**Тема доповіді:** Анонімність, ефективність та функціональність у світі криптовалют: аналіз на прикладі Monero та порівняння з іншими системами.

**Мета доповіді:** Розглянути ключові аспекти анонімності криптовалют, методи їх деанонімізації, порівняти ефективність з менш анонімними аналогами та обговорити питання ресурсів для смарт-контрактів.

---

**Частина 1: Вступ до анонімних криптовалют та методи забезпечення приватності (на прикладі Monero)**

Сьогодні ми розглянемо важливі аспекти функціонування сучасних криптовалют, зокрема питання анонімності та приватності. У світі, де цифрова конфіденційність стає все більш актуальною через масове збирання персональних даних, цензуру, політичні переслідування чи комерційне шпигунство, зростає інтерес до криптовалют, що забезпечують підвищений рівень захисту особистої інформації. Наша доповідь зосереджена на аналізі ключових технологій, що використовуються для забезпечення анонімності в криптовалютах, та розглядає приклад Monero — одного з найвідоміших проєктів у цій галузі.

Анонімність у криптовалютах — це здатність користувача приховати свою особистість і деталі транзакцій від сторонніх осіб, включаючи уряди, аналітичні компанії чи інші учасники мережі. Варто розрізняти псевдонімність, яку пропонує Bitcoin, і повну анонімність, яку забезпечують спеціалізовані криптовалюти. У Bitcoin кожна транзакція пов’язана з публічною адресою, яка хоч і не містить імені, але може бути пов’язана з конкретною особою через аналіз графу транзакцій або додаткову інформацію. Натомість справжня анонімність передбачає неможливість встановити зв’язок між адресами, транзакціями чи сумами.

Анонімність необхідна не лише тим, хто прагне приховати фінансову активність з особистих чи політичних причин. Вона є важливою складовою фінансового суверенітету, адже дозволяє особам здійснювати транзакції без ризику бути ідентифікованими або підданими репресіям. Також це захищає від дискримінації, небажаної реклами, викрадення даних і фінансової цензури.

Яскравим прикладом повноцінної анонімної криптовалюти є Monero (XMR). Вона була створена з фокусом на конфіденційність, незворотність транзакцій та взаємозамінність (fungibility), тобто кожна монета є рівнозначною, і її попередня історія не впливає на поточну цінність або прийняття. Для досягнення цього в Monero використовується низка інноваційних криптографічних технологій.

По-перше, **кільцеві підписи (Ring Signatures)** дають змогу приховати справжнього відправника транзакції. При створенні транзакції підпис додається до довільної групи можливих відправників (кільця), серед яких і є реальний автор. Завдяки цьому неможливо однозначно визначити, хто саме підписав транзакцію, що унеможливлює відстеження джерела коштів.

По-друге, **приховані адреси (Stealth Addresses)** — це механізм, за якого кожен отримувач транзакції має публічну адресу, але для кожної транзакції генерується унікальна одноразова адреса, на яку надходять кошти. Це дозволяє захистити фінансову історію отримувача, оскільки неможливо простежити, скільки коштів він отримав і від кого.

По-третє, **технологія RingCT (Ring Confidential Transactions)** забезпечує шифрування сум транзакцій, завдяки чому ніхто не бачить, скільки саме було надіслано. Цей протокол базується на прихованих зобов'язаннях (Pedersen Commitments) і нульових доказах знань (range proofs), що гарантують правильність обчислень без розкриття даних.

Крім того, Monero використовує **Dandelion++**, протокол для анонімізації на мережевому рівні. Він забезпечує розповсюдження транзакцій у два етапи: спочатку через один вузол (фаза «стебло»), а потім — через кілька інших у довільному порядку (фаза «пух»), завдяки чому складно ідентифікувати IP-адресу ініціатора.

Також важливо зазначити, що в Monero реалізовано динамічні розміри блоків, а її алгоритм видобутку RandomX оптимізований для звичайних процесорів, що ускладнює централізацію майнінгу й підвищує децентралізацію мережі.

Таким чином, технології анонімізації в Monero — це складний набір криптографічних механізмів, що взаємодіють між собою для досягнення максимально можливої приватності. Вони не лише захищають користувачів, а й створюють передумови для нових досліджень у сфері цифрової безпеки та стійкості проти деанонімізації. Приватність у таких криптовалютах — це не лише технічна характеристика, а й філософія свободи вибору у цифрову епоху.

---

**Частина 2: Деанонімізація, атаки та порівняння ефективності анонімних криптовалют**

Продовжуючи тему анонімності, важливо усвідомлювати, що абсолютна конфіденційність у криптовалютах — це радше ідеал, ніж досяжна реальність. Тому дослідження методів деанонімізації, аналіз потенційних векторів атак та оцінка рівня вразливості системи є критично важливими елементами забезпечення довгострокової безпеки анонімних криптовалют. Окрім цього, необхідно враховувати й компроміси: підвищена приватність часто досягається ціною зниження продуктивності, масштабованості або зручності користування.

Перш за все, слід розуміти, що деанонімізація — це процес ідентифікації реальної особи або встановлення зв'язку між транзакціями, які були спроєктовані як анонімні. Цей процес може здійснюватися через низку технічних, аналітичних і соціо-технічних засобів. Навіть найзахищеніші протоколи, такі як ті, що використовуються в Monero, не є повністю імунними до ризиків, хоча й істотно зменшують площину атаки.

Серед типових методів деанонімізації — **аналіз блокчейну**, що передбачає дослідження структур транзакцій, часових міток, кільцевих параметрів та повторного використання виходів. Хоча Monero впроваджує складні механізми захисту, певні історичні атаки показали, що ранні реалізації кільцевих підписів були частково вразливими, особливо за умов неуважного налаштування параметрів транзакцій. **Мережевий аналіз** також є поширеною технікою: незважаючи на використання протоколу Dandelion++, що заплутує джерело трансляції транзакції, можливо здійснити спроби ідентифікації IP-адрес ініціаторів через активне сканування або моніторинг входів у вузли.

Ще один серйозний вектор — це **атаки нульового дня**, які використовують невідомі або неусунені вразливості у програмному забезпеченні клієнтів, гаманців або бібліотек. Навіть при надійній криптографії людський фактор залишається вразливим — користувачі можуть самостійно розкрити метадані через сторонні сервіси, недостатньо захищені гаманці або невірне налаштування конфіденційності. До того ж, **зовнішні дані** — як-от інформація з соціальних мереж, злиті бази даних або KYC-реєстрації — можуть допомогти зв’язати анонімну транзакцію з конкретною особою.

Проте варто зазначити, що в умовах сучасної криптографії **Monero залишається однією з найстійкіших криптовалют до деанонімізації**. Її протокол постійно оновлюється, а спільнота активно реагує на виявлені загрози, вдосконалюючи як захист на рівні мережі, так і основні механізми анонімізації.

Разом з тим, забезпечення такої приватності неминуче пов’язане з **певними втратами ефективності**, особливо у порівнянні з менш анонімними криптовалютами, як-от Bitcoin чи Litecoin. Так, **розмір транзакцій у Monero значно більший**, оскільки включає кільцеві підписи, приховані адреси та зашифровані суми. Це збільшує обсяг зберігання блокчейну та навантаження на мережу. **Час підтвердження транзакцій у Monero менший (приблизно 2 хвилини проти 10 у Bitcoin)**, однак загальна пропускна здатність обмежується більшим розміром транзакцій. Водночас **масштабованість** також залишається проблемою: повні вузли потребують більше місця для зберігання та часу для синхронізації.

У плані обчислювальних ресурсів, перевірка транзакцій у Monero вимагає **більшої потужності процесора та оперативної пам’яті**, що може ускладнювати роботу легких клієнтів на мобільних або слабших пристроях. **Комісії за транзакції** також можуть бути вищими через загальний обсяг переданих даних, хоча цей показник значною мірою залежить від завантаження мережі в конкретний момент.

У підсумку, анонімні криптовалюти, як-от Monero, демонструють високий рівень технічної зрілості та криптографічної інноваційності, але вимагають свідомого ставлення до ризиків і обмежень. Їх захист від деанонімізації ґрунтується не лише на протоколах, а й на безперервному дослідженні, оновленнях і навчанні користувачів. Ціна приватності — це не лише обчислювальні ресурси, а й зусилля спільноти підтримувати безпеку в динамічному середовищі ризиків.

---

**Частина 3: Ресурси для смарт-контрактів та загальні висновки**

Окрім питань анонімності та ефективності, важливою складовою сучасної екосистеми криптовалют є смарт-контракти — автономні комп'ютерні програми, що автоматично виконують умови попередньо визначеної угоди між сторонами. Вони розміщуються та виконуються безпосередньо в блокчейні, завдяки чому виключається потреба в посередниках, а довіра між учасниками базується на математичній логіці та децентралізації, а не на суб'єктивній репутації. Для функціонування смарт-контрактів необхідні обчислювальні ресурси, які, зокрема в мережі Ethereum, оплачуються у вигляді газу (Gas) — одиниці, що відображає обчислювальну вартість операції.

У контексті Ethereum роль обчислювальної одиниці — газ, а роль розрахункової валюти — ефір (ETH). Кожна транзакція або виклик функції смарт-контракту споживає певну кількість газу. Користувач самостійно встановлює ліміт газу (Gas Limit) — максимальну кількість одиниць газу, яку він готовий витратити, та ціну газу (Gas Price) — скільки ефіру він готовий заплатити за кожну одиницю. Чим вища ціна газу, тим швидше транзакція потрапить у блок, оскільки валідатори віддають перевагу більш вигідним для них транзакціям.

Модель газу в Ethereum є фундаментальним елементом безпеки: вона запобігає нескінченному виконанню шкідливих або неоптимізованих програм, забезпечує економічний стимул для майнерів чи валідаторів, а також дозволяє ефективно розподіляти обчислювальні ресурси між учасниками мережі. Кожен цикл, кожна операція має фіксовану вартість — таким чином, виконання смарт-контракту прямо пов'язане з обсягом виконаної роботи.

Проте не всі криптовалюти мають однакову фокусну точку розвитку. У випадку з Monero, головним пріоритетом із самого початку була приватність, захист транзакцій і фінансова невидимість. Monero не розроблявся як платформа для смарт-контрактів на зразок Ethereum. Його внутрішня скриптова мова дуже обмежена — в ній реалізовано лише базову логіку перевірки транзакцій, без повноцінної підтримки умовного виконання, циклів чи зовнішніх викликів, що притаманні Turing-повним мовам програмування, які використовуються для створення смарт-контрактів в Ethereum або Polkadot.

На даний момент Monero не має нативної підтримки повноцінних смарт-контрактів. Водночас ведуться активні дослідження та дискусії щодо впровадження додаткових функцій — зокрема, через рішення другого рівня (Layer 2), які дозволили б додати елементи програмованості без втрати принципів приватності, що лежать в основі протоколу Monero. Проте таке поєднання — складні логічні умови з гарантією повної анонімності — є технічно надзвичайно складним завданням. Адже що більше даних потрібно обробляти, то більше зростає ризик витоку метаданих або порушення цілісності приховування інформації.

У порівнянні з Ethereum, Monero обирає модель глибокої конфіденційності та захисту даних на всіх рівнях, жертвуючи універсальністю та програмованістю. Ethereum, навпаки, є платформою для створення складних децентралізованих додатків, але на базовому рівні його транзакції є публічними. Для підвищення приватності в Ethereum використовуються додаткові технології, такі як міксери (Tornado Cash) або ZK-SNARKS

(zero-knowledge доказування), але вони поки що не є інтегрованими у саму основу мережі.

Отже, хоча смарт-контракти відіграють центральну роль у розвитку криптовалют нового покоління, вони також вимагають суттєвих ресурсів і мають власні обмеження. Monero, з іншого боку, демонструє інший підхід — максимальну увагу до приватності, навіть якщо це означає обмежену програмованість. Це підкреслює різні парадигми розвитку блокчейн-технологій: одна — зосереджена на прозорій децентралізованій логіці, інша — на цифровій невидимості та захисті користувача.

**Загальні висновки:**

- Дослідження методів анонімізації та деанонімізації є критично важливими для розвитку безпечних та приватних криптовалют. Monero демонструє передові підходи у забезпеченні конфіденційності.
- Підвищена анонімність часто досягається ціною певної втрати ефективності порівняно з прозорими системами, що створює необхідність пошуку балансу.
- Функціональність смарт-контрактів вимагає специфічних ресурсів (як газ та ефір в Ethereum) та архітектурних рішень, які можуть відрізнятися від пріоритетів криптовалют, сфокусованих на максимальній приватності, як Monero. Однак, дослідження в напрямку поєднання приватності та розширеної функціональності тривають.

**Дякуємо за увагу!**

| Показник | Monero | Bitcoin / Litecoin |
|---|---|---|
| **Розмір транзакції** | ~2–3 КБ через RingCT | ~250 Б |
| **Час блоку** | ≈2 хв | ≈10 хв |
| **Пропускна здатність** | Обмежена великим обсягом даних у блоці | Більше транзакцій у блоці |
| **Використання ресурсів** | Більше CPU & RAM для верифікації | Менше |
| **Комісії** | Залежить від розміру, зазвичай вищі | Нижчі через менший розмір |

| Операція | Споживання gas | Gas Price (Gwei) | Вартість (ETH) | Чому саме стільки? |
|---|---|---|---|---|
| **1. Розгортання контракту** | 500 000 | 30 | 0.015 ETH | Код зберігається в блокчейні (запис байткоду) |
| **2. Простий виклик (напр. transfer)** | 50 000 | 30 | 0.0015 ETH | Мінімум читання/запису в пам’ять |
| **3. Складна функція (з циклами/модифікаціями)** | 150 000 | 30 | 0.0045 ETH | Додаткові обчислення та storage-op |

**Пояснення:**

- **Gas Used** – залежить від кількості opcodes і записів у стейті.
- **Gas Price** – змінюється з мережею (зараз часто 20–50 Gwei).
- **ETH Cost** = Gas Used × Gas Price (в ETH).

---