Responses to the Reviewers of the Thesis Titled: "Capabilities and Limitations of Payment Channel Networks for Blockchain Scalability"

Marco Conoscenti

The author wishes to thank the reviewers for their thoughtful and very helpful suggestions. The comments have been carefully read and the manuscript has been revised accordingly. The responses are given in a point-by-point manner below.

Reviewer: Prof. Guido Boella

Review Comment: The problem of scalability, that is the search for methods to radically increase the number of transactions per second permitted by the system, is a central research theme in the study of blockchain and Digital Ledger Technologies in general.

Increasing the transaction throughput of a blockchain system is a crucial step towards mass user adoption of the technology.

This is already true for the simplest application of blockchain technology that can be conceived, the transfer of blockchain native tokens between users, and the problem is even more acute in cases where complicated smart contracts might be involved.

A variety of approaches for increasing the transaction throughput and address the scalability problems of blockchain technology have been proposed, ranging from adjustments of blockchain parameters (reducing the block latency and increasing the block size), to the use of novel consensus algorithms, to more radical solutions like sharding. One of the most promising methods to address the problem of scalability for simple token transactions are payment channel networks. In particular the Lightning Network, connected to the Bitcoin blockchain, is the most mature of such implementations, based on the use of Hash-TimeLock Contracts (HTLC) to allow trustless transactions between nodes in the network that are not necessarily connected to each other.

The work presented in the thesis presents a comprehensive analysis of the Lightning Network in its present incarnation, identifies potential shortcomings and issues of the system and discusses possible solutions to identified problems.

The study is based on the use of a simulator of payment channel networks called CLoTH, that has been designed and developed (in C) by the candidate

(the entire code repository is freely available). The main strength of CLoTH, when compared to similar efforts, is that it faithfully maps all the function calls and features found the lnd, one of the official implementations of the BOLT standard for the Lightning Network development (author should motivate the choice of lnd w.r.t. other existing implementations like c-lightning or eclair). This means that simulations run with CLoTH can be interpreted as faithful representations of what would happen in the real implementation of the Lightning Network.

Response: The reason of choosing `lnd` as a reference implementation is that it is the most documented of the LN implementations in terms of comments to the code. This clarification was added also in Section 3.1 of the thesis.

Review Comment: The CLoTH simulator can be initialized either providing a set of defining parameters, which translates into a synthetic HTLC payment network with the specified characteristics, or by providing a snapshot of the network (for example a snapshot of the real Lightning Network mainnet). The latter method has been used in the work presented in Chapter 4 and Chapter 6, where reasons for payment failures are identified and the impact of selected modifications and proposed improvements to the present structure have been studied. The creation of synthetic networks with specified average properties has been used in Chapter 5, in order to study the impact of each parameter of the HTLC network on its performance and identify ideal working condition that would optimize the working of the real deployment. Regarding Chapter 6, it is not clear why the hubs of the network were chosen based on the number of channels instead of using a well-known centrality measure on graphs.

Response: According to the definition of hub in network science, a hub is a node characterized by a high degree, namely, a high number of connections. This is the reason why hubs were chosen based on their number of channels. This clarification was added in Section 6.2. However, it would be interesting to use graph centrality measures for analyzing the most central network nodes via simulations. This direction will be pursed by future work, as specified in Chapter 6.

Review Comment: Once a payment network is instantiated, a set of transactions is submitted and these are processed by the simulator in discrete time steps, simulating what would happen in the network in an interval of specified duration. The duration time of the simulation has been chosen to correspond to 15 minutes in real-time, in order to be able to neglect interactions with the underlying blockchain. The lack of implementation of the interaction with the blockchain is one of the weaknesses of the CLoTH simulator, it is clearly identified and discussed by the author and earmarked for future development.

The raw output of the simulation is a dataset comprising outcomes (success/failure) of the payments submitted and some of their properties (execution time, number of hops, retrials, etc.). The output data are aggregated

and the corresponding statistics are produced, in order to provide statistically sound testing of hypotheses formalized in the presented research questions. The methodology employed in the analysis is well described and sound.

One of the weakest points of the thesis is that the results of the simulations are presented without an associated uncertainty. This only makes a qualitative discussion of the results possible, whereas stating uncertainties would have made a more quantitative, statistically motivated discussion of the results possible.

Response: The uncertainties, in the form of confidence intervals of the simulation results, are present in the files of the simulation results uploaded online, as mentioned in Appendix B. In the revised version of the thesis, the confidence intervals are presented and discussed also in the main text, when relevant (for instance, see Table 5.10 and the figures of the simulation results in Chapter 6).

Review Comment: In general the work performed and presented by the candidate is of good quality and the thesis itself is well written and show a thorough understanding of the underlying technology, its possibilities and its limitations.

The studies performed are of interest and well designed and executed, with the only exception of the presentation of simulation results without uncertainties, which would have allowed a more quantitative discussion.

The CLoTH simulator and some results have been described in one peer-reviewed journal publication and one conference proceedings contribution, underlying the good quality and the recognition of the validity of the work.

Reviewer: Prof. Giorgio Ventre

Review Comment: The thesis focuses on payment channel networks, one of the most promising solution to the issue of blockchain scalability. Payment channel networks enable unbounded off-chain payments which do not need to be stored on the blockchain. Specifically, the work focuses on the Lightning Network, a payment channel network built on top of Bitcoin, which leverages HTLC contracts to transfer off-chain payments.

The author developed CLoTH, an HTLC payment network simulator. It is a discrete-event simulator which simulates the execution of payments on a payment channel network and produces payment-related performance measures, such as probability of payment failures and average payment complete time.

Three groups of simulations are discussed in the thesis. In the simulations of the first group, a snapshot of the Lightning Network is analyzed to find non-operative configurations of the network. In the second group, the simulator generates synthetic networks which are studied varying the simulator input parameters. The third group of simulations investigates some protocol and network modifications, such as hubs removal and channel rebalancing strategies. This evaluator believes that the effort done on simulations increases greatly the

value of the thesis work.

The research presented in the thesis is of great interest. In the last years the blockchain has gained increasing attention and is considered as a breakthrough technology which influences economical and social aspects. The most prominent experts of the crypto-community see the Lightning Network as the solution to the largely-debated issue of blockchain scalability. Therefore, it is paramount to conduct thorough scientific investigations on the Lightning Network and payment channel networks.

With this regard, the CLoTH simulator presented in this work is a valuable tool for systematically analyzing payment channel networks. The simulator maps the Lightning Network code functions, thus ensuring the validity of simulation results. The batch means analysis performed by CLoTH is a valid and common methodology for discrete-event simulations: it provides statistically meaningful simulation results, constituted by mean, variance and confidence interval.

All the three groups of simulations are conducted with a reasonable methodology and lead to important findings. They allow the identification of some of the current main weaknesses and strengths of the Lightning Network, and they also prove the effectiveness of some protocol improvements designed in this work, such as the passive rebalancing approach.

At the same time, the research work presents the following weaknesses. The simulator itself is used to define intervals of the simulation input parameters. However, a more accurate analysis would be to use well-known approaches to define such intervals, like for instance resolving the maximum flow problem to find the maximum payment amount tolerated by the payment network.

Response: In future work, this and other types of analyses will be done on the Lightning Network and, basing on the results of these analyses, new simulations will be performed using the CLoTH simulator.

Review Comment: Confidence intervals of the simulations results are currently present only in the files uploaded online. However, they should be discussed in the main text when relevant.

Response: In the revised version of the thesis, confidence intervals are presented and discussed also in the main text (for instance, see the Figures of the simulations results in Chapter 6).

Review Comment: CLoTH can be improved by simulating also the blockchain. For instance, this would allow the analysis of the critical situation in which many payment channels are closed in the same moment and therefore many transactions are sent to the blockchain. The author clearly specifies that the blockchain will be introduced in the simulator in future work.

Response: As mentioned in Chapter 7, in future work the behavior of the blockchain will be simulated in CLoTH.

Review Comment: In general, the research work presented in the thesis is of high quality. Capabilities and limitations of payment channel networks are analyzed in a accurate and systematic way, and the proposed protocol improvements are effective according to the simulation results. The CLoTH simulator opens to numerous investigations on payment channel networks and can practically assist their future development.