Nexa Center for Internet & Society
Politecnico di Torino

Capabilities and Limitations of Payment Channel Networks for Blockchain Scalability

PhD Candidate: Marco Conoscenti

Supervisor: Prof. Juan Carlos De Martin
PhD course: Control and Computer Engineering, XXXI cycle

Outline

- The context
- Research goal
- Research method: the CLoTH simulator
- Simulation Results
- Conclusions and future work

THE CONTEXT

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

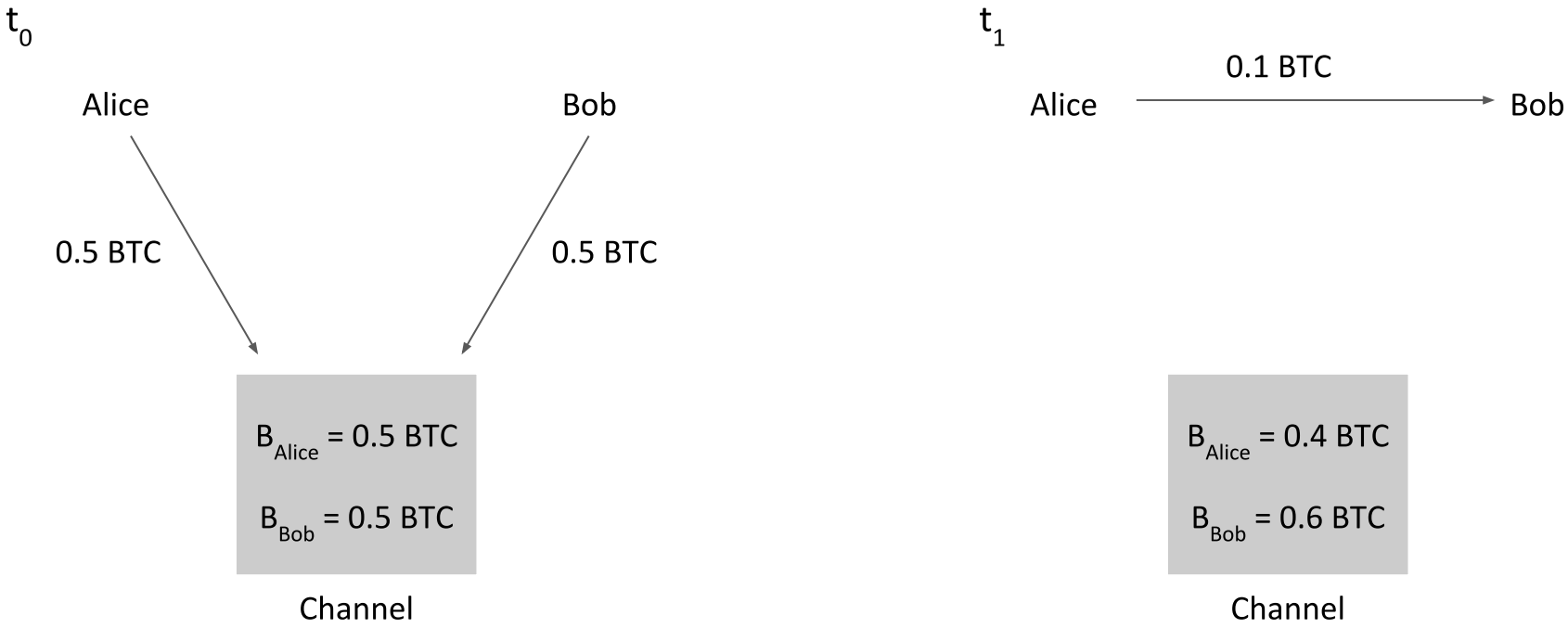
To keep Bitcoin decentralized, blockchain growth is limited
(7 transactions per second)

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

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

The LN on October 15th, 2019

4,345 nodes

30,624 channels

817.78 BTC (~6M $)

https://explorer.acinq.co/?utm_source=bitcoiner.today

The Lightning Network uses the Hashed Timelock Contract (HTLC) to transfer off-chain payments in a trustless way

Funds in transfer are locked until the payment succeeds or until a timeout expires

Issues of the LN

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

RESEARCH GOAL

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

The simulation was adopted as research method

CLoTH was developed, a simulator of HTLC payment channel networks

Research Questions

RQ1: Which are the non-operative cases of the Lightning Network?

RQ2: Which is the impact of the simulator input parameters on performance of payment channel networks?

RQ3: How do network and protocol modifications affect performance of the Lightning Network?

Simulations

- on the Lightning Network
- on synthetic networks
- on network and protocol modifications in the Lightning Network

THE CLoTH SIMULATOR

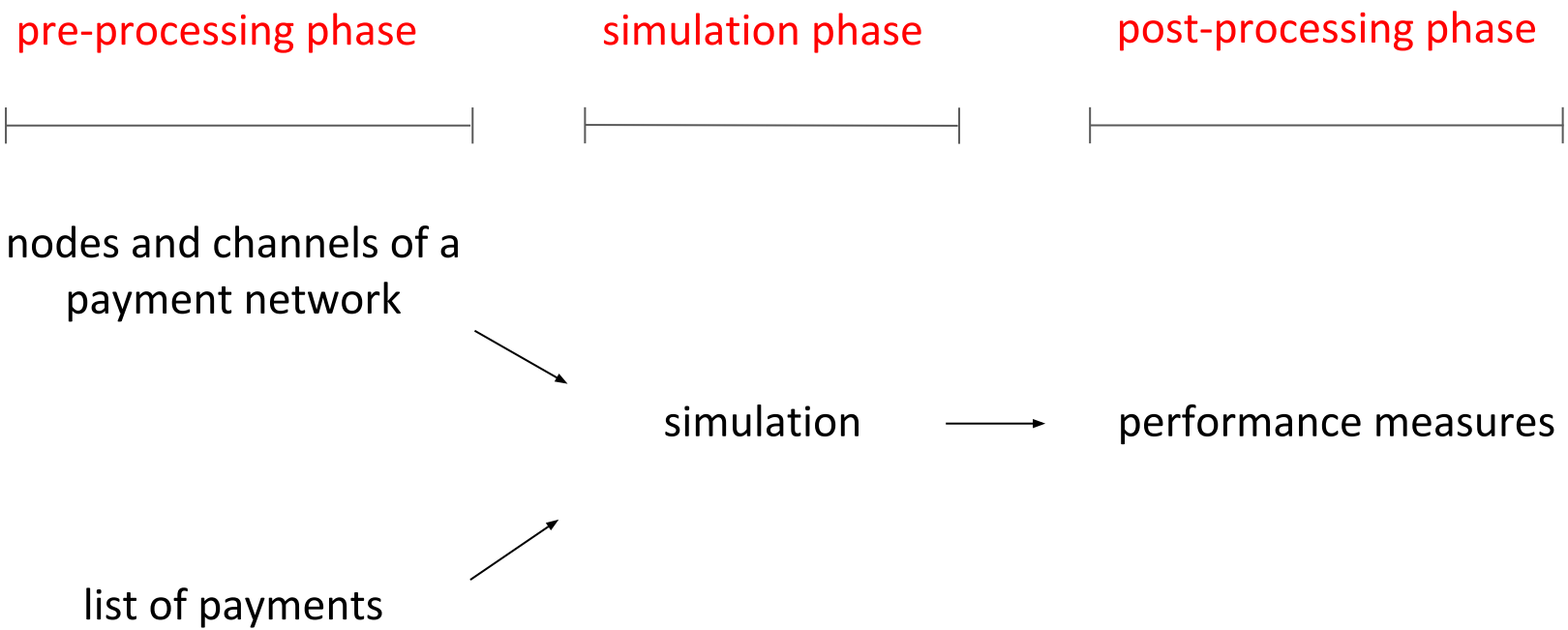
CLoTH is a discrete-event simulator written in C (~3,000 lines of code)

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

CLoTH is a precise mapping of the LN code functions

CLoTH allows systematic analyses of payment channel networks

CLoTH Workflow



Pre-Processing Phase

Input Modes

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

Network Input Parameters

- Number of nodes
- Average number of channels per node
- Network topology
- Uncooperative nodes probability
- Average channel capacity
- Gini index of channel capacity

Payment Input Parameters

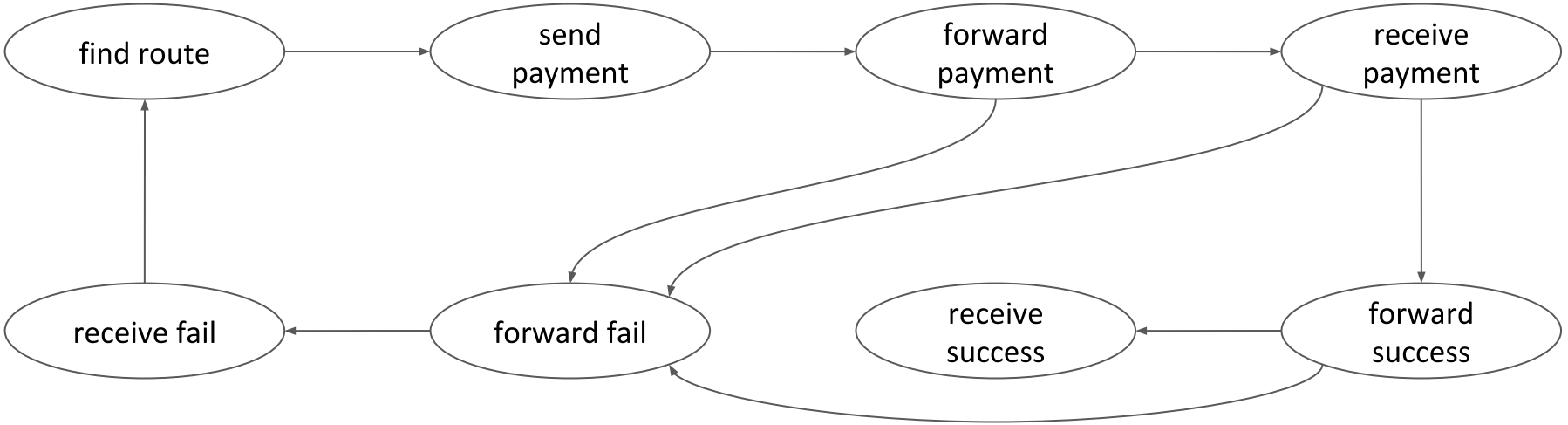
- Payment rate
- Payment amounts distribution
- Fraction of same-recipient payments

Simulation Phase

CLoTH simulates the execution of the input payments on the input network

A discrete-event simulation is run: events represent the flow of payments

CLoTH Event State Diagram



Post-Processing Phase

The performance measures are generated using the batch means method

Mean, variance and confidence intervals of the performance measures are computed

Performance Measures

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

SIMULATIONS ON THE LN

RQ1: Which are the non-operative cases of the Lightning Network?

The Lightning Network is defined as non-operative when the probability of payment success is below 50%

Simulation Design

A snapshot of the Lightning Network (June 2018) was given in input to CLoTH

The snapshot was constituted by

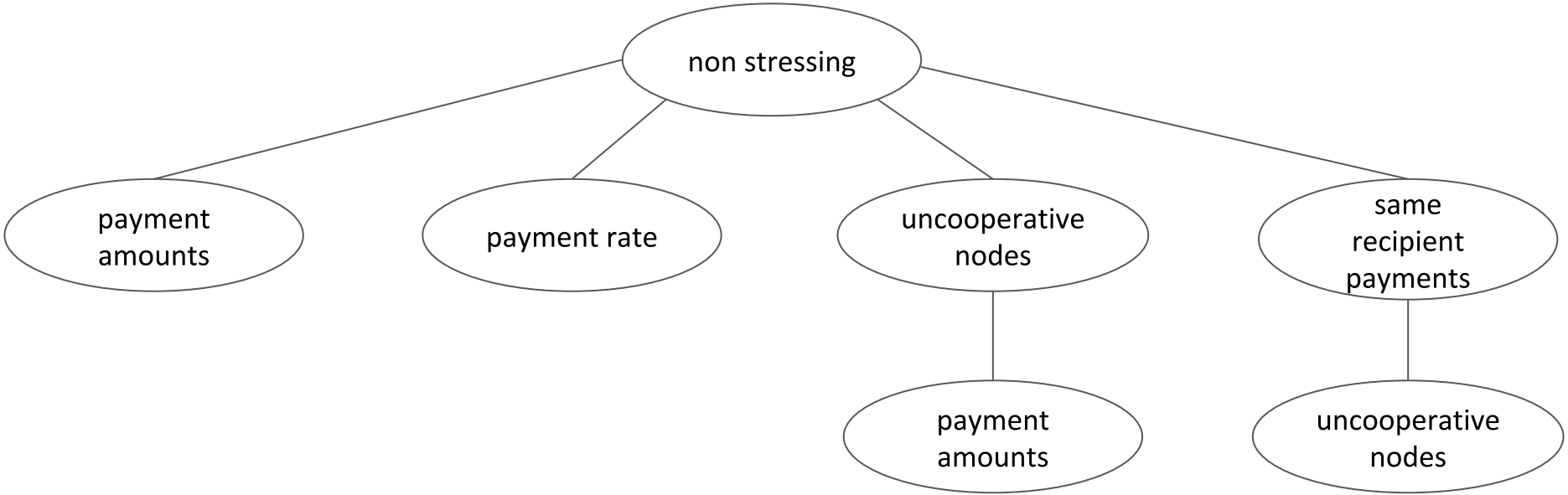
- 1,221 nodes
- 5,167 channels
- 318 satoshis as average channel capacity

Independent Variables

- Payment rate
- Payment amounts
- Fraction of same-recipient payments
- Probability of uncooperative nodes

For each independent variable, a stressing and non-stressing values were defined

Branch-And-Bound Simulation Strategy



Main Simulation Results

Payment Amounts

σ_a	P_s	P_{fr}	P_{fb}
5	46.13%	46.11%	7.72%

σ_a distribution of payment amounts

P_s probability of success

P_{fr} probability of failure for no route

P_{fb} probability of failure for unbalancing

Payment Rate

r_π	P_s	P_{fr}	P_{fb}
100 p/s	46.88%	25.17%	30.92%

r_π payment rate
P_s probability of success
P_{fr} probability of failure for no route
P_{fb} probability of failure for unbalancing

Payment Amounts + Uncooperative

σ_a	P_u	P_s	P_{fr}	P_{fb}	P_{fu}
4	10%	38.27%	46.10%	6.47%	9.13%

σ_a distribution of payment amounts
P_u probability of uncooperative nodes
P_s probability of success
P_{fr} probability of failure for no route
P_{fb} probability of failure for unbalancing
P_{fu} probability of failure for uncooperative nodes

Main Findings

- The main reasons of payment failures are the limited channel capacities and channel unbalancing
- Uncooperative nodes do not cause significant failures

SIMULATIONS ON SYNTHETIC NETWORKS

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

RQ2: Which is the impact of the simulator input parameters on performance of payment channel networks?

Simulation Design

The independent variables of these simulations were all the simulator input parameters

For each variable an interval was defined

One independent variable at a time
was varied within its interval

Main Simulation Results

Number of Channels

N_{ch}	P_s	P_{fr}	P_{fb}
3	59.61%	23.34%	16.77%
5	99.34%	0.31%	0.13%
8	99.82%	0.01%	0.0%
11	99.86%	0.0%	0.0%

N_{ch} channels per node
P_s probability of success
P_{fr} probability of failure for no route
P_{fb} probability of failure for unbalancing

Uncooperative Probability

P_u	P_s	P_{fu}
0.1%	99.27%	0.1%
1%	98.32%	1.04%
10%	87.47%	11.84%

P_u probability of uncooperative nodes

P_s probability of success

P_{fu} probability of failure for uncooperative nodes

Network Topology

N_h	P_s	L_r
1	99.88%	2.90
~5	99.85%	4.13
~20	99.83%	5.56
0	99.34%	10.34

N_h number of hubs
P_s probability of success
L_r length of payment route

Payment Amounts

σ_a	P_s	P_{fr}	P_{fb}
1	99.34%	0.31%	0.13%
2	99.13%	0.48%	0.19%
3	96.80%	2.30%	0.65%
4	93.69%	4.67%	1.33%
5	91.43%	6.40%	1.85%

σ_a distribution of payment amounts

P_s probability of success

P_{fr} probability of failure for no route

P_{fb} probability of failure for unbalancing

Main Findings

- Probability of success in the synthetic networks is high
- At least five channels per node are required to have 99% probability of success
- The higher the payment amounts, the higher the failures for no route and for unbalancing
- Uncooperative nodes do not constitute a serious issue

SIMULATIONS ON NETWORK AND PROTOCOL MODIFICATIONS

RQ3: How do network and protocol modifications affect performance of the Lightning Network?

The protocol modifications analyzed were rebalancing approaches

The network modifications were: removal of hubs and service-provider scenario

Simulation Design

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

The snapshot was constituted by

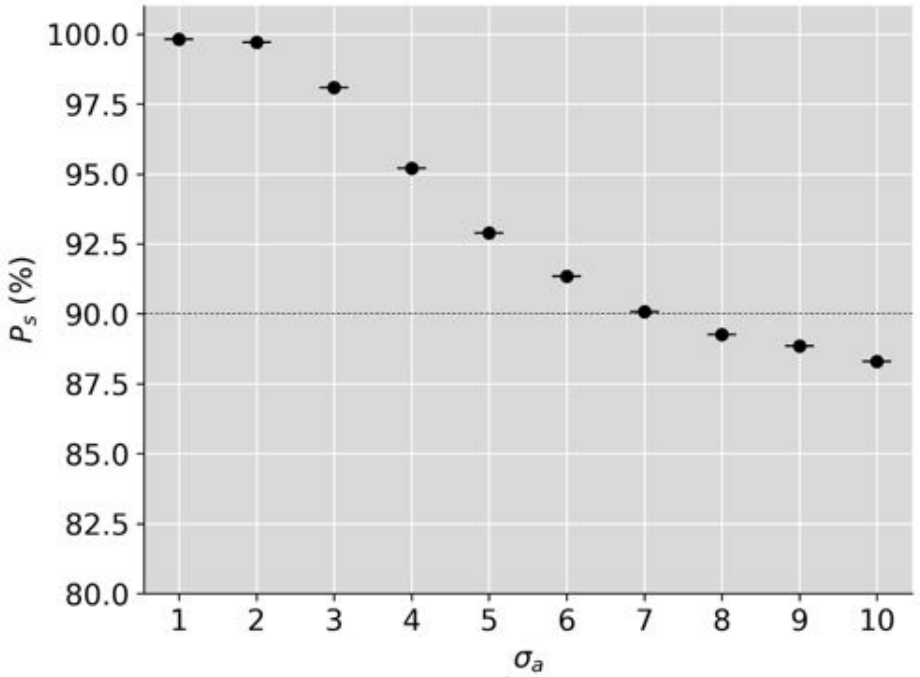
- 3,148 nodes
- 24,683 channels
- 2.67 millions of satoshis as average channel capacity

The independent variable was the distribution of payment amounts

Payment amounts range between 1 and 10K satoshis

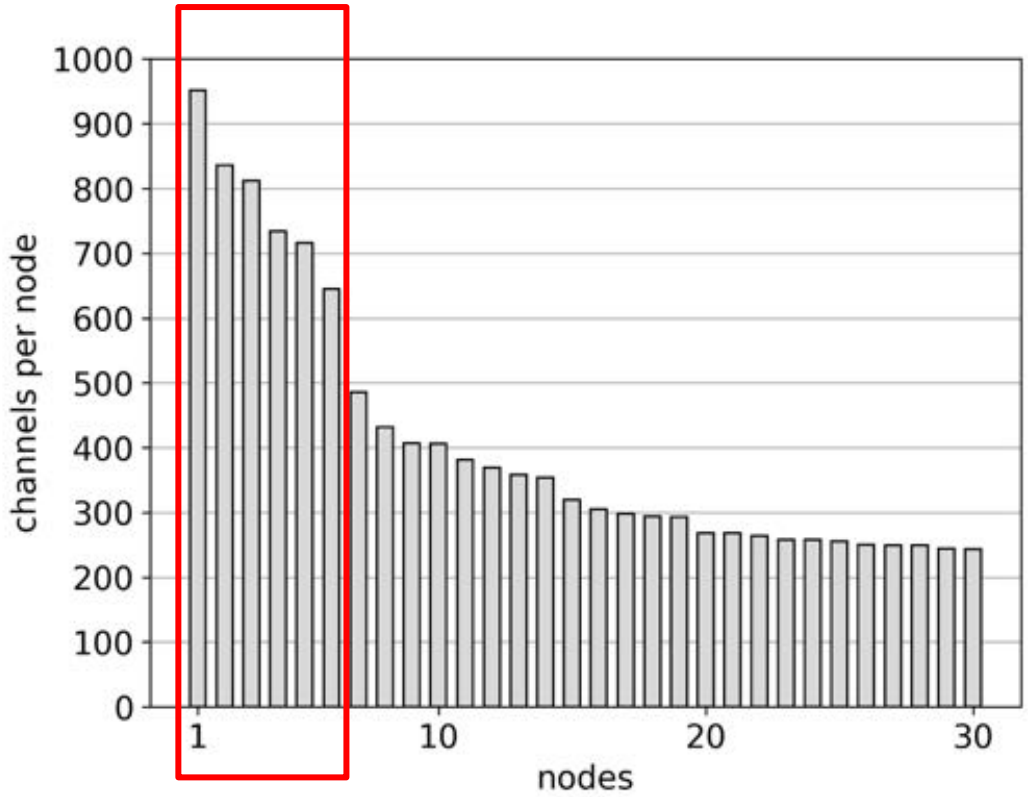
Preliminary simulations were performed to define the distribution of payment amounts

Payment Amounts in the LN



Hubs

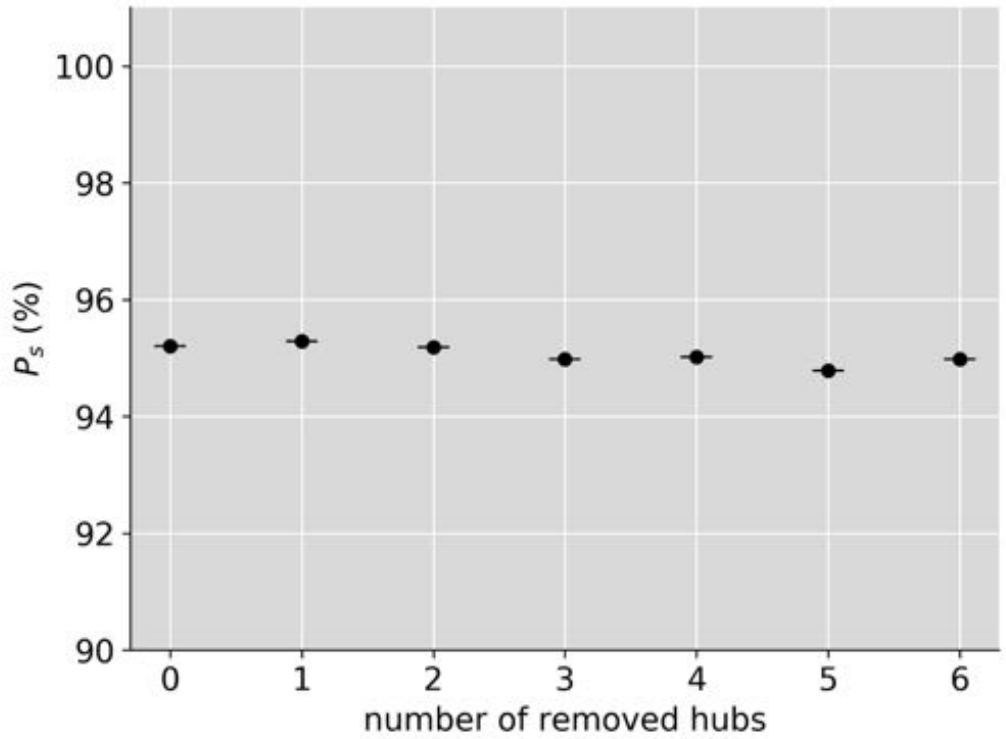
Hubs were chosen according to their number of channels


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

Payment amount distribution was fixed to an intermediate value

Removal of Hubs



Rebalancing Approaches

Two rebalancing approaches were designed: active rebalancing and passive rebalancing

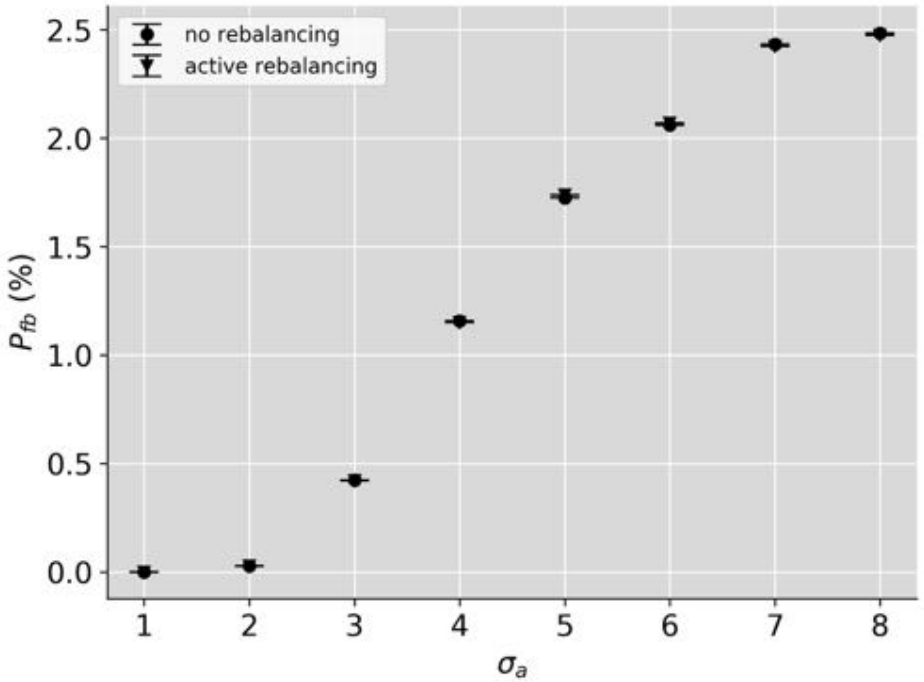
Active rebalancing: a node executes a self-payment to rebalance its own channels

Passive rebalancing: fees are kept inversely proportional to channel balances

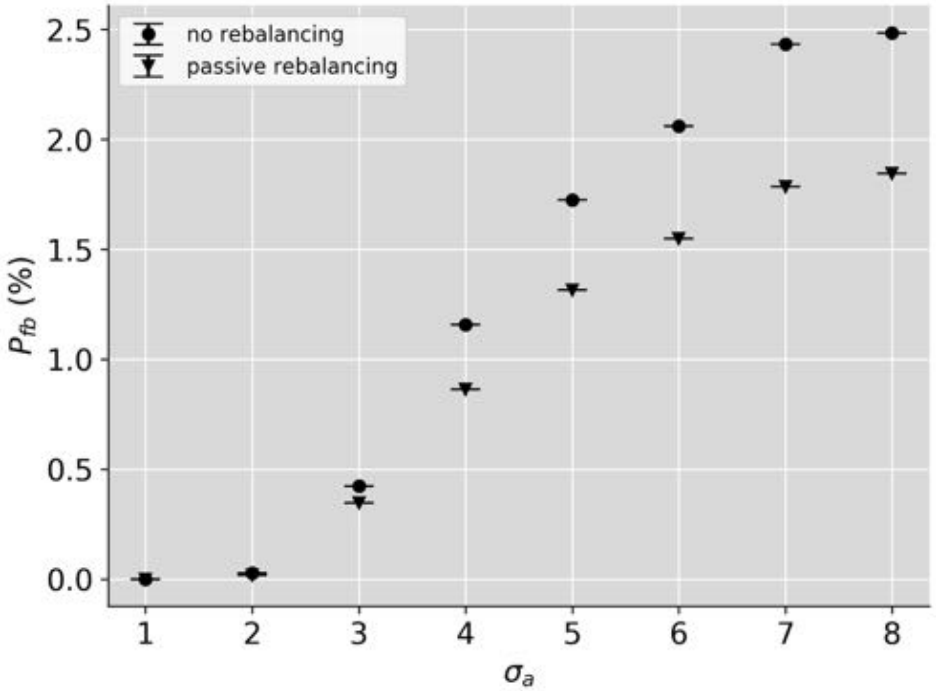
The approaches were implemented in CLoTH

Simulations were performed varying payment amounts

Active Rebalancing



Passive Rebalancing



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

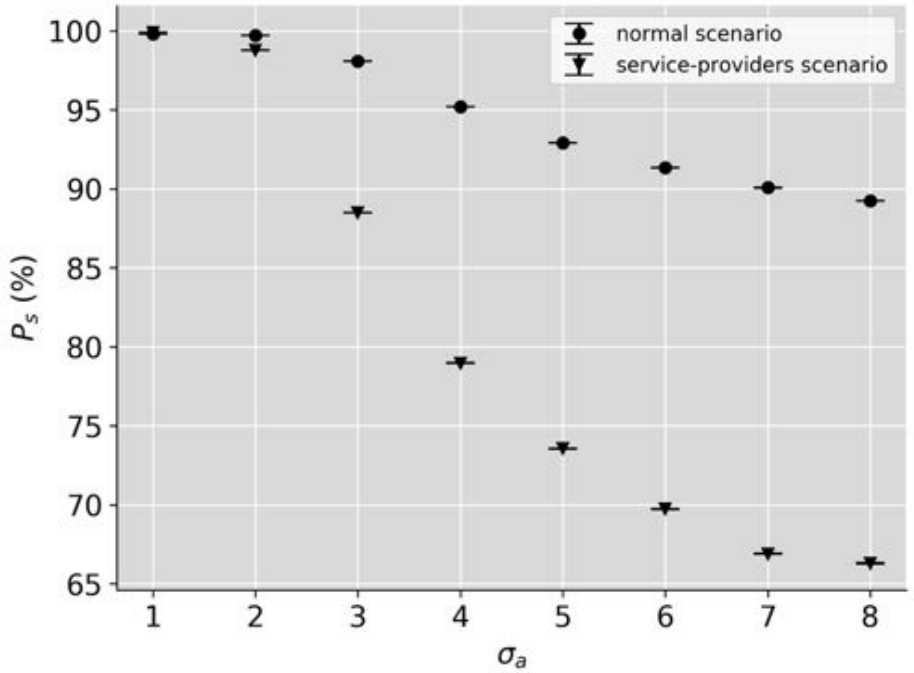
The Lightning Network nodes were divided into three classes:

- 188 service providers
- 1,781 payers
- 1,179 hybrid

The LN with the classes of nodes was given in input to CLoTH

Simulations were performed varying payment amounts

Service-Providers Scenario



Main Findings

- The LN is resilient to the removal of hubs
- In the service-providers scenario, channel unbalancing produces significant payment failures
- The passive rebalancing approach constitutes a promising solution to channel unbalancing

CONCLUSIONS AND FUTURE WORK

LN Strengthens

The Lightning Network can support a contained level of uncooperative 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

A possible solution is to split large payments into small ones

Channels unbalance
(especially in the service-providers scenario)

Possible solutions are channel rebalancing strategies

The passive rebalancing approach effectively tackles channel unbalancing

The most important contribution is CLoTH, a valuable tool for supporting the development of payment channel networks

Future Work

- Analyses of new protocol improvements
- Investigation on the LN central nodes
- Simulation of attack scenarios
- Implementation of the blockchain in the simulator

The Lightning Network is at an early stage

The Lightning Network is not completely trustless

The Lightning Network will not replace well-established payment systems

It may be useful for micropayments with minimal fees

THANK YOU