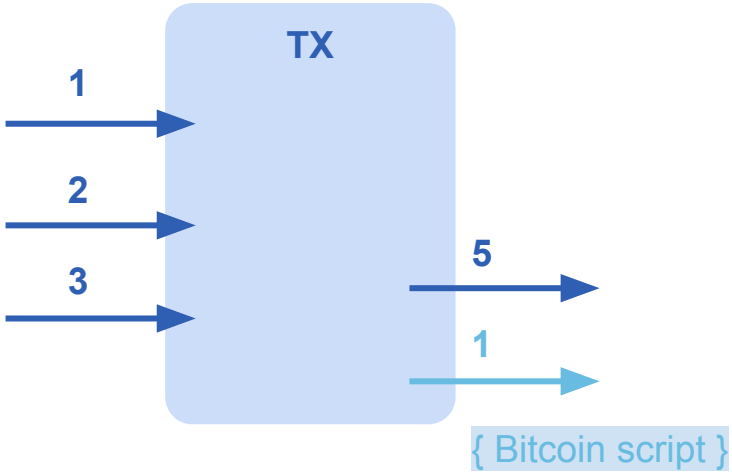
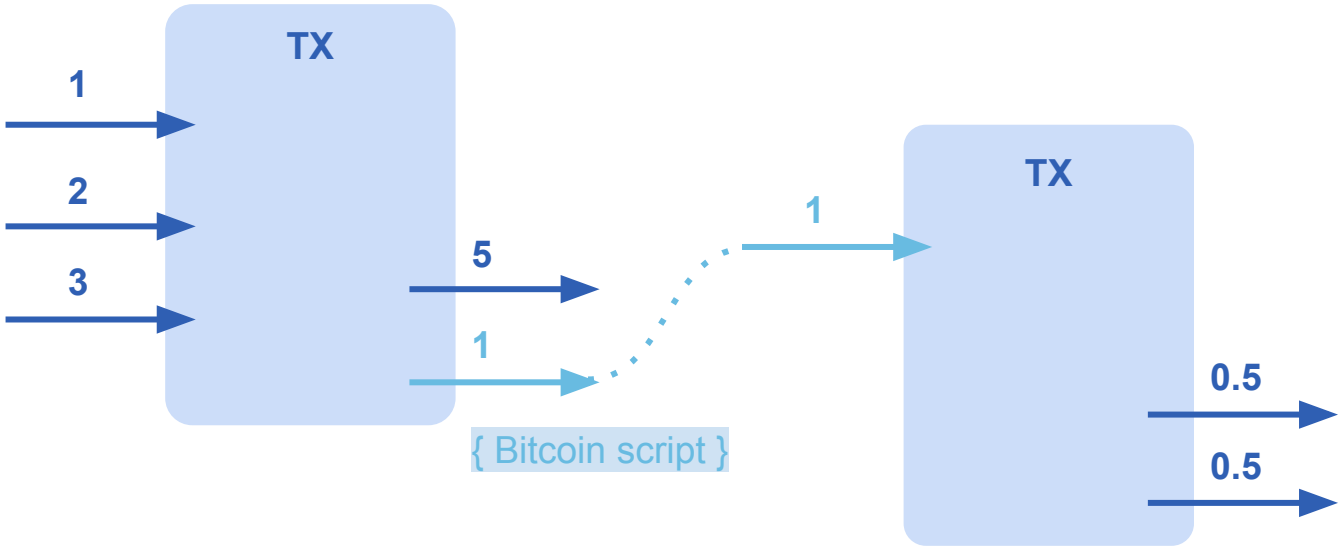
Lightning overview ⚡

Ололо пыщь пыщь

Igor Korsakov / bluewallet.io / Berlin / June, 2019

blue wallet

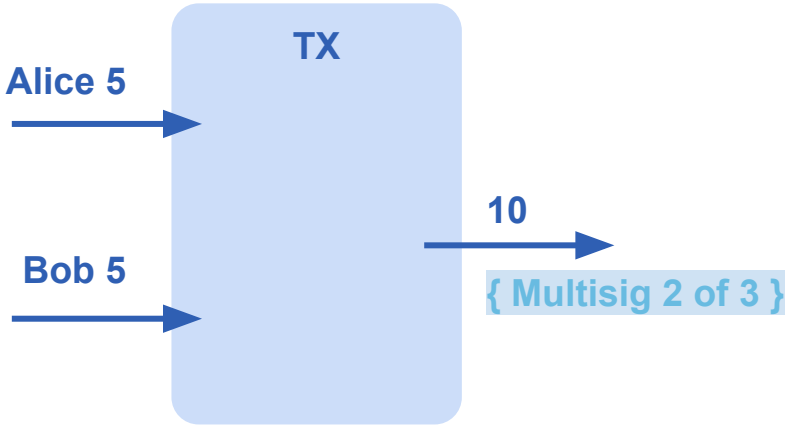




Bitcoin script

- Require 1 sig to spend
- Require M of N sigs to spend (multisig)

Multisig example

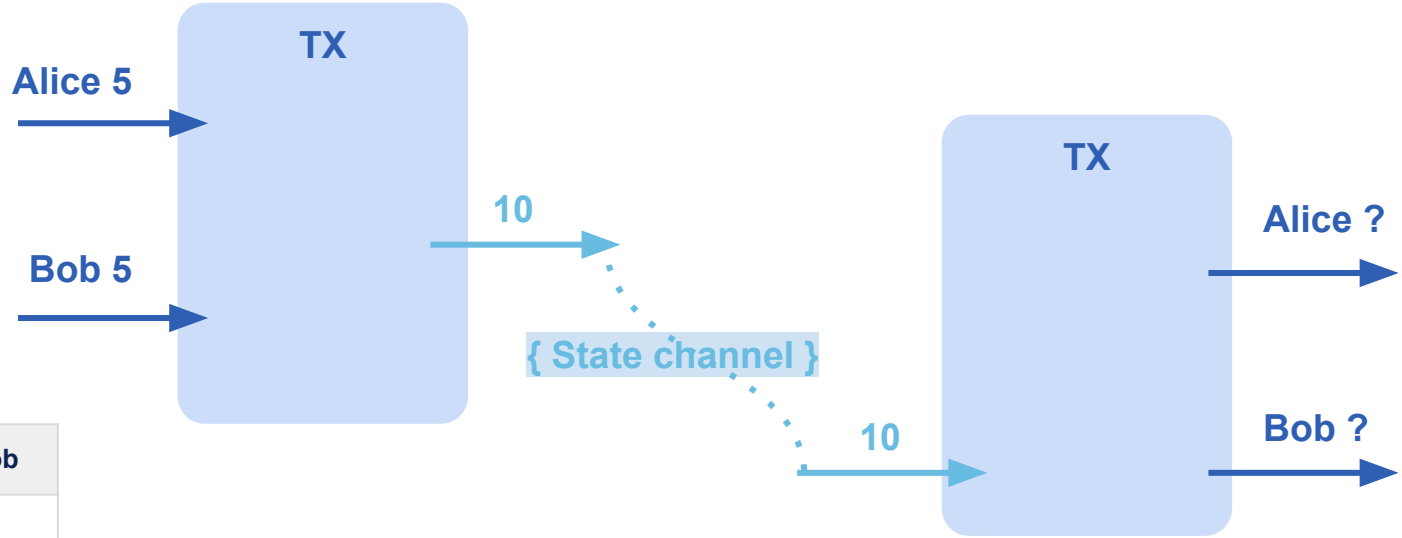


Keys

Alice
Bob
Charlie (escrow)

blue wallet

Payment Channels



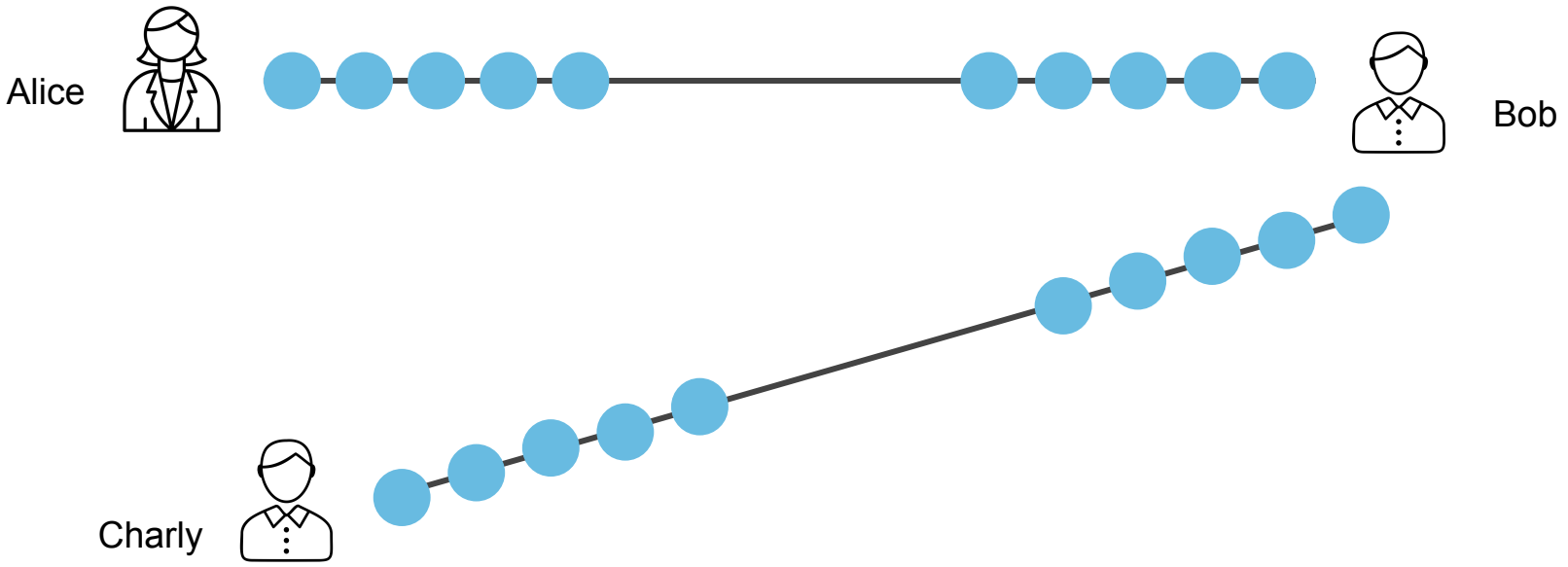
#	Alice	Bob
1 (init)	5	5
2	4	6
3	3	7
4	7	3

blue wallet

Payment Channels

blue wallet

Alice **can pay** Charly. For Bob it will look like more coins in one channel and less in other (+ fees)



blue wallet

Properties of LN

- LN works
- It’s lightning (lol) fast
- Txs are practically final and irreversible
- Coins in LN are the same bitcoins, there is no peg or conversion rate
- …
- Profit!
- BTC in LN are more liquid
- BTC in LN are more anonymous
- Onion routing, no historical data to analyse
- As LN economy grows, there is no reason to move coins out of LN

blue wallet

Properties of LN

- Renders 99,85% altcoins obsolete

If your business already accepts different coins, you can start accepting Lightning bitcoins for a bunch of benefits:

- Real bitcoins
- Instant
- Irreversible

blue wallet

Scalable?

1 channel can make up to 200 tx/sec

VISA: 24000 tx/sec

Silly math: 120 channels can have same throughput as VISA

That’s 240 nodes. Whole LN network: 7300 nodes

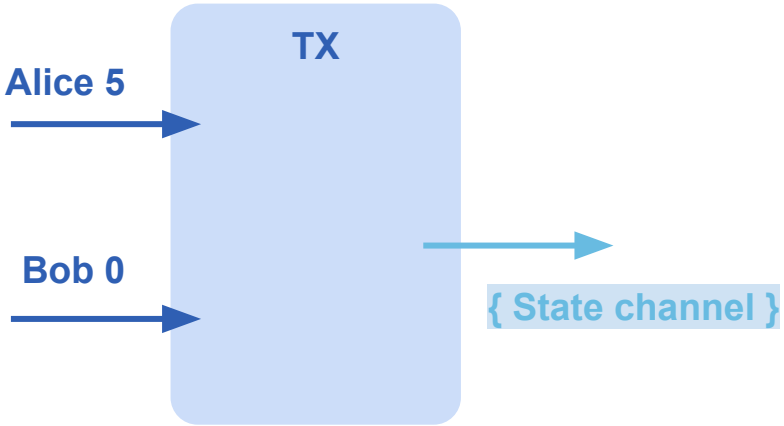
=>

LN = 30 x VISA

blue wallet

Bad stuff about LN

Remote party won't commit their coins with you (random nobody from teh interwebz) when you open a channel



blue wallet

Bad stuff about LN

Remote party won't commit their coins with you (random nobody from teh interwebz) when you open a channel

blue wallet

Bad stuff about LN

- Dual funded channels are not there yet, and might be problematic
- No incoming capacity
- A bunch of tricks (or even a paid service) to get incoming capacity

Solution:

- Apply efforts to maintain your node and incoming capacity
- Or use a payment processor:
  - Acinq Strike
  - Opennode
  - Coingate
  - Globee
  - lightningpay.co.uk

blue wallet

Bad stuff about LN

- Channel size is hard capped to ~0.16 BTC
- Payment size is also capped

=> OK if your average order < $100

- Network consists of mostly enthusiasts with small capacity channels and unreliable nodes: not good to reliably route payments
- It is more reliable to receive payments than send payments (when routing fails when sending payment, funds get stuck for some time)
- Nodes have to stay online all the time

blue wallet

Bad stuff about LN

- LN is as good as lightning economy, which is not huge atm (LNPizza, Bitrefill, Coincards, Zigzag)
- LN economy can’t grow faster than btc economy
- Real advantages of LN will be seen in next cycle of adoption, when people will be “Ok, if I pay for this via onchain, I’ll overpay THIS much. Better use offchain ”
- L1 is still more important than L2

blue wallet

Bad stuff about LN

- Offline payments are not convinient

blue wallet

The future of LN

- AMP
- Splicing
- Sphinx
- Channel factories
- Eltoo
- Trampoline payments
- Other smart-sounding words normies don’t care about

blue wallet

Now:

- Currently serving small merchants
- Serving small OTC exchanges (like Zigzag.io)
- Receiving LN payments is very reliable and convenient

Next: Increasing max payment size and max channel capacity:

- Serve medium-size merchants
- Process greater average order-size / high value transactions (more expensive goods sold online etc)
- Less routing failures because some channels capacity is insufficient
- Economically-significant nodes cluster around each other
- Onboard bigger exchanges (classic-ones, with order books and matchmaking)
- Exchange-to-exchange clearing

blue wallet

LN works with limited connectivity in remote places in the world

blue wallet

LN works with limited connectivity in remote places in the world

- Need to open a channel: create TX offline, broadcast via SMS (or pigeons)
- Monitor blockchain for opening & closing transactions: use satelite dish, blockchain is broadcasted from satelites globally
- …
- Profit!
- A group of people can transact even with very limited connectivity

blue wallet

LN: Interplanetary (intergallactic?) ready

~15 min light travel time

Can’t efficiently mine transactions with such propagation time. Party with minority hashrate will have way too many orphan blocks. Can’t transact onchain as well: on top of confirmation time adds signal travel time back and forth. Solution?

- Open a payment channel (15 min to deliver tx to Earth, plus 6 blocks confirmation)
- Transact locally as much as you want
- Close a channel when convinient (or don’t close at all)

blue wallet

About **Bluewallet**

blue wallet

bluewallet **last 3 months (Q1 2019)**

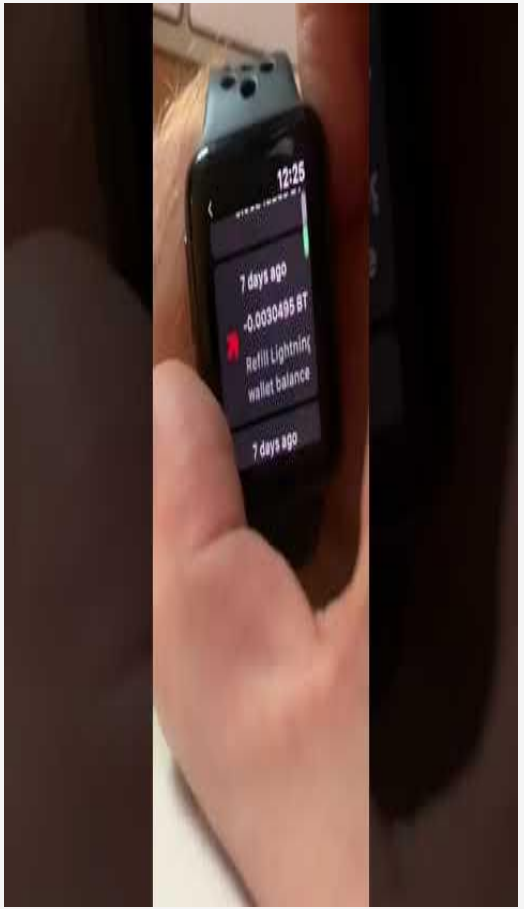
30 000 +
Downloads

80 000 +
Lightning TXs

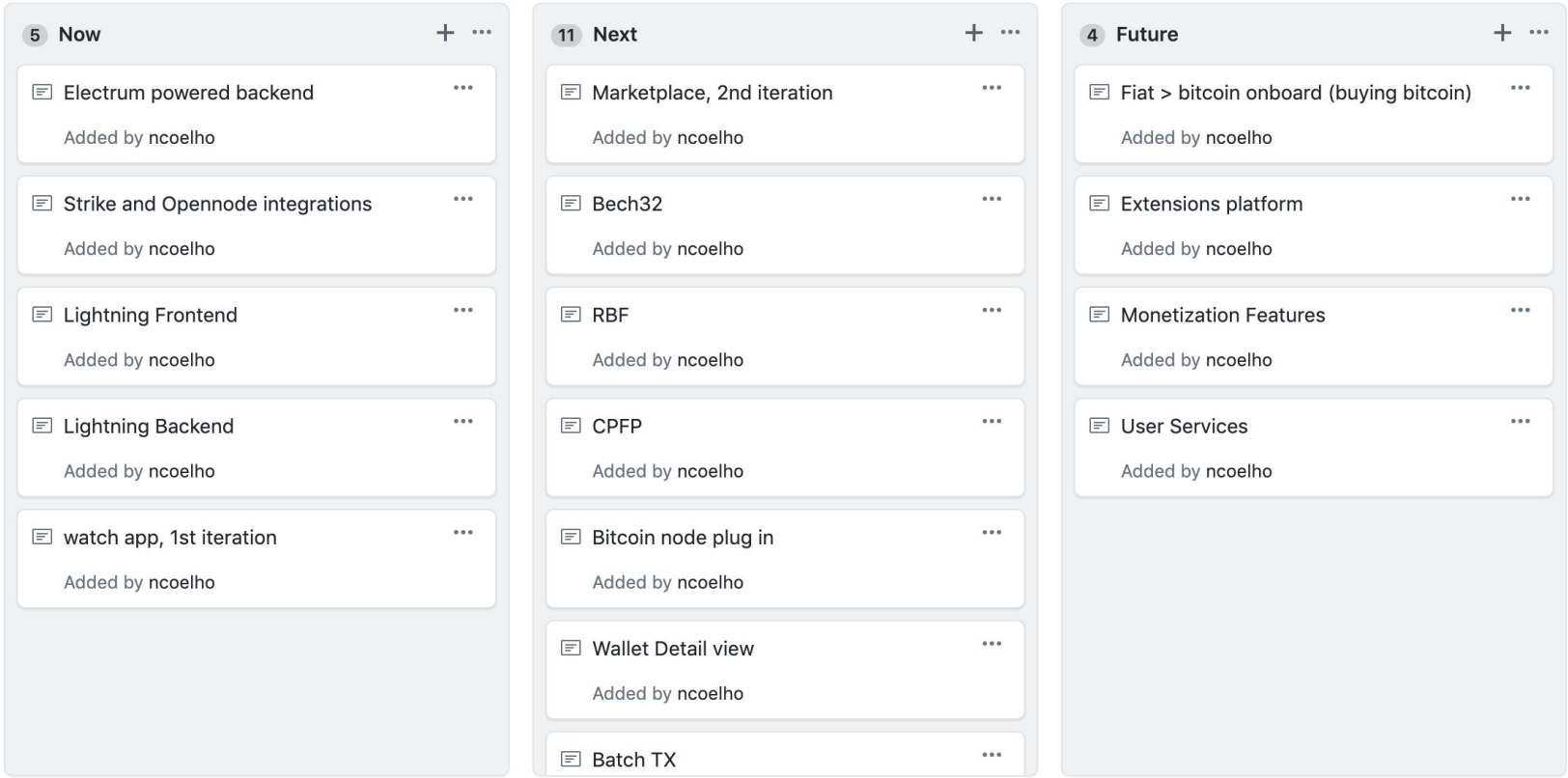
40 btc
Transacted in LN

blue wallet

Things we **are working on**



Roadmap on github (link)



i@bluewallet.io

“Not great, just ok”

“Only one coin”

“Just another wallet”

blue wallet

“Meh”

“It’s a custodial wallet”

“Some features”