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 then the monetary system has seen a rise and fall in value. Different implementations of Bitcoin, cryptocurrencies, have entered the market trying to solve different issues with the Bitcoin technology and extend cryptocurrencies use cases[8, 1]. As the cryptocurrency technology matures, different inherent issue with cryptocurrencies are tying to be solved. 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]. PCN allow a pair or group of users to exchange currency without having to push every transaction to the blockchain, this is done by having a start transaction that records all the balance of each channel and by a end transaction that records the final state of each channel. Using this technique allows for a series of transactions to take place without having to push each one onto the blockchain. Allowing for a higher throughput of currency exchange than if every transaction needed to be pushed to the blockchain.

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[5], SilentWhispers[2] and Spider Network[6]. As this relatively new technology emerges onto the market, different problems still need to be solved.

As of now the transaction load on PCN is relatively low, meaning that the throughput of payments is high. As PCN technology matures so will the load on the network, this brings forth interesting research topics. Some of these topic revolve around concurrency of payment requests in a PCN. There needs to be a way to ensure that the network does not becoming blocking and is able to handle payment requests. How will the network handle multiple payments being requested at the same time, how is the routing done to different nodes? Who gets priority and how can it be ensured that the throughput of the network is still possible.

What is the concrete problem you want to solve?

The problem that is being addressed in this research is how one deals with concurrency in a PCN, specifically looking ath the SpeedyMurmurs algorithm. As the load of the PCN increase how should the network handle when payment requests come in at the same time? Simulating concurrency for a PCN will allow for an in-depth analysis of how concurrency is currently implemented in SpeedyMurmurs. With the concurrency analysis different strategies can be examined to deal with concurrency and be implemented so that the PCN running SpeedyMurmurs will be able to function under a heavier load.

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

Concurrency within PCNs while not a new concept, is a field of research with limited amount of research focused mainly on investigating how payment channel networks deal with concurrency. Due to the relatively new concept of payment channels 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 usuage. SpeedyMurmurs has been tested against a dataset from Ripple, though due to the relatively low load concurrency within the dataset the PCN had low demand for concurrent requests and thus was not tested thoroughly.

How do you want to solve the problem?

To tackle the problem of concurrency observation in a PCN running SpeedyMurmurs a simulation will be created to simulate how an actual network may work. The analysis will be done on real data-sets and simulated data-sets. Seeing as all current work on actual data does not comprise of enough concurrent communication between exchanges.

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)

To evaluate if the concurrency implementations are actual solutions to helping congestion with proper concurrency control in SpeedyMurmurs, some baseline simulations will need to be made with no changes to the SpeedyMurmur algorithm. Then the base-line simulation will be compared to the changed concurrency handling of the algorithm. Throughput, volume-of-transactions-processed and time-delay will all be used to measure and compare.

What is your initial time plan?

To finish it on time.

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.