Лабораторна робота №2
Забара Павло ФЕ-41мп

Для другого типу лабораторних робіт

1. розгортання та запуск обраної анонімної валюти, протоколювання майнінгу, пошук слідів деанонімізації

```
base ~/home/uni/blockchain (18.53s)
docker pull zcashfr/zcash

Using default tag: latest
latest: Pulling from zcashfr/zcash
e62d08fa1eb1: Pull complete
f10e1bdddf3f: Pull complete
1cd62a315822: Pull complete
8ba2eca64c62: Pull complete
c1e9a37f19ec: Pull complete
9fe525454c71: Pull complete
39a92a2da2b5: Pull complete
2cae51d1db04: Pull complete
Digest: sha256:7f41072f70808e1457d8a3ca245d7ecef447ea8f90995f6028273269c065ff90
Status: Downloaded newer image for zcashfr/zcash:latest
docker.io/zcashfr/zcash:latest
```

```
base ~/home/uni/blockchain (0.09s)
docker volume inspect zcash-data

[
    {
        "CreatedAt": "2025-05-12T15:21:31Z",
        "Driver": "local",
        "Labels": null,
        "Mountpoint": "/var/lib/docker/volumes/zcash-data/_data",
        "Name": "zcash-data",
        "Options": null,
        "Scope": "local"
    }
]
```

```
base ~/home/uni/blockchain (0.088s)
docker volume inspect zcash-params

[
    {
        "CreatedAt": "2025-05-12T15:22:09Z",
        "Driver": "local",
        "Labels": null,
        "Mountpoint": "/var/lib/docker/volumes/zcash-params/_data",
        "Name": "zcash-params",
        "Options": null,
        "Scope": "local"
    }
]
```

```
docker run -d --name zcash --user root -v zcash-data:/root/.zcash -v zcash-params:/
root/.zcash-params -v ${PWD}/zcash.conf:/root/.zcash/zcash.conf -p 8232:8232 -p
127.0.0.1:8233:8233 zcashfr/zcash
```

The Docker container has been successfully created and started. Let me verify its status to ensure it's running properly.

```
docker ps --filter "name=zcash"
```

Perfect! The Zcash container is now running successfully. Here's what's configured:

1. Container ID: 95d2644899af
2. Image: zcashfr/zcash
3. Status: Up and running (for 4 seconds)
4. Ports properly mapped:
   - 8232 (RPC port): exposed to 0.0.0.0:8232
   - 8233 (P2P port): exposed to 127.0.0.1:8233
5. Volumes mounted:
   - zcash-data → /root/.zcash
   - zcash-params → /root/.zcash-params
   - local zcash.conf → /root/.zcash/zcash.conf

```
base ~/home/uni/blockchain (0.256s)
docker exec zcash zcash-cli getinfo
{
  "version": 3000050,
  "protocolversion": 170011,
  "walletversion": 60000,
  "balance": 0.00000000,
  "blocks": 0,
  "timeoffset": 0,
  "connections": 0,
  "proxy": "",
  "difficulty": 1,
  "testnet": false,
  "keypoololdest": 1747063861,
  "keypoolsize": 101,
  "paytxfee": 0.00000000,
  "relayfee": 0.00000100,
  "errors": ""
}
```

docker exec zcash zcash-cli getblockchaininfo


```
{
  "chain": "main",
  "blocks": 0,
  "headers": 0,
  "bestblockhash":
"00040fe8ec8471911baa1db1266ea15dd06b4a8a5c453883c000b031973dce08"
,
  "difficulty": 1,
  "verificationprogress": 1.642110739774387e-08,
  "chainwork":
"0000000000000000000000000000000000000000000000000000000000002000"
,
  "pruned": false,
  "size_on_disk": 1700,
  "commitments": 0,
  "valuePools": [
```

```
    {
      "id": "sprout",
      "monitored": true,
      "chainValue": 0.00000000,
      "chainValueZat": 0
    },
    {
      "id": "sapling",
      "monitored": true,
      "chainValue": 0.00000000,
      "chainValueZat": 0
    }
  ],
  "softforks": [
    {
      "id": "bip34",
      "version": 2,
      "enforce": {
        "status": false,
        "found": 1,
        "required": 750,
        "window": 4000
      },
      "reject": {
        "status": false,
        "found": 1,
        "required": 950,
        "window": 4000
      }
    },
    {
      "id": "bip66",
      "version": 3,
      "enforce": {
        "status": false,
        "found": 1,
        "required": 750,
        "window": 4000
      },
      "reject": {
        "status": false,
        "found": 1,
        "required": 950,
        "window": 4000
      }
    },
    {
      "id": "bip65",
```

```
      "version": 4,
      "enforce": {
        "status": false,
        "found": 1,
        "required": 750,
        "window": 4000
      },
      "reject": {
        "status": false,
        "found": 1,
        "required": 950,
        "window": 4000
      }
    }
  ],
  "upgrades": {
    "5ba81b19": {
      "name": "Overwinter",
      "activationheight": 347500,
      "status": "pending",
      "info": "See https://z.cash/upgrade/overwinter/ for
details."
    },
    "76b809bb": {
      "name": "Sapling",
      "activationheight": 419200,
      "status": "pending",
      "info": "See https://z.cash/upgrade/sapling/ for details."
    },
    "2bb40e60": {
      "name": "Blossom",
      "activationheight": 653600,
      "status": "pending",
      "info": "See https://z.cash/upgrade/blossom/ for details."
    },
    "f5b9230b": {
      "name": "Heartwood",
      "activationheight": 903000,
      "status": "pending",
      "info": "See https://z.cash/upgrade/heartwood/ for details."
    }
  },
  "consensus": {
    "chaintip": "00000000",
    "nextblock": "00000000"
  }
}
```

Вузол Zcash запущений, параметри завантажені, на json пейлоад видно процес синхронізації з мережею Zcash

```
base ~/home/uni/blockchain (0.185s)
docker exec zcash zcash-cli z_gettotalbalance
{
  "transparent": "0.00",
  "private": "0.00",
  "total": "0.00"
}
```

```
base ~/home/uni/blockchain (0.237s)
docker exec zcash zcash-cli getwalletinfo
{
  "walletversion": 60000,
  "balance": 0.00000000,
  "unconfirmed_balance": 0.00000000,
  "immature_balance": 0.00000000,
  "txcount": 0,
  "keypoololdest": 1747063861,
  "keypoolsize": 101,
  "paytxfee": 0.00000000,
  "seedfp": "86045ae3b1092867f2b8bf2665d68bbff84e8224ca65f444d14b384d412c4cb3"
}
```

Маємо порожній гаманець

Перший тип лаби

Анонімізація в Monero і Zcash

Monero (XMR)

Криптовалюта Monero побудована на основі **Cryptonote протоколу**, що забезпечує повну конфіденційність транзакцій. Основні механізми:

- **Кільцеві підписи (Ring Signatures):** приховують відправника, включаючи випадковий набір публічних ключів, чим більше набір публічних ключів, тим складніше знайти справжнього відправника, наразі включаються обов’язково 16

ключів

- **Stealth Addresses:** приховують одержувача шляхом створення одноразової адреси для кожної транзакції.Відправник використовує публічний ключ одержувача для створення одноразової адреси, одержувач може розпізнати та отримати доступ до коштів використовуючи свій приватний ключ.

  Таким чином унеможливлюється можливість аналізу блокчейну для визначення хто отримав кошти

- **Ring Confidential Transactions (RingCT):** повністю приховують суму транзакції, використовуючи Pedersen Commitments.

Завдяки цим трьом елементам Monero гарантує:
- неможливість відстежити відправника
- неможливість ідентифікувати одержувача
- неможливість побачити суму транзакції

ZCash (ZEC)

ZCash використовує **zk-SNARKs** — доказ з нульовим розголошенням. Підтримує два режими транзакцій:

- **t-транзакції:** публічні, як у Bitcoin.

- **z-транзакції:** анонімні. Можуть бути повністю шифрованими, приховуючи відправника, отримувача та суму.

ZCash забезпечує вибіркову приватність, однак лише **близько 15%** транзакцій в мережі є повністю захищеними (станом на 2024 рік).

Методи деанонімізації

Вразливості Monero:

- **Spent Output Analysis** — аналіз часто використовуваних ключів-міксинів у кільцевих підписах.

- **Аналіз часових міток** — кореляція транзакцій з відомими подіями.

- **KYC-біржі** — при перетині із централізованими біржами можлива прив’язка до реального користувача.

- **Атаки через вузли** — потенційна deanonymization через логування IP.

Однак: сучасна реалізація з 16-елементними кільцями, розширеним RingCT і забороною вибору маленьких кілець майже повністю нейтралізує ці ризики.

Технологічні відмінності

Технологія	Monero	Zcash
Криптографія	Розширені кільцеві підписи, Pedersen Commitments	zk-SNARKs (Zero-Knowledge Proofs)
Розмір транзакції	1.5–2.5 КБ (великі транзакції через шифрування)	~3–4 КБ (zk-SNARK доволі важкий)
Обчислювальні ресурси	Високі, але придатні для звичайного CPU	Дуже високі: потрібна велика пам’ять, CPU/GPU
Час підтвердження	~2 хвилини	~1.5 хвилини, але z→z може оброблятись довше

Типи контрактів і їх ресурсоємність

Gas — це одиниця роботи в EVM (Ethereum Virtual Machine).
ETH — загальна вартість транзакції = gasUsed × gasPrice.

Контракт	Розгортання (gas)	Виклик функції (gas)
ERC-20 токен	~300,000–400,000	transfer() ~50,000

SimpleVote (голосування)	~200,000	vote() ~45,000–60,000

2.2 Приклад розрахунку

Gas price: 20 Gwei
Used gas: 100,000
Вартість: 0.002 ETH ≈ $6 (за 1 ETH = $3000)

2.3 Оптимізація gas

- Зменшення записів у **storage**: найдорожча операція (~20,000 gas).
- Заміна на **view/pure** функції.
- Розділення складних транзакцій на менші.
- Використання **Layer-2**: Optimism, zkSync, Arbitrum.