Prof. Laurent Vanbever
Networked Systems Group

Scaling Cryptocurrencies: the data driven approach

Semester thesis proposal

Propagation delay significantly affects security and liveliness of any Blockchain system [3]. Particularly for Bitcoin, increased propagation delay is shown to cause temporal partitions [4], essentially leaving multiple Bitcoin clients with an outdated view of the chain and thus vulnerable to double-spending [2] and selfish mining attacks [5].

An early study [1] showed that the median time until a node receives a block is 6.5 seconds, whereas the mean is 12.6 seconds. The long tail of the distribution means that even after 40 seconds, there are still 5% of nodes that have not yet received the block. A more recent study [4] showed that even during a period of 2 months there was at least one time when the majority of the Bitcoin clients were out-of-sync for 5 minutes. While the implications of such delay are disruptive and not specific to Bitcoin [3] none of the aforementioned studies have investigated the root cause of the problem.

The goal of this project is threefold. First, we need to investigate the factors that contribute to increased propagation delay in certain parts of the peer-to-peer network. To that end, we will utilize months of propagation data from the Bitcoin network, which we have already collected. Potential causes of this temporal gap might include the lack of bandwidth, transmission delay, a small number of connections, the graph structure, or the client's increased load. Second, we will validate the revealed causes in simulation, and evaluate the impact of delay in different aspects of the system, such as propagation, validation, block creation, etc. Finally, we will work towards designing strategies to mitigate them. For instance, a client might need to increase or decrease the number of outgoing connections, select its peers in a bandwidth- or delay-aware manner or even migrate to another network in order to improve its times.

The required work can be split roughly into the following milestones:

1. Review literature for Blockchain systems with emphasis on their networking needs.
2. Analyze the propagation data we have already collected to find the propagation patterns and potential causes of temporal partition.
3. Validate findings in simulation
4. Design and implement a control system to detect and mitigate delay issues at the node level.

Requirements

- Some familiarity with Blockchain systems and networking concepts.
- Strong skills in programming and data analysis.

Contact

- Maria Apostolaki, apmaria@ethz.ch
- Prof. Dr. Laurent Vanbever, lvanbever@ethz.ch

References

[1] C. Decker and R. Wattenhofer. Information propagation in the bitcoin network. In *IEEE P2P 2013 Proceedings*, pages 1–10. IEEE, 2013.

[2] G. O. Karame, E. Androulaki, and S. Capkun. Double-spending fast payments in bitcoin. In *Proceedings of the 2012 ACM conference on Computer and communications security*, pages 906–917. ACM, 2012.

[3] R. Pass, L. Seeman, and A. Shelat. Analysis of the blockchain protocol in asynchronous networks. In *Annual International Conference on the Theory and Applications of Cryptographic Techniques*, pages 643–673. Springer, 2017.

[4] M. Saad, V. Cook, L. Nguyen, M. T. Thai, and A. Mohaisen. Partitioning attacks on bitcoin: Colliding space, time and logic. Technical report, Tech. Rep, 2019.

[5] A. Sapirshtein, Y. Sompolinsky, and A. Zohar. Optimal selfish mining strategies in bitcoin. In *International Conference on Financial Cryptography and Data Security*, pages 515–532. Springer, 2016.