Міністерство освіти і науки України
Національний технічний університет України
«Київський політехнічний інститут імені Ігоря Сікорського»
Фізико-технічний інститут
«Блокчейн та децентралізовані системи»
Лабораторна робота №2

Тема: “Реалізація смарт-контракту або анонімної криптовалюти.”
Мета роботи: «Отримання навичок роботи із смарт-контрактами або анонімними криптовалютами».
Виконав:
студент групи ФІ-41мн
Должко Назарій

ZCASH

Zcash (ZEC) — це криптовалюта з відкритим кодом, орієнтована на конфіденційність, яка використовує технологію **zk-SNARKs (Zero-Knowledge Succinct Non-Interactive Arguments of Knowledge)** для забезпечення повної анонімності.

1. Методи анонімізації в Zcash

zk-SNARKs (докази з нульовим розголошенням)

Цей механізм дозволяє перевіряти транзакцію без розкриття її учасників та суми. Це забезпечується математичною перевіркою правильності транзакції без необхідності показувати дані.

Shielded addresses (захищені адреси)

Zcash підтримує два типи адрес:

- **t-адреси** (прозорі): схожі на Bitcoin.
- **z-адреси** (захищені): транзакції між ними повністю приховують відправника, одержувача і суму.

Selective Disclosure (вибіркове розкриття)

Користувач може надати перегляд транзакцій певним сторонам (наприклад, аудиторам) без публічного розкриття.

---

2. Методи деанонімізації Zcash

Попри потужні механізми захисту, існують загрози:

Мішані транзакції

У Zcash дозволяється переказ між прозорими та захищеними адресами, що створює ризик deanonymization при неправильному використанні (наприклад, зняття коштів з t-адрес після отримання на z-адресу).

Аналіз графу транзакцій

Можливо поєднання відкритих частин блокчейну для побудови графу зв’язків між t- і z-адресами.

Мережеве спостереження

Так само, як і в Monero, можливий аналіз IP-адрес, якщо користувачі не використовують Tor або VPN.

Порівняння з Bitcoin

Параметр	Bitcoin	Zcash	Коментар
Анонімність	Низька	Висока (z-адреси)	Повна конфіденційність можливе
Тип транзакцій	Прозорі	Прозорі + захищені	Гнучкість використання
Об’єм транзакції	~250 байт	~2-10 КБ (для z-транзакцій)	Витрати пам’яті вищі
Алгоритм майнінгу	SHA-256	Equihash	ASIC-резистентний (на початку)

Підтримка бірж	Повна	Часткова	Через регуляторні ризики
Витрати на верифікацію	Середні	Високі (zk-SNARKs)	Високе навантаження на CPU/RAM

Висновок

Zcash використовує складну криптографію для захисту конфіденційності користувачів, проте її ефективність залежить від правильного використання z-адрес. У порівнянні з Monero, Zcash має більшу гнучкість (можна вибрати рівень анонімності), але водночас — більше ризиків deanonymization через людські помилки.