Nexa Center for Internet & Society
Politecnico di Torino

The Lightning Network: Capabilities and Limitations for Blockchain Scalability

Marco Conoscenti
Postdoctoral researcher in Computer Engineering

CrypTO Conference, Anywhere, 28 May 2021

Outline

- Bitcoin and scalability
- The Lightning Network
- My research
- Conclusions

BITCOIN AND SCALABILITY

Bitcoin is a decentralized crypto currency

The blockchain is a distributed public ledger which stores all the Bitcoin transactions

A distributed consensus protocol synchronizes the blockchain replicas

It is based on Proof of Work and economic incentives

It aims to ensure the decentralization of Bitcoin

The blockchain does not scale

Bitcoin can support at most 7 transactions per second

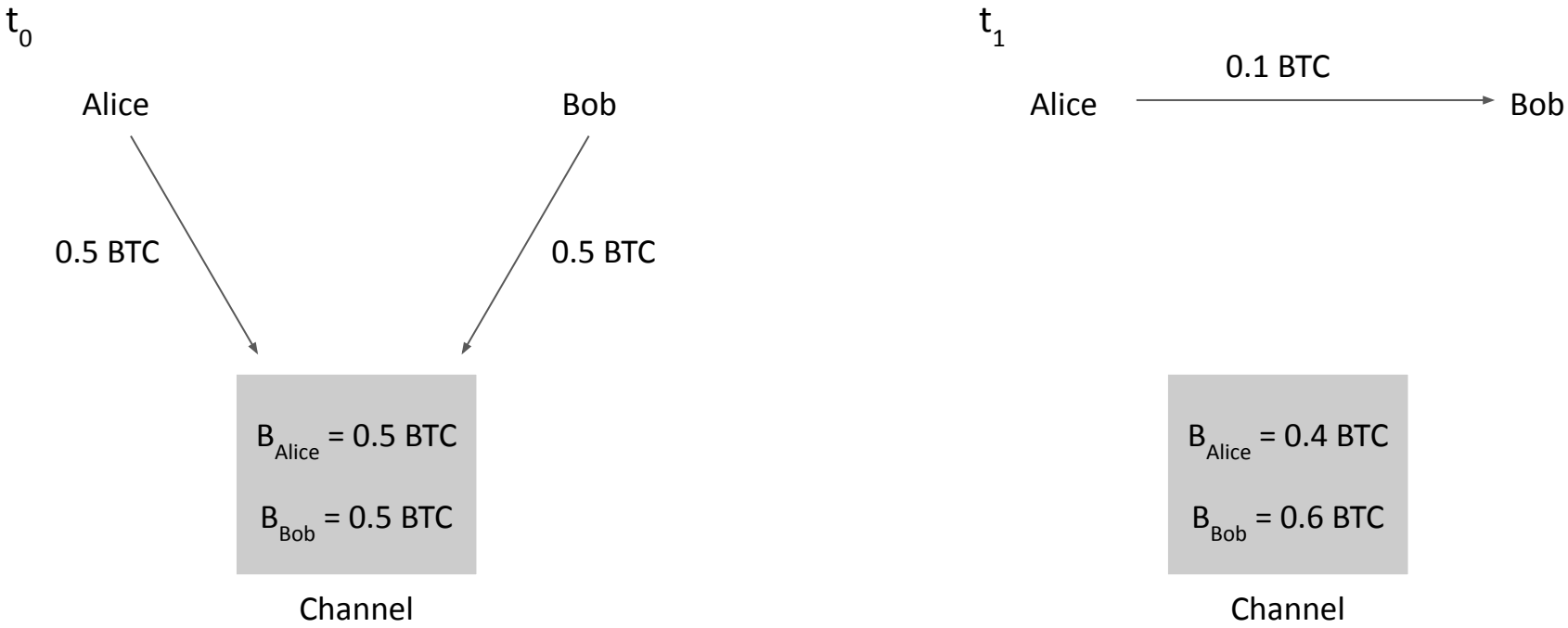
Blockchain growth is limited, to allow as many nodes as possible to store it

Payment channel networks are the most promising solution to the issue of scalability, as they preserve decentralization

Payment channel networks enable
off-chain payments

A payment channel is a channel between two parties whereby they transact off-chain

Payment Channel Example



A payment channel network is constituted by multiple linked payment channels

Payment Network Example

Alice

Bob

Carol

Dave

B_{Alice} = 0.5 BTC

B_{Bob} = 0.5 BTC

Channel

B_{Bob} = 0.5 BTC

B_{Carol} = 0.5 BTC

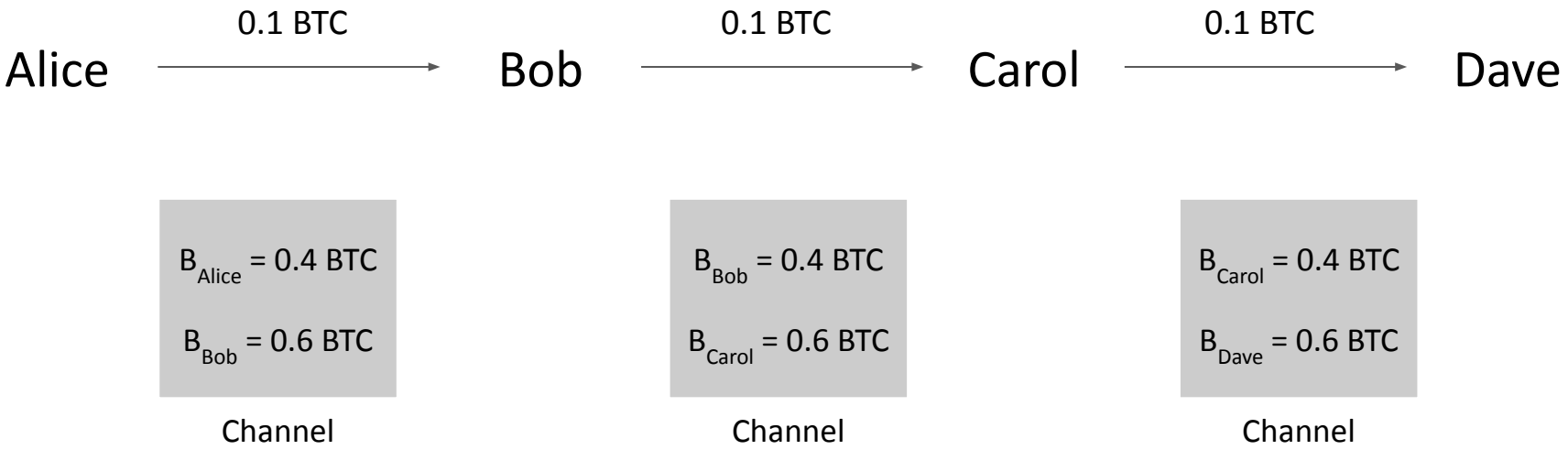
Channel

B_{Carol} = 0.5 BTC

B_{Dave} = 0.5 BTC

Channel

Payment Network Example



THE LIGHTNING NETWORK

The Lightning Network (LN) is the mainstream payment channel network, built for Bitcoin

The LN on May 27th, 2021

20K nodes

46K channels

1,300 BTC (~52M $)

https://1ml.com/

Payment Channel in LN

To open a payment channel in LN, Alice and Bob make a transaction in the Bitcoin blockchain.

The transaction contains the initial Alice and Bob balances.

After the transaction is confirmed, Alice and Bob can exchange off-chain payments by updating their balance state

To close the channel, Alice and Bob make a transaction in the blockchain

The transaction returns the final balances to Alice and Bob

The Lightning Network introduces the possibility of punishment

If Alice tries to steal money in the channel, Bob can take Alice's money

Punishment should guarantee
trustlessness

Punishment is not automatic:
Bob has to actively monitor the blockchain

Payment Network in LN

The Lightning Network allows the transfer of off-chain payments across multiple payment channels

The Lightning Network uses the Hashed Timelock Contract (HTLC)

The HTLC implements off-chain conditional payments in a payment channel

HTLC Example

If Bob shows a value R to Alice, Alice pays 0.1 BTC to Bob

If Bob does not show R within 24 hours, the payment does not occur

Money in an HTLC are locked until the payment succeeds or until the timeout expires

Alice

Bob

Carol

Dave

B_{Alice} = 0.5 BTC

B_{Bob} = 0.5 BTC

Channel

B_{Bob} = 0.5 BTC

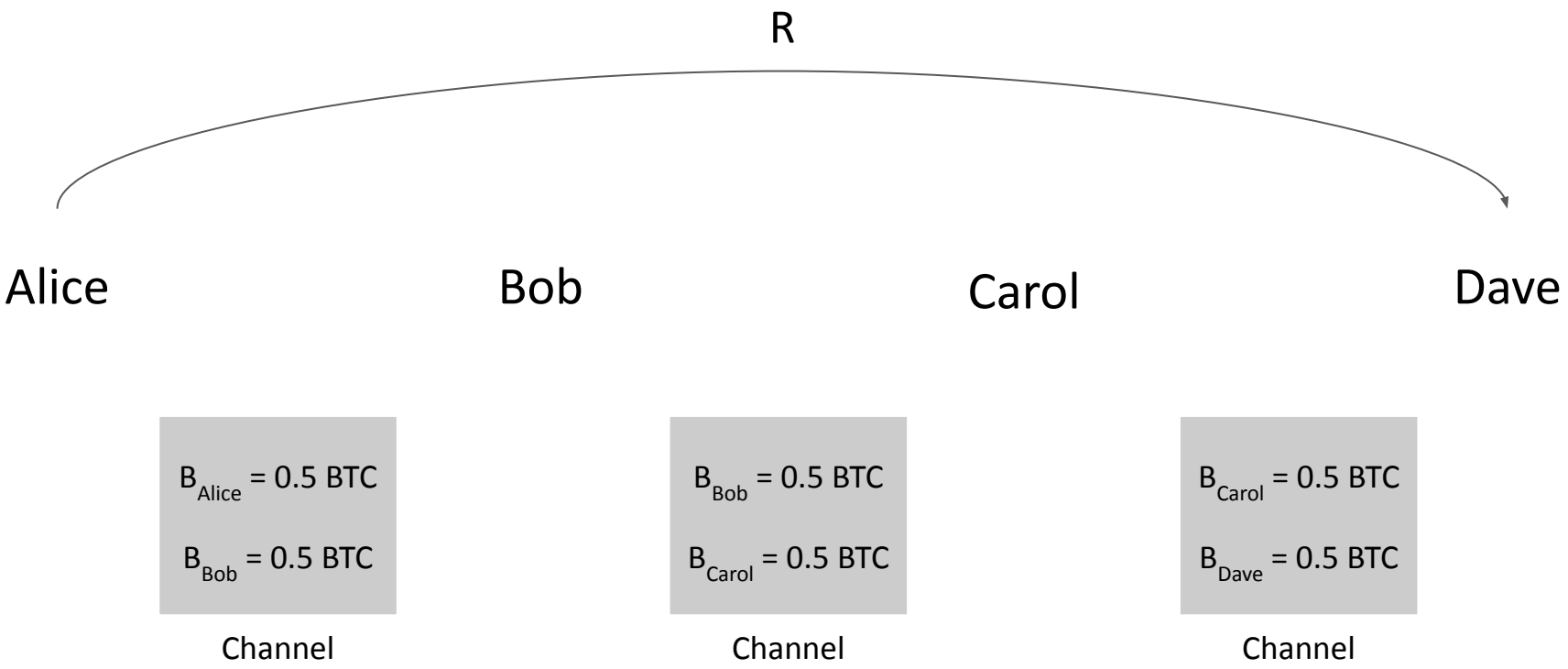
B_{Carol} = 0.5 BTC

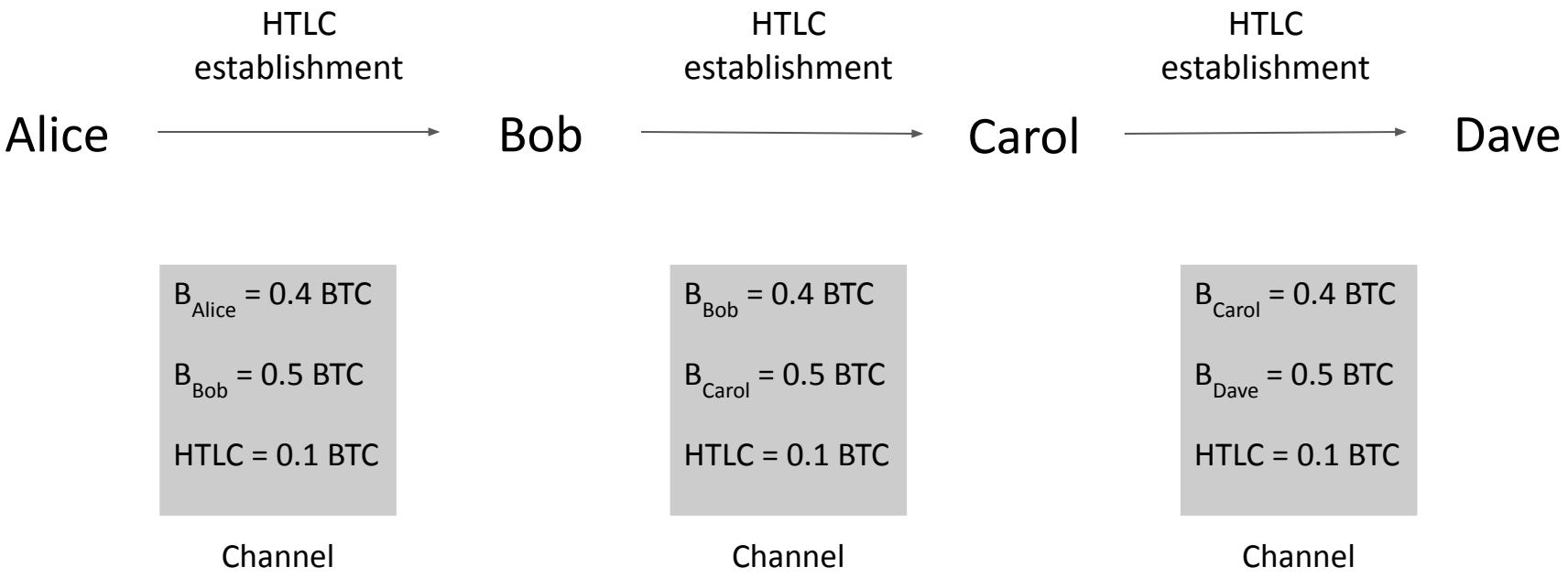
Channel

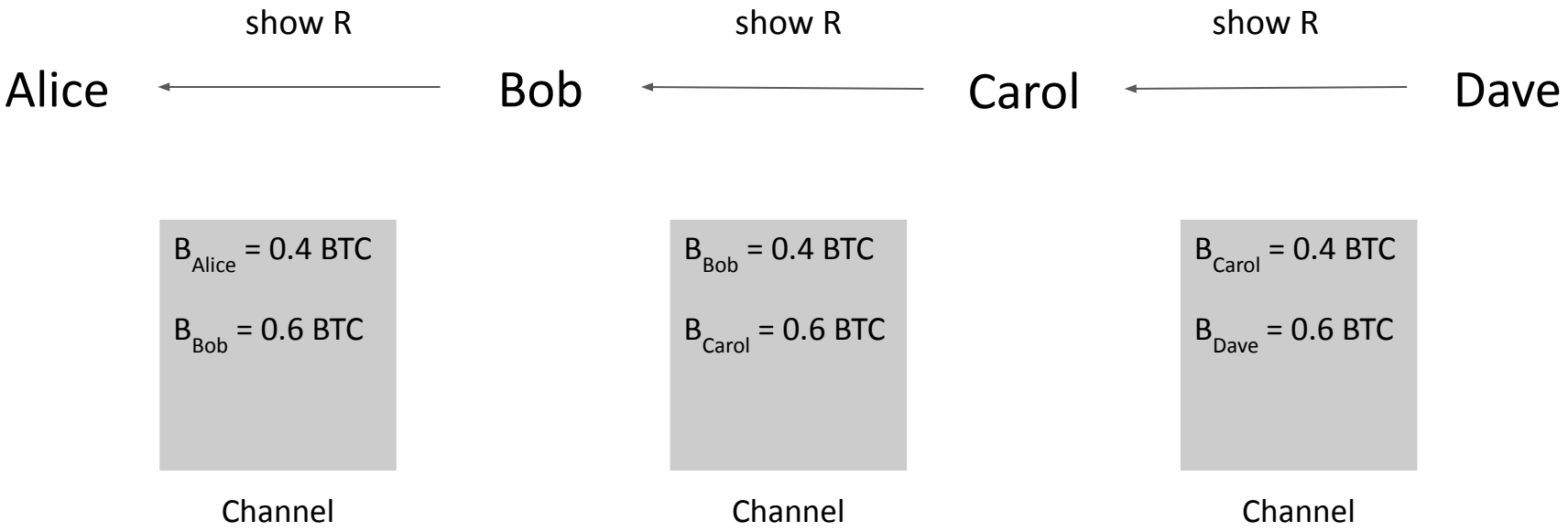
B_{Carol} = 0.5 BTC

B_{Dave} = 0.5 BTC

Channel


R
Alice
Bob
Carol
Dave
B_{Alice} = 0.5 BTC
B_{Bob} = 0.5 BTC
Channel
B_{Bob} = 0.5 BTC
B_{Carol} = 0.5 BTC
Channel
B_{Carol} = 0.5 BTC
B_{Dave} = 0.5 BTC
Channel


HTLC establishment
HTLC establishment
HTLC establishment
Alice
Bob
Carol
Dave
B_{Alice} = 0.4 BTC
B_{Bob} = 0.5 BTC
HTLC = 0.1 BTC
B_{Bob} = 0.4 BTC
B_{Carol} = 0.5 BTC
HTLC = 0.1 BTC
B_{Carol} = 0.4 BTC
B_{Dave} = 0.5 BTC
HTLC = 0.1 BTC
Channel
Channel
Channel


show R
show R
show R
Alice
Bob
Carol
Dave
B_{Alice} = 0.4 BTC
B_{Bob} = 0.6 BTC
B_{Bob} = 0.4 BTC
B_{Carol} = 0.6 BTC
B_{Carol} = 0.4 BTC
B_{Dave} = 0.6 BTC
Channel
Channel
Channel

The nodes apply fees to forward payments

Issues of the LN

- Routing
- Channel capacity limits payment amounts
- Channels are subject to unbalancing
- Faulty/malicious nodes cause lock of money

MY RESEARCH WORK

The research goal was to analyze capabilities and limitations of payment channel networks

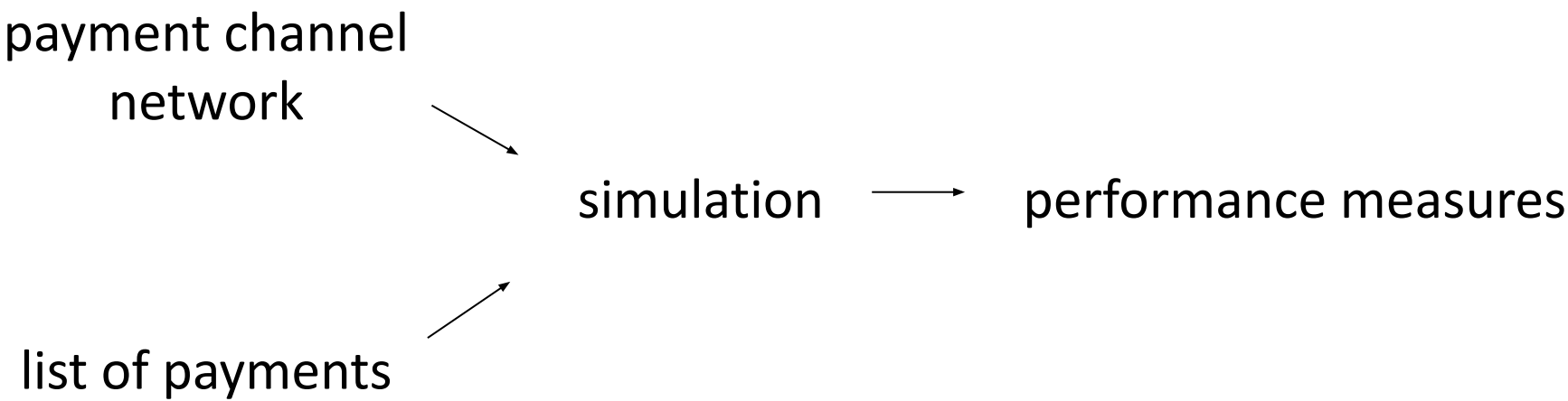
I developed CLoTH, a simulator of the Lightning Network

CLoTH is public and usable by anyone:

https://github.com/marcono/cloth

CLoTH simulates payments on a payment channel network and produces performance measures

CLoTH Workflow



CLoTH is a faithful reproduction of the LN code functions, thus producing reliable results

CLoTH allows:

- identification of issues of payment channel networks
- test of protocol improvements
- simulations of attacks
- analysis of the payment channel networks evolution

Input Modes

1. A complete specification of each node, channel and payment
2. A few input parameters, used to generate nodes, channels and payments

Input Parameters

- Number of nodes and channels
- Faulty nodes probability
- Average channel capacity
- Payment amounts
- Payment rate

Performance Measures

- Probability of payment success
- Probability of payment failure for no path
- Probability of payment failure for unbalancing
- Probability of payment failure for faulty nodes
- Payment complete time
- Number of payment attempts
- Payment route length

Simulations Done

- on the Lightning Network
- on synthetic networks
- on hubs, rebalancing and service providers in the Lightning Network

SIMULATIONS ON THE LN

A snapshot of the LN (December 2020) was given in input to CLoTH to study the LN performance

Success probability is 74% when payment amounts are ~10K satoshis

Payments fail because of insufficient channel capacity and unbalancing

It increases to 82% when large payments are split in smaller ones (Multi-Path-Payment)

SIMULATIONS ON SYNTHETIC NETWORKS

Synthetic networks are networks generated by CLoTH using the simulator input parameters

Payments were simulated on synthetic networks

Main Findings

With 3 channels per node, the probability of success was ~60%

At least 5 channels per node are required to have an high probability of success

A probability of faulty nodes lower than 10%
did not cause significant payment failures

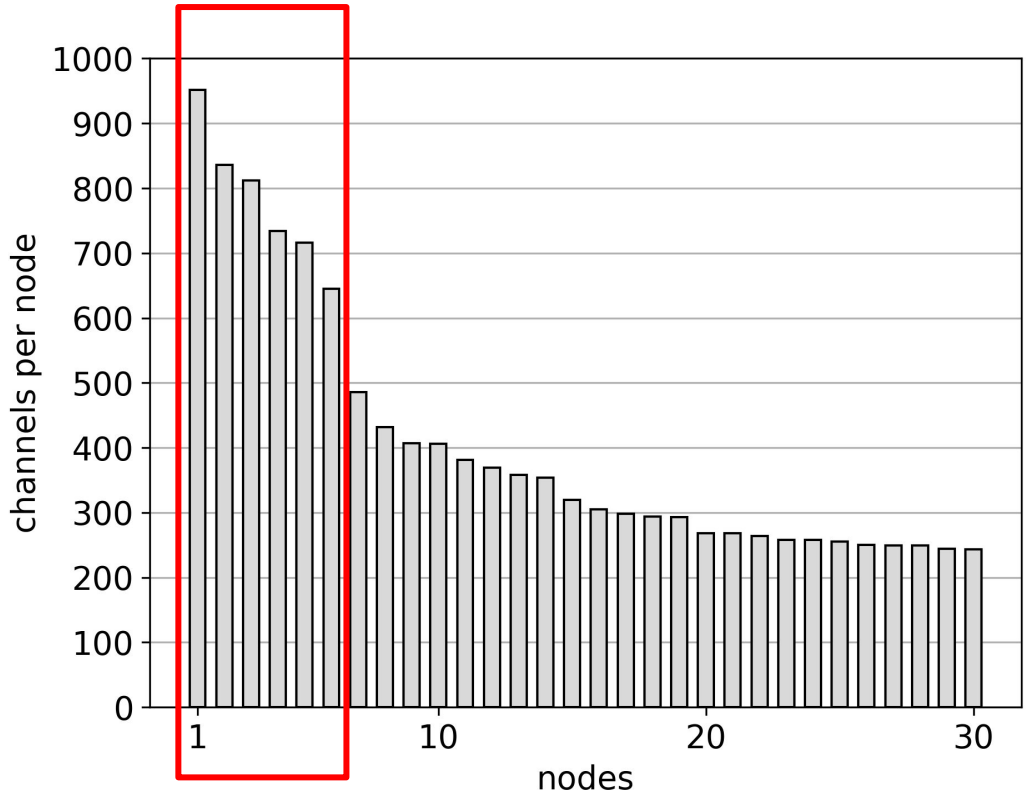
SIMULATIONS ON HUBS, REBALANCING APPROACHES AND SERVICE PROVIDERS

A snapshot of the Lightning Network (February 2019) was given in input to CLoTH

The simulated payments ranging between 1 and 10K satoshis

Hubs

Hubs are nodes having an high number of channels


1000
900
800
700
600
500
400
300
200
100
0
channels per node
1
10
20
30
nodes

Hubs were removed one by one and the resulting networks without hubs were given in input to CLoTH

Finding

Payment success probability remained constant when removing hubs

Rebalancing Approaches

I designed and implemented two rebalancing approaches: active rebalancing and passive rebalancing

Active rebalancing: a node executes a self-payment to rebalance its own channels

Passive rebalancing: fees are kept inversely proportional to channel balances

Active rebalancing did not improve performance

Passive rebalancing reduced by one fourth the failures for unbalancing

Service-Providers Scenario

A typical case of use of the LN in which most of the payments are directed to a few service-providers node

Channels directing to the service providers unbalanced: 26% of payments failed for unbalancing

CONCLUSIONS AND FUTURE WORK

LN Strengthens

The Lightning Network can support a contained level of faulty nodes probability (not higher than 10%)

The Lightning Network is resilient to the removal of six hubs (~20% of channels)

LN Weaknesses

Channel capacities strictly limit payment amounts

Payment success was lower than 90% when the highest payments are ~10K satoshis

Channels unbalance
(especially in the service-providers scenario)

Possible solutions are channel rebalancing strategies

The passive rebalancing approach effectively tackles channel unbalancing

Concluding remarks

The Lightning Network is at an early stage

The Lightning Network is not completely trustless

Irrational actors can cause serious damages to the network

In my opinion, the Lightning Network will not replace well-established payment systems

It may be useful for micropayments with minimal fees

THANK YOU

marco.conoscenti@polito.it