Біткоїн та криптовалютні технології
Лекція 8: Біткоїн-гаманці

Юрій Жикін

27 березня, 2025

Набір UTXO

- Увесь біткоїн в обігу представлений у вигляді **набору UTXO** - набору всіх невикористаних транзакційних виходів.
- Кожна “монета” (**UTXO**) складається з певної кількості **сатоші** та відповідного скрипту замикання.
- Щоб перевірити отриману транзакцію, користувач має переконатися, що транзакція правильно сформована, і що виходи, які вона використовує, входять до **множини UTXO**.
- Весь протокол Bitcoin працює для забезпечення **узгодженості набору UTXO**.

Володіння біткоїном

- **Володіння біткоїном** означає, що користувач може надати правильний **скрипт відмикання** до **скрипту замикання** деяких виходів з **набору UTXO**.
- Скрипти блокування є відкритими, тому кожен невикористаний транзакційний вихід повинен мати унікальний скрипт блокування.
- Інакше можна легко обчислити, скільки біткоїнів належить певній певному.
- **Біткоїн-гаманець** - це зазвичай програмне забезпечення для зберігання даних, необхідних для створення скриптів відмикання до відповідних UTXO.

Стандартні скрипти замикання

- **P2PK** — Pay to Public Key

```
<pubKey> OP_CHECKSIG;
```

- **P2MS** — Pay to Multi-Signature

```
<M> <pk1> ... <pkN> <N> OP_CHECKMULTISIG;
```

- **P2PKH** — Pay to Public Key Hash

```
OP_DUP OP_HASH160 <pubKeyHash> OP_EQUALVERIFY OP_CHECKSIG;
```

- **P2SH** — Pay to Script Hash

```
OP_HASH160 <scriptHash> OP_EQUAL;
```

- **P2WPKH** — Pay to **Witness** Public Key Hash

```
OP_0 <20-byte-witness-data>;
```

- **P2WSH** — Pay to **Witness** Script Hash

```
OP_0 <32-byte-witness-data>;
```

Відокремлений свідок

- Софтфорк у мережі, активований 24 серпня 2017 року.
- Запропонований у серії **пропозицій щодо покращення Біткоїна** (Bitcoin Improvement Proposals) — BIP-0141, BIP-0143, BIP-0144 та BIP-0148.
- Основна ідея полягає у винесенні великих скриптів відмикання з даних транзакцій, що включаються в блоки.

Біткоїн-адреси 1/4

- Біткоїн використовує кілька орієнтованих на людей способів кодування адрес та ключів:
  - **Base58Check**

    $$Base58Check(t, data) = Base58(t + data + HASH256(t + data)[0{:}4])$$

    де *Base58* використовує алфавіт

    123456789*ABCDEFGHJKLMNPQRSTUVWXYZabcdefghijkmnopqrstuvwxyz*
  - **Bech32**

    $$Bech32(t, data) = t + \text{"1"} + Base32'(data + Bech32Checksum(t, data))$$

    де *Base32'* використовує алфавіт

    *qpzry*9*x*8*gf*2*tvdw*0*s*3*jn*54*khce*6*mua*7*l*

Біткоїн-адреси 2/4

- Формати адрес для **P2PK** та **P2MS** не визначені.
- Формат адреси для **P2PKH**

```
OP_DUP OP_HASH160 <pubKeyHash> OP_EQUALVERIFY OP_CHECKSIG;
```

$A_{p2pkh} = Base58Check(0x00 + pubKeyHash)$

17VZNX1SN5NtKa8UQFxwQbFeFc3iqRYhem

$A'_{p2pkh} = Base58Check(0x6F + pubKeyHash)$

mipcBbFg9gMiCh81Kj8tqqdgoZub1ZJRfn

Біткоїн-адреси 3/4

- Формат адреси для **P2SH**

```
OP_HASH160 <scriptHash> OP_EQUAL;
```

$$A_{p2sh} = Base58Check(0x05 + scriptHash)$$

3EktnHQD7RiAE6uzMj2ZifT9YgRrkSgzQX

$$A'_{p2sh} = Base58Check(0xC4 + scriptHash)$$

2MzQwSSnBHWHqSAqtTVQ6v47XtaisrJa1Vc

Біткоїн-адреси 4/4

- Формат адреси для **P2WPKH/P2WSH**

```
OP_0 <20-or-32-byte witnessData>;
```

$$A_{p2wpkh/p2wsh} = Bech32(\text{"}bc\text{"} + witnessVersion + witnessData)$$

bc1qw508d6qejxtdg4y5r3zarvary0c5xw7k**v8f3t4**

$$A'_{p2wpkh/p2wsh} = Bech32(\text{"}tb\text{"} + witnessVersion + witnessData)$$

tb1qw508d6qejxtdg4y5r3zarvary0c5xw7k**xpjzsx**

Зберігання криптографічних ключів 1/2

- Усі стандартні скрипти замикання/відмикання базуються на наданні підпису, який відповідає публічному ключу, до якого прив'язаний скрипт блокування.
- Оскільки форма скрипту стандартизована, *єдиним елементом, що відрізняється*, є **публічний ключ або його хеш**.
- Єдиним елементом даних, необхідними для створення стандартного скрипту відмикання до стандартного скрипту замикання, є *відповідний приватний ключ*.

Зберігання криптографічних ключів 2/2

- Усі сучасні Біткоїн-гаманці є **сховищами криптографічних ключів** з додатковою функціональністю:
  - безпечне зберігання приватних ключів для “монет”, що належать користувачу,
  - генерація нових приватних і публічних ключів та адрес,
  - для кожного нового блоку або транзакції — перевірка, чи відповідає її скрипт блокування стандартному скрипту блокування/розблокування, який підходить до одного з наявних ключів (необов’язково),
  - конструювання нових транзакцій шляхом вибору підмножини UTXO для знищення та створення нових UTXO з додавання відповідних скриптів розблокування (необов’язково).

Прості гаманці з пулом ключів

- Найпростішим Біткоїн-гаманцем є **один приватний ключ**.
- Адреса є видимою в ланцюгу, тому при **повторному використанні адрес** легко обчислити кількість біткоїнів, що належать одному й тому ж користувачу.
- *Повторне використання адрес* — це погана практика, тому необхідна генерація нового ключа для кожної вхідної транзакції.
- Гаманець — це файл, який містить список ключів для всіх “монет”, що належать користувачу.
- Після кожної отриманої транзакції необхідно створювати нову резервну копію.
- Розмір сховища ключів постійно зростає, а видаляти старі ключі небезпечно, оскільки неможливо гарантувати, що їхні адреси не будуть використані повторно.

Ієрархічні детерміністичні гаманці 1/2

- **Ієрархічні детерміністичні гаманці** (**HD-гаманці**) були вперше запропоновані у 2011 році та стандартизовані у BIP-0032 у 2012 році.
- Основна ідея — використання **кореневого приватного ключа**, з якого генеруються дерево приватних ключів.
- **Приватний ключ у ієрархії може бути використаний для генерації дочірніх приватних ключів**.

  $CKD_{priv}(k_{par}, c_{par}, i) = HMACSHA512(c_{par}, k_{par} G || i) = I$

  $k_i = I[0{:}32] + k_{par} \pmod{n}$

  $c_i = I[32{:}64]$

- **Публічний ключ у ієрархії може бути використаний для генерації дочірніх публічних ключів, але не їхніх приватних ключів**.

  $CKD_{pub}(K_{par}, c_{par}, i) = HMACSHA512(c_{par}, K_{par} || i) = I$

  $K_i = (I[0{:}32])G + K_{par} = (I[0{:}32] + k_{par})G = k_i G$

  $c_i = I[32{:}64]$

Ієрархічні детерміністичні гаманці 2/2

- BIP-0039 визначає спосіб кодування кореневого ключа у вигляді послідовності слів.
- Більшість сучасних гаманців показують **BIP-0039-зерно** (**seed**) під час ініціалізації.
- Словник містить 2048 (2^{11}) слів.
- Послідовність з 12 слів містить 128 ($12 * 11 = 132$) криптографічної ентропії.
- Приклад:

```
fortune flush  weekend current
key     hero   snake   leopard
brisk   climb  timber  appear
```

Безпека: мобільні гаманці

- Існують десятки застосунків-гаманців для мобільних пристроїв (iOS та Android):
  - **BlueWallet** (iOS, Android, клієнт-сервер, можливість підключення до власного вузла),
  - **BlockStream Green** (iOS, Android, клієнт-сервер),
  - **Bitcoin Wallet** (Android, SPV-вузол).
- Основний недолік — ключі зберігаються на пристрої, підключеному до мережі, що саме по собі погано з точки зору безпеки.
- Будь-яке порушення безпеки, яке дозволяє отримати доступ до даних на пристрої, може призвести до витоку ключів ключів.
- Підходить для повсякденних транзакцій із невеликими сумами біткоїнів.

Безпека: апаратні гаманці

- Апаратні гаманці — це спеціалізовані **ізольовані** пристрої, призначені для генерації та зберігання криптографічних ключів:
  - **пристрої Trezor**
  - **пристрої Ledger**
  - **Coinkite Coldcard**
  - **Blockstream Jade**
  - **Shift Crypto BitBox02**

Безпека: холодне зберігання

- **Холодне зберігання** — це будь-який метод зберігання, який не передбачає використання програмного забезпечення або електронних пристроїв.
- HD-зерно можна записати на аркуші паперу й зберігати у надійному місці, або навіть просто запам'ятати.
- Щоб скористатися біткоїнами з холодного сховища, потрібно спочатку перенести ключ на пристрій, що може підписувати транзакції (апаратний чи мобільний гаманець).

Безпека: загальний підхід

- **Достатньо безпечний підхід** до зберігання біткоїнів:
  - згенерувати новий **кореневий приватний ключ** на спеціалізованому пристрої (апаратному гаманці),
  - створити **холодну резервну копію** кореневого приватного ключа (паперовий гаманець або металевий пристрій для зберігання ключів),
  - імпортувати **кореневий публічний ключ** на пристрій, який буде використовуватись для відстеження балансу (смартфон),
  - **видалити приватний ключ із спеціалізованого пристрою**.

Кінець

Дякую за увагу!