ДОДАТОК А

Графічний матеріал кваліфікаційної роботи

1

Міністерство освіти і науки України
Харківський національний університет радіоелектроніки

КВАЛІФІКАЦІЙНАРОБОТА НА ТЕМУ:
«Методипобудовита захистудецентралізованихсистем наоснові технологіїблокчейну»

Виконав:
ст. гр. СПм-22-5
Шевчук Є.В.

Керівник роботи:
доц. Федорченко В.М.

2

Аналіз проблеми

Побудова та захист блокчейну є ключовими проблемами всієї блокчейн індустрії. Децентралізовані блокчейн системи тісно пов'язані з фінансами, тож захист цих фінансів від крадіжок є ключовою темою, нехай дійсно масові атаки на блокчейн достатньо рідкісне явище, але одна така успішна атака може мати катастрофічні наслідки як для самої мережі, так і для всіх хто використовував її.

Сучасним популярним децентралізованим блокчейн рішенням зазвичай надто важко змінити принципи роботи своєї мережі, адже це буде потребувати згоди великої кількості користувачів, тож вразливості залишаються в них з моменту створення.

3

Мета кваліфікаційної роботи

Проєктування децентралізованої блокчейн мережі, яка буде мати оптимальні параметри захисту від загроз і атак а також бути достатньо ефективною.

4

Об’єкт. Предмет. Методи дослідження

Об’єктом дослідження є блокчейн.

Предметом дослідження є децентралізована блокчейн мережа.

Для досягнення поставлених цілей використовуються такі методи дослідження: аналіз та синтез літературних джерел, соціальні аспекти, аналіз протоколів та криптографії, аналіз мереж.

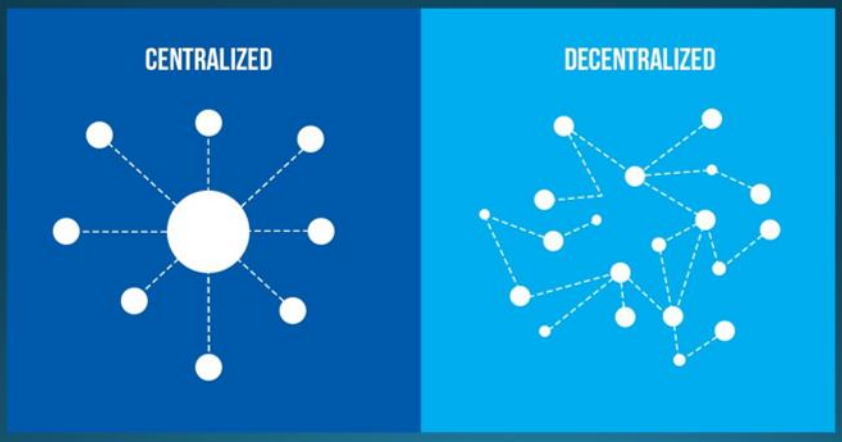
5

Постановка задачі

- Дослідити та проаналізувати блокчейн систему та методологію її побудови.
- Дослідити та проаналізувати вразливості децентралізованих блокчейн систем.
- Спроєктувати блокчейн з оптимальними параметрами захисту і ефективності

6

Концепція децентралізованої блокчейн системи



7

Рівні блокчейну

- Блокчейн може мати до 6 рівнів, прикладний рівень, рівень послуг і додаткових компонентів, рівень протоколу (конесенсусу) мережевий рівень, рівень даних, рівень апаратного забезпечення та інфраструктури.

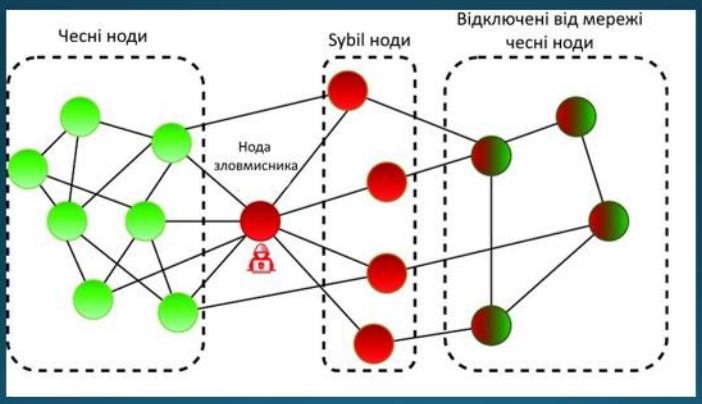
8

Класифікація блокчейн атак

Блокчейн атаки діляться на атаки механізму консенсусу, атаки мережі, і атаки клієнту, найнебезпечнішими і наймасштаьнішими атаками є атаки механізму консенсусу, наслідком успішної атаки на механізм консенсусу може бути повний занепад мережі, і втрата фінансів всіх клієнтів, атаки клієнту це атаки направлені на одну або декілька нод або клієнтів в мережі, для того щоб викрасти конкретно їх ресурси, атаки мережі націлені на

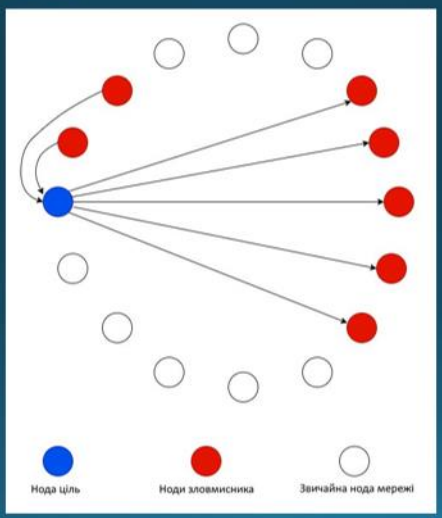
9

Атака sybil



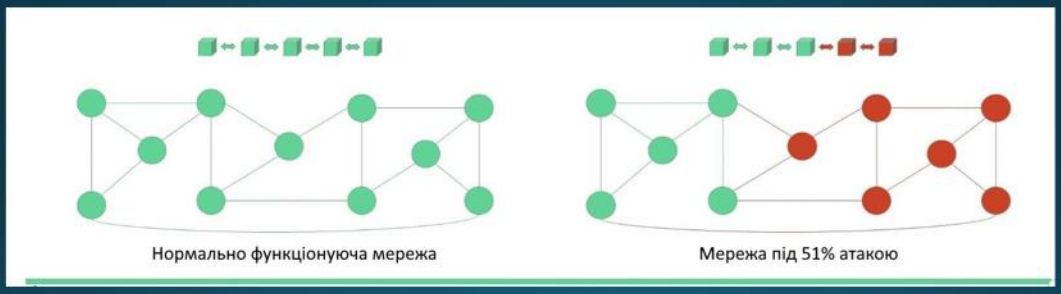
10

Атака eclipse



11

Атака 51%



12

DDoS

DDoS (розподілена відмова в обслуговуванні) — це атака на кібербезпеку, під час якої зловмисники переповнюють мережу, програму, сервер або систему спам-трафіком або фальшивими транзакціями.

13

Alien атака

Alien атака, також відома як забруднення пулу адрес, належить до методу атаки, який спонукає вузли одного ланцюга вдиратися та забруднювати один одного. Основною причиною вразливості є те, що та сама система ланцюга не визначає несхожі вузли в протоколі зв'язку.

14

Length extension attack

Атака Length Extension – це тип атаки, коли зловмисник може використовувати хеш і довжину першого повідомлення для обчислення хешу для контрольованого зловмисником другого повідомлення

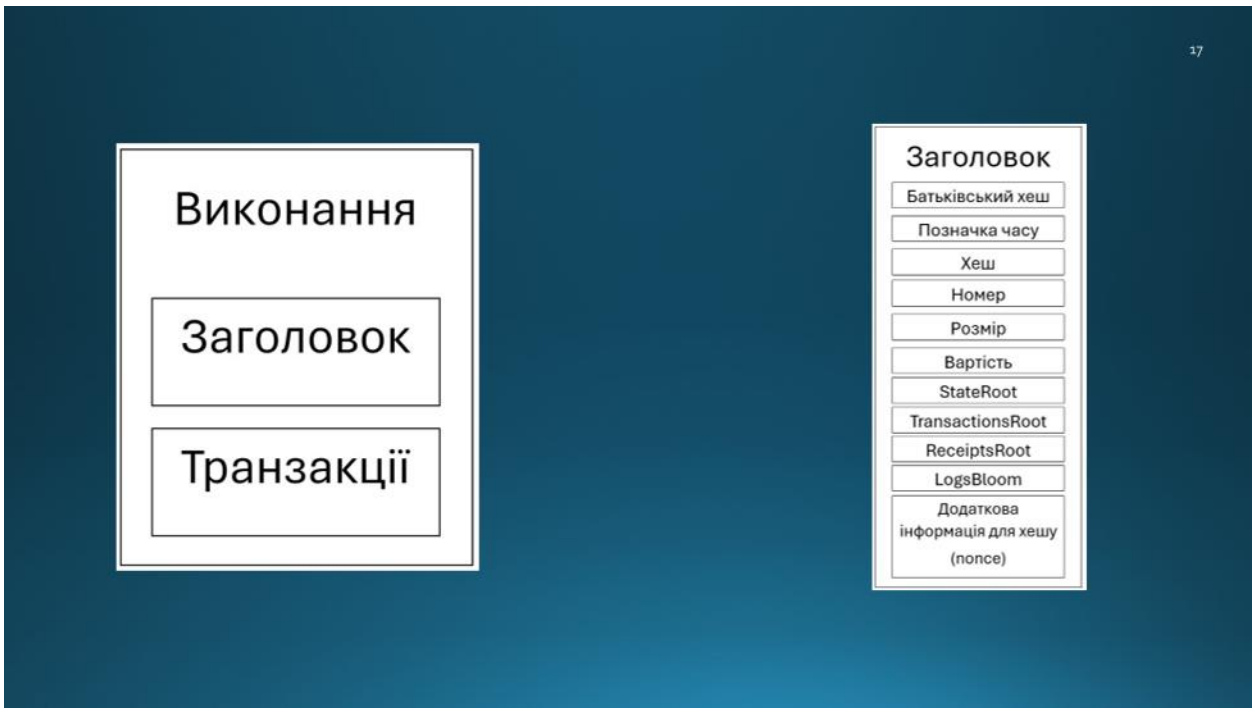
15

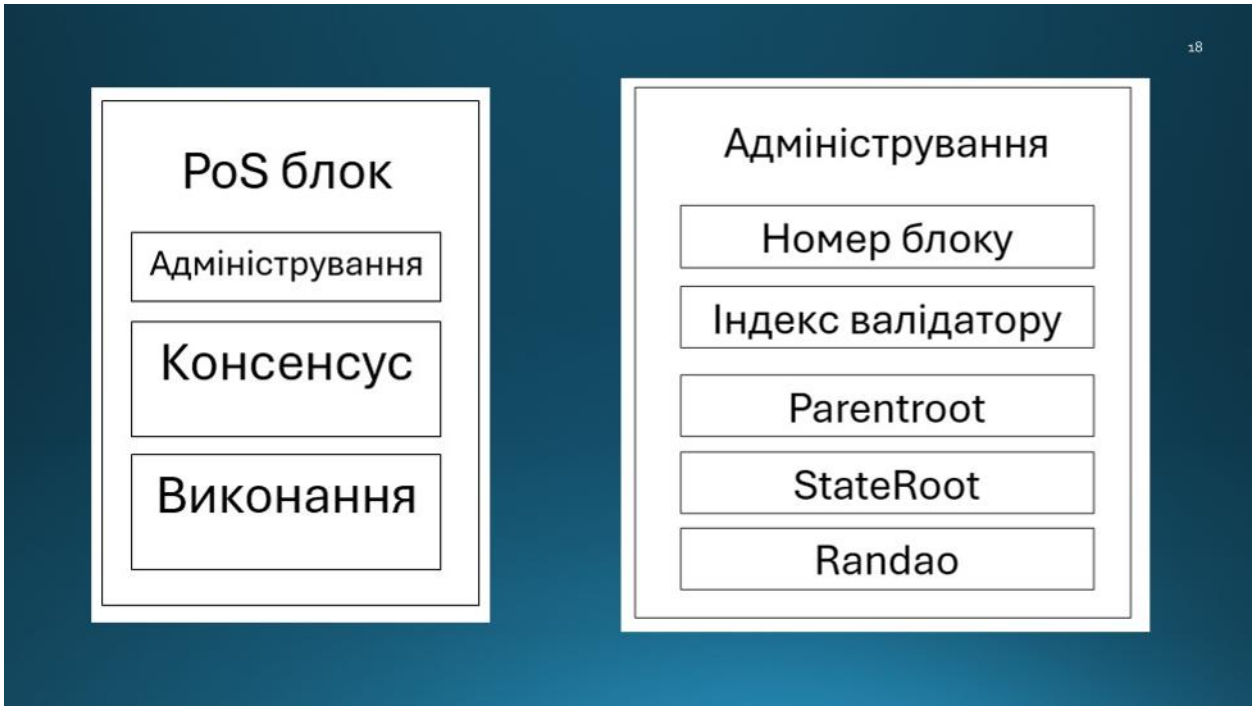
Атака підслуховування

Під час атаки підслуховування зловмисник стежить за мережею, щоб отримати приватні дані. Витягнувши конфіденційні дані, вони використовували їх для компрометації будь-якої частини мережі.

16

Проєктування блокчейну

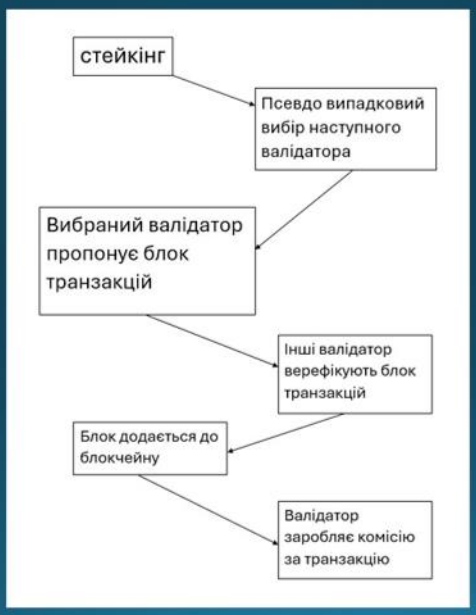

17
Виконання
Заголовок
Транзакції
Заголовок
Батьківський хеш
Позначка часу
Хеш
Номер
Розмір
Вартість
StateRoot
TransactionsRoot
ReceiptsRoot
LogsBloom
Додаткова інформація для хешу (nonce)


18
PoS блок
Адміністрування
Консенсус
Виконання
Адміністрування
Номер блоку
Індекс валідатору
Parentroot
StateRoot
Randao

19


Консенсус
Аттестації
Deposit root
Deposit count
Sync committee bits
Sync committee signature
Депозити
Voluntary exits
Proposer slashings
Attester slashings

20


стейкінг
Псевдо випадковий вибір наступного валідатора
Вибраний валідатор пропонує блок транзакцій
Інші валідатор верефікують блок транзакцій
Блок додається до блокчейну
Валідатор заробляє комісію за транзакцію

21

Висновки

На основі проведеного дослідження було виявлено ключові вразливості блокчейну, а також методологію його побудови.

Також було спроєктовано децентралізовану блокчейн мережу яка має максимальний захист при оптимальних параметрах ефективності.

22

Апробація

Шевчук Є. В., Федорченко В. М. Аналіз основних вразливостей і способів захисту механізму консенсусу в децентралізованих блокчейн системах. Національний університет “Полтавська політехніка імені Юрія Кондратюка”. Системи управління, навігації та зв’язку. 2024., № 3. С. 72-76.