УДК 004.056

ОГЛЯД ВРАЗЛИВОСТЕЙ СМАРТ-КОНТРАКТІВ ТА КРИПТОГРАФІЧНИХ МЕТОДІВ ДЛЯ ЗАХИСТУ ЧУТЛИВИХ ДАНИХ

Дужич Денис, Пузікова Анна

Центральноукраїнський державний університет імені Володимира Винниченка, м. Кропивницький, Україна

Використання блокчейн-технологій і смарт-контрактів у децентралізованих системах вимагає впровадження криптографічних методів для надійного захисту чутливих даних. У роботі виконано огляд основних вразливостей смарт-контрактів, що стосуються управління чутливими даними у нефінансових системах. Розглянуто сучасні криптографічні примітиви для захисту чутливих даних від цих вразливостей, такі як гомоморфне шифрування, протокол нульового розголошення та безпечні багатосторонні обчислення. Виконано порівняльний аналіз цих криптографічних примітивів, який демонструє основні переваги і обмеження цих методів щодо продуктивності, сумісності та рівня приватності.

Ключові слова: блокчейн, смарт-контракти, криптографічні примітиви.

A review of smart contract vulnerabilities and cryptographic methods for protecting sensitive data

D. Duzhych, A.Puzikova

Volodymyr Vynnychenko Central Ukrainian State University, Kropyvnytsky, Ukraine

The deployment of blockchain technologies and smart contracts in decentralized systems necessitates the use of cryptographic methods to ensure the secure protection of sensitive data. This study presents a review of the primary vulnerabilities of smart contracts associated with the management of sensitive data in non-financial systems. It examines contemporary cryptographic primitives for mitigating these vulnerabilities, including homomorphic encryption, zero-knowledge proofs, and secure multi-party computation. A comparative analysis of these cryptographic primitives is provided, highlighting their key advantages and limitations in terms of performance, compatibility, and data privacy.

Keywords: blockchain, smart contracts, cryptographic primitives.

Постановка проблеми. Блокчейн є розподіленою між багатьма пристроями базою даних, яка містить узгоджену, точну і повну історію записів подій, котрі неможливо непомітно підмінити [2, 5, 6, 8]. Всі дії в системі фіксуються у цьому реєстрі, що може дозволити автоматизувати точне ведення

повного обліку чи медичної історії, відстежування походження продукції, запис повної історії транзакцій по угоді або усіх голосів у голосуванні [3, 4, 5].

Велику роль у роботі блокчейну та взаємодії з ним відіграють смарт контракти, умови яких записані безпосередньо в коді на блокчейні, забезпечуючи надійність, прозорість та автоматизацію [10, 11]. Смарт контракти можуть автоматично надавати або відкликати дозволи на основі попередньо визначених умов, таких як наявність необхідних сертифікатів або попередню участь у поточному голосуванні, і навіть мати у собі завчасно програмовані механізми автоматичного вирішення конфліктних ситуацій на основі об'єктивних даних, зафіксованих у блокчейні [10].

За минуле десятиліття технологія блокчейн та смарт-контракти набули більш широкого застосування як частина багатьох типів систем, зокрема у децентралізованих системах управління, відстеження ланцюгів поставок, системах електронного голосування та зберігання й обробки медичних записів. У деяких з цих сфер прозорість блокчейну, яка є його ключовою перевагою, може стати небажаною вразливістю, створюючи можливість розкриття чутливої інформації – як то індивідуальні медичні дані, деталі голосування або ключова комерційна та фінансова інформація. Оскільки бізнес-логіка цих систем з використанням блокчейн реалізується через смарт-контракти, будь-яка помилка або недолік у їх безпеці має незворотні та каскадні наслідки на рівні даних, прав доступу та загальної довіри до системи [2, 4]. Таким чином, існує нагальна потреба впровадження проактивних криптографічних рішень, що надають можливість обробляти дані без їх розкриття.

Аналіз досліджень і публікацій. Огляд наукових праць показує, що питання застосування технологій блокчейн у різних галузях та гарантування їх інформаційної безпеки набуває особливої значущості.

У статті [3] розглянуто перспективи впровадження блокчейн-технологій у систему державного управління України на основі аналізу вітчизняного та зарубіжного досвіду. Також розглядаються виклики впровадження подібних

систем в Україні, серед яких вказано обмежену доступність мережі інтернет та ризики кібербезпеки смарт-контрактів.

У роботі [4] викладено процес розробки прототипу інформаційної системи для медичного закладу з використанням технології блокчейн. Підкреслюється критична потреба покращення безпеки й приватності інформації для цієї галузі, для чого необхідне застосування сучасних методів шифрування даних та відстеження запитів на доступ або внесення змін.

Роботи [6] та [10] оглядають та класифікують криптографічні вразливості технології блокчейн та інформаційних систем побудованих на її основі. Проводиться як загальний огляд літератури, що відноситься до криптографічних властивостей блокчейн, так і огляд окремих відомих властивостей з подальшим їх групуванням по класу вразливості та окремо по шарам систем.

У роботі [8] досліджуються власна криптографічна безпека технології блокчейн та застосування криптографічних підходів для надання додаткового захисту інформації.

Стаття [1] присвячена основним існуючим підходам до побудови систем електронного голосування та проводить порівняння узагальнених структур таких систем. Також демонструється важливість використання змішаних підходів.

Метою статті є огляд вразливостей блокчейн-систем та сучасних криптографічних методів для їх убезпечення, з акцентом на конфіденційність даних у випадках де це є критично важливою умовою.

Виклад основного матеріалу (результатів) дослідження. Завдяки децентралізованій природі блокчейну та механізмам консенсусу його записи забезпечують надійне підтвердження дій і правдивості даних. Це знижує витрати на перевірки, прискорює процеси та формує довіру між учасниками, адже всі бачать єдину незмінну історію. Водночас надмірна прозорість може призвести до розкриття приватних даних, зокрема порушення анонімності виборців чи розголошення медичної інформації.

Блокчейн забезпечує цілісність і прозорість даних, але не підходить для зберігання великих обсягів інформації чи виконання надмірно складних обчислень [2, 6, 8, 10]. Через обмежений розмір блоків зберігання детальних даних безпосередньо в ланцюгу веде до надмірності та зниження продуктивності, тому застосовують гібридний підхід: у блокчейні фіксують лише хеші та метадані, а основні дані зберігають поза мережею. Обчислювально складні операції часто виконуються у вторинних Layer-2 мережах, які групують і стискають транзакції та записують у блокчейн компактні підсумки [6, 10]. Детальні файли чи документи розміщують у зовнішніх сховищах – децентралізованих файлових системах, хмарних сервісах або спеціалізованих розподілених базах даних. Хеші цих даних заносять у блокчейн, що забезпечує їх незмінність та дає змогу виявити будь-які модифікації під час перевірки.

Блокчейн-системи, як правило, включають такі ключові структурні рівні: мережевий рівень, що охоплює вузли та однорангову взаємодію; консенсусний рівень, відповідальний за валідацію транзакцій; рівень даних, який забезпечує ведення незмінного реєстру; а також прикладний рівень, що містить смарт-контракти та децентралізовані додатки [8, 10]. Смарт-контракти є програмованою фіксованою бізнес-логікою, що виконуватиметься на прикладному рівні віртуальної машини блокчейну, наприклад Ethereum Virtual Machine, і часто є одним з основних місць атаки [6, 8, 11]. Вразливості смарт-контрактів призводять до каскадного впливу на фінансову та інформаційну безпеку системи. Ці вразливості поділяються на кілька категорій [6, 8, 10, 11]; розглянемо основні вразливості, що стосуються управління чутливими даними у нефінансових системах (Табл. 1).

Враховуючи, що аудит коду та архітектурні зміни не завжди можуть повністю вирішити проблему конфіденційності, необхідне впровадження криптографічних примітивів, здатних оперувати зашифрованими даними.

Таблиця 1.

Основні вразливості смарт-контрактів

Вид вразливості	Опис дії вразливостей	Рівень критичності для чутливих систем
Логічні помилки в коді (Logic bugs)	Призводять до некоректного виконання бізнес-логіки та несанкціонованого виведення активів. У системах голосування може призвести до повторного голосування або маніпуляції результатами.	Висока.
Вразливість обробки даних (Data handling)	Створює можливість для маніпуляцій зовнішніми даними. Впливає на точність інформації (наприклад, у ланцюгах поставок).	Середня.
Недостатній контроль доступу (Access Control)	Призводить до некоректної ініціалізації, відсутність авторизації. Надає несанкціонований доступ до функцій (наприклад, пауза контракту, зміна правил) у системах управління.	Критична.
Загроза кофіденційності (Confidentiality Threats)	Може спричинити відсутність анонімності, розкриття особистих даних через прозорість блокчейну. Є найбільш актуальною для систем голосування та медичних систем.	Критична.

Криптографічні примітиви для обчислень над приватними даними забезпечують можливість виконання операцій над конфіденційною інформацією без розкриття самих даних, що є критично важливим у контексті блокчейн-систем, приватних голосувань, фінансових сервісів та медичної аналітики. До основних класів таких примітивів належать гомоморфне шифрування (Homomorphic Encryption, HE) [1, 8, 12], що дозволяє виконувати арифметичні та логічні операції над шифротекстами; безпечні багатосторонні обчислення (Secure Multi-Party Computation, MPC) [1, 9], які забезпечують спільне виконання обчислень між учасниками без розкриття індивідуальних даних; протоколи

нульового розголошення (Zero-Knowledge Proofs, ZKP) [1, 7], що дають змогу довести істинність тверджень без розкриття інформації.

Основні види гомоморфного шифрування включають частково гомоморфне (Partially Homomorphic Encryption, PHE), яке підтримує виконання лише однієї операції, наприклад додавання або множення; обмежено гомоморфне (Somewhat Homomorphic Encryption, SHE), що дозволяє виконувати кілька операцій, але з обмеженою глибиною обчислень; та повністю гомоморфне (Fully Homomorphic Encryption, FHE), яке надає можливість здійснювати довільні обчислення безпосередньо над шифротекстами [5, 8, 12].

Протоколи нульового розголошення включають zk-SNARK, які забезпечують короткі та ефективні докази для блокчейнів, але потребують довіреної ініціалізації (trusted setup); zk-STARK, що не потребують trusted setup і забезпечують стійкість до квантових атак; а також інтерактивні та неінтерактивні ZK-докази, що дозволяють перевіряти істинність тверджень без розкриття додаткової інформації [1, 7, 8].

В таблиці 2 наведено порівняльний аналіз криптографічних примітивів ZKP, HE та MPC за критеріями, критичними для безпеки та впровадження у блокчейн-системи.

Таблиця 2.

Порівняльний аналіз криптографічних примітивів ZKP, HE та MPC.

Критерій	Zero-Knowledge Proofs	Homomorphic Encryption	Secure Multi-Party Computation
Основна мета	Верифікація цілісності даних та забезпечення конфіденційності учасників	Виконання обчислень над зашифрованими даними без їх розкриття	Розподілений контроль та довіра між співучасниками
Рівень приватності	Вхідні дані повністю приховані	Дані та результати обчислень залишаються конфіденційними	Вхідні дані залишаються прихованими від інших учасників

Продуктивність	Генерація доказів потребує значних ресурсів, верифікація швидка	Обчислення виконуються повільно, особливо для FHE	Повільне виконання через високу інтенсивність комунікації між учасниками
Сумісність з Ethereum Virtual Machine	Висока: компактні докази дозволяють інтеграцію у блокчейн	Низька: обмеження за розміром шифротексту та кількістю операцій	Низька: вимагає багатьох інтерактивних транзакцій і синхронізації
Стійкість до вразливостей	Захист від логічних помилок та порушень цілісності даних	Забезпечує захист від загроз конфіденційності	Захист доступу та управління ключами, запобігання витоку даних між учасниками

Основним обмеженням для широкого впровадження деяких методів гомоморфного шифрування, а особливо повністю гомоморфного шифрування, є високі обчислювальні витрати. Складність операцій останнього та великі розміри шифротекстів ускладнюють їх виконання безпосередньо на Ethereum Virtual Machine [1, 5, 11, 12]. Зазвичай цю проблему вирішують за допомогою гібридних архітектур off-chain/on-chain, у яких ресурсомісткі криптографічні обчислення виконуються поза блокчейном, тоді як сам блокчейн використовується лише для незмінного зберігання зашифрованих даних та верифікації доказів ZKP [7, 8, 11].

Висновки та перспективи подальших пошуків у напрямі дослідження.

Виконаний огляд досліджень засвідчує, що прозорість блокчейну, хоча й є його фундаментальною перевагою, одночасно створює критичні вразливості, пов’язані з конфіденційністю чутливих даних. Було встановлено, що для протидії цим загрозам необхідне впровадження спеціалізованих криптографічних примітивів, таких як гомоморфне шифрування, протоколи нульового розголошення та безпечні багатосторонні обчислення, які дозволяють виконувати обчислення та верифікацію результатів без розкриття самих даних.

Використання цих методів забезпечує баланс між прозорістю, цілісністю та приватністю даних, створюючи передумови для безпечного застосування блокчейн-технологій у чутливих сферах, включно з фінансовими сервісами, медичною аналітикою та конфіденційним голосуванням.

Перспективи подальших досліджень у даному напрямі включають пошук шляхів підвищення сумісності розглянутих криптографічних примітивів із Ethereum Virtual Machine та іншими популярними платформами смарт-контрактів, що сприятиме широкому впровадженню приватних та безпечних децентралізованих рішень у блокчейн-системах.

Список використаної літератури:

1. Остапець Д., Мотиленко В. Аналіз підходів до реалізації систем електронного голосування. *Системні технології*. 2024. Т. 6, вип. 155. С. 50–60. URL: https://journals.nmetau.edu.ua/index.php/st/article/view/1914 (дата звернення: 10.11.2025).
2. Ковальчук В. Блокчейн. Сфери застосування, вплив на сучасні технології та перспективи розвитку. *Молодь в науці: дослідження, проблеми, перспективи*. 2024. вип. 896. URL: https://ir.lib.vntu.edu.ua/handle/123456789/47451 (дата звернення: 10.11.2025).
3. Малахова Т., Давидюк Ю. Впровадження технологій блокчейн у процеси публічного управління: перспективи впровадження та сучасні виклики. *Публічно - управлінські та цифрові практики*. Київ, 2025. вип. 2. С. 78–88. URL: https://journals.dut.edu.ua/index.php/public/article/view/3223 (дата звернення: 10.11.2025).
4. Шматко О., Сальніков С. Модель децентралізованої системи обміну електричними медичними картками на основі технології блокчейн. *Системи управління, навігації та зв'язку*. Харків, 2024. Т. 2, вип. 76. С. 155–162. URL: https://journals.nupp.edu.ua/sunz/article/view/3373 (дата звернення: 10.11.2025).
5. Горбенко І. та ін. Можливості застосування механізмів повністю гомоморфного шифрування в системах електронного голосування. *Радіотехніка*. Харків, 2020. вип. 200. С. 98–113. URL: https://openarchive.nure.ua/entities/publication/d4a0db35-7c6f-450c-9903-01579ba24d66 (дата звернення: 10.11.2025).
6. Mahmood S., Chadhar M., Firmin S. Cybersecurity Challenges in Blockchain Technology: A Scoping Review. *Human Behavior and Emerging Technologies*. 2022. С. 11. URL: https://onlinelibrary.wiley.com/doi/10.1155/2022/7384000 (дата звернення: 10.11.2025).
7. Hasan J. Overview and Applications of Zero Knowledge Proof ZKP. *International Journal of Computer Science and Network*. 2019. С. 5. URL:

https://www.academia.edu/43094897/Overview_and_Applications_of_Zero_Knowledge_Proof_ZKP?sm=b (дата звернення: 10.11.2025).

8. Zhai S., Yang Y., Li J., Qiu C., Zhao J. Research on the Application of Cryptography on the Blockchain. *Journal of Physics: Conference Series*. 2019. вип. 1168. С. 8. URL: https://iopscience.iop.org/article/10.1088/1742-6596/1168/3/032077/meta (дата звернення: 10.11.2025).

9. Zhao C., Zhao S., Zhao M., Chen Z., Gao C., Hongwei L., Tan Y. Secure Multi-Party Computation: Theory, practice and applications. *Information Sciences*. 2019. Т. 476. С. 357–372. URL: https://www.sciencedirect.com/science/article/pii/S0020025518308338 (дата звернення: 10.11.2025).

10. Islam M., Islam S., Hossain M., Noor S., Islam R.Securing Blockchain Systems: A Layer-Oriented Survey of Threats, Vulnerability Taxonomy, and Detection Methods. *Future Internet*. 2025. Т. 17, вип. 205. URL: https://www.mdpi.com/1999-5903/17/5/205 (дата звернення: 10.11.2025).

11. Fadele A., Sulaimon H., Marisa M., Najeem O. Smart Contracts Security Application and Challenges: A Review. *Cloud Computing and Data Science*. 2024. Т. 5. вип. 1. С. 15-41. URL: https://ojs.wiserpub.com/index.php/CCDS/article/view/3271 (дата звернення: 10.11.2025).

12. Aronoff D. at all. SoK: Fully-homomorphic encryption in smart contracts. (Preprint. *Massachusetts Institute of Technology*). 2025. С. 15. URL: https://eprint.iacr.org/2025/527 (дата звернення: 10.11.2025).

Відомості про автора:

Дужич Денис Валентинович – студент ІІ курсу магістратури факультету інформаційних технологій, математики та природничих наук Центральноукраїнського державного університету імені Володимира Винниченка, тел. +380665298303, e-mail: duzhychcuspu@gmail.com.

Пузікова Анна Валентинівна – кандидат фізико-математичних наук, доцент кафедри інформаційних та цифрових технологій Центральноукраїнського державного університету імені Володимира Винниченка