Міністерство освіти і науки України
Національний технічний університет України
«Київський політехнічний інститут імені Ігоря Сікорського»
Фізико-технічний інститут

Технологія блокчейн та розподілені системи

Лабораторна робота 2
“Реалізація смарт-контракту або анонімної криптовалюти”

Виконали:
Студенти групи ФБ-42мп
Алькова Аліна, Юлія Легойда, Рябко Дмитро

Тема: Реалізація смарт-контракту або анонімної криптовалюти.
Мета роботи: «Отримання навичок роботи із смарт-контрактами або анонімними криптовалютами»

Завдання на лабораторну роботу

Для першого типу лабораторних:
-дослідження методів анонімізації/деанонімізації запропонованої криптовалюти із аналізом складності проведення атак деанонімізації і втрат ефективності анонімних криптовалют у порівнянні із Bitcoin/Litecoin;
-оцінка та обґрунтування необхідних ресурсів (гасу і ефіру), потрібних для функціонування смарт-контракту.

1. Методи деанонімізації/анонімізації у Monero та аналіз стійкості до атак

1.1 Методи анонімізації у Monero

Monero є однією з провідних криптовалют, що робить акцент на конфіденційності, використовуючи набір технологій, які забезпечують анонімність транзакцій на рівні блокчейну. Основними інструментами, які дозволяють досягти цього рівня приватності, є **кільцеві підписи, приховані адреси та конфіденційні кільцеві транзакції (RingCT).** Кожен із цих методів виконує специфічну роль у приховуванні ключових аспектів транзакції: відправника, одержувача та суми.

Кільцеві підписи (Ring Signatures) є основою для забезпечення анонімності відправника. Ця технологія дозволяє змішувати справжнього відправника транзакції з групою інших потенційних відправників, які називаються "міксинами". Коли транзакція створюється, кільцевий підпис включає кілька відкритих ключів, лише один із яких належить справжньому відправнику. Для зовнішнього спостерігача неможливо визначити, який саме ключ є справжнім, оскільки всі вони виглядають однаково правдоподібними. Це створює ефект "заплутування", який значно ускладнює відстеження джерела транзакції. З часом Monero збільшила мінімальний розмір кільця (наразі це 16), що ще більше підвищує рівень анонімності, оскільки більша кількість міксинів робить аналіз менш ефективним.

Приховані адреси (Stealth Addresses) відповідають за захист одержувача транзакції. У Monero кожна транзакція генерує унікальну одноразову адресу для одержувача, яка не пов’язана з його основною публічною адресою. Це означає, що навіть якщо хтось спостерігає за блокчейном, він не може пов’язати транзакцію з конкретною адресою одержувача. Відправник використовує публічний ключ одержувача для створення цієї одноразової адреси, а одержувач може розпізнати та отримати доступ до коштів за допомогою свого приватного ключа. Такий підхід усуває можливість аналізу блокчейну для визначення, хто отримав кошти, що є значною перевагою порівняно з Bitcoin, де адреси одержувачів є публічними.

Конфіденційні кільцеві транзакції (RingCT), введені в 2017 році, приховують суму транзакції. До цього в Monero суми транзакцій залишалися видимими, що дозволяло проводити певний аналіз, наприклад, зіставлення сум із відомими платежами. RingCT використовує криптографічні методи, зокрема зобов’язання Педерсена (Pedersen Commitments), для приховування суми, зберігаючи при цьому можливість перевірити, що сума вхідних і вихідних коштів збігається, без розкриття конкретних значень. Це забезпечує повну конфіденційність усіх трьох компонентів транзакції: відправника, одержувача та суми.

Monero вирізняється своєю здатністю забезпечувати повну on-chain анонімність, що є значною перевагою порівняно з Bitcoin, де конфіденційність залежить від зовнішніх інструментів,

таких як міксери чи Lightning Network. Комбінація кільцевих підписів, прихованих адрес і RingCT створює міцний бар'єр для відстеження, що робить Monero однією з найприватніших криптовалют на ринку.

1.2 Методи деанонімізації Monero та аналіз стійкості до атак

Незважаючи на потужні механізми анонімізації, Monero не є абсолютно невразливою до деанонімізації. Існують теоретичні та практичні методи, які дослідники та аналітичні компанії застосовували для спроб розкриття анонімності транзакцій. Ці методи включають **статистичний аналіз кільцевих підписів, аналіз часу та шаблонів транзакцій, а також атаки, що використовують недоліки в налаштуваннях мережі**, таких як низький розмір кільця. Крім того, урядові організації та приватні компанії, такі як Chainalysis, активно досліджують способи деанонімізації Monero, що додає ще один вимір до аналізу її стійкості.

Статистичний аналіз кільцевих підписів був одним із перших методів, які застосовувалися для деанонімізації Monero. У ранніх версіях мережі, коли розмір кільця був меншим (наприклад, 5–7), дослідники могли аналізувати набори міксинів, щоб визначити, які ключі частіше з'являються в певних транзакціях. Якщо, наприклад, один ключ регулярно використовувався як міксина, але ніколи як справжній відправник, це могло вказувати на його фіктивність. Такі методи, відомі як "аналіз витрачених виходів" (spent output analysis), дозволяли звузити коло потенційних відправників. Проте після введення обов'язкового розміру кільця 11 (а згодом 16) і вдосконалення алгоритмів вибору міксинів ці атаки стали значно менш ефективними. Сучасні кільцеві підписи включають достатню кількість ключів, щоб зробити статистичний аналіз трудомістким і неточним, особливо без доступу до додаткових даних.

Аналіз часу та шаблонів транзакцій є ще одним вектором атак. Оскільки Monero не приховує час створення транзакцій, зловмисники можуть зіставляти часові мітки з зовнішніми подіями, наприклад, із відомими платежами на біржах чи в магазинах. Якщо користувач регулярно проводить транзакції в певний час або з певною періодичністю, це може допомогти створити профіль його поведінки. Крім того, якщо транзакція Monero проходить через біржу, яка вимагає ідентифікації користувача (KYC), інформація про вхідні або вихідні кошти може бути пов'язана з реальною особою. Однак такі атаки залежать від зовнішніх джерел інформації, а не від слабкостей самого блокчейну Monero, що обмежує їх ефективність.

Атаки при низькому розмірі кільця були актуальними в минулому, коли користувачі могли самостійно вибирати розмір кільця, іноді встановлюючи його занадто низьким (наприклад, 3–5). У таких випадках ймовірність правильного визначення відправника зростала, оскільки менша кількість міксинів полегшувала аналіз. Після оновлень протоколу, які зробили великий розмір кільця обов'язковим, ця вразливість була усунута. Сучасні транзакції Monero використовують достатньо великий набір міксинів, щоб зробити подібні атаки непрактичними без значних обчислювальних ресурсів.

Дослідження з боку урядів і компаній, таких як IRS (Internal Revenue Service) і Chainalysis, є важливим аспектом аналізу стійкості Monero. У 2020 році IRS оголосила тендер на розробку інструментів для деанонімізації Monero, що свідчить про інтерес урядів до подолання її конфіденційності. Компанії, такі як Chainalysis, які спеціалізуються на аналізі блокчейнів, повідомляли про розробку методів відстеження Monero, хоча деталі їхніх підходів залишаються закритими. Ймовірно, вони поєднують аналіз блокчейну з зовнішніми даними, такими як інформація з бірж, IP-адреси вузлів або метадані транзакцій. Проте публічно доступні звіти вказують, що ці методи мають обмежену ефективність проти сучасних версій Monero, особливо якщо користувачі дотримуються найкращих практик, таких як уникнення повторного використання адрес і використання власних вузлів.

Поточна ефективність атак на Monero залишається низькою завдяки постійним оновленням протоколу. Введення обов'язкового великого розміру кільця, вдосконалення алгоритмів вибору міксинів і широке використання RingCT значно ускладнили деанонімізацію. Дослідження, проведені в 2017–2020 роках, показали, що ранні вразливості, такі як аналіз витрачених виходів, більше не є ефективними. Навіть у випадках, коли зловмисники мають доступ до значних обчислювальних ресурсів, успішна деанонімізація зазвичай вимагає комбінації даних із зовнішніх джерел, таких як біржі чи компрометовані вузли. Це робить Monero однією з найстійкіших до деанонімізації криптовалют на ринку.

2. Порівняльний аналіз з Bitcoin та Litecoin

2.1 Транзакції

Bitcoin

Транзакція Bitcoin відбувається тоді, коли сторона передає право власності на токен BTC або його частину іншій стороні. На відміну від жорсткої валюти, окремі біткоїни не мають жодної реальної форми. Натомість вони існують як лінії коду, записані в цифровому записі під назвою блокчейн. Транзакція стосується процесу передачі ідентифікаційного коду отримання Bitcoin іншій організації.

Люди доводять право власності на Bitcoin, пов'язуючи свій ідентифікаційний номер зі своєю персональною адресою Bitcoin. Ці адреси Bitcoin також називаються відкритим ключем, як ваше ім'я користувача в соціальних мережах. Він використовується для зберігання інформації про всі біткоїни, якими ви наразі володієте. Під час транзакції ви погоджуєтеся надіслати або отримати певну суму Bitcoin. Відправляючи BTC, ви підписуєте транзакцію за допомогою приватного ключа, який по суті діє як пароль і доводить, що маєте право переказати Bitcoin на іншу адресу.

Основна мета Bitcoin — забезпечити публічну і незмінну систему переказу коштів без посередників. Усі транзакції зберігаються у відкритому блокчейні, доступному для перегляду будь-якому користувачу. Адреси в Bitcoin є псевдонімними: вони не містять імен чи персональних даних, однак кожен може переглянути повну історію транзакцій цієї адреси, включно із сумами. Через це Bitcoin **не є анонімною** криптовалютою — при використанні спеціалізованих аналітичних інструментів можливе відстеження зв'язків між адресами й навіть ідентифікація користувачів.

Bitcoin використовує алгоритм майнінгу **SHA-256**, який добре підходить для ASIC-пристроїв. Час генерації одного блоку — приблизно 10 хвилин. Загальна емісія обмежена 21 мільйоном монет.

Litecoin

Litecoin (LTC) був створений у 2011 році як «полегшена» версія Bitcoin. Його блокчейн заснований на тому ж принципі, що й Bitcoin, але має ряд відмінностей: менший час генерації блоку (близько 2.5 хвилини) та інший алгоритм майнінгу — **Scrypt**, який спочатку був спрямований на протидію ASIC-пристроям, хоча з часом ця перевага була втрачена.

Як і у Bitcoin, **всі транзакції в Litecoin є публічними**. Це означає, що адреси і суми переказів доступні для будь-якого користувача, і конфіденційність користувача є лише умовною. Litecoin часто використовується для тестування нових функцій перед впровадженням у Bitcoin.

Загальний обсяг емісії Litecoin складає 84 мільйони монет, що вчетверо більше за Bitcoin.

Monero

Monero (XMR), запущена в 2014 році, є криптовалютою, орієнтованою на конфіденційність та анонімність. На відміну від Bitcoin і Litecoin, де інформація про транзакції доступна публічно, Monero повністю приховує:

- адресу відправника (за допомогою кільцевих підписів — ring signatures),
- адресу отримувача (stealth addresses),
- суму транзакції (Ring Confidential Transactions або RingCT).

Ці функції працюють автоматично для всіх користувачів, тому всі транзакції в Monero є приватними за замовчуванням. Це унеможливлює аналіз блокчейну для виявлення зв'язків між користувачами. Monero використовує алгоритм RandomX, який оптимізований для CPU-майнінгу та забезпечує опір ASIC-пристроям, сприяючи децентралізації. Блоки генеруються кожні 2 хвилини, а емісія монет є нескінченною (Monero має концепцію "tail emission" — постійна невелика винагорода для стимулювання майнінгу).

2.2 Розмір транзакції
У цьому підпункті буде проведено порівняльний аналіз розміру транзакцій у трьох криптовалютах: Bitcoin, Litecoin та Monero, з урахуванням особливостей структури блоків, впливу на продуктивність та вимог до системних ресурсів.

Bitcoin
Bitcoin зберігає всі транзакції у відкритому блокчейні без додаткового шифрування. Через це середній розмір транзакції є відносно невеликим — близько 300 байт. Це дозволяє зменшити загальне навантаження на мережу, полегшує зберігання даних та прискорює синхронізацію нодів. Максимальний розмір блоку з використанням SegWit становить до 4 МБ, чого достатньо для обробки кількох тисяч транзакцій у кожному блоці. Такий підхід дозволяє досягти високої ефективності, але повністю відкриває інформацію про відправників, одержувачів та суми переказів.

Litecoin
Litecoin має аналогічну структуру транзакцій до Bitcoin, проте завдяки меншому інтервалу між блоками (2.5 хв проти 10 хв у BTC), мережа обробляє більше транзакцій за той самий проміжок часу. Середній розмір транзакції у Litecoin становить приблизно 300–400 байт. Блоки мають той самий ліміт у 4 МБ, тому пропускна здатність є дещо вищою. Як і Bitcoin, Litecoin не забезпечує приватності транзакцій, усі дані є публічно доступними в блокчейні.

Monero
Monero побудовано з орієнтацією на повну конфіденційність. Усі транзакції в мережі за замовчуванням захищені за допомогою складних криптографічних методів: кільцевих підписів (Ring Signatures), прихованих адрес (Stealth Addresses) та конфіденційних транзакцій (RingCT). Це суттєво збільшує розмір кожної транзакції — в середньому від 1.5 до 2.5 кілобайтів, що у 5–8 разів більше, ніж у Bitcoin або Litecoin. Через це блоки в мережі Monero мають динамічний розмір, який адаптується до навантаження, але це також призводить до зростання блокчейну та збільшених вимог до зберігання і обчислень.

Monero — більше даних через криптографію → більші блоки.
Bitcoin — легше синхронізувати, менше вимог.

Критерій	Bitcoin	Litecoin	Monero
Середній розмір транзакції	~300 байт	~300–400 байт	~1.5–2.5 кілобайт

Максимальний розмір блоку	4 МБ (з SegWit)	4 МБ (з SegWit)	Динамічний
Анонімність	Ні	Ні	Так (за замовчуванням)
Вимоги до ресурсів	Низькі	Низькі	Високі

2.3 Продуктивність

У цьому підрозділі ми розглянемо продуктивність криптовалют Bitcoin, Litecoin та Monero за трьома ключовими критеріями: анонімність, швидкість обробки транзакцій та розмір комісій. Ці характеристики мають прямий вплив на зручність використання криптовалюти в реальному світі, масштабованість системи та прийнятність для різних категорій користувачів.

Bitcoin

Анонімність:
Bitcoin не забезпечує справжньої анонімності. Всі транзакції записуються в публічному блокчейні, де можна простежити шлях кожної монети від створення до поточного власника. Хоча імена користувачів не вказуються, за допомогою аналітики блокчейну та зв'язку з IP-адресами або біржами можлива деанонімізація користувачів. Це робить Bitcoin **псевдонімним**, але не анонімним.

Швидкість:
Bitcoin має інтервал генерації блоку близько **10 хвилин**, що призводить до середнього часу підтвердження транзакції від **10 до 60 хвилин**, залежно від завантаженості мережі. Швидкість транзакцій вважається **середньою** для криптовалют. Високе навантаження на мережу може значно впливати на час обробки.

Комісії:
Комісії в Bitcoin змінюються залежно від попиту. У періоди пікового навантаження вони можуть досягати кількох доларів за одну транзакцію. Проте в стандартних умовах комісії залишаються **нижчими**, ніж у Monero, але **вищими**, ніж у Litecoin.

Litecoin

Анонімність:
Litecoin, як і Bitcoin, не має вбудованих засобів для приховування особистих даних. Усі транзакції зберігаються у відкритому доступі, що унеможливлює повну конфіденційність. Тобто анонімність **відсутня**, і транзакції легко простежити.

Швидкість:
Завдяки коротшому часу створення блоку (**2.5 хвилини**), Litecoin дозволяє користувачам отримувати підтвердження набагато швидше. Це робить його привабливим для повсякденних платежів, мікротранзакцій та торгових операцій. Таким чином, Litecoin має **вищу** швидкість у порівнянні з Bitcoin та Monero.

Комісії:
Litecoin є однією з криптовалют з найнижчими комісіями. У більшості випадків користувачі

сплачують **менше ніж 1 цент** за транзакцію. Це робить Litecoin дуже ефективним з точки зору вартості переказів.

Monero

Анонімність:
Monero є еталоном приватності серед криптовалют. Усі транзакції в ньому за замовчуванням **повністю анонімні**, завдяки використанню кільцевих підписів, прихованих адрес та RingCT. Це унеможливлює простеження відправника, отримувача і суми переказу, що гарантує високий рівень конфіденційності навіть у порівнянні з іншими анонімними криптовалютами.

Швидкість:
Monero використовує динамічний розмір блоку та адаптивні параметри мережі. Середній час створення блоку становить близько **2 хвилин**, проте складність обробки шифрованих транзакцій зменшує загальну пропускну здатність. Тому **швидкість обробки вважається середньою**, оскільки кожна транзакція займає більше ресурсів, ніж у Bitcoin або Litecoin.

Комісії:
Високий рівень анонімності вимагає складних криптографічних обчислень, що впливає на розмір транзакцій та, відповідно, **підвищує комісії**. Хоча вони залишаються прийнятними, зазвичай комісії Monero є **вищими**, ніж у Bitcoin та Litecoin. Це є певною платою за повну приватність.

3. Оцінка ресурсів для смарт-контракту (Gas, Ether)

Monero не підтримує смарт-контракти напряму, тому всі подальші приклади стосуються Ethereum. Оцінка ресурсів у Ethereum вимірюється в gas, а розрахована вартість — у ETH.

3.1. Поняття Gas та Ether
Gas — внутрішня одиниця обчислювальної роботи в Ethereum; кожна операція EVM (запис у пам’ять, читання, арифметика, виклик контракту тощо) має свою вартість у gas.
Gas limit — максимальна кількість gas, яку відправник готовий витратити на транзакцію; невикористаний gas повертається.
Gas price — ціна одного gas у Wei (1 Gwei = 10^9 Wei).
Ether (ETH) — «грошова» одиниця мережі Ethereum; загальна вартість транзакції в ETH обчислюється як добуток фактично використаного gas на його ціну.

3.2. Приклад простого смарт-контракту
Типи контрактів для аналізу:
- ERC-20 токен (стандартний шаблон OpenZeppelin)
- Простий голосувальний контракт (SimpleVote)

Витрати gas при розгортанні:
- ERC-20 ≈ 300 000–400 000 gas
- SimpleVote ≈ 200 000 gas

Витрати gas при виклику функцій:
- Передача токенів (transfer) ≈ 50 000 gas
- Дозвіл списання (approve) ≈ 45 000 gas
- Перший виклик голосу (vote) ≈ 40 000–60 000 gas
- Повторний виклик із revert ≈ 21 000 gas

3.3. Розрахунок вартості в ETH (і USD)
Формула: вартість (ETH) = використаний gas × gas price (у Wei).
Приклад:

– gas price = 20 Gwei (20×10^9 Wei)
– використано 100 000 gas
– вартість = $100\,000 \times 20 \times 10^9$ Wei = 2×10^{15} Wei = 0,002 ETH
– за курсом 1 ETH = 2 000 USD це ≈ 4 USD
Для розгортання SimpleVote (200 000 gas) за тих самих умов ≈ 0,004 ETH або ~8 USD.

3.4. Основні поради з оптимізації
1. Мінімізувати записи в state (storage writes коштують ≈ 20 000 gas, читання ≈ 800 gas).
2. Використовувати view-функції для обчислень поза мережею.
3. Профілювати витрати за допомогою Hardhat/Gas Reporter, Remix або Tenderly.
4. Блоковий ліміт gas ≈ 30 млн gas – за необхідності розбивати складні транзакції.
5. Розглядати Layer-2 рішення (Optimism, Arbitrum, zk-Rollups) для зниження витрат.

Отже, смарт-контракти дають гнучкість, але вартість їх виконання прямопропорційна складності логіки. Планування gas і моніторинг цін дозволяють контролювати бюджет.

4. Висновки

- Monero забезпечує найвищий рівень приватності, однак не підтримує смарт-контракти.
- Ethereum-контракти потребують значних ресурсів у вигляді gas та ETH, особливо при частих оновленнях стану.
- Для повної конфіденційності в Ethereum необхідні додаткові шари (zk-SNARKs, Tornado Cash), що збільшує складність та вартість.
- Порівняно з Bitcoin, Ethereum пропонує широку екосистему смарт-контрактів, але вимагає ретельного контролю витрат та використання Layer-2 рішень для економії коштів.