cteva detalii despre acesta (partid/candidat independent)
getTotalVotes()	Funcție ce oferă numărul de voturi totale la momentul apelării
hasStarted()	Metodă booleană ce transmite dacă a inceput desfășurarea alegerii
hasFinished()	Metodă booleană ce transmite dacă s-a finalizat desfășurarea alegerii
isRunning()	Metodă booleană ce transmite dacă stadiul curent al alegerii este ”în desfășurare”
isEligible()	Această metodă oferă o valoare booleană în funcție de eligibilitatea față de procesul electoral al utilizatorului care o apelează, asigurând proprietatea de <b>eligibilitate</b>
alreadyVoted()	Prin prisma acestei metode verificăm dacă un anumit alegător a votat deja, asigurând astfel <b>unicitatea</b>
vote(uint)	Aceasta este cea mai importantă metodă, ea ne oferă posibilitatea de a înregistra un vot la procesul electoral. Pentru apelarea acestei metode există cerințe de <b>eligibilitate, unicitate, corectitudine și disponibilitate</b> pe care un utilizator trebuie să le îndeplinească. Un vot poate fi exercitat o singură dată, această practică se consolidează prin încercarea de oferire a fondurilor exacte pentru o unică tranzacție
whom()	Cu ajutorul acestei metode utilizatorul poate observa contribuția sa la vot, dar respectându-se intimitatea și corectitudinea prin neafișarea rezultatului înainte de finalizare alegerii.
constructor(args)	Constructorul asignează aspecte ce țin de procesul electoral.
getCandidateResults()	Similară metodei <i>getCandidateInfo</i> , singura modificare este o extensie prin care apare numărul de voturi ale candidaților, dar care este disponibil doar după finalizarea alegerilor pentru a nu influența alegătorii.

Pentru testare au fost adăugate două metode, un modificador și un atribut:

- resetVoteForAddress - această metodă poate fi accesată doar de creator, poate reseta votul unui alegător.
- setDate - această metodă setează data și durata alegerii.
- ownerOnly - modificador ce permite accesul doar creatorului.
- owner - atribut de tip adresă ce conține adresa creatorului

## 9.8 Remix IDE

Remix IDE a fost folosit pentru desfășurarea proceselor de testare și monitorizare a alegerilor ce sunt reprezentate prin contracte inteligente încărcate în rețeaua blockchain. Am folosit zona de test pe care o oferă acest mediu de dezvoltare, zonă care simulează comportamentul unei rețele blockchain, dar am folosit și opțiunea de monitorizare a contractelor inteligente încarcate pe rețeaua de test Sepolia.

## 9.9 Google Colab

Platforma Google Colab a fost folosită pentru procesul de pregătire a datelor, acest proces împărțindu-se în două categorii:

1. Alegeri - conține funcționalități ce țin de întregul proces de pregătire până la încărcare.
  - (a) Pregătire - datele sunt extrase din fișierele JSON, filtrate și pregătite pentru asignare.
  - (b) Generare și Asocierea - se vor genera portofele și seturi de chei de criptare pentru toți alegătorii eligibili, datele portofelelor fiind salvate în mod criptat în baza de date Firebase, iar legătura dintre alegător și portofel, și cheia de decriptare vor fi salvate pe Google Cloud Secret Manager.
  - (c) Asignare - sunt setate informațiile alegerilor, inclusiv adresele persoanelor eligibile de vot (pentru a se păstra anonimitatea).
  - (d) Încărcare - sunt încărcate contractele inteligente ale alegerilor.
2. Securitate - sunt create, asignate și folosite seturile de chei pentru informațiile sensibile și ale portofelelor.

## **9.10 NewsApi**

NewsApi a fost folosit pentru a oferi o zonă de informare utilizatorului, astfel oferindu-i acestuia date de interes legate de politică. Astfel, aplicăm o cerere specifică asupra articolelor pe care le dorim a fi afișate.

## **9.11 Mențiuni ce țin de mediu**

### **9.11.1 Ethereum și Sepolia**

Această secțiune reprezintă doar mențiunea utilizării rețelei de test Sepolia din cadrul Ethereum pentru încărcarea contractelor inteligente.

### **9.11.2 MetaMask**

Această secțiune reprezintă doar mențiunea utilizării MetaMask manageriarea și crearea portofelelor ce vor lua parte la alegeri.

### **9.11.3 Infura**

Această secțiune reprezintă doar mențiunea folosirii Infura pentru realizarea conexiunii dintre aplicație și rețeaua de test Sepolia.

# Capitolul 10

## Aplicația Mobilă

### 10.1 On Boarding

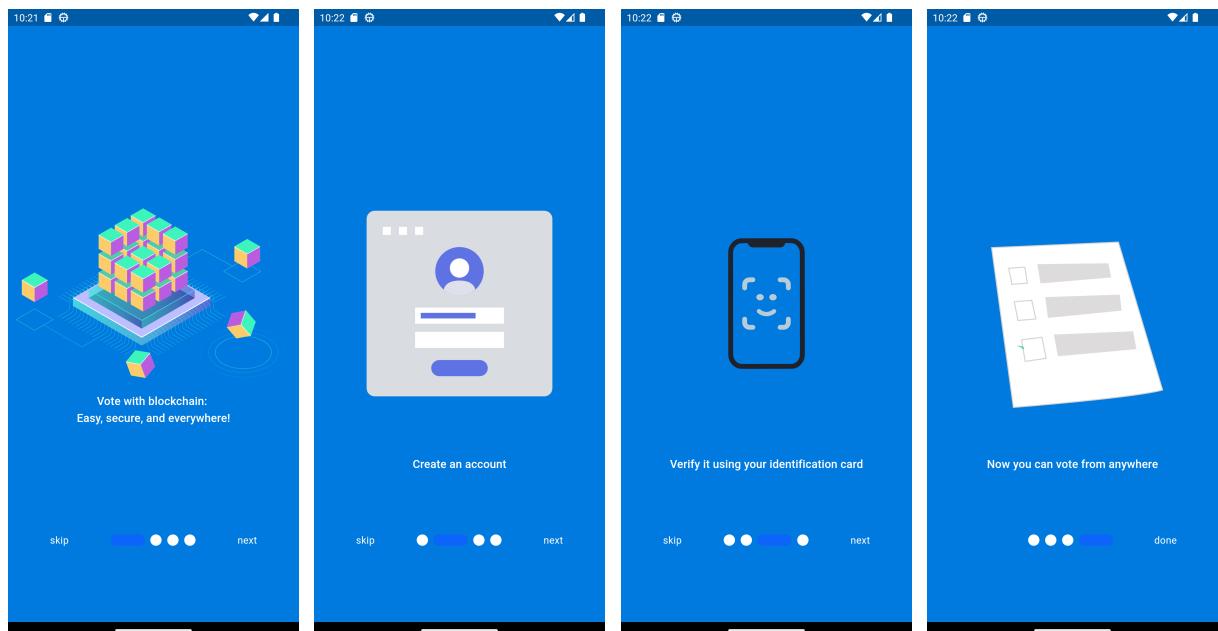
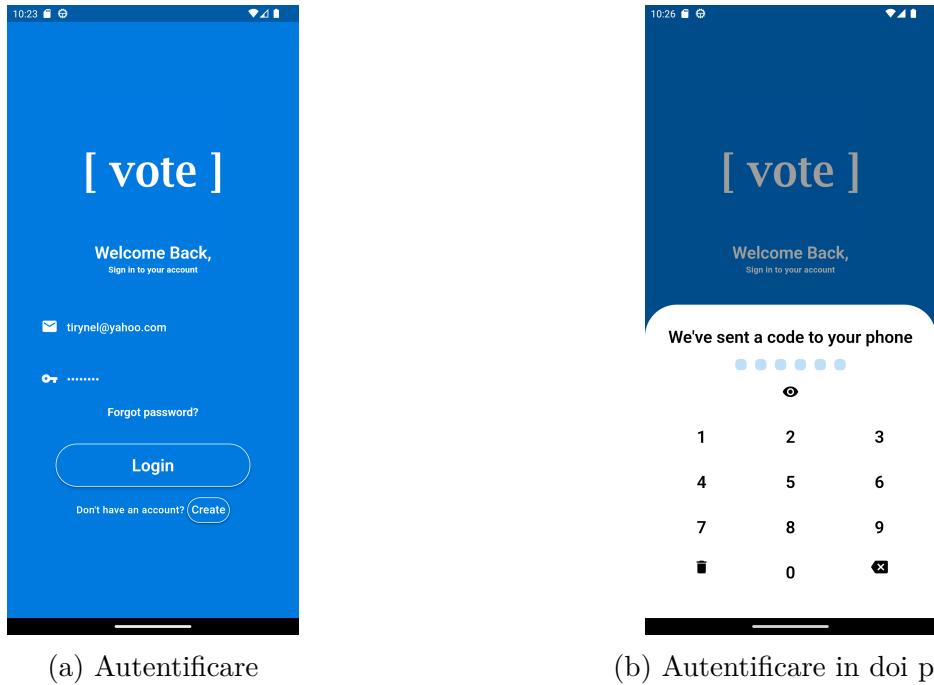


Figura 10.1: Ecranele de prezentare a aplicației

## 10.2 Login



(a) Autentificare

(b) Autentificare in doi pași

Figura 10.2: Ecranele pentru autentificare

### 10.2.1 Reset Password

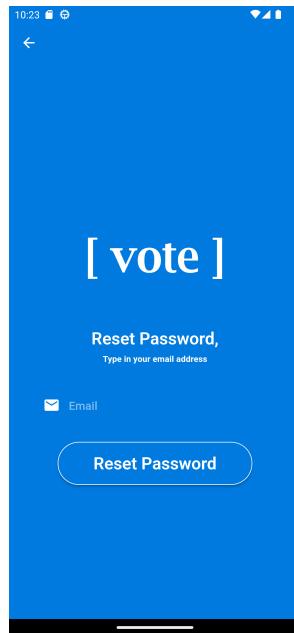


Figura 10.3: Ecran pentru resetarea parolei

## 10.3 Register

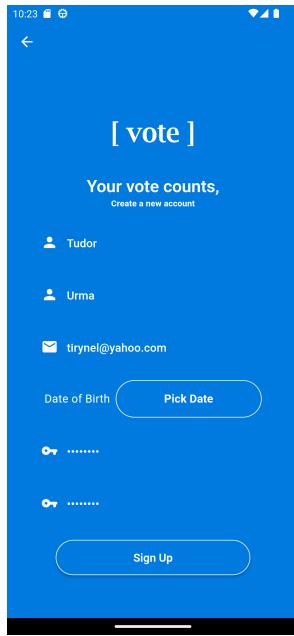


Figura 10.4: Ecran pentru înregistrare

## 10.4 Navigation

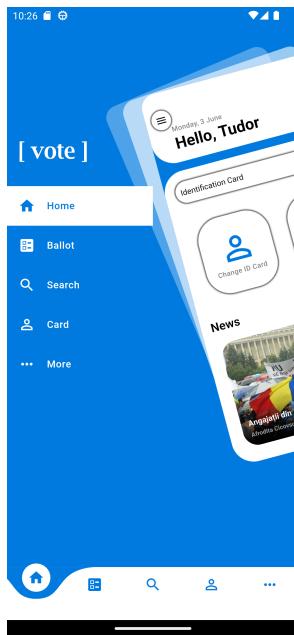


Figura 10.5: Bara și sertarul de navigație

## 10.5 Home

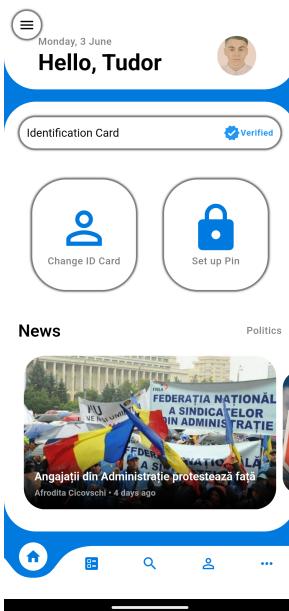
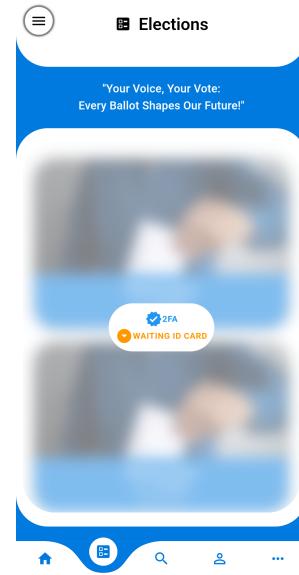


Figura 10.6: Ecranul acasă

## 10.6 Elections



(a) Alegeri cont verificat



(b) Alegeri cont neverificat

Figura 10.7: Ecranele pentru alegeri

### 10.6.1 Election



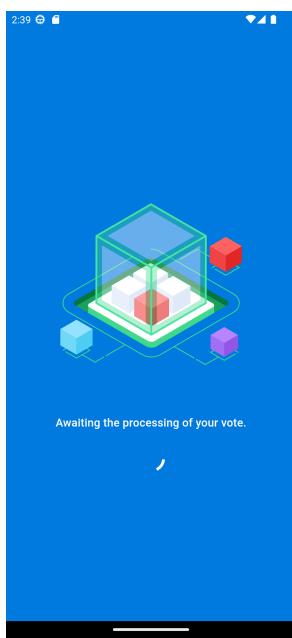
(a) Detaliile alegerii



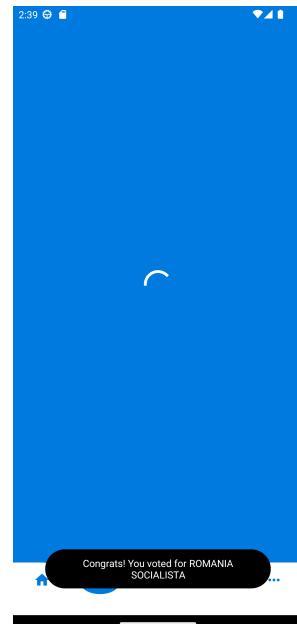
(b) Selecția unui candidat



(c) Exprimarea votului pentru candidatul ales



(d) Așteptarea pentru confirmarea alegerii



(e) Alegerea candidatului a fost finalizată cu succes

Figura 10.8: Ecranele pentru orice alegere

## 10.7 Search

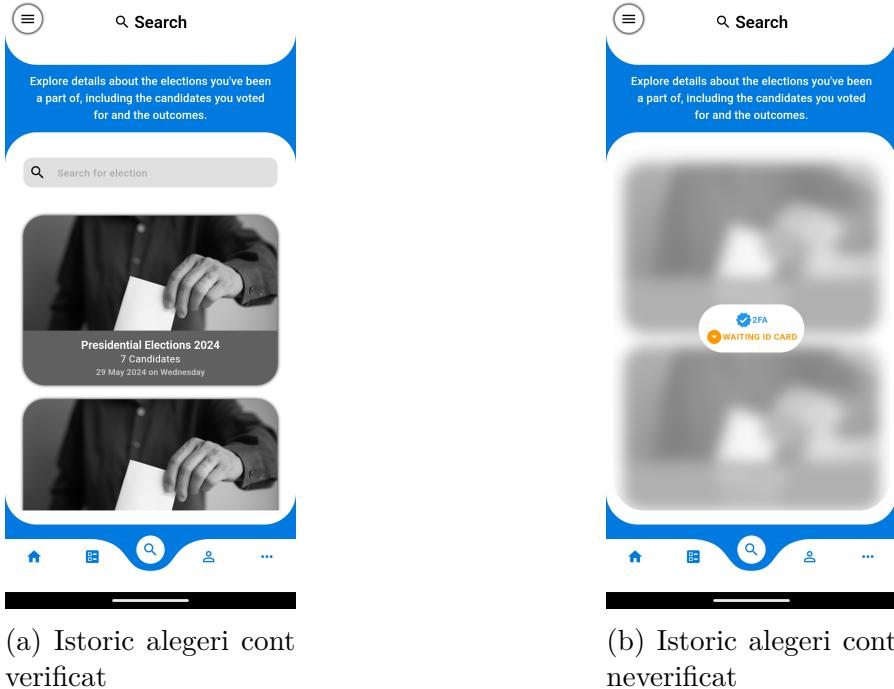


Figura 10.9: Ecranele pentru istoricul alegerilor

### 10.7.1 Election Statistics

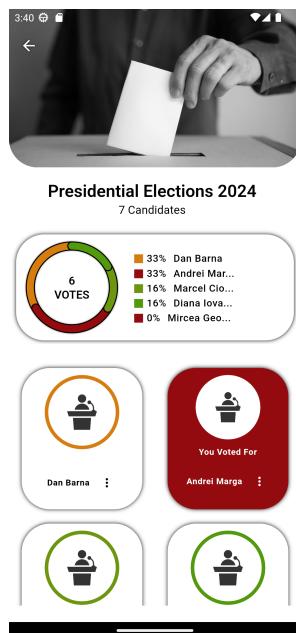


Figura 10.10: Ecranul pentru statisticile oricărei alegeri

## 10.8 Card

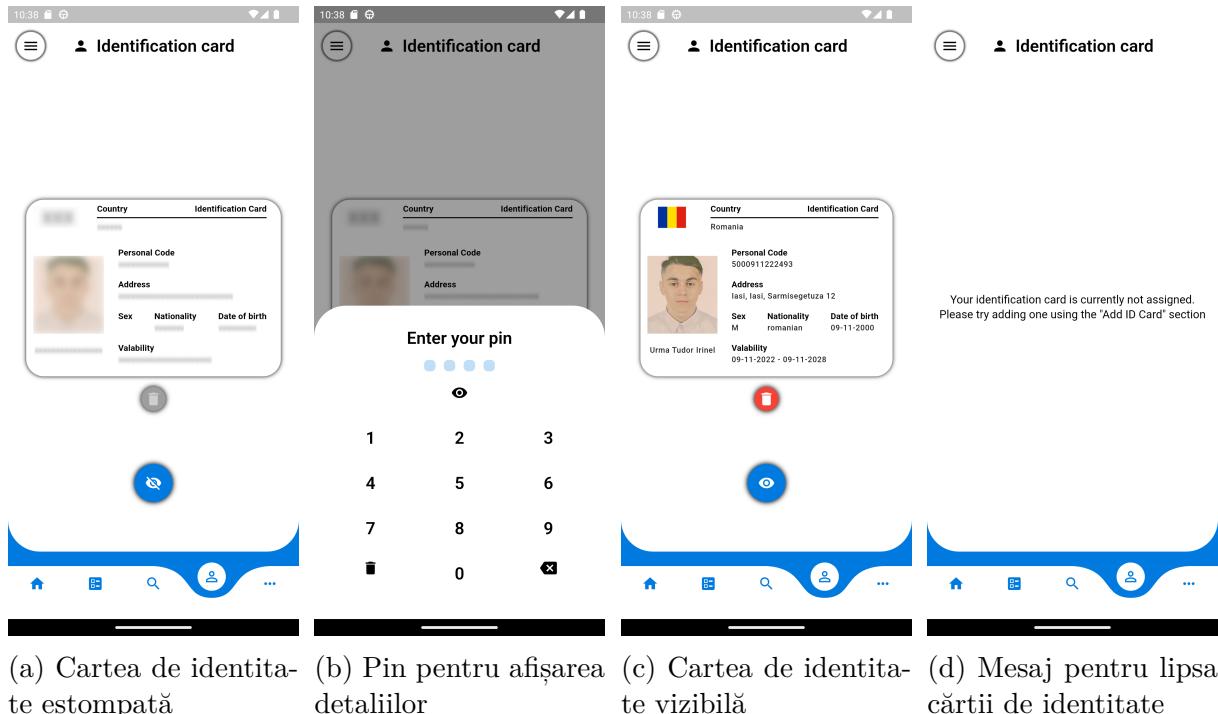


Figura 10.11: Ecranele de afișare a cărții de identitate

## 10.9 More

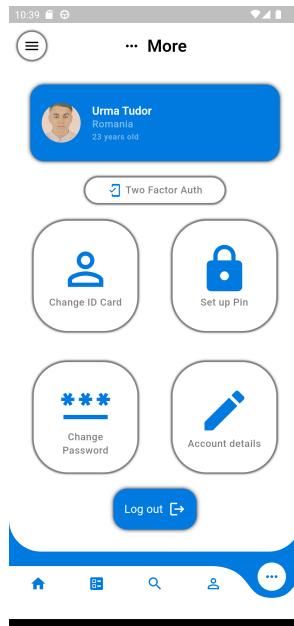
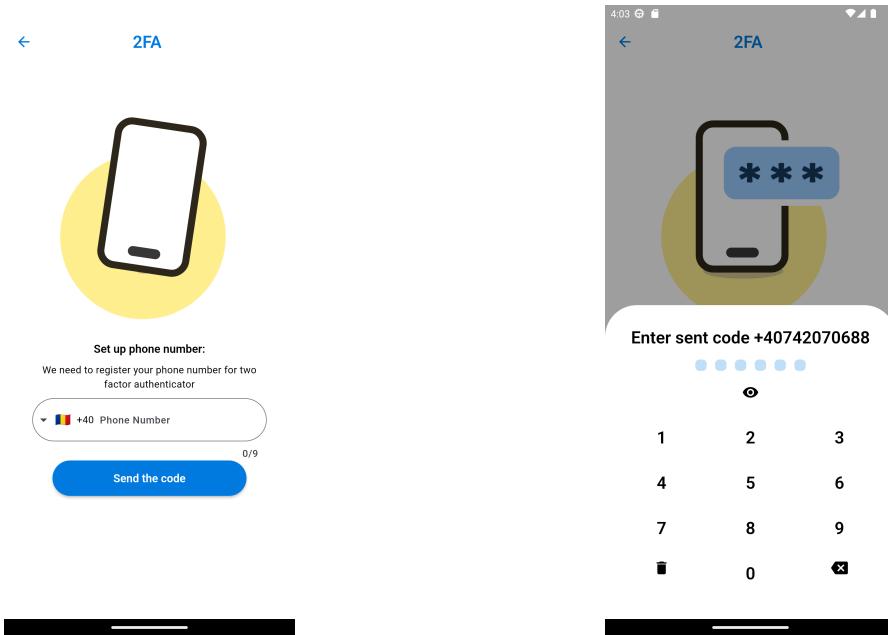


Figura 10.12: Ecran pentru secțiunea mai multe

### 10.9.1 Two Factor Authenticator

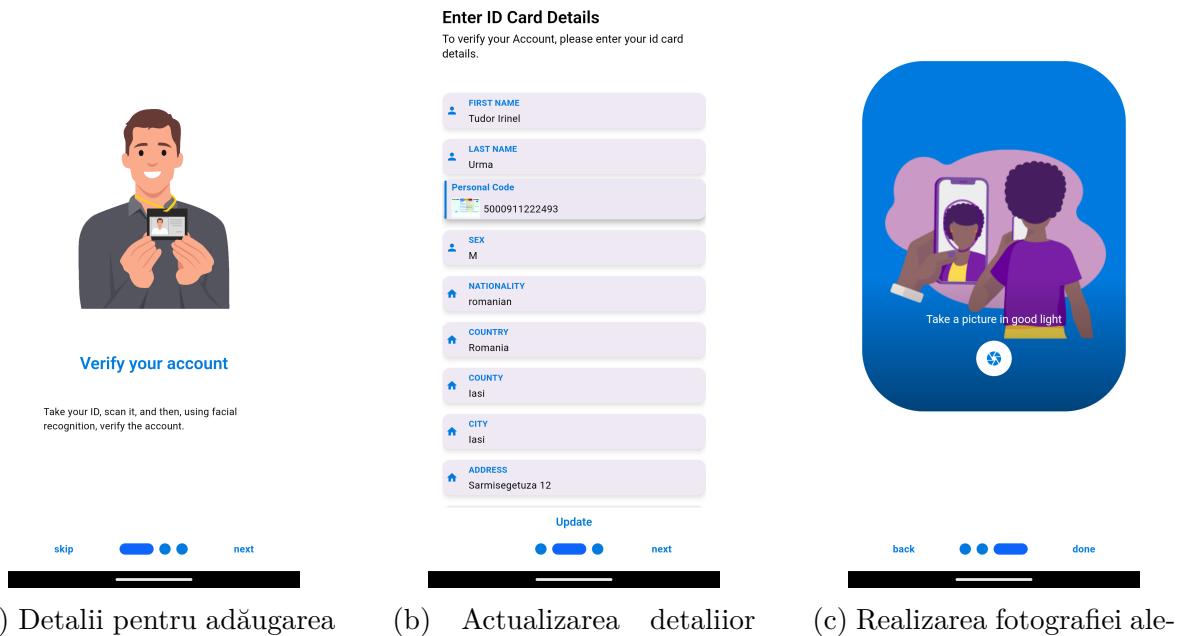


(a) Ecran pentru adăugarea autentificării în doi pași

(b) Cod de identificare primit pe numarul de telefon

Figura 10.13: Ecranele pentru configurarea autentificării în doi pași

### 10.9.2 Add/Change Id Card



(a) Detalii pentru adăugarea cărții de identitate

(b) Actualizarea detaliilor cărții de identitate

(c) Realizarea fotografiei ale gătorului

Figura 10.14: Ecrane pentru adăugarea cărții de identitate

### 10.9.3 Set up Pin

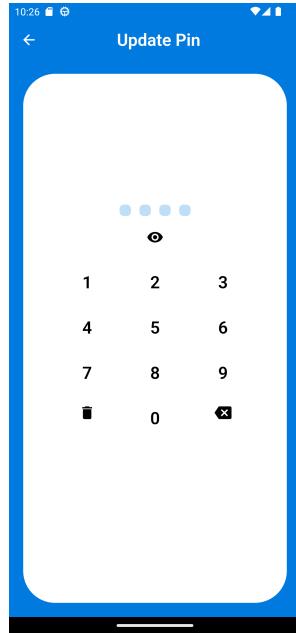
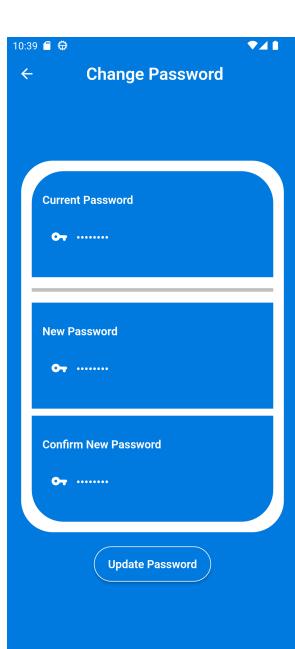
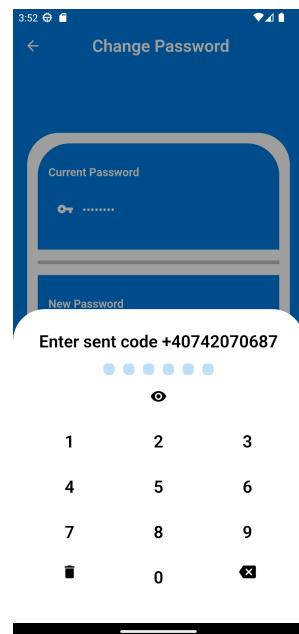


Figura 10.15: Ecran pentru setarea pin-ului

### 10.9.4 Change Password



(a) Schimbarea parolei



(b) Cod de identificare primit pe numarul de telefon

Figura 10.16: Ecranele pentru schimbarea parolei

### 10.9.5 Account Details

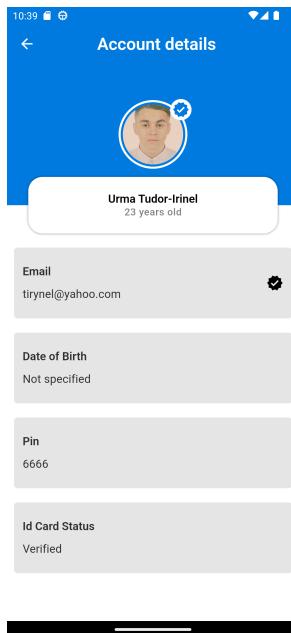


Figura 10.17: Ecran pentru detaliile contului și pentru verificarea email-ului

# Capitolul 11

## Analiză asupra aplicației

Acest capitol este destinat unei analize asupra implementării sistemului propus. Am reușit astfel să pun în aplicare toate cunoștințele rezultate în urma cercetărilor pentru a crea un sistem de vot bazat pe blockchain. Am reușit astfel să derulez un număr de procese electorale ce respectă condițiile cerute. Analiza este împărțită în cost, timp, avantaje, limitări și direcții viitoare.

### 11.1 Analiză de cost

Prin intermediul sistemului am reușit să monitorizez o medie a costurilor pentru întreaga desfășurarea a unui proces electoral de la inițializare până la strângerea de voturi. Vom calcula cantitatea de *benzină* pe care îl necesită fiecare aspect din cadrul procesului de alegere. *Benzina*, sau *gas*, este o unitate de masură ce prezintă volumul de calcul ce este necesar executării unei anumite operațiuni în blockchain-ul Ethereum. Întrucât prețul pe unitate de benzină poate dифeри de la o retea la alta, este imposibilă estimarea costului unei acțiuni în retea principală Ethereum pe baza datelor din retea de test Sepolia. Totuși, valoarea *benzinei* este una similară, fapt ce ne îndreaptă atenția spre această cantitate.

Operațiune	Cantitate de benzină
Construirea contractului asociat alegerii	1.715.005
Extragerea informațiilor ce țin de alegere	6.105
Extragerea informațiilor ce țin de un candidat	7.321
O exercitarea a dreptului de vot	67.788
Extragerea numărului de voturi pentru un candidat	5.201

Dacă dorim estimarea prețului unui proces electoral putem înlocui cantitatea de benzină cu valoarea sa, la momentul verificării prețul unitar este de 0.0008 RON. Trebuie menționat numărul de candidați estimativ, acesta fiind 15, iar pentru numărul de votanți

am ales să fie de 8.000.000, valoare ce reprezintă 50 % din populația României (procentaj de prezentare la vot extras din ultimii ani). Astfel tabelul devine.

Operațiune	Cantitate de benzină	Pret în ron
Construirea contractului asociat alegerii	1.715.005	1372 RON
Extragerea informațiilor ce țin de alegere	6.105	4.88 RON
Extragerea informațiilor ce țin de un candidat	7.321 x 15	87.85 RON
Exercitarea a dreptului de vot	67.788 x 8.000.000	433.843.200 RON
Extragerea numărului de voturi pentru un candidat	5.201 x 15	62,41 RON
<b>Cost Total</b>	<b>809.113.908.940</b>	<b>433.844.727,15 RON</b>

Astfel, prețul desfășurării unei alegerii în România ar fi de aproximativ 430 de mil de lei. O sumă mai mică decât valoarea pe care o are desfășurarea unei votări în cadrul alegerilor electorale din România, aceasta fiind de un miliard de lei. Desigur, aceste valori reprezintă doar o estimare, dar faptul că se poate observa o eficiență de cost la scară largă prezintă potențialul pe care îl oferă o astfel de abordare.

## 11.2 Analiză de timp

Voi prezenta măsurătorile temporale pe care le-am adunat pe parcursul desfășurărilor proceselor electorale din cadrul sistemului implementat.

Operațiune	Timp mediu (în ms)
Construirea contractului asociat alegerii	10527
Extragerea informațiilor ce țin de alegere	522
Extragerea informațiilor ce țin de un candidat	671
O exercitarea a dreptului de vot	5034
Extragerea numărului de voturi pentru un candidat	431

## 11.3 Avantaje

Această secțiune prezintă avantajele pe care sistemul propus reușește să le îndeplinească în contextul proceselor electorale. Voi păstra structura despre care am discutat în Capitolul 7 prezentând avantajele pe care fiecare secțiune acestea le oferă.

1. Structură - disponibilitate. 7.1)

2. Interfață - egalitate și libertate. (7.2)
3. Procesare a datelor - securitate, eligibilitate, anonimitate și verificabilitate, disponibilitate și unicitate. (7.3)
4. Logică - accesibilitate, anonimitate, integritate, democrație și singularitate, libertate, verificabilitate, eligibilitate, acuratețe, eficiență de cost și interoperabilitate. (7.4)

## 11.4 Limitări

Aplicația prezintă un mod fezabil prin care se poate desfășura un sistem de vot electronic bazat pe blockchain, dar există și anumite limitări. Voi prezenta aceste aspecte ținând cont de gravitate și probabilitate.

1. Scalabilitate - deși rezultatele sunt aparent optimiste pentru procesări la scară largă, acestea sunt doar aproximări, iar ele nu se pot materializa întrutotul.
2. Disponibilitate - pe parcursul testărilor s-a observat faptul că un flux mare de tranzacții poate dicta valabilitatea aplicației către utilizator.
3. Anonimitate - sistemul încearcă pastrarea intimității alegătorului, dar există posibilitatea identificării persoanei responsabile exercitării votului pentru un anumit candidat prin mijloace rău intenționate.
4. Identificare - deși întregul proces de identificare cuprinde o verificarea datelor cărții de identitate, verificare facială și autentificare în doi pași, acest lucru nu poate garanta că persoana care a desfășurat întreg procesul este și cea din spatele unei alegeri (un dispozitiv poate fi mutat de la o persoană la alta, se poate pierde, și.m.).

## 11.5 Directii viitoare

În urma cercetărilor, punerii în practică și a analizei sistemului de vot bazat pe blockchain se pot trage concluzii referitoare la direcțiile viitoare de interes. Se remarcă faptul că o varietate de dificultăți ale sistemelor de vot electronice pot fi rezolvate prin prisma tehnologiei blockchain, dar natura sa incipă din acest context prezintă mai mult aspecte spre care ar trebui îndreptată atenția. Astfel, direcțiile, pe care le propun prin prisma acestei disertații, sunt scalabilitatea, identitatea, eficiența energetică, intimitatea, acceptarea, împotrivirea și disponibilitatea.

# Capitolul 12

## Concluzii

In a conchide, această distortație bazată pe o cercetare minuțioasa a sistemelor de vot bazate pe blockchain și a tehnologiilor Ethereum, Flutter, Solidity, Web3dart și Firebase cu aplicații în sistemele de vot decentralizate, reușește să prezinte stadiul curent în care se situează nivelul dezvoltării acestora. Prin intermediul cercetării se realizează o propunere realistă de aplicabilitate a votului electronic, o implementare aferentă și o evaluare a acesteia.

Totodată, trebuie menționată imaturitatea sistemului, factor ce se remarcă prin lacunele aferente asupra scalabilității, identificării, încrederii și rezistenței. Aceste aspecte ar trebui abordate în profunzime prin prisma desfășurării unei astfel de proceduri electorale întrucât, punerea în aplicare, deschide oportunități noi de cercetare și face cunoscută această practică publicului larg.

Necesitatea introducerii unui astfel de sistem este dată de prevenirea infracționalității și îmbunătățirea dignității alegerilor electorale. Accesibilitatea acestui sistem de către orice persoană reprezintă un avantaj, întrucât facilitatea obținută în urma punerii în funcționalitate deplină, maximizează corectitudinea și integritatea sistemului. Astfel încurajează colectivul social în a-și valorifica votul, creând în acest fel o siguranță națională atât pentru cetățenii, ce aleg să contribuie la securitatea sistemului electoral folosind acest sistem substanțial îmbunătățit, cât și pentru puterea statală, căreia i se minimizează semnificativ efortul ce se depune în sistemul de vot tradițional.

Folosind această modalitate, potențialul în a ridica credibilitatea cadrului electoral este crescută, datorită tehnologiei blockchain, care îndepartează urmele de suspiciuni, pe care individul îndoctrinat le are în urma vechilor practici vicioase, prin claritatea din jurul sistemului și protecția împotriva fraudei, dar și protecția celui care își încredințează identitatea. De aici se deduce o altă trasatură benefică a noului sistem, intimitatea și respectarea dreptului fundamental al oricărui individ.

Magnitudinea acestei probleme, a siguranței, indiferent că este vorba de sistem sau de sinele propriu, poate fi cu ușurință neutralizată prin intermediul acestei noi tehnologii care promite să fie securizată.

Promptitudinea, pe care o promite sistemul de vot decentralizat este intangibilă, deoarece cercetările demonstrează acuratețea, transparența, securitatea, imutabilitatea și eficiența acestei practici a viitorului.

Excedentele aduse în urma unei simple comparații dintre cele două sisteme, cel tradițional și cel prin folosința capacitații tehnologiei într-o manieră a dezvoltării și evoluției sunt considerabil văzute în baza cercetării beneficiilor, pe care le aduce cea conturată în urma celei mai puternice unelte ale contemporanului, internetul. Cea din urmă având o precizie și concizie, detasat observabilă, în urma celor demonstrate.

Sistemul de vot decentralizat este o alegere a carei funcționalitate ar trebui reconsiderată, având în vedere sistemul actual, iar ulterior aplicată, pentru îmbunătățirea semnificativă a corpului electoral.

# Bibliografie

- [1] *Agora*, 2017, URL: <https://www.agora.vote/>.
- [2] Syed Taha Ali și Judy Murray, „An overview of end-to-end verifiable voting systems”, în *Real-World Electronic Voting* (2016), pp. 189–234.
- [3] Rachid Anane, Richard Freeland și Georgios Theodoropoulos, „E-voting requirements and implementation”, în *The 9th IEEE International Conference on E-Commerce Technology and The 4th IEEE International Conference on Enterprise Computing, E-Commerce and E-Services (CEC-EEE 2007)*, IEEE, 2007, pp. 382–392.
- [4] *Auðkenni.is*, 2018, URL: <https://www.audkenni.is/>.
- [5] Chiradeep BasuMallick, *What Are Smart Contracts?*, 2023, URL: [https://www.spiceworks.com/tech/innovation/articles/what-are-smart-contracts/#\\_001](https://www.spiceworks.com/tech/innovation/articles/what-are-smart-contracts/#_001).
- [6] Matthew Bernhard, Josh Benaloh, J Alex Halderman, Ronald L Rivest, Peter YA Ryan, Philip B Stark, Vanessa Teague, Poorvi L Vora și Dan S Wallach, „Public evidence from secret ballots”, în *Electronic Voting: Second International Joint Conference, E-Vote-ID 2017, Bregenz, Austria, October 24-27, 2017, Proceedings 2*, Springer, 2017, pp. 84–109.
- [7] Wouter Bokslag și Manon de Vries, „Evaluating e-voting: theory and practice”, în *arXiv preprint arXiv:1602.02509* (2016).
- [8] Anthony Cardillo și Aleksander Essex, „The threat of SSL/TLS stripping to online voting”, în *Electronic Voting: Third International Joint Conference, E-Vote-ID 2018, Bregenz, Austria, October 2-5, 2018, Proceedings 3*, Springer, 2018, pp. 35–50.
- [9] *Dart*, URL: <https://dart.dev/>.
- [10] *DecentraVote*, URL: <https://decentra.vote/>.
- [11] *Delegated Proof of Stake Consensus*, URL: <https://bitshares.org/delegated-proof-of-stake-consensus/>.
- [12] *Ethereum*, URL: <https://ethereum.org/en/>.

- [13] Go Ethereum., *Geth.ethereum.org*, 2018, URL: <https://geth.ethereum.org/>.
- [14] Aicha Fatrah, Said El Kafhali, Abdelkrim Haqiq și Khaled Salah, „Proof of concept blockchain-based voting system”, în *Proceedings of the 4th International Conference on Big Data and Internet of Things*, 2019, pp. 1–5.
- [15] Firebase, URL: <https://firebase.google.com/>.
- [16] Atsushi Fujioka, Tatsuaki Okamoto și Kazuo Ohta, „A practical secret voting scheme for large scale elections”, în *Advances in Cryptology—AUSCRYPT'92: Workshop on the Theory and Application of Cryptographic Techniques Gold Coast, Queensland, Australia, December 13–16, 1992 Proceedings* 3, Springer, 1993, pp. 244–251.
- [17] Shafi Goldwasser, Silvio Micali și Chales Rackoff, „The knowledge complexity of interactive proof-systems”, în *Providing sound foundations for cryptography: On the work of shafi goldwasser and silvio micali*, 2019, pp. 203–225.
- [18] Google Cloud Secret Manager, URL: <https://cloud.google.com/security/products/secret-manager>.
- [19] Google Colab, URL: <https://colab.google/>.
- [20] S Haber și WS Stornetta, *How to time-stamp a digital document* (pp. 437-455), 1991, URL: [https://www.spiceworks.com/tech/innovation/articles/what-are-smart-contracts/#\\_001](https://www.spiceworks.com/tech/innovation/articles/what-are-smart-contracts/#_001).
- [21] Mohammad Hajian Berenjestanaki, Hamid R. Barzegar, Nabil El Ioini și Claus Pahl, „Blockchain-Based E-Voting Systems: A Technology Review”, în *Electronics* 13.1 (2024), ISSN: 2079-9292, DOI: [10.3390/electronics13010017](https://doi.org/10.3390/electronics13010017), URL: <https://www.mdpi.com/2079-9292/13/1/17>.
- [22] Rifa Hanifatunnisa și Budi Rahardjo, „Blockchain based e-voting recording system design”, în *2017 11th International Conference on Telecommunication Systems Services and Applications (TSSA)*, IEEE, 2017, pp. 1–6.
- [23] Feng Hao, Peter YA Ryan și Piotr Zieliński, „Anonymous voting by two-round public discussion”, în *IET Information Security* 4.2 (2010), pp. 62–67.
- [24] Friðrik Þ Hjálmarsson, Gunnlaugur K Hreiðarsson, Mohammad Hamdaqa și Gísli Hjálmtýsson, „Blockchain-based e-voting system”, în *2018 IEEE 11th international conference on cloud computing (CLOUD)*, IEEE, 2018, pp. 983–986.
- [25] Infura, URL: <https://www.infura.io/>.
- [26] Uzma Jafar, Mohd Juzaiddin Ab Aziz și Zarina Shukur, „Blockchain for Electronic Voting System—Review and Open Research Challenges”, în *Sensors* 21.17 (2021), ISSN: 1424-8220, DOI: [10.3390/s21175874](https://doi.org/10.3390/s21175874), URL: <https://www.mdpi.com/1424-8220/21/17/5874>.

- [27] Ben Goldsmith Jordi Barrat i Esteve și John Turner, *International Experience with E-Voting*, 2012.
- [28] Ram Kesavan, David Gay, Daniel Thevessen, Jimit Shah și C Mohan, „Firestore: The nosql serverless database for the application developer”, în *2023 IEEE 39th International Conference on Data Engineering (ICDE)*, IEEE, 2023, pp. 3376–3388.
- [29] AE Keshk și Hatem M Abdul-Kader, „Development of remotely secure e-voting system”, în *2007 ITI 5th International Conference on Information and Communications Technology*, IEEE, 2007, pp. 235–243.
- [30] David Khoury, Elie F Kfoury, Ali Kassem și Hamza Harb, „Decentralized voting platform based on ethereum blockchain”, în *2018 IEEE International Multidisciplinary Conference on Engineering Technology (IMCET)*, IEEE, 2018, pp. 1–6.
- [31] Stefanos Leonardos, Daniël Reijnsbergen și Georgios Piliouras, „Weighted voting on the blockchain: Improving consensus in proof of stake protocols”, în *International Journal of Network Management* 30.5 (2020), e2093.
- [32] Jiaxing Li, Zhusong Liu, Long Chen, Pinghua Chen și Jigang Wu, „Blockchain-based security architecture for distributed cloud storage”, în *2017 IEEE international symposium on parallel and distributed processing with applications and 2017 IEEE international conference on ubiquitous computing and communications (ISPA/IUCC)*, IEEE, 2017, pp. 408–411.
- [33] Iuon-Chang Lin și Tzu-Chun Liao, „A survey of blockchain security issues and challenges.”, în *Int. J. Netw. Secur.* 19.5 (2017), pp. 653–659.
- [34] Yi Liu și Qi Wang, „An E-voting Protocol Based on Blockchain”, în (), URL: <https://eprint.iacr.org/2017/1043.pdf>.
- [35] Yinghui Luo, Yiqun Chen, Qiang Chen și Qinglin Liang, „A new election algorithm for DPos consensus mechanism in blockchain”, în *2018 7th international conference on digital home (ICDH)*, IEEE, 2018, pp. 116–120.
- [36] Luxoft, URL: <https://www.luxoft.com/>.
- [37] Patrick McCorry, Maryam Mehrnezhad, Ehsan Toreini, Siamak F. Shahandashti și Feng Hao, „On Secure E-Voting over Blockchain”, în *Digital Threats* 2.4 (2021), DOI: [10.1145/3461461](https://doi.org/10.1145/3461461), URL: <https://doi.org/10.1145/3461461>.
- [38] MetaMask, URL: <https://metamask.io/>.
- [39] Microsoft Azure Face API, URL: <https://azure.microsoft.com/en-in/pricing/details/cognitive-services/face-api/>.
- [40] Satoshi Nakamoto, *Bitcoin: A Peer-to-Peer Electronic Cash System*, 2008, URL: <https://bitcoin.org/bitcoin.pdf>.

- [41] *NewsApi*, URL: <https://newsapi.org/>.
- [42] Htet Ne Oo și Aye Moe Aung, „A survey of different electronic voting systems”, în *International Journal of Scientific Engineering and Technology Research* 3.16 (2014), pp. 3460–3464.
- [43] Mohammad Hajian Berenjestanaki Hamid R. Barzegar Nabil El Ioini Claus Pahl, „Blockchain-Based E-Voting Systems: A Technology Review”, în (2023), URL: [https://www.researchgate.net/publication/376645792\\_Blockchain-Based\\_E-Voting\\_Systems\\_A\\_Technology\\_Review](https://www.researchgate.net/publication/376645792_Blockchain-Based_E-Voting_Systems_A_Technology_Review).
- [44] *Polyas*, 1996, URL: <https://www.polyas.com/>.
- [45] *Python*, URL: <https://www.python.org/>.
- [46] *Remix IDE*, URL: <https://remix-ide.readthedocs.io/en/latest/>.
- [47] Heiz Eulau Roger Gibbings, *election*, 2024, URL: <https://www.britannica.com/topic/election-political-science>.
- [48] Peter YA Ryan, David Bismark, James Heather, Steve Schneider și Zhe Xia, „Prêt à voter: a voter-verifiable voting system”, în *IEEE transactions on information forensics and security* 4.4 (2009), pp. 662–673.
- [49] Muhammad Saad, Jeffrey Spaulding, Laurent Njilla, Charles Kamhoua, Sachin Shetty, DaeHun Nyang și Aziz Mohaisen, „Exploring the attack surface of blockchain: A systematic overview”, în *arXiv preprint arXiv:1904.03487* (2019).
- [50] *Sepolia*, URL: <https://www.alchemy.com/overviews/sepolia-testnet>.
- [51] Shalini Shukla, AN Thasmiya, DO Shashank și HR Mamatha, „Online voting application using ethereum blockchain”, în *2018 International Conference on Advances in Computing, Communications and Informatics (ICACCI)*, IEEE, 2018, pp. 873–880.
- [52] Abhay Singh, Ankush Ganesh, Rutuja Rajendra Patil, Sumit Kumar, Ruchi Rani și Sanjeev Kumar Pippal, „Secure Voting Website Using Ethereum and Smart Contracts”, în *Applied System Innovation* 6.4 (2023), ISSN: 2571-5577, DOI: [10.3390/asi6040070](https://doi.org/10.3390/asi6040070), URL: <https://www.mdpi.com/2571-5577/6/4/70>.
- [53] Siamak Solat, „Rdv: An alternative to proof-of-work and a real decentralized consensus for blockchain”, în *Proceedings of the 1st Workshop on Blockchain-enabled Networked Sensor Systems*, 2018, pp. 25–31.
- [54] *Solidity*, URL: <https://soliditylang.org/>.
- [55] Xin Sun, Quanlong Wang, Piotr Kulicki și Mirek Sopek, „A simple voting protocol on quantum blockchain”, în *International Journal of Theoretical Physics* 58 (2019), pp. 275–281.

- [56] Ajib Susanto, „Implementation of Smart Contracts Ethereum Blockchain in Web-Based Electronic Voting (e-voting)”, în *Jurnal Transformatika* 18 (Iul. 2020), p. 56, DOI: [10.26623/transformatika.v18i1.1779](https://doi.org/10.26623/transformatika.v18i1.1779).
- [57] Hamed Taherdoost, „Smart Contracts in Blockchain Technology: A Critical Review”, în *Information* 14.2 (2023), ISSN: 2078-2489, DOI: [10.3390/info14020117](https://doi.org/10.3390/info14020117), URL: <https://www.mdpi.com/2078-2489/14/2/117>.
- [58] Ruhi Taş și Ömer Özgür Tanrıöver, „A Systematic Review of Challenges and Opportunities of Blockchain for E-Voting”, în *Symmetry* 12.8 (2020), ISSN: 2073-8994, DOI: [10.3390/sym12081328](https://doi.org/10.3390/sym12081328), URL: <https://www.mdpi.com/2073-8994/12/8/1328>.
- [59] *Unit Time Stamp*, URL: <https://www.unixtimestamp.com/>.
- [60] *Voatz*, URL: <https://voatz.com/>.
- [61] *Votem*, URL: <https://votem.com/>.
- [62] Baocheng Wang, Jiawei Sun, Yunhua He, Dandan Pang și Ningxiao Lu, „Large-scale Election Based On Blockchain”, în *Procedia Computer Science* 129 (2018), 2017 INTERNATIONAL CONFERENCE ON IDENTIFICATION, INFORMATION AND KNOWLEDGE IN THE INTERNET OF THINGS, pp. 234–237, ISSN: 1877-0509, DOI: <https://doi.org/10.1016/j.procs.2018.03.063>, URL: <https://www.sciencedirect.com/science/article/pii/S1877050918302874>.
- [63] *Web3*, URL: <https://en.wikipedia.org/wiki/Web3>.
- [64] *Web3Dart*, URL: <https://pub.dev/packages/web3dart>.
- [65] Emre Yavuz, Ali Kaan Koç, Umut Can Çabuk și Gökhan Dalkılıç, „Towards secure e-voting using ethereum blockchain”, în *2018 6th International Symposium on Digital Forensic and Security (ISDFS)*, IEEE, 2018, pp. 1–7.
- [66] Wenbin Zhang, Yuan Yuan, Yanyan Hu, Shaohua Huang, Shengjiao Cao, Anuj Chopra și Sheng Huang, „A privacy-preserving voting protocol on blockchain”, în *2018 IEEE 11th International Conference on Cloud Computing (CLOUD)*, IEEE, 2018, pp. 401–408.