1. Основи криптовалют та анонімізації

1.1 Порівняння стандартних криптовалют (Bitcoin, Litecoin) та анонімних криптовалют (Zcash)

Bitcoin і Litecoin — представники першого покоління криптовалют, де всі транзакції публічні. Хоча користувачі і залишаються псевдонімними, транзакційна активність кожної адреси повністю доступна для аналізу. Це дозволяє аналітичним компаніям будувати графи зв'язків і з великою ймовірністю деанонімізовувати користувачів.

Zcash, навпаки, було створено з фокусом на приватність. Його ключова особливість — підтримка захищених транзакцій, у яких інформація про відправника, отримувача й суму повністю прихована. При цьому користувач сам обирає режим: прозорий (T-адреси) чи захищений (Z-адреси), що робить Zcash зручним як для відкритого, так і для конфіденційного використання.

1.2 Як анонімізація працює в криптовалютах, особливості Zcash

У Bitcoin реалізовано лише базову форму анонімності — псевдонімність. Для посилення конфіденційності там використовуються сторонні техніки, як-от мікшування монет, stealth-адреси або кільцеві підписи (використовуються, наприклад, у Monero).

Zcash натомість використовує криптографію нульового розголошення знань — zk-SNARKs. Ця технологія дозволяє підтвердити дійсність транзакції, не розкриваючи її зміст. Завдяки цьому повністю захищені транзакції (Z→Z) гарантують абсолютну анонімність усіх параметрів: відправника, одержувача та суми.

Система підтримує чотири типи переказів:

- T→T — повністю відкриті;
- T→Z і Z→T — частково захищені;
- Z→Z — повністю приватні.

Таким чином, Zcash поєднує сильну криптографічну приватність із гнучкістю вибору, що відрізняє його від Bitcoin (відкритість) і Monero (обов'язкова анонімність).

2. Методи анонімізації в Zcash

Однією з ключових особливостей криптовалюти Zcash є її здатність забезпечувати сильний рівень приватності фінансових транзакцій. Якщо більшість криптовалют базуються на псевдонімності — тобто приховують імена користувачів, але залишають публічними адреси та суми транзакцій — то Zcash реалізує **криптографічну**

анонімізацію, що унеможливлює спостереження за переміщенням коштів навіть при повному доступі до блокчейну. Основою такої анонімізації є протокол **zk-SNARKs** — zero-knowledge succinct non-interactive arguments of knowledge.

2.1 Використання zk-SNARKs

zk-SNARKs — це форма доказу з нульовим розголошенням, що дозволяє одній стороні (доводнику) підтвердити істинність певного твердження перед іншою стороною (верифікатором), не розкриваючи саму інформацію, яка це твердження обґрунтовує.

У випадку Zcash цей підхід дозволяє здійснювати перевірку транзакції — зокрема, чи є у відправника достатньо коштів, чи не дублюється транзакція, чи збережено баланс — **без необхідності розкривати адресу відправника, адресу отримувача чи суму переказу**. Це досягається шляхом створення криптографічного доказу, який верифікується іншими вузлами мережі, але не дає жодної інформації про вміст транзакції.

Завдяки цьому протокол zk-SNARKs вирішує основну дилему традиційних криптовалют: як забезпечити верифікацію транзакцій без компрометації приватності користувача.

Особливістю zk-SNARKs є також те, що доказ є коротким і може перевірятись дуже швидко, що робить його практичним для застосування у блокчейн-системах з обмеженими ресурсами.

2.2 Технічний опис приватних транзакцій у Zcash

У Zcash реалізовано два режими транзакцій — **транспарентний** (аналогічний до Bitcoin) і **захищений** (приватний). Для повної анонімності використовуються так звані **захищені транзакції між Z-адресами (Z→Z)**. У таких транзакціях усі ключові елементи — відправник, отримувач та сума — приховані, і лише zk-SNARK-доказ засвідчує їхню коректність.

Кожна захищена транзакція включає:

- **Приватний ключ відправника**, який не розкривається, але дозволяє створити доказ, що транзакція дозволена власником коштів.
- **Унікальні токени, що замінюють відкриту інформацію** — серіалізовані значення й мітки, які використовуються для запобігання повторному витрачанню без розкриття справжнього стану рахунку.
- **Шифрування метаданих**: інформація про отримувача зашифрована, доступна лише власнику відповідного ключа.
- **Використання «випадкових параметрів»** (randomness), що гарантують унікальність доказу навіть при однакових сумах і адресах.

Завдяки такій структурі транзакції в Zcash мають високу криптографічну стійкість і є нечутливими до стороннього аналізу. Проте варто зазначити, що створення таких транзакцій вимагає більше обчислювальних ресурсів, ніж звичайні операції.

3.3 Порівняння анонімізації Zcash з іншими криптовалютами, такими як Bitcoin

Bitcoin є найвідомішою криптовалютою з відкритим блокчейном, де всі транзакції публічні та прозоро відображаються в мережі. Кожна транзакція містить інформацію про відправника, отримувача та суму, що дає змогу за допомогою блокчейн-аналізу пов'язувати адреси з конкретними особами або діяльністю, особливо якщо адреси коли-небудь були асоційовані з біржами або сервісами, які вимагають ідентифікації (KYC). Таким чином, Bitcoin не забезпечує справжньої анонімності, а лише базову псевдонімність.

На відміну від цього, **Zcash** реалізує просунуті механізми конфіденційності, ґрунтуючись на технології zk-SNARKs — доказах з нульовим розголошенням. Вони дозволяють підтверджувати дійсність транзакції без розкриття жодної інформації про її учасників або суму переказу. У Zcash є два типи адрес: прозорі (як у Bitcoin) та захищені (shielded), які забезпечують повну анонімність.

Основні відмінності:

- У Bitcoin усі транзакції за замовчуванням публічні.
- У Zcash користувач може вибрати — виконати публічну чи анонімну транзакцію.
- zk-SNARKs в Zcash забезпечують сильні математичні гарантії приватності без необхідності довіряти стороннім вузлам або учасникам.

З іншого боку, Bitcoin має перевагу у стабільності, простоті та широкому прийнятті, але не відповідає вимогам користувачів, які шукають конфіденційність на рівні протоколу.

Таким чином, Zcash надає користувачам інструменти для захисту фінансової приватності, яких бракує в архітектурі Bitcoin, і підходить для сценаріїв, де конфіденційність має критичне значення.

4. Методи деанонімізації

Хоча Zcash є однією з найбільш технологічно просунутих криптовалют у сфері забезпечення анонімності, жодна система не є абсолютно захищеною. Навіть найсильніші криптографічні протоколи можуть бути скомпрометовані не безпосередньо, а через слабкі місця на рівні використання, реалізації або інтеграції з іншими

платформами. У цьому розділі розглянемо потенційні методи деанонімізації Zcash, а також порівняємо стійкість Zcash до атак з іншими криптовалютами — зокрема Bitcoin та Litecoin.

4.1 Огляд можливих методів деанонімізації для Zcash

Zcash забезпечує конфіденційність лише тоді, коли користувач застосовує **захищені транзакції** (Z→Z). Якщо ж транзакції відбуваються з використанням транспарентних адрес (T→T або Z→T), то певна частина метаданих — зокрема адреси або суми — залишається доступною для аналізу. Цей факт відкриває декілька векторів потенційної деанонімізації:

1. **Аналіз транспарентних транзакцій**. Якщо користувач виводить кошти із захищеного пулу (Z→T), ідентифікатори одержувача й сума знову стають публічними. Якщо подібні операції здійснюються регулярно, зловмисник може зіставити час, розмір і частоту переказів, щоб зробити припущення про попередні (захищені) транзакції.
2. **Витік метаданих через сторонні сервіси**. При використанні бірж, гаманець-сервісів або інфраструктури з обмеженим рівнем приватності користувач може залишити сліди, які дозволяють пов’язати адресу з IP-адресою або особистими даними.
3. **Поведінковий аналіз**. Навіть без прямого доступу до змісту транзакцій, можна відстежити типові шаблони поведінки — наприклад, одночасний вхід і вихід коштів із захищеного пулу, регулярні суми, однакові часові інтервали тощо.
4. **Часткове розкриття при змішаних транзакціях (T↔Z)**. Коли користувач перемикається між прозорими й захищеними адресами, він мимоволі створює зв’язки між цими режимами, які можна використовувати для аналітики.

Таким чином, навіть при застосуванні сильних криптографічних протоколів загальна приватність системи залежить від поведінки користувача та структури транзакційного ланцюга.

4.2 Вивчення вразливостей у протоколі Zcash, які можуть бути використані для деанонімізації

Історично Zcash неодноразово стикався з потенційними чи підтвердженими криптографічними вразливостями. Хоча більшість з них було виправлено до того, як вони стали загрозою для користувачів, варто розуміти природу таких ризиків:

- **Вразливість «Counterfeiting vulnerability» (2018)**: було виявлено теоретичну можливість створення фальшивих токенів без виявлення завдяки помилці у zk-SNARK-схемі. Хоча цю помилку було усунуто в оновленні Sapling, вона показала, що криптографічна складність протоколу створює додаткові ризики на рівні реалізації.

- **Проблема «turnstile effect»**: коли користувачі виводять кошти із захищеного пулу (Z→T), можна спробувати зіставити суми та часові мітки, щоб зробити припущення про відповідну вхідну транзакцію. Цей ефект суттєво обмежує практичну анонімність у випадках частих Z↔T операцій.
- **Trusted Setup**: початкові параметри zk-SNARKs були створені за допомогою довіреної установки (trusted setup), яка в теорії могла бути скомпрометована. Якщо приватні ключі, пов'язані з цією установкою, були несанкціоновано збережені, то зловмисник міг би створювати фальшиві докази. Для вирішення цієї проблеми Zcash поступово переходить до **Halo 2** — нової архітектури, яка не потребує trusted setup.
- **Вузька база користувачів захищених транзакцій**: за статистикою, повністю захищені Z→Z транзакції становлять меншість від усіх транзакцій у мережі. Це знижує **анонімну множину** (anonymity set) — тобто кількість потенційних учасників, серед яких прихований відправник. Чим менше таких учасників, тим легше провести deanonymization-атаку.

Таким чином, хоча протокол Zcash в теорії забезпечує сильний захист, його практична ефективність залежить від багатьох факторів: від налаштування системи до звичок користувачів.

4.3 Порівняння складності атак на Zcash з Bitcoin і Litecoin

Zcash суттєво відрізняється від Bitcoin та Litecoin за рівнем захисту особистих даних. Останні не надають жодних вбудованих механізмів анонімізації. Транзакції в цих мережах повністю прозорі: адреси, суми та часові мітки всіх переказів відкриті й легко доступні для аналізу.

Тому **деанонімізація користувачів Bitcoin чи Litecoin** зазвичай відбувається через:

- транзакційний граф-аналіз;
- співставлення з адресами, відомими з бірж або витоків;
- визначення шаблонів переказів;
- аналіз поведінки при повторному використанні адрес.

В цих випадках деанонімізація є не тільки можливою, але й активно використовується правоохоронними органами, фінансовими установами й аналітичними фірмами (Chainalysis, CipherTrace тощо).

У випадку **Zcash**, повністю захищені транзакції Z→Z надають значно вищий рівень стійкості до таких атак, і класичні методи аналізу стають марними. Однак Zcash більш вразливий до так званих **«інформаційних атак»** — спостереження за виведенням коштів, побічною інформацією, частковою деанонімізацією через Z↔T транзакції тощо.

Отже:

- У **Bitcoin і Litecoin** анонімність відсутня за замовчуванням, і деанонімізація є прямолінійною.
- У **Zcash** реалізовано високорівневу приватність, але її ефективність значною мірою залежить від правильного використання протоколу і обережності з боку користувача.

5. Аналіз ефективності анонімних криптовалют

Анонімізація у криптовалютах, хоч і підвищує рівень приватності, неминуче впливає на ефективність транзакцій. Найбільш очевидний наслідок — зростання обсягу даних, які супроводжують захищені транзакції. У випадку Zcash, використання zk-SNARKs передбачає генерацію та верифікацію складних криптографічних доказів, що значно перевищують за розміром і обчислювальною складністю звичайні (прозорі) транзакції. Як результат, це призводить до додаткового навантаження на мережу й збільшує час обробки.

З точки зору пропускної здатності, захищені транзакції у Zcash повільніші за стандартні, і лише незначна частка користувачів систематично використовує повністю приватні операції. Це частково пояснюється вимогами до апаратних ресурсів для генерації zk-SNARK-доказів, а також обмеженнями у підтримці захищених транзакцій з боку криптобірж і гаманців.

У порівнянні з Bitcoin та Litecoin, які використовують значно простішу модель транзакцій (UTXO без приватності), Zcash має нижчу швидкість транзакцій у секундах і меншу кількість оброблених транзакцій на блок при однаковому розмірі блоку. Наприклад, у Bitcoin блок створюється кожні ~10 хвилин, а в Litecoin — кожні 2,5 хвилини, тоді як у Zcash час створення блоку теж становить приблизно 75 секунд, але обсяг інформації у блоці в разі великої кількості приватних транзакцій може стати вузьким місцем.

Масштабованість також є викликом для анонімних криптовалют. Традиційні криптовалюти мають змогу впроваджувати такі рішення, як SegWit або Lightning Network, які дозволяють збільшувати кількість транзакцій без зміни основного протоколу. Натомість для Zcash складність інтеграції подібних рішень збереженням анонімності потребує глибших криптографічних змін.

Таким чином, хоча Zcash надає високий рівень приватності, це відбувається ціною зниження ефективності: як у швидкості транзакцій, так і в масштабованості системи. Це створює додаткові виклики при його інтеграції у високонавантажені фінансові сервіси, але при цьому робить його цінним інструментом у контекстах, де анонімність має пріоритет над швидкістю.