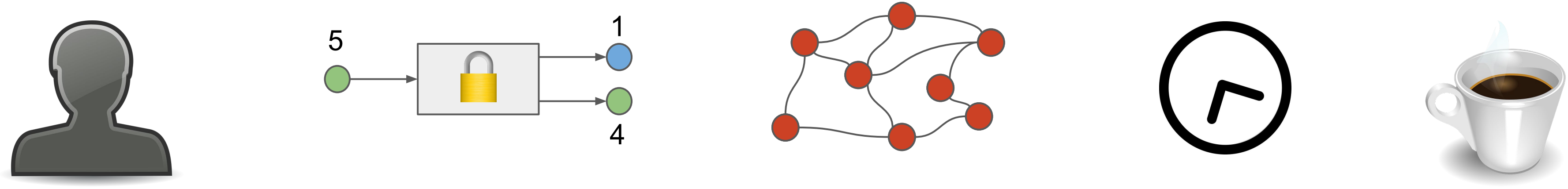
Blockstream

Buying Coffee at Lightning Speed

Dr. Christian Decker

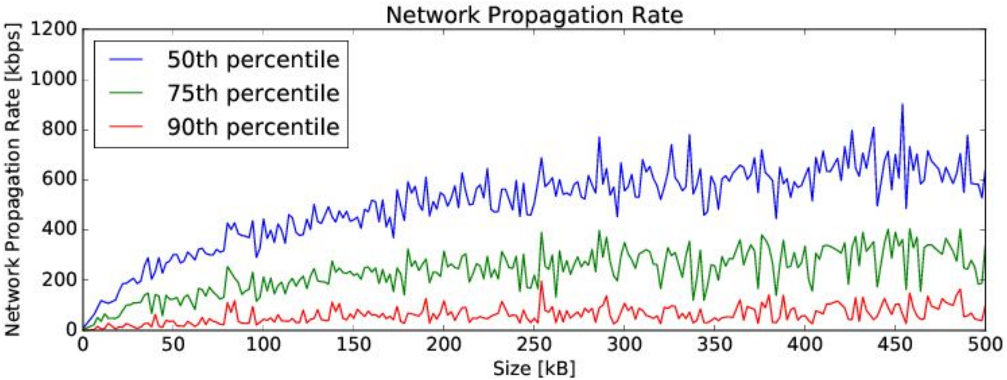
Core Tech Engineer

Let’s buy a coffee

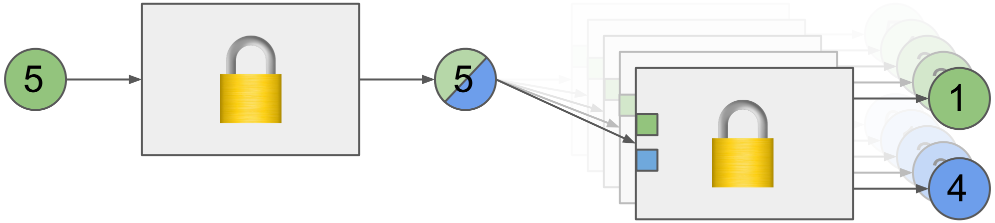


Bitcoin does not scale!

- 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



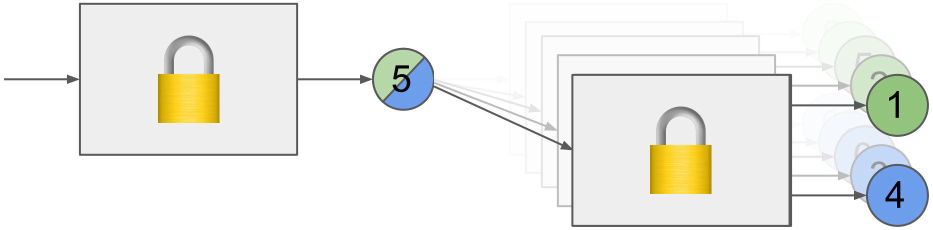
Simple Micropayment Channel



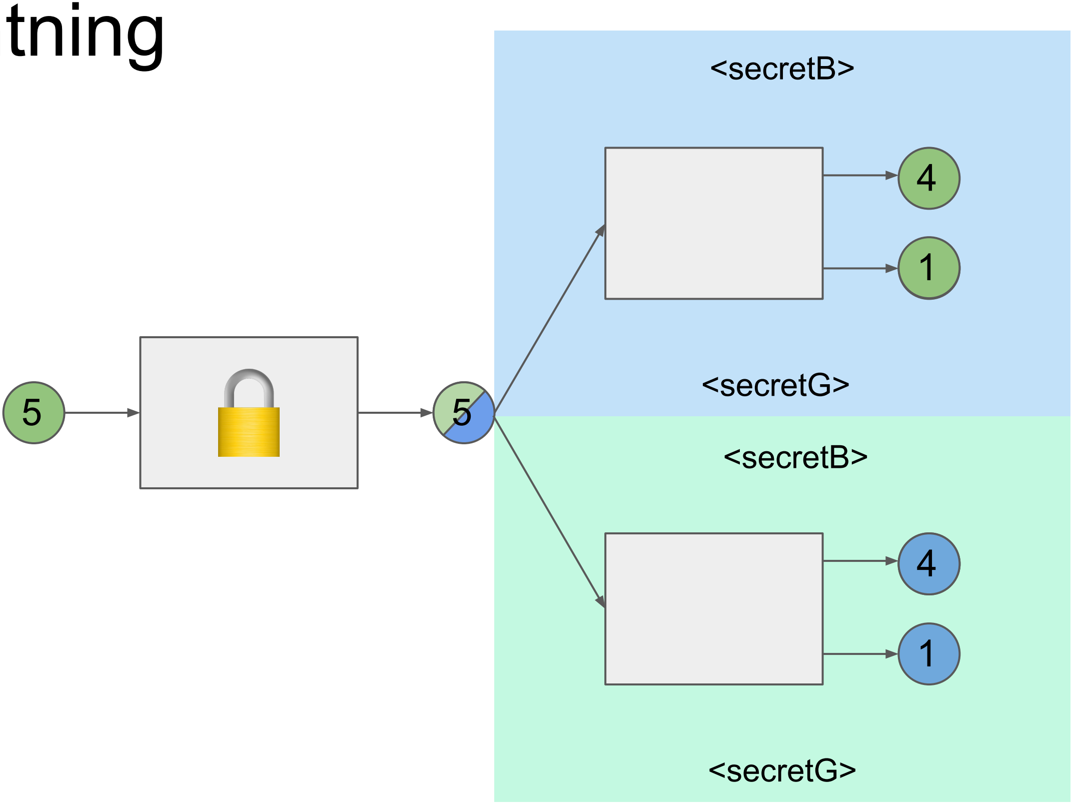
Replacement strategies

- Replace by Incentive
- Replace by Timelock
- Replace by Thread

Duplex Micropayment Channels



Lightning



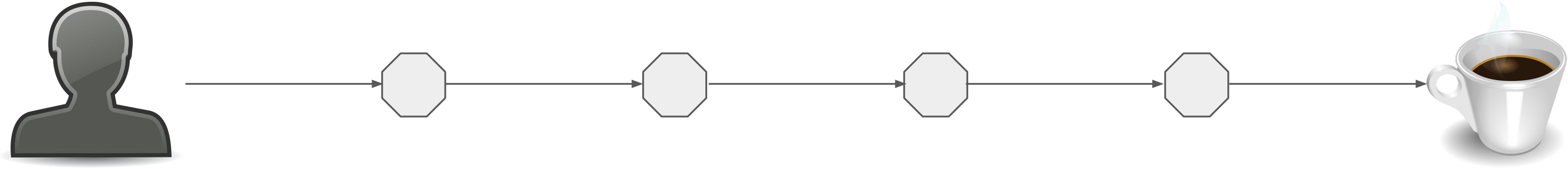
Blue after T=100

OR Green + <secretB>

Green after T=100

OR Blue + <secretG>

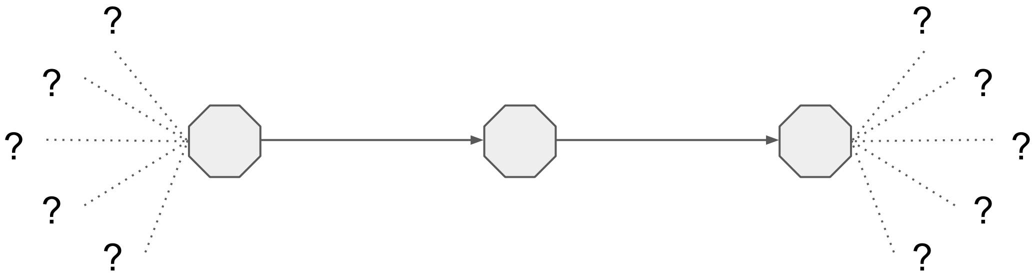
Secure Multihop Transfers



Hashed Timelock Contract (HTLC)

```
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

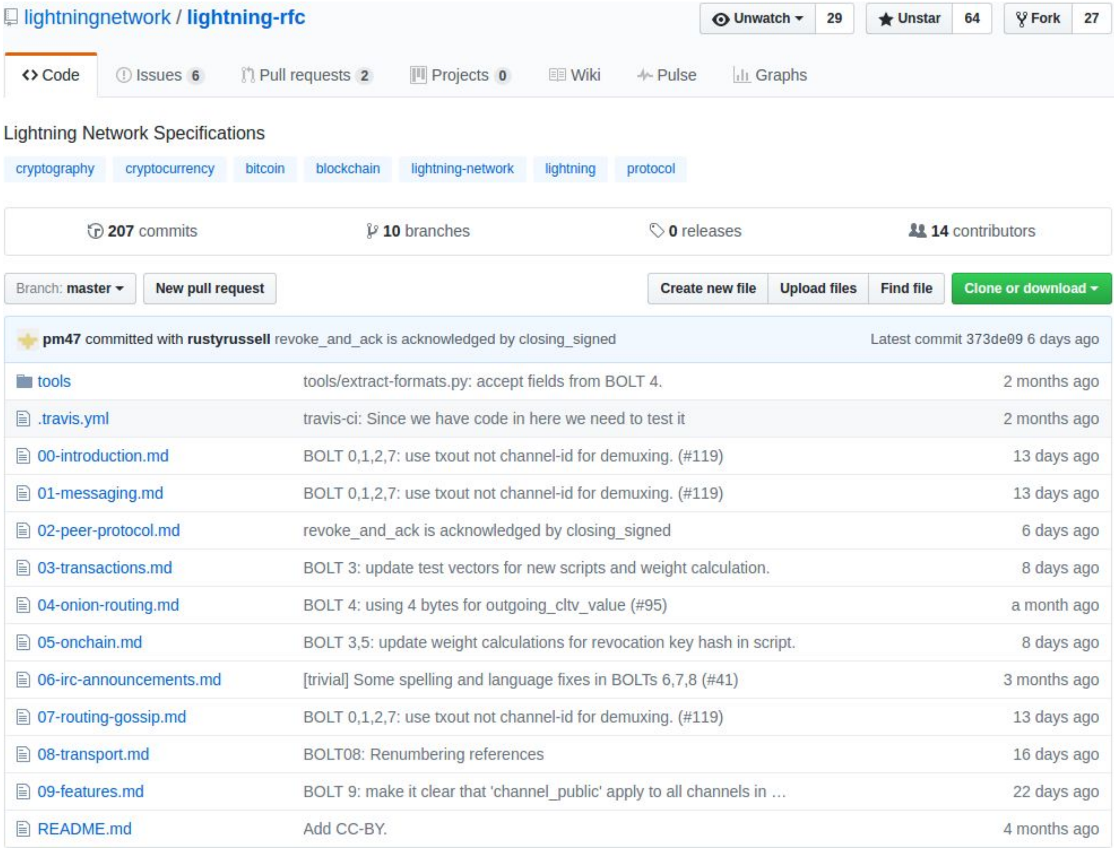
Blockstream

eclair

Lightning Labs

MIT DCI

BitFury



lightningnetwork / lightning-rfc

Lightning Network Specifications

cryptography cryptocurrency bitcoin blockchain lightning-network lightning protocol

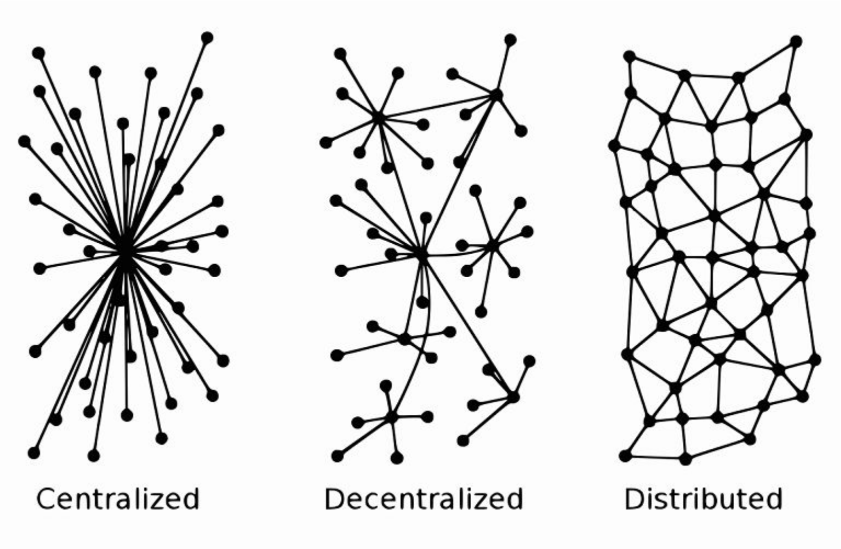
207 commits 10 branches 0 releases 14 contributors

pm47 committed with rustyrussell revoke_and_ack is acknowledged by closing_signed Latest commit 373de09 6 days ago

tools	tools/extract-formats.py: accept fields from BOLT 4.	2 months ago
.travis.yml	travis-ci: Since we have code in here we need to test it	2 months ago
00-introduction.md	BOLT 0,1,2,7: use txout not channel-id for demuxing. (#119)	13 days ago
01-messaging.md	BOLT 0,1,2,7: use txout not channel-id for demuxing. (#119)	13 days ago
02-peer-protocol.md	revoke_and_ack is acknowledged by closing_signed	6 days ago
03-transactions.md	BOLT 3: update test vectors for new scripts and weight calculation.	8 days ago
04-onion-routing.md	BOLT 4: using 4 bytes for outgoing_cltv_value (#95)	a month ago
05-onchain.md	BOLT 3,5: update weight calculations for revocation key hash in script.	8 days ago
06-irc-announcements.md	[trivial] Some spelling and language fixes in BOLTs 6,7,8 (#41)	3 months ago
07-routing-gossip.md	BOLT 0,1,2,7: use txout not channel-id for demuxing. (#119)	13 days ago
08-transport.md	BOLT08: Renumbering references	16 days ago
09-features.md	BOLT 9: make it clear that 'channel_public' apply to all channels in …	22 days ago
README.md	Add CC-BY.	4 months ago

Open Problems

- Routing (Link-State vs Distance-Vector)
- Network Topology
- Segwit Activation
- Payment decoupling



Blockstream

Thanks! Questions?