POLITECNICO DI TORINO

Dipartimento di Automatica e Informatica

PhD in Computer and Control Engineering

XXXI cycle

Supervisor

Prof. Juan Carlos De Martin

Scaling Solutions for the Blockchain

PhD Candidate: *Marco Conoscenti*

1. Context

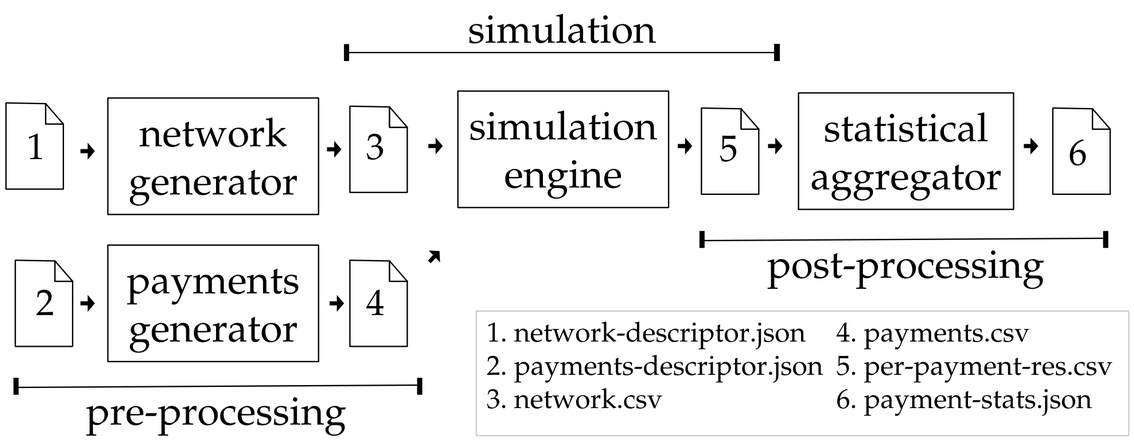
The Bitcoin blockchain is affected by a well-known **scalability problem**: it supports only 7 transactions per second [1]. **Off-chain scaling solutions** aim to address the scalability problem by building a **payment network**, i.e., a network of payment channels where to route off-blockchain payments, not subject to the scalability limit.

2. Goal

The main goal of the PhD research project is to analyze the performance of the scaling solutions. In fact, the **Lightning Network** – that is the mainstream payment network for Bitcoin – presents problems which might prevent it from becoming a healthy payment system: the payment amount is constrained by the economic capacity of payment channels; channels capacities are subject to depletion; uncooperative peers may cause payment failures.

3. The CLoTH Simulator

I developed CLoTH, **the first simulator for payment networks** [2]. CLoTH allows to analyze problems of payment networks and to estimate the effect of optimization actions.



The simulator takes as input parameters defining a payment network (e.g., number of peers and of payment channels) and payments (e.g., payment amounts). It runs a discrete-event simulation, executing the input payments on the input network. It produces payment-related performance measures, e.g., probability of payment success and payment complete time.

4. Main Simulation Results

I ran two groups of simulations:

1) Simulations on the Lightning Network, to **discover configurations in which a payment is more likely to fail than to succeed** on such network. As showed in the two tables below, two of such configurations occurred when the payments amount was of the order of 1$ and when the payment rate was 100 payments per second on average. To support such payments amount and such rate, **more and higher-capacity channels should be open.**

A	P_s	P_{fr}	P_{fc}
~1$	46.13%	46.11%	7.72%

R	P_s	P_{fr}	P_{fc}
100 pps	43.88%	25.17%	30.92%

A = payment amount; P_s = succeeded payments; P_{fr} = failed payments (no route); P_{fc} = failed payments (capacity depleted); R= payment rate.

2) Simulations on synthetic networks generated by the simulator, to estimate the impact on performance of each simulator input parameter. **I discovered network configurations that guarantee a good performance of payment networks**, such as the one showed in the table below.

N_{ch}	C_{ch}	P_s	T
5	1$	99.34%	1391.92 ms

N_{ch} = channels per peer; C_{ch} = channels capacity; P_s = succeeded payments; T = payment complete time.

5. References

[1] “Blockchain for the Internet of Things: a Systematic Literature Review”. Conoscenti M., Vetrò A., De Martin J.C. In Proceedings of the 13th IEEE/ACS International Conference of Computer Systems and Applications. 2016.

[2] “The CLoTH Simulator for HTLC Payment Networks with Introductory Lightning Network Performance Results”. Conoscenti M., Vetrò A., De Martin J.C., Spini F. In Information. 2018.