Blockchain scaling: Lightning Network

BOLDARE

Tomasz Konieczny

Boldare - Senior QA Engineer

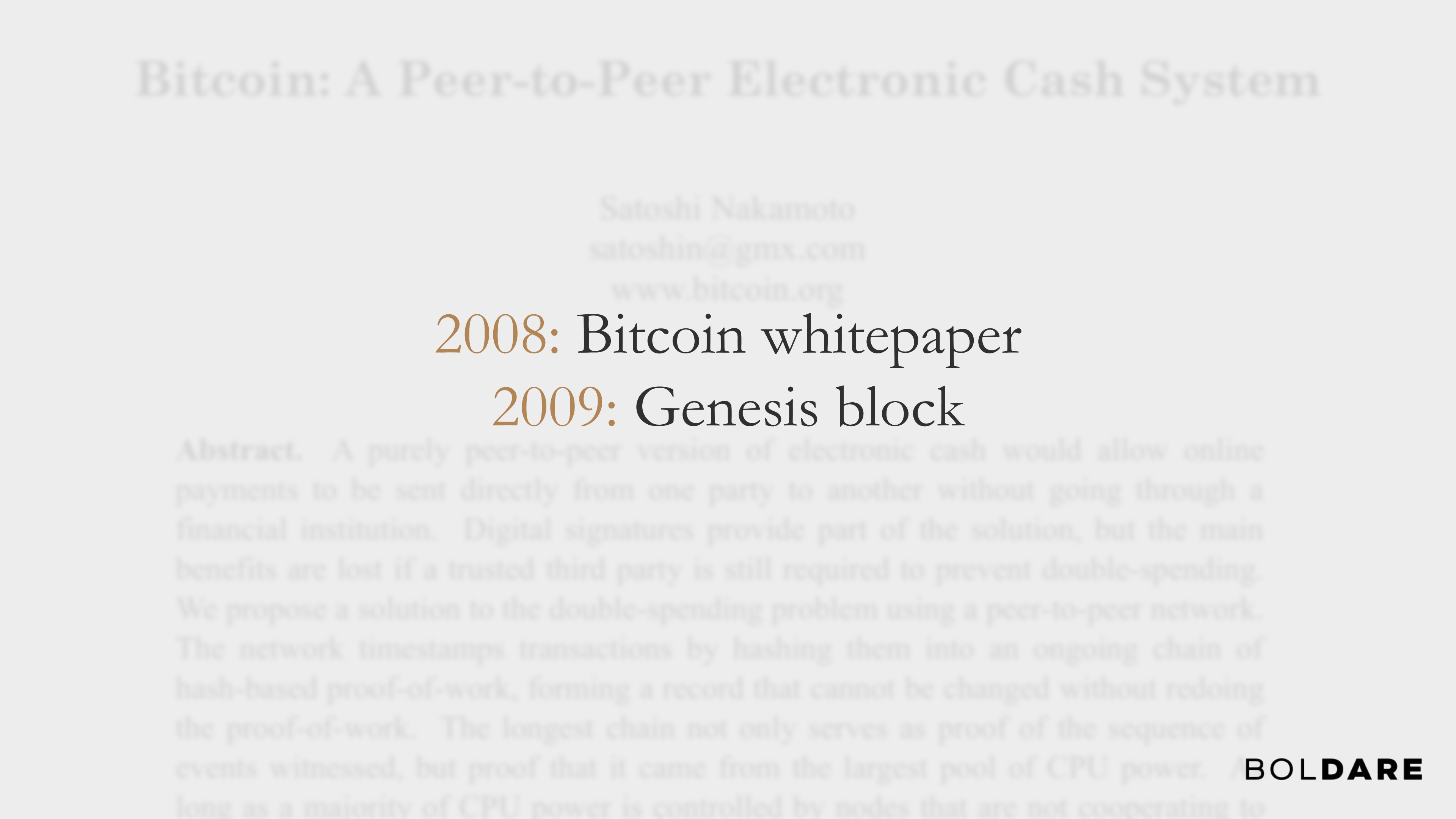
tomasz.konieczny@boldare.com

Plan

A bit of history

2008: Bitcoin whitepaper

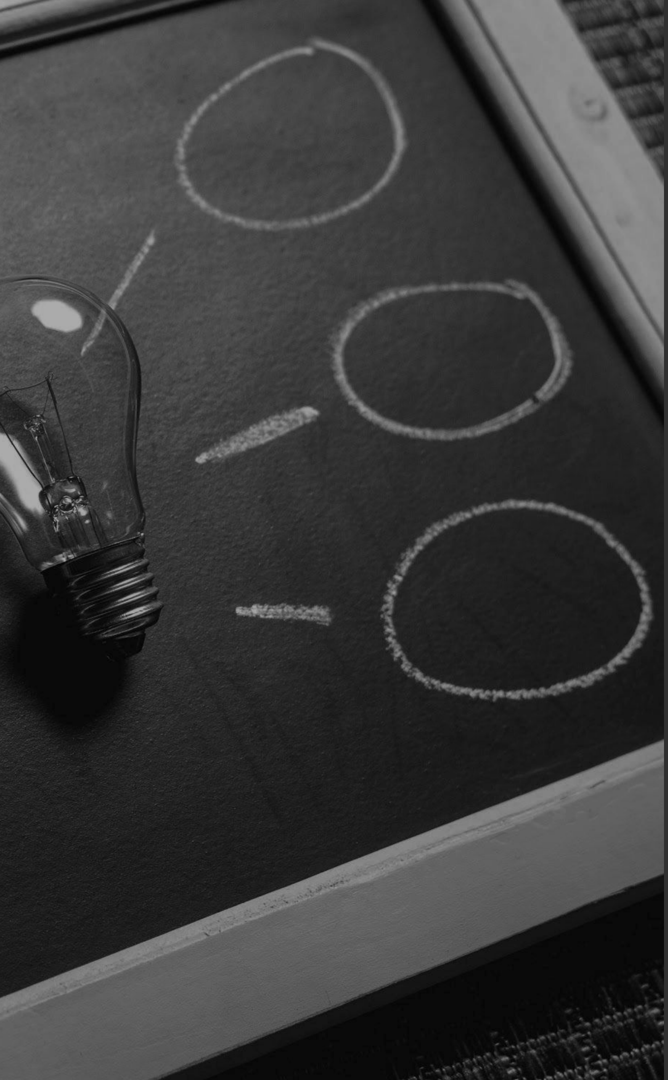
2009: Genesis block



Bitcoin: A Peer-to-Peer Electronic Cash System

Satoshi Nakamoto
satoshin@gmx.com
www.bitcoin.org

Abstract. A purely peer-to-peer version of electronic cash would allow online payments to be sent directly from one party to another without going through a financial institution. Digital signatures provide part of the solution, but the main benefits are lost if a trusted third party is still required to prevent double-spending. We propose a solution to the double-spending problem using a peer-to-peer network. The network timestamps transactions by hashing them into an ongoing chain of hash-based proof-of-work, forming a record that cannot be changed without redoing the proof-of-work. The longest chain not only serves as proof of the sequence of events witnessed, but proof that it came from the largest pool of CPU power. A long as a majority of CPU power is controlled by nodes that are not cooperating to



Transaction system - goals

- Secure
- Independent
- Trustless
- Censorship resistant
- Irreversible transactions

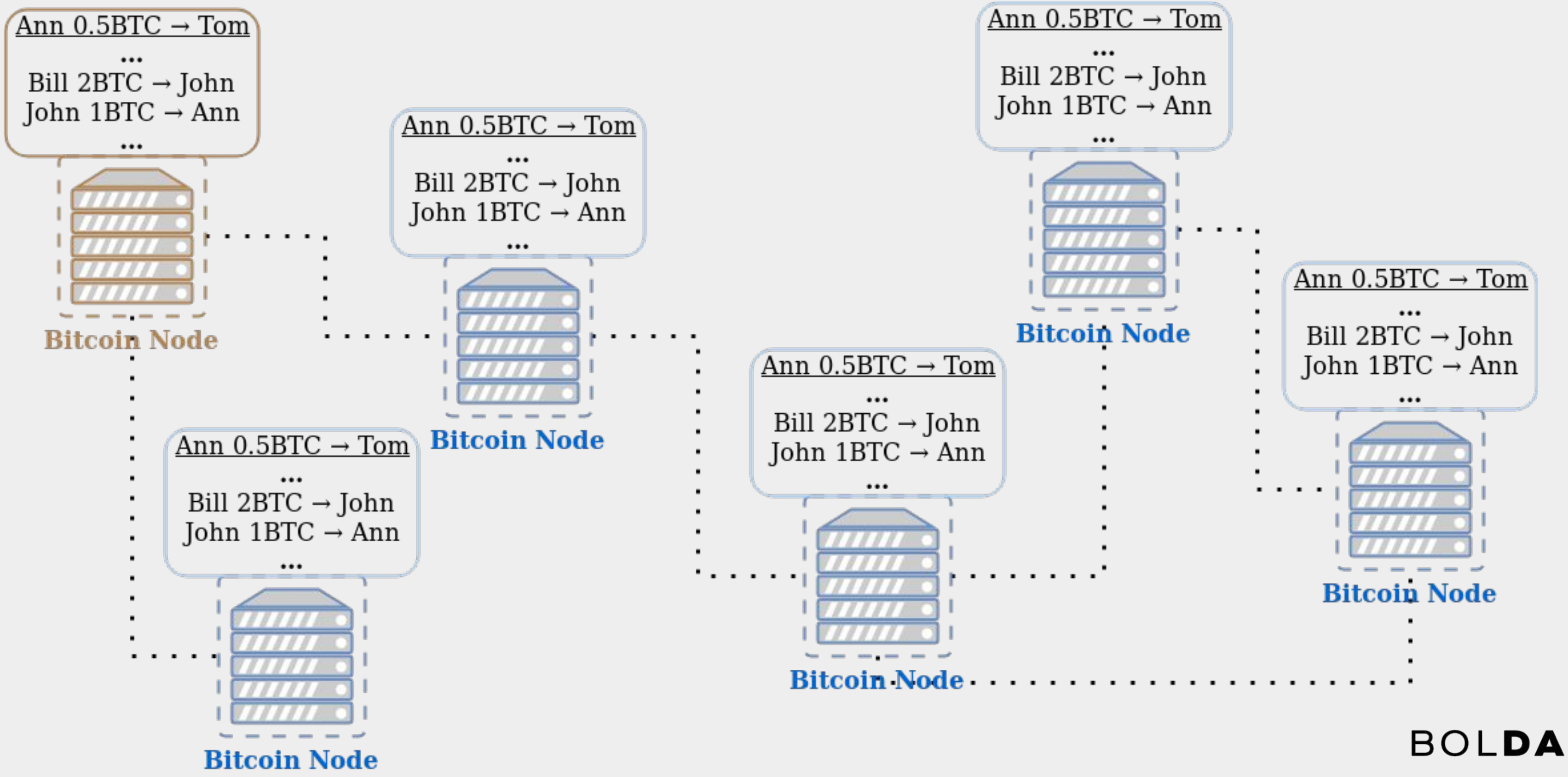
BOLDARE

Solution: Blockchain

Possible problems?

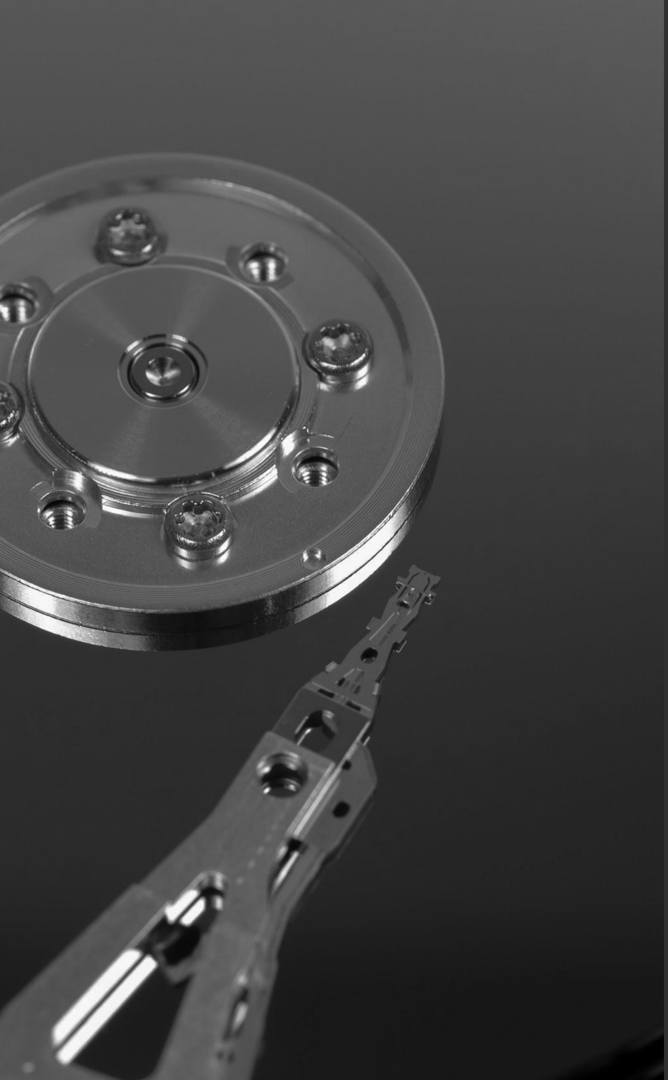
“We very, very much need such a system, but the way I understand your proposal, it does not seem to scale to the required size.”

Blockchain - Distributed ledger



BOLDARE

Satoshi’s answer



Block size limit

- Why?
- 1MB
- Only about 7-20tps
- Block size - consensus rule

On-chain scaling

- “Increase block size”
  - 2MB
  - 16MB
  - No limit
- “Decrease block time”
- Required hard fork
  - Update of all clients
- Performance

Do we really need every transaction on-chain?

Blockchain is often treated like a goal to achieve but should be just a solution.

The goal?

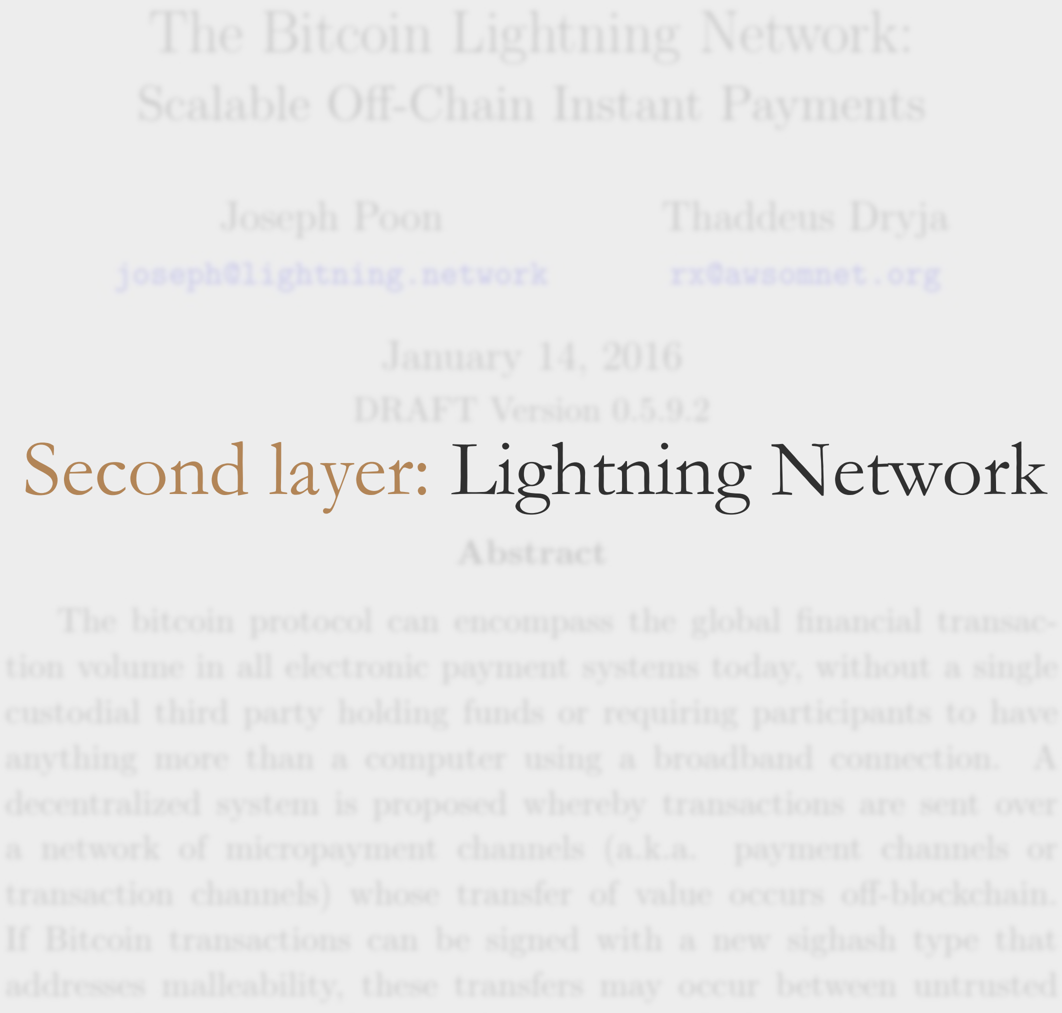
Increase network capacity.

Smart contracts?

Off-chain scaling concept

- Layer above blockchain
- Some of data “stored” off-chain
- Blockchain?
  - ❑ Blockchain as Arbiter
  - ❑ “Protocol”

Second layer: Lightning Network



The Bitcoin Lightning Network:
Scalable Off-Chain Instant Payments

Joseph Poon
joseph@lightning.network

Thaddeus Dryja
rx@awsomnet.org

January 14, 2016
DRAFT Version 0.5.9.2

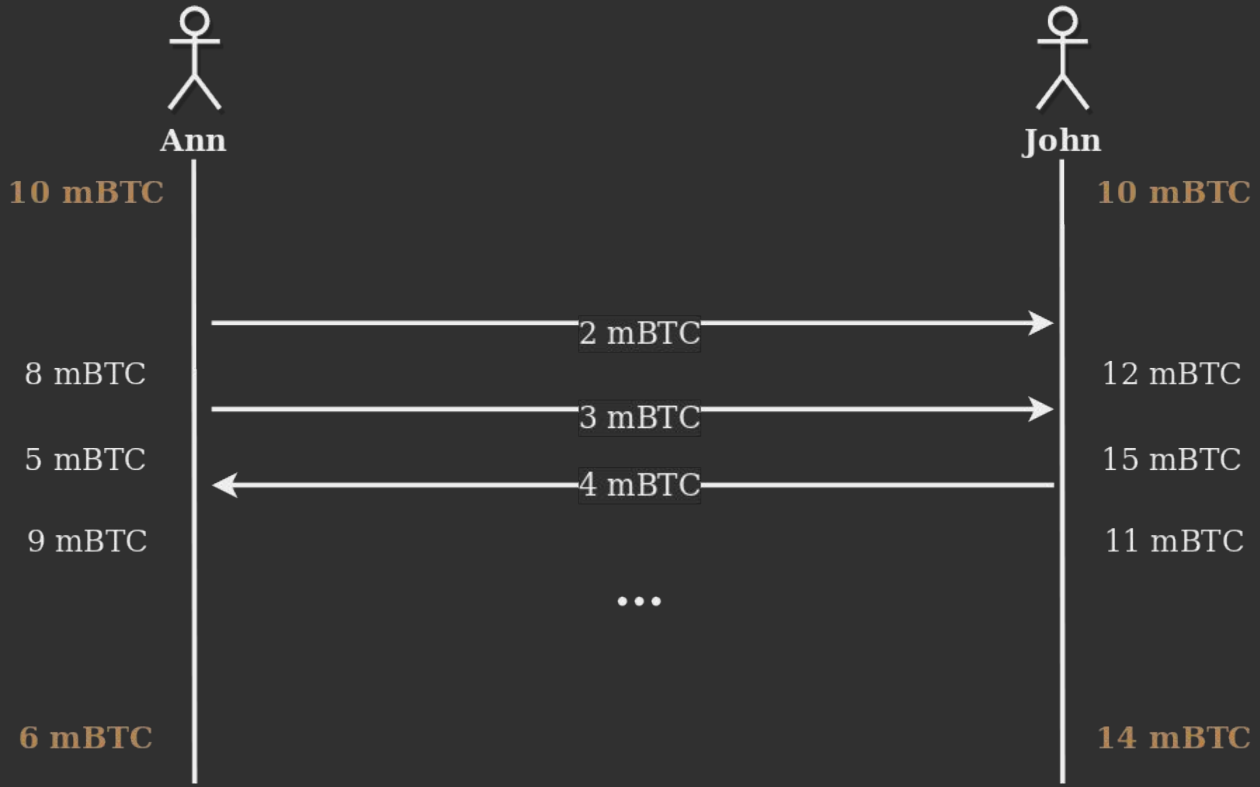
Abstract

The bitcoin protocol can encompass the global financial transaction volume in all electronic payment systems today, without a single custodial third party holding funds or requiring participants to have anything more than a computer using a broadband connection. A decentralized system is proposed whereby transactions are sent over a network of micropayment channels (a.k.a. payment channels or transaction channels) whose transfer of value occurs off-blockchain. If Bitcoin transactions can be signed with a new sighash type that addresses malleability, these transfers may occur between untrusted

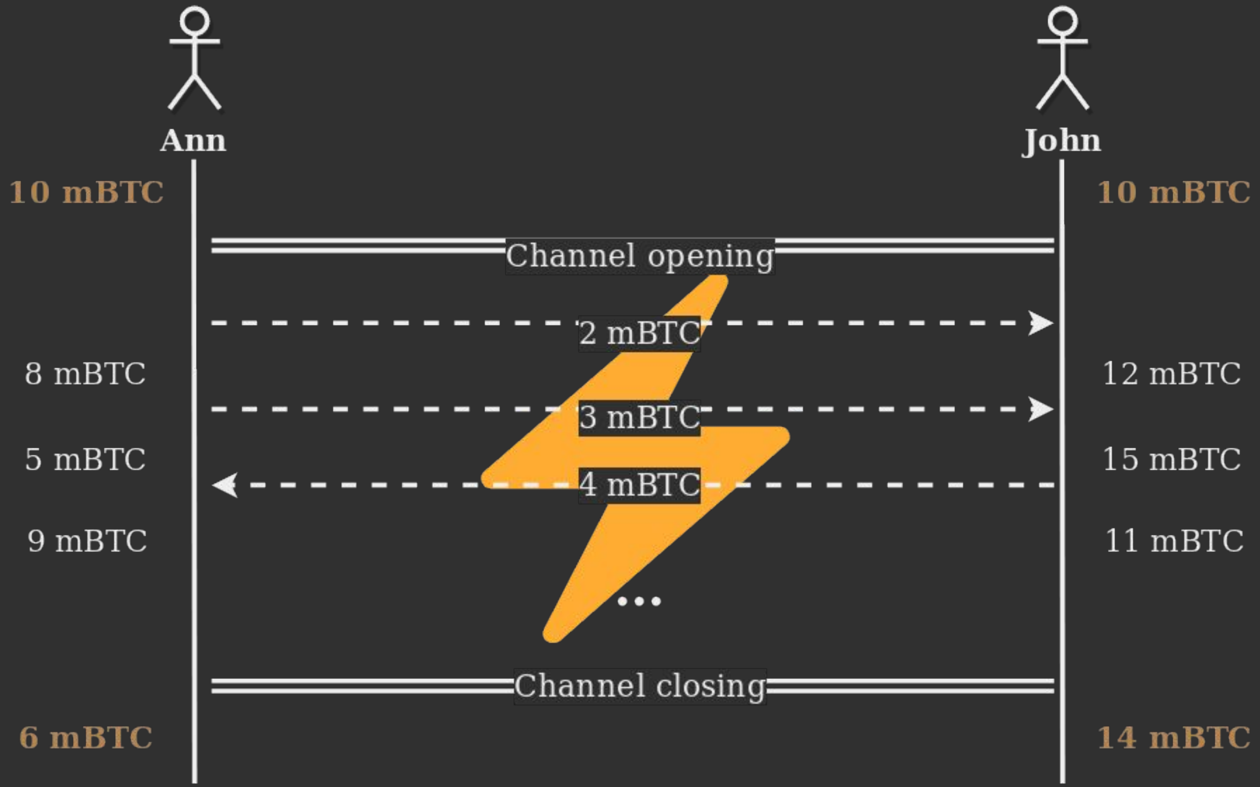
“Scalable Off-Chain Instant Payments”

Bidirectional Payment Channels

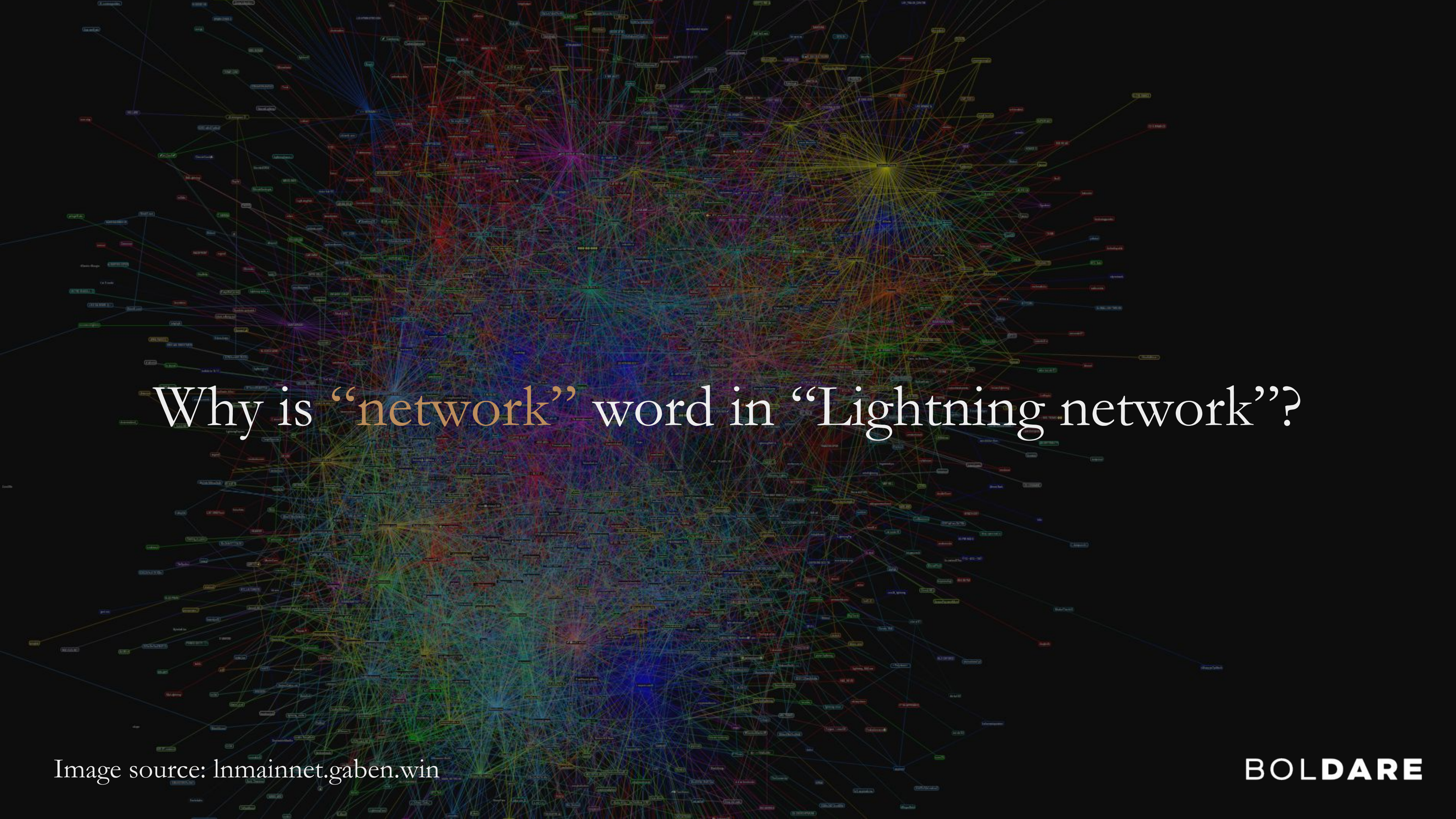
On-chain transactions



Payment channel



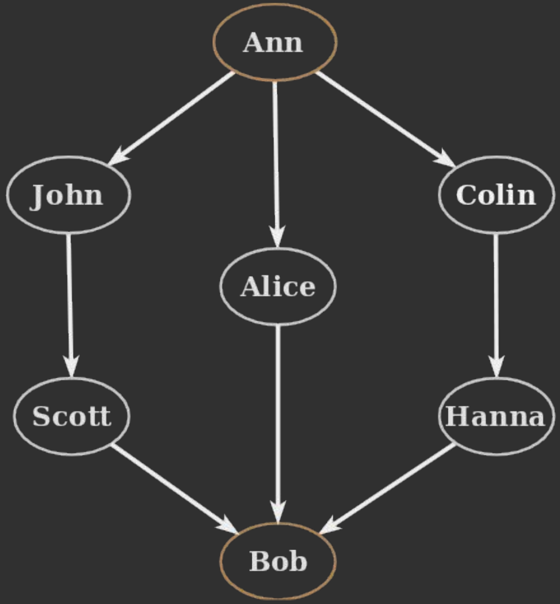
BOLDARE



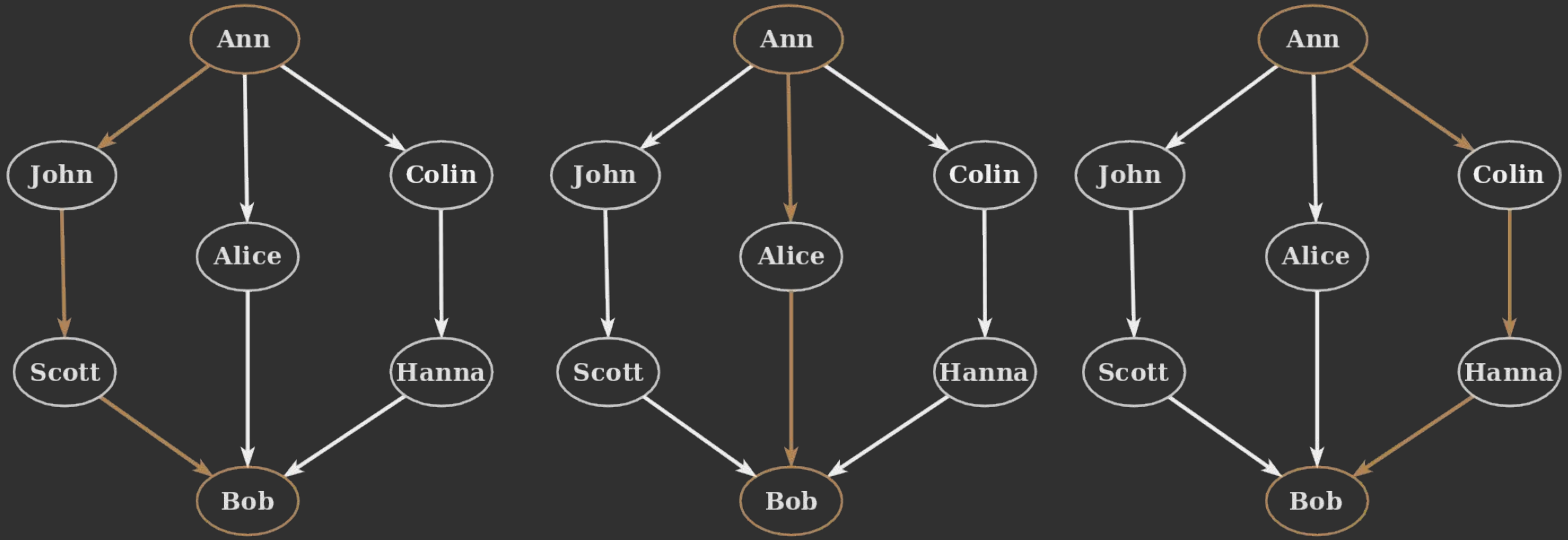
Why is “network” word in “Lightning network”?

Image source: lnmainnet.gaben.win

Payment routing



Payment routing

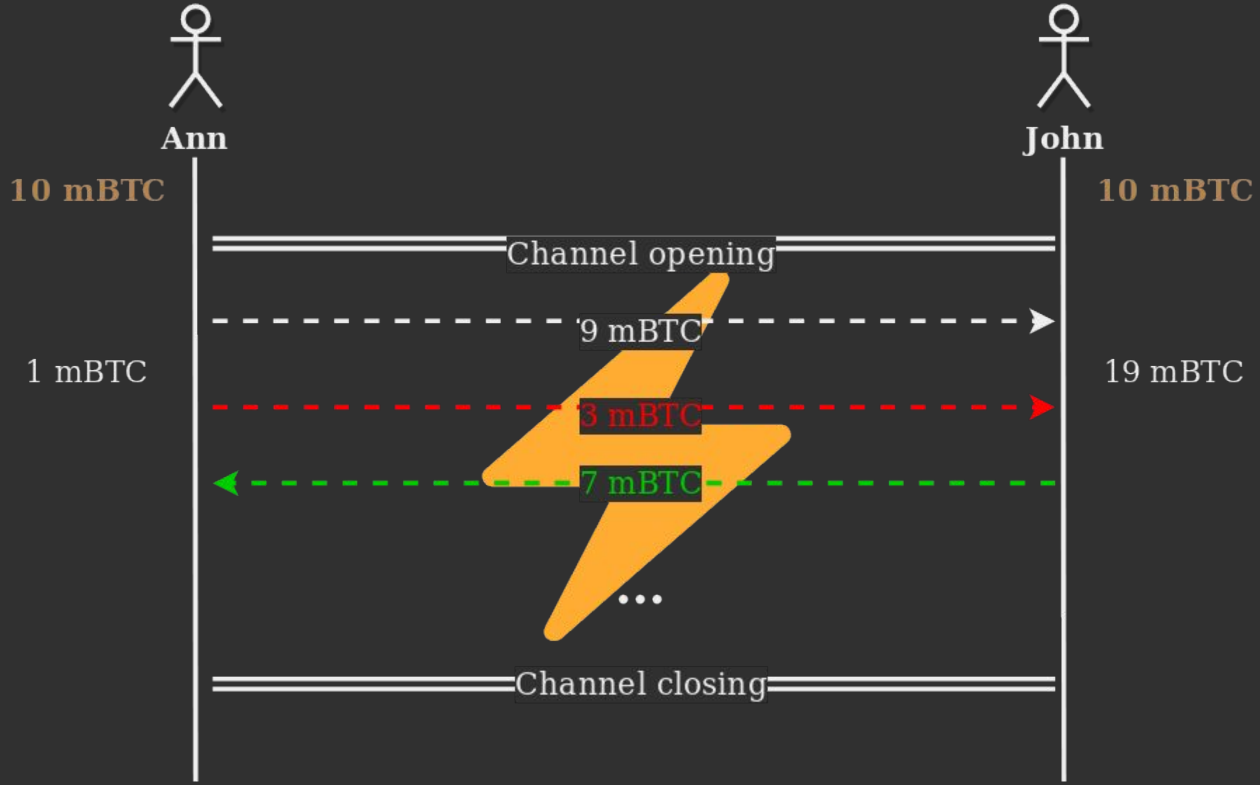


How routing works?

What is known?

- Payment channels
- Channels capacity

Channel state?



Trying possible routes

Scalable, instant, anonymous

Onion routing

Onion routing

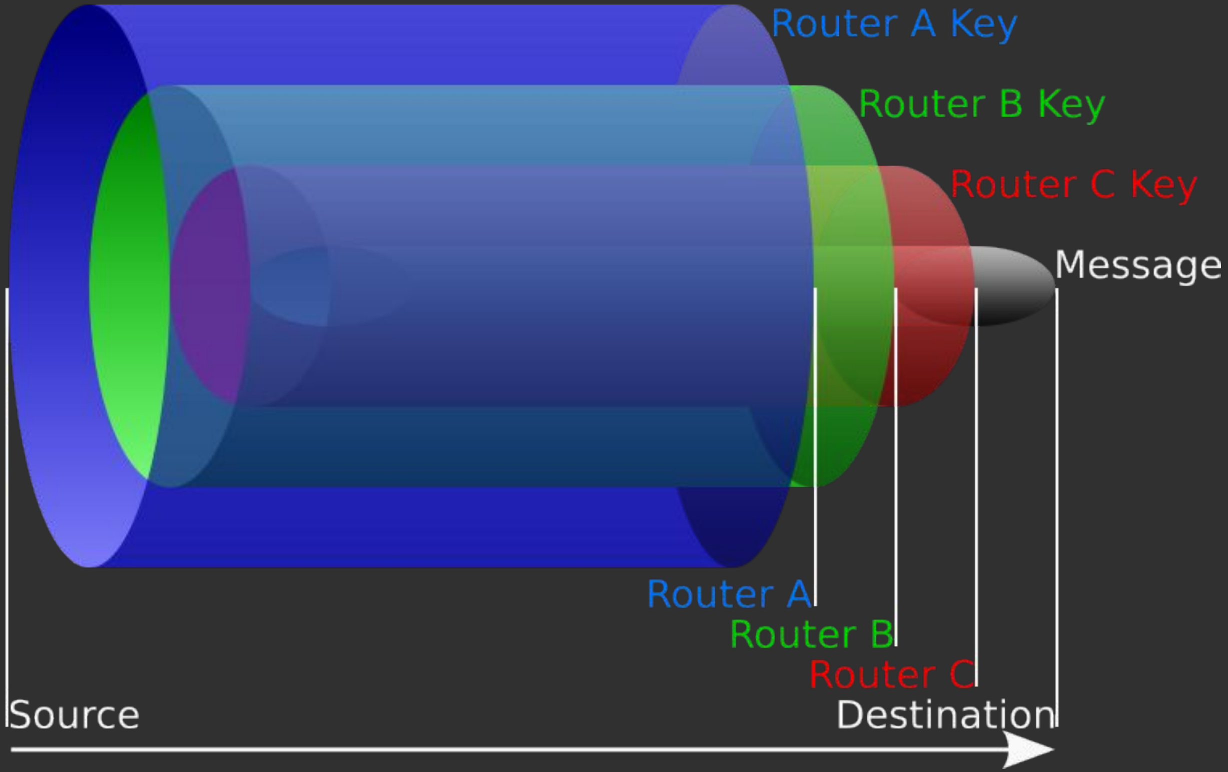
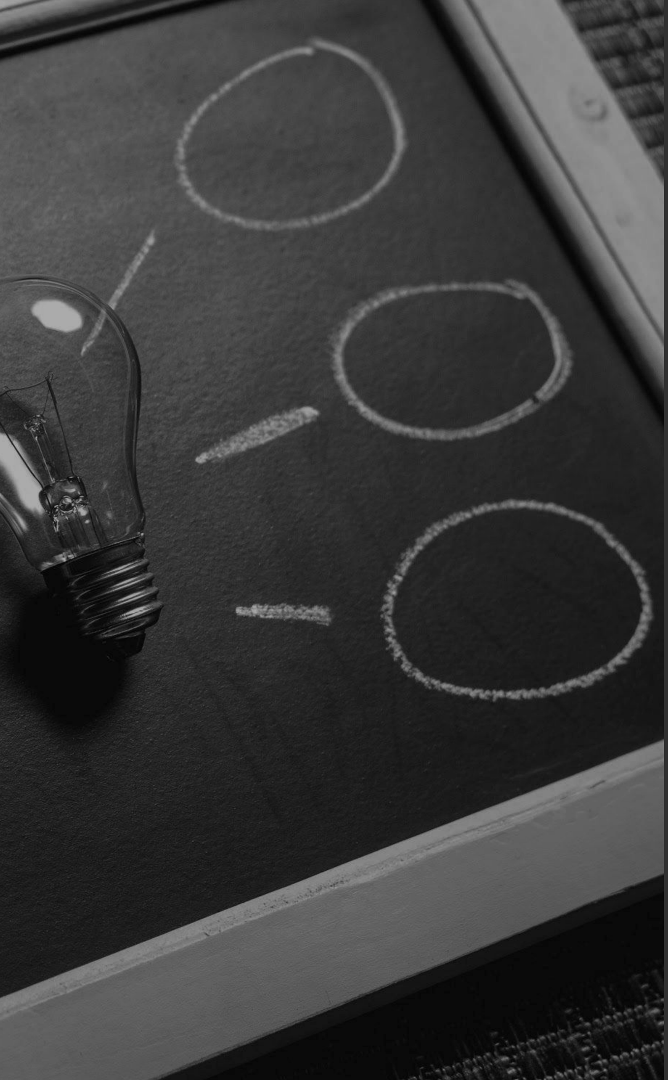


Image source: wikipedia.org - HANtwister (CC BY-SA 3.0)

Current state?

Lightning Protocol 1.0

BOLDARE



Implementations

- LND (Go)
- eclair (Scala)
- c-lightning (C)

Bitcoin Mainnet

It’s not just Bitcoin-limited

tomasz.konieczny@boldare.com

BOLDARE