Bitcoin and Cryptocurrency Technologies
Lecture 10: Bitcoin Scalability 2/2

Yuri Zhykin

Apr 28, 2025

Second Layer Solutions

- Perform transactions in a second-layer network and use main Bitcoin network (chain) as a settlement layer.
- Signed Bitcoin transaction is a payment that can be "claimed" by publishing it to the Bitcoin network.
- Second-layer payments can be implemented with signed Bitcoin transactions that are only published when settlement is needed.
- Until **settlement transaction** is published, **double spending** is still possible.

Payment Channels 1/2

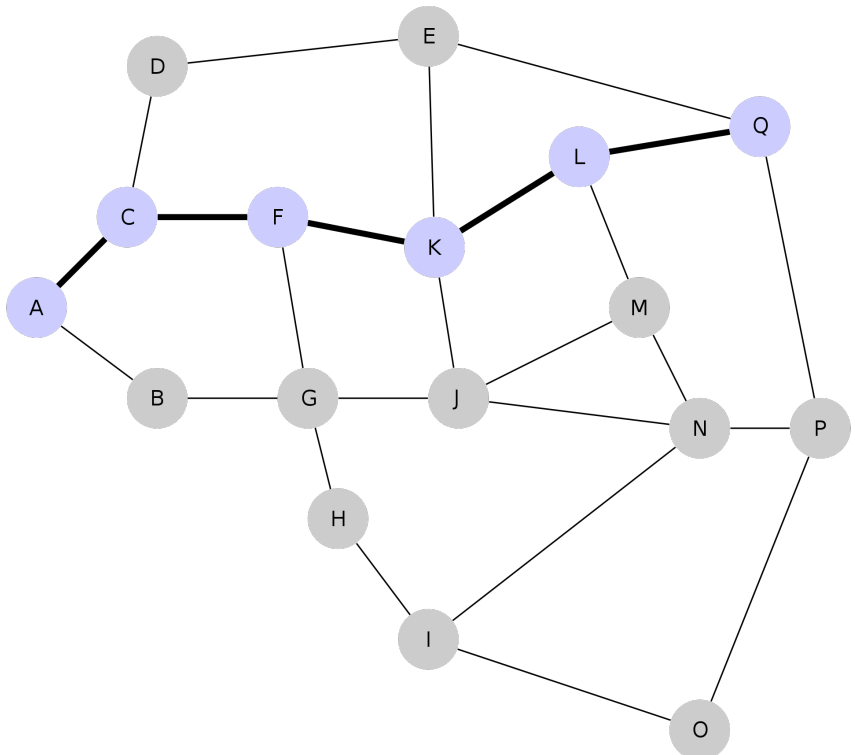
- **Payment channel** is a construction that allows **two** parties to transact Bitcoin without submitting any transactions to the Bitcoin network.
- **Bidirectional payment channel** is somewhat similar to a payment check that splits a joint bank account between two parties.
  - joint bank account with ballance N;
  - both parties A and B "own" $N/2$ portions of the ballance;
  - both parties sign a check that pays $N/2$ money to A and B;
  - when party A wants to pay M money to party B, they **sign a new check** that pays $N/2 - M$ to party A and $N/2 + M$ to party B and **destroy the old checks**.

Payment Channels 2/2

- Several proposals: Spillman, CLTV, Poon-Dryja, Decker-Wattenhofer duplex payment channels, Decker-Russell-Osuntokun eltoo Channels.
- Poon-Dryja payment channels were presented in the Lightning Network paper.
- Channel backing funds are locked into a 2-of-2 multisig.
- Before the funding transaction is even signed, commitment transactions for each party are first written and signed.
- As it requires referring to transactions that have not been signed yet, it requires using a transaction format that separates signatures from the part of the transaction that is hashed to generate the txid, such as Segregated Witness.

Lightning Network 1/2

- A network of bidirectional payment channels that allows to execute multi-hop payments, propagating funds through a series of payment channels.
- Proposed in 2015, mainnet network started operation in early 2018.



Lightning Network 2/2

- Every channel is a 2-of-2 multisig “joint account”
- Funding transaction:

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

Lightning Network 3/2

- Two payout transactions are created immediately, one for each participant.
- Remote output looks like this:

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

- Local output looks like this:

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

Lightning Network 2/2

- Entity A wants to pay entity B and there is a path within the network between them $A, C_1, C_2, ..., C_n, B$:
  - B generates a random value R and computes a hash $H = hash(R)$ and provides H to A;
  - A and creates an additional HTLC (Hash Timelock Contract) output and updates it's channel with 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 updates its payment channels with C_2 and so on, until C_n updates channel with B.
  - B provides R to C_n and pulls funds, C_n provides R to C_{n-1} and so on until C_1 pulls funds from A.

Lightning Network Usage

- 11,380 nodes (20,478 nodes in 2021),
- 42,459 channels (45,774 channels in 2021),
- 4,230.60 BTC = $400,334,511 (1,332.25 BTC = $52,290,595 in 2021),
- Ongoing research, improvements and new feature development,
- Games, online shops and other businesses.

Recommended Resources

- **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

The End

Thank you!