Internship Proposal (Research): "Fair transactions ordering in a blockchain"

Keywords: Fairness, Blockchain, Knapsack problems, Statistical tests

Host intitute: Max-Planck Institute for Software Systems (MPI-SWS), Saarbrücken, Germany

Supervisors:
Krishna Gummadi (MPI-SWS) – `https://people.mpi-sws.org/~gummadi/` – `gummadi@mpi-sws.org`
Patrick Loiseau (Inria & Ecole Polytechnique) – `http://lig-membres.imag.fr/loiseapa/` – `patrick.loiseau@inria.fr`

Background

In a blockchain system, a set of miners compete to be the first to discover a new *block* that gets added on top of the existing chain—then every miner restarts its computation from the new chain. When a miner discovers a new block, it takes *transactions* from a pool of transactions (called Mempool) to include in the block. Many blockchain systems (e.g., Bitcoin and Etherium), however, are increasingly often congested [1]: when a block is discovered, there are more transactions in the Mempool that can be included in the block. This raises the question of how to select which transactions to include, and in which order. This question is critical in many applications of blockchains as (*i*) delays in the transactions commit (i.e., inclusion in a block) may be detrimental or costly to transactions issuers and (*ii*) transactions order might be a critical defining characteristic for instance to define property.

The norm in terms of transaction selection by miners was not defined in the original bitcoin protocol. Instead, it is drawn from a code called getblocktemplate (GBT) [2], which changed in 2016. Currently, this transactions selection is mainly based on *feerate* (that is on the fee per kB that the miner will receive if including that transaction), with the rationale that it incentivizes miners. In recent work [1], however, we observed that this norm is far from being always respected by miners. Many large mining pools today offer "acceleration services" to prioritize transactions for an extra fee that is paid through a private channel (contrary to the public feerate). This is dangerous for other transaction issuers as they do not get the full picture needed to adjust the offered feerate. More generally, while the question is critical, there is currently no reflection on what the norm for transaction selection should be, how to enforce it, and what is its implication on the incentives and economic ecosystem surrounding the blockchain.

Goal of the internship

The goal of this internship is to answer the above questions by proposing a *fair transaction selection and ordering* norm for blockchain, along with mechanisms to satisfy it and to enforce it; and to analyze the effect of different norms on the blockchain and mining ecosystems. Specifically, we will go through the following research questions (subject to time and to preference of the student):

(*i*) *What is a fair norm?* We will consider multiple aspects of the transactions including feerate, waiting time, or transaction amount and propose metrics of fairness for transaction ordering appropriate for different contexts.

(*ii*) *How to perform fair selection/ordering?* Each block is limited by a size of 1 MB and different transactions have different sizes. Hence the problem of transactions selection is a knapsack problem, yielding the question: how to solve this knapsack problem under the above fairness constraint? We may look for pseudopolynomial time algorithms based on dynamic programming and for approximation ratios for simpler greedy algorithms.

(*iii*) *How to enforce fair selection/ordering?* The issue here is that mining is often done in a peer-to-peer fashion and different miners in the network have different views of the system. In particular they may have different transactions in the Mempool at a given point in time (and different arrival times for those transactions). Hence the question is how can the system detect, with this partial information, if a miner deviates from the prescribed norm. We will study methods based on statistical tests in the spirit of [4, 5, 3].

(*iv*) *What is the effect of different miners following different norms?* The question here is how can we characterize the ordering that would result from different miners following different ordering norms (in particular given their respective mining power, i.e., likelihood to be discovering a block), and the incentives that this would create for transactions issuers.

We have collected a large amount of data on past transactions that can be used, for each of these questions, to perform numerical analyses based on realistic inputs.

Additional information

The internship will be hosted at the Max-Planck Institute for Software Systems (MPI-SWS) in Saarbrücken, Germany, and jointly supervised by Krishna Gummadi from MPI-SWS and Patrick Loiseau from Inria Grenoble, with a possibility (not mandatory) to spend a period in Grenoble. For more information, please contact `gummadi@mpi-sws.org` and `patrick.loiseau@inria.fr`.

References

[1] J. Messias, M. Alzayat, B. Chandrasekaran, and K. P. Gummadi. On Blockchain Commit Times: An analysis of how miners choose Bitcoin transactions. In *Proceedings of the KDD Workshop on Smart Data for Blockchain and Distributed Ledger (SDBD)*, 2020.

[2] `https://en.bitcoin.it/wiki/Getblocktemplate`

[3] K. Lev-Ari, A. Spiegelman, I. Keidar, and D. Malkhi. FairLedger: A Fair Blockchain Protocol for Financial Institutions. In *Proceedings of the 23rd International Conference on Principles of Distributed Systems (OPODIS)*, 2019.

[4] A. Asayag, G. Cohen, I. Grayevsky, M. Leshkowitz, O. Rottenstreich, R. Tamari, and D. Yakira. A Fair Consensus Protocol for Transaction Ordering. In *Proceeding of the 26th International Conference on Network Protocols (ICNP)*, 2018.

[5] A. Orda and O. Rottenstreich. Enforcing Fairness in Blockchain Transaction Ordering. *In Proceedings of the 2019 IEEE International Conference on Blockchain and Cryptocurrency (ICBC)*, 2019.