Buying Coffee at Lightning Speed

Dr. Christian Decker
Core Tech Engineer
Let’s buy a coffee
Bitcoin does not scale!

- Disk space: <500 transactions per second
- Processing power: <200 transactions per second
- Network bandwidth: <100 transactions per second
- Artificial 1MB limit: <3 transactions per second
Simple Micropayment Channel
Replacement strategies

- Replace by Incentive
- Replace by Timelock
- Replace by Thread
Duplex Micropayment Channels
Lightning

Blue after T=100
OR Green + <secretB>

Green after T=100
OR Blue + <secretG>
Secure Multihop Transfers
Hashed Timelock Contract (HTLC)

```plaintext
OP_IF
  OP_HASH160 <secrethash> OP_EQUALVERIFY
  <green-pubkey>
OP_ELSE
  36 OP_CSV
  <blue-pubkey>
OP_ENDIF
OP_CHECKSIG
```
Onion Routing
Advantages

- Improved scalability
- Real-time transfers
- Improved privacy
- Fast experimentation
Meet the Community

- Blockstream
- eclair
- Lightning Labs
- MIT DCI
- BitFury
Open Problems

- Routing (Link-State vs Distance-Vector)
- Network Topology
- Segwit Activation
- Payment decoupling
Thanks! Questions?