UNIVERSITATEA “LUCIAN BLAGA” DIN SIBIU

FACULTATEA DE INGINERIE

DEPARTAMENTUL DE CALCULATOARE ŞI INGINERIE ELECTRICĂ

**PROIECT DE DIPLOMĂ**

Conducător ştiinţific: As. dr. ing. Chiș Radu

Absolvent: Voicu Casiana

Specializarea: Tehnologia Informației

Sibiu 2020

UNIVERSITATEA “LUCIAN BLAGA” DIN SIBIU

FACULTATEA DE INGINERIE

DEPARTAMENTUL DE CALCULATOARE ŞI INGINERIE ELECTRICĂ

**SISTEM BLOCKCHAIN CU APLICAȚIE ÎN VOTUL ELECTRONIC**

Conducător ştiinţific: As. dr. ing. Chiș Radu

Absolvent: Voicu Casiana

Specializarea: Tehnologia Informației

**Cuprins**

[1. Introducere 6](#_Toc42341620)

[1.1 PREZENTAREA TEMEI 6](#_Toc42341621)

[1.2 MOTIVAȚIA ALEGERII TEMEI 7](#_Toc42341622)

[1.3 CERINȚE GENERALE 7](#_Toc42341623)

[2. Considerații teoretice 8](#_Toc42341624)

[2.1 TEHNOLOGIA BLOCKCHAIN 8](#_Toc42341625)

[**2.1.1** **Tipuri de Blockchain** 8](#_Toc42341626)

[**2.1.2** **Aplicabilitate** 9](#_Toc42341627)

[**2.1.3** **Criptografie** 10](#_Toc42341628)

[**2.1.4** **Structura unui Blockchain** 13](#_Toc42341629)

[2. Considerații teoretice 19](#_Toc42341630)

[3. Rezolvarea temei de proiect 20](#_Toc42341631)

[4. Concluzii 21](#_Toc42341632)

[5. Bibliografie 22](#_Toc42341633)

# Introducere

## PREZENTAREA TEMEI

Aflându-ne într-o perioadă în care tehnologia evoluează în continuu, ne dorim ca multe servicii sa devină cât mai accesibile și totodată sigure, astfel încât să ne ușureze munca, dar să avem încredere în ceea ce folosim.

Una din problemele întâlnite în această eră digitală este implementarea unui sistem de vot electronic, care să ofere siguranță utilizatorului și încredere că votul său este un vot secret și doar el poate să își exercite dreptul pentru acesta. Implementarea unui sistem centralizat în acest caz ar părea mult mai simplu de realizat si mult mai prietenos, din punct de vedere al interfeței pentru utilizatori, însă în acest caz intervin probleme de securitate, care pot aduce efecte negative asupra drepturilor omului.

Acest proiect reprezintă o soluție în cazul implementării unui sistem de vot, folosind tehnologia Blockchain, fiind un sistem descentralizat, realizat pentru un caz particular, în cadrul unei campanii electorale a unei instituții universitare, în vederea alegerii unui președinte pentru consiliul studenților.

Prin folosirea unui sistem descentralizat în cadrul unei aplicații de vot, un număr de noduri prestabilite în rețea permit eliminarea problemelor legate de securitate, acestea fiind noduri care nu influențează candidații sau votanții, fiind disponibile în cadrul facultății, de către persoane specializate, care nu au niciun interes în a frauda campania electorala.

Un utilizator va deține două chei, una publică și una privată care vor fi stocate pe calculatorul propriu, iar autentificarea în aplicația de vot se va face pe baza unei parole, care este creată in momentul în care acesta își va crea setul de chei și pe care o va utiliza ori de cate ori dorește să voteze. Pentru ca un utilizator să se înscrie în cadrul acestui sistem, este necesar ca acesta să își autorizeze datele de înregistrare prin intermediul unei semnături digitale, care apoi este trimisă prin platforma de email, folosind adresa sa din cadrul universității, unei persoane specializate, care mai apoi îl va adăuga în sistem, iar acesta își poate îndeplini dreptul de vot.

Scopul acestui proiect este de realiza un sistem descentralizat cu aplicație în votul electronic și de a compara acest tip de aplicație cu un sistem centralizat de vot.

## MOTIVAȚIA ALEGERII TEMEI

În primul rând, realizarea unui sistem de vot electronic cât mai sigur, care are ca scop înlocuirea votului obișnuit, în cadrul unei instituții, în care nu este necesar un personal mare care să se ocupe de contorizarea, validarea și verificarea voturilor si a votanților, dar și reducerea timpului petrecut de către studenți, toate aceste lucruri fiind digitalizate și accesibile. Astfel, în cazul unei situații în care este necesară o campanie electorală rapidă, acest proiect reprezintă o soluție pentru eliminarea problemelor elaborare mai sus.

În al doilea rând, tehnologia Blockchain a reprezentat un interes personal în vederea acumulării de noi cunoștințe și de înțelegere a acestui tip de sistem, pe baza aplicării acestuia în cadrul aplicației dezvoltate.

## CERINȚE GENERALE

În primul rand, s-a dorit implementarea unui sistem distribuit si descentralizat care să permită comunicarea nodurilor aflate în rețea dar și transmiterea de tranzacții de la utilizatori către noduri, pentru ca acestea să fie validate si adăugate în Blockchain.

Comunicarea nodurilor este realizată prin transmiterea si recepționarea unor mesaje care în general conțin informații referitoare la datele utilizatorilor, votul acestora, blocurile noi formate dar si starea curentă a sistemului.

În al doilea rând, s-a dorit implementarea unui Wallet, o aplicație destinată utilizatorilor, pentru posibilitatea votării dar și pentru verificarea datelor acestora.

În al treilea rând, realizarea unei aplicații Web, pentru vizualizarea și analizarea datelor din cadrul sistemului distribuit.

# Considerații teoretice

## TEHNOLOGIA BLOCKCHAIN

Blockchain reprezintă o bază de date ce conține înregistrări de tranzacții, care este distribuită, validată si menținută de o rețea de calculatoare din întreaga lume.**[1]**Este o structură de date formată din blocuri, fiecare bloc conține informații referitoare la blocul anterior, formând un lanț de blocuri într-o ordine liniară și cronologică.**[2]**

O astfel de bază de date, reprezintă o soluție în situația în care aceasta este alterată sau modificată, aspectul fiind sesizat și mai apoi respins, pentru ca informația să nu fie distribuită incorect.

Astfel, această tehnologie o caracterizăm ca fiind distribuită, prin transmiterea informațiilor în mod egal de-a lungul nodurilor din rețea dar și descentralizată prin care fiecare nod în rețea funcționează independent, fără să fie necesar ca acestea să depindă de un anume server.

### **Tipuri de Blockchain**

Exista mai multe tipuri de astfel de sisteme:

* Public

În care nu este necesară permisiunea, iar orice persoană poate să participe și să facă tranzacții în cadrul blockchain-ului, securitatea fiind dependentă de numărul de noduri din cadrul rețelei.

* Privat

Un Blockchain din cadrul unui mediu restrictiv, cu o rețea de noduri închisă, fiind util în cazul unor organizații care utilizează sistemul pentru uz intern. În acest caz doar persoanele selectate pot avea acces în cadrul rețelei de noduri.**[3]** Această lucrare prezintă o aplicabilitate a acestui tip de Blockchain, fiind vorba de un sistem de vot electronic în cadrul universității, în care accesul este permis doar persoanelor autorizate.

### **Aplicabilitate**

Acest tip de tehnologie rezolvă diferite probleme întâlnite în mai multe domenii, însă înainte de a îl utiliza, este necesar să știm de ce avem nevoie de un astfel de sistem, ce soluții aduce în comparație cu un sistem centralizat și ce fel de Blockchain să utilizăm.

Pe lângă cunoscutele criptomonede, care de-a lungul timpului s-au dezvoltat excepțional, Blockchain-ul este utilizat atât în băncile digitale, cât și în sistemele de gestionare a identității pentru eradicarea problemelor actuale precum nesiguranța datelor și fraudarea identității.**[4]**

Totodată, este folosit și în cadrul sistemelor medicale pentru prevenirea unor situații precum gestionarea sigură a înregistrărilor electronice de sănătate, securitatea datelor în studiile clinice și trasabilitatea medicamentelor. **[5]**

Numeroase avantaje sunt întâlnite și în cadrul guvernului, stocarea securizată a datelor, reducerea procesele care intensificau forța de muncă dar și creșterea încrederii în guvern și în sisteme civile on-line. **[6]**

Alte domenii care au recurs la utilizarea acestuia sunt: sportul, media și divertisment, politic și anume votul digital, cum prevede de altfel această lucrare.

Votarea prin cadrul acestui sistem a adus numeroase interese și în cadrul Uniunii Europene, care a descris într-un articol publicat pe site-ul oficial, impactul pozitiv dar și negativ al utilizării blockchain-ului. Acest tip de votare permite alegătorilor să dețină o copie a procesului verbal de vot, iar istoricul voturilor înregistrate nu poate să fie schimbat, deoarece acest lucru poate fi observat de către orice persoană care a votat. Sunt deja implementate astfel de sisteme de votare la nivel de organizații, cum sunt alegerile interne din Danemarca și voturile acționarilor din Estonia, iar UE aduce numeroase soluții pentru dezvoltarea pe mai multe arii a proiectelor deja existente. Se ia în considerare și un sistem care combină democrația directă, în care un cetățean votează în cadrul unei alegeri electorale, cu un sistem de delegați, prin votul către un alt cetățean, fie politician, jurnalist, om de încredere sau chiar o cunoștință. **[7]**

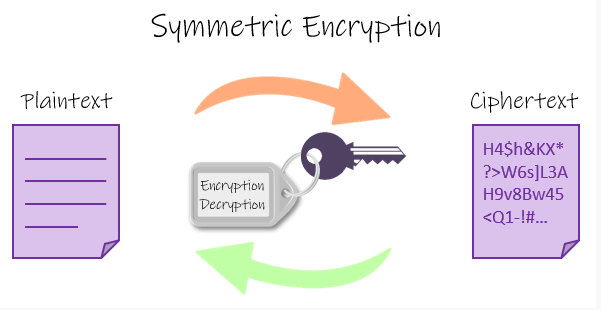
### **Criptografie**

Criptografia reprezintă o ramură a matematicii care se ocupă cu securizarea informației, precum și cu autentificarea și restricționarea accesului într-un sistem informatic. Urmărește următoarele obiective: confidențialitatea, integritatea datelor, autentificarea și non-repudierea. **[8]**

Tehnologia blockchain include tehnici avansate de criptografie pentru a preveni coruperea, duplicarea sau chiar distrugerea datelor.

#### Criptografie Simetrică

Reprezintă modalitatea prin care o singură cheie este utilizată pentru a cripta si decripta un mesaj.

Utilizând algoritmi de criptare simetrică, informația este convertită într-o formă care poate fi decriptată doar de persoanele care dețin cheia.

**Figură 2.1.3.1.1‑1 Criptare Simetrică**

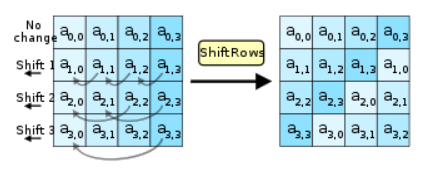
##### AES

Algoritm cunoscut inițial ca și Rijndael, reprezintă standardizarea avansată de criptare, care are în vedere o criptare pe blocuri (blocuri de stare), în care lungimea blocului este restricționată pe 128 de biți iar lungimea cheii (parametru de intrare) poate avea 128, 192 sau 256 de biți. În funcție de lungimea cheii, există un număr de runde, care reprezintă iterațiile procesului de criptare, astfel pentru 128 de biți avem 10 runde, pentru 192 de biți câte 12, iar pentru 256 biți vom avea 14 parcurgeri. **[9]**

Datele sunt structurate sub forma unor matrici, cu 4 linii si 4 coloane, numită matrice de stare, care va conține 128 de biți pentru fiecare bloc, atfel fiecare grup de 16 bytes dintr-un fișier va fi reprezentat printr-o astfel de matrice.

Procesul de criptare constă în următorii pași:

1. Sunt generate subchei de lungime diferită folosind algoritmul Rjindael.
2. Subsetul de chei este combinat cu informația curentă printr-o operație de XOR.
3. Substituție neliniară de bytes, în care se va procesa blocul printr-o tabelă de substituție pentru a produce o valoare alternativă. Acest lucru se realizează independent pentru fiecare octet în parte.
4. Mutarea rândurilor, cum este descrisă în figura 2.1.3.1.1-1



**Figură 2.1.3.1.1‑1 Procesul de rotire a rândurilor – AES**

1. Amestec de coloane, care este o transformare liniară a coloanelor din cadrul blocului.Fiecare coloană este reprezentată ca o matrice de 4 linii si o singură coloana, este va fii înmulțită cu o matrice de 4x4, numită corpul Galois și setată ca inversă de intrare și ieșire.**[10]**

Procesul de decriptare constă în schimbarea ordinii pașilor de mai sus, fiind un proces invers, astfel vom avea următoarea ordine : 1, 5, 4 și 3.

Astfel, siguranța oferită de acest algoritm este dată de o implementare corectă a acestuia și a unei chei potrivite.

#### Criptografie Asimetrică

Deseori numită și criptare computațională cu chei publice, unde o pereche de chei este folosită pentru două scopuri, o cheie publică, folosită pentru criptarea datelor si o cheie privată folosită pentru decriptarea informației.

Fie M, un mesaj oarecare, criptarea acestuia cu o cheie publică pk este reprezentată de Eₚₖ(M) = C. Decriptarea se realizează folosind cheia privată sk astfel: Dₛₖ(C) = M.

Având în vedere scopul acestei lucrări, folosirea criptografiei asimetrică în cadrul tehnologiei Blockchain constă în utilizarea acestor tipuri de chei în cadrul unor semnături digitale, aspect pe care îl voi detalia în capitolul 2.1.3.2.2, situația fiind diferită față de reprezentarea de mai sus.

Astfel, mesajul este criptat utilizând cheia privată, iar decriptarea se va realiza folosind cheia publică. **[11]** Astfel operațiile de mai sus devin:

Eₛₖ(M) = C (pentru criptare)

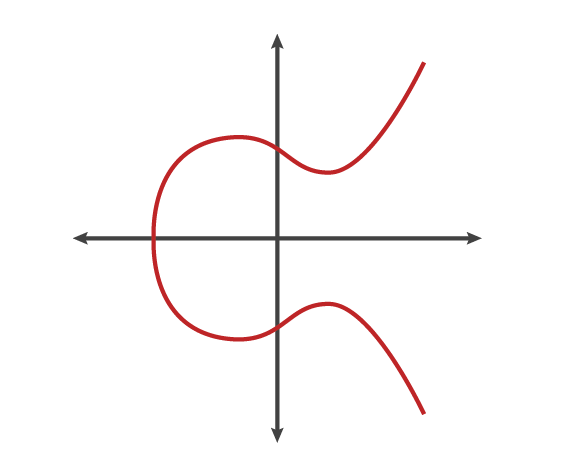
Dₚₖ(C) = M (pentru decriptare)

##### Criptografie bazată pe curbe eliptice (ECC)

Reprezintă o metodă alternativă a algoritmului RSA, o abordare folosită pentru criptarea bazată pe cheia publică, prin utilizarea unor calcule matematice bazate pe curbe eliptice pentru a genera securitatea dintre perechea de chei. Deși a demonstrat același nivel de securitate ca și RSA, prezintă un avantaj major, având dimensiunea cheilor mai mica față de acesta.

O astfel de curbă eliptică reprezintă un set de puncte care satisfac următoarea ecuație:

Pe baza valorilor date de a și b, se va determina forma curbei. Acest tip de criptografie folosește aceste curbe pe câmpuri finite pentru a crea un secret, care nu poate fi descoperit decât de cel care deține cheia privată. **[12]** Graficul este reprezentat în figura 2.1.3.2.1-1.



**Figură 2.1.3.2.1‑1 Reprezentarea Curbei Eliptice**

O linie poate fi desenat

### **Structura unui Blockchain**

#### Blocuri

**Figură 2.1.3.2.1‑1 Structura blocurilor înlănțuite**

Așa cum sugerează și numele, Blockchain este format dintr-un lanț de blocuri, fiecare bloc conține:

* Indexul blocului.

Acesta este incrementat la fiecare adăugare de bloc nou în baza de date.

* Câmpul ce conține ora și data la care blocul a fost procesat.
* Un câmp care conține informații legate de tranzacțiile procesate.

În cadrul acestui câmp sunt vizualizate toate datele ce formează una sau mai multe tranzacții verificate si aprobate.

* Hash-ul blocului anterior.

Pentru a putea adăuga un nou bloc este necesar ca în acest bloc să existe detalii legate de blocul anterior, astfel se poate realiza conexiunea dintre ele pentru a putea menține cronologia dintre acestea dar și verificarea corectitudinii datelor anterioare.

* Hash-ul blocului curent.

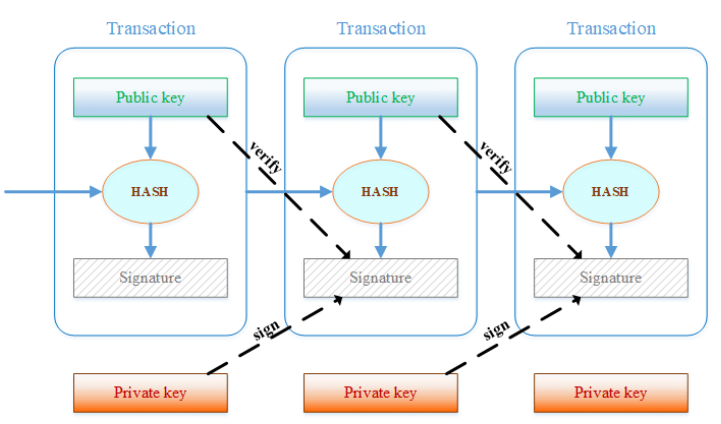
Acesta reprezintă semnătura digitală a blocului curent, fiind format din datele legate de tranzacții, data și ora înregistrării blocului, indexul blocului curent și hash-ul anterior. Acesta este recalculat de către fiecare nod din rețea pentru validarea acestuia și introducerea în baza de date.

* Starea bazei de date, care este reprezentată tot printr-un hash si sugerează starea curentă a blockchain-ului.

Primul bloc din cadrul lanțului de blocuri poartă numele de bloc de geneză. Acesta este deseori referit ca fiind blocul cu numărul 0, cum fiecare bloc din cadrul blockchain-ului are o referință către blocul anterior, în interiorul primului bloc acest câmp este 0. **[8]** În general, acest bloc este scris direct în aplicația software.**[9]**

#### Tranzacții

Blockchain-ul în sine reprezintă o colecție de tranzacții care sunt procesate, verificate si validate, pentru ca acestea să fie mai apoi incluse în blocuri și distribuite în întreaga rețea de noduri. Un bloc poate să conțină fie o singură tranzacție, fie o listă de tranzacții.



**Figură 2.1.3.2.1‑1 Structura tranzacțiilor**

O tranzacție conține următoarele câmpuri:

* Cheia publică a persoanei care trimite tranzacția.
* Cheia publică a destinatarului tranzacției.
* Datele tranzacției, care reprezintă valoarea transferată între două Wallet-uri, aici poate sa fie vorba fie de un număr de criptomonede, fie un vot, cum este în cazul acestei aplicații. Altfel spus, aici este reprezentată semnificația tranzacției.
* Hash-ul tranzacției.
* Semnătura digitală, orice tranzacție trebuie semnată pentru a putea preveni o posibilă alterare și pentru a demonstra autenticitatea ei.**[10]** Unicitatea ei este datorată cheii private a emițătorului împreună cu hash-ul tranzacției curente.

Astfel, dacă cineva încearcă să utilizeze aceeași semnătura pentru orice tranzacție, aceasta o să fie respinsă de către nodurile din rețea.**[11]**

* Data la care s-a realizat înregistrarea tranzacției.

# Considerații teoretice

# Rezolvarea temei de proiect

# Concluzii

# Bibliografie

1. <http://article.sapub.org/10.5923.j.computer.20180802.02.html>
2. <https://www.enisa.europa.eu/topics/csirts-in-europe/glossary/blockchain>
3. <https://101blockchains.com/types-of-blockchain/>
4. <https://consensys.net/blockchain-use-cases/digital-identity/>
5. <https://consensys.net/blockchain-use-cases/healthcare-and-the-life-sciences/>
6. <https://consensys.net/blockchain-use-cases/government-and-the-public-sector/>
7. <https://www.europarl.europa.eu/RegData/etudes/IDAN/2017/581948/EPRS_IDA(2017)581948_EN.pdf>
8. <http://irek.ase.md/xmlui/bitstream/handle/123456789/236/Zgureanu%20A.%20Criptarea%20%C5%9Fi%20Securitatea%20Informa%C5%A3iiei.%20Note%20de%20curs.pdf?sequence=1&isAllowed=y>
9. <https://ro.wikipedia.org/wiki/AES>
10. <https://securityboulevard.com/2020/04/advanced-encryption-standard-aes-what-it-is-and-how-it-works/>
11. Carte Bruce pg 4
12. <https://www.keycdn.com/support/elliptic-curve-cryptography>
13. <https://medium.com/@tecracoin/what-is-genesis-block-and-why-genesis-block-is-needed-1b37d4b75e43>
14. <https://en.bitcoin.it/wiki/Genesis_block#:~:text=A%20genesis%20block%20is%20the,that%20utilize%20its%20block%20chain.>
15. <https://bitcoin.org/en/how-it-works>
16. <https://wiki.trezor.io/Transaction_signature>