Nexa Center for Internet & Society
Politecnico di Torino

Blockchain: features and scalability

Marco Conoscenti
PhD student

Outline

- The Bitcoin blockchain features
- Demystyfication
- Our research on Lightning Network

THE BITCOIN BLOCKCHAIN

Definitions - Bitcoin

Bitcoin is a decentralized crypto currency

Decentralized:
operated by a peer-to-peer network

Crypto:
created and controlled by cryptography

Definitions - Blockchain

The ledger storing all Bitcoin transactions

How to build a cryptocurrency system?

Cryptocoin version 0

- A trusted central entity creates cryptocoins
- It gives 1 cryptocoin to Alice
- Alice can transfer this cryptocoin to Bob
- Double-spending problem: Alice can transfer the same cryptocoin to Carol

Cryptocoin version 1

- A trusted central entity creates cryptocoins
- A trusted central entity registers all cryptocoin transfers in a public ledger
- Centralization problem:
  - Censorship
  - Single point of failure
  - Uncontrolled creation of coins

Bitcoin

- Bitcoin achieves decentralization
  - Each peer has a copy of the ledger
  - Each peer validates new transactions
  - Each peer inserts new transactions
  - Each peer creates new coins
- Bitcoin uses a distributed consensus protocol

Distributed consensus protocol

- Having more copies of the ledger, it ensures that
  - All peers agree on the same version of the ledger
  - The ledger stores only valid transactions

Distributed consensus before Bitcoin

- Distributed consensus is possible only if at most N nodes are faulty/malicious
- Sybil attack problem

Sybil attack

An attacker creates nodes which seem different but are all under his control

Distributed consensus before Bitcoin

- Distributed consensus is possible only if at most N nodes are faulty/malicious
- Sybil attack problem
  - An attacker can create more than N faulty/malicious nodes
- Only solution is to identify and trust nodes

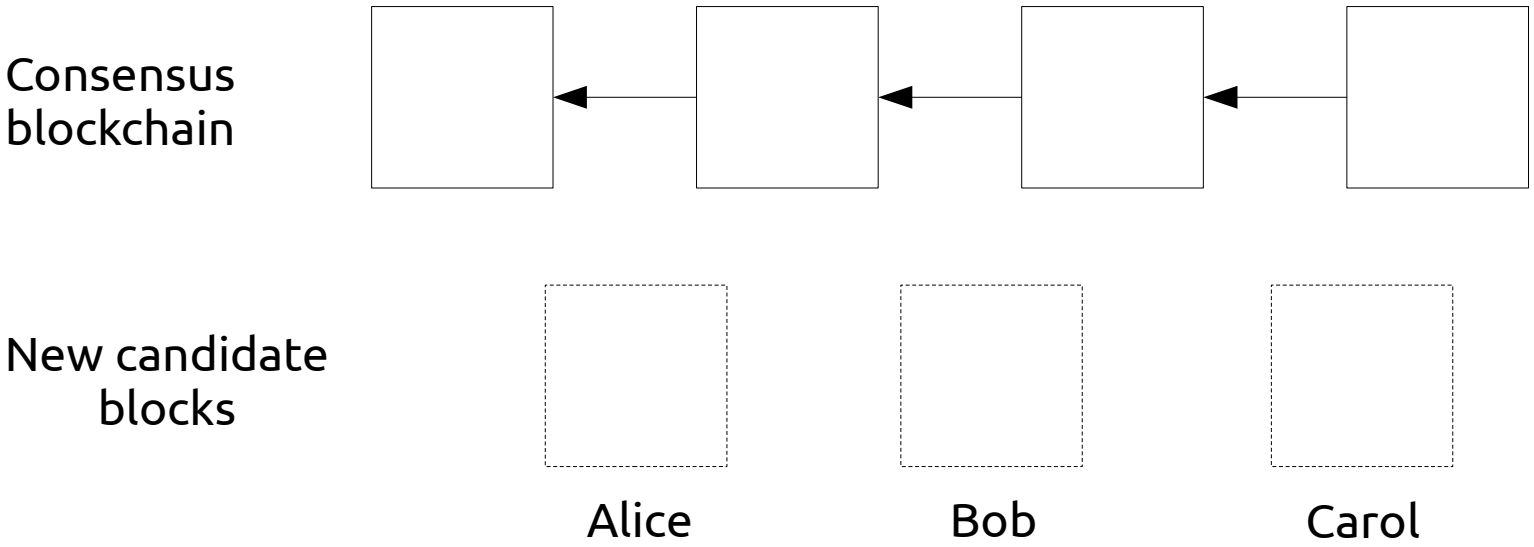
The key novelty in Bitcoin

A distributed consensus protocol which works in
a public environment,
without identifying and trusting peers

Bitcoin protocol

- New transactions are broadcasted to the peers
- Each peer assembles a block
- One of the blocks is selected and added to the blockchain

Bitcoin protocol – Block selection



The block of the peer which first solves a crypto-puzzle is selected

Proof of Work

- Difficult to compute
- Probability that a peer inserts a block is proportional to its computational power
  - Computational power cannot be monopolized
- Resistant to Sybil attack

Economic incentives

To incentivize peers to produce blocks with valid transactions

DEMYSTIFICATION

Truths

“Private/permissioned blockchains” are just distributed databases

Truths

Blockchains need cryptocurrencies

OUR RESEARCH

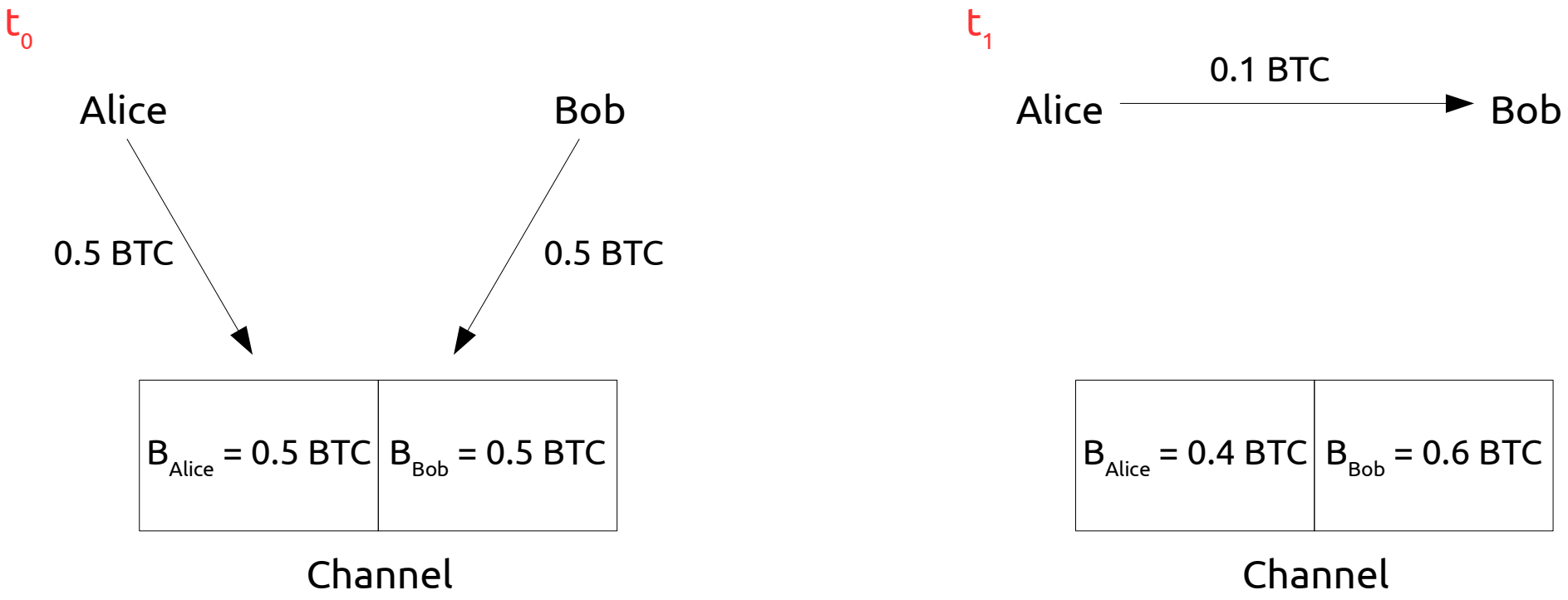
Scalability problem

- Blockchain growth is limited by design
- The Bitcoin blockchain only supports 7 transactions per second
- Two categories of solutions
  - Remove the limit
  - Off-chain scaling solutions

Off-chain scaling solutions

- Off-chain scaling solutions allow off-chain transactions
- Off-chain solutions use
  - Payment channel: a direct payment channel among two parties whereby they transact off-chain
  - Payment network: more payment channels connected together

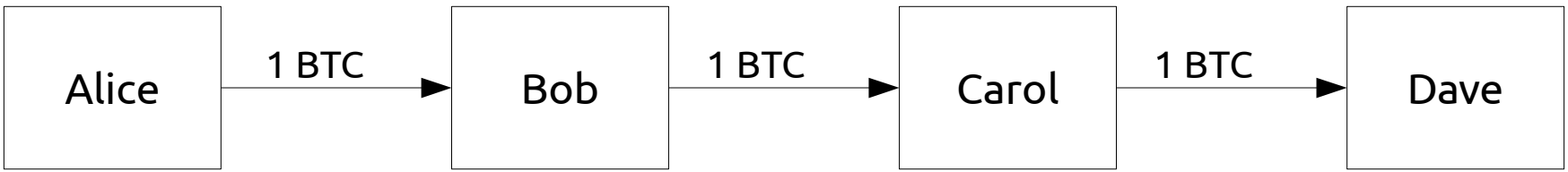
Payment channel example



The Lightning Network

The implementation of payment channels and payment network for Bitcoin

The Lightning Network



- Routing constraint: channel capacity ≥ payment amount
- Funds in transfer are locked in all channels of the route

Research motivation

The Lightning Network may be unfeasible in a totally distributed topology

Research motivation

- To connect millions of peers, many channels per peer are needed
- Each peer must divide up its funds for each of its channels
- The result is channels with low capacity, unable to route payments

Research motivation

The typical peer churning in distributed networks causes economic damage due to locked funds

Research question

What is the performance of the Lightning Network w.r.t. different topologies?

Different levels of distribution of bitcoins
Different numbers of channels per peer

Research method

I developed a Lightning Network simulator in C

Simulations – Input parameters

- Number of peers
- Number of open channels per peers
- Gini coefficient
- Probability that peers go offline

Simulations – Performance measures

- Time to perform payments
- Fraction of failed payments
  - For no path
  - For not enough capacity
  - For non-cooperative peers

Simulations – Expected results

- With high number of channels per peer, many unviable routes
- Better performance with “hub&spoke” topology

References

- Bitcoin and Cryptocurrencies technology
- Bitcoin wiki
- “Private blockchain” is just a confusing name for a shared data base
- The Origins of the Blocksize Debate
- Understanding the Lightning Network
- Lightning network: will it save Bitcoin? Or break it?

THANK YOU