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-42мн

Сергеєв Станіслав

Dash.

Dash це друга за популярністю криптовалюта з вбудованим мезанізмом анонімізації.

Метод анонімізації в Dash

PrivateSend – це механізм перемішування платежів, заснований на CoinJoin. Він працює так:

- Користувачі об'єднують свої транзакції, щоб приховати джерело та призначення коштів.

- Кожна транзакція проходить кілька раундів перемішування через мастерноди, що ускладнює відстеження.

- Після змішування кошти повертаються власнику на нові анонімні адреси.

Мастерноди – спеціальні вузли, які керують процесом перемішування. Вони забезпечують децентралізовану обробку транзакцій, що підвищує рівень конфіденційності.

Методи деанонімізації в Dash.

- Аналіз транзакцій – незважаючи на перемішування, можна використовувати статистичні методи для виявлення зв'язків між адресами. Метод вимагає побудови графів взаємодії між адресами, що потребує значних обчислювальних ресурсів.

- Кластеризація адрес – аналітичні платформи можуть групувати адреси, що взаємодіють між собою, і визначати їх власників. Застосовуються алгоритми машинного навчання для групування пов'язаних адрес.

- Атаки на мастерноди – якщо зловмисник контролює значну кількість мастернод, він може відстежувати перемішування та розкривати зв'язки між транзакціями. Потребує значних фінансових вкладень.

Аналіз втрат ефективності Dash у порівнянні з Bitcoin.

	Dash	Bitcoin
Середній час підтвердження транзакцій	Використовує функцію InstantSend, 1-2 секунди	10 хвилин (1 блок)
Пропускна здатність	40-56 TPS	7 TPS
Енерговитрати на транзакцію	200-400 кВт*год	700-1000кВт*год

Розмір блоку	До 2 Мб	1-2 Мб
Стійкість до атак	Менш стійка	Більш стійка

Dash є ефективнішим для швидких і дешевих транзакцій, але поступається Bitcoin у безпеці, децентралізації.

Оцінка та обґрунтування необхідних ресурсів (гасу і ефіру), потрібних для функціонування смарт-контракту.

Для функціонування платформи необхідні:

- Комісія за транзакції менше 1 цента, що є економічно вигідним.
- Застава для мастернод (1000 DASH), 10% винагороди за блок іде на розвиток мережі.