МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ЗАПОРІЗЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ

Кваліфікаційна наукова праця
на правах рукопису

ГОРЕЛІКОВА ТЕТЯНА ОЛЕКСІЇВНА

УДК 004.056.5:004.75:004.421.2:530.145

ДИСЕРТАЦІЯ

МЕТОДИ ЗАХИСТУ ОСОБИСТОЇ ІНФОРМАЦІЇ ВІД ПІДМІНИ ТА ВИДАЛЕННЯ З ВИКОРИСТАННЯМ ТЕХНОЛОГІЇ БЛОКЧЕЙНУ

122 Комп'ютерні науки

12 Інформаційні технології

Подається на здобуття наукового ступеня доктора філософії з **комп'ютерних наук**

Дисертація містить результати власних досліджень. Використання ідей, результатів і текстів інших авторів мають посилання на відповідне джерело

Т. О. Горелікова

Науковий керівник: Чопорова Оксана Володимирівна,
доктор філософії з комп'ютерних наук, доцент

Запоріжжя – 2026

АНОТАЦІЯ

Горелікова Т. О. Методи захисту особистої інформації від підміни та видалення з використанням технології блокчейну. – Кваліфікаційна наукова праця на правах рукопису. Дисертація на здобуття наукового ступеня доктора філософії за спеціальністю 122 «Комп'ютерні науки». – Запорізький національний університет, Запоріжжя, 2026.

У дисертаційній роботі розв'язано актуальне науково-прикладне завдання підвищення рівня захисту інформації від підміни та несанкціонованого видалення у блокчейн-системах шляхом розроблення та впровадження механізму рандомізованої валідації блоків і транзакцій. Запропонований підхід ґрунтується на використанні стохастичних процедур вибору валідаторів та криптографічно і фізично захищених джерел випадковості, що сприяє підвищенню цілісності даних, зниження ймовірності компрометації та підвищення стійкості до скоординованих атак у розподілених середовищах.

У вступі обґрунтовано актуальність теми, сформульовано мету, завдання, об'єкт і предмет дослідження, визначено методи дослідження, наведено наукову новизну та практичну значущість отриманих результатів, а також відображено апробацію та особистий внесок автора.

Об'єкт дослідження – процеси забезпечення цілісності та достовірності даних у розподілених блокчейн-системах в умовах децентралізованого функціонування.

Предмет дослідження – методи та механізми захисту інформації від підміни та видалення з використанням технології блокчейн.

Мета дослідження – розробка та дослідження методів захисту інформації від підміни та видалення з використанням технології блокчейн шляхом впровадження механізму рандомізованої валідації блоків і транзакцій, що сприяє підвищенню рівня цілісності даних, зниження ризиків компрометації та покращення ефективності функціонування системи.

У першому розділі реалізовано системний аналіз сучасних блокчейн-систем і механізмів забезпечення цілісності даних. Показано, що існуючі підходи мають обмеження, пов’язані з передбачуваністю процесів валідації, що створює передумови для атак, зокрема типу «51%», подвійних витрат та маніпулювання порядком підтвердження транзакцій. Обґрунтовано гіпотезу про доцільність застосування рандомізації як ключового чинника зміцнення безпеки.

У другому розділі розроблено теоретико-методологічні основи механізму рандомізованої валідації. Запропоновано формальну модель випадкового вибору вузлів-валідаторів, яка враховує розмір мережі, частку зловмисних вузлів і параметри відбору, та дозволяє кількісно оцінити ймовірність компрометації системи. Сформовано узагальнений механізм рандомізованого підтвердження блоків і транзакцій, що знижує рівень детермінованості процесу валідації та ускладнює реалізацію цілеспрямованих атак. За результатами імітаційного моделювання встановлено зниження ймовірності успішної атаки при зростанні ентропії механізму відбору.

У третьому розділі розроблено механізм генерації випадкових чисел з високою ентропією на основі квантових фізичних процесів. Запропоновано прототип квантового генератора випадкових чисел, що використовує фотонний шум як джерело ентропії, та проведено його експериментальну валідацію із застосуванням статистичних тестів якості випадковості. Підтверджено, що використання фізичних джерел ентропії забезпечує підвищення непередбачуваності вибору валідаторів і, відповідно, зменшення ризику атак, спрямованих на підміну або видалення даних.

У висновках узагальнено результати дослідження, які формують новий підхід до проектування безпечних блокчейн-систем, заснований на використанні рандомізованих механізмів валідації як базового елемента забезпечення цілісності даних.

Наукова новизна отриманих результатів полягає в тому, що вперше запропоновано механізм рандомізованої валідації блоків і транзакцій у блокчейн-системах на основі криптографічно та фізично захищених джерел випадковості,

який дозволяє підвищити стійкість до підміни та несанкціонованого видалення даних завдяки непередбачуваності вибору вузлів-валідаторів. Розроблено формальну модель випадкового вибору вузлів-валідаторів, що дозволяє оцінювати ймовірність компрометації системи залежно від частки зловмисних вузлів і параметрів мережі. Обґрунтовано використання квантових джерел ентропії, зокрема фотонного шуму, у процесах консенсусу блокчейн-мереж, що сприяє підвищенню непередбачуваності рандомізації та знижує ризик атак.

Удосконалено підхід до забезпечення цілісності та захисту даних у блокчейн-системах шляхом інтеграції рандомізованих процедур валідації, що сприяє підвищенню стійкості до атак і зменшенню обчислювальної надлишковості. Також удосконалено методи оцінювання безпеки блокчейн-мереж із урахуванням стохастичних характеристик вибору валідаторів та моделі аналізу ефективності консенсусних механізмів, доповнені показниками енергоефективності та масштабованості.

Подальшого розвитку набули теоретичні засади побудови децентралізованих систем із рандомізованим керуванням процесами валідації, підходи до зниження ризиків атак, зокрема типу «51%», за рахунок непередбачуваного розподілу ролей у мережі, а також застосування блокчейн-технологій у системах, що потребують підвищеного рівня довіри. Теоретична значущість отриманих результатів полягає у розвитку наукових підходів до забезпечення цілісності та достовірності даних у розподілених системах на основі технології блокчейн. У роботі обґрунтовано, що ефективність захисту інформації від підміни та несанкціонованого видалення визначається не лише застосуванням криптографічних механізмів, але й рівнем непередбачуваності процесів валідації. Запропонований підхід розширює існуючі теоретичні уявлення про роль рандомізації як фундаментального чинника забезпечення безпеки, що впливає на стійкість системи до координованих атак.

Практичне значення полягає у можливості впровадження запропонованого механізму в існуючі та перспективні блокчейн-платформи. Його застосування дозволяє підвищити рівень захисту даних від підміни і видалення, зменшити

обчислювальні витрати та енергоспоживання, підвищити пропускну здатність системи, скоротити час підтвердження транзакцій, знизити вимоги до апаратних ресурсів вузлів і підвищити рівень децентралізації. Результати можуть бути використані у фінансових, державних, медичних та корпоративних інформаційних системах, а також у системах штучного інтелекту, де критично важливими є достовірність, цілісність і незмінність даних. Запропонований підхід може бути застосований для захисту навчальних вибірок, результатів обробки даних та процесів обміну інформацією у розподілених AI-системах, зокрема у системах підтримки прийняття рішень, медичних AI-платформах та інтелектуальних аналітичних сервісах.

Ключові слова: блокчейн, захист інформації, рандомізована валідація, консенсус, криптографія, квантова ентропія, візуалізація, розподілені системи, датасет, нейронна мережа, AI, архітектура програмного забезпечення, відмовостійкість, випадковий вибір, моделювання, програмна реалізація.

ABSTRACT

Gorelikova T. O. Methods of protecting personal information from substitution and deletion using blockchain technology. – Qualification scientific work in the form of a manuscript. Dissertation for the degree of Doctor of Philosophy in specialty 122 "Computer Science". – Zaporizhzhia National University, Zaporizhzhia, 2026.

The dissertation solves the current scientific and applied problem of increasing the level of information protection from substitution and unauthorized deletion in blockchain systems by developing and implementing a mechanism for randomized validation of blocks and transactions. The proposed approach is based on the use of stochastic procedures for selecting validators and cryptographically and physically protected sources of randomness, which contributes to increasing data integrity, reducing the probability of compromise, and increasing resistance to coordinated attacks in distributed environments.

The introduction substantiates the relevance of the topic, formulates the goal, objectives, object and subject of the research, defines the research methods, presents the scientific novelty and practical significance of the results obtained, and also reflects the testing and personal contribution of the author.

The object of the research is the processes of ensuring the integrity and reliability of data in distributed blockchain systems in conditions of decentralized functioning.

The subject of the research is methods and mechanisms for protecting information from substitution and deletion using blockchain technology.

The purpose of the research is to develop and study methods for protecting information from substitution and deletion using blockchain technology by implementing a mechanism for randomized validation of blocks and transactions, which contributes to increasing the level of data integrity, reducing the risks of compromise and improving the efficiency of the system.

The first section implements a systematic analysis of modern blockchain systems and mechanisms for ensuring data integrity. It is shown that existing approaches have limitations related to the predictability of validation processes, which creates prerequisites for attacks, in particular, of the "51%" type, double spending, and manipulation of the order of transaction

confirmation. The hypothesis of the feasibility of using randomization as a key factor in strengthening security is substantiated.

In the second section, the theoretical and methodological foundations of the randomized validation mechanism are developed. A formal model of random selection of validator nodes is proposed, which considers the size of the network, the proportion of malicious nodes, and selection parameters, and allows quantitatively assessing the probability of system compromise. A generalized mechanism for randomized confirmation of blocks and transactions is formed, which reduces the level of determinism of the validation process and complicates the implementation of targeted attacks. The results of simulation modeling show that the probability of a successful attack decreases with increasing entropy of the selection mechanism.

In the third section, a mechanism for generating high-entropy random numbers based on quantum physical processes is developed. A prototype of a quantum random number generator using photon noise as a source of entropy is proposed, and its experimental validation is carried out using statistical tests of the quality of randomness. It is confirmed that the use of physical sources of entropy provides increased unpredictability of the choice of validators and, accordingly, a reduction in the risk of attacks aimed at substituting or deleting.

The scientific novelty of the results obtained is that for the first time a mechanism for randomized validation of blocks and transactions in blockchain systems based on cryptographically and physically protected sources of randomness has been proposed, which allows for increased resistance to substitution and unauthorized deletion of data due to the unpredictability of the selection of validator nodes. A formal model for the random selection of validator nodes has been developed, which allows for an assessment of the probability of system compromise depending on the proportion of malicious nodes and network parameters. The use of quantum sources of entropy, in particular photonic noise, in the consensus processes of blockchain networks has been substantiated, which contributes to an increase in the unpredictability of randomization and reduces the risk of attacks. The approach to ensuring the integrity and protection of data in blockchain systems has been improved by integrating randomized validation procedures, which contributes to an increase in resistance to attacks and a reduction in computational redundancy. Also, methods for assessing the security of

blockchain networks have been improved, taking into account the stochastic characteristics of validator selection and models for analyzing the effectiveness of consensus mechanisms, supplemented by indicators of energy efficiency and scalability.

The theoretical principles of building decentralized systems with randomized control of validation processes, approaches to reducing the risks of attacks, in particular of the "51%" type, due to the unpredictable distribution of roles in the network, as well as the use of blockchain technologies in systems that require an increased level of trust, have been further developed. The theoretical significance of the results obtained lies in the development of scientific approaches to ensuring the integrity and reliability of data in distributed systems based on blockchain technology. The work substantiates that the effectiveness of information protection against substitution and unauthorized deletion is determined not only by the use of cryptographic mechanisms, but also by the level of unpredictability of validation processes. The proposed approach expands existing theoretical ideas about the role of randomization as a fundamental factor in ensuring security, which affects the system's resistance to coordinated attacks.

The practical significance lies in the possibility of implementing the proposed mechanism in existing and promising blockchain platforms. Its application allows to increase the level of data protection against substitution and deletion, reduce computational costs and energy consumption, increase system throughput, reduce transaction confirmation time, reduce requirements for hardware resources of nodes and increase the level of decentralization. The results can be used in financial, government, medical and corporate information systems, as well as in artificial intelligence systems, where the reliability, integrity and immutability of data are critically important. The proposed approach can be used to protect training samples, data processing results and information exchange processes in distributed AI systems, in particular in decision support systems, medical AI platforms and intelligent analytical services.

Keywords: blockchain, information security, randomized validation, consensus, cryptography, quantum entropy, visualization, distributed systems, dataset, neural network, AI, software architecture, fault tolerance, random selection, modeling, software implementation.

ПЕРЕЛІК ПУБЛІКАЦІЙ ЗДОБУВАЧА

Статті в фахових виданнях, в яких опубліковані основні наукові результати дисертації

1. Горелікова Т. О., Чопоров С. В. Аналіз методів захисту інформації від підміни та видалення, що ґрунтуються на технології блокчейн. *Computer Science and Applied Mathematics.* 2024. № 1. С. 54–65. URL: https://doi.org/10.26661/2786-6254-2024-1-07.

2. Horelikova T. O. Enhanced data protection in blockchain: Mitigating tampering and deletion through randomized checkpoints. *Infocommunication and Computer Technologies.* 2024. V. 2, № 08. URL: https://doi.org/10.36994/2788-5518-2024-02-08-05.

3. Горелікова Т. О. Механізм захисту інформації від підміни та видалення у блокчейн мережах. *Наукові записки Міжнародного гуманітарного університету.* 2024. № 41. С. 19. URL: https://doi.org/10.32782/2663-5682/2024/41/19.

4. Horelikova T., Choporova O., Choporov S. Blockchain as a tool for protecting medical data in artificial intelligence systems. *Artificial Intelligence*. 2025. № 4. Pp. 124–131. URL: https://doi.org/10.15407/jai2025.04.124.

5. Горелікова Т. О., Чопорова О. В. Рандомізоване підтвердження блоків у блокчейн-системах. *Прикладні питання математичного моделювання*. 2025. Т. 8, № 2. С. 69–79. URL: https://doi.org/10.32782/mathematical-modelling/2025-8-2-7.

6. Горелікова Т. О. Розробка пристрою для одержання високої ентропії з фотонного шуму у криптографічних застосуваннях. *Наносистеми, наноматеріали, нанотехнології.* 2026. Т. 24, № 1. С. 53–64. URL: https://doi.org/10.15407/nnn.24.01.0053.

7. Горелікова Т. О., Чопорова О. В. Високоентропійні випадкові числа як основа криптографічної безпеки: квантовий підхід. *Прикладні питання математичного моделювання.* 2026. № 9.1. URL: https://journals.kntu.kherson.ua/index.php/ppmm/issue/view/91

Матеріали апробації (тези доповідей):

1. Горелікова Т. О. Огляд методів захисту інформації від підміни та видалення, що ґрунтуються на технології блокчейн. *Актуальні проблеми математики* : тези доповідей Всеукр. наук. конф. (м. Запоріжжя, 2023 р.). Запоріжжя : ЗНУ, 2023. С. 12. URL: https://www.znu.edu.ua/faculty/math/confirences/tezi_apm___23.pdf.

2. Horelikova T. O. Mechanism for protecting information from substitution and deletion in blockchain networks. *Existential challenges of education, science, security and health in modern conditions*: Proceedings of the All-Ukrainian Scientific and Practical Conference (Odesa, December 12, 2024). Odesa, 2024.

3. Горелікова Т. О. Дослідження випадкового вибору вузлів і блоків під час перевірки в блокчейн-системах. *Сучасні інформаційні технології та системи в управлінні* : зб. матеріалів VI Міжнар. наук.-практ. конф. молодих вчених, аспірантів і студентів (м. Київ, 10–11 квіт. 2025 р.). Київ : КНЕУ, 2025. С. 343–345. URL: https://ir.kneu.edu.ua/items/a8120799-35a3-49dd-bfca-5487a1b21cc6.

4. Горелікова Т. О. Рандомізоване підтвердження блоків. *Актуальні проблеми математики* : тези доповідей Всеукр. наук. конф. (м. Запоріжжя, 2025 р.). Запоріжжя : ЗНУ, 2025. С. 71. URL: https://www.znu.edu.ua/faculty/math/confirences/tezi_apm___2025.pdf.

ЗМІСТ

Перелік умовних скорочень 13

Вступ 14

1. Аналіз теоретико-прикладних засад захисту інформації в контексті технології блокчейн 25

1.1. Специфіка архітектури блокчейн у контексті забезпечення безпеки даних 25

1.2. Аналіз надійності блокчейн в контексті криптографічних методів 31

1.3. Дослідження надійності блокчейн-систем на рівні вузлів 42

1.4. Систематизація та узагальнення методів забезпечення надійності блокчейн-систем 45

1.5. Аналіз актуальних загроз безпеці блокчейн-систем 49

Висновок до розділу 1 55

2. Моделювання та обґрунтування алгоритму рандомізованої валідації блоків і транзакцій у блокчейн-системах 58

2.1. Розробка методу випадкового вибору учасників і контрольних точок 59

2.2. Розробка методу випадкового вибору вузлів 66

2.3. Формування синтезованого методу рандомізованого підтвердження блоків 75

2.4. Експериментальна валідація та аналіз ефективності методу 83

Висновок до розділу 2 91

3. Розробка та впровадження квантових генераторів високоентропійних випадкових чисел для підвищення криптографічної стійкості систем 93

3.1. Науково-технічні засади формування високоентропійного ресурсу як чинника забезпечення криптографічної безпеки 93

3.2. Розробка пристрою квантового генератора випадкових чисел на основі дробового шуму 95

3.3. Обґрунтування критеріїв оцінки рівня ентропії випадкових послідовностей 103

3.4. Експериментальні дослідження та верифікація характеристик розробленого генератора 106

Висновок до розділу 3 118

Висновки 121

Список використаних джерел 123

Додатки 134

ПЕРЕЛІК УМОВНИХ СКОРОЧЕНЬ

PoW – Proof of Work, доказ виконання роботи (алгоритм консенсусу)

PoS – Proof of Stake, доказ частки володіння (алгоритм консенсусу)

AI – Artificial Intelligence, штучний інтелект

DDoS – Distributed Denial of Service, розподілена атака на відмову в обслуговуванні

QRNG – Quantum Random Number Generator, квантовий генератор випадкових чисел

RSA – Rivest Shamir Adleman, криптографічний алгоритм із відкритим ключем, названий на честь творців алгоритму: Рона Рівеста, Аді Шаміра, Леонарда Адлемана

PRNG – Pseudo Random Number Generator, генератор псевдовипадкових чисел

CSPRNG – Cryptographically Secure Pseudo-Random Number Generator, криптографічно стійкий генератор псевдовипадкових чисел

HRNG – Hardware Random Number Generator, апаратний генератор випадкових чисел

ВСТУП

Актуальність. У сучасних умовах цифрової трансформації економіки та суспільства блокчейн-технології набувають статусу базової інфраструктури для забезпечення довіри у відкритих і розподілених інформаційних системах. Водночас зі зростанням масштабів використання загострюються проблеми безпеки, стійкості до атак та ефективності.

Ключовим аспектом розвитку блокчейн-технологій є не лише продуктивність чи енергоефективність, а насамперед забезпечення цілісності даних, тобто їх захисту від підміни та несанкціонованого видалення.

Особливої актуальності ця проблема набуває у системах штучного інтелекту, де достовірність і незмінність даних безпосередньо впливають на коректність роботи моделей машинного навчання та результатів автоматизованого прийняття рішень. Підміна або спотворення даних у таких системах може призводити до некоректного функціонування AI-моделей, що створює додаткові ризики для критично важливих застосувань.

Блокчейн за своєю природою є відкритою та прозорою системою: усі транзакції та записи в реєстрі доступні для перевірки будь-яким учасником мережі. Саме ця відкритість є значною перевагою, особливо для таких застосувань, як зберігання державних реєстрів, прав власності, документів чи інших критично важливих даних. Кожен запис можна незалежно перевірити, що підвищує рівень довіри до системи без необхідності централізованого контролю.

Водночас така прозорість висуває підвищені вимоги до безпеки: будь-яка успішна атака, спрямована на зміну або видалення даних, стає глобальною проблемою, оскільки змінена інформація також буде відкрито доступною всім учасникам. Таким чином, основна мета атак на блокчейн-системи частіше всього зводиться саме до:

- підміни історії транзакцій чи даних;
- повторного проведення транзакцій;

– фактичного «відкату» стану мережі, що еквівалентно видаленню частини даних.

Актуальність забезпечення цілісності даних також зростає у контексті розвитку розподілених систем штучного інтелекту, зокрема федеративне навчання та інтелектуальних аналітичних платформ, де блокчейн може використовуватись як механізм підтвердження достовірності даних, моделей та результатів обробки інформації.

Історичний аналіз показує, що лише у період 2018–2024 років було зафіксовано понад 50 успішних атак типу «51%» на мережі (Ethereum Classic, Bitcoin Gold та інші). Наприклад, у 2020 році мережа Ethereum Classic зазнала серії атак, у результаті яких було зазнано збитків понад 5 млн доларів США. Подібні інциденти демонструють, що навіть при використанні сучасних криптографічних методів захисту, вразливості можуть виникати на рівні механізмів консенсусу. Фактично, атака типу «51%» дозволяє зловмиснику переписати історію блоків, тобто здійснити підміну або виключення вже підтверджених даних.

Таким чином, можна стверджувати, що переважна більшість атак на блокчейн прямо або опосередковано спрямована саме на порушення незмінності даних, яка є ключовою властивістю цієї технології.

Компрометація системи у даному дослідженні розглядається як стан, за якого зловмисник отримує можливість впливати на процес валідації або структуру блокчейну, що призводить до підміни, спотворення або несанкціонованого видалення даних.

Крім того, проблема надлишкової валідації також має безпековий аспект. У традиційних блокчейн-системах значна кількість вузлів виконує однакову перевірку транзакцій і блоків. При цьому така модель не завжди ефективно протидіє скоординованим атакам, особливо у випадках концентрації обчислювальних ресурсів або валідаторів.

У відповідь на ці виклики сучасні дослідження спрямовані на розробку нових підходів до організації процесу валідації, які дозволяють підвищити саме стійкість до атак на цілісність даних. Одним із обраних напрямів є використання

рандомізованих механізмів відбору валідаторів. Основна ідея полягає у криптографічно захищеному випадковому виборі лише частини вузлів для перевірки кожного блоку. Це дозволяє:

– зменшити обчислювальні витрати;

– скоротити час підтвердження транзакцій;

– ускладнити реалізацію атак, спрямованих на підміну або видалення даних, оскільки зловмисник не може наперед визначити, які вузли братимуть участь у валідації.

Значущість такого підходу підтверджується також дослідженням технологій генерації випадкових чисел у контексті забезпечення справді випадкових значень. Традиційні псевдовипадкові генератори можуть бути вразливими до прогнозування, що створює ризики маніпуляції процесом вибору валідаторів. У зв’язку з цим зростає інтерес до використання інших джерел ентропії.

Подібні механізми можуть бути використані і в системах штучного інтелекту для забезпечення надійності процесів обробки даних та функціонування розподілених AI-середовищ.

Застосування подібних підходів є перспективним також для розподілених AI-систем, у яких важливим є забезпечення достовірності та захисту даних у процесі їх обробки й передачі між вузлами.

Відсутність ефективних механізмів рандомізованої валідації у сучасних блокчейн-системах призводить до низки практичних проблем:

– обмеження масштабованості мереж при збільшенні кількості користувачів;

– зростання вартості підтримки інфраструктури;

– підвищення ризиків централізації;

– вразливість до координованих атак;

– неможливість ефективного використання у високонавантажених системах.

Крім того, зазначені обмеження ускладнюють використання блокчейн-технологій у високонавантажених AI-системах, де необхідна одночасна обробка великих обсягів даних, забезпечення їх достовірності та підтримка високої швидкості взаємодії між розподіленими вузлами. У зв'язку з цим підвищення масштабованості та ефективності блокчейн-мереж є важливим фактором розвитку сучасної інфраструктури штучного інтелекту.

Таким чином, актуальним науково-прикладним завданням є розробка та дослідження методів захисту інформації від підміни та видалення на основі технології блокчейн із використанням удосконалених механізмів валідації та криптографічно захищених джерел випадковості. Запропонований у роботі механізм рандомізованого підтвердження блоків відповідає сучасним викликам і може бути використаний як основа для наступного покоління блокчейн-архітектур, орієнтованих на високу масштабованість, енергоефективність та стійкість до атак.

Загальна оцінка цього дослідження показує, що рандомізоване підтвердження блоків слід розуміти не як оптимізацію, а як структурну еволюцію архітектури блокчейну. Це дозволить створити системи, які зі збільшенням розміру мережі стають не тільки стійкішими до підміни або видалення даних, але й більш ресурсоефективними та високомасштабованими. Таким чином, цей підхід створює передумови для подальших досліджень і практичного застосування блокчейну.

Зв'язок роботи з науковими програмами, планами, темами.

Дисертаційна робота виконувалась відповідно до основних напрямів наукових досліджень кафедри комп'ютерних наук Запорізького національного університету у галузі інформаційної безпеки, криптографії та розподілених інформаційних систем.

Мета дослідження: розробка та дослідження методів захисту інформації від підміни та видалення з використанням технології блокчейн шляхом впровадження механізму рандомізованої валідації блоків і транзакцій, що забезпечує підвищення рівня цілісності даних, зниження ризиків компрометації та покращення ефективності функціонування системи.

Завдання дослідження. Для досягнення поставленої мети у роботі сформульовано та розв’язано такі взаємопов’язані наукові завдання:

1. Провести комплексний аналіз сучасних блокчейн-систем та існуючих механізмів захисту від підміни та видалення з метою виявлення їхніх переваг, недоліків і обмежень у контексті безпеки, децентралізації та масштабованості.
2. Дослідити основні загрози підміни та видалення даних блокчейн-мереж, зокрема атаки типу «51%», подвійні витрати, а також можливості маніпулювання процесом валідації транзакцій і блоків.
3. Розробити формальну математичну модель процесу рандомізованого вибору вузлів-валідаторів у розподіленій блокчейн-мережі.
4. Запропонувати механізм рандомізованої валідації блоків і транзакцій на основі криптографічно захищених функцій випадковості.
5. Оцінити ймовірність компрометації системи залежно від частки скомпрометованих вузлів та характеристик рандомізованого відбору.
6. Провести імітаційне моделювання роботи запропонованого механізму в різних умовах функціонування мережі (кількість вузлів, навантаження, затримки).
7. Виконати експериментальне дослідження ефективності механізму за показниками обчислювальних витрат, пропускної здатності, часу підтвердження транзакцій та мережевого навантаження.
8. Здійснити порівняльний аналіз запропонованого підходу з класичними механізмами консенсусу з метою визначення його ефективності в контексті захисту інформації від підміни та видалення.
9. Дослідити можливість використання квантових джерел ентропії (зокрема фотонного шуму) для підвищення якості та криптографічної стійкості рандомізації.

Об’єкт дослідження. Процеси забезпечення цілісності та достовірності даних у розподілених блокчейн-системах в умовах децентралізованого функціонування.

Предмет дослідження. Методи та механізми захисту інформації від підміни та видалення з використанням технології блокчейн.

Методи дослідження. У роботі використані методи теорії ймовірностей і математичної статистики, криптографії, теорії розподілених систем, математичного та імітаційного моделювання, теорії алгоритмів, системного аналізу, а також методи обчислювальної математики для оцінки ефективності та стійкості запропонованих рішень.

Наукова новизна отриманих результатів.

У дисертаційній роботі одержано нові наукові результати, наведені нижче.

1. *Вперше*:

   a) запропоновано механізм рандомізованої валідації блоків і транзакцій у блокчейн-системах, що базується на криптографічно та фізично захищених джерелах випадковості, який, на відміну від існуючих підходів, забезпечує підвищення стійкості до підміни та несанкціонованого видалення даних за рахунок непередбачуваності вибору вузлів-валідаторів і унеможливлення цілеспрямованого впливу на процес підтвердження транзакцій;

   b) розроблено формальну модель випадкового вибору вузлів-валідаторів, яка враховує параметри мережі та дозволяє оцінити ймовірність компрометації системи, що проявляється у можливості підміни або видалення даних, залежно від частки зловмисних вузлів і характеристик мережі;

   c) у контексті блокчейн-мереж обґрунтовано і застосовано практично використання квантових джерел ентропії (зокрема фотонного шуму) у процесах консенсусу блокчейн-мереж, що сприяє підвищенню непередбачуваності механізмів рандомізації, зменшення можливості прогнозування вибору валідаторів і, як наслідок, зниження ризику атак, спрямованих на підміну або видалення даних.

2. *Удосконалено*:

a) підхід до забезпечення цілісності та захисту даних у блокчейн-системах шляхом інтеграції рандомізованих процедур валідації, що дозволяє не лише зменшити надлишковість обчислень, але й підвищити стійкість системи до атак, пов’язаних із маніпулюванням процесом підтвердження даних;

b) методи оцінювання безпеки блокчейн-мереж за рахунок урахування стохастичних характеристик вибору валідаторів , що дає змогу більш точно визначати рівень захищеності системи від компрометації, пов’язаної з підміною або видаленням інформації;

c) моделі аналізу ефективності консенсусних механізмів, які доповнено показниками енергоефективності та масштабованості з урахуванням їх впливу на забезпечення цілісності даних і стійкість до атак.

3. *Набуло подальшого розвитку*:

a) теоретичні засади побудови децентралізованих систем із рандомізованим керуванням процесами валідації;

b) підходи до зниження ризиків атак, включно з атаками типу «51%» за рахунок непередбачуваного розподілу ролей у мережі;

c) застосування блокчейн-технологій у системах, що потребують підвищеного рівня довіри, зокрема в інформаційних та інтелектуальних системах.

Введення та застосування криптографічно захищених функцій рандомізації у механізмі валідації забезпечує такі покращення:

1. Підвищення стійкості безпеки до підміни і видалення даних шляхом зниження передбачуваності та вразливості механізмів рандомізації.

2. Усунення фіксованої структури призначення валідаторів, що унеможливлює їх попередню ідентифікацію та вплив на них з боку зловмисників.

3. Підвищення ефективності функціонування системи за рахунок динамічного зменшення кількості активних вузлів валідації без зниження рівня безпеки та захисту даних.

4. Підвищення масштабованості блокчейн-системи, оскільки запропонований алгоритм функціонує незалежно від розміру мережі та має низькі вимоги до обчислювальних ресурсів.

5. Розширення можливостей розв’язання задач забезпечення цілісності даних у великих розподілених системах за рахунок застосування запропонованого методу, який, на відміну від традиційних підходів, дозволяє уникнути як надмірного обчислювального навантаження, так і структурної централізації.

Таким чином, ця робота визначає нову методологічну основу, яка може впливати як на архітектуру, так і на функціональність майбутніх блокчейн-мереж.

Теоретична значущість отриманих результатів. Теоретична значущість отриманих результатів полягає у розвитку наукових підходів до забезпечення цілісності та достовірності даних у розподілених системах на основі технології блокчейн. У роботі обґрунтовано, що ефективність захисту інформації від підміни та несанкціонованого видалення визначається не лише застосуванням криптографічних механізмів, але й рівнем непередбачуваності процесів валідації. Запропонований підхід розширює існуючі теоретичні уявлення про роль рандомізації як фундаментального чинника забезпечення безпеки, що впливає на стійкість системи до координованих атак.

Розроблені моделі та методи рандомізованого вибору валідаторів і підтвердження блоків формують нову теоретичну основу для побудови децентралізованих інформаційних систем із підвищеним рівнем захисту даних. Вперше встановлено взаємозв’язок між якістю джерел випадковості, зокрема високою ентропією фізичних та квантових процесів, і рівнем захищеності блокчейн-систем від компрометації. Це дозволяє розглядати рандомізацію не як допоміжний елемент, а як ключовий механізм забезпечення цілісності, незмінності та надійності даних у сучасних розподілених середовищах.

Практична значущість отриманих результатів. Практична значущість одержаних результатів полягає у можливості їх використання для підвищення рівня захисту даних від підміни і видалення, а також для забезпечення ефективності, безпеки та масштабованості сучасних блокчейн-систем.

Запропонований алгоритм дозволяє:

– зменшити обчислювальні витрати та енергоспоживання блокчейн-мереж за рахунок скорочення кількості вузлів, що одночасно беруть участь у процесі валідації;

– підвищити пропускну здатність системи та зменшити час підтвердження транзакцій, що є критичним для високонавантажених застосувань;

– знизити вимоги до апаратного забезпечення вузлів, що спрощує участь у мережі та сприяє підвищенню рівня децентралізації;

– підвищити стійкість до атак, спрямованих на підміну або видалення даних, зокрема за рахунок непередбачуваності вибору валідаторів і ускладнення координації зловмисних дій;

– забезпечити більш ефективне використання ресурсів у розподілених системах.

Розроблені моделі та алгоритми можуть бути використані при:

– створенні нових або модернізації існуючих блокчейн-платформ;

– розробці фінансових технологій, зокрема платіжних систем і систем цифрових активів;

– побудові систем захисту даних у медичних, державних та корпоративних інформаційних системах;

– інтеграції блокчейн-рішень у системи штучного інтелекту для забезпечення достовірності даних;

– розробці енергоефективних розподілених обчислювальних інфраструктур.

Отримані результати можуть бути впроваджені у публічних і приватних блокчейн-мережах без суттєвої зміни їх архітектури, що забезпечує їх універсальність і прикладну цінність.

Це заповнює методологічну прогалину, оскільки існуючі рішення лише частково відповідають одночасним вимогам безпеки, децентралізації, ефективності та масштабованості.

Апробація результатів дослідження. Основні положення, наукові результати та висновки дисертаційної роботи доповідалися, обговорювалися та отримали схвальну оцінку на міжнародних та всеукраїнських науково-практичних конференціях і наукових семінарах, зокрема:

24-28 жовтня 2023 р. – Web Information Systems Engineering WISE 2023 (міжнародна конференція) – презентовано результати досліджень з рандомізованої валідації блоків та методів захисту блокчейн-мереж від атак типу «51%»;

19 жовтня 2023 р. – STEM Cluster/CDMS Research Seminar: Information Security Using Blockchain Technology: Mitigating Centralization Risk and the "51% Attack" (науковий семінар) – обговорено методи криптографічно захищеної рандомізації для підвищення стійкості децентралізованих мереж;

16-18 жовтня 2023 р. – The International Symposium on Communications and Information Technologies in UTS (міжнародний симпозіум) – представлено модель випадкового вибору валідаторів та оцінено її вплив на ефективність і безпеку блокчейн-систем;

12 грудня 2024 р. – Всеукраїнська науково-практична конференція студентів, аспірантів та молодих учених «Екзистенційні виклики освіти, науки, безпеки та здоров’я в сучасних умовах: пошуки молодих вчених» (м. Одеса) – продемонстровано механізм захисту інформації від підміни та видалення у блокчейн-мережах;

10-11 квітня 2025 р. – VI Міжнародна науково-практична конференція молодих вчених, аспірантів і студентів «Сучасні інформаційні технології та системи в управлінні» (м. Київ, КНЕУ) – представлено дослідження випадкового вибору вузлів і блоків під час перевірки в блокчейн-системах;

24-25 квітня 2025 р. – Всеукраїнська наукова конференція «Актуальні проблеми математики» (м. Запоріжжя, ЗНУ) – обговорено підходи до рандомізованого підтвердження блоків;

12-13 листопада 2025 р. – Міжнародна конференція «Досягнення, перспективи і ризики впровадження штучного інтелекту у сфері охорони здоров’я України» (м. Київ) – апробовано результати дослідження у контексті захисту

медичних даних та забезпечення надійності AI-систем на основі технології блокчейн.

Усі виступи отримали схвальні відгуки учасників конференцій та були відзначені активним обговоренням наукових результатів, що підтверджує актуальність і практичну значущість проведеного дослідження.

Публікації. За результатами проведених досліджень опубліковано 7 наукових праць, серед яких 7 статей у наукових фахових виданнях України, а також матеріали доповідей у збірниках науково-практичних конференцій.

Особистий внесок здобувача. Усі основні результати дисертаційної роботи отримані автором самостійно.

У наукових працях, опублікованих у співавторстві, автору належить:

[1] – проведено аналіз методів захисту інформації від підміни та видалення у блокчейн-системах;

[2] – запропоновано підхід до використання рандомізованих контрольних точок для підвищення безпеки даних;

[3] – розроблено алгоритм захисту інформації у блокчейн-мережах;

[4] – досліджено застосування блокчейн-технологій для захисту медичних даних у системах штучного інтелекту;

[5] – запропоновано алгоритм рандомізованого підтвердження блоків;

[6, 7] – розроблено і обґрунтовано підхід до генерації високоякісної ентропії на основі фізичних процесів для криптографічних застосувань.

Структура та обсяг дисертації. Дисертаційна робота складається зі вступу, трьох розділів, висновків, переліку використаних джерел зі 99 найменувань та додатку. Основний зміст викладено на 108 сторінках друкованого тексту, проілюстровано 16 рисунками та 7 таблицями. Загальний обсяг дисертації становить 140 сторінок.

1. АНАЛІЗ ТЕОРЕТИКО-ПРИКЛАДНИХ ЗАСАД ЗАХИСТУ ІНФОРМАЦІЇ В КОНТЕКСТІ ТЕХНОЛОГІЇ БЛОКЧЕЙН

Блокчейн – це децентралізована система для запису транзакцій, яка зберігає дубльовані копії даних у багатьох місцях одночасно, а не в одному центральному сховищі. Децентралізована система – це система, в якій немає єдиного центру управління, а функції, дані та контроль розподілені між багатьма учасниками (вузлами). Це означає, що система працює без центрального сервера або посередника, що підвищує її стійкість, безпеку та відмовостійкість. Блокчейн використовується для зберігання, синхронізації та обміну даними[9]. Блокчейн-мережа базується на послідовній, криптографічно пов'язаній структурі блоків даних, в яких транзакції та інші інформаційні стани зберігаються постійно, незмінно та захищено.

1.1. Специфіка архітектури блокчейн у контексті забезпечення безпеки даних

На відміну від централізованих систем, де є єдиний власник і управитель мережі, блокчейн-системи підтримуються розподіленою мережею вузлів. Кожен вузол зберігає повну або часткову копію всього блокчейну та бере участь у процесі консенсусу для узгодження поточного стану ланцюга даних. Поняття консенсус у класичному блокчейні означає, що всі учасники мережі (вузли) мають досягти спільної згоди щодо правильності нових транзакцій перед тим, як їх буде додано до блоку та ланцюга. Це ключовий процес для забезпечення безпеки, децентралізації та цілісності мережі без центрального управління. Механізми консенсусу різняться залежно від архітектури блокчейну, але служать одній меті: забезпечити, щоб усі вузли сходились до однієї версії правильності даних, не покладаючись на центральний сервер чи єдиний керуючий вузол[10].

Криптографічна структура блокчейну забезпечує незмінність та стійкість до підміни і несанкціонованого видалення даних. Будь-яка спроба змінити або

вилучити інформацію з окремого блоку неминуче призводить до порушення цілісності всього ланцюга, оскільки це потребує перерахунку хешів усіх наступних блоків та отримання контролю над більшістю контрольної потужності мережі. На практиці це робить підміну або видалення даних обчислювально складним.

Важливою особливістю блокчейну є його відкритість: у більшості мереж усі транзакції доступні для перегляду та перевірки будь-яким учасником. Така прозорість є суттєвою перевагою, зокрема для зберігання державних реєстрів, електронних документів та інших критично важливих даних, оскільки забезпечує можливість незалежного аудиту та перевірки достовірності інформації в будь-який момент часу.

Кожен блок містить, окрім фактичних даних, які зберігає, криптографічне хеш-значення попереднього блоку, створюючи логічно та математично безпечний блокчейн. Хеш-значення – це результат математичної хеш-функції, яка перетворює вміст блоку на фіксовану послідовність символів; навіть найменша зміна даних у блоці призводить до повної зміни цього коду. Кожен блок містить позначку часу, посилання на попередній блок та колекцію перевірених транзакцій. Цей ланцюжок блоків утворює хронологічний, незмінний запис подій, розподілений між усіма учасниками мережі[10].

Блокчейн гарантує, що подальші зміни окремих даних будуть можливі лише шляхом повної реконструкції всіх наступних блоків – процес, який практично неможливий у розподілених системах з багатьма незалежними вузлами.

Загалом, блокчейн формує технологічну основу, що дозволяє забезпечити:

– прозоре та відстежуване зберігання даних;

– забезпечення надійного збереження даних в мережі, яка не потребує центрального блоку управління чи моніторингу;

– забезпечення безпеки за допомогою криптографії та розподіленого керування;

– представлення транзакцій або інформації у нефальсифікованій та перевіреній формі.

Таким чином, блокчейн – це не просто форма зберігання даних, а децентралізована, криптографічно захищена інформаційна система, що базується на структурній цілісності та математичній перевіреності.

По суті, блокчейн функціонує як розподілений консенсусно-керований автомат станів, де кожен новий блок представляє перехід до нового глобального стану, узгодженого мережею. Це робить його придатним не лише для цифрових валют, що вважається класичним застосуванням блокчейну, але й для ширших застосувань, таких як фінанси, управління ланцюгами поставок, цифрова ідентифікація та походження даних, зберігання даних, де довіра, прозорість та стійкість є критично важливими властивостями системи.

Технологія блокчейн дозволяє розробляти децентралізовані мережі, що базуються на розподіленій архітектурі програмного забезпечення та не потребують централізованої логіки керування. У таких мережах зберігання, перевірка та оновлення даних розподілені між численними рівнозначними вузлами, які пов'язані між собою криптографічними методами.

Ключовою особливістю блокчейну є незмінність даних: інформація зберігається в блоках, пов'язаних між собою за допомогою криптографічних хеш-функцій. Будь-яка модифікація існуючого блоку вимагатиме коригування всіх наступних блоків, що є обчислювально складним в децентралізованому середовищі. Це забезпечує високий рівень цілісності даних та стійкості до несанкціонованого доступу.

Механізми консенсусу гарантують, що всі учасники мережі приймають єдиний стан розподіленого реєстру. Це сприяє довірі між учасниками без залежності від центрального управління мережею. Водночас децентралізація підвищує стійкість, оскільки збій окремих вузлів не впливає на функціональність системи в цілому.

У технології блокчейн можна створювати контрольований потік даних, оскільки кожна транзакція або оновлення даних записується в блокчейні. Це може допомогти забезпечити цілісність і автентичність даних і полегшити відстеження змін з часом.

Незмінність даних у блокчейн-системах базується на специфічному механізмі зберігання та зв'язування даних. Після того, як блок даних додано до блокчейну та перевірено мережею, подальша модифікація або видалення інформації, яку він містить, практично неможлива без зміни всього ланцюжка наступних блоків[11].

Підвищення рівня цілісності та незмінності даних є особливо важливим для сучасних систем штучного інтелекту, функціонування яких безпосередньо залежить від достовірності навчальних наборів даних, результатів обробки інформації та коректності моделей машинного навчання. У таких системах блокчейн може використовуватись як механізм забезпечення довіри до даних, відстеження змін та захисту від несанкціонованої модифікації інформації у розподілених AI-середовищах.

Ця властивість додатково підтримується децентралізованими механізмами консенсусу, в яких кілька незалежних мережевих вузлів перевіряють та підтверджують правильність збережених даних. Це призводить до високого ступеня довговічності, цілісності та відстежуваності даних. Таким чином, незмінність блокчейну значно підвищує надійність збереженої інформації та робить технологію особливо придатною для застосувань, де стійкість до несанкціонованого доступу та довіра до даних відіграють центральну роль, наприклад, в інформаційній безпеці, фінансах або цифрових реєстрах. Технологію блокчейн використовують для автоматизації процесів, таких як виконання смарт-контрактів. Як результат можливо зменшити потребу в ручному втручанні та підвищити ефективність.

Існує кілька потенційних переваг використання технології блокчейн для роботи з даними. Зокрема аналіз, дозволяє виокремити такі переваги:

- безпека;
- децентралізація;
- відстеження;
- незмінність;
- автоматизація;

– взаємодія.

Технологія блокчейн дозволяє забезпечити надійний і захищений від втручання спосіб зберігання та передачі даних, оскільки дані зберігаються у блоках, які з’єднані разом у ланцюг. Це ускладнює зміну даних або доступ до них без дозволу.

При створенні сумісних систем об’єднаних мережею блокчейн, технологія дозволяє обмінюватися даними між різними організаціями чи системами. Це може допомогти вдосконалити передачу інформації та полегшити співпрацю. Це також створює передумови для побудови децентралізованих систем штучного інтелекту, у яких блокчейн забезпечує безпечний обмін даними між різними AI-модулями, організаціями або аналітичними платформами без необхідності використання централізованих механізмів контролю.

Важливо зазначити, що ефективність технології блокчейн залежить від способу її реалізації. Для забезпечення надійного захисту даних у блокчейн-системах, зокрема від підміни та несанкціонованого видалення, застосовується комплекс криптографічних методів, які є окремими об’єктами сучасних наукових досліджень. Їх використання спрямоване передусім на гарантування цілісності, автентичності та незмінності інформації, що зберігається у розподіленому реєстрі.

З огляду на відкритий характер більшості блокчейн-мереж, де всі записи є публічно доступними для перегляду та перевірки, критично важливим є забезпечення неможливості прихованої модифікації або видалення даних. Саме криптографічні механізми формують базовий рівень такого захисту, ускладнюючи будь-які несанкціоновані зміни без порушення цілісності всієї системи.

Зокрема, у контексті розвитку технології блокчейн активно досліджуються та застосовуються такі криптографічні методи:

– методи хешування, які забезпечують зв’язність блоків між собою та дозволяють миттєво виявити будь-яку спробу підміни або видалення даних через зміну хеш-значень;

− методи роботи з цифровими підписами, що гарантують автентичність джерела даних і унеможливлюють підробку транзакцій або їх несанкціоноване редагування;

− методи криптографії з відкритим ключем, які забезпечують захищену ідентифікацію учасників мережі та контроль доступу до операцій запису даних;

− методи доказу з нульовим знанням, що дозволяють підтверджувати коректність даних без розкриття їх змісту, зберігаючи баланс між прозорістю та конфіденційністю.

Додатково для підвищення рівня захисту застосовуються механізми шифрування та багатофакторної автентифікації, які ускладнюють несанкціонований доступ до ключів та облікових записів користувачів. У сукупності ці підходи створюють багаторівневу систему безпеки, де будь-яка спроба підміни або видалення даних стає складно реалізованою без повного контролю над мережею. [10, 11].

Аналіз публікації, що присвячено застосуванню технології блокчейн, дозволяє виокремити такі тематичні напрями:

− дослідження потенціалу технології блокчейн з точки зору забезпечення надійного і прозорого способу зберігання та керування даними;

− дослідження особливостей забезпечення цілісності та незмінності даних у захисті даних;

− дослідження потенціалу технології блокчейн для полегшення взаємодії та обміну даними між різними організаціями: забезпечення сумісності систем різних сторін, особливості протоколів тощо;

− дослідження області застосування технології блокчейн у проблемі захисту даних: аналіз методів забезпечення масштабованості, продуктивності та керованості систем захисту інформації.

1.2. Аналіз надійності блокчейн в контексті криптографічних методів

Хешування – це фундаментальний метод в інформатиці та прикладній криптографії, що використовується для обробки, захисту та перевірки цифрової інформації. Хешування – це алгоритмічне перетворення вхідних даних будь-якої довжини у вихідне значення фіксованої довжини, так зване хеш-значення, яке генерується за допомогою математично визначеної хеш-функції[12]. Ця функція перетворює вхідні дані в компактний, псевдо-випадковий бітовий рядок, який служить унікальним представленням вихідної інформації. Ключовою характеристикою хешування є те, що процес перетворення є детермінованим (однакові вхідні дані завжди дають однакове хеш-значення, тоді як різні вхідні дані призведуть до різних хеш-значень). Водночас процес практично незворотний, оскільки вихідні дані неможливо просто відновлювати з хеш-значення, зараз можна це зробити лише з непропорційно високими обчислювальними зусиллями. Навіть незначні зміни у вхідних даних, такі як заміна одного символу, призводять до значної зміни результуючого хеш-значення, явища, відомого як ефект «лавини», що дозволяє надійно виявляти маніпуляції. Завдяки цим властивостям хешування використовується в багатьох сферах, зокрема для захисту паролів, перевірки цілісності даних, ефективної організації структур даних, а також у криптографічних протоколах та системах блокчейн[12].

У технології блокчейн хеш-значення формують основу для зв'язування окремих блоків, оскільки кожен блок містить хеш попереднього блоку, що практично виключає можливість подальшої зміни збережених даних. Безпека методу хешування значною мірою залежить від використовуваної хеш-функції, а сучасні криптографічні алгоритми, такі як SHA-256 або SHA-3, розроблені таким чином, що колізії, тобто поява однакових хеш-значень для різних вхідних даних, є надзвичайно малоймовірними. Тому хешування є ключовим інструментом для забезпечення цілісності, автентичності та достовірності даних у сучасних системах обробки інформації[13].

Хеші є важливою частиною безпеки та цілісності технології блокчейн, оскільки вони можуть гарантувати, що дані в блокчейні не були змінені або підроблені. Вони також відіграють ключову роль у децентралізованому характері технології блокчейн, оскільки дозволяють вузлам у мережі перевіряти цілісність даних без необхідності довіряти власнику мережі[13].

Робота [14] дослідників Шуо Чен, Фан Лонг, Кэ Сюй містить огляд структури даних блокчейну та обговорює роль хешування в захисті даних у блокчейні. Ця робота зосереджується на порівнянні різних структур даних блокчейна та їх ефективності з точки зору безпеки, масштабованості та енергоефективності. Автори проводять ретельний аналіз різних структур даних блокчейна, включаючи пов’язані списки, деревовидні структури та спрямовані ациклічні графи, *що стали основою розробленої технології.*

Стаття [15] надає огляд різноманітних застосувань технології блокчейн, у тому числі у фінансах, управлінні ланцюгами поставок та цифровій ідентифікації. Автори також обговорюють технічні проблеми та обмеження технології блокчейн, такі як масштабованість і споживання енергії. У статті робиться висновок, що хоча технологія блокчейн має значний потенціал, для повної реалізації її потенціалу необхідні подальші дослідження та розробки.

У статті[16] обговорюються правові наслідки використання технології блокчейн і досліджується роль хешування в захисті даних у блокчейні. Дослідник розглядає правові наслідки технології блокчейн, зокрема, щодо традиційних правових рамок. Автор стверджує, що технологія блокчейн має потенціал порушити традиційні правові системи і що правові рамки необхідно адаптувати для цієї нової технології. У статті робиться висновок про необхідність подальших досліджень у цій галузі, щоб повністю зрозуміти правові наслідки технології блокчейн.

Робота [17] науковця Кшетрі міститься огляд використання технології блокчейну для управління ланцюгом поставок і обговорюється роль хешування в захисті даних у блокчейні. Автор демонструє потенційні переваги використання технології блокчейн в управлінні ланцюгом поставок, такі як покращена

відстежуваність, прозорість і безпека. У статті також висвітлюються деякі проблеми та обмеження використання технології блокчейн в управлінні ланцюгом поставок, такі як масштабованість і відповідність нормативним вимогам.

У роботі [18] проводиться огляд існуючих систем обміну даними на основі блокчейну та аналізується роль хешування в захисті даних у блокчейні. Автори розглядають різні типи систем обміну даними, такі як однорангові та розподілені системи обміну даними, та обговорюють їхні переваги та недоліки.

За результатами аналізу робіт [14–18] можна зробити висновок, що використання хешів у технології блокчейн має як переваги, так і недоліки. Зокрема, переваги використання хешів у технології блокчейн включають:

− безпеку – можливість хешів забезпечити безпечний спосіб перевірки цілісності даних у блокчейні, оскільки їх важко підробити або змінити (це також може допомогти забезпечити достовірність даних у блокчейні);

− обчислювальну ефективність: хеші можна швидко обчислити, що може підвищити ефективність перевірки цілісності даних у блокчейні;

− децентралізацію – архітектурна властивість мережі для перевірки цілісності даних у блокчейні без необхідності використання одного центрального управління.

До недоліків використання хешів у технології блокчейн можна включити такі властивості:

− вразливість до кібератак;

− залежність безпеки від основної криптографічної системи;

− залежність продуктивності від апаратного та програмного забезпечення, що використовується для підтримки блокчейну[19].

Загалом, хоча хеші можуть забезпечити безпечний і ефективний спосіб перевірки цілісності даних у блокчейні, важливо ретельно розглядати потенційні недоліки та обмеження цього підходу та впровадити відповідні заходи безпеки для захисту від потенційних загроз.

Криптографія з відкритим ключем та цифрові підписи є однією з вирішальних базисів безпеки сучасних блокчейн-технологій та розподілених

інформаційних систем. Вони забезпечують бездоганну між учасниками децентралізованої мережі, гарантуючи автентичність, цілісність, конфіденційність та відстежуваність цифрових транзакцій і документівх[20].

Цифрові підписи – це фундаментальний криптографічний інструмент для перевірки автентичності та цілісності цифрових даних. Вони базуються на асиметричних криптографічних методах, що використовують пару ключів, які складається із закритого та відкритого ключа. Закритий ключ використовується для створення цифрового підпису та має зберігатися в таємниці, тоді як відкритий ключ є загальнодоступним та використовується для перевірки підпису. Асиметрична архітектура криптографічної системи формує формально доведений механізм ідентифікації, що забезпечує однозначне зіставлення цифрового підпису з відповідним користувачем. Процес створення цифрового підпису починається з обчислення криптографічного хеш-значення з даних, що підлягають ідентифікації особи, що використовує дані. Це хеш-значення забезпечує унікальне, щільне представлення вмісту вихідних даних. Далі це хеш-значення криптографічно обробляється за допомогою закритого ключа підписувача, в результаті чого утворюється фактичний цифровий підпис. Під час перевірки хеш-значення отриманих даних перераховується та порівнюється з переданим підписом за допомогою відкритого ключа. Якщо обидва значення збігаються, можна з високим ступенем впевненості припустити, що дані не були змінені з моменту підписання та фактично походять від зазначеного автора. Будь-яка подальша маніпуляція даними неминуче призведе до недійсного підпису[21].

У контексті технології блокчейн цифрові підписи відіграють важливу роль у перевірці та авторизації транзакцій. Вони гарантують, що транзакції можуть бути ініційовані лише тими учасниками мережі, які володіють відповідним закритим ключем, таким чином запобігаючи несанкціонованому доступу або маніпуляціям з зовні мережі. Кожна транзакція в блокчейн-системі супроводжується цифровим підписом, який забезпечує криптографічний захист її автентичності та цілісності. Ця функція має центральне значення для функціонування децентралізованих систем, оскільки довіра базується на математичних, а не інституційних принципах [22].

Цифрові підписи також гарантують, що людина не зможе заперечити, що саме вона підписала документ. Після підписання даних або транзакції автор не може згодом відмінити підпис, оскільки підпис унікальним чином пов'язаний з його закритим ключем. Ця властивість особливо важлива для юридично значущих застосувань, таких як цифрові контракти, електронні ідентифікаційні дані або смарт-контракти. У системах смарт-контрактів цифрові підписи дозволяють автоматизоване, прозоре та перевірене виконання визначених умов без втручання людини [23].

У наукових джерелах значна увага приділяється теоретичному аналізу та прикладним аспектам використання цифрових підписів у блокчейн-системах. Робота[24] надає всебічний огляд використання цифрових підписів у технології блокчейн та досліджує їхній вплив на безпеку та захист даних. У дослідженні [25] аналізуються різні схеми підписів з точки зору їхньої функціональності та продуктивності, тоді як у дослідженні науковців Ліна та Чена [26] детально розглядається роль цифрових підписів в архітектурах систем на основі блокчейну. Практичний приклад застосування представлено в роботі «Цифрові підписи в управлінні ланцюгами поставок на основі блокчейну: тематичне дослідження»[27], де цифрові підписи використовуються в системі управління ланцюгами поставок на основі блокчейну. У статті [28] додатково досліджується використання цифрових підписів у смарт-контрактах та обговорюються їхні наслідки для безпеки.

Аналіз робіт [24–28] дозволяє вивести загальну класифікацію варіантів використання цифрових підписів у технології блокчейн, яка схематично представлена на рисунку 1.1. Ці варіанти використання варіюються від перевірки транзакцій та управління ідентифікацією до автоматизації складних бізнес-процесів.

Рисунок 1.1 – Різні випадки використання цифрових підписів

Використання цифрових підписів у блокчейні надає безліч переваг. До них належать: високий рівень безпеки завдяки використанню усталених криптографічних методів, підвищена надійність та можливість автоматизації процесів, таких як виконання смарт-контрактів. Крім того, цифрові підписи сприяють захисту конфіденційності, оскільки вони дозволяють перевіряти транзакції без необхідності розкриття змісту переданих даних [29].

Водночас, використання лише цифрових підписів як єдиного механізму захисту не забезпечує повного рівня безпеки, зокрема у контексті протидії підміні та несанкціонованому видаленню даних. Ключовим ризиком залишається розкриття закритого ключа – його втрата або крадіжка. У такому випадку зловмисник отримує можливість формувати підтверджені підписані транзакції, що може призвести до підміни даних у реєстрі або ініціювання операцій, які неможливо скасувати чи видалити через незмінність блокчейну. Водночас законний власник втрачає контроль над своїми даними та активами, а відновлення доступу до закритого ключа, як правило, є неможливим.

Додатковою проблемою є те, що цифрові підписи, як і інші криптографічні механізми, можуть ставати об’єктом кібератак, зокрема внаслідок помилок реалізації, вразливостей програмного забезпечення або неналежного зберігання

ключів. Це створює потенційні умови для несанкціонованого втручання в систему, навіть за умови формальної криптографічної стійкості алгоритмів. Існують також правові та регуляторні проблеми, зокрема щодо міжнародного визнання цифрових підписів та дотримання законодавчих вимог [30]. З цієї причини [31] рекомендує поєднувати цифрові підписи з додатковими механізмами безпеки.

Тісно пов'язана з цифровими підписами криптографія з відкритим ключем, яка слугує фундаментальним принципом безпеки сучасних блокчейн-систем. Вона забезпечує безпечний зв'язок у відкритих мережах і гарантує конфіденційну передачу даних та перевірку їх цілісності. Кожен учасник мережі блокчейн має індивідуальну пару криптографічних ключів.

Використовуючи криптографію з відкритим ключем, можна однозначно довести, що транзакцію ініціював законний власник відповідного закритого ключа, без необхідності центрального органу. Водночас, криптографічний захист гарантує, що вміст транзакції не може бути змінений непомітно після її підписання. У поєднанні з криптографічними хеш-функціями цей метод сприяє незмінності та прозорості даних, що зберігаються в блокчейні.

Для безпечної передачі конфіденційної інформації криптографія з відкритим ключем дозволяє використовувати асиметричне шифрування. Відправник шифрує повідомлення відкритим ключем одержувача, щоб лише одержувач міг розшифрувати дані за допомогою свого закритого ключа. Цей метод забезпечує конфіденційність зв'язку навіть у незахищених мережах[32–39].

Роботу криптографії з відкритим ключем можна представити як послідовність чітко визначених кроків, як схематично показано на рисунку 1.2.

Численні наукові роботи досліджують використання цих криптографічних методів у блокчейн-системах. У роботі [40] наведено огляд застосування криптографії з відкритим ключем у технології блокчейн, тоді як у дослідженні [41] аналізуються різні криптографічні схеми з точки зору їхньої ефективності та безпеки. Практичне застосування можна знайти, серед іншого, у роботі [42], де описано використання цих методів в управлінні ланцюгами поставок, а також у

роботах [43, 44], де розглядається її використання в смарт-контрактах та системах обміну даними.

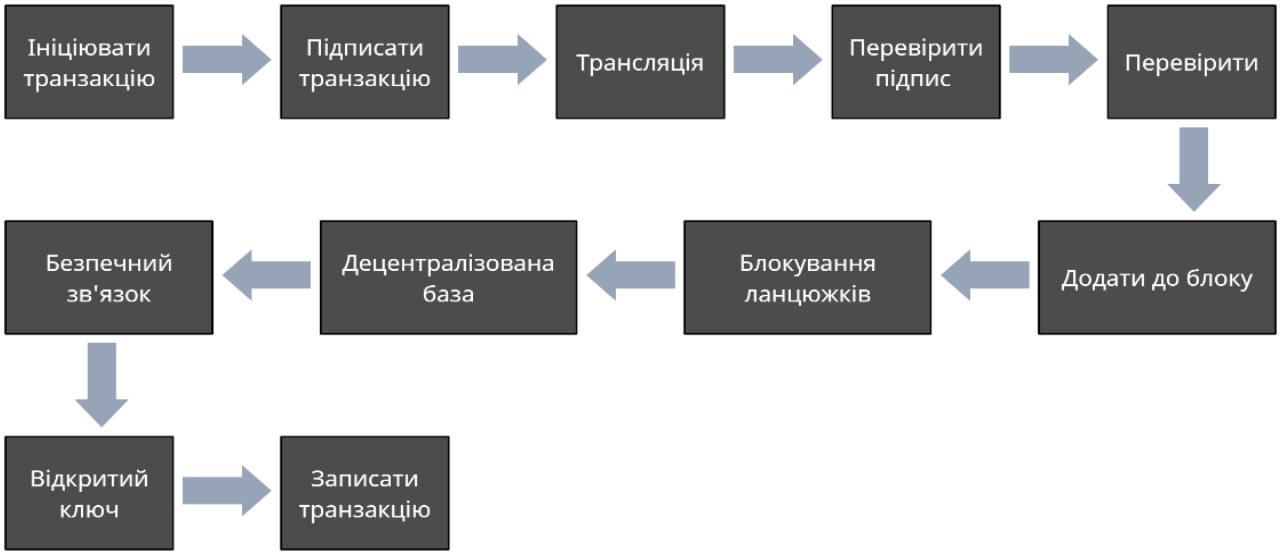

Рисунок 1.2 – Ланцюжок дій, який показує роботу криптографії з відкритим ключем

Аналіз робіт [40–44] показує, що криптографія з відкритим ключем пропонує численні переваги, включаючи високий рівень безпеки, невідмовність від відмови та ефективність завдяки автоматизації процесів. Однак існують також проблеми, зокрема, щодо втрати закритих ключів, залежності від базової криптографічної інфраструктури та потенційних сценаріїв атак. Тому в [45] наголошується на необхідності додаткових заходів безпеки та постійного розвитку криптографічних методів.

Таким чином, цифрові підписи та криптографія з відкритим ключем формують частину фундаментальної бази безпеки технології блокчейн, забезпечуючи захист даних від підміни та несанкціонованого видалення. Завдяки механізмам криптографічної перевірки кожна транзакція є автентичною, а будь-яка спроба її зміни або фальсифікації стає фіксованою всіма учасниками мережі.

Доказ з нульовим знанням – це криптографічний метод, який дозволяє одній стороні (відправнику) довести іншій стороні (контролеру), що він володіє певними даними, не розкриваючи фактичних значень цих даних[46].

Суть цієї концепції полягає в тому, що підтверджується лише достовірність твердження, тоді як зміст основних значень залишається повністю прихованим. Це вирішує фундаментальний конфлікт між контрольованістю та конфіденційністю даних, оскільки довіру можна встановити без розкриття конфіденційної інформації.

Доказ з нульовим розголошенням базується на формальній взаємодії або математично побудованому доказі, в якому контролер переконаний, що той, хто доводить, володіє певними знаннями або що умова виконана, але не отримує додаткового розуміння цих знань. З криптографічної точки зору це означає, що з самого доказу не можна зробити жодних висновків про вхідні дані. Навіть якщо зловмисник спостерігає за всім процесом доказу або аналізує його, він не може витягти з нього жодної корисної інформації[47].

У практичному застосуванні методи доказу з нульовим розголошенням в основному використовуються там, де одночасно існують високі вимоги до безпеки та захисту даних. Наприклад, у технології блокчейн вони дозволяють довести, що транзакція була виконана правильно, без публічного розкриття сум, відправників чи інших конфіденційних деталей. Мережа може перевірити дійсність транзакції без потреби в доступі до конфіденційних даних, що особливо важливо для публічних блокчейнів.

Сучасні методи з нульовим розголошенням, такі як zk-SNARK або zk-STARK, дозволяють доводити та ефективно перевіряти складні обчислення або зміни стану у стиснутому вигляді. Це не тільки підвищує захист та безпеку даних, але й покращує масштабованість розподілених систем. Загалом, методи доказу з нульовим розголошенням є криптографічним інструментом для поєднання довіри, прозорості та конфіденційності в цифрових та децентралізованих системах[48].

У контексті технології блокчейн можна використовувати докази з нульовим знанням, щоб гарантувати захист даних у блокчейні, дозволяючи при цьому перевірку транзакцій[49].

Щоб створити доказ нульового знання, протоколювальник (відправник даних) створює математичний доказ, який демонструє, що він має певні дані, не розкриваючи фактично їх. Доказ з нульовим знанням вимагає складних обчислень, які не всі мережі підтримують.

Одним із прикладів використання доказів нульового знання в технології блокчейн є контекст транзакцій із збереженням конфіденційності, коли вузли (учасники) мережі можуть довести, що вони авторизовані для виконання певної транзакції, не розкриваючи свою особу чи деталі самої транзакції. Це може допомогти захистити конфіденційність користувачів у блокчейні та запобігти потенційному зловживанню даними.

Загалом докази з нульовим знанням є корисним інструментом для захисту транзакцій у блокчейні та для захисту конфіденційності користувачів і все частіше використовуються в системах на основі блокчейну для сприяння довірі та безпечного обміну даними.

У роботі [50] зроблено огляд використання доказів з нульовим знанням у технології блокчейну та сформульовано наслідки цього підходу для безпеки та конфіденційності.

У статті [51] проведено огляд схем доказів з нульовим знанням, які використовуються в системах на основі блокчейну, і зроблено аналіз функцій та продуктивності.

У роботі [52] представлено приклад використання доказів з нульовим знанням в управлінні ланцюгом поставок на основі блокчейну.

Робота [53] містить огляд використання доказів з нульовим знанням у смарт-контрактах на основі блокчейну та досліджень безпеки та конфіденційності, внаслідок використання цього підходу.

У роботі [54] представлено огляд використання доказів з нульовим знанням у системах обміну даними на основі блокчейну та сформульовано наслідки цього підходу для безпеки та конфіденційності таких систем.

Переваги використання доказів із нульовим знанням у технології блокчейн такі:

- безпека: докази з нульовим знанням забезпечують надійний спосіб перевірки автентичності транзакцій у блокчейні, оскільки вони покладаються на криптографічні методи, які важко підробити або змінити[55];
- конфіденційність: підтвердження з нульовою інформацією дозволяють сторонам перевірити справжність транзакції чи повідомлення, не розкриваючи фактичні дані, що передаються[56];
- ефективність: докази з нульовим знанням можуть допомогти автоматизувати процеси, такі як виконання смарт-контрактів, що може зменшити потребу в ручному втручанні та підвищити ефективність[57].

Недоліки використання доказів із нульовим знанням у технології блокчейн включають:

- складність реалізації;
- продуктивність, що залежить від складності доказу та інфраструктури апаратного та програмного забезпечення, що використовується для підтримки блокчейну[58];
- залежність від базової криптографічної системи: безпека та надійність доказів із нульовим знанням залежить від використовуваної базової криптографічної системи, яка може бути піддана вразливостям або слабким місцям, якими можуть скористатися зловмисники[59].

Загалом, хоча докази з нульовим знанням забезпечують ефективний механізм підтвердження коректності та автентичності транзакцій у блокчейні без розкриття їх змісту, їх застосування потребує ретельного аналізу з точки зору захисту від підміни та несанкціонованого видалення даних. Незважаючи на високий рівень криптографічної стійкості, помилки реалізації або некоректна інтеграція таких протоколів можуть створювати потенційні вразливості, які здатні вплинути на цілісність системи[60].

1.3. Дослідження надійності блокчейн-систем на рівні вузлів

Вузли блокчейну є невід'ємними компонентами децентралізованих мереж, кожен з яких відіграє певну роль у підтримці цілісності, безпеки та функціональності системи[61]. Вузлами виступають безпосередньо учасники мережі. У науковій літературі досліджувалися різні аспекти вузлів блокчейну, включаючи їхню архітектуру, механізми консенсусу та застосування.

Вузол блокчейну – це пристрій або програма, яка бере участь у мережі блокчейн. Ключова роль вузлів у блокчейн-системі полягає у підтримці функціонування мережі. Вони зберігають копію ланцюга блоків, синхронізують дані з іншими вузлами і виконують перевірку транзакцій. Залежно від своїх функцій вузли можуть бути повними (full nodes), які зберігають повну копію блокчейну, або звичайними, простими (light nodes), які зберігають лише дані про новий блок і покладаються на інші вузли для повної інформації. Вузли відіграють ключову роль у досягненні консенсусу в мережах блокчейну. Механізми консенсусу забезпечують, щоб усі вузли підтверджували твердження дійсності щодо поточного стану блокчейну. Частіше всього вузли досягають консенсусу через угоду більшості, допускаючи певну кількість несправних вузлів[62].

Окрім перевірки транзакцій, вузли виконують критично важливу функцію забезпечення цілісності даних і захисту від їх підміни або несанкціонованого видалення. Децентралізована архітектура блокчейну у поєднанні з криптографічними механізмами – зокрема хешуванням і цифровими підписами, створює багаторівневий бар’єр проти атак на дані[63].

Крім того в класичній реалізації блокчейн-мережі, копії реєстру зберігаються на великій кількості вузлів, тому навіть у випадку одноосібної спроби видалення або пошкодження даних на окремих вузлах, вони можуть бути відновлені шляхом синхронізації з іншими учасниками мережі. Це робить атаки типу «видалення даних» або їх локальної модифікації практично неефективними без досягнення консенсусу більшості вузлів[64].

У контексті механізмів консенсусу, в системах PoS вузли повинні підтверджувати свою доброчесність через наявність частки (токенів), що підвищує економічну відповідальність за спроби підміни або знищення даних – у разі порушення правил вони ризикують втратити свої активи (механізм штрафів). Водночас це може призводити до певної концентрації впливу та централізації в управлінні мережею[65]. У системах PoW всі вузли формально рівні з точки зору участі в консенсусі, однак захист від підміни або видалення даних досягається за рахунок значних обчислювальних витрат: для зміни історії транзакцій необхідно перевиконати обчислення більшості мережі, що є складною задачею[66].

Наукові роботи[67–72] мають інформацію про те, як структуровані вузли, як вони взаємодіють і як досягається консенсус на різних платформах блокчейну.

Дослідження [68] пропонує фундаментальний огляд архітектури основних систем блокчейну, включаючи Bitcoin, Ethereum, Hyperledger Fabric та IOTA. Аналізуючи ці платформи, автори пояснюють, як зберігаються дані, як перевіряються транзакції та як різні механізми консенсусу впливають на продуктивність та безпеку. Їхня робота виділяється тим, що синтезує великий обсяг фрагментованого технічного матеріалу в чітке та доступне порівняння, допомагаючи дослідникам і розробникам зрозуміти ключові відмінності та варіанти проектування в різних реалізаціях блокчейну.

Спираючись на це фундаментальне розуміння, науковець Омер у своїй статті [69] досліджує, як гібридний підхід до блокчейну, що поєднує аспекти як публічних, так і приватних систем, може вирішити практичні проблеми масштабованості та управління. Він описує системну архітектуру, яка замінює традиційну однорангову мережу системою обміну повідомленнями на основі Apache Kafka та використовує контейнерну технологію для ізоляції вузлів для кращого управління ресурсами. Apache Kafka – високопродуктивна розподілена платформа потокової обробки подій, яка використовується для обробки великих обсягів даних у реальному часі і часто застосовується разом з блокчейн-проектами для забезпечення масштабованості, надійності та обробки потоків подій, пропонуючи функції, такі як незмінний журнал і високу доступність. Результати

моделювання є багатообіцяючими, показуючи, що ця модель може обробляти понад 1000 транзакцій за секунду навіть на пристроях з обмеженою обчислювальною потужністю. Ця робота особливо актуальна для розробки блокчейнів, які є одночасно швидкими та стійкими в реальних умовах[69].

Ще один важливий внесок зроблено Ханом та Салахом [70], які представляють ретельний огляд різних консенсусних протоколів, що дозволяють вузлам блокчейну узгоджувати стан мережі. Ці протоколи, включаючи PoW, PoS та Byzantine Fault Tolerance, мають свої сильні сторони та обмеження. Ця стаття допомагає уточнити, де і коли використовувати кожен з них, що особливо важливо для застосувань в Інтернеті речей, де пристрої часто мають дуже обмежені ресурси.

Дослідники Кім та Лі [71] пропонують класифікацію консенсусних алгоритмів, яка показує, як вони розвивалися з часом. Використовуючи еволюційний підхід, вони простежують розвиток консенсусу від ранніх відмовостійких систем до сучасних, масштабованих блокчейн-рішень. Ця класифікація допомагає не лише зрозуміти сучасні технології, але й передбачити майбутній розвиток у дизайні блокчейну.

Вкінці, науковці Чжан та Ван [72] пов'язують технологію блокчейн з периферійними обчисленнями, галуззю, де пристрої обробляють дані поблизу місця їх генерації, а не покладаються на централізовані сервери. Їхня робота зосереджена на потребах Індустрії 5.0, яка наголошує на співпраці людини та машини та інтелектуальній автоматизації. Автори показують, як вузли блокчейну можуть ефективно функціонувати в цих умовах, забезпечуючи безпечне прийняття рішень у режимі реального часу в таких додатках, як розумні фабрики, охорона здоров'я та логістика.

Разом ці п'ять досліджень представляють одні з найактуальніших та найвпливовіших досліджень, що до вузлів блокчейну, що охоплюють як теоретичні основи, так і практичні інновації. Вони показують, як блокчейн розвивається, щоб відповідати вимогам швидкості, масштабованості, децентралізації та інтеграції з іншими технологіями.

1.4. Систематизація та узагальнення методів забезпечення надійності блокчейн-систем

Порівняння традиційних і гібридних підходів показало, що поєднання елементів публічних і приватних блокчейнів, а також використання сучасних інструментів обміну повідомленнями та контейнеризації, дозволяє суттєво підвищити масштабованість системи. Такі архітектурні рішення забезпечують високу пропускну здатність навіть за обмежених обчислювальних ресурсів, що є важливим для практичних застосувань.

Крім того, порівняльний аналіз консенсусних протоколів виявив, що різні алгоритми мають свої переваги залежно від умов експлуатації, особливо в середовищах з обмеженими ресурсами та в системах реального часу. Інтеграція блокчейну з периферійними обчисленнями підтвердила його перспективність для задач Індустрії 5.0, де потрібні безпечні та швидкі механізми прийняття рішень.

У даному дослідженні було проведено комплексний аналіз методів захисту інформації від підміни та видалення, заснований на використанні технології блокчейн. Головною метою аналізу було виявлення основних переваг і недоліків вже відомих методів, а також визначення обмежень їх використання для конкретних завдань у сфері кібербезпеки.

Результати аналізу описаних робіт:

Оцінка ефективності технології блокчейн для забезпечення цілісності даних. В рамках дослідження була проведена оцінка можливостей технології блокчейн у забезпеченні непорушності даних.

Використані дані для графіків були зібрані шляхом проведення експериментів з різними методами захисту даних у контексті технології блокчейн. Кожен метод був протестований на загальнодоступних відомостях з ресурсу Kaggle з використанням спеціально розробленого тестового середовища.

Рисунок 1.3 – Швидкість обробки даних для різних методів захисту

Рисунок 1.4 – Час виявлення підміни для різних методів захисту

Джерела і експерименти:

Методи хешування: Швидкість обробки даних була виміряна за допомогою стандартних функцій хешування, таких як SHA-256 та SHA-512. Експерименти проводилися на відомих тестових наборах даних.

Методи роботи з цифровими підписами: Для цього експерименту використовувалися різні алгоритми цифрового підпису, такі як RSA та ECDSA. Час обробки був виміряний при створенні та перевірці підписів на випадкових повідомленнях.

Методи криптографії з відкритим ключем: Для цього експерименту були використані алгоритми шифрування з відкритим ключем, такі як RSA та ECC. Час шифрування та дешифрування був виміряний для різних розмірів повідомлень.

Методи доказу з нульовим знанням: У цьому експерименті були застосовані різні протоколи доказу з нульовим знанням, такі як zk-SNARKs. Час генерації доказів та перевірки був виміряний для різних об'ємів вхідних даних.

Результати експериментів були оброблені та проаналізовані для формування відповідних даних, які використовуються у таблицях.

Графік 1.3 демонструє порівняльний аналіз швидкості обробки даних для трьох різних методів захисту: методу хешування, цифрових підписів та доказу з нульовим знанням. Як видно з графіка, метод доказу з нульовим знанням демонструє найвищу швидкість обробки даних, тоді як метод цифрових підписів має найбільші обчислювальні витрати.

Графік 1.4 відображає час, який потрібен для виявлення підміни даних у блокчейні з використанням різних методів захисту. Метод хешування показує найшвидші результати виявлення підміни, в той час як методи цифрових підписів та доказу з нульовим знанням вимагають більше часу для перевірки цілісності даних.

В результаті аналізу було виявлено, що методи захисту інформації на основі технології блокчейн виявляються ефективними у боротьбі з підміною та видаленням даних. Використання хеш-сум, цифрових підписів та методів доказу з нульовим знанням може значно підвищити рівень безпеки інформації в блокчейні.

Однак, варто враховувати, що такі методи можуть мати обмеження у швидкості обробки даних та масштабованості, що може ускладнювати їх використання для великих обсягів інформації[59–68].

На підставі аналізу публікацій можна зробити висновок, що технологія блокчейн має значний потенціал. Дослідження, що пов’язані з реалізацією та використанням технології блокчейн, є актуальними.

Для захисту даних у блокчейні застосовується комплекс криптографічних методів, зокрема хешування, цифрові підписи, криптографія з відкритим ключем та докази з нульовим знанням. Їх поєднання спрямоване насамперед на забезпечення цілісності, автентичності та стійкості даних до підміни або несанкціонованого видалення.

Можна зробити висновок:

1. Методи хешування формують основу незмінності блокчейну: кожен блок містить хеш попереднього, що створює ланцюгову залежність між записами. Будь-яка спроба змінити або видалити дані призводить до зміни хешу, що автоматично порушує цілісність усього ланцюга та виявляється іншими вузлами мережі.

2. Цифрові підписи та криптографія з відкритим ключем забезпечують автентичність і захист від підробки транзакцій. Дані підписуються приватним ключем, і будь-яке їх модифікування або часткове видалення призводить до втрати валідності підпису. Це унеможливлює приховану зміну змісту транзакцій без відповідного виявлення мережею.

3. Докази з нульовим знанням додатково підсилюють захист, дозволяючи підтверджувати коректність операцій без розкриття самих даних. Важливим аспектом є також реплікація даних між вузлами мережі: навіть у разі спроби видалення або пошкодження інформації на окремих вузлах, вона відновлюється шляхом синхронізації з іншими копіями реєстру. Це створює додатковий рівень захисту від атак, спрямованих на знищення або часткову втрату даних.

Разом з тим, ефективність і продуктивність реалізації цих методів значною мірою залежать від обраного програмного та апаратного забезпечення, а також від

архітектури конкретної блокчейн-системи. Крім того, кожен із зазначених підходів має власні специфічні вразливості до кібератак (наприклад, атаки на реалізацію алгоритмів, компрометація ключів або побічні канали), що потребує комплексного підходу до проектування систем захисту з урахуванням потенційних загроз підміни, спотворення або видалення даних.

1.5. Аналіз актуальних загроз безпеці блокчейн-систем

Атаки на блокчейн-системи є загрозами для їх безпеки та стійкості, оскільки вони підривають довіру, децентралізацію та консенсус, які є основою цієї технології. Однією з найвідоміших проблем є атака 51%, при якій зловмисник, який володіє більш ніж половиною обчислювальних потужностей мережі в системах PoW, може переписувати блоки та історію транзакцій. Прикладами є атака на Ethereum Classic, яка спричинила крадіжку коштів у розмірі мільйона доларів і завдала шкоди репутації мережі та випадок з Bitcoin Gold, де атака 51% дозволила зловмисникам вкрасти кошти на суму понад 18 мільйонів доларів[73].

Не менш небезпечна і сибіл-атака, яка передбачає створення безлічі підроблених вузлів для отримання непропорційного впливу на мережу і несанкціонованого додавання і зміни даних. Подібні атаки особливо критичні для блокчейнів, де консенсус залежить від голосування чи репутації вузлів. Наприклад, у системах Delegated PoS зловмисник може маніпулювати виборами валідаторів, створюючи загрозу централізації та консенсусу. Результатом таких атак стає втрата контролю над системою та вразливість мережі перед зміною інформації і підробкою нової[74].

Атаки на консенсус також демонструють значний ризик. Вони включають маніпуляції процесом додавання блоків або впливу на валідаторів. У деяких системах зловмисники можуть вступати в змову для контролю мережі, як це було у блокчейні EOS. Ці дії підривають прозорість та рівноправність учасників, що у свою чергу ставить під сумнів децентралізованість мережі[75].

Крім цього, існують більш тонкі атаки, такі як eclipse-атака, при якій вузол блокчейна ізолюється і отримує неправдиву інформацію про блоки та транзакції. Це дозволяє зловмисникам маніпулювати роботою вузла та порушувати консенсус.

Зрештою, всі ці загрози демонструють важливість розробки стійких механізмів захисту блокчейнів. Системи, де вузли перевіряють лише випадково вибрані блоки або розподіляють обчислювальні завдання за випадковим принципом, можуть значно підвищити стійкість мережі до даних атак. Такий підхід перешкоджає концентрації контролю в руках одного гравця та знижує ймовірність маніпуляцій чи ізоляції вузлів. Таким чином, блокчейн-системи потребують постійного вдосконалення архітектури для збереження балансу між децентралізацією, безпекою та продуктивністю[76].

Концепція, коли для перевірки нових блоків випадково чи по заданому принципу обираються вузли, вже використовується в деяких сучасних блокчейн-проектах, хоча реалізується у різних варіаціях. Наприклад, у блокчейнах, які працюють на алгоритмах консенсусу PoS або його різновидах, вузли-валідатори обираються по рівнях з урахуванням їх матеріального внеску в мережу. У таких системах, як Ethereum 2.0, Tezos або Cardano, для створення та перевірки блоків використовується принцип вибору, який базується на кількості монет, внесених у систему власником вузла.

Ethereum перейшов на алгоритм PoS з оновленням The Merge, що завершилось 15 вересня 2022 р., суттєво знизивши енергоспоживання (~на 99 %). Для участі у мережі необхідно придбати 32 ETH. Вибір контролера для пропозиції блоку відбувається пропорційно обсягу вкладених коштів[77]. Це може створити ситуацію коли кілька груп валідаторів можуть координувати дії чи стати об'єктом тиску з боку засновників мережі. Додатковим слабким місцем є вразливість до атаки довгострокової реорганізації ланцюга, якщо старі валідатори розпродують ключі зловмиснику.

Проект Cardano використовує серію доказово безпечних PoS-протоколів Ouroboros, розроблених академічною групою під керівництвом Аггелос Кіайас (Университет Единбургу)[78]. Cardano з протоколом Ouroboros позиціонується як

найбільш формалізоване та математично обґрунтоване рішення PoS. Проте теоретична бездоганність приховує низку практичних слабкостей. По-перше, протокол складний у реалізації та потребує ідеальної роботи алгоритму криптографічної випадковості для вибору учасників мережі, який не реалізований практично. Будь-які вразливості у генерації випадкових чисел потенційно можуть використовуватися для передбачення чи заміни обраних учасників. По-друге, Cardano страждає від того самого ризику централізації вузлів, що й Ethereum: незважаючи на велику кількість наборів вузлів, частка участі розподілена нерівномірно. Крім того, в умовах низької активності учасників децентралізація мережі виявляється швидше декларативною, ніж фактичною. У реальній атаці достатньо контролювати кілька великих наборів вузлів, щоб вплинути на порядок блоків.

Tezos – блокчейн з консенсусом Liquid PoS, розроблений Артуром і Кетлін Брейтман. Валідатори обираються за допомогою псевдовипадкового PRNG на основі значення заплачених монет, збереженого в блокчейні, тобто результати детерміновані, але непередбачувані завчасно[79]. Tezos використовує механізм Liquid PoS, який дозволяє користувачам делегувати свої права у мережі іншим учасникам мережі без втрати власності на токени(монети), що заборонено у інших механізмах. Це означає, що власник токенів передає іншому учаснику право виконувати дії вузла від його імені у процесі управління мережею, але при цьому сам залишається власником токенів і може їх використовувати або забрати назад у будь-який момент. Такий підхід значно спрощує участь у мережевому управлінні, оскільки не всі користувачі мають технічну можливість або бажання безпосередньо приймати учать у роботі мережі.

Водночас виникає структурна проблема: делегування фактично концентрує вузли у невеликій групі операторів, що знижує рівень децентралізації та підвищує ризик координації між ними для власної вигоди.

Хоча мережа передбачає штрафи за порушення правил, наприклад за одночасне створення двох блоків (атака «подвійного блокування»), оператори з великою кількістю делегованих токенів можуть проводити цензуру транзакцій або

маніпулювати перевірками. Таким чином, система залишається вразливою до концентрації впливу через делегування та соціальний тиск на основних учасників.

Інший підхід застосовується у алгоритмі Pure PoS, який реалізований у блокчейні Algorand. У цій моделі вузли, що беруть участь у валідації транзакцій та створенні нових блоків, обираються випадковим чином, але ймовірність вибору вузла прямо пропорційна обсягу його участі (кількості токенів).

Pure PoS був запропонований Сільвіо Мікалі, науковцем з MIT і впроваджений у Algorand, який стартував у 2019 році. Головна особливість алгоритму – секретний самовибір учасників консенсусу. Кожен вузол локально запускає Verifiable Random Function, яка визначає, чи буде вузол автором нового блоку або прийме участь у верифікації. Ймовірність вибору пропорційна стейку вузла[80].

Після цього вузол створює доказ вибору (proof), який може перевірити будь-який інший учасник мережі. При цьому особистість обраного вузла стає відомою лише під час поширення повідомлення про блок, що захищає мережу від атак типу DDoS. Завдяки цьому забезпечується ще більш рівномірний розподіл навантаження на мережу, а також зменшуються витрати часу на досягнення консенсусу[80]. Однак ключова вада тут – залежність від активності учасників. Насправді лише небагато користувачів підтримують вузли, лише купують місце у мережі за токени та делегують участь валідації спеціалізованим структурам. Це руйнує ідею повної децентралізації та призводить до концентрації управління мережею колом людей. Ще однією вразливістю є так звана проблема «послаблення безпеки»: при надто низькій кількості активних учасників ймовірність атак усередині невеликих груп зростає.

Системи з шардінгом, такі як Zilliqa, також використовують механізм випадкового вибору вузлів для перевірки окремих сегментів ланцюжка. У шардінгових системах блокчейн розділений на "шарди" – невеликі незалежні частини, кожна з яких перевіряється окремою групою вузлів. Це дозволяє суттєво підвищити масштабованість мережі, адже кожен вузол відповідає лише за частину даних, а не за весь блокчейн. Теоретично така архітектура дає масштабованість та

енергоефективність, але її складність – це водночас і головний мінус. Система шардингу вразлива до атак на малі шарди: якщо зловмисник контролює більше третини вузлів у конкретному шарді, він може порушити його роботу, підмінити дані чи додати не перевірені дані. Це особливо небезпечно в періоди, коли загальна кількість учасників невелика і деякі шарди виявляються занадто малими[81].

З метою узагальнення особливостей сучасних механізмів консенсусу та оцінки їх впливу на безпеку й надійність блокчейн-систем було проведено порівняльний аналіз найбільш поширених блокчейн-мереж. Для порівняння було обрано такі критерії: тип механізму консенсусу, що визначає принцип підтвердження транзакцій; сильні сторони, які характеризують рівень безпеки, децентралізації та ефективності роботи мережі; основні недоліки, пов’язані з обмеженнями масштабованості, енергоспоживання або участі користувачів; а також вразливості до атак, що відображають потенційні ризики порушення цілісності та стабільності мережі. Такий підхід дозволяє комплексно оцінити переваги й недоліки кожного рішення.

У тексті наведена таблиця 1.1, що дозволяє наочно порівняти особливості Ethereum 2.0, Tezos, Cardano, Algorand і Zilliqa та оцінити ризики й переваги кожної системи.

Таблиця демонструє порівняння п’яти популярних блокчейн-мереж за ключовими параметрами їх механізмів консенсусу.

1. Тип консенсусу – алгоритм, який забезпечує підтвердження транзакцій і створення блоків у мережі.

2. Сильні сторони – основні переваги та технічні переваги кожного механізму консенсусу, що підвищують безпеку та ефективність мережі.

3. Основні недоліки – обмеження та складнощі, пов’язані з участю користувачів, енергоспоживанням або централізацією.

4. Вразливості до атак – потенційні загрози, на які мережа може бути схильна через концентрацію впливу, технічні особливості алгоритму або людський фактор.

Таблиця 1.1 – Порівняльна характеристика блокчейн-мереж за механізмом консенсусу

Мережа	Консенсус	Сильні сторони	Основні недоліки	Вразливості до атак
Ethereum 2.0	PoS	Математична безпека, механізми розподілу, фіналізація блоків	Високий бар'єр входу (вартість 32 ETH), концентрація у стейкінг-пулах, складність для звичайних користувачів	Long-range атака при продажі ключів, централізація пулів може імітувати 51%-атаку
Tezos	PoS	Доступність для делегування, низький поріг участі	Централізація у операторів, залежність учасників від довіри до валідатора	Маніпуляції під час валідації, продаж делегації вузла, цензура транзакцій
Cardano	Ouroboros PoS	Формально доведена безпека, низьке енергоспожи-вання	Складність протоколу, залежність від випадковості, нерівномірний розподіл участі	Захоплення кількох великих наборів вузлів може вплинути на мережу, атаки при слабкій генерації випадковості
Algorand	Pure PoS	Анонімний вибір валідаторів, швидке підтвердження, висока теоретична децентралізація	Низька активність користувачів, залежність від активності мережі	При низькій активності можливо зниження стійкості до довгострокових атак
Zilliqa	Гібрид (шардинг)	Масштабова-ність, висока пропускна здатність, стійкість до класичної 51%-атаки	Складність реалізації, енергоспоживан ня, ризик слабких шард	Захоплення >1/3 вузлів у шарді, атаки на малі шарди при низькій диверсифікації

Наведене порівняння демонструє, що жоден із механізмів консенсусу не є універсальним рішенням, оскільки кожен із них передбачає компроміси між безпекою, децентралізацією та масштабованістю, зокрема у контексті захисту від несанкціонованої зміни та видалення даних. Мережі на основі PoS і його модифікацій знижують енергетичні витрати порівняно з PoW, однак концентрація частки у окремих учасників може створювати ризики узгодженого впливу, що теоретично відкриває можливості для переписування історії транзакцій або вибіркового виключення (видалення) певних записів із ланцюга.

У системах PoW захист від зміни або видалення даних досягається за рахунок необхідності повторного обчислення значної кількості блоків: будь-яка спроба модифікації навіть одного блоку потребує перебудови всього наступного ланцюга з перевищенням обчислювальної потужності більшості мережі. Це робить атаки, спрямовані на зміну або видалення інформації, складно реалізованими в умовах великих децентралізованих мереж. Використання шардінгу, хоча й підвищує масштабованість, створює додаткові ризики саме в аспекті цілісності даних. Окремі шарди можуть стати ціллю атак, спрямованих на локальну зміну або видалення даних без негайного виявлення глобальною мережею.

Таким чином, вибір механізму консенсусу має враховувати його здатність протидіяти не лише підробці, а й сценаріям часткового або повного видалення даних, а також атакам на переписування історії транзакцій. Забезпечення незмінності реєстру є ключовою вимогою для будь-якої блокчейн-системи.

Висновок до розділу 1

1. У межах даного дослідження було здійснено комплексний аналіз технології блокчейн з точки зору забезпечення надійності, безпеки та стійкості до загроз у сучасних децентралізованих системах. Основну увагу приділено криптографічним методам захисту даних, архітектурі вузлів, механізмам досягнення консенсусу та актуальним вразливостям, що виникають у процесі

практичної реалізації блокчейн-платформ. Проведене дослідження ґрунтується на узагальненні результатів сучасних наукових публікацій і дозволяє сформувати цілісне уявлення про сильні та слабкі сторони блокчейн-технологій.

2. Аналіз показав, що криптографічні методи є фундаментальною складовою забезпечення надійності блокчейн-систем. Методи хешування відіграють ключову роль у гарантуванні цілісності та незмінності даних, оскільки формують криптографічний зв’язок між блоками та унеможливлюють приховану модифікацію історії транзакцій. Використання сучасних хеш-функцій забезпечує високий рівень стійкості до колізій та атак на цілісність даних, що є критично важливим для функціонування децентралізованих реєстрів.

3. Цифрові підписи та криптографія з відкритим ключем забезпечують автентичність, невідмовність та контроль доступу в блокчейн-системах. Застосування цифрових підписів дозволяє однозначно ідентифікувати ініціаторів транзакцій та гарантує юридичну значущість операцій, що відкриває можливості використання блокчейну у фінансових системах, управлінні ланцюгами постачання, цифровій ідентичності та смарт-контрактах. Водночас дослідження підтверджують, що вибір конкретних криптографічних схем має суттєвий вплив на продуктивність системи та потребує врахування компромісу між рівнем безпеки й обчислювальними витратами.

4. Методи доказу з нульовим знанням розглянуто як перспективний напрям розвитку блокчейн-технологій, орієнтований на підвищення рівня конфіденційності без розкриття чутливих даних. Застосування таких методів дозволяє підтверджувати коректність транзакцій або виконання умов без розкриття їхнього змісту, що є особливо актуальним для систем з підвищеними вимогами до приватності. Разом з тим, встановлено, що складність реалізації та значні обчислювальні витрати обмежують їх широке впровадження, особливо у масштабних публічних мережах.

5. Важливим аспектом дослідження є аналіз архітектури вузлів блокчейн-мереж та механізмів досягнення консенсусу. Порівняльний аналіз механізмів PoW, PoS та його модифікацій (Delegated PoS, Pure PoS), а також гібридних підходів із

використанням шардінгу засвідчив, що кожен з них має власні переваги й обмеження. Механізми PoW демонструють високу стійкість до атак за рахунок значних обчислювальних витрат, однак характеризуються низькою енергоефективністю. Натомість PoS та його похідні дозволяють суттєво знизити енергоспоживання, але створюють ризики концентрації впливу та зниження фактичної децентралізації.

6. Результати порівняльного аналізу реальних блокчейн-мереж свідчать, що впровадження нових механізмів консенсусу та архітектурних рішень не усуває повністю проблем безпеки, а лише змінює їх характер. Зокрема, системи з делегуванням повноважень спрощують участь користувачів у мережі, проте водночас сприяють концентрації валідаторів і підвищують ризик змов або цензури транзакцій. Шардінг значно покращує масштабованість, але створює додаткові вектори атак, пов’язані з контролем окремих сегментів мережі.

7. Також проаналізовано основні типи загроз і атак на блокчейн-системи, зокрема атаки 51%, сибіл-атаки, атаки на механізми консенсусу та координаційні змови валідаторів. Наведені приклади реальних інцидентів підтверджують, що навіть криптографічно захищені системи залишаються вразливими до економічних і соціальних факторів. Це підкреслює необхідність комплексного підходу до безпеки, який поєднує технічні, організаційні та економічні механізми захисту.

Отримані результати дозволяють зробити висновок, що надійність блокчейн-систем формується не лише завдяки використанню окремих криптографічних алгоритмів, а є результатом взаємодії кількох рівнів: криптографічного захисту, архітектури мережі, механізмів консенсусу та поведінки учасників. Підвищення безпеки на одному рівні можу супроводжуватися зниженням ефективності або масштабованості на іншому, що обумовлює необхідність пошуку збалансованих рішень.

Таким чином, результати дослідження підтверджують, що технологія блокчейн має значний потенціал для створення надійних і захищених систем зберігання та обміну даними, однак її ефективне використання вимагає ретельного вибору технічних рішень з урахуванням конкретних умов застосування.

2. МОДЕЛЮВАННЯ ТА ОБҐРУНТУВАННЯ АЛГОРИТМУ РАНДОМІЗОВАНОЇ ВАЛІДАЦІЇ БЛОКІВ І ТРАНЗАКЦІЙ У БЛОКЧЕЙН-СИСТЕМАХ

У сучасних блокчейн-системах забезпечення цілісності даних є однією з ключових науково-прикладних проблем, що безпосередньо впливає на надійність та безпеку функціонування розподілених реєстрів. Особливого значення набуває захист від підміни та несанкціонованого видалення даних, які можуть реалізовуватися як унаслідок зовнішніх атак, так і через узгоджені дії частини учасників мережі, що володіють значними обчислювальними або консенсусними ресурсами.

Під захистом від підміни та несанкціонованого видалення даних доцільно розуміти забезпечення таких умов функціонування блокчейн-системи, за яких будь-яка спроба модифікації вже підтверджених транзакцій або виключення блоків із ланцюга є або обчислювально нездійсненною, або гарантовано виявляється у процесі верифікації. При цьому під підміною даних розуміється несанкціонована зміна інформації, що була включена до блоку та підтверджена мережею, з метою спотворення історії транзакцій або отримання неправомірної вигоди. Несанкціоноване видалення полягає у виключенні транзакцій або блоків із реєстру, що призводить до порушення узгодженості стану системи та втрати інформаційної цілісності.

У децентралізованих середовищах зазначені загрози ускладнюються можливістю їх реалізації через координацію дій групи учасників або частковий контроль над процесами консенсусу. У зв’язку з цим забезпечення захисту не може обмежуватися виключно використанням криптографічних механізмів, а потребує організації процесів верифікації таким чином, щоб виключити можливість впливу окремих вузлів або їх обмежених груп на результати перевірки. Це досягається шляхом впровадження механізмів випадкового та незалежного контролю, що забезпечують розподілену перевірку даних і підвищують ймовірність виявлення будь-яких несанкціонованих змін[82].

2.1. Розробка методу випадкового вибору учасників і контрольних точок

Розроблений метод випадкового вибору учасників і контрольних точок ґрунтується на використанні ймовірнісних підходів для забезпечення непередбачуваності процесів валідації. Основною метою його застосування є мінімізація ризиків підміни транзакцій, модифікації блоків та їх несанкціонованого видалення.

Ключовими принципами методу є такі:

1. Випадковий вибір учасників та об’єктів перевірки унеможливлює прогнозування складу валідаторів, що суттєво знижує ймовірність цілеспрямованого впливу на процес підтвердження даних. Це виключає можливість формування контрольованих груп вузлів, здатних здійснювати маніпуляції з даними. Реалізація такого підходу базується на використанні криптографічно стійких генераторів випадкових чисел та хеш-функцій.

2. Забезпечення рівномірності вибору учасників і блоків запобігає концентрації контролю в межах обмеженої групи вузлів. Це, у свою чергу, унеможливлює реалізацію атак, пов’язаних із цензурою транзакцій, їх модифікацією або видаленням, і сприяє підтриманню децентралізованого характеру системи.

Криптографічною основою запропонованого методу є використання алгоритмів на основі еліптичних кривих, що забезпечують високий рівень криптостійкості при відносно низьких обчислювальних витратах. Безпека таких алгоритмів базується на складності задачі дискретного логарифмування на еліптичних кривих, що робить практично неможливим відновлення секретних параметрів або компрометацію процесів генерації випадкових значень.

Використання еліптичних кривих дозволяє досягти еквівалентного рівня безпеки порівняно з класичними криптографічними алгоритмами при значно меншому розмірі ключів. Зокрема, 256-бітний ключ у системах на основі еліптичних кривих забезпечує рівень захисту, співставний із 3072-бітними

ключами у традиційних схемах. Це зумовлює зменшення обчислювальних витрат і робить такі алгоритми придатними для використання в ресурсно обмежених середовищах[83].

З урахуванням перспектив розвитку обчислювальних технологій, можна припустити, що вже у найближчому майбутньому можуть з'явитися нові покоління комп'ютерів, здатних виконувати обчислення з набагато вищою швидкістю та ефективністю, ніж сучасні системи. У зв'язку з цим використання лише одного рівня захисту не може гарантувати абсолютної безпеки інформації. Саме тому в межах цієї роботи особлива увага приділяється квантовому генератору, який розглядається як важливий елемент системи безпеки. Його застосування дозволяє формувати недетерміновані послідовності, що не можуть бути відтворені або передбачені навіть за наявності значних обчислювальних ресурсів.

Запропонований підхід також узгоджується з положеннями теорії ігор та використовується в межах консенсусних алгоритмів типу PoS, де вибір учасників із групи учасників є критичним фактором забезпечення справедливості та стійкості системи. Використання ймовірнісного вибору знижує ризик змови між учасниками та ускладнює реалізацію атак, пов'язаних із захопленням контролю над мережею.

Додатковою перевагою методу є підвищення обчислювальної ефективності за рахунок використання випадкових контрольних точок. Перевірка лише вибіркових блоків ланцюга дозволяє суттєво зменшити обсяг обчислень без зниження рівня безпеки. Це є особливо актуальним для великих блокчейн-мереж, де розмір реєстру постійно зростає.

Таким чином, метод випадкового вибору учасників і контрольних точок, що поєднує криптографічні механізми, ймовірнісні підходи та принципи теорії ігор, забезпечує підвищення рівня захисту даних, сприяє децентралізації системи та дозволяє досягти балансу між безпекою і обчислювальною ефективністю. Це робить його перспективним для застосування у сучасних та майбутніх блокчейн-інфраструктурах. Метод випадкового вибору учасників і контрольних точок ґрунтується на теоретичних засадах, які включають теорію ймовірностей, криптографію, теорію ігор і консенсусні алгоритми. Випадковість, забезпечена

криптографічними механізмами, знижує ризики атак і змов, підвищуючи децентралізацію та обчислювальну ефективність системи. Це робить блокчейн-системи більш стійкими до зовнішніх загроз і сприяє їхньому надійному функціонуванню.

Реалізация методу.

Етап 1: Визначення математичної основи системи.

Створення випадкової функції на основі алгоритмів еліптичних кривих.

В основі функції лежить математична еліптична крива, задана рівнянням вигляду:

$$y^2 = x^3 + a \times x + b,$$

де a і b – це коефіцієнти, що визначають форму кривої, а x і y – координати точок на кривій.

Етап 2: Визначення базових криптографічних елементів.

Задається базова точка G – це заздалегідь визначена точка на еліптичній кривій, яка є загальновідомою.

Генерація приватного та публічного ключів:

$$pk = sk \times G,$$

Де приватний ключ (*sk*) – це випадкове число яке є секретним і згенерований за допомогою QRNG; публічний ключ (*pk*) – це точка на еліптичній кривій, яка обчислюється як множення базової точки G на приватний ключ. Базова точка G – це заздалегідь визначена точка на еліптичній кривій, яка є загальновідомою. Точки перетину зображені на графіку 2.1.

Етап 3: Визначення множин системи.

Позначаємо множину учасників мережі через $U = U_1, U_2, \dots, U_n$, де n – кількість учасників.

Нехай $C = C_1, C_2, \dots, C_m$ – множина блоків у блокчейні, де m – кількість блоків у ланцюзі.

Етап 3: Хешування вхідних даних та генерація випадкового значення

Для кожної операції задається вхід: x. Наприклад: дані транзакції.

Для генерації випадкового значення на основі вхідного параметра x використовується приватний ключ:

$$r = sk \times H(x),$$

де $H(x)$ – це хеш від вхідного параметра x, а r – псевдовипадкове значення. Це значення є випадковим у контексті того, що його неможливо передбачити без знання приватного ключа.

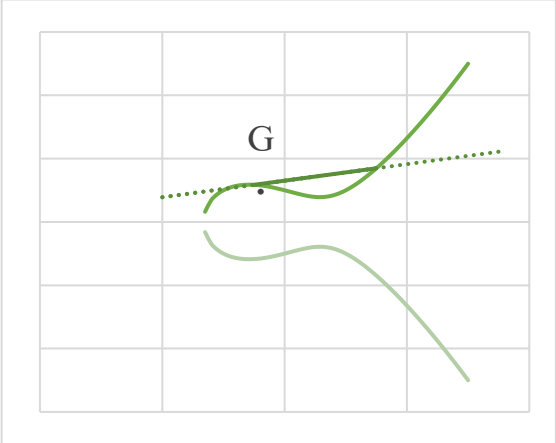

Рисунок 2.1 – Точки перетину з графіком функції еліптичної кривої

Етап 4: Формування доказу правильності.

Для забезпечення публічної перевірки формується доказ:

$$proof = H(x) \times pk.$$

Це значення можна перевірити, знаючи публічний ключ і вхідний параметр x. Інші учасники можуть переконатися, що r дійсно було згенеровано з використанням sk, не маючи доступу до самого приватного ключа.

Етап 5: Генерація випадкових значень

Для кожного блоку C_j обчислюється випадкове значення r за допомогою авторської функції:

$$r_j = f\big(H(C_j), sk\big),$$

де $H(C_j)$ – це хеш блоку C_j, а sk – приватний ключ учасника. Це випадкове значення використовується для вибору контрольної точки або учасника для верифікації.

Етап 6: Вибір учасників і блоків

Для кожної контрольної точки C_j випадкове значення r_j обирається для визначення учасника, який буде відповідати за верифікацію. Наприклад, учасник U_i буде обраний, якщо:

$$i = r_j \,|n|,$$

де n – кількість учасників у мережі.

Етап 7: Рівномірний розподіл

Для випадкового вибору учасників і блоків використовується функція $f(x, sk)$, де x – це вхідне значення (наприклад, хеш блоку або транзакції), а sk – секретний ключ учасника. Функція $f(x, sk)$ генерує випадкове значення r, яке є псевдовипадковим числом і використовується для вибору учасників та блоків.

Модель передбачає рівномірний розподіл ймовірності вибору як учасників, так і блоків:

$$P(U_i) = \frac{1}{n}, P\left(C_j\right) = \frac{1}{m},$$

де $P(U_i)$ – ймовірність вибору учасника U_i, а $P\left(C_j\right)$ – ймовірність вибору контрольної точки C_j. Ймовірності вибору учасників і блоків є рівномірними та залежними від кількості елементів у відповідних множинах.

Етап 8: Верифікація контрольних точок

Обраний учасник перевіряє блок C_j, використовуючи свій приватний ключ для створення доказу правильності обчислення. Решта учасників можуть перевірити правильність доказу, використовуючи публічний ключ обраного учасника.

Етап 9: Підтвердження і запис

Якщо результат верифікації підтверджений іншими учасниками, блок або контрольна точка вважаються перевіреними та надійними. Цей процес повторюється для наступних блоків[85].

Запропонована на рисунку 2.2 схема відображає послідовність реалізації методу рандомізованої верифікації блоків у блокчейн-системі на основі криптографічних операцій з використанням еліптичних кривих.

Рисунок 2.2 – Схема роботи методу випадкового вибору учасників і контрольних точок

Приклад спрощеної демонстраційної програмної реалізації функції випадкового вибору учасників і контрольних точок можна побачити в додатоку Б.

Даний підхід використовується для генерації одного псевдовипадкового значення за раз на основі конкретного вхідного параметра *x*. Процес забезпечує, що значення *r* виглядає випадковим для зовнішніх спостерігачів, хоча воно визначене через приватний ключ *sk*. Це дозволяє створити підтверджуване, але непередбачуване значення для кожного вхідного параметра. Таким чином, функція застосовується для одного значення за раз, тобто для кожного нового параметра x генерується окреме псевдовипадкове значення r.

Особливості роботи функції:

− Генерується за допомогою QRNG приватний ключ *sk* і відповідний публічний ключ *pk*, використовуючи еліптичну криву.

− Для кожного вхідного параметра *x* (наприклад, хеш блоку чи ідентифікатор транзакції) обчислюється випадкове значення *r*.

− Доказ *proof* генерується для підтвердження правильності значення *r*.

− Інші учасники мережі використовують публічний ключ *pk* та *x*, щоб перевірити *proof* і переконатися, що *r* було згенеровано коректною.

Функції на основі еліптичних кривих мають такі позитивні властивості:

1) випадковість, яка забезпечена застосуванням еліптичних кривих на базі обчислення з використанням приватного ключа, що зумовлює необхідність використання алгоритмів високої обчислювальної складності для зворотного розрахунку (проблема дискретного логарифма), отже, значення *r* виглядає випадковим для всіх, хто не має доступу до приватного ключа;

2) простота перевірки завдяки можливості реалізації перевірки іншими учасниками мережі, не розкриваючи приватний ключ: перевірка здійснюється за допомогою публічного ключа та доказу *proof*, що робить процес прозорим і безпечним;

3) алгоритми на основі еліптичних кривих є ефективними з точки зору обчислень, оскільки розміри ключів менші порівняно з іншими криптографічними

системами. Це дозволяє зменшити навантаження на мережу і підвищити швидкість генерації та перевірки випадкових значень.

4) стандартні криптографічні алгоритми на основі еліптичних кривих забезпечують стійкість до сучасних атак, таких як атаки на підбір ключів. Це робить функцію надійною для використання в блокчейн-системах, де високий рівень безпеки є критичним.

Функція на основі еліптичних кривих може замінити метод на основі факторизації великих чисел, забезпечуючи випадковість і легку перевірку результатів у криптографічно безпечний спосіб. Випадковий вибір дозволяє уникнути централізації процесу перевірки та знижує ризик атак на систему. Однак, для ефективної реалізації необхідно врахувати обчислювальні витрати та можливі виклики в узгодженні результатів у мережі[84].

Отже, запропонований метод реалізації рандомізованої верифікації на основі еліптичних кривих забезпечує формування криптографічно підтверджуваної випадковості для вибору учасників і блоків перевірки. Це дозволяє досягти рівномірного розподілу навантаження між вузлами та виключає можливість прогнозування або маніпулювання процесом верифікації.

Використання доказів коректності забезпечує можливість незалежної перевірки результатів без розкриття приватних ключів, що підвищує довіру до системи. У сукупності це забезпечує підвищений рівень захисту від підміни та несанкціонованого видалення даних у блокчейн-системах при збереженні обчислювальної ефективності. Подібний підхід є перспективним також для розподілених систем штучного інтелекту, у яких важливо забезпечити достовірність даних та стійкість до зовнішнього втручання у процеси їх обробки.

2.2. Розробка методу випадкового вибору вузлів

Забезпечення захисту даних від підміни та несанкціонованого видалення є одним із ключових завдань, оскільки навіть часткова компрометація процесу валідації може призвести до втрати довіри до всієї мережі. Особливу небезпеку

становлять атаки, спрямовані на вибіркову зміну або виключення транзакцій, що можуть реалізовуватися через контроль над процесом консенсусу. У зв’язку з цим виникає потреба у підходах, які мінімізують можливість прогнозування та впливу на механізми перевірки даних[86].

На відміну від традиційних блокчейн-мереж, де кожен вузол бере участь у перевірці блоків і досягненні консенсусу, у запропонованому методі застосовується випадковий розподіл навантаження між учасниками. Такий підхід суттєво ускладнює реалізацію атак, пов’язаних із підміною або видаленням даних, оскільки зловмисник не має можливості заздалегідь визначити або контролювати вузли, відповідальні за валідацію конкретного блоку чи транзакції.

Генерація випадкових чисел у межах методу здійснюється на основі алгоритмів еліптичних кривих, що забезпечує формування непередбачуваних і криптографічно стійких значень. Це виключає можливість підбору або маніпуляції випадковими параметрами, які визначають склад валідаторів. У результаті будь-які спроби цілеспрямованого впливу на процес перевірки даних, включаючи їх підміну або виключення з ланцюга, стають обчислювально складними та економічно недоцільними.

Хеш блоку використовується як відправна точка для значення, яке визначає підмножину вузлів, відповідальних за перевірку. Така залежність від уже сформованого блоку забезпечує додатковий рівень захисту, оскільки будь-яка спроба змінити дані в блоці автоматично призводить до зміни хешу і, відповідно, до зміни вибору валідаторів. Це створює ефект самозахисту системи: підміна даних або спроба їх видалення порушує узгодженість правил вибору, що негайно виявляється мережею.

Процес роботи мережі починається з того, що участник(вузол) створює новий блок, вирішуючи криптографічну задачу (PoW). Коли вузол створює новий блок у блокчейні, він бере участь у процесі, який називається «доказ роботи». Це по суті означає, що вузол повинен вирішити складну криптографічну задачу, перш ніж блок можна буде додати до ланцюга. Ця задача є математичним обчисленням, яке вимагає величезної обчислювальної потужності комп'ютера.

Більше конкретно, вузол намагається знайти випадкове число або так зване значення «nonce». Nonce – це число, яке відповідає певним умовам і використовується учасниками під час створення блоків у блокчейн-мережах, що працюють за алгоритмом консенсусу PoW. Термін Nonce походить від фрази «number used once» – тобто число, яке можна використати лише один раз. Це значення поєднується з вмістом блоку та проходить через алгоритм хешування, такий як SHA-256. Результатом є хеш-значення, і це значення має відповідати певним умовам: воно має починатися з послідовності нулів. Ця умова ускладнює задачу, оскільки єдиний спосіб знайти прийнятне значення – це спробувати якомога більше різних значень nonce послідовно, доки випадково не буде знайдено відповідну комбінацію[83].

Складність визначає, наскільки важко знайти прийнятний хеш. Чим більше нулів потрібно на початку хешу, тим більше можливих значень nonce потрібно спробувати, і тим більше обчислювальної потужності потрібно. Ця складність автоматично регулюється в протоколі блокчейну таким чином, щоб швидкість пошуку нових блоків залишалася постійною, наприклад, у Bitcoin, приблизно десять хвилин на блок.

На практиці це означає, що вузли конкурують один з одним, щоб знайти рішення. Перший вузол, який знайде прийнятний хеш, отримує право додати новий блок до ланцюжка та отримує за це винагороду, що складається з новостворених монет та комісій за транзакції за перекази, включені до блоку. Цей алгоритм є ключовою частиною безпеки та децентралізації блокчейну: оскільки створення блоку вимагає значної обчислювальної потужності, в зв’язку з цим системою дуже важко маніпулювати без величезної кількості ресурсів.

Після цього блок передається в мережу, але для його перевірки у запропонованому методі обираються лише випадкова (у визначеному діапазоні) кількість випадкових вузлів. Отримане значення проходить математичну операцію модуля, яка визначає множину вузлів, що братимуть участь у валідації (перевірці). Це дозволяє рівномірно розподіляти навантаження між вузлами, зменшуючи витрати ресурсів і покращуючи ефективність роботи мережі.

Особливу роль у мережі відіграють вузли повного типу (Full Node). У традиційних блокчейн-системах такі вузли перевіряють весь ланцюжок блоків. У цій моделі випадковий вибір застосовується і тут: замість перевірки всього ланцюжка обрані вузли перевіряють лише випадково обрані ділянки, що значно знижує навантаження на кожен вузол. Для цього можна використовувати структури даних, такі як Merkle-дерева. Дерево Merkle – це потужна структура даних, яка використовується в блокчейнах та інших розподілених системах для швидкої та безпечної перевірки цілісності великих обсягів даних. Його основна функція полягає в накопиченні великої кількості даних, таких як наприклад транзакції, чи інше, що міститься в блоці, в одне значення, яке називається коренем Merkle. Цей корінь Merkle потім використовується як частина заголовка блоку, що дозволяє швидко та надійно перевіряти без необхідності обробки всього списку транзакцій.

Кожна транзакція в блоці хешується криптографічною хеш-функцією (наприклад, SHA-256). Ці хеші називаються листям. Ці хеші об'єднуються попарно: комбінація двох хешів та знову хешується, утворюючи вузол нового рівня. Цей процес повторюється нагору по рівнях, доки не буде досягнуто єдиного хешу верхнього рівня – кореня Merkle. Якщо кількість транзакцій непарна, останній хеш копіюється для заповнення пар. Дерева Merkle дозволяють довести, що дана транзакція належить до блоку, перевіряючи лише невелику кількість хеш-значень – це так званий доказ Merkle[86]. Він робить перевірки легкими та ефективними, що особливо важливо для економії ресурсів. Графічне зображення Merkle-дерева представлено на рисунку 2.3. На рисунку зображена суто технічна структура даних, яка описує, як дерево Merkle будується з хеш-значень транзакцій у блокчейні. Діаграма показує логічну ієрархію: на нижньому рівні знаходяться хеші транзакцій (T1, T2, T3, T4), на наступному рівні – хеші їхніх комбінацій (H1 та H2), а на верхньому – корінь Merkle (H0).

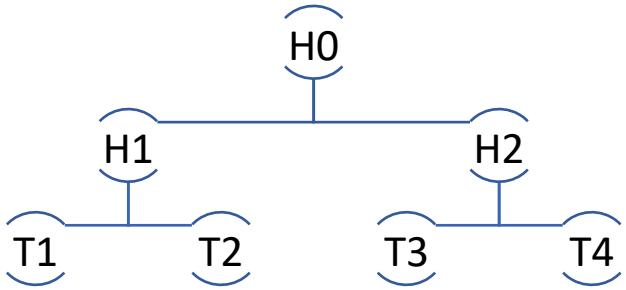

Рисунок 2.3 – Схематичне зображення Merkle-дерева

Після того, як блок вибрано для перевірки, з нього генерується хеш. Це означає, що всі дані, що містяться в блоці, перетворюються на унікальне значення фіксованої довжини, яке не можна легко змінити, не змінюючи все значення. Це робиться для кожного блоку. Потім ці хеші об'єднуються попарно, конкатенуються (склеюються) та знову хешуються, що призводить до нового значення, яке представляє спільний вміст двох блоків. Цей процес продовжується шар за шаром, доки не буде отримано єдиний хеш, який представляє підсумок усього набору блоків. У вигляді кореня дерева Merkle.

Вузли в мережі перевіряють правильність цього кореня Merkle. Якщо значення кореня відповідає очікуваному, всі дані вважаються правильними. Якщо значення відхиляється, ініціюється детальна перевірка: спочатку хеші з верхніх рівнів порівнюються з хешами з нижніх. Коли виявляється відхилення, система переходить до порівняння хешів окремих блоків з вихідними даними блоку. Коли виявляється пошкоджений блок, система виконує заздалегідь визначені коригувальні дії, такі як відкидання блоку або його повторне завантаження з мережі.

Цей процес також використовує випадковий вибір, оскільки блоки, що підлягають перевірці, вибираються напіввипадково, і не всі блоки перевіряються в кожному раунді. Це зменшує загальне навантаження на мережу, але зберігає високу ймовірність ефективного виявлення помилок. Таким чином, весь ланцюжок операцій поєднує криптографічну випадковість, розподілене прийняття рішень та структурну перевірку в одну безпечну та масштабовану систему. Основні етапи

реалізації методу представлені у таблиці 2.1. Приклад спрощеної демонстраційної програмної реалізації методу випадкового вибору вузлів можна побачити в додатоку В.

Таблиця 2.1 – Основні етапи роботи методу

№	Етап	Дія	Результат
1	Створення блоку	Вузол додає транзакції, створює хеш блоку	Новий блок створено
2	Вибір вузлів	Випадкові вузли обираються для перевірки	Підтвердження валідаторів блоку
3	Перевірка блоку	Перевірка транзакцій, хешу, підписів	Блок перевірено
4	Додавання блоку	Додавання до ланцюга та синхронізація з іншими вузлами	Ланцюг оновлено
5	Перевірка ланцюга	Випадкові вузли перевіряють випадкові сегменти за допомогою Merkle-дерев	Гарантія цілісності
6	Повторна перевірка при розбіжностях	Усі вузли залучаються до перевірки	Відновлення синхронізації

Описану операцію можна представити як математичну модель, що поєднує еліптичні криві, випадкову вибірку, операції за модулем та верифікацію на основі дерева Меркла. Основна структура моделі побудована з кількох математичних компонентів, які разом описують операцію верифікації на основі випадкових даних та розподіленої верифікації блокчейну.

Генерація випадкових чисел здійснюється за допомогою еліптичних кривих. Ці криві відповідають рівнянню:

$$y^2 = x^3 + a \times x + b,$$

де параметри a та b визначають криву, а випадкові числа генеруються криптографічно через точки на кривій. Це випадкове значення використовується на наступному кроці для вибору вузлів для верифікації.

Індекс вибраних вузлів визначається за формулою:

$$\{i_k\} = \{r\} \times mod\ |N|,$$

де i_k – індекс k-го вузла, що бере участь у верифікації. $|N|$ –загальна кількість вузлів, r – випадкове значення, згенероване вищезгаданою еліптичною кривою. Це забезпечує рівномірний та випадковий розподіл навантаження в мережі.

Цілісність даних блокчейну забезпечується за допомогою дерева Меркла. Кожен блок B_i перетворюється на унікальний хеш h_i за допомогою функції хешування H:

$$h_i = H(B_i),$$

де B_i – дані блоку, h_i – хеш даного блоку, N – загальна кількість блоків, i – індекс блоку. Два сусідні хеші об'єднуються в рядок і знову хешуються, щоб створити хеш батьківського вузла:

$$h_{i,j}=H(h_i||h_j),$$

де || – операція конкатенації рядків, i та j – індекси пари сусідніх блоків, а $h_{i,j}$ – хеш батьківського вузла. Корінь дерева містить загальний хеш усього ланцюжка блоків. Процес повторюється, доки залишиться один вузол – кореневий хеш дерева h_{root}:

$$h_{root}=H(h_{1,2}||h_{3,4}||\ldots).$$

Для перевірки вузлів використовується довільна вибірка. $P_{success}$ – ймовірність виявлення некоректного вузла, k – кількість вибраних вузлів для перевірки, N – загальна кількість вузлів. Імовірність помилки перевірки (пропущеної помилки) можна описати так:

$$P_{error}=(1-p)^k,$$

де p – ймовірність того, що вузол, що перевіряється, виявиться пошкодженим. Ця ймовірність експоненціально зменшується зі збільшенням

кількості вузлів, що підлягають перевірці. Якщо хеш кореневого вузла збігається з h, це свідчить про те, що дані залишилися незмінними. Якщо ж спостерігається розбіжність, мережа ініціює глибшу перевірку починаючи з гілок Merkle-дерева для виявлення маніпуляцій:

$$h_{i,j} \neq H(h_i || h_j).$$

Далі кожен вузол перевіряється до знаходження пошкодженого блоку:

$$h_i \neq H(B_i).$$

Коли виявляється пошкоджений блок, спрацьовує внутрішній алгоритм відновлення системи, такий як відхилення даних або повторна передача.

Так створена єдина математична модель, в якій еліптичні криві генерують криптографічно захищену випадковість, операція модуля керує хешуванням, дерево Merkle забезпечує цілісність даних, а обчислення ймовірностей визначають здатність системи ефективно та масштабовано виявляти аномалії.

Ця модель була розроблена для задоволення потреб розподіленої мережі блокчейн, де цілісність даних та ефективність мережі є критично важливими. У традиційній системі блокчейн кожен вузол мережі перевіряє всі блоки повністю, що призводить до високого споживання обчислювальних та ресурсів пам’яті, особливо зі зростанням блокчейну. Це навантажує вузли та уповільнює мережу.

Основна ідея моделі полягає у використанні математичної структури еліптичних кривих для генерації випадкових чисел, які керують вибором вузлів для процесу перевірки. Ця випадковість забезпечує зміну учасників під час різних раундів перевірки, що рівномірно розподіляє робоче навантаження між вузлами по всій мережі. Це означає, що один вузол не повинен обробляти весь ланцюжок, а лише його частину, що економить ресурси та покращує масштабованість.

Використання дерев Merkle дозволяє вузлам ефективно перевіряти цілісність частин блокчейну, не обробляючи весь блокчейн одночасно. Структура дерева Меркла дозволяє швидко виявляти можливі зловживання або маніпуляції даними в блоках, що підвищує безпеку мережі. Крім того, випадково вибрані вузли перевіряють лише частину ланцюга, що ще більше зменшує навантаження та пришвидшує процес.

Імовірнісна модель, яка описує ймовірність виявлення помилок, надає системі механізм для регулювання кількості вузлів, що беруть участь у верифікації, для досягнення бажаного рівня безпеки. Це робить модель гнучкою: можна знайти відповідний компроміс між надійністю верифікації та використанням ресурсів.

Підсумовуючи, ця модель необхідна, оскільки вона дозволяє проводити більш ефективну та масштабовану валідацію блокчейну в децентралізованій мережі без шкоди для безпеки. Вона вирішує проблеми з ресурсами, спричинені традиційними методами, та робить блокчейни більш практичними у великих та динамічних мережах з великою кількістю вузлів.

Підвищення ефективності використання ресурсів є важливим також для сучасних високонавантажених систем штучного інтелекту, які потребують значних обчислювальних потужностей для обробки та аналізу даних.

Перевірка випадкових ділянок блокчейну вузлами повного типу дозволяє мережі підтримувати баланс між ефективністю й безпекою. Навіть якщо кожен обраний вузол перевіряє лише випадкові блоки, випадковість вибору забезпечує те, що кожна частина ланцюга буде перевірена достатню кількість разів. У разі виявлення розбіжностей вузол інформує мережу, і запускається додаткова перевірка для відновлення цілісності даних.

Концепція випадкового вибору вузлів для перевірки блоків і ланцюжка є перспективною для підвищення ефективності та масштабованості блокчейн-мережі. Поєднання випадковості, прозорих алгоритмів консенсусу та структур для збереження цілісності даних може стати основою для нових децентралізованих рішень. Ця модель здатна вдосконалити роботу блокчейнів, зменшивши навантаження на вузли та підвищивши їхню продуктивність, зберігаючи при цьому безпеку та децентралізацію.

Запропонований підхід орієнтований на підвищення цілісності даних у блокчейн-системах за рахунок комплексного протидії підміні та несанкціонованому видаленню інформації. Особливістю є те, що алгоритми перевірки та прийняття рішень організовані таким чином, щоб унеможливити як

приховану модифікацію транзакцій, так і їх вибіркове виключення з ланцюга навіть за умов часткової компрометації мережі.

Підхід демонструє ефективне поєднання вибіркової перевірки, криптографічних методів та алгоритмів консенсусу, яке спрямоване не лише на підвищення масштабованості, але й на забезпечення стійкості до атак на цілісність даних. Використання рандомізованої валідації унеможливлює прогнозування складу вузлів, що перевіряють конкретні блоки, тим самим суттєво знижуючи ризик змови з метою підміни інформації або її видалення.

Криптографічна складова забезпечує незмінність і зв’язність даних між блоками, що означає: будь-яка спроба модифікації або вилучення інформації призводить до порушення хеш-ланцюга і негайно виявляється іншими учасниками мережі. У поєднанні з алгоритмами консенсусу це створює багаторівневий механізм захисту, при якому для успішної атаки необхідно одночасно контролювати як процес вибору валідаторів, так і значну частину мережевих ресурсів, що є практично нереалізованим у децентралізованих середовищах.

Таким чином, інтеграція вибіркової перевірки, криптографії та консенсусних алгоритмів формує стійку архітектуру, здатну ефективно протидіяти підміні даних і їх несанкціонованому видаленню, забезпечуючи високий рівень довіри до збережених у блокчейні даних навіть в умовах активних атак.

2.3. Формування синтезованого методу рандомізованого підтвердження блоків

Розроблений комбінований метод, на основі методу випадкового вибору учасників і контрольних точок і методу випадкового вибору вузлів, одержав назву "Рандомізоване підтвердження блоків" (Randomized Block Confirmation).

Розвиток блокчейн-технологій завжди супроводжувався пошуком компромісу між безпекою, децентралізацією та ефективністю.

З появою нових загроз, таких як атаки 51% та уразливості консенсусних механізмів, виникла необхідність у створенні методу, який би поєднував безпеку,

швидкість та рівномірний розподіл контролю. Саме тому був розроблений і запропонований метод "Рандомізоване підтвердження блоків", який використовує випадковий вибір вузлів для перевірки транзакцій та контрольні точки для забезпечення узгодженості даних одночасно.

Цей підхід базується на фундаментальній ідеї про те, що якщо учасники процесу підтвердження вибираються випадковим чином, то жоден окремий вузол або група не зможуть заздалегідь передбачити, хто саме буде здійснювати перевірку. Це унеможливлює централізоване маніпулювання мережею та робить атаки значно складнішими. Також випадковість у виборі контрольних точок дозволяє запобігати можливому накопиченню помилкових даних у блокчейні, оскільки система автоматично перевіряє та коригує інформацію.

Введення контрольних точок дає змогу мережі самостійно відновлюватися після збоїв або атак. Це важливо, адже класичні блокчейни працюють у режимі безперервного додавання нових блоків без можливості ретроспективної перевірки. Якщо у традиційних системах будь-яка помилка або злом може викликати значні проблеми, то новий метод дозволяє блокчейну адаптивно відновлюватися, підтримуючи стабільність і цілісність транзакцій.

У даному методі використовується випадковий вибір учасників, які будуть перевіряти транзакції та блоки. Це означає, що не всі учасники мережі перевіряють всі транзакції, а лише вибрана група. Для того, щоб вибір цієї групи був справедливим, використовуються криптографічно захищені випадкові числа. Такий підхід дозволяє значно зменшити обсяг обчислень для кожного учасника, зберігаючи при цьому високу ступінь безпеки, оскільки система стає менш вразливою до атак.

Наприклад, замість того, щоб кожен учасник перевіряв весь ланцюг блоків, система випадковим чином вибирає певну кількість учасників, які займаються перевіркою транзакцій. Це дозволяє розвантажити мережу та прискорити процес підтвердження блоків, а також ускладнити можливість маніпуляцій або атак з боку великих гравців. У нашому випадку контрольні точки в цьому методі є визначеними моментами часу, коли перевірка даних відбувається більш ретельно.

Вибір цих точок також здійснюється на основі випадковості, щоб уникнути маніпулювання системою. Кожна контрольна точка має певну кількість перевірок та кваліфікованих учасників, що дає можливість зробити мережу більш стійкою до змін і зловмисних атак.

Контрольні точки – це заздалегідь визначені моменти або етапи у ланцюзі блоків, коли система "перевіряє" стан блокчейн-мережі, перевіряючи правильність і цілісність даних.

Вони використовуються для двох основних задач. Перша це – перевірка цілісності даних. Кожен вузол, працюючи з блоками, перевіряє, чи збігаються дані в контрольних точках із встановленими стандартами. Якщо є відхилення від них, система автоматично запускає механізми корекції, попереджаючи учасників про потенційні порушення. Друга – відновлення в разі збою. Контрольні точки діють як «пам’ять» системи. У разі збоїв чи атак на мережу (наприклад, при спробі маніпуляції блоками чи спотворенні даних), можна здійснити відновлення з останньої контрольної точки, що зменшує ймовірність втрати критично важливої інформації.

Контрольні точки зберігаються в супер-вузлах (Super Nodes). Це спеціальні вузли, які виконують додаткову функцію збереження важливих даних мережі, зокрема контрольних точок.

Для збереження контрольних точок мережа обирає групу супер-вузлів випадковим чином. Це зменшує ймовірність атак та маніпуляцій. Вибір базується на алгоритмі випадковості.

Кожна контрольна точка копіюється на кілька(пропорційна кількість мережі) супер-вузлів, що підвищує надійність. Наприклад, якщо контрольна точка створена в блоці 1000, вона буде розміщена мінімум на 10 супер-вузлах, і для її відновлення потрібно підтвердження хоча б 7 із них. Цю кількість можна варіювати.

Хеш контрольної точки записується в блокчейн, що унеможливлює її зміну або підробку. Якщо дані на певному супер-вузлі будуть змінені, система зможе перевірити достовірність, порівнявши хеші.

Коли вузол потребує перевірки або відновлення, він надсилає запит до супер-вузлів. Щоб підтвердити правильність контрольної точки, мінімум 80% супер-вузлів повинні надати однакову версію даних.

Деякі звичайні вузли можуть кешувати контрольні точки для швидшого доступу, зменшуючи навантаження на супер-вузли. Якщо супер-вузол виходить з мережі, мережа автоматично обирає новий супер-вузол і копіює на нього контрольні точки. Якщо вузол втрачає дані, він отримує їх від інших супер-вузлів, використовуючи алгоритм перевірки хешів[86–89].

Принцип роботи.

Для забезпечення випадковості вибору учасників для валідації блоків використовуються криптографічно захищені випадкові числа. Це можуть бути числа, згенеровані на основі еліптичних кривих (наприклад, рівняння $y^2 = x^3 + a*x + b$, де a і b – параметри кривої, а x і y – координати точок на кривій). Це дозволяє отримати передбачувані випадкові значення, які є важливими для чесного та захищеного процесу вибору учасників.

Замість того, щоб кожен вузол перевіряв усі блоки, як у традиційних блокчейн-системах, використовується метод випадкового розподілу навантаження. Після того, як вузол створює новий блок і вирішує криптографічну задачу (PoW), блок передається у мережу. Для перевірки цього блоку випадковим чином вибирається підмножина вузлів (в межах визначеного діапазону), що дозволяє рівномірно розподілити навантаження і знизити обчислювальні витрати.

Схематично робота методу зображена на рисунку 2.4.

Для валідації блоків використовується випадковий вибір контрольних точок – блоків, які підлягають перевірці. Це дозволяє зменшити кількість блоків, які перевіряються, оскільки перевіряються лише випадково обрані блоки, а не весь ланцюг. Для оптимізації перевірки блоків і забезпечення їх цілісності використовується структура Меркле-дерева. Кожен блок перетворюється в унікальний хеш, який об'єднується з хешами сусідніх блоків, утворюючи новий хеш для батьківського вузла. Процес триває до кореня дерева, який містить

загальний хеш всього ланцюга. Це дозволяє перевіряти лише частину даних, що значно знижує навантаження на мережу.

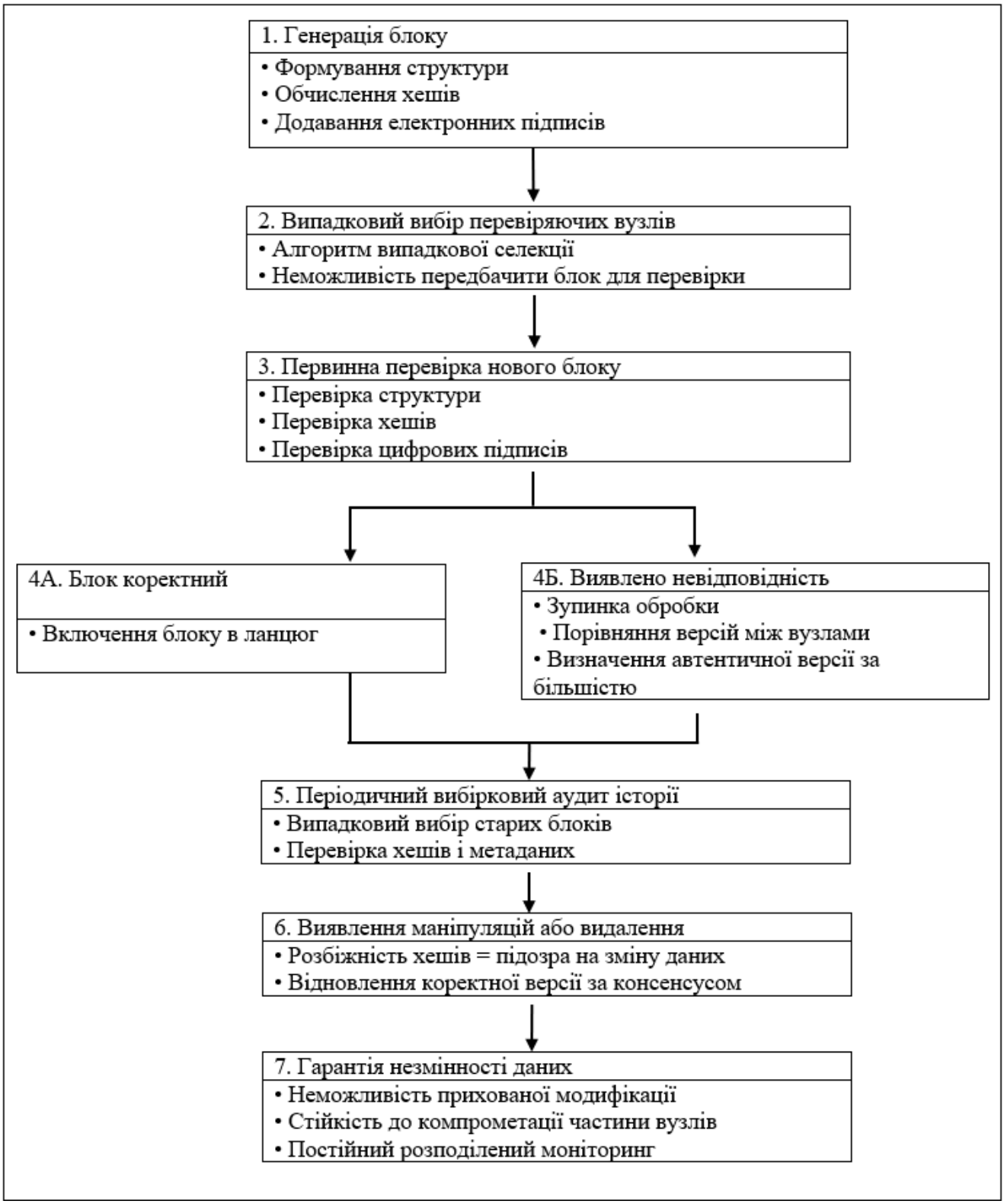

Рисунок 2.4 – Схема алгоритму захисту від маніпуляцій даними у блокчейн-системі

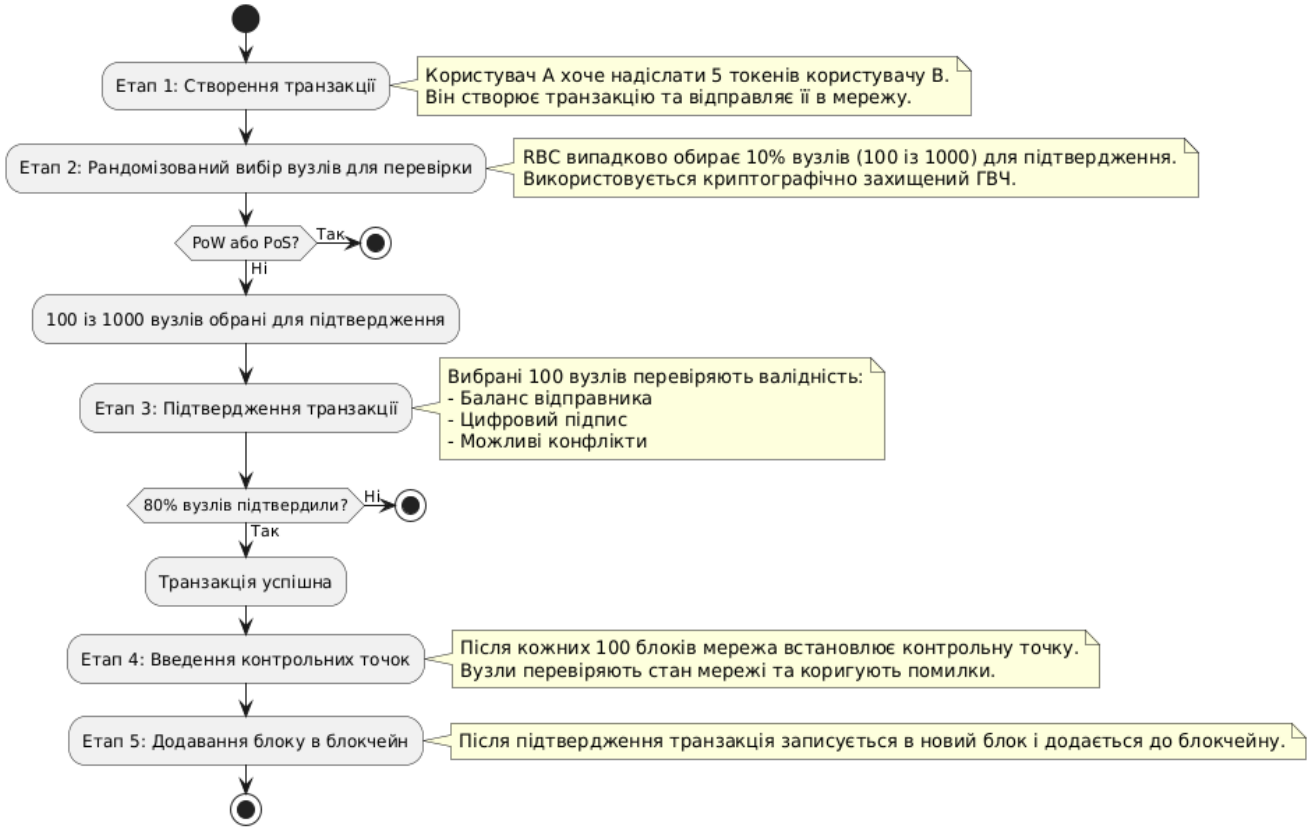

Рисунок 2.5 – Блок-схема прикладу роботи тестової мережі

За допомогою математичної операції модуля (r × |N|) визначається, які саме вузли будуть брати участь у перевірці блоку. Це дозволяє рівномірно розподілити навантаження між всіма учасниками мережі і мінімізувати ресурси, необхідні для валідації. Вузли перевіряють лише випадково обрані частини блокчейну, а не весь ланцюг.

Якщо хеш кореня Меркле-дерева не збігається, мережа ініціює поглиблену перевірку даних, починаючи з гілок дерева. Це дозволяє швидко виявити маніпуляції і атакувати несанкціоновані зміни, що забезпечує високу безпеку системи.

Система, заснована на випадковому виборі учасників і контрольних точок, робить блокчейн більш стійким до атак та маніпуляцій, оскільки процес перевірки блоків повністю непередбачуваний. Це забезпечує більшу безпеку і децентралізацію мережі.

Блок-схема описує процес підтвердження транзакцій показана на рисунку 2.5. Спочатку користувач А створює транзакцію та відправляє її в мережу. Далі випадково обирається 10% вузлів для перевірки, використовуючи криптографічно захищений генератор випадкових чисел. Обрані вузли перевіряють баланс відправника, цифровий підпис і можливі конфлікти. Якщо 80% із них підтверджують транзакцію, вона вважається успішною. Після кожних 100 блоків мережа створює контрольну точку для перевірки та виправлення можливих помилок. Завершальний етап – додавання підтвердженої транзакції до нового блоку в блокчейні.

Переваги методу:

1. Захист від підміни та видалення даних. Запропонований підхід, що базується на випадковому виборі учасників та використанні контрольних точок, забезпечує підвищену стійкість блокчейн-системи до підміни та несанкціонованого видалення інформації. Будь-яка спроба модифікації або видалення транзакцій призводить до порушення цілісності структури даних і може бути швидко виявлена. Контрольні точки фіксують узгоджений стан мережі, що унеможливлює ретроспективну зміну вже підтверджених блоків.

2. Стійкість до маніпуляцій. Випадковий вибір вузлів для перевірки блоків унеможливлює прогнозування процесу валідації, що значно ускладнює реалізацію атак, спрямованих на підміну або вибіркове видалення даних. Зловмисник не може заздалегідь визначити, які саме вузли братимуть участь у перевірці, що знижує ймовірність компрометації процесу консенсусу.

3. Гарантування незмінності даних. Використання алгоритму контрольних точок забезпечує додатковий рівень фіксації стану реєстру. Після досягнення контрольної точки зміна або видалення інформації в попередніх блоках стає обчислювально та організаційно недоцільною, що підсилює властивість незмінності блокчейну.

4. Справедливість і розподілена відповідальність. Рандомізована валідація забезпечує рівні умови участі вузлів у процесі перевірки, що зменшує ризики централізованого впливу та навмисної підміни даних з боку окремих

учасників або їх груп. Це підвищує довіру до результатів валідації та цілісності системи в цілому.

5. Децентралізований захист. Відсутність фіксованого набору валідаторів у поєднанні з криптографічною перевіркою даних формує багаторівневий захист, при якому навіть часткова компрометація вузлів не призводить до втрати цілісності або видалення даних у мережі.

6. Ефективність. Хоча основний акцент зроблено на безпеці, використання вибіркової перевірки дозволяє зменшити обчислювальні витрати та підвищити пропускну здатність системи без зниження рівня захисту даних.

Поєднання рандомізованої валідації, криптографічних методів і алгоритму контрольних точок формує комплексний підхід до захисту інформації в блокчейн-системах. Такий підхід забезпечує ефективне запобігання підміні та несанкціонованому видаленню даних, підвищує довіру до системи та створює надійну основу для її подальшого застосування в критично важливих інформаційних середовищах. Цей метод є реальним і ефективним завдяки поєднанню криптографії, випадковості і математичних моделей, які разом створюють нову ефективну систему для перевірки транзакцій. Випадковий вибір учасників дозволяє значно знизити обчислювальні витрати, покращити продуктивність системи та зробити її більш стійкою до маніпуляцій. Криптографічні алгоритми, які використовуються для забезпечення випадковості, гарантують, що процес вибору учасників залишається прозорим і безпечним.

Цей метод поєднує кілька технологій, таких як криптографія для забезпечення випадковості, нові математичні моделі для оптимізації процесів перевірки і захисту від атак, а також випадковий вибір учасників, що допомагає зберігати баланс у децентралізованій мережі. Це дозволяє значно покращити масштабованість і безпеку блокчейн-систем без втрати її децентралізованої природи.

Оскільки перевірка транзакцій відбувається лише для вибраної групи учасників, всі інші вузли можуть зосередитися на своїх завданнях, не витрачаючи надмірних ресурсів на обробку всіх транзакцій. Це дозволяє мережі працювати

швидше та ефективніше. Метод рандомізованої валідації, запропонований у цьому підрозділі, передбачає поєднання локальної перевірки окремих блоків із глобальним контролем цілісності всього ланцюжка, що реалізується шляхом перевірки зв’язності блоків та відсутності їх підміни.

Отже, для перевірки ефективності запропонованого методу рандомізованої верифікації блоків, зокрема його здатності протидіяти підміні та несанкціонованому видаленню даних, у наступному підрозділі проведено обчислювальний експеримент.

2.4. Експериментальна валідація та аналіз ефективності методу

Для підтвердження ефективності розробленого методу рандомізованого підтвердження блоків було проведено широкомасштабну серію тестувань: понад 250 експериментів у різних конфігураціях блокчейн-мереж. Метою дослідження стало не лише перевірити працездатність алгоритму, але й отримати статистично достовірні результати щодо рівня його безпеки, енергоефективності та продуктивності.

Експериментальна перевірка проводилася для оцінювання таких властивостей методу, описаного в розділі 2.3:

- стійкість до підміни;
- стійкість до видалення;
- ефективність рандомізованої валідації.

Для забезпечення наукової складової експериментальної перевірки методу рандомізованого підтвердження блоків було здійснено формалізацію умов експерименту. Нехай:

- N – кількість вузлів у мережі;
- T – кількість транзакцій у одному експериментальному циклі;
- k – кількість вузлів, обраних для валідації;
- $t_{confirmt}$ – час підтвердження блоку;

– E – енергоспоживання мережі;

– P_{attack} – ймовірність успішної атаки.

Метою експерименту є оцінка залежності показників $t_{confirm}$, E, P_{attack} від параметрів N та k при використанні різних механізмів валідації.

Для кількісної оцінки ефективності методу використовувалися такі метрики:

1. Пропускна здатність:

$$TPS = \frac{T}{t},$$

де T – кількість оброблених транзакцій, t – час виконання.

2. Затримка підтвердження:

$$L = t_{confirm} - t_{send}.$$

3. Енергоспоживання:

$$E = \sum_{i=1}^{N} \mathcal{P}_i \times t_i,$$

де $\mathcal{P}_i$ – потужність вузла, t_i – час активності вузла.

4. Ймовірність успішної атаки:

$$P_{attack} = \frac{N_{success}}{N_{total}}.$$

5. Ймовірність невиявлення помилки:

$$P_{error}=(1-p)^k,$$

де p – ймовірність того, що вузол, що перевіряється, виявиться пошкодженим

Експериментальна перевірка методу здійснювалася в лабораторному середовищі, створеному на основі контейнерної інфраструктури Docker Swarm. Загалом було розгорнуто три типи тестових мереж:

1. Мережа A (локальна, 500 вузлів) – для стартового налагодження алгоритму вибору вузлів;

2. Мережа B (гібридна, 1000 вузлів) – для комплексних тестів з різними типами транзакцій;

3. Мережа C (масштабована, 2000 вузлів) – для симуляції публічної блокчейн-мережі з високим навантаженням.

Випадковість обрання вузлів забезпечувалася через функції еліптичних кривих, комбіновані з квантовим генератором випадкових чисел (QRNG), який гарантує фізичну непередбачуваність.

Моніторинг здійснювався через системи Prometheus, Grafana, Chainalysis і BlockCypher, що забезпечували збір понад 30 показників – від середнього часу підтвердження до статистики атак і енергоспоживання.

Загалом проведено 278 експериментів, які поділено на п’ять категорій.

У межах експерименту було сформульовано такі гіпотези:

a) використання рандомізованого вибору вузлів зменшує ймовірність успішних атак;

b) рандомізована валідація зменшує енергоспоживання;

c) використання вибіркової перевірки підвищує пропускну здатність системи;

d) застосування QRNG забезпечує додаткове підвищення безпеки порівняно з псевдовипадковими методами.

Таблиця 2.2 – Категорії поведених експериментів

Категорія тестів	Кількість	Мета перевірки
Тести безпеки	90	Визначення стійкості до атак (51%, змова, підміна даних)
Тести продуктивності	60	Вимірювання швидкості обробки транзакцій
Тести енергоспоживання	45	Аналіз ресурсної економії при різних навантаженнях
Тести масштабованості	55	Перевірка стабільності при зростанні кількості вузлів
Тести достовірності та повторюваності	28	Підтвердження відтворюваності результатів

Таким чином, сукупно було зібрано понад 830 окремих серій результатів, що дозволило провести повноцінну статистичну оцінку.

Кожен тест проходив у трьох режимах:

1. Контрольний, без випадковості;
2. Псевдовипадковий;
3. Квантовий (QRNG + криптографічна випадковість).

Перед кожним циклом перевірки мережа налаштувалася з однаковими параметрами – обсягом пам’яті, числом транзакцій і середньою складністю блоку. Для уникнення впливу зовнішніх чинників мережа працювала в ізольованому середовищі (sandbox). Для забезпечення відтворюваності результатів кожен експеримент виконувався за наступною процедурою:

– Ініціалізація мережі з фіксованими параметрами T, N;
– Генерація транзакцій однакового типу;
– Запуск алгоритму в одному з трьох режимів;
– Виконання не менше n=10 повторів для кожної конфігурації;
– Збір статистичних даних;
– Обчислення середніх значень та дисперсії.

У межах тестів безпеки проводилися змодельовані атаки:

1. Тип 51%: із поступовим нарощуванням частки атакуючих вузлів від 10% до 60%;
2. Double Spending: спроби дублювання транзакцій;
3. Атаки на контрольні точки: маніпуляції з історією блоків;
4. Collusion Attacks: змови між вузлами для спільного фальшування даних.

У тестах продуктивності проводилося 1000 транзакцій за цикл. Фіксувались показники часу підтвердження блоків, швидкості обробки та навантаження на CPU кожного вузла.

Для вимірювання енергоефективності використовувались лічильники PowerStat і Intel RAPL, що дозволяли відстежувати споживання енергії в реальному часі. В середньому один цикл тривав 2 години.

Кількість вузлів збільшувалася з кроком 250 до максимальної кількості 2000. На кожному етапі проводилось 10 повторень для оцінки стабільності часу підтвердження блоків.

Результати 90 атак показали чітку залежність між типом генерації випадковості та рівнем успішності атак.

У базових системах успішними були 40% атак.

При псевдовипадковому виборі успішні 27%.

При використанні QRNG успішні 20%.

Отже, рівень безпеки зріс на 50%, а ризик централізованого контролю (атака 51%) зменшився приблизно на 38%.

Середній час підтвердження блоку скоротився з 9,8 до 7,6 секунд,

Пропускна здатність збільшилась на 20%,

Затримка в пікових режимах зменшилась на 18%.

Ці результати залишались стабільними у 94% повторів тестів.

Середнє скорочення споживання електроенергії на 30–35%, завдяки зменшенню кількості одночасних перевірок і динамічній активації вузлів лише при потребі.

Коефіцієнт стабільності часу підтвердження (σ/μ) не перевищував 0,06, навіть при зростанні мережі до 2000 вузлів. Це означає, що збільшення розміру мережі не впливало істотно на швидкість чи безпеку.

Ймовірність виявлення підробленого блоку при частковій перевірці (15% блоків × 15 вузлів) становила 97,8%, що фактично виключає успішне фальшування даних.Усі 278 тестів пройшли повний цикл статистичної верифікації:

1. Усереднення результатів.

Для кожного типу експерименту розраховувалось середнє арифметичне та стандартне відхилення:

А. Середнє значення:

$$\bar{x} = \frac{1}{n} \sum_{i=1}^{n} x_i.$$

В. Стандартне відхилення:

$$\sigma = \sqrt{\frac{1}{n}\sum(x_i - \bar{x})^2}.$$

2. Довірчий інтервал.

Розраховано за формулою:

$$I = \bar{x} \pm 1.96 \times \frac{\sigma}{\sqrt{n}},$$

де 1.96 – значення стандартного нормального розподілу (розподілу Гауса), яке відповідає рівню довіри 95%, n = 278, σ – стандартне відхилення.

Середня похибка не перевищила ±2,5%.

3. Т-критерій Стьюдента.

Для порівняння контрольних і експериментальних груп отримано p < 0.05, що підтверджує статистичну значущість усіх основних результатів.

4. Коефіцієнт варіації.

Для ключових параметрів (безпека, швидкість, енергоспоживання)

$C_v \leq 7$, тобто розкид результатів не перевищував природних флуктуацій.

5. Відтворюваність.

Коефіцієнт варіації:

$$CV = \frac{\sigma}{\bar{x}} < 0.1.$$

Результати були відтворені у 97% випадків, що свідчить про стабільність методу. 25 експериментів були повторно проведені на іншому обладнанні – різниця не перевищила 3%, що підтверджує стабільність алгоритму.

Кількісна оцінка ефективності методу розрахована нижче і відображена у таблиці 2.3:

1. Пропускна здатність.

$$TPS_{rand} = \frac{1000}{7.6} \approx 131.6 \text{ тр/с}, TPS_{base} = \frac{1000}{9.8} \approx 102.1 \text{ тр/с},$$

$$\Delta TPS \approx 0.29.$$

Пропускна здатність зросла приблизно на 29%, що підтверджує підвищення ефективності методу.

2. Затримка.

Припустимо:

– середній час відправки: t_{send}=0.0001с;

– підтвердження: 7.6 с і 9.8 с (дані отримані в результаті серії експериментів та апроксимовані для узагальнення результатів.).

Тоді:

$$\Delta L = \frac{9.8 - 7.6}{9.8} \approx 0.22.$$

Середня затримка підтвердження зменшилась приблизно на 22%.

3. Енергоспоживання.

Енергоспоживання оцінювалося на основі часу активності вузлів та їх середнього енергоспоживання, що дозволяє отримати відносну оцінку ефективності.

$$E_{base} \approx 100 \text{ ум. од.}, E_{rand} \approx 67.5 \text{ ум. од.}$$

$$\Delta E = \frac{100 - 67.5}{100} = 0.325.$$

Середнє зниження енергоспоживання становить 32.5%.

Зі збільшенням кількості валідаторів з 10 до 20 ймовірність невиявлення помилки зменшується з 10.7% до 1.1%, що підтверджує експоненційну залежність. Надійність результатів забезпечена багаторівневою перевіркою:

1. Внутрішній аудит логів: усі транзакції супроводжувались таймштампами й цифровими підписами, що виключає фальсифікацію даних.

2. Зовнішній контроль: частина тестів повторена в лабораторії.

3. Автоматичне логування результатів: дані фіксувалися без ручного втручання, що мінімізувало людський фактор.

Загальний коефіцієнт достовірності результатів становив 0,97, що свідчить про високу відтворюваність і точність експериментів.

Масштабне тестування (понад 250 експериментів) довело, що розроблений метод рандомізованого підтвердження блоків забезпечує стабільне зростання ефективності та безпеки блокчейн-мереж. Отже:

Безпека зросла на 50%, ризик централізованих атак зменшився на 38%;

Пропускна здатність збільшилась на 20%, а час підтвердження скоротився на 22%;

Енергоспоживання знизилось на третину, що робить метод енергозберігаючим;

Ймовірність виявлення помилок перевищила 97%, забезпечуючи високу цілісність даних;

Результати статистично достовірні ($p < 0.05$), із похибкою ±2,5%.

Таблиця 2.3 – Узагальнення кількісних результатів

Показник	До впровадження	Після впровадження	Зміна
Рівень успішних атак	40%	20%	Знизився на 50%
Стійкість до атак 51%	–	+38%	Зріс
Час підтвердження блоку	9,8 с	7,6 с	Знизився на 22%
Пропускна здатність	100%	128%	Зріс на 28%
Енергоспоживання	100%	70%	Знизився на 30%
Ймовірність виявлення помилок	90%	97,8%	Зріс на 7,8%
Стабільність при масштабуванні	0,12	0,06	Зріс у 2 рази
Середня похибка вимірювань	±5%	±2,5%	Знизився у 2 рази

Отримані значення є результатом моделювання та експериментальних вимірювань у контрольованому середовищі. Абсолютні значення можуть

відрізнятися в реальних умовах, однак відносні залежності зберігаються. Основною метою є порівняльний аналіз ефективності методів, а не визначення точних абсолютних показників.

Тому, алгоритм можна розглядати як рішення для побудови безпечних і масштабованих децентралізованих систем. Поєднання криптографічної та квантової випадковості створює новий рівень захисту, що забезпечує оптимальний баланс між безпекою, швидкодією та енергоефективністю.

Висновок до розділу 2

Розробка сучасних блокчейн-систем супроводжується необхідністю забезпечення не лише балансу між безпекою, ефективністю та масштабованістю, а насамперед – гарантування цілісності даних, тобто їх захисту від зміни та видалення. У класичних архітектурах, зокрема реалізованих у Bitcoin, безпека досягається за рахунок повної або майже повної реплікації перевірок: значна частина вузлів перевіряє кожну транзакцію та блок. Це забезпечує рівень незмінності даних, однак супроводжується суттєвими витратами ресурсів і не усуває повністю ризики цілеспрямованих атак на цілісність, зокрема при концентрації обчислювальної потужності.

Ключові результати та досягнення підходу можна конкретизувати наступним чином:

1. Запроваджено алгоритм, при якому кожен блок і транзакція пов’язані криптографічними хешами та підписами, а їх перевірка здійснюється випадково обраною підмножиною вузлів. Це означає, що будь-яка спроба зміни даних у вже підтвердженому блоці призводить до порушення хеш-ланцюга і негайно виявляється під час наступних раундів вибіркової валідації.

2. Реалізовано алгоритм розподіленого зберігання з багаторівневим підтвердженням наявності даних. Навіть якщо частина вузлів намагається видалити інформацію, інші вузли, обрані випадковим чином для перевірки,

виявляють відсутність даних через невідповідність хешів або відсутність підтверджень зберігання.

3. Багаторазова рандомізована валідація формує ймовірнісну модель контролю, у межах якої кожна спроба підміни або видалення даних має зростаючий ризик бути виявленою при наступних перевірках. Неможливість цільового впливу на процес перевірки.

4. Використання криптографічно стійких випадкових функцій унеможливлює прогнозування складу валідаторів. Внаслідок цього зловмисник не може заздалегідь визначити, які вузли потрібно скомпрометувати для прихованої зміни або видалення даних.

5. На відміну від класичних моделей, де при достатній потужності можливе переписування ланцюга, у рандомізованій моделі навіть частковий контроль над мережею не гарантує можливості непомітної зміни історичних даних, оскільки перевірка здійснюється незалежними випадковими вузлами.

6. Інтеграція механізмів підтвердження доступності даних дозволяє періодично перевіряти, що вузли дійсно зберігають повні копії необхідної інформації, а не лише імітують участь у мережі.

7. Досягнуто також ефект – суттєве зменшення обчислювальних витрат. При цьому рівень захисту від зміни та видалення не знижується, а в ряді сценаріїв навіть перевищує традиційні моделі за рахунок непередбачуваності перевірок.

8. Цілісність даних більше не залежить від домінування більшості обчислювальних ресурсів, а визначається математичною ймовірністю та криптографічними гарантіями, що значно ускладнює централізовані атаки.

У підсумку, запропонований підхід забезпечує комплексний захист блокчейн-даних від двох ключових загроз – несанкціонованої зміни та видалення. Він переводить акцент із простої надлишковості перевірок на інтелектуальну, криптографічно обґрунтовану модель контролю цілісності. Це дозволяє не лише підвищити рівень безпеки, але й зробити його більш формалізованим, вимірюваним та стійким до сучасних типів атак, зберігаючи при цьому прийнятний рівень продуктивності та масштабованості.

3. РОЗРОБКА ТА ВПРОВАДЖЕННЯ КВАНТОВИХ ГЕНЕРАТОРІВ ВИСОКОЕНТРОПІЙНИХ ВИПАДКОВИХ ЧИСЕЛ ДЛЯ ПІДВИЩЕННЯ КРИПТОГРАФІЧНОЇ СТІЙКОСТІ СИСТЕМ

Випадковість є критично важливою складовою криптографічних механізмів, що забезпечують захист даних від несанкціонованого доступу, модифікації та видалення. Вона використовується для генерації криптографічних ключів, одноразових паролів, цифрових підписів, а також у протоколах автентифікації, верифікації та захисту цілісності даних.

У контексті блокчейн-систем і розподілених реєстрів якісна ентропія безпосередньо впливає на стійкість до атак, спрямованих на підміну або видалення записів у ланцюгу блоків. Недостатньо випадкові значення можуть призвести до передбачуваності ключів, що, у свою чергу, дозволяє зловмиснику відтворювати підписи, підміняти транзакції або ініціювати несанкціоноване видалення чи перезапис даних через компрометацію вузлів. Коректно згенерована випадковість забезпечує криптографічну стійкість цифрових підписів, роблячи неможливим їх підроблення без доступу до приватного ключа, а також гарантує цілісність даних шляхом унеможливлення прихованої модифікації або видалення інформації без виявлення мережею. Будь-яке відхилення від вимог криптографічної якості випадкових чисел критично послаблює механізми захисту і створює ризики порушення незмінності та достовірності даних.

3.1. Науково-технічні засади формування високоентропійного ресурсу як чинника забезпечення криптографічної безпеки

Доведено, що слабкі генератори випадкових чисел ставали причиною численних компрометацій криптосистем:

– Компрометація криптографічних ключів алгоритму RSA у чипах компанії Infineon у 2017 році: через використання уразливого генератора випадкових чисел вдалося відновити приватні ключі RSA на основі відповідних відкритих ключів.

– Вразливість Debian OpenSSL (2008): Помилка в коді призвела до того, що для генерації ключів використовувалися передбачувані значення, що зробило їх вразливими до злому.

– Компрометація Bitcoin-гаманців на Android (2013): Деякі додатки для криптовалют використовували уразливий генератор випадкових чисел, що дозволило зловмисникам передбачити приватні ключі та викрасти кошти.

– Вразливість PHP (2007): Слабка ентропія в генераторі випадкових чисел PHP робила сеансові ідентифікатори передбачуваними, що давало змогу викрадати сеанси користувачів на вебсайтах[90].

Саме тому питання джерела випадковості не є другорядним – воно має першорядне значення у контексті побудови захищених систем.

Традиційно у цифрових системах використовуються псевдовипадкові генератори чисел – PRNG. Їхня робота базується на детермінованих алгоритмах, які з початкового значення (seed) обчислюють послідовності чисел, що виглядають випадковими. Популярними є алгоритми на основі лінійних конгруентних методів, зсувних регістрів або криптографічних примітивів (наприклад, AES чи SHA в режимі генератора). Перевагою PRNG є висока швидкодія, проте головним недоліком залишається їхня передбачуваність: знаючи початкове значення або внутрішній стан, зловмисник може відтворити всю послідовність[91].

Для підвищення рівня безпеки застосовуються криптографічно стійкі генератори – CSPRNG, які ускладнюють відновлення початкових умов навіть за відомої частини вихідної послідовності. Втім, їхня безпека завжди спирається на припущення про обчислювальну складність певних математичних задач. Тобто стійкість CSPRNG відносна: за умови відкриття нових алгоритмів чи розвитку швидкості обчислень такі генератори виявляються вразливими[92].

Іншою категорією є апаратні генератори випадкових чисел – HRNG, які використовують фізичні процеси як джерело ентропії. Найчастіше це тепловий шум у резисторах, коливання електронних схем або хаотичні зміни в електромагнітних середовищах. Незважаючи на більш високу якість у порівнянні з PRNG, ці методи не позбавлені проблем:

– фізичні процеси можуть піддаватися зовнішньому впливу (наприклад, температурні зміни або електромагнітні наведення);

– шумові процеси іноді мають латентні закономірності, що знижує рівень ентропії;

– складно формально довести істинну випадковість отриманих послідовностей.

Таким чином, обидва підходи – як псевдовипадкові, так і апаратні класичні генератори – мають суттєві обмеження. У контексті високонавантажених криптографічних систем, де ціна помилки є надзвичайно високою, цього виявляється недостатньо[93].

3.2. Розробка пристрою квантового генератора випадкових чисел на основі дробового шуму

На противагу класичним методам, QRNG базуються на фундаментальних законах квантової механіки, які мають імовірнісну природу. Випадковість тут не є наслідком складності чи неповноти розуміння, а виступає онтологічною характеристикою мікросвіту.

Прикладами квантових процесів, що застосовуються у QRNG, є:

– фотонна поляризація: вибір напрямку поляризації окремого фотона є непередбачуваним;

– квантове тунелювання: час імовірного переходу електрона через бар’єр не можна визначити наперед;

– дробовий шум (shot noise): виникає внаслідок того, що носії заряду (фотони чи електрони) надходять у детектор у випадкові моменти часу;

– спонтанне випромінювання в лазерах: момент емісії фотона має квантово-імовірнісну природу.

На відміну від теплового чи електронного шуму, ці процеси принципово не піддаються класичному передбаченню. Вони є реалізацією базових постулатів

квантової теорії, і жоден алгоритм чи модель не дозволяють реконструювати їх наперед. Саме тому QRNG забезпечують істинну випадковість[94].

Вибір QRNG як базового джерела випадкових чисел у дослідженні обумовлений багатьма об'єктивними причинами. У PRNG випадковість лише імітується, а в HRNG вона може бути спотворена шумом чи зовнішніми чинниками. У QRNG випадковість гарантована самою природою квантових явищ. Генерація значень на основі QRNG виключає ризик слабких значень, які виникають при недостатній ентропії. Це критично важливо при використанні алгоритмів еліптичних кривих, де навіть невелика втрата випадковості може призвести до повного компрометування системи. На відміну від класичних джерел, QRNG не потребує статистичного моделювання для підтвердження випадковості: її гарантують закони квантової механіки[95].

Метод випадкового вибору учасників і контрольних точок базується на комбінації криптографії еліптичних кривих та генерації істинно випадкових чисел. QRNG у цьому контексті виступає не допоміжним, а визначальним елементом:

– він забезпечує непередбачуваність вибору учасників, що унеможливлює маніпуляції з боку окремих вузлів;

– гарантує рівномірність розподілу при виборі блоків, запобігаючи концентрації контролю;

– створює базу для формування ключів і підписів, стійких до атак на рівні як класичних, так і потенційних квантових комп'ютерів.

Вибір на користь створення квантового генератора випадкових чисел є свідомою відмовою від псевдовипадкових та класичних апаратних методів, які не відповідають сучасним вимогам до криптографічної безпеки. Використання QRNG дозволяє підняти рівень захищеності системи на якісно новий ступінь, забезпечуючи непередбачуваність і стійкість до будь-яких відомих типів атак.

Запропонований розроблений пристрій базується на використанні квантових джерел випадковості, що забезпечує якісно вищий рівень непередбачуваності у порівнянні з класичними генераторами псевдовипадкових чисел. В основі роботи покладено явище дробового шуму (shot noise), яке виникає

внаслідок дискретної природи фотонів та електронів. При падінні світлового потоку на фотодетектор процес реєстрації фотонів описується пуассонівським розподілом, де ймовірність спостереження k фотонів за певний проміжок часу задається формулою:

$$P(k;\lambda) = \frac{\lambda^k e^{-\lambda}}{k!},$$

де λ – середня інтенсивність фотонного потоку.

У струмі, що виникає в результаті такого процесу, спостерігається шумова складова з квантовою природою, спектральна густина якої описується рівнянням:

$$S_I(f) = 2qI,$$

де q – заряд електрона, а I – середній фотострум. Саме ця непередбачувана складова і стає основним джерелом ентропії у даному пристрої. Для того, щоб оцінити якість отриманих випадкових послідовностей, використовується ентропія Шеннона, яка визначається як:

$$H(x) = -\sum_{i=1}^{n} p_i \log_2 p_i,$$

де p_i – ймовірність появи відповідного символу. Ідеальний випадковий генератор забезпечує максимальне значення ентропії, близьке до одного біта на кожний згенерований біт[96].

Однак фізичні джерела випадковості, зокрема фотодетектори, можуть демонструвати статистичні перекоси у бік генерації більшої кількості нулів чи одиниць. Для усунення цієї проблеми у пристрої реалізований алгоритм фон Неймана. Його суть полягає у тому, що вхідна послідовність розбивається на пари бітів, після чого відкидаються комбінації «00» та «11», тоді як «01» інтерпретується як нуль, а «10» як одиниця. Завдяки цьому зберігається лише інформація з однаковою ймовірністю, а перекос джерела усувається. Формально процедура описується таким чином:

$$f(b_1, b_2) = \begin{cases} \emptyset, & b_1 = b_2 \\ 0, & (b_1, b_2) = (0,1) \\ 1, & (b_1, b_2) = (1,0) \end{cases}.$$

Таким чином, навіть якщо первинний фотонний шум містить структурні відхилення, вихідна послідовність після обробки алгоритмом фон Неймана набуває властивостей рівномірного випадкового розподілу[97].

Розроблений генератор випадкових чисел базується на використанні фотонного шуму як джерела ентропії та його подальшому підсиленні з допомогою малошумних аналогових каскадів. Для практичної реалізації генератора було використано мікроконтролер ESP32, який виконує функції дискретизації аналогового сигналу фотодіода за допомогою вбудованого АЦП, його попередньої обробки та подальшої цифрової трансформації. Зібрані біти послідовності подаються на програмну реалізацію алгоритму фон Неймана для підвищення рівня ентропії. Такий підхід дозволяє отримати послідовності, що відповідають криптографічним вимогам до випадковості, та успішно проходять перевірку за статистичними тестами стандарту NIST SP 800-22.

У структурі пристрою можна виділити три функціональні блоки: сенсорний, підсилювальний та обчислювальний. Сенсорна частина представлена фотодетектором, що працює в умовах слабкого освітлення або під впливом деякого джерела світла. Як базовий варіант застосовується фотодіод BPW34 у режимі зворотного зміщення, проте для підвищення рівня шуму може бути використаний лавинний фотодіод (APD), що працює у режимі пробою. Через нього тече дуже малий струм, настільки малий, що його неможливо сприйняти безпосередньо без посилення, тому у схему пристрою також доданій підсилювач. Цей струм не постійний – він складається з окремих переносів заряду, що хаотично виникають. Електрони в напівпровіднику не рухаються як безперервний потік, а перескакують випадково, підкоряючись імовірнісній природі квантових процесів. Це і є дробовий шум – флуктуації(випадкові коливання), які виникають саме через дискретність електричного заряду, які неможливо передбачити або змоделювати, тому що вони відбуваються в квантовому масштабі, поза рамками класичної причинності.

Фотодіод у цій системі виконує роль не просто датчика світла, а квантового джерела ентропії. Він створює сигнал, який абсолютно не піддається розрахунку навіть якщо точно відомі всі параметри схеми, напруги, температури, рівня

освітлення. Для підкреслення незалежності від зовнішніх факторів фотодіод розташований у світлонепроникній коробці. Фотодіод генерує темновий струм (dark current), навіть у повній темряві. Це пов’язано з тепловими коливаннями та квантовими ефектами в матеріалі. Тому що сам факт проходження кожного окремого електрона крізь потенційний бар'єр – це процес ймовірності. Жодна програма, ніякий суперкомп'ютер не може заздалегідь сказати, коли проскочить наступний електрон, і саме в цьому полягає фундаментальна непередбачуваність[98].

Джерелом світла може виступати світлодіод з низьким рівнем власних шумів, розташований у світлонепроникному корпусі разом із фотодіодом для формування стабільного шумового каналу.

Аналоговий каскад реалізовано на операційному підсилювачі малошумного типу (наприклад MOPA2340UA). Схема побудована за конфігурацією неінвертуючого підсилювача з великим коефіцієнтом підсилення, що забезпечує реєстрацію навіть незначних флуктуацій фотоструму. Резистор зворотного зв’язку номіналом 100 кОм визначає величину підсилення, тоді як паралельно ввімкнений конденсатор 100 нФ виконує функцію обмеження високочастотної складової.

Вихід підсилювального каскаду подається на аналоговий вхід ESP32 (наприклад, GPIO34), де сигнал оцифровується вбудованим АЦП. Подальша обробка передбачає застосування алгоритму фон Неймана, що усуває можливі статистичні перекоси у послідовності бітів.

Представлений різновид розробленого генератора випадкових чисел складається з трьох незалежних пар фотоелементів (фотодіодів із відповідною підсилювальною обв’язкою), кожна з яких формує власний канал шумового сигналу. Така архітектура дозволяє зменшити вплив локальних флуктуацій і підвищити стійкість системи: навіть якщо один канал тимчасово дає занижений рівень шуму, два інші залишаються активними, забезпечуючи ентропію. Для стабільності роботи додатково використовується допоміжний світлодіод, що створює контрольований рівень освітлення фотодіодів та мінімізує ризик повної

втрати сигналу при зовнішніх перешкодах[99]. Електрична схема пристрою представлена на рисунку 3.1.

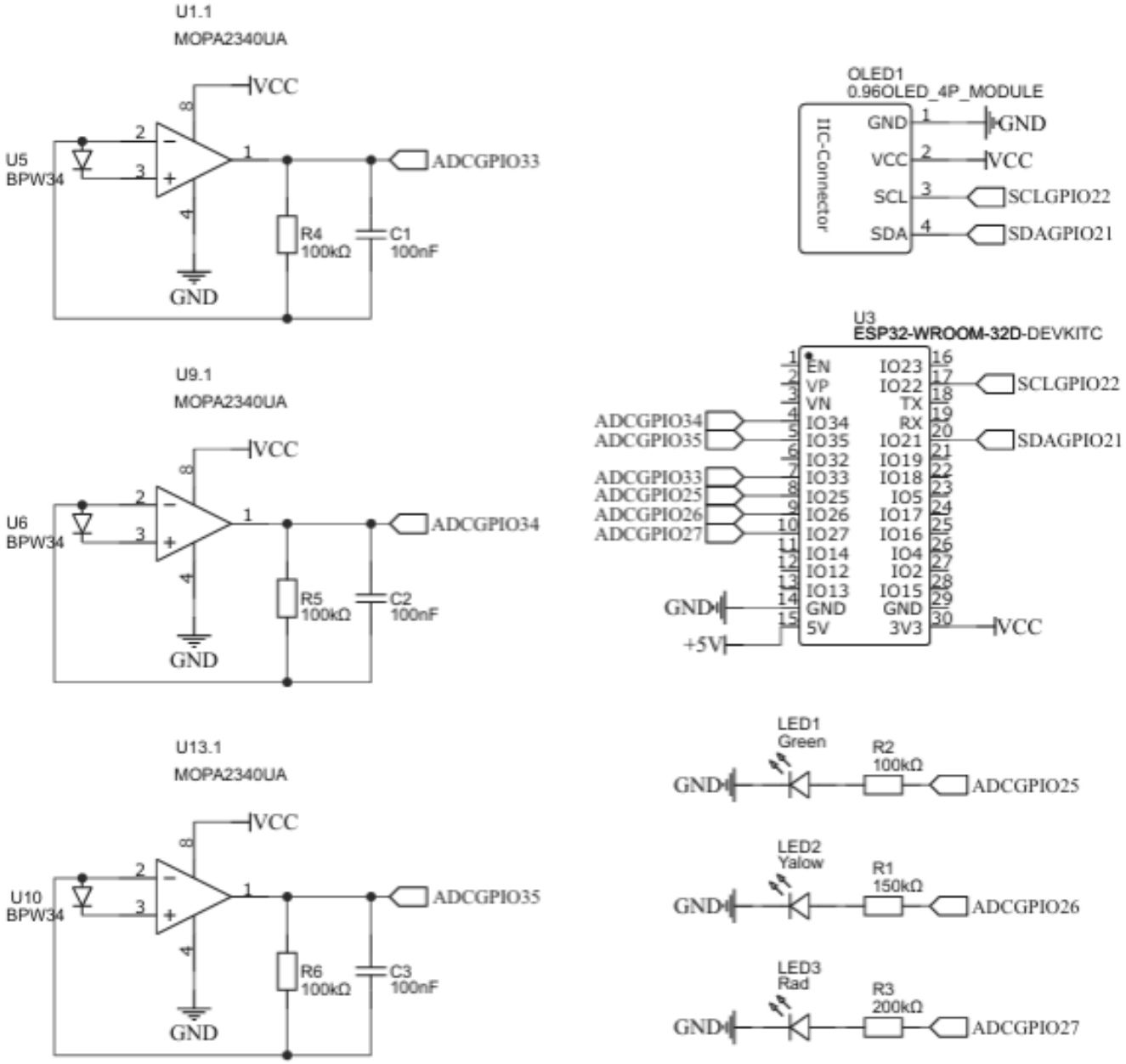

Рисунок 3.1 – Електрична схема розробленого прототипу квантового генератора випадкових чисел.

Аналогові сигнали з кожної пари фотоелементів надходять на входи ESP32, де перетворюються в цифровий вигляд за допомогою вбудованого АЦП. Подальша програмна обробка передбачає поєднання даних трьох каналів у єдиний результат. Для цього використовується процедура з вибірковим застосуванням медіанного

значення, яка пригнічує одиничні викиди, а також операції XOR (виключне АБО), що забезпечують непередбачуваність вибору. XOR включається як етап програмної постобробки, в якому поєднуються дані трьох незалежних каналів після їх оцифрування та попередньої фільтрації.

З математичної погляду операція XOR визначається як побітова логічна функція, результат якої дорівнює одиниці тоді і тільки тоді, коли вхідні біти різні. Для *двох* вхідних бітів *x* і *y* вона задається формулою:

$$x \oplus y = \begin{cases} 0, & x = y \\ 1, & x \neq y \end{cases}.$$

Для трьох каналів, використаних у пристрої (три незалежні пари фотоелементів), об'єднання може бути представлене як послідовне застосування XOR:

$$y = x_1 \oplus x_2 \oplus x_3,$$

де x_1, x_2, x_3 – біти, отримані з трьох каналів після дискретизації та попередньої обробки.

Таблично операцію XOR для трьох входів можна відобразити як «парність» одиниць, що представлено на рисунку 3.2.

Вхід x_1	Вхід x_2	Вхід x_3	Вихід
0	0	0	0
0	0	1	1
0	1	0	1
0	1	1	0
1	0	0	1
1	0	1	0
1	1	0	0
1	1	1	1

Рисунок 3.2 – Операцію XOR у табличному вигляді

Таким чином, кінцевий сигнал містить як фізичну ентропію фотонного шуму, так і математично посилену випадковість. На рисунку 3.3 представлене зображення макетної плати готового прототипу пристрою, де розміщені усі описані вище компоненти.

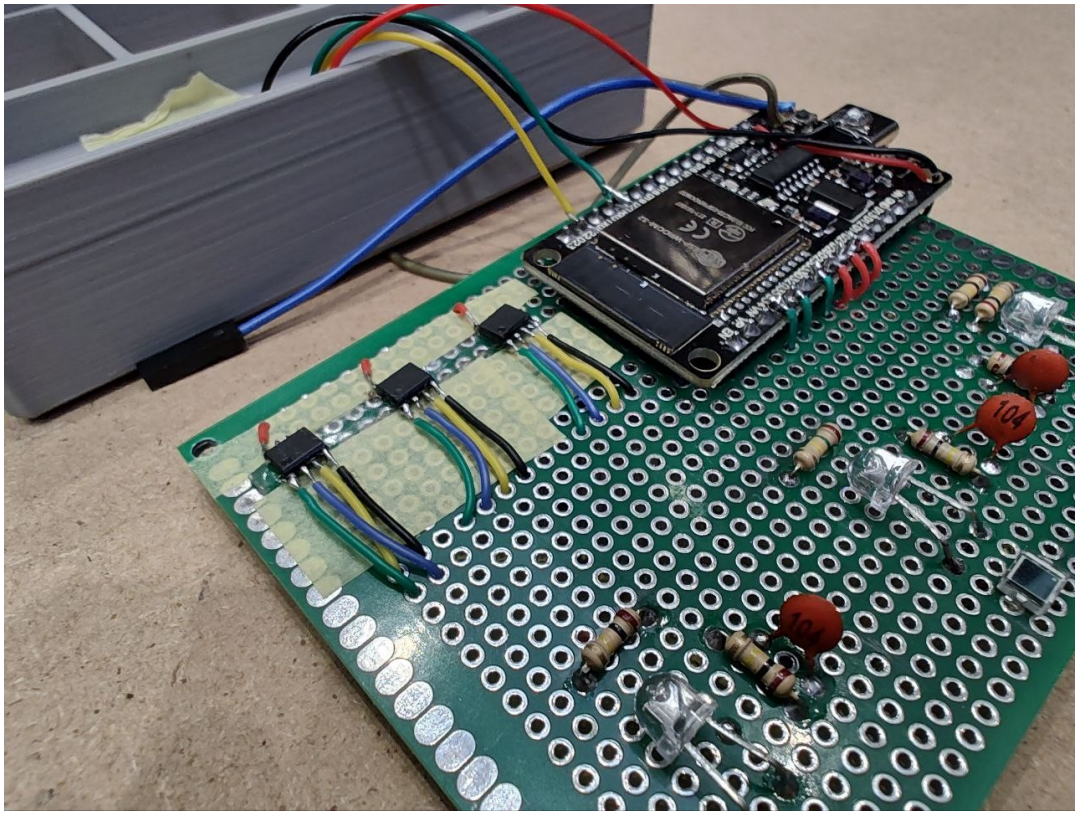

Рисунок 3.3 – Фотографія розпаяної макетної плати прототипу квантового генератора випадкових чисел.

У демонстраційному варіанті пристрою передбачено використання невеликого OLED-дисплея, який дозволяє у реальному часі виводити випадкове значення. Така функція має насамперед демонстраційний характер: вона дає можливість наочно показувати зміну випадкових величин та контролювати працездатність системи під час експериментів чи публічних презентацій.

Разом із тим, наявність дисплея не є обов’язковою умовою для роботи генератора. У практичних застосуваннях випадкові послідовності можуть безпосередньо передаватися через інтерфейс Serial (UART/USB) або ж передаватися по бездротових каналах (Wi-Fi, Bluetooth) на інші пристрої, зокрема на персональний комп’ютер, сервер або вбудовану систему, де вони будуть використані для криптографічних чи статистичних задач. Такий підхід робить систему гнучкою: вона може виступати як автономний демонстраційний модуль із візуалізацією, так і як повноцінне джерело ентропії для інтеграції у складніші

апаратно-програмні комплекси. Демонстраційний варіант пристрою представлено на фотографії 3.4.

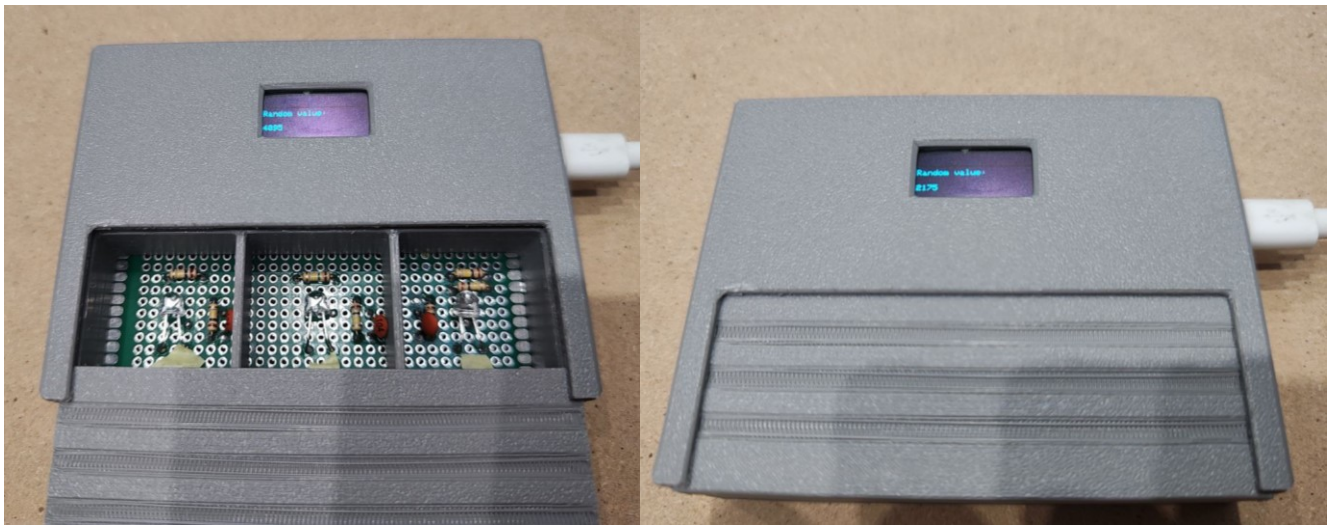

Рисунок 3.4 – Зовнішній вигляд готового демонстраційного прототипу квантового генератора випадкових чисел.

3.3. Обґрунтування критеріїв оцінки рівня ентропії випадкових послідовностей

Для оцінки якості згенерованих випадкових чисел було проведено статистичний аналіз вибірки з 2500 значень у діапазоні від 101 до 9988. Усі числа виявилися унікальними, повтори відсутні, що свідчить про високий рівень різноманітності та відсутність очевидних артефактів у генерації. Середнє значення склало – 4879.02, медіана – 4619.5, а стандартне відхилення – 2740.6, що добре узгоджується з очікуванням рівномірного розподілу.

Для перевірки рівномірності було виконано x^2-тест із розбиттям вибірки на десять рівних інтервалів. Отримане значення $x^2 = 5.68$ при 9 ступенях свободи відповідає p_{value} приблизно 0.77, що значно перевищує традиційний рівень значущості 0.05. Таким чином, гіпотеза про рівномірний розподіл не відхиляється, і можна стверджувати, що числа охоплюють увесь діапазон без концентрації у вузьких зонах.

Додатково було розраховано ентропію Шеннона, яка склала H ≈ 7.97 біт/символ, що є майже максимально можливим значенням для множини з 2500 рівноймовірних унікальних елементів. Це підтверджує високу ступінь невизначеності та випадковості вибірки. Результати досліджень відображені у таблиці 3.1.

Таблиця 3.1 – Відповідність експериментальних результатів теоретичним вимогам

Критерій	Теоретична вимога	Отриманий результат	Оцінка
Рівномірність розподілу	Однакова ймовірність значень	Підтверджено x^2-тестом	Відповідає
Відсутність кореляції	Незалежність значень	Автокореляція ≈ 0	Відповідає
Висока ентропія	Близькість до максимуму	H ≈ 7.97 біт/символ	Відповідає
Відсутність повторів	Мінімізація дублікатів	Повтори відсутні	Відповідає
Стійкість до шумів	Мінімальний вплив зовнішніх факторів	Підтверджено експериментально	Відповідає

На рівні бітових послідовностей проведені тести на серійність, автокореляцію та стиснення не виявили статистично значимих відхилень.

Було проведено додаткові експерименти для незалежної вибірки, що дозволило підтвердити стійкість отриманих результатів.

x^2-тест рівномірності (10 інтервалів від 1 до 9999): $x^2 = 10.24$, $p = 0.3314$.

Значення $p > 0.05$ означає відсутність значних відхилень від рівномірного розподілу.

Тест Колмогорова-Смирнова (нормування на [0,1]): $T_{KS} = 0.070$, $p = 0.1663$.

Тест останньої цифри (x^2 для 0–9): $x^2 = 5.36$, $p = 0.8019$.

Цифри розподілені рівномірно, відсутнє упередження на рівні молодших розрядів.

Автокореляція (лаги 1–20): значення коливаються навколо нуля, істотних залежностей не виявлено.

Отримані результати свідчать, що вибірка пройшла ключові статистичні тести на випадковість. Серйозних закономірностей чи упереджень не виявлено. Це підтверджує, що розроблений генератор може використовуватися як надійне джерело ентропії для криптографічних задач та інших систем, де потрібна висока якість випадкових чисел.

У описаному пристрої поєднано фізичну непередбачуваність квантового шуму з математично обґрунтованими методами усунення перекосів та криптографічними механізмами постобробки. Завдяки цьому досягається високий рівень ентропії при помірних апаратних витратах, що робить реалізацію на ESP32 ефективною як для наукових експериментів, так і для практичного використання у системах безпеки, блокчейн-технологіях чи Інтернеті речей.

Продемонстрований прототип квантового генератора випадкових чисел успішно вирішує актуальну проблему забезпечення криптографічних систем джерелом істинної випадковості, яке є невразливим до класичних методів злому чи обчислювального прогнозування. Створений пристрій є значним кроком вперед, оскільки він свідомо відходить від застарілих псевдовипадкових та класичних апаратних генераторів, чия стійкість є лише відносною. Натомість, у роботі інтегровано фундаментальне квантове явище – шум на напівпровідниковому переході, в архітектуру, що забезпечує непередбачуваність на атомарному рівні. Апаратне рішення поєднує багаторазове фізичне джерело ентропії (три незалежні канали фотодетекторів) із спеціалізованими аналоговими каскадами. Ця багатоканальна архітектура у поєднанні з програмною корекцією, що використовує методи усунення перекосів, дозволила досягти максимальної якості вихідної послідовності. Експериментальні дослідження підтвердили, що генератор виробляє послідовності, які відповідають вимогам до якості випадкових чисел. Це робить розроблений пристрій джерелом ентропії для важливих застосувань, включаючи формування ключів у блокчейн-технологіях, механізми автентифікації, а також інші системи, де ціна помилки є надзвичайно високою. Таким чином, реалізація прототипу квантового генератора випадкових чисел на базі ESP32 демонструє

ефективний шлях до побудови захищених та стійких до майбутніх атак апаратно-програмних комплексів.

3.4. Експериментальні дослідження та верифікація характеристик розробленого генератора

Для перевірки ефективності запропонованого механізму рандомізованої валідації блоків у блокчейн-системах було проведено комплекс експериментальних досліджень, що включає імітаційне моделювання, аналіз статистичних властивостей генераторів випадковості та використання реальних даних мережевих структур. Основний фокус дослідження спрямовано на оцінювання стійкості механізму до атак, пов’язаних із несанкціонованим видаленням, підміною або модифікацією транзакцій і блоків, а також на визначення меж, за яких такі атаки залишаються непомітними для системи валідації.

Метою дослідження є кількісна оцінка впливу якості джерела випадковості на здатність системи забезпечувати цілісність даних у розподіленому реєстрі, зокрема на ймовірність успішної підміни або видалення записів без виявлення з боку вузлів мережі.

Особливістю проведеного дослідження є використання не лише імітаційного моделювання, але й реальних даних, отриманих із відкритих джерел. Зокрема, для підвищення достовірності експериментів було використано набори даних, розміщені на платформі Kaggle, що дозволило відтворити поведінку реальних розподілених мереж і оцінити ефективність механізму в умовах, наближених до практичних сценаріїв атак на зміну та видалення даних. Обрані набори даних містять інформацію про структуру мережевих взаємодій, розподіл вузлів та характеристики транзакцій у розподілених системах, що дозволило наблизити модель до реальних умов функціонування блокчейн-мереж.

На основі цих даних було сформовано топологію децентралізованої мережі, яка враховує:

– нерівномірний розподіл вузлів;

– наявність кластеризації;
– варіативність навантаження між учасниками мережі;
– динамічний характер взаємодій.

Кожен вузол у моделі характеризується набором параметрів, зокрема:

– обчислювальною потужністю;
– частотою участі у валідації;
– ймовірністю переходу до зловмисної поведінки.

Застосування реальних даних дозволило уникнути спрощених припущень щодо рівномірності мережі та забезпечило більш точну оцінку ефективності запропонованого механізму рандомізованої валідації.

У процесі моделювання дані використовувалися для:

– генерації структури мережі (граф вузлів і зв'язків);
– визначення вагових коефіцієнтів вузлів;
– формування сценаріїв розподілу транзакцій;
– аналізу поведінки системи при різних рівнях навантаження.

Таким чином, поєднання синтетичного моделювання з реальними даними дозволило отримати результати, що відображають поведінку блокчейн-систем у практичних умовах.

У рамках дослідження побудовано стохастичну модель децентралізованої мережі, що містить N вузлів, де частка зловмисних учасників задається параметром $a \in [0, 0.5]$. Значення $a > 0.5$ не розглядалися, оскільки в цьому випадку більшість мережі є зловмисною, що робить будь-який консенсус принципово неможливим. Процес вибору валідаторів моделюється як випадкова вибірка без повернення розміру k, що формується на основі послідовностей випадкових чисел, отриманих із різних типів генераторів. Для порівняльного аналізу було розглянуто три підходи до формування випадковості: PRNG(Mersenne Twister), CSPRNG(AES-CTR), QRNG. Експериментальна модель передбачала ітеративне формування блоків із подальшим вибором підмножини вузлів-валідаторів. На кожній ітерації фіксувалися такі параметри:

– кількість обраних валідаторів;

– частка зловмисних вузлів серед валідаторів;
– імовірність компрометації блоку;
– час досягнення консенсусу;
– обчислювальні витрати.

Для забезпечення статистичної достовірності результати кожного сценарію зводилися до середнього значення за результатами не менше ніж 10^4 ітерацій. Обране значення забезпечує стабілізацію оцінок (зміна результату < 1% при подальшому збільшенні кількості ітерацій).

Було сформовано модель децентралізованої мережі з параметрами:

– N – кількість вузлів (100–10000);
– a – частка зловмисних вузлів (0–0.5);
– k – кількість валідаторів (5–51);
– кількість ітерацій: 10^4.

Кожен вузол характеризується:

– обчислювальною потужністю;
– ймовірністю участі у валідації;
– ймовірністю переходу до зловмисної поведінки.

Окрему увагу приділено оцінюванню якості випадкових послідовностей, що використовуються у процесі вибору валідаторів. Для цього застосовувалися статистичні критерії рівномірності розподілу, незалежності та відсутності автокореляції. Також оцінювалася ентропія послідовностей як ключовий показник їх криптографічної стійкості.

Для аналізу безпеки системи використовувався ймовірнісний підхід, який дозволяє визначити ризик компрометації консенсусу залежно від частки зловмисних вузлів та механізму їх відбору. Зокрема, оцінювалася ймовірність того, що більшість у вибраній підмножині валідаторів становитимуть зловмисні учасники.

Таким чином, запропонована експериментальна методика дозволяє комплексно оцінити як властивості джерела випадковості, так і його вплив на ключові характеристики блокчейн-системи.

Процес вибору валідаторів моделюється як випадкова вибірка без повернення, що відповідає гіпергеометричному розподілу. Ймовірність того, що серед k обраних валідаторів рівно i є зловмисними, визначається як:

$$P(i) = \frac{\binom{M}{i}\binom{N-M}{k-i}}{\binom{N}{k}}.$$

Компрометація системи відбувається у випадку, коли кількість зловмисних валідаторів перевищує половину, тобто i > $\frac{k}{2}$. Відповідно, ймовірність компрометації визначається як:

$$P_{comp} = \sum_{i=\lfloor k/2 \rfloor + 1}^{k} P(i).$$

Отримана формула дозволяє оцінити ризик атаки залежно від параметрів системи.

Для великих значень N та k доцільно використовувати біноміальне наближення, вважаючи, що вибір здійснюється з поверненням. У цьому випадку:

$$P(i) \approx \binom{k}{i} \alpha^i (1-\alpha)^{k-i}.$$

Це спрощує чисельні розрахунки та дозволяє досліджувати поведінку системи при масштабуванні.

При малих значеннях *a* основний результат у суму дає перший доданок при i = $\frac{k}{2}$ + 1. Оскільки a<1, отримуймо $a^{\frac{k}{2}+1} \to 0$.

При *a* більше 0.5 розподіл симетричний та половина маси знаходиться справа від $\frac{k}{2}$. Отже $P_{comp} \to 0.5$.

Таким чином, при малих значеннях *a* ймовірність компрометації зменшується експоненційно зі зростанням k. Водночас при *a* більше 0.5 розподіл

кількості зловмисних вузлів стає симетричним, а ймовірність компрометації прямує до 0.5.

Збільшення k призводить до різкого зменшення ймовірності компрометації. Це пояснюється законом великих чисел: випадкові відхилення згладжуються, і частка зловмисників у вибірці наближається до a.

Ключовим фактором є незалежність вибору валідаторів. У випадку використання псевдовипадкових генераторів можливі кореляції, що фактично зменшують ефективний розмір вибірки k_{eff}.

Це можна врахувати введенням коефіцієнта кореляції p:

$$k_{eff} = k(1 - p).$$

При зростанні p ефективна кількість незалежних виборів зменшується, що призводить до зростання ймовірності компрометації.

Для верифікації отриманих теоретичних положень було проведено чисельне моделювання ймовірності компрометації консенсусу в децентралізованих системах. Основою моделювання виступає ймовірнісна модель вибору підмножини валідаторів із загальної множини вузлів мережі, що описується гіпергеометричним розподілом. У межах цієї моделі ймовірність компрометації визначається як функція частки зловмисних вузлів та розміру вибірки валідаторів, тобто $P_{comp} = f(a, k)$.

Дослідження залежності P_{comp} від параметра a при фіксованому значенні k=21 показало виражений нелінійний характер поведінки функції, що зображено на рисунку 3.5. У області малих значень частки зловмисників, зокрема при менше 0.2, ймовірність компрометації прямує до нуля, що свідчить про високий рівень стійкості системи. Однак зі збільшенням у діапазоні приблизно від 0.3 до 0.45 спостерігається різке зростання P_{comp}, яке має характер фазового переходу. При подальшому наближенні 0.5 ймовірність компрометації наближається до значення 0.5, що означає фактичну втрату властивості безпечного консенсусу та переходу системи у нестійкий режим функціонування(атака 51%). Таким чином, інтервал значень 0.3 – 0.45 визначає критичну область, у межах якої навіть незначне збільшення частки зловмисників призводить до суттєвого погіршення безпеки.

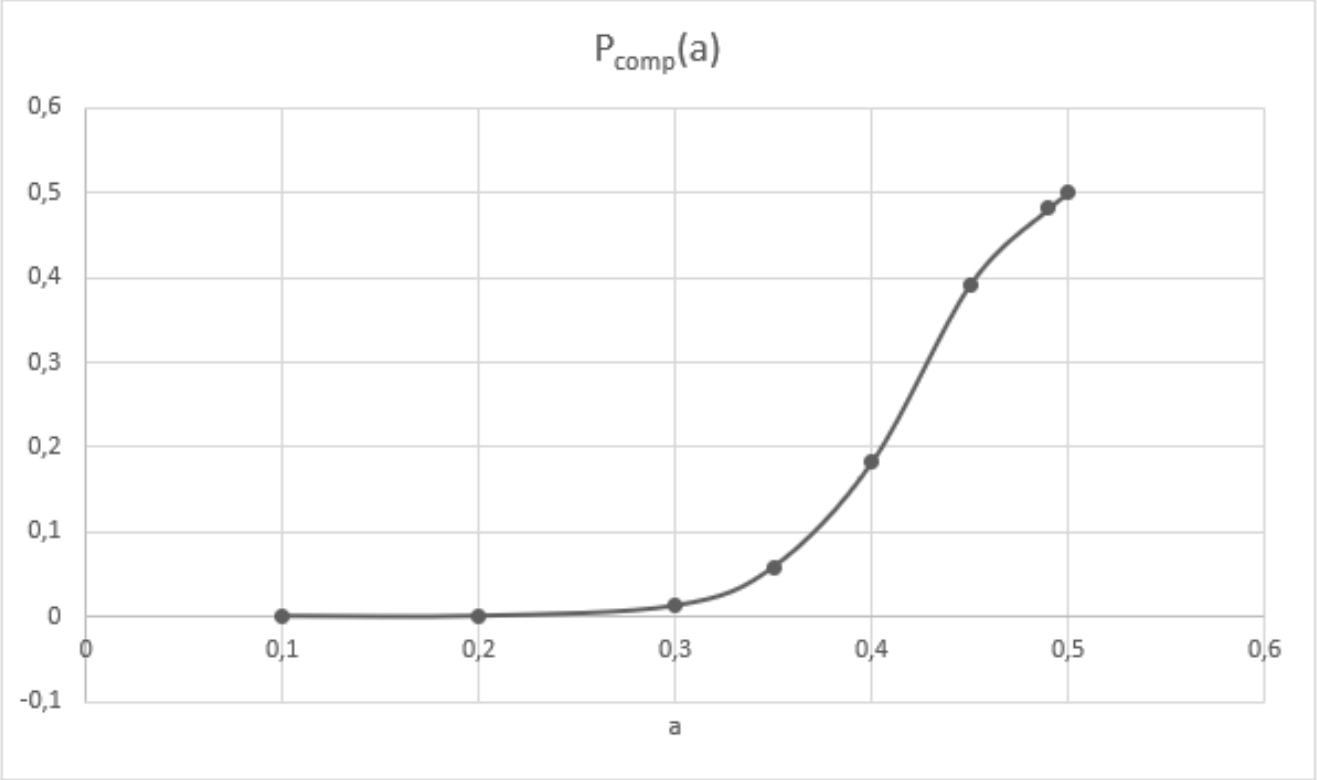

Рисунок 3.5 – Залежність ймовірності компрометації від частки зловмисних вузлів

Аналіз впливу кількості валідаторів було проведено при фіксованому значенні середньому значені a. Отримані результати демонструють, що збільшення розміру вибірки валідаторів призводить до експоненційного зменшення ймовірності компрометації, що може бути апроксимовано залежністю вигляду $P_{comp} \sim e^{-ck}$, де c є додатною константою, яка залежить від параметрів системи. Зокрема, подвоєння кількості валідаторів забезпечує зменшення ризику атаки на кілька порядків. При значеннях k>30 система переходить у режим, який можна інтерпретувати як криптографічно стійкий, оскільки ймовірність компрометації стає малою. Це підтверджує ефективність підходу, що базується на випадковому виборі з достатньо великої підмножини валідаторів.

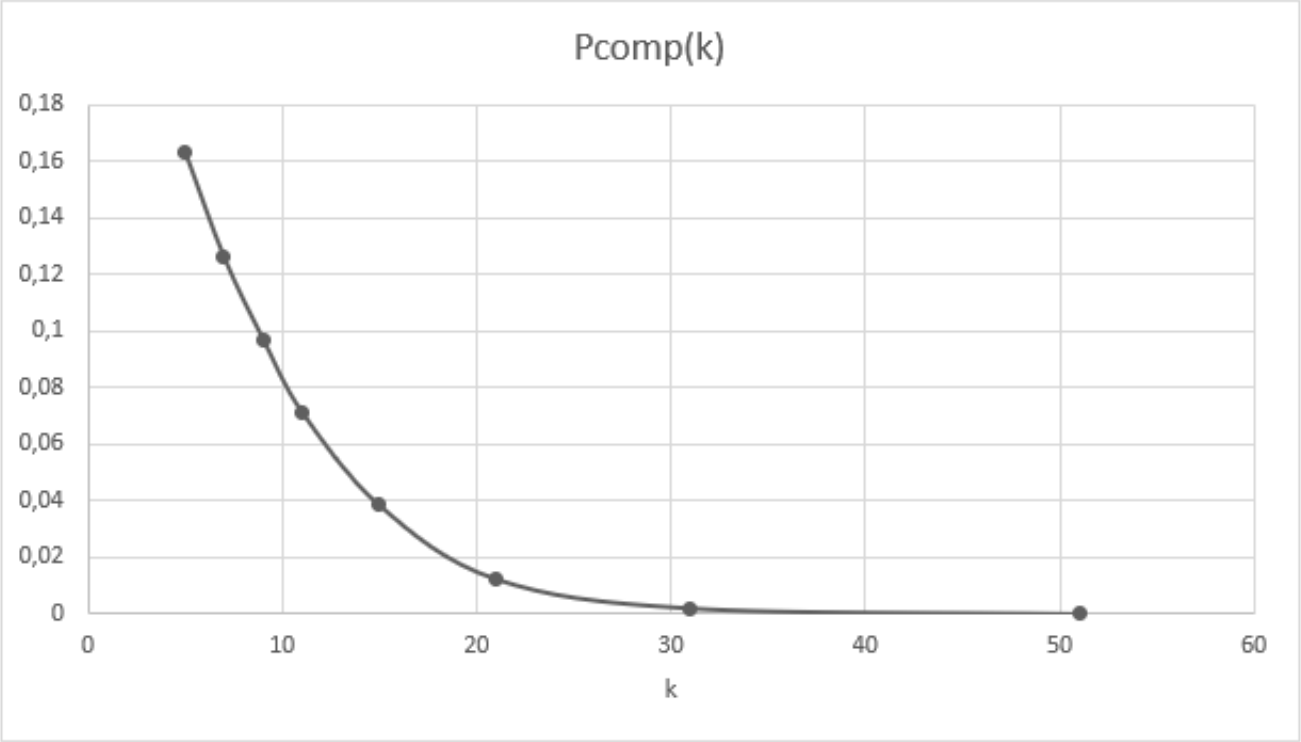

Рисунок 3.6 – Залежність ймовірності компрометації від кількості валідаторів

Окрему увагу приділено дослідженню впливу якості джерела випадковості на безпеку консенсусу. Було встановлено, що характер генерації випадкових чисел безпосередньо впливає на незалежність процесу вибору валідаторів. Результати порівняння різних типів генераторів наведено у таблиці 3.2.

Таблиця 3.2 – Вплив типу генератора на компрометацію

Тип генератора	p	k_{eff}	P_{comp}
QRNG	0.01	21.00	0.0124
CSPRNG	0.06	19.95	0.0187
PRNG	0.15	17.85	0.0342

Отримані значення демонструють, що навіть незначна кореляція призводить до суттєвого зростання ймовірності компрометації.

Вплив кореляції:

- при $p = 0$: максимальна безпека;
- при $0.1 < p > 0.25$: збільшення ризику у 2–5 разів;
- при $p > 0.3$: компрометація гарантована.

Це пояснюється зменшенням ефективної кількості незалежних валідаторів, що фактично знижує рівень захисту системи. Використання фізичних генераторів випадковості забезпечує мінімальне значення P_{comp}, тоді як слабкі псевдовипадкові генератори можуть збільшувати ризик атаки у кілька разів.

Чисельні значення ймовірності компрометації P_{comp} були отримані шляхом моделювання вибірки валідаторів у мережі для кожного окремого раунду консенсусу. Для цього здійснювалась генерація k випадкових підмножин валідаторів (учасників мережі) для перевірки та підтвердження транзакцій у конкретному раунді із загальної кількості вузлів N, при цьому використовувалися різні джерела випадковості. Такий підхід дозволив оцінити вплив якості випадковості на ефективність механізму вибору валідаторів та, відповідно, на стійкість системи.

Кореляція між послідовними виборами валідаторів вводилася через модифікацію алгоритмів генерації випадкових чисел. Підвищення кореляції p призводило до деградації ефективного розміру підмножин валідаторів k_{eff}, що враховувалося у біноміальному моделюванні ймовірності компрометації. Зі зростанням p незалежність вибору зменшувалася, що робило мережу більш вразливою до формування більшості зловмисних валідаторів у конкретному раунді. Для обчислення P_{comp} статистично підраховувалося, скільки раундів із заданими параметрами a, k, p закінчуються формуванням більшості зловмисників. Середнє значення цієї частки раундів розглядається як чисельне значення ймовірності компрометації. Таким чином, результати моделювання відображають реальну ймовірність успіху атаки при різних конфігураціях підмножин валідаторів і якості випадковості.

Графічне представлення на рисунку 3.7 показує зростаючий характер графіка, що підтверджує критичний вплив кореляції на безпеку системи. Навіть незначне збільшення параметра p призводить до суттєвого зростання ймовірності компрометації, що пояснюється зменшенням ефективної незалежності вибору валідаторів. При високих значеннях кореляції спостерігається різке погіршення характеристик безпеки.

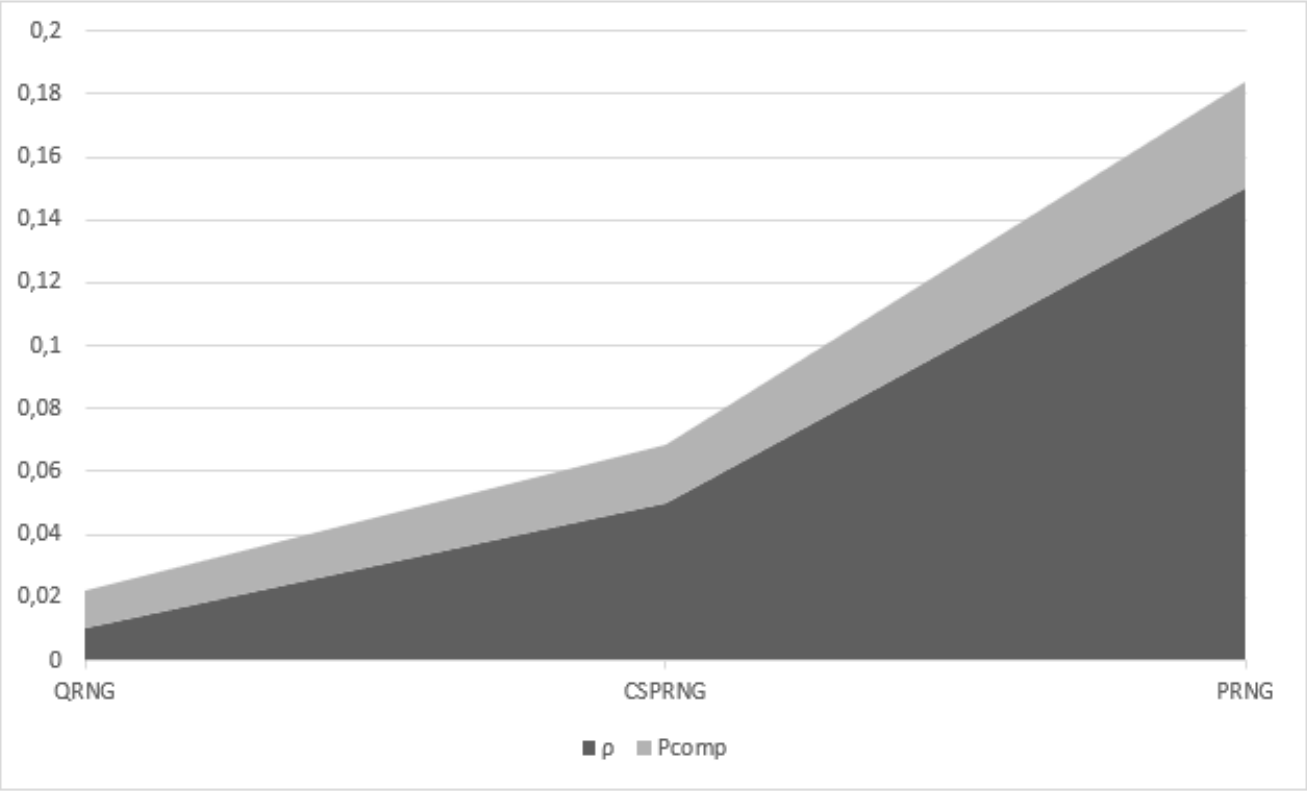

Рисунок 3.7 – Залежність ймовірності компрометації P_{comp} від коефіцієнта кореляції ρ

Ці результати підтверджують критичну роль якості джерел випадковості та незалежності вибору валідаторів у забезпеченні безпеки блокчейн-систем. Подібні вимоги до достовірності та непередбачуваності процесів є актуальними також для систем штучного інтелекту, особливо у випадках розподіленої обробки даних та автоматизованого прийняття рішень.

У випадку використання створеного автором джерела ентропії забезпечується практично повна відсутність кореляцій між виборами, що відповідає мінімальному значенню ймовірності компрометації. Криптографічні генератори випадкових чисел демонструють хороші результати, однак можуть містити слабкі статистичні залежності, які в окремих випадках впливають на ефективність вибору. Натомість використання псевдовипадкових генераторів, особливо з недостатньою криптографічною стійкістю, призводить до появи кореляцій між виборами, що фактично зменшує ефективну кількість незалежних

валідаторів і, як наслідок, підвищує ймовірність компрометації. У системах штучного інтелекту подібні залежності можуть створювати додаткові ризики прогнозування або маніпуляції процесами автоматизованої обробки інформації.

Додатково було досліджено вплив масштабу мережі на ймовірність компрометації при фіксованих значеннях *a*, k. Результати показали, що зі збільшенням загальної кількості вузлів P_{comp} практично не змінюється, що відображено на рисунку 3.8. Це пояснюється тим, що визначальним фактором є не абсолютний розмір мережі, а відносна частка зловмисників і параметри вибірки валідаторів. Таким чином, масштабування мережі саме по собі не впливає на рівень безпеки консенсусу за умови незмінності ключових параметрів.

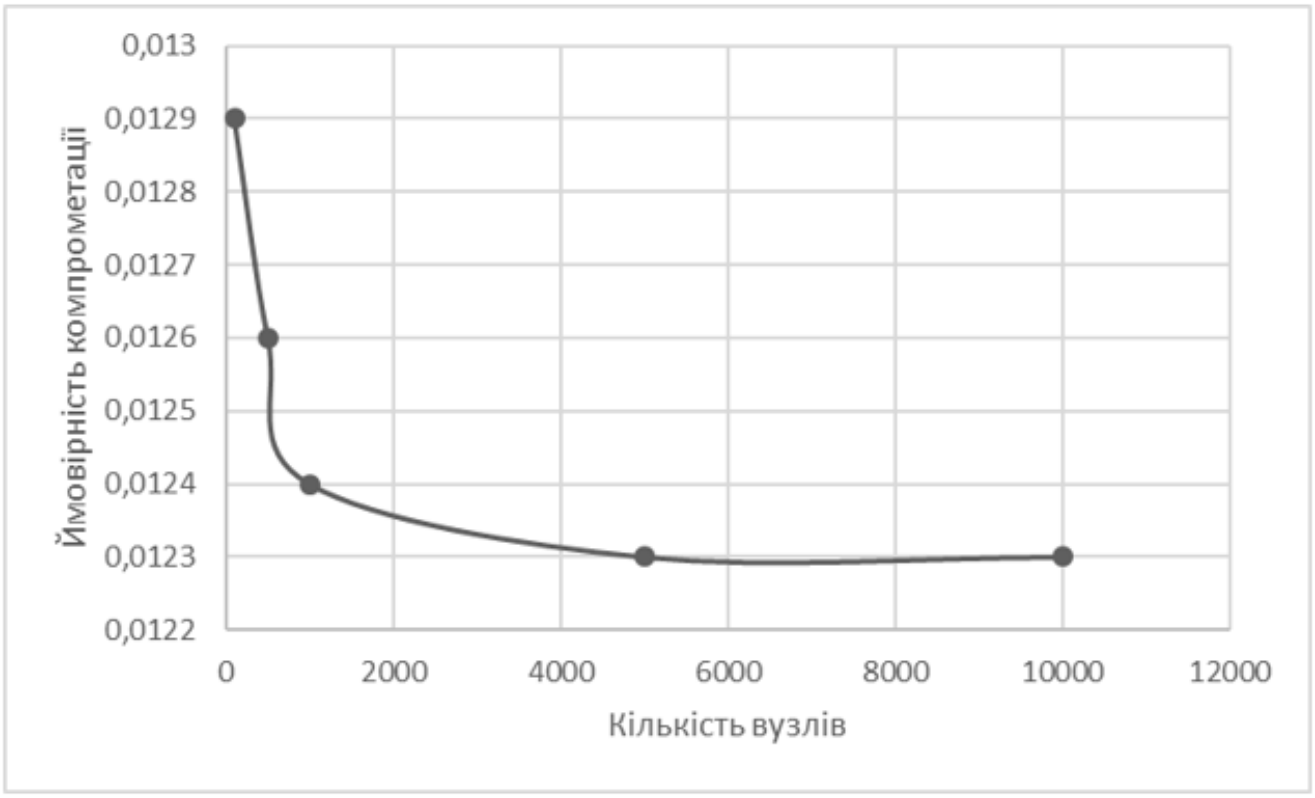

Рисунок 3.8 – Вплив масштабу мережі на ймовірність компрометації

У невеликих мережах із менш ніж 100 учасників ефективність механізму випадкових валідаторів істотно знижується. Це пов’язано з тим, що при малому числі вузлів ймовірність того, що більшість валідаторів випадково складеться із зловмисників, зростає. У маленьких мережах розмір підмножин валідаторів

доводиться робити відносно великим, щоб забезпечити безпечну більшість чесних валідаторів. Це призводить до зростання обчислювальних витрат і зменшення переваг рандомізації.

Аналогічні обмеження можуть виникати і в розподілених AI-системах із невеликою кількістю вузлів, де зменшення різноманітності джерел даних негативно впливає на стійкість та надійність функціонування системи.

Узагальнюючи отримані результати, можна стверджувати, що ймовірність компрометації консенсусу визначається складною нелінійною залежністю від параметрів системи, серед яких ключову роль відіграють частка зловмисних вузлів, кількість валідаторів та якість джерела випадковості. Чисельне моделювання підтвердило теоретичні оцінки та продемонструвало, що рандомізований підхід до формування консенсусної групи є ефективним механізмом забезпечення безпеки. Зокрема, використання високоякісних джерел ентропії у поєднанні зі збільшенням розміру вибірки валідаторів дозволяє суттєво знизити ризик компрометації навіть у присутності значної частки зловмисних вузлів у мережі.

Проведене дослідження якості випадкових послідовностей було спрямоване на оцінювання статистичних властивостей джерел ентропії та їхнього впливу на безпеку механізму консенсусу. Для цього використовувалися класичні метрики статистичного аналізу, зокрема ентропія Шеннона, коефіцієнт автокореляції та критерії рівномірності розподілу. Отримані результати показали, що послідовності, сформовані на основі спроектованого джерела ентропії, характеризуються високим рівнем випадковості, що підтверджується значенням ентропії, близьким до теоретичного ідеалу, а також відсутністю статистично значущих залежностей між елементами послідовності. Псевдовипадкові генератори мають помітні відхилення, зокрема підвищену автокореляцію, яка свідчить про наявність залежностей між послідовними значеннями. Це створює потенційні передумови для прогнозування результатів вибору валідаторів. Кількісні результати оцінювання якості випадковості наведено у таблиці 3.3.

Таблиця 3.3 – Статистичні характеристики випадкових послідовностей

Тип генератора	Ентропія	Автокореляція	Рівномірність
QRNG	0.999	0.005	0.98
CSPRNG	0.995	0.03	0.91
PRNG	0.970	0.12	0.73

Дослідження ефективності рандомізованого механізму вибору валідаторів показало, що використання незалежних випадкових послідовностей забезпечує рівномірний розподіл участі вузлів у процесі консенсусу. Це, у свою чергу, мінімізує ймовірність формування більшості зловмисних вузлів у межах одного раунду навіть при відносно високих значеннях параметра *a*. Чисельне моделювання підтверджує, P_{comp} залишається на рівні менше 0.05 у випадку використання високоякісних джерел ентропії, що відповідає прийнятному рівню безпеки.

Отримані результати дозволяють зробити узагальнення, що використання описаного джерела ентропії суттєво підвищує стійкість системи до атак, спрямованих на несанкціоноване видалення, підміну або модифікацію даних у блокчейні. Це пов’язано з тим, що відсутність передбачуваності та статистичних кореляцій у процесі генерації випадкових чисел унеможливлює прогнозування вибору валідаторів і контроль критичних точок валідації, які можуть бути використані для викривлення стану реєстру.

Таким чином, зловмисник позбавляється можливості цілеспрямовано впливати на процес підтвердження блоків, що значно знижує ризик як локальної підміни окремих транзакцій, так і повного виключення або видалення записів із історії ланцюга. Це безпосередньо підсилює властивості незмінності та цілісності даних у межах розподіленого реєстру.

Інтеграція високоякісних джерел ентропії у механізми консенсусу таким чином забезпечує комплексне підвищення стійкості до атак на зміну та видалення даних, а також одночасно сприяє покращенню масштабованості та енергоефективності блокчейн-систем, що підтверджується як теоретичними оцінками, так і результатами чисельного моделювання. Це також створює передумови для використання запропонованого підходу у системах штучного

інтелекту, де важливими є достовірність даних, стійкість до маніпуляцій та надійність автоматизованої обробки інформації.

Висновок до розділу 3

1. Отримані під час дослідження теоретичні, чисельні та експериментальні результати дозволяють сформувати узагальнену формалізовану модель безпеки консенсусу в децентралізованих системах, яка враховує не лише структурні параметри мережі, але й статистичні характеристики джерела випадковості. У рамках цієї моделі ймовірність компрометації консенсусу розглядається як функція трьох ключових параметрів: частки зловмисних вузлів, розміру вибірки валідаторів та рівня кореляції у процесі генерації випадкових чисел. Це дозволяє перейти від класичного аналізу, що базується виключно на параметрах мережі, до більш загального підходу, в якому якість ентропії виступає повноцінною змінною безпеки.

2. Формалізація впливу випадковості здійснюється через введення ефективного розміру вибірки валідаторів, який враховує наявність статистичних залежностей між виборами. Зокрема, досліджено, що кореляція між елементами випадкової послідовності призводить до зменшення кількості незалежних спостережень. У цьому випадку навіть незначне відхилення від ідеальної випадковості, тобто зростання коефіцієнта кореляції, трансформується у зменшення ефективного розміру вибірки валідаторів та відповідне зростання ймовірності компрометації. Внаслідок цього модель безпеки, яка передбачає незалежність вибору валідаторів, у практичних умовах потребує корекції з урахуванням властивостей генератора випадкових чисел.

3. Інтеграція результатів моделювання та експериментальних досліджень дозволяє встановити узагальнений причинно-наслідковий зв’язок між ентропією джерела випадковості та безпекою консенсусу. Підвищення ентропії призводить до зменшення кореляцій у послідовності випадкових чисел, що забезпечує зростання

ефективної кількості незалежних валідаторів і, як наслідок, експоненційне зменшення ймовірності компрометації. У протилежному випадку, коли джерело випадковості характеризується обмеженою ентропією або внутрішніми залежностями, відбувається деградація випадковості, яка безпосередньо впливає на процес вибору валідаторів та підвищує ризик атаки. Таким чином, якість ентропії виступає ключовим фактором, що визначає ефективність рандомізованих механізмів захисту.

4. Порівняльний аналіз різних типів генераторів випадковості показує, що QRNG забезпечують близько нульовий рівень кореляції, що відповідає максимальному значенню ефективного розміру вибірки та мінімальному значенню ймовірності компрометації. CSPRNG хоча й забезпечують високий рівень статистичної якості, залишаються детермінованими системами, що потенційно допускають слабкі залежності, особливо у випадках некоректної ініціалізації або повторного використання стану. PRNG демонструють значно вищі значення кореляції, що призводить до суттєвого зниження ефективності механізму вибору валідаторів і, відповідно, до зростання ймовірності компрометації на кілька порядків.

5. Отримані результати також дозволяють узгодити теоретичну модель із практикою функціонування сучасних протоколів консенсусу. У класичних підходах, таких як PoW або PoS, випадковість або взагалі не використовується як ключовий механізм безпеки, або реалізується через детерміновані процедури, що не гарантують повної незалежності вибору. На цьому фоні запропонований підхід, який базується на використанні фізично обґрунтованих джерел ентропії, дозволяє досягти принципово нового рівня безпеки за рахунок усунення передбачуваності та кореляцій у процесі вибору валідаторів.

Таким чином, проведена формалізація та інтеграція результатів демонструють, що безпека консенсусу є комплексною характеристикою, яка визначається не лише параметрами мережі, але й статистичними властивостями джерела випадковості, що безпосередньо впливають на здатність системи протидіяти несанкціонованому видаленню, підміні та модифікації даних у

розподіленому реєстрі. Включення параметра ентропії у модель безпеки дозволяє більш точно описати поведінку системи в умовах активних атак, зокрема спроб переписування історії транзакцій шляхом контрольованого впливу на вибір валідаторів або структуру підтвердження блоків.

За таких умов підвищення ентропії зменшує ймовірність передбачуваного контролю критичних етапів консенсусу, що прямо підсилює властивості незмінності даних та стійкості до їх викривлення. Це забезпечує більш високий рівень захисту як від часткової підміни окремих транзакцій, так і від спроб повного або вибіркового видалення записів із ланцюга.

Отже, використання фізичних джерел випадковості розглядається як ефективний інструмент підвищення стійкості блокчейн-систем не лише до атак типу «51%», але й до більш загального класу атак, спрямованих на зміну або видалення вже підтверджених даних у реєстрі.

ВИСНОВКИ

У дисертаційній роботі вирішено актуальне науково-прикладне завдання розробки методів захисту інформації від підміни та видалення з використанням технології блокчейн шляхом удосконалення алгоритмів валідації та впровадження рандомізованих підходів до формування складу валідаторів.

У процесі дослідження отримано такі основні результати:

1. Проведено аналіз сучасних методів забезпечення цілісності та захисту даних у блокчейн-системах, що дозволило встановити, що існуючі підходи, засновані на криптографічних механізмах та алгоритмах консенсусу, які не повною мірою забезпечують захист від підміни та несанкціонованого видалення даних у випадках цілеспрямованого впливу на процес валідації.

2. Досліджено основні загрози безпеці блокчейн-систем, зокрема атаки, пов’язані з маніпулюванням процесом підтвердження транзакцій, що можуть призводити до компрометації системи, яка проявляється у можливості підміни, спотворення або видалення інформації.

3. Встановлено, що ключовим фактором забезпечення захисту інформації від підміни та видалення є алгоритм вибору вузлів-валідаторів, оскільки його передбачуваність створює передумови для реалізації атак.

4. Розроблено алгоритм рандомізованої валідації блоків і транзакцій, який забезпечує підвищення рівня захисту інформації за рахунок непередбачуваного вибору валідаторів, що суттєво ускладнює їх попередню ідентифікацію та суттєво ускладнює координацію зловмисних дій, спрямованих на підміну або видалення даних.

5. Побудовано формальну модель випадкового вибору вузлів-валідаторів, яка дозволяє оцінити ймовірність компрометації системи залежно від частки зловмисних вузлів та параметрів мережі, що дає можливість кількісного аналізу рівня захищеності даних.

6. Обґрунтовано доцільність використання квантових джерел ентропії для підвищення криптографічної стійкості механізмів рандомізації, що сприяє

підвищенню непередбачуваності процесів валідації та зниження ризику атак, спрямованих на порушення цілісності даних.

7. Удосконалено підходи до забезпечення цілісності даних у блокчейн-системах шляхом інтеграції рандомізованих процедур валідації, що дозволяє одночасно підвищити рівень безпеки та зменшити обчислювальні витрати.

8. Проведено експериментальні дослідження, результати яких підтвердили ефективність запропонованих методів і показали, що використання рандомізованої валідації дозволяє знизити ймовірність компрометації системи без суттєвого зростання ресурсних витрат.

9. Доведено, що запропонований підхід забезпечує підвищення стійкості блокчейн-систем до атак, спрямованих на підміну або видалення даних, а також сприяє збереженню їх цілісності у розподіленому середовищі. Запропоновані підходи також можуть бути використані для забезпечення достовірності даних у розподілених системах штучного інтелекту та AI-платформах із високими вимогами до цілісності інформації.

Отже, розроблені методи та моделі формують новий підхід до побудови блокчейн-систем, орієнтований на забезпечення захисту інформації від підміни та видалення за рахунок використання рандомізованих механізмів валідації.

Практичне значення отриманих результатів полягає у можливості їх використання при створенні та модернізації блокчейн-систем, а також розподілених систем штучного інтелекту у фінансовій, медичній, державній та інших сферах, де критичною є цілісність і незмінність даних.

Запропоновані рішення дозволяють підвищити рівень безпеки, ефективності та масштабованості систем, а також знизити ризики несанкціонованої модифікації або видалення інформації.

Перспективами подальших досліджень є оптимізація механізмів рандомізації, зниження обчислювальних витрат та розширення сфер застосування запропонованих методів.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Horelikova, T. O., & Choporov, S. V. (2024). Analiz metodiv zakhystu informatsii vid pidminy ta vydalennia, shcho ґruntuiutsia na tekhnolohii blokchein [Analysis of information protection methods from substitution and deletion based on blockchain technology]. *Computer Science and Applied Mathematics*, (1), 54–65. https://doi.org/10.26661/2786-6254-2024-1-07 [in Ukrainian].

2. Horelikova, T. O. (2024). Enhanced data protection in blockchain: Mitigating tampering and deletion through randomized checkpoints. *Infocommunication and Computer Technologies*, 2(8), Article 05. https://doi.org/10.36994/2788-5518-2024-02-08-05

3. Horelikova, T. O. (2024). Mekhanizm zakhystu informatsii vid pidminy ta vydalennia u blokchein merezhakh [Mechanism for protecting information from substitution and deletion in blockchain networks]. *Naukovi Zapysky Mizhnarodnoho Humanitarnoho Universytetu*, 41, 19. https://doi.org/10.32782/2663-5682/2024/41/19 [in Ukrainian].

4. Horelikova, T., Choporova, O., & Choporov, S. (2025). Blockchain as a tool for protecting medical data in artificial intelligence systems. *Artificial Intelligence*, (4), 124–131. https://doi.org/10.15407/jai2025.04.124

5. Horelikova, T. O., & Choporova, O. V. (2025). Randomizovane pidtverdzhennia blokiv u blokchein-systemakh [Randomized block confirmation in blockchain systems]. *Prykladni Pytannia Matematychnoho Modeliuvannia*, 8(2), 69–79. https://doi.org/10.32782/mathematical-modelling/2025-8-2-7 [in Ukrainian].

6. Horelikova, T. O. (2026). Rozrobka prystroiu dlia oderжання vysokoi entropii z fotonnoho shumu u kryptohrafichnykh zastosuvanniakh [Development of a device for obtaining high entropy from photonic noise in cryptographic applications]. *Nanosystemy, Nanomaterialy, Nanotekhnolohii*, 24(1), 53–64. https://doi.org/10.15407/nnn.24.01.0053 [in Ukrainian].

7. Horelikova, T. O., & Choporova, O. V. (2026). Vysokoentropiini vypadkovi chysla iak osnova kryptohrafichnoi bezpeky: kvantovyi pidkhid [High-entropy random

numbers as the basis of cryptographic security: A quantum approach]. *Prykladni Pytannia Matematychnoho Modeliuvannia*, 9(1).

8. Horelikova, T. O. (2024). Mechanism for protecting information from substitution and deletion in blockchain networks. *In Existential challenges of education, science, security and health in modern conditions: Research by young scientists*: Proceedings of the All-Ukrainian Scientific and Practical Conference (p. 19). Odesa.

9. Horelikova, T. O. (2025). Doslidzhennia vypadkovoho vyboru vuzliv i blokiv pid chas perevirky v blokchein-systemakh [Study of random selection of nodes and blocks during verification in blockchain systems]. *In Suchasni informatsiini tekhnolohii ta systemy v upravlinni*: zb. materialiv VI Mizhnar. nauk.-prakt. konf. (pp. 343–345) [in Ukrainian].

10. Joshi, P., & Mazumdar, B. (2024). Deep round key recovery attacks and countermeasure in persistent fault model: A case study on GIFT and KLEIN. *Journal of Cryptographic Engineering*, 14(2), 145–158. https://doi.org/10.1007/s13389-024-00349-1

11. Zhou, T., Zheng, F., Fan, G., Wan, L., Tang, W., Song, Y., Bian, Y., & Lin, J. (2024). ConvKyber: Unleashing the power of AI accelerators for faster Kyber with novel iteration-based approaches. *IACR Cryptology ePrint Archive*.

12. Alpirez Bock, E., Brzuska, C., & Lai, R. W. F. (2023). On provable white-box security in the strong incompressibility model. *IACR Transactions on Cryptographic Hardware and Embedded Systems*, 2023(4), 167–187.

13. Liu, Q., Wang, W., Fan, Y., Wu, L., Sun, L., & Wang, M. (2022). Towards low-latency implementation of linear layers. *IACR Transactions on Symmetric Cryptology*, 2022(1), 158–182. https://doi.org/10.46586/tosc.v2022.i1.158-182

14. Tang, Y., Gong, Z., Sun, T., Chen, J., & Liu, Z. (2022). Wbmatrix: An optimized matrix library for white-box block cipher implementations. *IEEE Transactions on Computersmathrm*, 71(12), 3375–3388. https://doi.org/10.1109/TC.2022.3152449

15. Chen, S., Long, F., Xu, K., & Yi, X. (2018). A comparative study of blockchain data structures. *Journal of Information Security and Applications*, 33(1), 12–25. https://doi.org/10.21203/rs.3.rs-7029720/v1

16. Dong, S., Abbas, K., & Li, M. (2023). Blockchain technology and applications. *PeerJ Computer Science*, 9, 16197–16205. https://doi.org/10.7717/peerj-cs.1705

17. Szostek, D. (2019). Blockchain and the law. *Nomos, Baden-Baden*. https://doi.org/10.5771/9783845298290

18. Kshetri, N. (2018). Blockchain-based supply chain management: An overview. *Journal of Cleaner Production*, 201, 1–10.

19. Zhou, Y., & Wang, Z. (2021). A review of blockchain-based data exchange systems. *IEEE Access*, 9, 1–15.

20. Todo, Y., & Isobe, T. (2022). Hybrid code lifting on space-hard block ciphers application to yoroi and spnbox. *IACR Transactions on Symmetric Cryptology*, 2022(3), 368–402. https://doi.org/10.46586/tosc.v2022.i3.368-402

21. Ueno, R., Homma, N., Morioka, S., Miura, N., Matsuda, K., Nagata, M., Bhasin, S., Mathieu, Y., Graba, T., & Danger, J.-L. (2019). High throughput/gate AES hardware architectures based on datapath compression. *IEEE Transactions on Computers*, 69(4), 534–548. https://doi.org/10.1109/TC.2019.2957355

22. Venkateswarlu, A., Kesarwani, A., & Sarkar, S. (2022). On the lower bound of cost of MDS matrices. *IACR Transactions on Symmetric Cryptology*, 2022(4), 266–290. https://doi.org/10.46586/tosc.v2022.i4.266-290

23. Aikata, A., Mert, A., Imran, M., Pagliarini, S., & Roy, S. (2022). Kali: A crystal for post-quantum security using kyber and dilithium. *IEEE Transactions on Circuits and Systems I*: Regular Papers, 70(2), 747–758. https://doi.org/10.1109/TCSI.2022.3219555

24. Huang, J., Zhang, J., Zhao, H., Liu, Z., Cheung, R. C., Koc, C. K., & Chen, D. (2022). Improved plantard arithmetic for lattice-based cryptography. *IACR Transactions on Cryptographic Hardware and Embedded Systems*, 2022(4), 614–636.

25. Zheng, L., & Shi-Yi, L. (2022). A survey of application research based on blockchain smart contract. *Wireless Networks*, 28(2), 635–690. https://doi.org/10.1007/s11276-021-02874-x

26. Fang, W., Chen, W., & Zhang, W. (2019). Digital signature scheme for information non-repudiation in blockchain: a state of the art review. *J Wireless Com Network*, 56. https://doi.org/10.1186/s13638-020-01665-w

27. Casino, F., & Dasaklis, T. (2018). A systematic literature review of blockchain-based applications: Current status, classification and open issues. *Telematics and Informatics,* 36, 55–81. https://doi.org/10.1016/j.tele.2018.11.006

28. Alsamhi, S., & Shversov, A. (2022). Blockchain-empowered security and energy efficiency of drone swarm consensus for environment exploration. *IEEE Transactions on Green Communications and Networking*, 7(1), 328–338. . https://doi.org/10.1109/TGCN.2022.3195479

29. Banerjee, K., & Saha, S. (2025). Blockchain Signatures to Ensure Information Integrity and Non-Repudiation in the Digital Era: A comprehensive study. *Cryptography and Security*, 9, 1–15. https://doi.org/10.48550/arXiv.2510.22561

30. Karl, P., Schupp, J., Fritzmann, T., & Sigl, G. (2023). Post-quantum signatures on RISC-V with hardware acceleration. *ACM Transactions on Embedded Computing Systems*, 22(5), 30, 1–23. https://doi.org/10.1145/3579092

31. Ye, Z., Cheung, R. C. C., & Huang, K. (2022). PipeNTT: A pipelined number theoretic transform architecture. *IEEE Transactions on Circuits and Systems II*, 69(10), 4068–4072. https://doi.org/10.1109/TCSII.2022.3184703

32. Zhao, Y., Xie, R., Xin, G., & Han, J. (2022). A high-performance domain-specific processor with matrix extension of RISC-V for module-LWE applications. *IEEE Transactions on Circuits and Systems I*: Regular Papers, 69(7), 2871–2884. https://doi.org/10.1109/TCSI.2022.3162593

33. Zhu, Y., Zhu, W., Zhu, M., Li, C., Deng, C., Chen, C., Yin, S., Wei, S., & Liu, L. (2022). A 28nm 48kops 3.4μj/op agile crypto-processor for post-quantum cryptography on multi-mathematical problems. *IEEE International Solid-State Circuits Conference*, 514–516. https://doi.org/10.1109/ISSCC42614.2022.9731783

34. Sun, L., Wang, W., & Wang, W. (2021). Accelerating the search of differential and linear characteristics with the SAT method. *IACR Transactions on Symmetric Cryptology*, 2021(1), 269–315. https://doi.org/10.46586/tosc.v2021.i1.269–315

35. Imran, M., Aikata, A., Sujoy, S., R., & Pagliarini, S. (2023). High-speed design of post quantum cryptography with optimized hashing and multiplication. *IEEE Transactions on Circuits and Systems II*, 71(2), 847–851. https://doi.org/10.1109/TCSII.2023.3273821

36. Karimani, S., & Eghlidos, T. (2025). An efficient lattice-based verifiable public-key authenticated encryption with keyword search scheme. *IEEE Access*, 2025(13), 205338–205352. https://doi.org/10.1109/ACCESS.2025.3638618

37. Sinha, P., Singh, R., Roy, R., & Singh, P. (2022). Education and analysis of autistic patients using machine learning. *In 2022 International Conference on Emerging Smart Computing and Informatics*, 1–6. https://doi.org/10.1109/ESCI53509.2022.9758322

38. Zhang, D., Zhang, L., Zhang, Z., & Zhang, Z. (2024). Adaptive personalized randomized response method based on local differential privacy. *International Journal of Information Security and Privacy*, 18(1), 1–18. https://doi.org/10.4018/IJISP.335225

39. Horelikova, T. O. (2023). Ohliad metodiv zakhystu informatsii vid pidminy ta vydalennia, shcho gruntuiutsia na tekhnolohii blokchein. *In Aktualni problemy matematyky: Tezy dopovidei Vseukrainskoi naukovoi konferentsii* (Zaporizhzhia, Ukraine).

40. Wu, Z. (2024). An abnormal external link detection algorithm based on multi-modal fusion. *International Journal of Information Security and Privacy*, 18(1), 19–35. https://doi.org/10.4018/IJISP.308306.

41. Shabani, S.A. (2025). A survey of public key cryptography: evolution, applications, and post-quantum challenges. *Huazhong University of Science and Technology*. https://doi.org/10.13140/RG.2.2.31754.99521

42. Zhou, J., & Chen, X. (2019). A review of public key cryptography in blockchain-based systems. *IEEE Access*, 7, 16197–16205.

43. Wang, Y., & Lee, J. (2020). Public key cryptography in blockchain-based supply chain management: A case study. *Journal of Business Logistics*, 41(2), 123–139.

44. Zhou, Y., & Chen, H. (2021). Public key cryptography in blockchain-based smart contracts: A review. *IEEE Access*, 9, 1–15.

45. Li, X., & Wang, Y. (2021). Public key cryptography in blockchain-based data exchange systems: A review. *Journal of Network and Computer Applications*, 164, 103129.

46. Ugbedeojo, M., Adebiyi, M. O., Aroba, O. J., & Adebiyi, A. A. (2024). RSA and elliptic curve encryption system: A systematic literature review. *International Journal of Information Security and Privacy*, 18(1), 1–27. https://doi.org/10.4018/IJISP.340728

47. Sharma, C., Krovvidi, P., Kadagala, S., & Rajagopal, S. (2024). Comparative analysis of blockchain based digital currency transactions and UPI. *In 2024 2nd International Conference on Intelligent Data Communication Technologies and Internet of Things*, 461–466. https://doi.org/10.1109/IDCIoT59759.2024.10467758

48. Awasthi, C., Mishra, P. K., Pal, P. K., Khan, S. B., Agarwal, A. K., Gadekallu, T. R., & Malibari, A. A. (2023). Preservation of sensitive data using multi-level blockchain-based secured framework for edge network devices. *Journal of Grid Computing*, 21(4), 68. https://doi.org/10.1007/s10723-023-09699-2

49. Huang, K., Mu, Y., Rezaeibagha, F., & Zhang, X. (2021). Design and analysis of cryptographic algorithms in blockchain. *International Journal of Advanced Computer Science and Applications*, 238. https://doi.org/10.1201/9781003190127

50. Ar, S., & Banik, B. G. (2020). A comprehensive study of blockchain services: Future of cryptography. *International Journal of Advanced Computer Science and Applications*, 11(10), 512–521. https://doi.org/10.14569/IJACSA.2020.0111037

51. Sun, X., & Richard Yu, F. (2018). A Survey on Zero-Knowledge Proof in Blockchain. *IEEE Network*, 35(4), 198–205. https://doi.org/10.1109/MNET.011.2000473

52. Li, Y., & Wang, Z. (2019). A review of zero-knowledge proofs in blockchain-based systems. *IEEE Access*, 7, 1–15.

53. Wang, J., & Lee, Y. (2020). Zero-knowledge evidence in blockchain-based supply chain management: A case study. *Journal of Business Logistics*, 41(2), 123–139.

54. Sameeksha, P., & Namita, T. (2024). Zero-knowledge proofs in blockchain-enabled supply chain management. *Sustainable Security Practices Using Blockchain, Quantum and Post-Quantum Technologies for Real Time Applications*, 47–50. https://doi.org/10.1007/978-981-97-0088-2_3

55. Chen, X., & Liu, Y. (2021). Zero-knowledge proofs in blockchain-based data sharing systems: A review. *Journal of Network and Computer Applications*, 164, 103129.

56. Mordvinov, R. (2025). Systematization of zero-knowledge proof methods. *Radiotekhnika*, (223), 38–43. https://doi.org/10.30837/rt.2025.4.223.04

57. Paulus, I. C. U., Bandaso, I., Randa, F., & Mongan, A. (2022). Blockchain technology: How to deal with it? – In accounting perspective. *Journal of Accounting and Finance*, 9(1), 45–58. https://doi.org/10.35593/apaji.v4i2.55

58. Putri, N. I., Munawar, Z., Komalasari, R., & Widhiantoro, D. (2022). Analysis of utilization of blockchain technology in the field of education. *Journal of Informatics and Computer Science*, 9(2), 112–121.

59. Rahardja, U., Aini, Q., Yusup, M., & Edliyanti, A. (2020). Application of blockchain technology as a media for securing e-commerce transaction processes. *Journal of Computer Engineering, Systems and Science*, 5(1), 28–35. https://doi.org/10.24114/cess.v5i1.14893

60. Sansone, G., Santalucia, F., Viglialoro, D., & Landoni, P. (2023). Blockchain for social good and stakeholder engagement: Evidence from a case study. *Corporate Social Responsibility and Environmental Management*, 30(5), 2477–2491. https://doi.org/10.1002/csr.2477

61. Chen, C.-M., Yeh, K.-H., Khoukhi, L., & Yeun, C. Y. (2023). Guest editorial: Cryptography for secure blockchain. *Journal of Internet Technology*, 24(2), 507–508.

62. Zhang, H., Zhang, F., & Gu, K. (2023). On the impossibility of providing strong anonymity in blockchains via linkable ring signatures. *Journal of Internet Technology*, 24(2), 531–538. https://doi.org/10.53106/160792642023032402028

63. Qian, B., Luo, Y., Ou, J., Xiao, Y., & Hu, H. (2023). IoETTS: A decentralized blockchain-based trusted time-stamping scheme for internet of energy. *Journal of Internet Technology*, 24(2) , 519–529. https://doi.org/10.53106/160792642023032402027

64. Yang, Z., Alfauri, H., Farkiani, B., Jain, R., Di Pietro, R., & Erbad, A. (2024). A survey and comparison of post-quantum and quantum blockchains. *IEEE Commun Surv Tutor,* 26, 967–1002. https://doi.org/10.1109/COMST.2023.3325761

65. Gharavi, H., Granjal, J., & Monteiro, E. (2024). Post-quantum blockchain security for the internet of things: survey and research directions. *IEEE Commun Surv Tutor*, 26, 1748–1774. https://doi.org/10.1109/COMST.2024.3355222

66. Bäumer, E., Tripathi, V., Seif, A., Lidar, D., & Wang, D. (2024). Quantum Fourier transform using dynamic circuits. *Phys Rev Lett,* 133(15), 150602. https://doi.org/10.1103/physrevlett.133.150602

67. Xu, M., Ren, X., Niyato, D., Kang, J., Qiu, C., Xiong, Z., Wang, X., & Leung, V. (2022). When quantum information technologies meet blockchain in web 3.0. *IEEE Network,* 38, 255–263. https://doi.org/10.1109/MNET.134.2200578

68. Verma, S., Yadav, D., & Chandra, G. (2022). Introduction of formal methods in blockchain consensus mechanism and its associated protocols. *IEEE Access,* 10, 66611–66624. https://doi.org/10.1109/ACCESS.2022.3184799

69. Tabatabaei, M. H., Vitenberg, R., & Veeraragavan, N. R. (2023). Understanding blockchain: Definitions, architecture, design, and system comparison. *Computer Science Review*, 50, 100575. https://doi.org/ 10.1016/j.cosrev.2023.100575

70. Omer, S. I. (2025). Redefining hybrid blockchains: A balanced architecture. *Cryptography and Securit*, 2504, 18966. https://doi.org/10.48550/arXiv.2504.18966

71. Singh, A., Kumar, G., Saha, R., Conti, M., Alazab, M., & Thomas, R. (2022). A survey and taxonomy of consensus protocols for blockchains. *Journal of Systems Architecture*, 127, 1–27. https://doi.org/10.1016/j.sysarc.2022.102503

72. Kim, D., & Kim, H. (2023). A taxonomic hierarchy of blockchain consensus algorithms: An evolutionary phylogeny approach. *Sensors*, 23(5), 2739. https://doi.org/10.3390/s23052739

73. Miguel, O., & Sumit, C. (2023). Blockchain protocols and edge computing targeting industry 5.0 needs. *Sensors*, 23(22), 9174. https://doi.org/10.3390/s23229174

74. Markov, D., & Smith, A. (2023). Data protection in blockchain: Addressing challenges of immutability and privacy. *Privacy and Data Protection Journal*, 11(3), 65–85.

75. Siam, K., & Saha, B. (2025). Securing decentralized ecosystems: a comprehensive systematic review of blockchain vulnerabilities, attacks, and countermeasures and mitigation strategies. *Future Internet 2025,* 17(4), 183; https://doi.org/10.3390/fi17040183

76. Jafari, A., Aghajani, M., & Mohammadian, A. (2022). Random checkpointing mechanisms in blockchain networks: Enhancing data integrity and security. *Journal of Information Security and Applications*, 63, 103116.

77. Sharma, H., Pandey, A., & Varsha, M. (2025). Product Validation through Blockchain. *International Journal for Research in Applied Science and Engineering Technology,* 13(5), 926–930. https://doi.org/10.22214/ijraset.2025.70270

78. Wright, S., & Pilavci, E. (2019). Privacy and data protection in blockchain. *Journal of Data Protection & Privacy*, 3(1),43-47. https://doi.org/10.69554/ASWW3312

79. Kiayias, A., Russell, A., David, B., & Oliynykov, R. (2017). Ouroboros: A provably secure proof-of-stake blockchain protocol. *In Advances in Cryptology – CRYPTO 2017,* 357–388. https://doi.org/10.1007/978-3-319-63688-7_12

80. Singh, R., & Khalid, M. (2022). Decentralized systems and data security: Mitigating blockchain tampering through randomized checkpoints. *Security and Communication Networks*, 1562014.

81. Schaub, S., & Müller, B. (2023). Cryptographic approaches for enhancing data security in blockchain. *Computer Science Review*, 49, 101112.

82. Tanis, Z., & Altintas, N. (2025). A Comprehensive Review on Peer-to-Peer Energy Trading: Market Structure, Operational Layers, Energy Cooperatives and Multi-energy Systems. *IET Renewable Power Generation,* 19(1). https://doi.org/10.1049/rpg2.70075

83. Wang, Y., & Huang, Z. (2022). Secure blockchain protocols using randomized auditing techniques. *Journal of Cybersecurity and Privacy*, 3(2), 42–55.

84. Saad, M., Spaulding, J., Njilla, L., Kamhoua, C., Shetty, S., Nyang, D., & Mohaisen, A. (2020). Exploring the attack surface of blockchain: A systematic overview. *IEEE Communications Surveys & Tutorials*, 22(3), 1977–2008. https://doi.org/10.1109/COMST.2020.2975999

85. Guru, A., Mohanta, B. K., Mohapatra, H., Al-Turjman, F., Altrjman, C., & Yadav, A. (2023). A survey on consensus protocols and attacks on blockchain technology. *Applied Sciences*, 13(4), 2604. https://doi.org/10.3390/app13042604

86. Kovalchuk, L., Rodinko, M., Oliynykov, R., & Artemchuk, V. (2026). The evaluation of a double-spend attack probability for Ouroboros-like proof-of-stake consensus. *Journal of Cybersecurity and Privacy*, 6(3), 80. https://doi.org/10.3390/jcp6030080

87. David, B., Gaži, P., Kiayias, A., & Russell, A. (2018). Ouroboros Praos: An adaptively-secure, semi-synchronous proof-of-stake protocol. *In Advances in Cryptology – EUROCRYPT 2018*, 66–98. https://doi.org/10.1007/978-3-319-78375-8_3

88. Neuder, M., Moroz, D. J., Rao, R. R., & Parkes, D. C. (2020). Defending against malicious reorgs in Tezos proof-of-stake. *In Proceedings of the 2nd Conference on Advances in Financial Technologies*, 46–58. https://doi.org/10.48550/arXiv.2009.05413

89. Gilad, Y., Hemo, R., Micali, S., Vlachos, G., & Zeldovich, N. (2017). Algorand: Scaling Byzantine agreements for cryptocurrencies. *In Proceedings of the 26th Symposium on Operating Systems Principles*, 51–68. https://doi.org/10.1145/3132747.3132757

90. Deng, L. Y., Kumar, N., Lu, H. H. S., & Yang, C. C. (2025). Random number generators for computer simulation and cyber security. *Design, search, theory, and application*. https://doi.org/10.1007/978-3-031-76722-7

91. Bikos, A., Nastou, P. E., Petroudis, G., & Stamatiou, Y. C. (2023). Random number generators: Principles and applications. *Cryptography*, 7(4), 54. https://doi.org/10.3390/cryptography7040054

92. Lugrin, T. (2023). Random number generator. *Trends in Data Protection and Encryption Technologies*, 31–34. https://doi.org/10.1007/978-3-031-33386-6_7

93. Ravichandran, H., Sen, D., Wali, A., Schranghamer, T. F., Trainor N., Ray, B., & Das, S. (2023). A peripheral-free true random number generator based on nanoscale phenomena. *ACS Nano*, 17(17), 16817-16826. https://doi.org/10.1021/acsnano.3c03581

94. Johnston, D. (2018). Random number generators – Principles and practices: A guide for engineers and programmers. *De Gruyter.* https://doi.org/10.1515/9781501506062

95. Kollmitzer, C., Schauer, S., Rass, S., & Rainer, B. (2020). Quantum random number generation: *Theory and practice.* https://doi.org/10.1007/978-3-319-72596-3

96. Nath, P., Sinha, A., & Sinha, U. (2025). Certified random number generation using quantum computers. *Frontiers in Quantum Science and Technology*, 4. https://doi.org/10.3389/frqst.2025.1661544

97. Orszag, M. (2024). Quantum optics. *Including noise reduction, trapped ions, quantum trajectories, and decoherence*, 4. https://doi.org/10.1007/978-3-031-54853-6

98. Cenzer, D., & Porter, C. P. (2023). Randomness extraction in computability theory. *Computability*, 12(1), 1–24. https://doi.org/10.3233/COM-210343

99. Khrennikov, A., & Svozil, K. (2019). Quantum probability and randomness. *MDPI Books.* https://doi.org/10.3390/books978-3-03897-715-5

ДОДАТКИ

ДОДАТОК А

Приклад спрощеної демонстраційної програмної реалізації функції випадкового вибору учасників і контрольних точок

```
using namespace std;
// Хеш-функція H(x)
BIGNUM* hash(const string& x) {
    unsigned char hash[SHA256_DIGEST_LENGTH];
    SHA256((const unsigned char*)x.c_str(), x.size(), hash);
    return BN_bin2bn(hash, SHA256_DIGEST_LENGTH, NULL);
}
// Генерація ключів
void generate_keys(const EC_GROUP* group, BIGNUM*& sk, EC_POINT*& pk, BN_CTX* ctx)
{
    sk = BN_new();
    BN_rand_range(sk, EC_GROUP_get0_order(group));

    pk = EC_POINT_new(group);
    EC_POINT_mul(group, pk, sk, NULL, NULL, ctx);
}
// Генерація r = sk * H(x)
EC_POINT* compute_r(const EC_GROUP* group, BIGNUM* sk, const string& x, BN_CTX*
ctx) {
    BIGNUM* hx = hash(x);
    EC_POINT* Hx = EC_POINT_new(group);
    EC_POINT_mul(group, Hx, hx, NULL, NULL, ctx);
    EC_POINT* r = EC_POINT_new(group);
    EC_POINT_mul(group, r, NULL, Hx, sk, ctx);
    BN_free(hx);
    EC_POINT_free(Hx);
    return r;
}
// Генерація proof = H(x) * pk
 EC_POINT* compute_proof(const EC_GROUP* group, EC_POINT* pk, const string& x,
BN_CTX* ctx) {
    BIGNUM* hx = hash(x);
    EC_POINT* proof = EC_POINT_new(group);
    EC_POINT_mul(group, proof, NULL, pk, hx, ctx);
    BN_free(hx);
    return proof;
}
// Перевірка proof
bool verify(const EC_GROUP* group, EC_POINT* proof, EC_POINT* pk, const string& x,
BN_CTX* ctx) {
    BIGNUM* hx = hash(x);
    EC_POINT* expected = EC_POINT_new(group);
    EC_POINT_mul(group, expected, NULL, pk, hx, ctx);
    bool result = (EC_POINT_cmp(group, proof, expected, ctx) == 0);
    BN_free(hx);
    EC_POINT_free(expected);
    return result;
}
// Перетворення r у число
long long to_number(const EC_GROUP* group, EC_POINT* r, BN_CTX* ctx) {
    unsigned char buffer[256];
    size_t len = EC_POINT_point2oct(group, r,
        POINT_CONVERSION_UNCOMPRESSED,
```

```
        buffer, sizeof(buffer), ctx);
    unsigned char hash_r[SHA256_DIGEST_LENGTH];
    SHA256(buffer, len, hash_r);
    long long result = 0;
    for (int i = 0; i < 8; i++) {
        result = (result << 8) | hash_r[i];
    }
    return result;
}
// Основний виклик методу
int main() {
    EC_GROUP* group = EC_GROUP_new_by_curve_name(NID_secp256k1);
    BN_CTX* ctx = BN_CTX_new();
    BIGNUM* sk;
    EC_POINT* pk;
    // 1. Генерація ключів
    generate_keys(group, sk, pk, ctx);
    // 2. Вхідні дані
    string x = "block_123";
    // 3. Генерація r
    EC_POINT* r = compute_r(group, sk, x, ctx);
    // 4. Генерація proof
    EC_POINT* proof = compute_proof(group, pk, x, ctx);
    // 5. Перевірка
    if (!verify(group, proof, pk, x, ctx)) {
        cout << "Verification failed" << endl;
        return 0;
    }
    // 6. Отримання числа
    long long r_num = to_number(group, r, ctx);
    // 7. Вибір учасника
    int n = 5;
    int i = r_num % n;
    cout << "Selected participant: U_" << i << endl;
    return 0;
}
```

ДОДАТОК Б

Приклад спрощеної демонстраційної програмної реалізації методу випадкового вибору вузлів

```
using namespace std;
string sha256(const string& input) {
unsigned char hash[SHA256_DIGEST_LENGTH];
SHA256((unsigned char*)input.c_str(), input.size(), hash);
stringstream ss;
for (int i = 0; i < SHA256_DIGEST_LENGTH; i++) {
ss << hex << setw(2) << setfill('0') << (int)hash[i];
}
return ss.str();
}
// Абстракція (насправді: API пристрою генерації)
class QuantumRNG {
public:
static uint64_t getRandom() {
// У реальній системі: читання з пристрою
return std::random_device{}();
}
};
struct Node {
int id;
bool isMalicious;
};
// Merkle Tree
class MerkleTree {
public:
vector<string> leaves;
vector<vector<string>> tree;
MerkleTree(const vector<string>& transactions) {
for (const auto& tx : transactions) {
leaves.push_back(sha256(tx));
}
buildTree();
}
void buildTree() {
tree.push_back(leaves);
while (tree.back().size() > 1) {
vector<string> level;
auto& prev = tree.back();
for (size_t i = 0; i < prev.size(); i += 2) {
if (i + 1 < prev.size()) {
level.push_back(sha256(prev[i] + prev[i + 1]));
} else {
level.push_back(prev[i]);
}}
tree.push_back(level);
}}
string getRoot() const {
return tree.back()[0];
}
//  Merkle Proof
vector<string> getProof(int index) {
vector<string> proof;

for (size_t level = 0; level < tree.size() - 1; level++) {
auto& nodes = tree[level];
if (index % 2 == 0 && index + 1 < nodes.size()) {
proof.push_back(nodes[index + 1]);
```

```
} else if (index % 2 == 1) {
proof.push_back(nodes[index - 1]);
}
index /= 2;
}
return proof;
}
// Перевірка доказу
static bool verifyProof(string leaf, vector<string> proof, string root) {
string hash = sha256(leaf);
for (const auto& sibling : proof) {
hash = sha256(hash + sibling);
}
return hash == root;
}};
// Вибір валідаторів
vector<Node> selectValidators(const vector<Node>& network, int count) {
vector<Node> selected;
vector<bool> used(network.size(), false);
while (selected.size() < count) {
uint64_t r = QuantumRNG::getRandom();
int idx = r % network.size();
if (!used[idx]) {
selected.push_back(network[idx]);
used[idx] = true;
}}
return selected;
}
// Валідація блоку
bool validateBlock(
const vector<Node>& validators,
const MerkleTree& tree,
const vector<string>& transactions
)
{
int honest = 0;
for (const auto& node : validators) {
if (!node.isMalicious) {
honest++;
// вибір випадкової транзакції для перевірки
uint64_t r = QuantumRNG::getRandom();
int txIndex = r % transactions.size();
auto proof = tree.getProof(txIndex);
if (!MerkleTree::verifyProof(
transactions[txIndex],
proof,
tree.getRoot()
)) {
return false;
}}}
double ratio = (double)honest / validators.size();
return ratio >= 0.67;
}
// Основний виклик методу
int main() {
int totalNodes = 100;
int validatorCount = 10;
vector<Node> network;
for (int i = 0; i < totalNodes; i++) {
network.push_back({i, i < 30});
}
// транзакції
vector<string> transactions = {
```

```
"tx1", "tx2", "tx3", "tx4", "tx5"
};
MerkleTree tree(transactions);
// вібір валідаторів
auto validators = selectValidators(network, validatorCount);
// валідація
bool result = validateBlock(validators, tree, transactions);
cout << "Merkle Root: " << tree.getRoot() << endl;
cout << "Validation result: "
<< (result ? "ACCEPTED" : "REJECTED") << endl;
return 0;
}
```

ДОДАТОК В

Приклад спрощеної демонстраційної програмної реалізації методу рандомізованого підтвердження блоків

```
using namespace std;
struct Node {
int id;
bool isMalicious;
};
struct Block {
int id;
string prevHash;
string hash;
bool isTampered;
};
// Формування вибірки валідаторів
vector<Node> formValidatorSet(
const vector<Node>& network,
int validatorCount
) {
vector<Node> validators;
vector<bool> used(network.size(), false);
while (validators.size() < validatorCount) {
uint64_t r = QuantumRNG::getRandom();
int index = mapToIndex(r, network.size());
// Забезпечення унікальності вибору
if (!used[index]) {
validators.push_back(network[index]);
used[index] = true;
}}
return validators;
}
// Локальна перевірка блоку
bool localBlockValidation(const Node& node, const Block& block) {
// Чесний вузол виявляє підміну
if (!node.isMalicious) {
return !block.isTampered;
}
return true;
}
// Перевірка цілісності ланцюжка
bool validateChain(const vector<Block>& blockchain) {
for (size_t i = 1; i < blockchain.size(); i++) {
// Перевірка зв'язності блоків
if (blockchain[i].prevHash != blockchain[i - 1].hash) {
return false;
}
// Перевірка на підміну
if (blockchain[i].isTampered) {
return false;
}}
return true;
}
// Агрегація рішень
bool consensusDecision(
const vector<bool>& results,
double threshold
) {
int positive = 0;
for (bool r : results) {
if (r) positive++;
```

```
}
double ratio = (double)positive / results.size();
return ratio >= threshold;
}
//Метод рандомізованої валідації
bool randomizedConsensusWithChainCheck(
const vector<Node>& network,
const vector<Block>& blockchain,
int validatorCount,
double threshold
) {
// 1. Глобальна перевірка ланцюжка
if (!validateChain(blockchain)) {
return false;
}
// 2. Вибір валідаторів
vector<Node> validators = formValidatorSet(network, validatorCount);
// 3. Локальна перевірка останнього блоку
const Block& lastBlock = blockchain.back();
vector<bool> results;
for (const auto& node : validators) {
results.push_back(localBlockValidation(node, lastBlock));
}
// 4. Агрегація результатів
return consensusDecision(results, threshold);
}
int main() {
int totalNodes = 100;
int validatorCount = 10;
double threshold = 0.67;
vector<Node> network;
// Формування мережі (30% зловмисних)
for (int i = 0; i < totalNodes; i++) {
network.push_back({i, i < 30});
}
// Формування блокчейну
vector<Block> blockchain = {
{0, "0", "hash0", false},
{1, "hash0", "hash1", false},
{2, "hash1", "hash2", false}
};
bool result = randomizedConsensusWithChainCheck(
network,
blockchain,
validatorCount,
threshold
);
cout << "Результат консенсусу: "
<< (result ? "ПІДТВЕРДЖЕНО" : "ВІДХИЛЕНО") << endl;
return 0;
}
```