MINISTERUL EDUCAŢIEI ŞI CERCETĂRII AL REPUBLICII MOLDOVA
Universitatea Tehnică a Moldovei
Facultatea Calculatoare, Informatică şi Microelectronică
Departamentul Ingineria Software și Automatică

Admis la susţinere
Şef departament:
FIODOROV Ion dr., conf.univ.

„___” _____ 2025

ANALIZA COMPARATIVĂ A UNOR SISTEME BLOCKCHAIN PRIN PRISMA CONTRACTELOR INTELIGENTE

Teza de master

Student: _____ **Bîrcă Felix-Mihail-Andrei, TI-231M**

Coordonator: _____ **Bîtca Ernest, asist. univ.**

Consultant: _____ **Cojocaru Svetlana, asist.univ.**

Chişinău, 2025

REZUMAT

Analiza domeniului de studiu: Acest capitol prezintă o privire de ansamblu detaliată asupra mai multor blockchain-uri, inclusiv Bitcoin, Ethereum, Solana, Tron, The Open Network (TON) și Cardano. Fiecare platformă este analizată în detaliu din perspectiva caracteristicilor specifice, a scopurilor și a avantajelor tehnologice pe care le oferă. Bitcoin este descris ca fiind prima și cea mai populară monedă digitală, oferind un nivel ridicat de securitate și acceptare globală, pe când Ethereum este evidențiat pentru contractele inteligente și capabilitățile sale extinse de dezvoltare de aplicații descentralizate. Solana, Tron, TON și Cardano sunt discutate pentru inovațiile semnificative pe care le aduc în termeni de scalabilitate, eficiență energetică, timpi de execuție reduși și suport avansat pentru contracte inteligente. Fiecare dintre aceste blockchain-uri este evaluat pentru a înțelege rolul lor în dezvoltarea ecosistemului blockchain modern și contribuția lor la îmbunătățirea tehnologiilor existente.

Modelarea și analiza cerințelor: Capitolul descrie în detaliu cerințele necesare pentru dezvoltarea unei aplicații ce utilizează contracte inteligente. Este efectuată o analiză cuprinzătoare a cerințelor tehnice și funcționale, începând de la nevoile utilizatorilor finali până la standardele tehnice specifice necesare pentru implementare. De asemenea, sunt detaliate componentele critice ale arhitecturii tipice a unei aplicații bazate pe blockchain, incluzând elemente precum nodurile, mecanismele de consens, și protocoalele de securitate, evidențiind modul în care interacționează aceste componente pentru a asigura integritatea, securitatea și transparența datelor. În plus, sunt prezentate și exemple de utilizare pentru a ilustra cum aceste cerințe se aplică în scenarii reale.

Criteriile de comparare: În acest capitol sunt prezentate criteriile detaliate prin care sunt comparate diversele blockchain-uri analizate, oferind o privire cuprinzătoare asupra avantajelor și dezavantajelor fiecărei platforme. Printre criterii se numără performanța și scalabilitatea, costurile de execuție, ușurința în dezvoltare, precum și flexibilitatea și funcționalitatea oferite de fiecare platformă. Performanța este evaluată în funcție de rapiditatea tranzacțiilor, capacitatea de a gestiona un număr mare de utilizatori și eficiența resurselor. Costurile sunt analizate nu doar din perspectiva costurilor de execuție a contractelor, ci și din perspectiva costurilor de implementare și întreținere.

Implementare și comparație: Capitolul prezintă implementarea contractelor inteligente pe trei platforme diferite: Ethereum (utilizând Solidity), Cardano (utilizând Aiken) și The Open Network (utilizând Solidity). Sunt analizate diferențele majore între aceste implementări în ceea ce privește performanța, cum ar fi numărul de tranzacții pe secundă, costurile asociate execuției contractelor, timpul de execuție, precum și ușurința în dezvoltare și mentenanță. În plus, sunt prezentate provocările specifice întâlnite în timpul dezvoltării fiecărei implementări, oferind o comparație clară între diferitele abordări de dezvoltare și avantajele fiecărei platforme în funcție de complexitatea și scopul aplicației.

ABSTRACT

Domain analysis: This chapter provides a detailed overview of several blockchains, including Bitcoin, Ethereum, Solana, Tron, The Open Network (TON), and Cardano. Each platform is thoroughly analyzed from the perspective of specific features, goals, and technological advantages they offer. Bitcoin is described as the first and most popular digital currency, offering a high level of security and global acceptance. Ethereum is highlighted for its smart contracts and its extensive capabilities for developing decentralized applications. Solana, Tron, TON, and Cardano are discussed for their significant innovations in terms of scalability, energy efficiency, reduced execution times, and advanced support for smart contracts. Each of these blockchains is evaluated to understand their role in the development of the modern blockchain ecosystem and their contribution to improving existing technologies.

Requirements Modeling and Analysis: This chapter describes in detail the requirements necessary for developing an application that uses smart contracts. A comprehensive analysis of technical and functional requirements is conducted, starting from the needs of end users to the specific technical standards required for implementation. The critical components of a typical blockchain-based application architecture are also detailed, including elements such as nodes, consensus mechanisms, and security protocols. The chapter highlights how these components interact to ensure data integrity, security, and transparency. Additionally, use cases are presented to illustrate how these requirements apply in real-world scenarios.

Comparison Criteria: This chapter presents detailed criteria for comparing the analyzed blockchains, providing a comprehensive view of the advantages and disadvantages of each platform. The criteria include performance and scalability, execution costs, ease of development, as well as the flexibility and functionality offered by each platform. Performance is evaluated based on transaction speed, the capacity to handle a large number of users, and resource efficiency. Costs are analyzed not only in terms of smart contract execution costs but also from the perspective of implementation and maintenance expenses.

Implementation and Comparison: This chapter presents the implementation of smart contracts on three different platforms: Ethereum (using Solidity), Cardano (using Aiken), and The Open Network (using Solidity). Major differences between these implementations are analyzed in terms of performance, such as the number of transactions per second, execution costs, execution time, as well as ease of development and maintenance. Additionally, specific challenges encountered during the development of each implementation are discussed, providing a clear comparison between different development approaches and the advantages of each platform depending on the complexity and purpose of the application.

CUPRINS

ABREVIERI ȘI DEFINIȚII

dApp – Decentralized Application (aplicație descentralizată)

TON – The Open Network

EVM – Ethereum Virtual Machine

TVM – TON Virtual Machine

Token – Reprezentare digitală a unui activ sau drept pe blockchain

OpCode – Coduri de Operații (instrucțiuni la nivel de bază pentru execuția smart contracts)

Multisig – Multi-signature (securizare care necesită aprobarea mai multor chei private)

Smart Contract – Program automatizat care rulează pe blockchain

NFT – Non-Fungible Token (token unic utilizat pentru reprezentarea activelor digitale)

TPS – Transactions Per Second (numărul de tranzacții procesate într-o secundă)

PoW – Proof of Work (mecanism de consens bazat pe rezolvarea problemelor matematice)

PoS – Proof of Stake (mecanism de consens bazat pe staking de tokeni)

PoH – Proof of History (mecanism de consens care creează o înregistrare cronometrată a evenimentelor)

DeFi – Decentralized Finance (finanțe descentralizate) Ecosistem de aplicații financiare construite pe blockchain, care funcționează fără intermediari tradiționali, cum ar fi băncile.

Mempool – Memory Pool (piscină de memorie) Spațiul de stocare temporară al tranzacțiilor care nu au fost încă incluse într-un bloc pe blockchain. Minerii sau validatorii selectează tranzacțiile din mempool pentru a le adăuga în blocuri.

UTXO – Unspent Transaction Output (ieșire de tranzacție necheltuită) Model utilizat de blockchain-uri precum Bitcoin, unde tranzacțiile sunt bazate pe intrări și ieșiri. Ieșirile necheltuite devin intrări pentru tranzacții viitoare.

eUTXO – Extended Unspent Transaction Output (model extins de ieșire de tranzacție necheltuită) Versiune îmbunătățită a modelului UTXO, utilizată de blockchain-uri precum Cardano. eUTXO permite o mai mare flexibilitate pentru smart contracts și execuția paralelă a tranzacțiilor.

INTRODUCERE

Sistemele blockchain și-au început drumul ca un simplu registru de tranzacții, prin intermediul Bitcoin. Totuși, trebuie subliniat că și implementarea unui registru de tranzacții descentralizat reprezintă o realizare semnificativă. Aceasta a adus în atenția publicului concepte fundamentale, precum funcționarea unui sistem în care nodurile nu se bazează pe încrederea reciprocă [1] și mecanismele inovatoare de consens care asigură securitatea și stabilitatea acestora.

Bitcoin este limitat în ceea ce privește aplicabilitatea sa, deși validează conceptul de monedă virtuală, nu funcționează ca un mediu computațional descentralizat. Sistemele dezvoltate în anii următori vor avea ca obiectiv rezolvarea acestor limitări. Ethereum, de exemplu, permite deja implementarea și utilizarea contractelor inteligente pentru crearea aplicațiilor descentralizate, un pas semnificativ înainte care demonstrează potențialul practic al blockchain-urilor.

Una dintre premisele fundamentale ale aplicațiilor descentralizate este eliminarea intermediarilor și descentralizarea proceselor și controlului. În aplicațiile tradiționale, intermediarii, cum ar fi băncile, platformele de social media sau guvernele, sunt responsabili pentru administrarea datelor, tranzacțiilor și acordurilor între utilizatori. Această centralizare aduce riscuri, cum ar fi manipularea datelor, cenzura și comisioane excesive.

Aplicațiile descentralizate permit utilizatorilor să interacționeze direct între ei, folosind contracte inteligente care execută automat tranzacțiile și procesele fără a depinde de o entitate centrală. Acest lucru descentralizează puterea și oferă un control mai mare utilizatorilor asupra datelor și tranzacțiilor lor.

Contractele inteligente reprezintă coloana vertebrală a aplicațiilor descentralizate și una dintre principalele inovații care au permis dezvoltarea dApps. Conceptul de contract inteligent, introdus în blockchain-ul Ethereum, este un cod autonom care se execută automat atunci când sunt îndeplinite anumite condiții prestabilite.

Aplicațiile descentralizate folosesc contracte inteligente pentru a automatiza procesele și a elimina necesitatea unei terțe părți pentru a valida și executa tranzacțiile. Aceste contracte pot automatiza o gamă largă de aplicații, de la tranzacții financiare și gestionarea activelor, la jocuri și platforme de socializare.

Un alt factor esențial care a condus la dezvoltarea dApps a fost nevoia de transparență și securitate în diverse industrii. În aplicațiile tradiționale, datele sunt de obicei gestionate de o singură entitate, ceea ce le face vulnerabile la atacuri, fraude și manipulări. Utilizatorii nu au întotdeauna acces la modul în care sunt procesate și stocate datele lor, ceea ce poate duce la lipsă de transparență.

Aplicațiile descentralizate rulează pe blockchain, care este un registru distribuit și imutabil, oferind transparență completă în toate acțiunile care se desfășoară în cadrul aplicației. Fiecare tranzacție și proces este înregistrat public pe blockchain, permițând oricui să verifice corectitudinea și integritatea acțiunilor. De asemenea, securitatea este asigurată prin criptografie și descentralizare, ceea ce face dificilă manipularea datelor sau compromiterea aplicației.

În multe tranzacții și interacțiuni economice, părțile implicate nu au întotdeauna încredere una în cealaltă și trebuie să se bazeze pe intermediari sau sisteme juridice pentru a asigura respectarea acordurilor. Acest lucru poate adăuga complexitate și costuri ridicate.

Utilizând aplicațiile descentralizate elimină nevoia de încredere reciprocă între părți, deoarece contractele inteligente asigură automat respectarea regulilor prestabilite și executarea corectă a acordurilor. În acest fel, părțile pot interacționa direct, fără a fi necesară verificarea și validarea din partea unei autorități terțe.

Blockchain-ul și dApps au introdus conceptul de token-uri, care sunt folosite ca unități de valoare în cadrul sistemeleor descentralizate. Tokenurile pot reprezenta proprietăți digitale, drepturi de vot, recompense sau alte forme de valoare. Acest lucru a permis dezvoltatorilor să creeze economii descentralizate, în care utilizatorii sunt stimulați să participe activ la rețea și să contribuie la creșterea ecosistemului.

Pe măsură ce mai multe blockchain-uri și ecosisteme de dApps au fost dezvoltate, s-a creat nevoia de interoperabilitate între aceste sisteme, pentru a permite tranzacții și interacțiuni fără întreruperi între blockchain-uri diferite. Aplicațiile tradiționale funcționează într-un ecosistem izolat, unde datele nu sunt partajate între sisteme fără integrare complexă.

Un alt factor care a contribuit la dezvoltarea dApps a fost dorința de a combate cenzura și de a oferi utilizatorilor libertatea de exprimare în mediile online. Aplicațiile tradiționale centralizate pot fi manipulate sau cenzurate de guverne sau companii private, limitând accesul la anumite informații sau blocând conturi fără transparență.

Un aspect deosebit de important al sistemelor blockchain este capacitatea acestora de a susține economie colaborativă și comunități autonome. Prin utilizarea token-urilor și a mecanismelor de guvernanță descentralizată, utilizatorii pot participa activ la luarea deciziilor în cadrul rețelelor blockchain și pot beneficia direct de succesul platformelor pe care le susțin. Această formă de organizare reduce dependența de structurile ierarhice tradiționale și stimulează implicarea comunității în dezvoltarea și extinderea ecosistemului.

De asemenea, integrarea tehnologiilor blockchain în sectoare precum sănătatea, logistica și educația subliniază potențialul lor transformator. De exemplu, în sectorul medical, blockchain-ul poate asigura o mai bună gestionare a dosarelor pacienților, oferind acces securizat și transparent atât pacienților, cât și furnizorilor de servicii medicale. În logistică, trasabilitatea produselor de-a lungul lanțului de aprovizionare devine mai eficientă, reducând riscul de fraudă și creșterea încrederii între parteneri. Aceste utilizări demonstrează că blockchain-ul și aplicațiile descentralizate pot contribui la eficientizarea și securizarea proceselor dintr-o varietate de domenii.

BIBLIOGRAFIE

[1] S. Nakamoto, „Bitcoin: A Peer-to-Peer Electronic Cash System”. [Online]. Disponibil la: https://bitcoin.org/bitcoin.pdf

[2] G. A. Pierro și A. Amoordon, „Gas Fees and Unconfirmed Transactions in Ethereum: A Proof-of-Stake (PoS) Focus”, în *2024 IEEE International Conference on Software Analysis, Evolution and Reengineering - Companion (SANER-C)*, Rovaniemi, Finland: IEEE, mar. 2024, pp. 1–8. doi: 10.1109/SANER-C62648.2024.00011.

[3] P. Kasireddy, „The Architecture of a Web 3.0 application”. [Online]. Disponibil la: https://www.preethikasireddy.com/post/the-architecture-of-a-web-3-0-application

[4] Н. МАКЕЕВ, „Трилемма блокчейна”, prezentat la Conferința tehnico-științifică a studenților și doctoranzilor, 2024, pp. 290–293. [Online]. Disponibil la: http://repository.utm.md/handle/5014/27963

[5] „TVM Instructions”, 2024. [Online]. Disponibil la: https://docs.ton.org/v3/documentation/tvm/instructions

[6] V. Buterin, „Ethereum: A Next-Generation Smart Contract and Decentralized Application Platform”, 2014.

[7] M. I. Mehar *și colab.*, „Understanding a Revolutionary and Flawed Grand Experiment in Blockchain: The DAO Attack”, *J. Cases Inf. Technol.*, vol. 21, nr. 1, pp. 19–32, ian. 2019, doi: 10.4018/JCIT.2019010102.

[8] A. Popov, „The Open Network (TON): A Scalable and Secure Blockchain”, 2021.

[9] M. Ramezanian și F. Sheikh, „The Role of TON in Enabling Scalable Blockchain Applications”, *Int. J. Blockchain Technol.*, vol. 6, nr. 1, pp. 23–35.

[10] L. Erkök, *SBV: SMT Based Verification in Haskell*. [Online]. Disponibil la: https://github.com/LeventErkok/sbv

[11] P. Lamela Seijas, A. Nemish, D. Smith, și S. Thompson, „Marlowe: Implementing and Analysing Financial Contracts on Blockchain”, în *Financial Cryptography and Data Security*, vol. 12063, M. Bernhard, A. Bracciali, L. J. Camp, S. Matsuo, A. Maurushat, P. B. Rønne, și M. Sala, Ed., în Lecture Notes in Computer Science, vol. 12063. , Cham: Springer International Publishing, 2020, pp. 496–511. doi: 10.1007/978-3-030-54455-3_35.

[12] С. ХМЕЛЬ și Л. РОТАРУ, „Будущее квантовых компьютеров”, prezentat la Conferința tehnico-științifică a studenților și doctoranzilor, 2021, pp. 246–249. [Online]. Disponibil la: http://repository.utm.md/handle/5014/16204