Lightning Network

Ante Sosa

Faculty of Computer and Information Science University of Ljubljana

August 16, 2019

Agenda

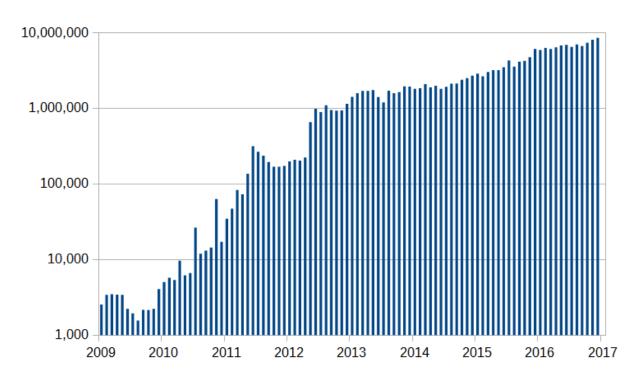
- 1 Bitcoin
- 2 Scalability problem
- 3 Lightning Network
- 4 Payment channels
- **5** Network of payment channels
- 6 Conclusion

Bitcoin

- 2008.
- Satoshi Nakamoto.
- Peer to peer network.
- Digital ledger.
- Proof of work.
- Transactions.

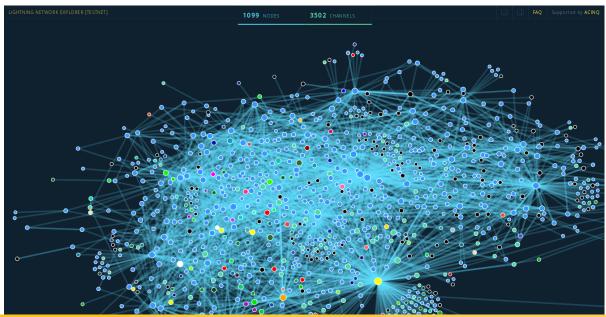
Scalability problem

- Higher fees and slower transactions.
- Competing with Visa.
- Various proposed solutions.



Lightning Network

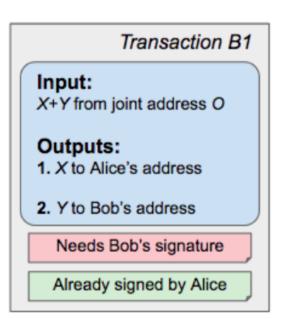
- 2015.
- Joseph Poon and Thaddeus Dryja.
- The main idea.
- Off chain solution.
- Payment channels.



Ante Sosa Lightning Network August 16, 2019 5 / 11

Payment channels

Input: X+Y from joint address O Outputs: 1. X to Alice's address 2. Y to Bob's address Already signed by Bob Needs Alice's signature



Payment channels

Transaction Ai

Input:

X+Y from joint address O

Outputs:

 X' to Alice's address (only after T blocks)

1.2. X' to Bob's address (if Bob show AKi key)

2. Y' to Bob's address

Already signed by Bob

Needs Alice's signature

4

Bob reveals BK(i-1)

Transaction Bi

Input:

X+Y from joint address O

Outputs:

1. X' to Alice's address

2.1. Y' to Bob's address (only after T blocks)

or

Y' to Alice's address (if Alice shows BKi key)

Needs Bob's signature

Already signed by Alice

4

Alice reveals AK(i-1)

Network of payment channels

- Payment channel with intermediary.
- Sending funds over the network.
- Routing and optimal paths.
- Cost of each path is determined by dinamic factors:
 - network topology.
 - channels throughput.
 - availability of nodes.
 - intermediaries fees.

Conclusion

- Early stage of development.
- Negative sides.
- Improved anonymity.
- 5 500 Nodes, 23 000 channels filled up with more then 620 bitcoins.

Ante Sosa Lightning Network August 16, 2019

9 / 11

References

- Satoshi Nakamoto, Bitcoin: A Peer-to-Peer Electronic Cash System, www.bitcoin.org. (2008)
- Bitcoin developer guide, https://bitcoin.org/en/developer-guide
- Giovanni Di Stasi, Stefano Avallone, Roberto Canonico, Giorgio Ventre, Routing payments on the Lightning Network, University Federico II of Napoli (Italy)
- Joseph Poon, Thaddeus Dryja, The Bitcoin Lightning Network: Scalable Off-Chain Instant Payments

Questions



Ante Sosa Lightning Network August 16, 2019 11 / 11