Біткоїн та криптовалютні технології
Лекція 10: Масштабування Біткоїна 2/2

Юрій Жикін

5 травня, 2025

Протоколи другого рівня

- Контракти (Транзакції) виконуються в межах протоколу-надбудови, а основна Біткоїн-мережа (ланцюг блоків) використовується як рівень фіналізації контрактів.
- Підписана Біткоїн-транзакція — це платіж, який можна “заявити” шляхом публікації її в мережі Bitcoin.
- Платежі другого рівня можуть бути реалізовані за допомогою підписаних транзакцій, які публікуються лише у разі необхідності фіналізації.
- До моменту публікації **фіналізуючої транзакції**, **повторне витрачання коштів** все ще можливе.

Платіжні канали 1/2

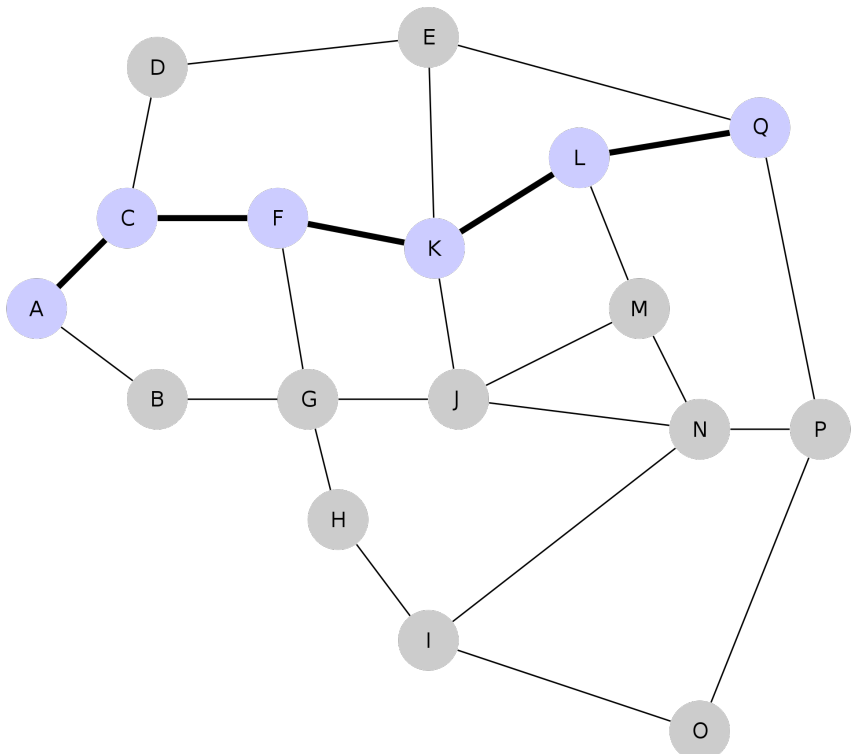
- **Платіжний канал** — це конструкція, яка дозволяє **двом** сторонам здійснювати платежі без надсилання транзакцій до Біткоїн-мережі.
- **Двосторонній платіжний канал** дещо подібний до платіжного чека, який розподіляє спільний банківський рахунок між двома сторонами.
  - спільний банківський рахунок з балансом N одиниць;
  - обидві сторони A і B "володіють" частинами балансу по $N/2$;
  - обидві сторони підписують чек, що виплачує по $N/2$ одиниць A і B;
  - коли сторона A хоче заплатити M одиниць стороні B, вони **підписують новий чек**, який виплачує $N/2 - M$ стороні A та $N/2 + M$ стороні B, та **знищують старі чеки**.

Платіжні канали 2/2

- Існує кілька пропозицій: канали Спіллмана, CLTV, канали Пуна-Драйї, дуплексні платіжні канали Деккера-Ваттенхофера, канали eltoo Деккера-Рассела-Осунтокуна.
- Платіжні канали Пуна-Драйї були представлені в оригінальній публікації.
- Кошти, що лежать в основі каналу, блокуються мультипідписом 2-з-2.
- Ще до того, як фінансуюча транзакція підписується, спочатку створюються й підписуються транзакції-зобов'язання (commitment) для кожної сторони.
- Оскільки потрібно посилатися на транзакції, які ще не підписані, необхідно формат транзакцій, що відокремлюють підписи від частини транзакції, яка хешується для створення txid (Segregated Witness).

Мережа Lightning 1/4

- Мережа двосторонніх платіжних каналів, яка дозволяє здійснювати багатоетапні платежі, передаючи кошти через послідовність платіжних каналів.
- Запропонована у 2015 році; почала працювати на початку 2018 року.



Мережа Lightning 2/4

- Кожен канал — це “спільний рахунок” з мультипідписом 2-з-2
- Фінансуюча транзакція:

```
OP_2 <A public key> <B public key> OP_2 OP_CHECKMULTISIG
```

Мережа Lightning 3/4

- Одразу створюються дві транзакції-зобов'язання — по одній для кожного учасника.
- Вихід для віддаленої сторони виглядає так:

```
<remote public key> OP_CHECKSIG
```

- Вихід для локальної сторони виглядає так:

```
OP_IF
    <revocation public key>
OP_ELSE
    <delay> OP_CHECKSEQUENCEVERIFY OP_DROP
    <local delayed pubkey>
OP_ENDIF
OP_CHECKSIG
```

Мережа Lightning 2/2

- Сутність A хоче заплатити сутності B, і в мережі існує шлях між ними: $A, C_1, C_2, ..., C_n, B$:
  - B генерує випадкове значення R, обчислює хеш $H = hash(R)$ і передає H сутності A;
  - A створює додатковий HTLC (контракт з хеш-таймлоком) і оновлює свій канал із C_1:

```
OP_IF
  HASH160 <H> OP_EQUAL
  <B public key> OP_CHECKSIG
OP_ELSE
  <locktime> OP_CHECKLOCKTIMEVERIFY
  <A public key> OP_CHECKSIG
OP_ENDIF
```

  - C_1 оновлює свій платіжний канал із C_2 і так далі, доки C_n не оновить канал із B.
  - B передає R до C_n і отримує кошти; C_n передає R до C_{n-1} і так далі, доки C_1 не отримає кошти від A.

Використання мережі Lightning

- 11,380 вузлів (20,478 вузлів у 2021 році),
- 42,459 каналів (45,774 канали у 2021 році),
- 4,230.60 BTC = $400,334,511 (1,332.25 BTC = $52,290,595 у 2021 році),
- Тривають дослідження, удосконалення та розробка нових функцій,
- Ігри, онлайн-магазини та інші бізнеси.

Рекомендовані ресурси

- **Basis of Lightning Technology**
  - https://github.com/lightning/bolts
- **Mastering the Lightning Network**
  - by Andreas Antonopoulos, Olaoluwa Osuntokun, and René Pickhardt.
  - https://github.com/lnbook/lnbook

Кінець

Дякую за увагу!