# Motivation thesis

yuupvengelshoven

February 2019

## 1 Motivation

**What is your research area and why is it important?**

10 years ago Bitcoin was introduced as a peer-to-peer decentralized digital currency[3]. Since the start of bitcoin, the monetary system has seen rise and fall in value due to the amount of trust to that currency. Throughout the life time of Bitcoin, many different forums of cryptocurrencies have entered the market trying to solve issues or extend the Bitcoin technology[8, 1]. These different implemntations stem from the research that is being done on cryptocurrencies, some of this research focuses on increasing the total throughput of transactions on the blockchain. Currently the amount of transactions that can be processed by Bitcoin is in the order of 10,000 times slower than that of credit-card solutions for transactions [7].

One solution to the problem of slow transaction rates is to make use of Payment-Channel Network (PCN) and bundle transactions[4]. A payment-channel allows a pair or group of users to exchange currency without having to push every transaction to the blockchain, such a channel can be opened by pushing a funding balance for each channel on the blockchain. To store the final state of the payment-channel a settling balance is pushed to the blockchain, closing the payment channels. When these channels are connected in a larger network, and users are able to transact with users through node hoping one is making use of a PCN. Using this technique allows for a series of transactions to take place without having to push each one onto the blockchain. Allowing the cryptocurrency achieve a higher throughput of transactions.

The idea of PCN has become an increasingly interesting topic for the past 3-4 years, as different implementations of the PCNs solution come to the market. The Lightning Network is an example for Bitcoin[4] though new research has brought forth the SpeedyMurmurs, SilentWhispers and Spider Network As this relatively new technology emerges onto the market, different problems still need to be solved.

As of now the transaction load on PCNs is relatively low, meaning that the succes-rate of transaction being accepted is high. As the PCN technology gets more widely adopted, the load on the network will increase. Such increases on

network load bring forth interesting research topics concerning PCNs. Presently little research has revolved concurrency of transaction requests in a PCN. There needs to be a way to ensure that the network does not lock and end up in a state where transactions are no longer processed through the network. How will the network handle multiple payments being requested at the same time, how to split payments over multiple paths in a constantly changing network? How is priority established and how can it be ensured that the throughput of transaction remains high in the network.

**What is the concrete problem you want to solve?**

The focus in this research will address how one deals with concurrency in a PCN, specifically looking at the SpeedyMurmurs algorithm. SpeedyMurmurs handles transactions by blocking funds for a short time frame, blocking of funds leads to race-conditions where multiple players try to lock the same funds for their transaction causing the network to stop functioning. Research needs to be done investigating how the blocking of funds causes the network to stop processing payments while concurrent transactions are requested. What type of concurrency algorithms, blocking or non-blocking are best able to deal with concurrency in the network and how these algorithms can allow for a high throughput of successful transactions in the PCN. Simulating concurrency for a PCN will allow for an in-depth analysis of how concurrency is currently working and being handled by SpeedyMurmurs, and different blocking and non-blocking algorithms can be simulated for their validadity of being able to handle concurreny in a PCN.

**Why is it important in the context of the research area?**

PCNs, while not a new concept, is an area of research still with a lot of novel ideas to be investigated. Research into how PCNs deal with concurrency is one of the novel topics that will become increasing relevant as PCNs become more widespread. Due to the relatively new concept of PCNs overlayed on a cryptocurrency network, researching how these networks will work under higher workload will allow for the technology to grow and stay ahead of the implementation and usage. SpeedyMurmurs has yet to be tested on how resilent it is during concurrent transactions in the network. Once the evaluation has taken place of the throughput of transactions during concurrency. Different concurrency solutions e.g. blocking, non-blocking or patially-blocking the network can be applied and compared to the evaluation of how concurrency is currently handled in SpeedyMurmurs. Such evaluation will highlight how SpeedyMurmurs may want to deal with concurrent transactions within the network.

**How do you want to solve the problem? How do you want to evaluate that your solution is good? (Also: why is the problem challenging and an actual research problem, not just implementation)**

Evaluating how concurrency is currently handled within SpeedyMurmurs will be done on the basis of a simulated PCN. The simulation will have be run with a varying amount of transaction load. The evaluation of how SpeedyMurmurs handles different load scenarios willl be done on different metrics. These metrics are throughput, volume-of-transactions-process and transaction-time. A reference evaluation will be done with the vanilla SpeedyMurmurs algorithm, the vanilla algorithm will be compared to different implementations of how to deal with concurreny. A solution will be seen as viable if it is able to out perform the vanilla SpeedyMurmurs in the measured metrics.

**What is your initial time plan?**

# References


[1] Vitalik Buterin et al. A next-generation smart contract and decentralized application platform. *white paper*, 2014.

[2] Giulio Malavolta, Pedro Moreno-Sanchez, Aniket Kate, and Matteo Maffei. Silentwhispers: Enforcing security and privacy in decentralized credit networks. In *NDSS*, 2017.

[3] Satoshi Nakamoto et al. Bitcoin: A peer-to-peer electronic cash system. 2008.

[4] Joseph Poon and Thaddeus Dryja. The bitcoin lightning network: Scalable off-chain instant payments, 2016.

[5] Stefanie Roos, Pedro Moreno-Sanchez, Aniket Kate, and Ian Goldberg. Settling payments fast and private: Efficient decentralized routing for path-based transactions. *arXiv preprint arXiv:1709.05748*, 2017.

[6] Vibhaalakshmi Sivaraman, Shaileshh Bojja Venkatakrishnan, Mohammad Alizadeh, Giulia Fanti, and Pramod Viswanath. Routing cryptocurrency with the spider network. *arXiv preprint arXiv:1809.05088*, 2018.

[7] Manny Trillo. Stress test prepares visanet for the most wonderful time of the year. *URl: http://www. visa. com/blogarchives/us/2013/10/10/stress-testprepares-visanet-for-the-most-wonderful-time-of-the-year/index. html*, 2013.

[8] Gavin Wood. Ethereum: A secure decentralised generalised transaction ledger. *Ethereum project yellow paper*, 151:1–32, 2014.