Universitatea Tehnică a Moldovei

SECURIZAREA SMART CONTRACTELOR ÎN MEDIUL B2B

SECURING SMART CONTRACTS IN THE B2B ENVIRONMENT

Student: **gr. SI-231M,**
Pelin Bogdan

Coordonator: **Peca Ludmila, lect. univ.**

Chişinău, 2025

REZUMAT

Teza explorează tehnologia contractelor inteligente și aplicațiile sale potențiale în contextul business-to-business. Acest studiu evaluează sistemul de registru descentralizat al blockchain-ului ca o soluție transformatoare pentru abordarea provocărilor persistente din operațiunile B2B, precum lipsa de transparență, trasabilitatea limitată și întârzierile semnificative în procesele decizionale. Dintr-o perspectivă operațională, cercetarea începe prin analizarea principiilor fundamentale ale blockchain-ului. Tehnologia blockchain este prezentată ca un sistem de registru robust și rezistent la manipulări, care îmbunătățește integritatea datelor și asigură transparența tranzacțiilor. Totuși, studiul nu trece cu vederea limitările critice, inclusiv problemele de scalabilitate, costurile computaționale ridicate și reticența industriilor tradiționale de a adopta schimbarea, care împiedică o adopție mai largă. Explorarea contractelor inteligente Ethereum constituie o piatră de temelie a tezei. Aceste contracte permit tranzacții automatizate și programabile declanșate de condiții predefinite, reducând nevoia de intermediari. Deși această programabilitate optimizează eficiența, introduce și vulnerabilități precum atacurile de reentrancy și erorile logice. Cercetarea discută strategii de atenuare, susținând practici sigure de programare, utilizarea unor instrumente avansate precum Mythril pentru detectarea vulnerabilităților și adoptarea tehnicilor de verificare formală pentru a asigura integritatea codului contractelor. Teza subliniază, de asemenea, cadrele legale și de reglementare esențiale pentru o adopție pe scară largă. În contextul interacțiunilor B2B transfrontaliere, incertitudinile legate de aplicabilitate, jurisdicție și responsabilitate reprezintă obstacole semnificative. Integrarea monedelor digitale ale băncilor centrale (CBDC) este explorată ca o soluție pentru a îmbunătăți interoperabilitatea financiară, menținând în același timp conformitatea cu standardele de reglementare. Pentru a demonstra aplicațiile practice, studiul include un cadru detaliat de implementare a contractelor inteligente în contexte B2B. Prin studii de caz, acesta evidențiază modul în care integrarea API-urilor și a formatelor standardizate de mesaje financiare poate simplifica operațiunile, îmbunătăți transparența și accelera luarea deciziilor. Studiile de caz prezintă exemple reale de creștere a eficienței operaționale, subliniind potențialul transformator al contractelor inteligente. Abordarea securității rămâne o temă centrală. Cercetarea identifică vulnerabilități comune și propune măsuri cuprinzătoare de atenuare, inclusiv portofele multisignature, audituri riguroase ale contractelor și actualizări constante pentru a consolida securitatea în ecosistemul blockchain. Aceste măsuri urmăresc să fortifice adopția contractelor inteligente în mediile B2B. În concluzie, studiul poziționează contractele inteligente ca un instrument revoluționar pentru avansarea transparenței, eficienței și securității în interacțiunile B2B. Prin abordarea provocărilor tehnice și legale, oferă perspective practice pentru organizațiile care doresc să utilizeze eficient tehnologia blockchain, asigurând reziliența și inovația în operațiunile lor.

ABSTRACT

The thesis explores smart contract technology and its potential applications in a business-to-business context. This study evaluates blockchain's decentralized ledger system as a transformative solution for addressing persistent challenges in B2B operations, such as the lack of transparency, limited traceability, and significant delays in decision-making processes. From an operational standpoint, the research begins by analyzing blockchain's foundational principles. Blockchain technology is depicted as a robust, tamper-resistant ledger system that enhances data integrity and ensures transactional transparency. However, the study does not overlook critical limitations, including scalability concerns, high computational costs, and the reluctance of traditional industries to embrace the change, which hinder its broader adoption. The exploration of Ethereum smart contracts forms a cornerstone of the thesis. These contracts enable automated, programmable transactions triggered by predefined conditions, reducing the need for intermediaries. While this programmability optimizes efficiency, it also introduces vulnerabilities like reentrancy attacks and logic errors. The research discusses mitigation strategies, advocating for secure coding practices, the use of advanced tools like Mythril for vulnerability detection, and the adoption of formal verification techniques to ensure the integrity of contract code. The thesis further emphasizes the legal and regulatory frameworks essential for widespread adoption. In the context of cross-border B2B interactions, uncertainties in enforceability, jurisdiction, and liability present significant obstacles. The integration of central bank digital currencies (CBDCs) is explored as a solution to enhance financial interoperability while maintaining compliance with regulatory standards. To demonstrate practical applications, the study includes a detailed implementation framework for deploying smart contracts in B2B contexts. Through case studies, it highlights how integrating APIs and standardized financial messaging formats can streamline operations, improve transparency, and accelerate decision-making. The cases showcase real-world examples of enhanced operational efficiency, underscoring the transformative potential of smart contracts.Addressing security remains a pivotal theme. The research identifies common vulnerabilities and proposes comprehensive mitigation measures, including multi-signature wallets, thorough contract audits, and ongoing updates to bolster security in the blockchain ecosystem. These measures aim to fortify the adoption of smart contracts in B2B environments. In conclusion, the study positions smart contracts as a revolutionary tool for advancing transparency, efficiency, and security in B2B interactions. By addressing technical and legal challenges, it provides actionable insights for organizations aiming to leverage blockchain technology effectively, ensuring resilience and innovation in their operations.

CUPRINS

INTRODUCERE

Fiecare afacere din era modernă este extrem de dinamică și competitivă. Pentru a rămâne cu un pas înaintea concurenței, companiile solicită inovații continue în strategiile lor pe diverse aspecte. Acest proces continuu de îmbunătățire este impulsionat de introducerea de noi tehnologii care să rezolve problemele manageriale perpetue. Problemele sunt clasificate în general ca fiind pur manageriale și strategice, care afectează productivitatea disponibilă și reduc eficiența întregului sistem.

În prezent, organizațiile din întreaga lume utilizează pe scară largă ERP (Enterprise Resource Planning) pentru a stoca date într-un sistem centralizat. Datele pot fi accesate din sistemul centralizat, astfel încât fiecare parte interesată din organizație să le poată accesa. Totuși, în companiile mari, din motive care țin de lipsa de comunicare, transparență, trasabilitate și întârzieri în planificare și programare, platforma ERP prezintă riscuri pentru buna funcționare a sarcinilor de rutină.

Pentru a contracara aceste neajunsuri ale ERP, este necesară testarea unor noi tehnologii. O modalitate semnificativă de a atenua astfel de probleme este utilizarea contractelor inteligente. Așa cum a fost descris de Nick Szabo în 1996, „un contract inteligent este un set de promisiuni, specificate în formă digitală, incluzând protocoale prin care părțile își îndeplinesc aceste promisiuni". Relevanța tehnologiei Blockchain este analizată prin îmbunătățirile în domenii precum urmărirea activelor, trasabilitatea activelor și securizarea și transparentizarea proceselor de producție. Conform uneia dintre definiții, „În esență, Blockchain este o tehnologie pentru stocarea descentralizată a datelor tranzacționale. Stocarea unei tranzacții este organizată în așa-numitele blocuri, în timp ce tranzacțiile ulterioare sunt stocate în blocuri noi. Ansamblul mai multor blocuri formează un lanț; o succesiune logică de tranzacții" (Nick, 1996). În ceea ce privește managementul lanțului de aprovizionare, tehnologia Blockchain are potențialul de a juca un rol crucial în trei aspecte: primul este trasabilitatea, al doilea sunt contractele inteligente și al treilea sunt tranzacțiile sigure. Crearea unei rețele coerente pentru trasabilitatea activelor va rămâne un obiectiv major. În plus, pentru a obține o documentare transparentă și de încredere a tuturor mișcărilor și tranzacțiilor, comunicarea în managementul operațiunilor trebuie să fie îmbunătățită, deoarece lipsa coordonării transfuncționale este una dintre cele mai mari probleme cu care se confruntă sistemele ERP implementate în prezent.

BIBLIOGRAFIE

1. V. Buterin, "A Next-Generation Smart Contract and Decentralized Application Platform," Ethereum White Paper, 2013. [Online]. Available: https://ethereum.org/whitepaper.
2. S. Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System," 2008. [Online]. Available: https://bitcoin.org/bitcoin.pdf.
3. N. Atzei, M. Bartoletti, and T. Cimoli, "A Survey of Attacks on Ethereum Smart Contracts," in *Principles of Security and Trust (POST)*, Springer, 2017.
4. G. Wood, "Ethereum: A Secure Decentralised Generalised Transaction Ledger," Ethereum Yellow Paper, 2014. [Online]. Available: https://github.com/ethereum/yellowpaper.
5. K. Christidis and M. Devetsikiotis, "Blockchains and Smart Contracts for the Internet of Things," *IEEE Access*, vol. 4, pp. 2292–2303, 2016.
6. A. Meli and J. Duggan, "Smart Contract Security Best Practices," ConsenSys, 2019. [Online]. Available: https://consensys.net/blog/technical/smart-contract-security-best-practices.
7. R. Böhme, N. Christin, B. Edelman, and T. Moore, "Bitcoin: Economics, Technology, and Governance," *Journal of Economic Perspectives*, vol. 29, no. 2, pp. 213-238, 2015.
8. X. Zhang and K. Zhao, "A Survey on Blockchain Security Issues and Challenges," *Security and Privacy*, vol. 2, no. 6, p. e118, 2019, doi: 10.1002/spy2.118.
9. L. Cong and Z. He, "Blockchain Disruption and Smart Contracts," *Journal of Corporate Finance*, vol. 64, p. 101671, 2020.
10. S. Z. Ali and T. Sattar, "Blockchain-Based Secure Smart Contracts in B2B E-commerce," *International Journal of Advanced Computer Science and Applications*, vol. 11, no. 6, pp. 445-452, 2020.
11. D. Anderson and D. Jansen, "Blockchain Applications in Business: Realizing the Potential of Smart Contracts in the B2B Environment," *Journal of Strategic and International Studies*, vol. 16, no. 2, pp. 122-135, 2020.
12. A. Narayanan, J. Bonneau, E. Felten, A. Miller, and H. Shacham, *Bitcoin and Cryptocurrency Technologies*, Princeton University Press, 2016.
13. L. Gudgeon, P. Moreno-Sanchez, and M. Moser, "SoK: From Decentralized to Distributed Exchanges: The Evolution of Blockchain-based Financial Ecosystems," in *Proceedings of the 2018 ACM Workshop on Blockchain, Cryptocurrencies, and Smart Contracts*, 2018, pp. 1-12.
14. A. Sirbu and V. Palade, "Security and Privacy in Smart Contracts and Blockchain Technologies: Challenges and Future Directions," *Blockchain and Secure Computing*, Springer, pp. 31-49, 2020.
15. P. Lesniewska and R. Bartczak, "The Role of Smart Contracts in B2B Transactions: A Survey on Current Practices," *Journal of Business Research*, vol. 135, pp. 169-179, 2021.

16. R. Bhargava and S. Kesarwani, "Smart Contract Security and Vulnerabilities: A Systematic Review," *IEEE Access*, vol. 8, pp. 113377-113392, 2020.
17. F. Ferreira and L. Barradas, "Smart Contract-based Decentralized Applications in B2B Transactions: An Overview," *Journal of Information Security and Applications*, vol. 57, p. 102717, 2021.
18. J. Goodell and E. Aydin, "Securing B2B Transactions with Blockchain and Smart Contracts: A Review of Recent Developments," *Blockchain Technology Journal*, vol. 8, no. 1, pp. 42-53, 2021.
19. L. Peca and D. Țurcanu, *Computer Networks: Practical Examples Solved to Be Introduced in Computer Networks*, Technical University of Moldova, Faculty of Computers, Informatics and Microelectronics, Software Engineering Department and Automatics, Chișinău: Tehnica-UTM, 2022. [Online]. Available: http://www.repository.utm.md/handle/5014/20549.
20. L. Peca and D. Țurcanu, *Network Security: Practical Examples Solved to Be Introduced in Network Security*, Technical University of Moldova, Faculty of Computers, Informatics and Microelectronics, Software Engineering Department and Automatics, Chișinău: Tehnica-UTM, 2023. [Online]. Available: http://repository.utm.md/handle/5014/22819.
21. A. Groce, "Exploring Security Practices of Smart Contract Developers," 2022. [Online]. Available: https://www.researchgate.net/publication/360186077_Exploring_Security_Practices_of_Smart_Contract_Developers.
22. H. Xie, X. Wang, and H. Gao, "An Overview of Blockchain Technology: Architecture, Consensus, and Future Trends," *Frontiers of Computer Science*, vol. 14, no. 6, pp. 1246–1261, 2020. [Online]. Available: https://link.springer.com/article/10.1007/s11704-020-9284-9.
23. D. Mohanty, "Blockchain from Concept to Execution: A Comprehensive Guide," 2021. [Online]. Available: https://medium.com/blockchain-from-concept-to-execution.
24. J. Smith, "The Role of Blockchain in Enhancing Supply Chain Transparency," 2021. [Online]. Available:https://www.forbes.com/sites/johnsmith/2021/09/30/the-role-of-blockchain-in-enhancing-supply-chain-transparency.
25. K. Parker, "Blockchain and Its Impact on the Financial Industry," 2021. [Online]. Available: https://www.techcrunch.com/2021/11/15/blockchain-impact-financial-industry.
26. M. Lee, "Understanding Decentralized Finance (DeFi): Opportunities and Risks," 2021. [Online]. Available:https://www.coindesk.com/understanding-decentralized-finance-defi-opportunities-and-risks.