МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ДОНЕЦЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ ІМЕНІ ВАСИЛЯ СТУСА

ЄРМАК ДМИТРО МИКОЛАЙОВИЧ

Допускається до захисту:
В.о. завідувача кафедри
прикладної математики та
кібербезпеки,
_____Луценко А.В.
«__»_____20__р.

РОЗРОБКА ГЕНЕРАТОРА КРИПТОВАЛЮТНИХ АДРЕС ДЛЯ БЛОКЧЕЙН-ТРАНЗАКЦІЙ

Спеціальність 125 Кібербезпека
Кваліфікаційна (бакалаврська) робота

Науковий керівник:
Загоруйко Л.В.,
к.т.н., доцент, доцент кафедри
прикладної математики та кібербезпеки
_____
(підпис)

Оцінка : ___/ ___ / _____
(бали/за шкалою ЄКТС/за національною шкалою)

Голова ЕК: _____
(підпис)

Вінниця – 2025

АНОТАЦІЯ

Єрмак Д.М. Розробка генератора криптовалютних адрес для блокчейн-транзакцій. Спеціальність 125 «Кібербезпека». Донецький національний університет імені Василя Стуса, Вінниця, 2025.

У кваліфікаційній (бакалаврській) роботі досліджено процес генерації криптовалютних адрес з підвищеним рівнем безпеки шляхом шифрування приватного ключа за допомогою алгоритму AES-256. Реалізований підхід підвищує безпеку зберігання приватних ключів, запобігає їх компрометації та забезпечує захист від несанкціонованого доступу під час зберігання на локальних пристроях. Результати дослідження можуть бути використані для вдосконалення існуючих програмних криптогаманців, підвищення рівня безпеки транзакцій у блокчейн-мережах та створення нових рішень у сфері кібербезпеки.

Ключова слова: криптовалюта, блокчейн, криптографія, атака на блокчейн, транзакція. 49 с., 5рис., 6 формул, 42 джерел.

ANNOTATION

Yermak D.M. Developing of a Cryptocurrency Address Generator for Blockchain Transactions. Specialty 125 «Cybersecurity». Vasyl Stus Donetsk National University, Vinnytsia, 2025.

The qualification (bachelor's) work investigates the process of generating cryptocurrency addresses with an enhanced level of security by encrypting the private key using the AES-256 algorithm. The implemented approach improves the security of private key storage, prevents its compromise, and ensures protection against unauthorized access during storage on local devices. The research findings can be applied to enhance existing software crypto wallets, increase the security level of transactions in blockchain networks, and develop new solutions in the field of cybersecurity.

Key words: cryptocurrency, blockchain, cryptography, attack on the blockchain, transaction.

49 pp., 5 figures, 6 formulas, 42 sources.

СПИСОК СКОРОЧЕНЬ

ECDSA - Elliptic Curve Digital Signature Algorithm.

PoW - Proof-of-Work.

PoS - Proof of Stake.

TPS - Transactions Per Second.

DApps - Decentralized Applications.

DeFi - Decentralized Finance.

SHA - Secure Hash Algorithm.

RIPEMD - RACE Integrity Primitives Evaluation Message Digest.

AES - Advanced Encryption Standard.

CBC - Cipher Block Chaining.

IV - Initialization Vector.

ЗМІСТ

ВСТУП

Актуальність роботи. Сучасний розвиток інформаційних технологій і цифрових фінансових інструментів супроводжується значним зростанням кіберзагроз і висуває підвищені вимоги до захисту даних. У цьому контексті критичну роль відіграють надійні технології захисту, здатні забезпечити безпеку, прозорість та цілісність інформації. Блокчейн виступає однією з найбільш інноваційних і перспективних технологій для досягнення цих цілей. Його унікальна структура та функціональні можливості здатні забезпечити високий рівень захищеності інформації та гарантувати безпечність транзакцій.

Блокчейн є розподіленою базою даних, де кожен вузол мережі зберігає копію всієї інформації, що дозволяє забезпечити незмінність і надійність даних. Така структура виключає необхідність центрального органу контролю, зменшуючи ризик зловживань або маніпуляцій з боку третіх осіб. Прозорість і децентралізація, властиві блокчейн-технології, знижують ризики атак з боку зловмисників, адже будь-які спроби змінити дані потребують зламу більшості вузлів, що майже неможливо реалізувати на практиці. Завдяки цим властивостям блокчейн вже активно впроваджується у різних сферах – від фінансових послуг і криптовалют до систем ідентифікації, охорони здоров'я та захисту персональних даних.

Однак, зростаюча популярність блокчейну викликає і нові виклики в сфері безпеки. Забезпечення безпеки блокчейн є критично важливим для його успішного функціонування, адже технологія розвивається, збільшується кількість користувачів криптовалют і відповідно обсяги транзакцій вимагають ефективних і безпечних механізмів генерації адрес для взаємодії з блокчейном. Вразливість приватних ключів до крадіжок або втрати є одним із головних викликів безпеки криптовалютних систем. У зв’язку з цим виникає необхідність у створенні генераторів криптовалютних адрес, які б поєднували стандартні криптографічні алгоритми з додатковими механізмами захисту, зокрема шифруванням приватного ключа. Дослідження методів захисту приватних ключів, зокрема через використання симетричного шифрування (наприклад,

AES), є актуальним напрямом для підвищення надійності програмних гаманців та генераторів адрес.

Метою роботи є розробка та дослідження програмного модуля для генерації криптовалютних адрес, що забезпечує високий рівень безпеки шляхом шифрування приватного ключа за допомогою алгоритму AES, з дотриманням загальноприйнятих стандартів (ECDSA, SHA-256, Base58Check) у сфері блокчейн-технологій.

Об'єктом дослідження є криптографічні методи формування криптовалютних адрес у блокчейн-системах.

Предметом дослідження є алгоритмічні рішення та програмні засоби генерації криптовалютних адрес із використанням шифрування приватного ключа, а також засоби захисту ключової інформації в децентралізованих мережах.

РОЗДІЛ І КІБЕРБЕЗПЕКА У ФІНАНСОВІЙ ЕКОСИСТЕМІ: РИЗИКИ ТА ЗАХИСТ КРИПТОВАЛЮТ І БЛОКЧЕЙНУ

1.1. Криптовалюти як новий етап розвитку фінансової системи

Сучасний фінансовий світ зазнав суттєвих змін з появою цифрових технологій, які відкрили нові способи здійснення платежів. Одним із найяскравіших проявів цієї еволюції стала поява криптовалют — цифрових або віртуальних засобів обміну, заснованих на принципах криптографії. Вони забезпечують безпечність транзакцій, контроль за випуском нових одиниць та верифікацію передачі активів без участі центральних фінансових установ.

На відміну від традиційних фіатних валют, випуск та обіг яких контролюються центральними банками, криптовалюти функціонують у децентралізованих мережах, побудованих на основі технології блокчейн. Це інноваційне рішення дозволяє не лише забезпечити прозорість та незмінність транзакцій, а й значно знизити ризик фальсифікацій. Саме децентралізація і високий рівень безпеки зробили криптовалюти важливим елементом сучасної фінансової екосистеми, що стрімко набирає популярності в усьому світі.

Теоретичні основи криптовалют були закладені ще в 1983 році американським криптографом Девідом Чаумом, який запропонував концепцію електронних грошей із використанням криптографії. Проте широке визнання криптовалюти отримали лише в останні десятиліття, особливо після запуску Bitcoin у 2009 році, що став першою повністю децентралізованою цифровою валютою. Незважаючи на свою відносно коротку історію існування, криптовалюти вже встигли пережити численні періоди волатильності, зокрема у 2013 році, коли їхня ринкова вартість зазнала значних коливань.

Криптовалюти поєднують у собі принципи віртуальних грошей та криптографічного захисту інформації. Основний принцип їхньої роботи полягає в децентралізованому виробництві монет, яке контролюється всією мережею користувачів, а не централізованою фінансовою установою. Це означає, що

жодна окрема особа чи організація не має можливості прискорити або сфальсифікувати випуск нових одиниць. Кількість криптовалюти, що перебуває в обігу, зазвичай визначається наперед і є публічно відомою, що виключає ризик неконтрольованої емісії.

Перекази криптовалют здійснюються через однорангові мережі, що дозволяє виконувати транзакції без посередників. Це не тільки підвищує швидкість операцій, але й знижує їхню вартість, роблячи міжнародні перекази більш доступними порівняно з традиційними банківськими системами[1].

Криптовалюти вирізняються низкою унікальних характеристик, що визначають їхню цінність та функціональні можливості в сучасній економічній системі[2-3]:

1. Безпека: Завдяки використанню криптографічних методів, криптовалютні транзакції є високозахищеними від підробки та несанкціонованого втручання. Кошти, що зберігаються в криптовалютах, захищені криптографічною системою на основі відкритого ключа. Однак для здійснення транзакцій з віртуальними валютами потрібен ще й приватний ключ, який є тільки у власника. Поєднання надійного криптографічного методу та довгих чисел робить його практично неможливим для злому.

2. Децентралізація: Відсутність центрального органу управління або контролю є однією з визначальних рис криптовалют. Мережа підтримується розподіленою спільнотою учасників, що забезпечує стійкість до цензури та єдиної точки відмови[4].

3. Прозорість: Усі операції, що відбуваються в блокчейн-мережі, є публічно доступними для перегляду та верифікації. Хоча ідентичність учасників може залишатися анонімною, самі транзакції прозорі та незмінні.

4. Обмежена емісія: Деякі криптовалюти, такі як Bitcoin, мають наперед визначену максимальну кількість одиниць, що сприяє дефляційним властивостям активу та потенційному збереженню вартості в довгостроковій перспективі.

5. Глобальна доступність: Криптовалютні транзакції можуть здійснюватися між будь-якими користувачами, незалежно від їх географічного розташування, часто з нижчими комісіями та швидшим часом обробки порівняно з традиційними міжнародними переказами.

6. Анонімність: Транзакції з віртуальною валютою та подібні рахунки не пов'язані з реальними особами. Власник отримує віртуальні монети на адресу, яка насправді є випадковим алфавітно-цифровим рядком. Хоча потоки транзакцій можна проаналізувати, зв'язок між адресою та реальною особою встановити досить малоймовірно.

1.2. Історія розвитку блокчейн-технології

У сучасну епоху цифрової взаємодії, коли обмін персональними даними став невід'ємною частиною онлайн-комунікації, питання захисту конфіденційності та створення безпечних цифрових ідентифікаторів набуло особливої актуальності. Хоча технологія блокчейн здебільшого асоціюється з криптовалютами на зразок біткоїна, її можливості виходять далеко за межі цього застосування. Блокчейн не лише змінює підходи до цифрових транзакцій, але й відкриває нові горизонти у сфері захисту даних та управління цифровою ідентичністю, здійснюючи це на абсолютно новому рівні.

Блокчейн – це спосіб запису інформації, який запобігає змінам, злому або маніпуляціям із системою. Це розподілений реєстр, який копіює та розподіляє дані про транзакції між комп'ютерами, що беруть участь у блокчейні[5].

Блокчейн-технологія – це структура, яка зберігає записи про транзакції, відомі як блоки, у кількох базах даних, що утворюють "ланцюжок" і з'єднані через однорангові вузли в мережі. Це сховище часто називають "цифровою книгою"[6].

Кожна транзакція в цьому реєстрі підтверджується цифровим підписом власника, який засвідчує її справжність та захищає від підробки. Таким чином, інформація в електронному реєстрі є високозахищеною.

Простими словами, це як електронна таблиця Google, до якої мають доступ багато комп'ютерів у мережі. Вона містить записи про транзакції на основі реальних покупок: кожен може переглядати ці дані, але не змінювати їх[7].

Історію та еволюцію технології блокчейн можна простежити за кількома ключовими віками та подіями за останні кілька десятиліть. Короткий огляд її еволюції [8-10]:

Ера до біткоїна:

Концепція ланцюжка блоків, пов'язаних криптографією, з'явилася на початку 1990-х років. У 1991 році Стюарт Хейбер і В. Скотт Сторнетта представили криптографічну систему для позначення часу в цифрових документах, щоб забезпечити їхню незмінність.

Біткоїн Whitepaper (2008):

Сучасна ера блокчейну розпочалася з публікації у жовтні 2008 року окремою особою або групою осіб, відомими як Сатоші Накамото, технічного документу під назвою «Біткоїн: однорангова електронна грошова система». У документі було запропоновано децентралізовану цифрову валюту і описано блокчейн як технологію, що лежить в її основі.

Genesis Block (2009):

3 січня 2009 року Сатоші Накамото здобув перший блок блокчейну Біткоїна, відомий як генезис-блок. Це ознаменувало народження біткоїна і початок практичного застосування технології блокчейн.

Ранній розвиток (2009-2013):

У перші роки біткоїн набув популярності серед шифрувальників, ентузіастів криптографії, яких приваблювала його обіцянка децентралізації та стійкості до цензури.

Розробники та підприємці почали вивчати альтернативні варіанти використання блокчейну, окрім криптовалюти, зокрема децентралізовані додатки (DApps), смарт-контракти та управління цифровими активами.

Очікується, що майбутнє технології блокчейн буде зосереджене на масштабованості, стійкості та інтеграції з новими технологіями, такими як штучний інтелект, Інтернет речей і квантові обчислення.

Загалом, історія та еволюція технології блокчейн відображає її шлях від концептуальної ідеї до проривної сили з далекосяжними наслідками для різних галузей і секторів.

1.3. Структура блокчейну

Структура блокчейну складається з декількох ключових компонентів, включаючи блоки, ноди(вузли), транзакції та механізми консенсусу.

Основні компоненти блокчейну:

• Блоки - це фундаментальні одиниці блокчейну, що містять список транзакцій. Кожен блок криптографічно пов'язаний з попереднім, утворюючи ланцюжок блоків, який є незмінним і захищеним від підробки[11].

• Ноди - це учасники мережі, які підтримують копію блокчейну і підтверджують транзакції. Майнери, які виконують процес додавання нових блоків до блокчейну за допомогою майнінгу, є різновидом вузлів у мережі[12].

• Транзакції являють собою угоди або передачу активів між сторонами, записані в блокчейні. Кожна транзакція криптографічно захищена і додається до блоку для перевірки[13].

• Механізми консенсусу - це протоколи, які забезпечують згоду між вузлами мережі щодо дійсності транзакцій. Proof of Work, Proof of Stake - поширені алгоритми консенсусу, що використовуються в мережах блокчейн[14].

1.4. Основи роботи блокчейну

Блокчейн складається з послідовно з’єднаних блоків, кожен із яких містить три основні компоненти: дані, хеш і хеш попереднього блоку. Блок є базовою одиницею блокчейну, що представляє собою набір інформації, яка додається до

ланцюжка в хронологічному порядку. Таким чином, формується єдина база даних транзакцій, спільна для всіх вузлів мережі, тобто комп'ютерів або серверів.

Щоб створити новий блок, використовується унікальний номер, відомий як Nonce, який вибирають майнери для розв'язання криптографічної задачі. Цей процес називається «Proof of Work». Після успішного вирішення задачі новий блок додається до ланцюжка.

Хеш є унікальним ідентифікаційним кодом, який створюється на основі даних блоку, хешу попереднього блоку та часової позначки. Він гарантує цілісність даних, оскільки навіть найменша зміна вмісту блоку призведе до створення нового хешу, що робить дані незмінними.

Перед додаванням нового блоку до ланцюжка, його автентичність перевіряється алгоритмом консенсусу . Більшість вузлів у мережі мають підтвердити блок, забезпечуючи безпеку і виключаючи необхідність у посередниках.

Кожен блок у блокчейні має унікальні характеристики, які дозволяють ідентифікувати його за номером, висотою або хешем заголовка. Дані блоків шифруються за допомогою хеш-функцій, що робить їх недоступними для зміни або видалення.

Таким чином, блокчейн виступає як цифровий нотаріус, що фіксує транзакції з часовими позначками, забезпечуючи їхню достовірність і захист від підробок.

Рисунок 1.1 Принцип роботи технології Блокчейн

1.5. Види блокчейну

1. Публічні блокчейни - це відкриті мережі, де кожен може брати участь у транзакціях і підтверджувати блоки. Зазвичай такі мережі пропонують економічні стимули для учасників, які забезпечують їхню безпеку, та використовують алгоритми “ Proof of stake” або “ Proof of work”. Біткоїн та Ефіріум є прикладами публічних блокчейнів, відомих своєю децентралізованістю та прозорістю[15].

Основними характеристиками публічного блокчейну є [16]:

- Відкритість і прозорість

Публічні блокчейни вирізняються абсолютною прозорістю: інформація про всі транзакції доступна для всіх авторизованих учасників мережі в режимі реального часу. Такий підхід забезпечує максимальну відкритість даних, що виключає можливість приховування інформації або фальсифікації записів. Кожен вузол може здійснювати перевірку легітимності транзакцій, що підвищує рівень довіри до системи та знижує ймовірність виникнення шахрайських схем.

- Обмежена пропускна здатність.

Одним із суттєвих недоліків публічних блокчейнів є низька швидкість обробки транзакцій. Це зумовлено великою кількістю вузлів, кожен з яких має здійснити верифікацію даних та виконати алгоритм Proof-of-Work. У середньому, публічні блокчейни здатні обробляти близько 7 транзакцій на секунду, тоді як мережа Ethereum підтримує близько 15 транзакцій на секунду (TPS).

- Надійність та довіра

Публічні блокчейни характеризуються високим рівнем довіри та надійності завдяки своїй децентралізованій структурі. На відміну від приватних блокчейнів, у публічних мережах учасники не зобов'язані перевіряти автентичність інших вузлів для підтвердження достовірності транзакцій. Це зумовлено відкритістю мережі та прозорістю процесів, де кожен вузол функціонує незалежно, а перевірка даних здійснюється колективно. Така архітектура мінімізує ризики шахрайства, оскільки взаємодія між вузлами відбувається без необхідності особистої довіри.

- Безпека та захищеність

Публічні блокчейни забезпечують високий рівень безпеки завдяки децентралізованій верифікації транзакцій та використанню сучасних методів криптографічного захисту. Усі вузли в мережі беруть участь у перевірці даних, що значно ускладнює можливість несанкціонованого втручання з боку зловмисників. Крім того, механізми консенсусу, зокрема Proof-of-Work, гарантують стійкість до модифікації даних. Згідно з думками експертів, криптографічні алгоритми, що застосовуються у публічних блокчейнах, забезпечують вищий рівень захисту порівняно з приватними блокчейнами.

- Високе енергоспоживання

Підтримка публічних блокчейнів потребує значних енергетичних ресурсів, що обумовлено використанням алгоритму Proof-of-Work. Майнінг та процеси верифікації даних вимагають виконання складних обчислювальних операцій, що суттєво підвищує рівень енергоспоживання. Це, у свою чергу, має негативний вплив не лише на економічні показники, але й на екологічне середовище, що

робить питання енергоефективності одним із ключових у сфері розвитку блокчейн-технологій.

- Проблеми масштабованості

Масштабованість є ще одним викликом для публічних блокчейнів. Збільшення кількості учасників та транзакцій створює навантаження на мережу, що ускладнює її розширення та оптимізацію. З метою вирішення цієї проблеми впроваджуються технології другого рівня, такі як Lightning Network у мережі Bitcoin, що дозволяють значно знизити навантаження та підвищити ефективність обробки транзакцій.

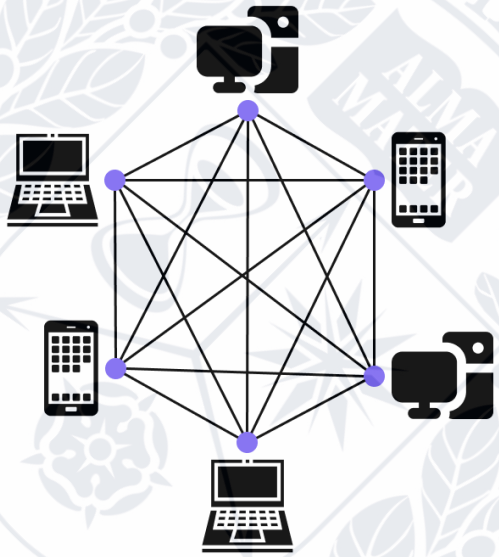

Рисунок 1.2 Публічний блокчейн

2. Приватні блокчейни є спеціалізованою версією технології блокчейн, призначеною для використання всередині окремої мережі. На відміну від публічних блокчейнів, які відкриті для всіх і забезпечують повну прозорість, приватні блокчейни працюють на основі дозволів, надаючи доступ і можливість підтверджувати транзакції лише авторизованим учасникам. Така модель забезпечує вищий рівень безпеки, конфіденційності та контролю, що робить приватні блокчейни особливо привабливими для бізнесу, який прагне оптимізувати процеси та захистити конфіденційну інформацію[17].

Основними характеристиками приватного блокчейну є [16]:

- Швидкість та пропускна здатність

Приватні блокчейни демонструють значно вищу швидкість обробки транзакцій у порівнянні з публічними блокчейнами. Це зумовлено обмеженою кількістю вузлів у мережі, що сприяє підвищенню швидкості підтвердження транзакцій. Кожен вузол у приватному блокчейні має можливість швидко здійснювати верифікацію даних, що дозволяє суттєво збільшити кількість транзакцій за одиницю часу. У деяких випадках пропускна здатність приватних блокчейнів може досягати від кількох тисяч до сотень тисяч транзакцій на секунду (TPS).

- Масштабованість

Приватні блокчейни також характеризуються високою масштабованістю. Додавання нових вузлів до існуючої мережі відбувається швидко та без значних затримок, що сприяє легкому розширенню системи. Крім того, видалення або додавання вузлів не чинить значного впливу на загальну роботу мережі, що забезпечує її гнучкість та ефективність. Це робить приватні блокчейни привабливими для корпоративних рішень, де важливими є швидкість і можливість масштабування без збоїв у роботі.

- Потреба у формуванні довіри

На відміну від публічних блокчейнів, що функціонують як відкритий реєстр, приватні блокчейни вимагають побудови довірчих відносин між учасниками. Це пов’язано з обмеженим доступом до мережі, де лише визначена група користувачів має можливість здійснювати транзакції та брати участь у верифікації. У такому середовищі критично важливо забезпечити довіру до центрального управління та до учасників мережі.

- Знижений рівень безпеки

Одним із основних недоліків приватних блокчейнів є потенційна вразливість до атак з боку третіх осіб. Якщо зловмисник отримає доступ до центральної системи управління, він може здійснити несанкціоновані дії з усією мережею. Це робить приватні блокчейни менш захищеними порівняно з публічними, де відсутність центрального управління ускладнює можливість компрометації всієї системи.

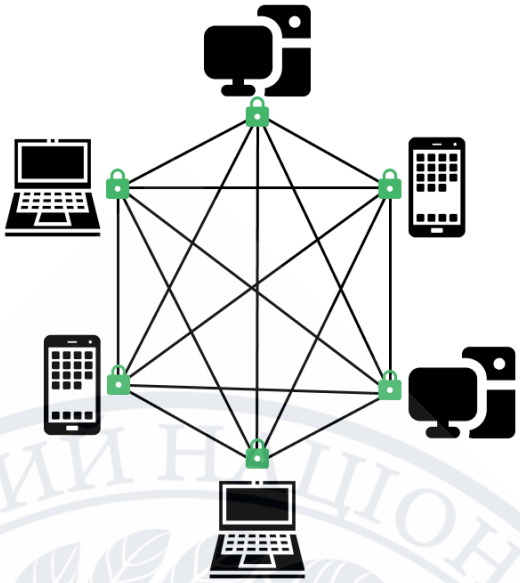

Рисунок 1.3 Приватний блокчейн

3. Блокчейн консорціуму складається з попередньо вибраного набору вузлів або комп'ютерів, які відповідають за контроль доступу до ресурсів мережі блокчейн. Його метою є усунути єдину автономію приватного блокчейну, маючи кілька суб'єктів або організацій, відповідальних за консенсус і прийняття рішень на користь усієї мережі [18].

Основними характеристиками блокчейну консорціуму є [19]:

- Контроль доступу та дозволи

Однією з ключових переваг цього типу блокчейну є можливість ефективного контролю доступу до мережі. Для підключення та взаємодії в межах мережі потрібні дозволи на рівні системи та окремих вузлів. Кожен обліковий запис користувача та кожен вузол отримують набір визначених ролей і дозволів, що регламентують їхні права доступу та операційні можливості. Такий підхід забезпечує підвищений рівень безпеки та чітку організацію процесів.

- Децентралізоване управління на основі консенсусу

Управління в блокчейні здійснюється децентралізовано за допомогою механізмів консенсусу, в яких беруть участь авторизовані вузли. Ці вузли спільно визначають правила функціонування мережі, забезпечуючи прозорість і контроль над дотриманням встановлених політик. Такий підхід спрощує управління інфраструктурою та підвищує рівень узгодженості рішень.

- Низьке споживання енергії та обчислювальних ресурсів

На відміну від публічних блокчейнів, консорціумні мережі не використовують енерговитратні алгоритми консенсусу на зразок Proof-of-Work (PoW), що потребують значних обчислювальних потужностей для розв'язання складних математичних задач. Це дозволяє суттєво знизити енергоспоживання та ресурси для підтримки працездатності мережі.

- Конфіденційність та приватність даних

Блокчейн консорціумну забезпечує високий рівень конфіденційності транзакцій і приватності даних. Такий підхід є особливо важливим для корпоративних рішень та децентралізованих додатків (DApps), де критично важливо захищати комерційну та особисту інформацію від несанкціонованого доступу.

- Висока пропускна здатність

Мережі блокчейну консорціумну демонструють високу швидкість обробки транзакцій. Це забезпечується швидким досягненням консенсусу між авторизованими вузлами-валідаторами, що спрощує узгодження стану реєстру та підвищує ефективність роботи системи.

- Безпека та масштабованість

Цей блокчейн забезпечує підвищену стійкість до збоїв і атак навіть у випадку непередбачуваної або зловмисної поведінки деяких вузлів. Децентралізована структура управління унеможливлює компрометацію всієї мережі, що підвищує рівень безпеки та забезпечує стійкість до зовнішніх загроз.

4. Гібридний блокчейн.

З метою оптимізації обчислювальних потужностей та зниження вимог до зберігання даних пропонується використання гібридної моделі блокчейну, яка поєднує централізовані елементи серверів з децентралізованою природою блокчейн-мереж. У цій моделі мережа складається з двох основних компонентів: особистого блокчейну для взаємодії користувачів із серверною інфраструктурою та глобального блокчейну, що об'єднує сервери в єдину систему. Глобальний

блокчейн функціонує як ланцюг блокчейнів, розподілених між серверами, з періодичним оновленням даних.

Архітектура гібридного блокчейна є особливо корисною для сучасних онлайн-бізнесів, таких як банківські установи та платформи електронної комерції, де сервери розміщені в різних географічних точках. Відповідно до цієї моделі, кожен користувач отримує доступ до свого особистого блокчейну, що містить лише його дані та транзакції, забезпечуючи високий рівень конфіденційності. Жоден користувач не має доступу до даних інших учасників мережі, що підвищує рівень захисту інформації.

У гібридному блокчейні використовуються один або декілька приватних майнерів, які розподілені в мережі та керуються локальними політиками бізнесу. Відмінністю цієї моделі є те, що майнери не змагаються за розв'язання складних математичних задач, як у класичному Proof-of-Work (PoW). Замість цього вони займаються додаванням нових блоків та формуванням гешів у мережі, що підвищує ефективність і безпеку. Такий підхід знижує ризик виникнення атак типу "selfish mining", оскільки відомі обчислювальні можливості кожного майнера. У традиційній моделі PoW майнери витрачають значні обсяги електроенергії під час обчислювальних операцій. Впровадження приватних майнерів дозволяє справедливо розподілити процеси майнінгу між вузлами, значно знижуючи енергоспоживання.

У запропонованій моделі кожен користувач зберігає локальну копію свого особистого блокчейну, що включає всі його транзакції та дані. При здійсненні нової транзакції з пристрою користувача відправляється запит на обробку до майнерів у мережі. Обраний майнер за допомогою алгоритму вибору здійснює обчислення та генерує два типи гешів: глобальний та приватний. Отриманий приватний геш повертається користувачу, після чого нові блоки зв'язуються у ланцюг на основі цього гешу.

Дані користувача зберігаються як локально на його пристрої, так і на серверних вузлах мережі. В локальному сховищі міститься 50% інформації, інші 50% розміщуються на серверах бізнес-мережі. Кожен сервер містить копію

глобального блокчейну, що включає блоки всіх підключених користувачів. Зв'язок між цими блоками забезпечується за допомогою глобального гешу, згенерованого майнером. Таким чином, користувачі можуть отримувати доступ лише до своїх даних, що гарантує конфіденційність і захист від несанкціонованого доступу [20].

1.6. Основні види атак на блокчейн

Багато людей праві, коли вважають, що блокчейн за своєю суттю є безпечним. Блокчейн, безумовно, дає організаціям переваги, але він має суттєві недоліки через певні проблеми з безпекою.

Найголовніші проблеми безпеки блокчейну та їх вирішення.

1. Атака 51%.

Атака 51% - це ситуація, коли група майнерів в мережі блокчейн може отримати контроль над більш ніж 50% хешрейту мережі. Цей контроль може дозволити їм маніпулювати мережею різними способами[21].

Наприклад, вони можуть перешкоджати новим транзакціям отримувати підтвердження, фактично зупиняючи платежі між користувачами. Вони також можуть скасовувати транзакції, які були завершені під їхнім контролем, що потенційно може призвести до подвійного витрачання монет.

Ризики 51% атаки.

У разі успіху зловмисники можуть перервати запис нових блоків, не даючи іншим майнерам завершити створення блоків.

Вони також можуть скасувати транзакції, що дозволить їм двічі витратити монети. Це підриває цілісність блокчейну і може призвести до втрати довіри до мережі.

У той час як великі мережі менш схильні до успішних атак через їх розмір і складність, менші мережі є більш вразливими.

Запобігти атаці 51% складно через децентралізовану природу мереж блокчейн. Однак, існують заходи, які можна вжити для зменшення ризику.

Наприклад, впровадження механізму консенсусу, коли для отримання статусу валідатора вузли зобов'язані вкласти певну кількість власних токенів, може ускладнити отримання контролю над більшою частиною мережі для одного суб'єкта.

Крім того, регулярний моніторинг мережі та використання передових криптографічних методів може допомогти виявити і запобігти потенційним атакам.

2. Сибіл атака.

Сибіл-атака - це тип загрози безпеці, коли один суб'єкт створює кілька шахрайських вузлів, намагаючись отримати контроль над мережею блокчейн. Ця атака може вплинути на будь-яку однорангову мережу, включаючи мережі блокчейн.

Сибіл-атака спрямована на те, щоб витіснити автентичні вузли мережі. У разі успіху зловмисник може змінити блокчейн, що потенційно може поставити під загрозу завершеність мережі. Під завершеністю блокчейну розуміють концепцію, згідно з якою після запису транзакції в блокчейн її не можна змінити або скасувати. Ця концепція має вирішальне значення для того, щоб транзакції в блокчейні вважалися дійсними і заслуговували на довіру.

Механіка сибіл-атаки.

Під час сибіл-атаки зловмисник створює кілька фальшивих вузлів, щоб обдурити мережу і змусити її сприймати ці шахрайські акаунти як легітимні. Якщо зловмисник успішно проникне в мережу з достатньою кількістю шкідливих вузлів, він може використати цей вплив проти чесних вузлів на свою користь.

Наприклад, у мережі блокчейн, де майнери голосують за пропозиції, зловмисник може використовувати кілька облікових записів, щоб переважати голоси легітимних вузлів. Зловмисники також можуть перехоплювати та аналізувати конфіденційні дані користувачів, такі як IP-адреси, ставлячи під загрозу конфіденційність та безпеку користувачів.

Щоб зменшити ризик сибіл-атак, блокчейн-мережі використовують механізми консенсусу, в тому числі Proof of Work і Proof of Stake. Ці механізми не запобігають Сибіл атакам повністю, але вони роблять неможливим для зловмисника успішно здійснити таку атаку.

Наприклад, в механізмі Proof of Work можливість створення блоку пропорційна загальній обчислювальній потужності механізму. Це означає, що зловмисник повинен володіти комп'ютерною потужністю, необхідною для створення нового блоку, що робить виконання Сибіл атаки складним і дорогим завданням[22].

3. Фішинг.

Фішингова атака на блокчейн націлена на учасників блокчейну за допомогою фішингових електронних листів для отримання їхніх облікових даних з метою викрадення валюти з їхніх рахунків [23].

1.7. Висновок до розділу 1

Криптовалюти стали ключовим етапом розвитку сучасної фінансової системи, запропонувавши децентралізований підхід до обігу цифрових активів. Використання технології блокчейн забезпечує безпеку, прозорість та незмінність транзакцій, усуваючи необхідність у посередниках і підвищуючи ефективність фінансових операцій. Відсутність централізованого управління та обмежена емісія підсилюють надійність криптовалют як засобу збереження вартості. Незважаючи на виклики, пов’язані з волатильністю та масштабованістю, криптовалюти закладають фундамент для подальших інновацій у сфері цифрових фінансів, стимулюючи перехід до більш відкритої та доступної економічної моделі.

РОЗДІЛ ІІ. КІБЕРБЕЗПЕКА ДЕЦЕНТРАЛІЗОВАНИХ МЕРЕЖ: КРИПТОГРАФІЯ, КОНСЕНСУС ТА ЗАХИСТ ГАМАНЦІВ

2.1. Криптографічні методи безпеки блокчейну

Криптографія лежить в основі технології блокчейн, забезпечуючи основні механізми безпеки, необхідні для здійснення безпечних транзакцій. Використовуючи криптографічні методи, такі як криптографія з відкритим ключем, хеш-функції та цифровий підпис, блокчейн-системи пропонують підвищену безпеку, прозорість та ефективність у широкому спектрі галузей.

Ключові криптографічні компоненти в блокчейні:

1. Хеш-функції.

Хеш-функції - це алгоритми, які перетворюють вхідні дані на рядок символів фіксованого розміру, відомий як хеш. Вони створюють унікальний хеш для кожного окремого входу, полегшуючи перевірку цілісності даних.

Хешування в блокчейні виконує кілька важливих функцій. По-перше, воно робить спроби підробки даних очевидними. Ця незмінність підвищує безпеку блокчейну.

Хешування оптимізує процеси зберігання та пошуку даних у блокчейні. Кожен фрагмент інформації унікально ідентифікується за допомогою хешу, що спрощує доступ для всіх і забезпечує ефективне зберігання в децентралізованій мережі.

Крім того, алгоритми консенсусу використовують хешування для перевірки транзакцій у децентралізованій мережі. Хешування також є необхідним для створення цифрових підписів під час або після процесу верифікації транзакцій, що підвищує рівень конфіденційності та автентичності. Загалом, використання хешування в блокчейні є головним елементом для підтримки прозорості, безпеки та децентралізованої природи технології, забезпечуючи надійну та захищену від підробок історію транзакцій [24].

2. Система відкритих ключів.

Криптографія з відкритим ключем - це протокол безпеки, який забезпечує безпеку даних, якими ми обмінюємося через транзакції в мережі блокчейн. Цей аспект має вирішальне значення в мережі типу «точка-точка», якою є блокчейн. Тому що в такій мережі вузли особисто не знають і не довіряють один одному. Існує потреба у створенні надійної системи безпеки. Крім того, це усуває необхідність для всіх вузлів знати і довіряти один одному особисто.

Криптографія з відкритим ключем - це асиметричний тип криптографії, де використовується пара ключів (відкритий і закритий). Вони використовуються для шифрування/дешифрування інформації та верифікації користувачів. Процес криптографії з відкритим ключем забезпечує дві речі, а саме:

1) Шифрування інформації на стороні відправника за допомогою відкритого ключа (одержувача). Це гарантує, що жодна третя сторона не зможе отримати доступ або зрозуміти зашифровану інформацію в мережі або поза нею. Тільки одержувач може розшифрувати і прочитати повідомлення, використовуючи свій власний приватний ключ.

2) Підписання повідомлення або інформації для перевірки за допомогою особистого ключа відправника. Це підтверджує особу відправника і свідчить про те, що він є легітимним вузлом у мережі блокчейн. Одержувач перевіряє це за допомогою відкритого ключа відправника. Цей процес верифікації користувачів у мережі відбувається за допомогою цифрових підписів.

Таким чином, криптографія з відкритим ключем - це спосіб надання цифрової ідентичності користувачеві. Завдяки цьому можна здійснювати безпечні транзакції в мережі блокчейн[25].

3. Цифровий підпис.

Цифрові підписи є фундаментальним будівельним блоком у блокчейні, який використовується в основному для автентифікації транзакцій. Коли користувачі надсилають транзакції, вони повинні довести кожному вузлу в системі, що вони мають право витрачати ці кошти, не даючи при цьому іншим користувачам витрачати їх. Кожен вузол мережі перевіряє надіслану транзакцію і перевіряє роботу всіх інших вузлів, щоб узгодити правильний стан.

Наприклад, якщо Антон хоче відправити Олегу один біткоїн, перший повинен підписати транзакцію на 1 біткоїн своїм приватним ключем і відправити її вузлам мережі. Майнери, які знають відкритий ключ Антона, перевірять умови транзакції і підтвердять підпис. Після підтвердження дійсності блок, що містить цю транзакцію - готовий [26].

2.2. Механізми консенсусу та їх роль у забезпеченні безпеки блокчейн-мереж

Механізм консенсусу - це програмний інструмент, який використовується в системах блокчейн для досягнення децентралізованої згоди щодо стану реєстру. Як правило, він працює в мережі, що складається з численних процесів і користувачів. Впровадження механізмів консенсусу приносить значні переваги криптовалютам, блокчейнам і розподіленим реєстрам, замінюючи повільні людські процеси верифікації та аудиту.

Таким чином, алгоритми консенсусу забезпечують надійність мережі і встановлюють довіру між невідомими одноранговими учасниками в розподіленому обчислювальному середовищі. По суті, протокол консенсусу гарантує, що кожен новий блок, який додається до блокчейну, є єдиною версією істини, яка узгоджена всіма вузлами блокчейну. Протокол консенсусу складається з певних цілей, таких як досягнення згоди, взаємодія, співпраця, рівні права для кожного вузла і обов'язкова участь кожного вузла в процесі консенсусу. Отже, алгоритм консенсусу спрямований на пошук загальної згоди, яка є виграшною для всієї мережі.

Механізм консенсусу функціонує як основа мереж блокчейн, керуючи тим, як транзакції перевіряються і додаються до незмінного реєстру. Він починається з поширення транзакцій по мережі, де кожен вузол перевіряє автентичність і цілісність вхідних транзакцій. Після перевірки ці транзакції об'єднуються в блоки, і майнери або валідатори пропонують ці блоки мережі. Потім починається процес консенсусу, який варіюється в залежності від обраного механізму, в ході якого вузли співпрацюють, щоб узгодити наступний блок, який буде додано до

ланцюжка. Ця спільна робота гарантує, що всі учасники прийдуть до одностайного рішення щодо стану реєстру, зберігаючи прозорість і довіру до децентралізованої системи. Після досягнення консенсусу обраний блок підтверджується і додається до блокчейну. Механізми заохочення, такі як винагорода для майнерів або валідаторів, стимулюють активну участь і підтримують безпеку та цілісність мережі. В цілому, механізм консенсусу сприяє створенню децентралізованого і стійкого середовища, що дозволяє мережам блокчейн ефективно функціонувати без потреби в центральних органах влади[27].

У технології блокчейн різні механізми консенсусу є життєво важливими для підтримки гармонії та безпеки мережі. Найбільш відомими є: Proof of Stake (PoS), Proof of Work (PoW), кожен з яких пропонує унікальні підходи до досягнення консенсусу в децентралізованому середовищі.

1. Proof of Work (PoW) - це алгоритм, який вимагає від учасників мережі розв'язання складних математичних рівнянь, щоб довести, що вони є легітимними користувачами і підтвердити транзакції. Процес розв'язання математичних рівнянь називається майнінгом. Кожен пристрій для майнінгу винагороджується певною кількістю криптовалюти.

PoW створює безпечну і надійну мережу, яка є стійкою до зловмисників і запобігає подвійним витратам.

Основна мета PoW - створити безпечну мережу, в якій транзакції та дані не можуть бути змінені або зламані. Коли користувач ініціює транзакцію, умови контракту програмуються в мережі. Користувачі повинні надати рішення математичного рівняння, яке відповідає певному набору умов.

Умови запрограмовані в реєстрі, який є базою даних, що реєструє всі транзакції, які відбуваються в мережі. PoW необхідний, оскільки він захищає всі дані про транзакції в блокчейні, що робить практично неможливим втручання в дані і створення фальшивих записів про транзакції [28].

На рисунку 2.1 представлено як працює Proof of Work.

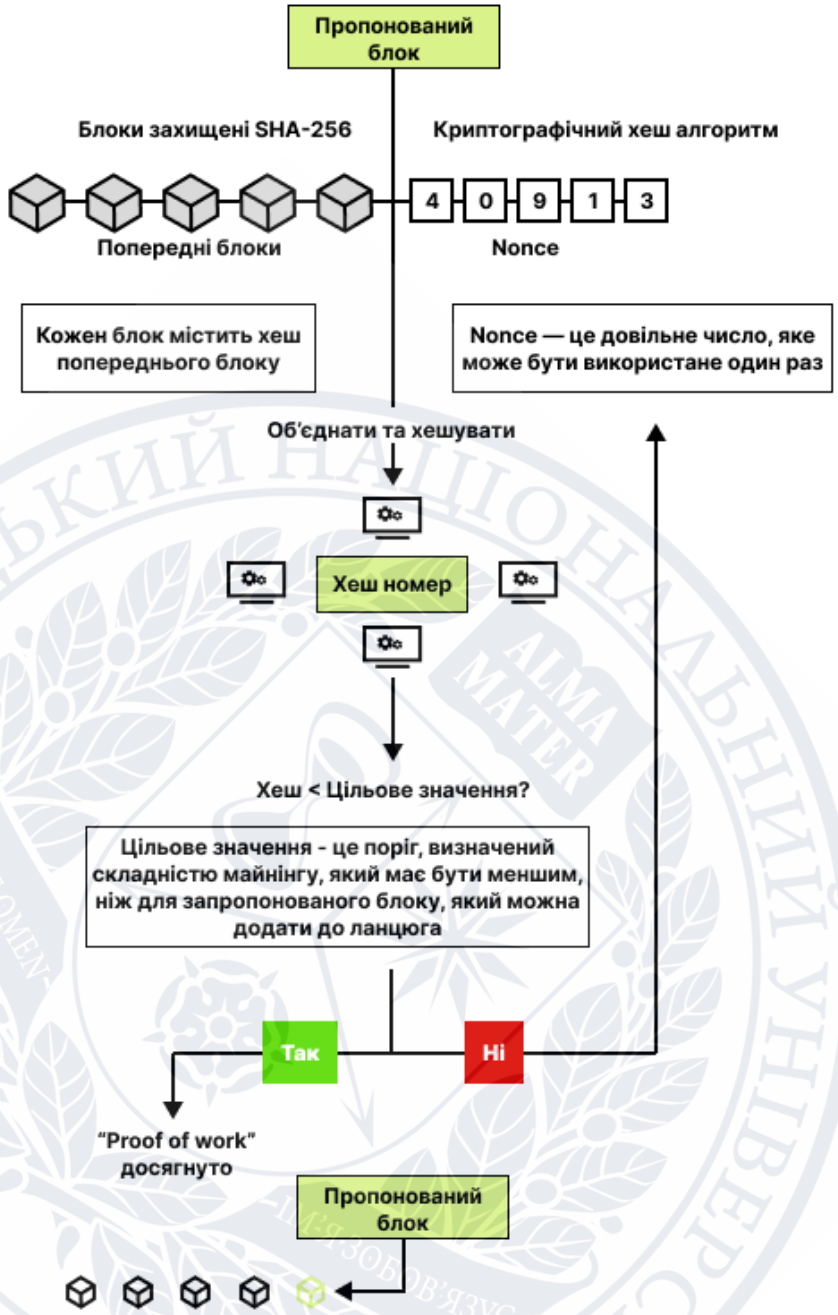

Рисунок 2.1 Схема роботи механізму консенсусу Proof of Work.

2. Proof of Stake (PoS) — це алгоритм консенсусу, що забезпечує верифікацію та підтвердження транзакцій у блокчейн-мережах. Його основна мета полягає у створенні нового блоку в ланцюгу шляхом вибору валідатора на основі кількості заблокованих активів, що належать цьому учаснику. PoS був розроблений як енергоефективніша та децентралізована альтернатива Proof of Work (PoW), що потребує значних обчислювальних ресурсів для підтримки мережі. У 2022 році блокчейн Ethereum відмовився від PoW на користь PoS, визнавши його більш

стійким та енергоефективним підходом. Інші популярні блокчейни, такі як Tezos і Cardano, також використовують PoS у своїх протоколах.

Архітектура та принцип роботи.

Proof of Stake реалізує процес верифікації транзакцій за допомогою валідаторів, які блокують (стейкають) свої активи у спеціальному смарт-контракті. Чим більша кількість заблокованих активів, тим вища ймовірність бути обраним для генерації наступного блоку. Цей підхід підвищує рівень безпеки мережі, оскільки шахрайська поведінка призводить до втрати заблокованих активів. Такий механізм штрафів формує високий рівень відповідальності серед учасників та сприяє чесності у процесах верифікації.

Механізм консенсусу та вибір валідаторів.

Валідатори в мережі PoS обираються випадковим чином, однак із врахуванням обсягу заблокованих активів. Це забезпечує децентралізацію та запобігає централізації обчислювальних потужностей, як у випадку PoW. Концепція "один токен — один голос" підсилює цей підхід: чим більше активів утримує користувач, тим більша ймовірність стати валідатором. Водночас це підвищує фінансову відповідальність, оскільки втрата стейку в разі шахрайства може досягати значних сум.

Енергоефективність та відсутність конкуренції.

На відміну від PoW, де учасники змагаються в розв'язанні складних обчислювальних задач, у PoS цей процес відсутній. Це дозволяє значно знизити енергоспоживання та витрати на підтримку мережі. Вибір валідаторів відбувається автоматично, без необхідності потужних обчислювальних потужностей, що робить PoS більш екологічним і стійким до масштабування.

Використання в DeFi та механізм стейкінгу.

Proof of Stake активно використовується в децентралізованих фінансах (DeFi) як механізм стейкінгу. Стейкінг передбачає блокування активів у мережі для отримання винагороди з часом. Це може бути реалізовано через смарт-контракти, які забезпечують безпеку збереження заблокованих активів. У DeFi

користувачі мають можливість отримувати відсоток від своїх інвестицій за підтримку роботи мережі, що робить цей підхід популярним серед інвесторів.

Механізм штрафів та підтримка безпеки.

PoS забезпечує високий рівень безпеки завдяки механізму штрафів. Якщо валідатор ініціює або підтверджує підозрілу транзакцію, він ризикує втратити свій стейк або навіть бути заблокованим від участі в процесах верифікації в майбутньому. Такий підхід стимулює валідаторів дотримуватися чесної поведінки, оскільки фінансові ризики можуть бути значними.

Отже, Proof of Stake є енергоефективною та безпечною альтернативою Proof of Work, яка підвищує рівень децентралізації та знижує витрати на підтримку блокчейн-мереж. Використання механізму стейкінгу в DeFi ще більше підсилює його популярність, забезпечуючи інвесторам додаткові джерела доходу та підвищену безпеку транзакцій[29-30].

2.3. Криптовалютні гаманці

Криптовалютний гаманець - це програмне забезпечення, яке зберігає публічні та приватні ключі і взаємодіє з різними блокчейнами, що дозволяє користувачам надсилати та отримувати цифрову валюту і контролювати свій баланс.

За допомогою електронного гаманця можна зберігати, надсилати та отримувати різні валюти. Усередині гаманця криптовалюти не зберігаються як реальні гроші. Блокчейн фіксує та архівує кожну транзакцію. Транзакція з гаманцем передбачає переказ валюти між двома адресами. Для того, щоб транзакція відбулася, потрібен приватний ключ відправника і публічний ключ одержувача. Будь-яка кількість монет, що належить відправнику, може бути переведена на відкритий ключ (або адресу) одержувача. Для перевірки того, що транзакція була розпочата і виконана відправником, він підписує транзакції цифровим підписом, використовуючи свій приватний ключ [31].

Криптовалютні гаманці класифікуються на апаратні, програмні та паперові (останні наразі вважаються застарілими). Залежно від особливостей функціонування, зокрема наявності або відсутності підключення до мережі Інтернет, їх також поділяють на дві категорії: «гарячі» та «холодні». Основна відмінність між цими типами полягає в тому, що «гарячі» гаманці потребують постійного з'єднання з Інтернетом, тоді як «холодні» працюють в офлайн-режимі, що забезпечує вищий рівень безпеки для зберігання криптовалют.

Види криптогаманців:

1. Мобільний гаманець.

Мобільні гаманці — це програмні застосунки, призначені для встановлення на смартфони. Вони є зручним інструментом для користувачів, які здійснюють регулярні транзакції з криптовалютою як засобом оплати, оскільки забезпечують оперативний доступ до активів у будь-якому місці. Типовим прикладом є Trust Wallet [32].

2. Вебгаманець.

Вебгаманці забезпечують доступ до криптовалютних активів через інтернет-браузери, такі як Google Chrome, Firefox, Edge та інші. Вони поділяються на два основні типи: ті, що функціонують у вигляді вебсервісів, та ті, що працюють як розширення браузера з локальним зберіганням ключів. Прикладом такого гаманця є MetaMask [33].

3. Апаратний гаманець.

Апаратні гаманці — це спеціалізовані фізичні електронні пристрої, створені для безпечного зберігання криптовалют. Вони використовують генератор випадкових чисел для створення пари ключів: приватного та публічного. Згенеровані ключі зберігаються на пристрої, який не має постійного підключення до мережі Інтернет, що мінімізує ризики несанкціонованого доступу. Для здійснення транзакцій апаратний гаманець необхідно під’єднати до комп’ютера або смартфона. Прикладом є пристрій Trezor [34].

4. Паперовий гаманець.

Паперовий гаманець являє собою фізичний носій, на якому надрукований приватний ключ, часто у вигляді QR-коду. Завдяки офлайн-зберіганню ключів, такий формат забезпечує високий рівень захисту від кібератак, шкідливого програмного забезпечення та інших цифрових загроз.

5. Комп’ютерний гаманець.

Комп’ютерні криптовалютні гаманці функціонують на більшості операційних систем, зокрема Windows, Linux і macOS. Вони передбачають зберігання приватних ключів безпосередньо на жорсткому диску персонального комп’ютера. Для їх використання необхідне встановлення відповідного програмного забезпечення. Прикладом стаціонарного гаманця є Exodus, який також має мобільну версію [35].

Більшість криптовалютних гаманців класифікуються як кастодіальні або некастодіальні, причому основною відмінністю між ними є ступінь контролю користувача над приватними ключами.

Кастодіальні гаманці функціонують за участі посередницьких структур, зокрема криптовалютних бірж або інших централізованих платформ, які здійснюють зберігання та управління приватними ключами від імені користувача. Такий підхід забезпечує вищу зручність користування, зокрема можливість відновлення доступу до активів у разі втрати облікових даних. Водночас він передбачає делегування відповідальності за безпеку активів третій стороні, що зумовлює необхідність високого рівня довіри до сервісу.

Некастодіальні гаманці, навпаки, передбачають повну відповідальність користувача за зберігання приватних ключів і seed-фраз. У цьому випадку виключно користувач здійснює управління криптовалютними активами, що сприяє підвищенню рівня безпеки та конфіденційності. Однак така автономія супроводжується ризиком безповоротної втрати доступу до активів у разі втрати або компрометації ключів, оскільки механізми відновлення обмежені або взагалі відсутні.

Узагальнюючи, кастодіальні гаманці орієнтовані на користувачів, які надають перевагу зручності та простоті експлуатації, тоді як некастодіальні — на

осіб, що прагнуть повного контролю над своїми цифровими активами та підвищеного рівня безпеки [36].

Як уже зазначалось криптовалютний гаманець – це лише програмний або апаратний засіб, який дозволяє генерувати, зберігати та використовувати приватні й публічні ключі для виконання криптовалютних транзакцій, але сам він не зберігає кошти, а лише ключі, які дають доступ до них у блокчейні. Основними елементами гаманця є:

1. Приватний ключ - є основою всієї криптографічної безпеки у криптовалютній системі. Це унікальний 256-бітний (32-байтовий) номер, згенерований випадковим або детермінованим способом, який дозволяє власнику авторизовувати транзакції, пов’язані з конкретною адресою у блокчейні. Приватний ключ виступає своєрідним "паролем доступу" до цифрових активів. У разі його втрати — доступ до коштів стає назавжди неможливим. У разі компрометації — активи можуть бути вкрадені зловмисником. Тому приватний ключ є головним елементом, який потребує максимального захисту.

2. Публічний ключ генерується на основі приватного ключа за допомогою криптографічного алгоритму еліптичної кривої (наприклад, secp256k1 у Bitcoin). Хоча публічний ключ є похідним від приватного, він не дозволяє оберненого обчислення — тобто неможливо отримати приватний ключ, маючи лише публічний (за нинішнього стану криптографічної науки). Публічний ключ виконує роль "ідентифікатора" користувача в мережі: інші учасники блокчейну можуть перевірити транзакції за допомогою відкритого ключа та підтвердити, що їх дійсно підписав власник відповідного приватного ключа. У деяких криптовалютах (наприклад, Ethereum) адреса користувача напряму є результатом хешування публічного ключа.

3. Криптовалютна адреса — це хеш-функція, застосована до публічного ключа. У Bitcoin, наприклад, адреса генерується через послідовність: спочатку застосовується SHA-256 до публічного ключа, а потім RIPEMD-160, після чого додаються контрольна сума та кодування у форматі Base58Check. Це забезпечує не лише компактне представлення ключа, але й додатковий рівень

захисту від помилок при введенні. Адреса не містить конфіденційної інформації та може бути відкрито розповсюджена для отримання транзакцій. Таким чином, криптовалютна адреса виконує аналогічну функцію до номера банківського рахунку у традиційній фінансовій системі.

4. Мнемонічна фраза (seed - фраза) - є послідовністю з 12–24 слів, що генеруються відповідно до стандарту BIP39 із попередньо визначеного словника, який містить 2048 слів. Порядок слів у фразі має критичне значення, оскільки зміна навіть одного елемента або його позиції призводить до генерації іншого криптографічного ключа. Формування seed - фрази здійснюється на основі випадкового числа, згенерованого локально на пристрої користувача — комп'ютері або мобільному телефоні.

Мнемонічна фраза виконує функцію ключа для відновлення доступу до криптовалютних активів у разі втрати, викрадення, фізичного пошкодження або виходу з ладу пристрою. Завдяки їй можливо відновити гаманець шляхом доступу до відповідних даних у блокчейні. Проте збереження seed - фрази в електронному вигляді, навіть у зашифрованому форматі, на пристроях або серверах з підключенням до Інтернету створює загрозу компрометації з боку зловмисників. У разі викрадення мнемонічної фрази зловмисник може імпортувати її в новий гаманець і повністю заволодіти активами користувача.

Оскільки криптовалютні транзакції, як правило, є анонімними і незворотними, втрата або компрометація послідовності слів унеможливлює відновлення втрачених коштів. Тому експерти з безпеки настійливо рекомендують користувачам зберігати seed - фразу у фізичному вигляді, наприклад, записаною на папері. Проте й такий підхід має низку недоліків: паперові носії вразливі до пошкоджень унаслідок пожеж, затоплення або втрати через неуважність [37].

2.4. Висновок до розділу 2

У процесі дослідження були розглянуті основні криптографічні методи та технології, що забезпечують безпеку блокчейн-мереж і криптовалютних транзакцій. Визначено ключову роль хеш-функцій, криптографії з відкритим ключем та цифрових підписів у підтримці цілісності, прозорості та конфіденційності даних.

Механізми консенсусу, такі як Proof of Work (PoW) та Proof of Stake (PoS), довели свою ефективність у забезпеченні децентралізованої згоди та захисту від несанкціонованих змін у блокчейні. Розглянуто різні види криптовалютних гаманців та методи зберігання приватних ключів, включаючи симетричне шифрування AES-256, яке підвищує безпеку доступу до цифрових активів.

Таким чином, поєднання криптографічних методів, механізмів консенсусу та надійних підходів до захисту ключів формує стійку основу для безпечного функціонування блокчейн-технологій.

РОЗДІЛ ІІІ. ПІДВИЩЕННЯ БЕЗПЕКИ КРИПТОВАЛЮТНИХ ТРАНЗАКЦІЙ ЧЕРЕЗ ШИФРУВАННЯ ПРИВАТНИХ КЛЮЧІВ.

3.1. Захист приватних ключів у блокчейн-мережах: підвищення безпеки з використанням AES-256

На сучасному етапі розвитку блокчейн-технологій питання забезпечення безпеки криптовалютних транзакцій та зберігання приватних ключів є одним із найважливіших. Приватний ключ — це основа криптографічного захисту, яка гарантує виключний доступ до активів власника гаманця. Компрометація приватного ключа неминуче призводить до втрати контролю над криптовалютними коштами, тому необхідно застосовувати додаткові методи захисту.

Традиційна схема генерації криптовалютної адреси складається з таких основних етапів:

1. Генерація приватного ключа.
2. Отримання публічного ключа з приватного.
3. Формування криптовалютної адреси шляхом хешування публічного ключа.

Цей підхід хоч і є стійким до підбору завдяки криптографічним властивостям еліптичних кривих, проте він не враховує можливих ризиків, пов'язаних із крадіжкою приватного ключа при його зберіганні. Зокрема, якщо файл з приватним ключем буде викрадений або прочитаний сторонніми особами, доступ до активів буде втрачено.

Для підвищення рівня безпеки під час зберігання приватного ключа у даній роботі запропоновано використовувати алгоритм симетричного шифрування AES-256. Advanced Encryption Standard — це алгоритм симетричного шифрування, затверджений Національним інститутом стандартів і технологій США (NIST) [38].

Запропонована схема (рис. 3.1) включає додатковий крок — шифрування приватного ключа перед його збереженням або використанням. Це дозволяє забезпечити, що навіть у випадку викрадення даних отримати доступ до активів буде неможливо без правильного пароля.

Рисунок 3.1 Оновлена схема генерації криптовалютної адреси

Такий підхід забезпечує підвищений рівень безпеки шляхом додавання симетричного шифрування на етапі генерації та зберігання приватного ключа. Це ускладнює несанкціонований доступ до ключів навіть у випадку компрометації файлової системи або доступу до даних.

1. Генерація приватного ключа.

Приватний ключ є основним елементом криптографічної аутентифікації в блокчейн-системах. Він являє собою випадково згенероване 256-бітне число, яке забезпечує доступ до криптовалютних активів та дозволяє підписувати транзакції. В межах дослідження процес генерації приватного ключа було реалізовано з використанням бібліотеки ecdsa, що базується на еліптичних кривих.

Для генерації приватного ключа застосовується крива SECP256k1 — стандартна еліптична крива, що використовується в більшості блокчейн-мереж,

таких як Bitcoin та Ethereum. Це математичне представлення кривої у вигляді рівняння[39]:

(3.1)

$$y^2 = x^3 + 7$$

Приватний ключ є 32-байтовим числом, яке генерується криптографічно безпечно та зберігається у зашифрованому вигляді для запобігання несанкціонованому доступу.

2. Отримання публічного ключа.

Публічний ключ обчислюється на основі приватного ключа за допомогою еліптичних криптографічних перетворень. Для цього використовується множення точки на кривій SECP256k1[40]:

(3.2)

$$P = k \cdot G,$$

де

$P -$ згенерована точка, яка є публічним ключем;

$k -$ приватний ключ;

$G -$ фіксована початкова точка (генератор) на еліптичній кривій.

Публічний ключ має розмір 64 байти (32 байти для координати X та 32 байти для координати Y). Для оптимізації місця під час зберігання та передачі використовується стиснене представлення, яке складає 33 байти. У цьому випадку зберігається лише координата X та один біт для визначення парності координати Y.

3. Шифрування приватного ключа (AES-256).

В рамках підвищення безпеки приватного ключа було реалізовано симетричне шифрування за допомогою алгоритму AES-256 у режимі CBC[41]. Цей підхід забезпечує:

- Захист приватного ключа навіть у разі компрометації файлової системи;
- Неможливість доступу до ключа без знання пароля.

Процес шифрування включає наступні кроки:

1) Формування пароля користувача. Користувач вводить пароль, який є основою для створення AES-ключа.

2) Генерація ключа AES. З пароля створюється 256-бітний ключ за допомогою хешування алгоритмом SHA-256.

3) Генерація IV [42]. Для забезпечення криптографічної стійкості використовується випадково згенерований вектор ініціалізації (IV), який додається до кожного блоку даних.

4) Процес шифрування. Приватний ключ зашифровується з використанням AES-256 у режимі CBC:

(3.3)

$$C_i = E_k(P_i \oplus C_{i-1})$$

де

C_i −зашифрований блок даних;

P_i −відкритий текст (приватний ключ);

C_{i-1} −попередній зашифрований блок;

E_k −операція шифрування з ключем.

4. Формування криптовалютної адреси.

Адреса в блокчейні слугує ідентифікатором для отримання транзакцій. Вона створюється шляхом багатоетапного хешування публічного ключа:

1) Хешування публічного ключа за алгоритмом SHA-256:

(3.4)

$$H_1 = SHA256(PK)$$

2) Хешування результату за допомогою RIPEMD-160:

(3.5)

$$H_2 = RIPEMD160(H_1)$$

3) Додавання префікса мережі. Наприклад, для Bitcoin додається 1 байт (0x00).

4) Розрахунок контрольної суми. Застосовується подвійне SHA-256 до даних з префіксом, після чого беруться перші 4 байти як контрольна сума.

5) Формування остаточної адреси. Злиття префікса, хешу та контрольної суми кодується у форматі Base58Check [43], що дозволяє уникнути помилок під час копіювання або передачі адреси.

Таким чином, фінальна адреса є надійним індикатором отримання транзакцій і не розкриває інформацію про приватний ключ.

5. Дешифрування приватного ключа (AES-256).

1) Введення пароля. Користувач вводить пароль, який був використаний під час шифрування.

2) Генерація AES-ключа. Пароль перетворюється у 256-бітний ключ шляхом хешування SHA-256.

3) Режим CBC і використання IV. Виконується розшифрування кожного блоку даних, використовуючи той самий вектор ініціалізації (IV), що був застосований під час шифрування:

(3.6)

$$P_i = D_k(C_i) \oplus C_{i-1}$$

де

P_i −відновлений блок відкритого тексту;

C_i −зашифрований блок;

D_k −операція дешифрування з ключем k.

6. Переваги оновленого процесу генерації адреси.

Впровадження шифрування приватного ключа за допомогою AES-256 підвищує рівень безпеки криптографічного гаманця:

1) Захищає від викрадення у випадку фізичного доступу до пристрою;

2) Ускладнює несанкціонований доступ до криптоактивів навіть при компрометації файлової системи;

3) Забезпечує безпечне зберігання приватних ключів у зашифрованому вигляді.

3.2. Програмна реалізація генерації криптовалютної адреси з підвищеним рівнем безпеки (AES-256).

3.2.1. Загальна структура та призначення програми

Розроблений програмний код реалізує процес генерації криптовалютної адреси на основі еліптичних кривих, шифрування приватного ключа за алгоритмом AES-256 та побудову фінальної адреси у форматі Base58. Такий підхід підвищує рівень безпеки шляхом додавання симетричного шифрування приватного ключа, що знижує ризики несанкціонованого доступу.

3.2.2. Опис компонентів програмного коду

Імпорт необхідних бібліотек.

```
import os
import ecdsa
import hashlib
import base58
from Crypto.Cipher import AES
from Crypto.Util.Padding import pad, unpad
```

На першому етапі виконано підключення необхідних бібліотек:

os — для генерації випадкових чисел (приватного ключа).

ecdsa — для роботи з еліптичними кривими, що використовуються під час створення відкритого ключа.

hashlib — для обчислення хешів SHA-256 та RIPEMD-160.

base58 — для кодування адреси у форматі Base58Check.

Crypto.Cipher та Crypto.Util.Padding — для реалізації шифрування приватного ключа за допомогою AES-256.

Функція для генерації приватного ключа.

```
def generate_private_key():
    return os.urandom(32).hex()
```

Функція generate_private_key() відповідає за створення приватного ключа.

Використовується метод os.urandom(32), який генерує 32 байти випадкових даних (256 біт), що відповідає стандарту безпеки криптовалютних протоколів.

Метод .hex() конвертує байти у шістнадцятковий формат для зручності подальшого використання.

Приватний ключ є базою для створення відкритого ключа та кінцевої адреси користувача.

Функція для створення відкритого ключа на основі приватного ключа.

```
def private_to_public(private_key_hex):
    private_key_bytes = bytes.fromhex(private_key_hex)
    sk = ecdsa.SigningKey.from_string(private_key_bytes,
curve=ecdsa.SECP256k1)
    vk = sk.verifying_key
    public_key_bytes = b'\x04' + vk.to_string()
    return public_key_bytes.hex()
```

Функція private_to_public() виконує перетворення приватного ключа у відкритий ключ:

Вхідний параметр — це шістнадцяткове представлення приватного ключа.

Конвертація в байтовий формат (bytes.fromhex).

Створення об'єкта SigningKey, що використовує еліптичну криву SECP256k1.

Генерація відкритого ключа (verifying_key) через множення точки генератора на еліптичній кривій.

До відкритого ключа додається префікс 0x04, що вказує на некомпресовану форму ключа.

Фінальний результат конвертується у шістнадцятковий формат для зручності використання.

Функція для створення адреси.

```
def public_to_address(public_key_hex):
    public_key_bytes = bytes.fromhex(public_key_hex)
    sha256_hash = hashlib.sha256(public_key_bytes).digest()
    ripemd160_hash = hashlib.new('ripemd160', sha256_hash).digest()
    address_bytes = b'\x00' + ripemd160_hash
    checksum = hashlib.sha256(hashlib.sha256(address_bytes).digest()).diges
t()[:4]
    final_address = base58.b58encode(address_bytes + checksum).decode()
    return final_address
```

Процес створення адреси включає:

Хешування відкритого ключа за допомогою алгоритму SHA-256.

Додаткове хешування отриманого результату через RIPEMD-160.

Додавання префікса мережі (0x00 для Bitcoin) до отриманого хешу.

Формування контрольної суми — подвійне SHA-256 від хешу з префіксом. Беруться перші 4 байти для забезпечення цілісності.

Кодування у форматі Base58Check, що спрощує передачу адреси та усуває схожі символи (наприклад, "0" та "O").

Функція для шифрування приватного ключа (AES-256).

```
def encrypt_private_key(private_key_hex, password):
    key = hashlib.sha256(password.encode()).digest()  # Генерація ключа AES з
пароля
    cipher = AES.new(key, AES.MODE_CBC)
    encrypted_data = cipher.encrypt(pad(bytes.fromhex(private_key_hex),
AES.block_size))
    return cipher.iv.hex() + encrypted_data.hex()  # IV (ініціалізаційний вектор)
+ шифротекст
```

Шифрування приватного ключа реалізовано за допомогою алгоритму AES-256 у режимі CBC:

Пароль користувача хешується алгоритмом SHA-256 для формування 256-бітного AES-ключа.

Створюється об'єкт шифрування з режимом CBC (блочне шифрування з використанням ініціалізаційного вектора — IV).

Приватний ключ доповнюється до розміру блоку AES (pad).

Формується результат: IV + зашифровані дані.

Функція для розшифрування приватного ключа.

```
def decrypt_private_key(encrypted_private_key_hex, password):
    key = hashlib.sha256(password.encode()).digest()
    encrypted_private_key_bytes = bytes.fromhex(encrypted_private_key_hex)
    iv = encrypted_private_key_bytes[:16] #Виділення IV
    encrypted_data = encrypted_private_key_bytes[16:] #Виділення шифрованого ключа
    cipher = AES.new(key, AES.MODE_CBC, iv)
    decrypted_data = unpad(cipher.decrypt(encrypted_data), AES.block_size)
    return decrypted_data.hex()
```

Розшифрування виконується у зворотному порядку:

З введеного пароля генерується AES-ключ.

Виділяються IV (перші 16 байт) та зашифровані дані.

Відбувається розшифрування та видалення додаткових байтів (unpad).

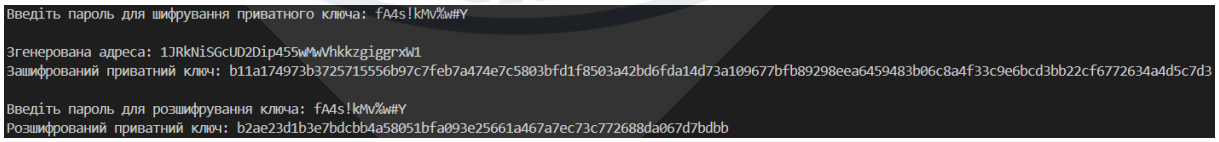

Рисунок 3.2 Результат роботи програми

3.3. Висновок до розділу 3

Запропонована реалізація процесу генерації криптовалютної адреси з додатковим шифруванням приватного ключа підвищує рівень безпеки та стійкість до несанкціонованого доступу. Метод шифрування AES-256 забезпечує захист навіть у випадку компрометації файлової системи.

ВИСНОВКИ

У процесі виконання бакалаврської роботи було розглянуто теоретичні та практичні аспекти генерації криптовалютних адрес із підвищеним рівнем безпеки шляхом шифрування приватного ключа за допомогою алгоритму AES-256. Запропонований підхід базується на класичній технології формування адрес на основі криптографічних методів, включаючи еліптичні криві (SECP256k1) та хешування (SHA-256, RIPEMD-160). Основною новизною роботи стало інтегрування симетричного шифрування AES-256 для захисту приватного ключа, що значно підвищує стійкість до атак з боку зловмисників.

Запропонована схема генерації криптовалютних адрес охоплює такі етапи:

Генерація приватного ключа, що реалізується за допомогою криптографічно безпечного генератора випадкових чисел.

Отримання публічного ключа шляхом використання еліптичних кривих SECP256k1.

Шифрування приватного ключа із застосуванням AES-256 у режимі CBC для підвищення конфіденційності.

Формування криптовалютної адреси з використанням алгоритмів SHA-256 та RIPEMD-160 для отримання унікального хешу публічного ключа.

Під час дослідження також було здійснено порівняльний аналіз методів зберігання приватних ключів, включаючи апаратні, програмні та паперові гаманці. Визначено, що використання симетричного шифрування в запропонованій моделі знижує ризик компрометації ключа під час зберігання на пристрої користувача. Це забезпечує додатковий рівень безпеки у випадку фізичного доступу до пристрою або несанкціонованого втручання.

Таким чином, результати дослідження підтверджують ефективність інтеграції алгоритму AES-256 для шифрування приватного ключа як засобу підвищення безпеки криптовалютних транзакцій. Запропонована модель може бути адаптована для використання в різних криптовалютних платформах,

сприяючи захисту активів користувачів від кібератак та підвищуючи загальний рівень конфіденційності операцій.

Цей підхід відкриває перспективи для подальших досліджень у напрямку підвищення безпеки криптовалютних систем, включаючи інтеграцію мультипідписів, використання алгоритмів постквантового шифрування та впровадження більш стійких методів зберігання приватних ключів.

СПИСОК ВИКОРИСТАНИХ ПОСИЛАНЬ

1. Basic Aspects of Cryptocurrencies. URL: https://www.researchgate.net/publication/292586903_Basic_Aspects_of_Cryptocurrencies (дата звернення 25.02.2025).

2. Cryptocurrency – Definition, Functions, Advantages And Risks. URL: https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=&ved=2ahUKEwjftOLi75ONAxUNGxAIHaZ0FngQFnoECB4QAQ&url=http%3A%2F%2Fjournals-lute.lviv.ua%2Findex.php%2Fpidpr-torgi%2Farticle%2Fdownload%2F935%2F886%2F&usg=AOvVaw02As_7sP55POYLG9c9qidB&opi=89978449 (дата звернення 25.02.2025).

3. Pros and Cons of Cryptocurrency: A Brief Overview. URL: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=5093439 (дата звернення 27.02.2025).

4. Decentralized Money: A Comprehensive Review on Cryptocurrencies. URL: https://www.researchgate.net/publication/374739909_Decentralized_Money_A_Comprehensive_Review_on_Cryptocurrencies (дата звернення 27.02.2025).

5. Blockchain Beyond the Hype A Practical Framework for Business Leaders (дата звернення 27.02.2025).

6. Sandeep Kumar Panda ·Ajay Kumar Jena ·Santosh Kumar Swain ·Suresh Chandra Satapathy. Blockchain Technology:Applications and Challenges (дата звернення 27.02.2025).

7. A Brief History of Blockchain Technology That Everyone Should Read. URL: https://kriptomat.io/blockchain/history-of-blockchain/ (дата звернення 04.03.2025).

8. History and evolution of blockchain technology. URL: https://medium.com/@psnavya90/history-and-evolution-of-blockchain-technology-5f0de0508f13 (дата звернення 04.03.2025).

9. International Research Journal of Engineering and Technology (IRJET). Blockchain Technology: History, Concepts, and Applications (дата звернення 04.03.2025).

10. Mastering Blockchain. Distributed ledger technology, decentralization, and smart contracts explained. URL: https://users.cs.fiu.edu/~prabakar/cen5079/Common/textbooks/Mastering_Blockchain_2nd_Edition.pdf (дата звернення 04.03.2025).

11. What Is a Block in the Crypto Blockchain, and How Does It Work? URL: https://www.investopedia.com/terms/b/block-bitcoin-block.asp#:~:text=A%20block%20is%20a%20file,new%20blocks%20can%20be%20created (дата звернення 04.03.2025).

12. Types of Nodes in Blockchain. URL: https://utimaco.com/service/knowledge-base/blockchain/what-are-the-types-of-nodes-in-blockchain#:~:text=Blockchain%20nodes%20are%20the%20moderators,determine%20the%20types%20of%20nodes (дата звернення 04.03.2025).

13. Blockchain transaction. URL: https://www.web3labs.com/blockchain-explained-what-is-a-blockchain-transaction#:~:text=A%20transaction%20represents%20an%20action,interacting%20with%20a%20smart%20contract (дата звернення 09.03.2025).

14. Consensus Mechanisms. URL: https://usa.visa.com/solutions/crypto/consensus-mechanisms.html (дата звернення 09.03.2025).

15. Blockchain in Data Analytics. URL: https://www.researchgate.net/publication/343601688_Introduction_to_Blockchain (дата звернення 09.03.2025).

16. Blockchain Technology and its Types-A Short Review. URL: https://www.researchgate.net/publication/359051731_Blockchain_Technology_and_its_Types-A_Short_Review (дата звернення 09.03.2025).

17. An Introduction to Private Blockchain. URL: https://www.geeksforgeeks.org/private-blockchain/ (дата звернення 09.03.2025).

18. Elisa, N., Yang, L., Li, H., Chao, F. & Naik, N. (2019). Consortium blockchain for security and privacy-preserving in e-government systems (дата звернення 09.03.2025).

19. A Consortium Blockchain-Based Secure and Trusted Electronic Portfolio Management Scheme. URL: https://www.mdpi.com/1424-8220/22/3/1271 (дата звернення 21.03.2025).

20. Hybrid Blockchain. URL: https://www.bibliomed.org/mnsfulltext/71/71-1589089941.pdf?1746727080 (дата звернення 21.03.2025).

21. 51% Attack. URL: https://www.coinbase.com/ru/learn/crypto-glossary/what-is-a-51-percent-attack-and-what-are-the-risks (дата звернення 21.03.2025).

22. Sybil Attack. URL: https://www.coinbase.com/ru/learn/crypto-glossary/what-is-a-sybil-attack-in-crypto (дата звернення 21.03.2025).

23. Blockchain Security. URL: https://www.kaspersky.com/resource-center/definitions/what-is-blockchain-security (дата звернення 10.04.2025).

24. Hashing: The Backbone of Blockchain Technology. URL: https://shardeum.org/blog/blockchain-hashing/ (дата звернення 10.04.2025).

25. Public Key Cryptography in Blockchain. URL: https://data-flair.training/blogs/public-key-cryptography/ (дата звернення 10.04.2025).

26. Digital signatures. URL: https://www.coinbase.com/ru/developer-platform/discover/dev-foundations/digital-signatures (дата звернення 23.04.2025).

27. Consensus in Blockchain.URL: https://cyberscope.medium.com/what-is-consensus-in-blockchain-2742be9b7af0 (дата звернення 23.04.2025).

28. Proof of Work. URL: https://www.scalingparrots.com/en/proof-of-work-how-it-works/#:~:text=The%20Bitcoin%20Network%3A%20Bitcoin%20is,on%20a%20shared%20public%20ledger (дата звернення 23.04.2025).

29. Consensus mechanisms in blockchain. URL: https://hacken.io/discover/consensus-mechanisms/ (дата звернення 14.05.2025).

30. Proof of Work vs. Proof of Stake in Cryptocurrency. URL: https://www.researchgate.net/publication/369870684_Proof_of_Work_vs_Proof_of_Stake_in_Cryptocurrency (дата звернення 14.05.2025).

31. Cryptocurrency wallets: assessment and security. URL: https://www.researchgate.net/publication/369477425_Cryptocurrency_wallets_assessment_and_security (дата звернення 14.05.2025).

32. Trust. URL: https://trustwallet.com (дата звернення 17.05.2025).

33. Metamask. URL: https://metamask.io (дата звернення 17.05.2025).

34. Trezor. URL: https://trezor.io (дата звернення 17.05.2025).

35. Exodus. URL: https://www.exodus.com (дата звернення 17.05.2025).

36. Що таке криптогаманець і як його вибрати? URL: https://academy.binance.com/uk-UA/articles/crypto-wallet-types-explained (дата звернення 17.05.2025).

37. Securing Cryptocurrency Wallet Seed Phrase Digitally with Blind Key Encryption. URL: https://www.researchgate.net/publication/348544696_Securing_Cryptocurrency_Wallet_Seed_Phrase_Digitally_with_Blind_Key_Encryption (дата звернення 17.05.2025).

38. Advanced Encryption Standard. URL: https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.197-upd1.pdf (дата звернення 17.05.2025).

39. Mathematical and Economic Foundations of Bitcoin. URL: https://www.researchgate.net/publication/340651746_Mathematical_and_Economic_Foundations_of_Bitcoin (дата звернення 17.05.2025).

40. Research on Elliptic Curve Crypto System with Bitcoin Curves – SECP256k1, NIST256p, NIST521p and LLL URL: https://www.researchgate.net/publication/369069505_Research_on_Elliptic_Curve_C

rypto_System_with_Bitcoin_Curves_-_SECP256k1_NIST256p_NIST521p_and_LLL (дата звернення 18.05.2025).

41. Enhanced and authenticated cipher block chaining mode. URL: https://www.researchgate.net/publication/369299515_Enhanced_and_authenticated_cipher_block_chaining_mode (дата звернення 18.05.2025).

42. Hybrid Encryption System with Initialization Vector for Secure Data Transmission. URL: https://www.researchgate.net/publication/382947361_Hybrid_Encryption_System_with_Initialization_Vector_for_Secure_Data_Transmission (дата звернення 18.05.2025).

43. Base58Check encoding. URL: https://en.bitcoin.it/wiki/Base58Check_encoding (дата звернення 18.05.2025).

ДЕКЛАРАЦІЯ

про дотримання академічної доброчесності

Я, *Єрмак Дмитро Миколайович, здобувач вищої освіти, ООП «Кібербезпека», автор кваліфікаційної (бакалаврської) роботи на тему: «Розробка генератора криптовалютних адрес для блокчейн-транзакцій»*

Повністю вказується ПІБ та статус (освітня (освітньо-наукова) програма – для здобувачів вищої освіти, назва кваліфікаційної роботи)

що нижче підписалась/підписався, розуміючи та підтримуючи загальновизнані засади справедливості, доброчесності та законності,

ЗОБОВ'ЯЗУЮСЬ:

дотримуватися принципів та правил академічної доброчесності, що визначені законодавством України, локальними нормативними актами Донецького національного університету імені Василя Стуса, положеннями, правилами, умовами, визначеними іншими суб'єктами, та не допускати їх порушення.

ПІДТВЕРДЖУЮ:

що мені відомі положення статті 42 Закону України «Про освіту»;

що у даній роботі не представляла/представляв чиїсь роботи повністю або частково як свої власні. Там, де я скористалася/скористався працею інших, я зробила/зробив відповідні посилання на джерела інформації;

що дана робота не передавалась іншим особам і подається вперше, не порушує авторських та суміжних прав закріплених статтями 21-25 Закону України «Про авторське право та суміжні права», а дані та інформація не отримувались в недозволений спосіб.

УСВІДОМЛЮЮ:

що ця робота може бути перевірена університетом на плагіат або інші порушення академічної доброчесності, в тому числі з використанням спеціалізованих сервісів;

що у разі порушення академічної доброчесності, до мене можуть бути застосовані процедури, передбачені законодавством України та Кодексом академічної доброчесності та корпоративної етики Донецького національного університету імені Василя Стуса, іншими локальними нормативними актами університету, та я можу бути притягнута/притягнутий до академічної відповідальності.

_____ _____

(дата) (підпис)