Analysis of the Confirmation Time in Proof-of-Work Blockchains

Ivan Malakhov, Andrea Marin, Sabina Rossi, Daria Smuseva
Università Ca' Foscari Venezia
{ivan.malakhov,marin,sabina.rossi,daria.smuseva}@unive.it

Abstract

In blockchain networks driven by Proof of Work, clients spend a certain amount of cryptocurrency (called fees) to control the speed of confirmation of the transactions that they generate. In fact, transactions are confirmed according to a strong priority policy that favours those offering the highest fees. The problem of determining the optimal fee to offer to satisfy certain delay requirements is still widely open and, at the state of the art, mainly reactive methods based on historical data are available. In this work, we propose a queueing model based on the exact transient analysis of a $M/M^B/1$ system to address this problem. The model takes into account (*i*) the state of the Mempool (the backlog of pending work) when the transaction is generated, (*ii*) the current transaction arrival intensity and (*iii*) the distribution of the fees offered by other transactions to the miners. The outcome of our analysis allows us to provide an algorithm to quickly compute the expected transaction confirmation time given the blockchain state, and to highlight new insights on the relations between the transaction fees and confirmation time in BTC blockchain.

1. Introduction

In recent years, the economic system that allows blockchain distributed ledgers to operate has attracted a lot of attention. In particular, the fees offered by the users to pay for the services provided by the system have been recognized as a pivotal aspect of this technology [1, 2, 3].

Blockchains are distributed ledgers based on peer-to-peer consensus protocols that are becoming widely popular nowadays. Such networks enable the technology for many applications that require the permanent and immutable storage of data.

Several protocols have been devised to reach consensus in blockchain, possibly inspired by the Byzantine fault tolerance problem. In this talk, we consider the original and mostly applied consensus protocol: the *Proof of Work* (PoW) that is applied in Bitcoin blockchain [4].

In PoW blockchains, miners (i.e., users that verify the transactions and consolidate the blocks) receive a new transaction and store it in a special buffer for pending transactions that is usually called *Mempool*. A transaction that leaves the Mempool and is included in a block is said *confirmed*.

Each block of the chain contains a subset of the transactions present in the Mempool at the moment of its consolidation and the maximum amount of transactions that fit in a block is given by some invariant properties of the blockchain, e.g., in BTC it is 1 MB or on average 2,300 transactions per block.

As far as this talk is concerned, the crucial aspect of the mining process is the way in which the transactions are selected from the Mempool by the miners.

We discuss a queueing model to answer the following questions: *given the state of the Mempool and the intensity of the workload, what is the expected number of blocks that a transaction offering a certain fee should wait for its confirmation?* Since the workload conditions change with time, the hardness of the competition for the transaction confirmations changes as well. In Figure 1, we show the correlation between the offered fees and the intensity of the workload.

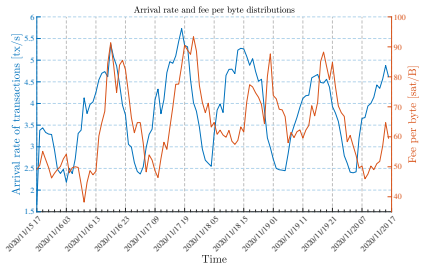
2. Methodology

Since the confirmation of transactions takes place in batches, i.e., the newly generated block contains all the transactions that it can fit, the whole stochastic process underlying the Mempool can be seen as $M/M^B/1$ queueing process [5, 6] where M denotes that both the transaction inter-arrival times and the inter-block generation times are independent and exponentially distributed, B is the batch size that corresponds to the block capacity, and 1 denotes that the system consolidates one block at a time.

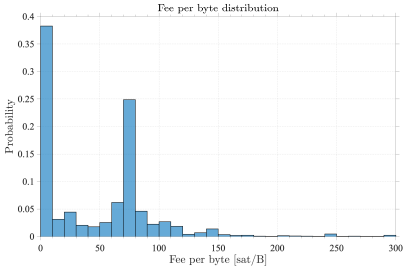
We give the transient solution of such a system based on the technique of generating functions and an extensive set of experiments with the aim of studying the impact of the Mempool state and the system's load factor on the choice of the fee to offer in order to satisfy certain delay requirements on the transaction confirmation.

We believe that the results proposed in this work are of high importance for every transaction issuer. Clearly, to optimize the costs it is crucial for them to know the minimum fee to pay in order to have their transactions confirmed within a certain desirable time, as in case, for example, of speculative exchanges of the cryptocurrency. Conversely, one may also be keen to know how long the confirmation delay would be if a certain fee for the transaction is set.

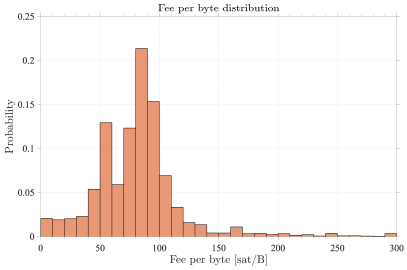
Figures 1b and 1c show empirical probability density function of fee-per-byte ratios for two periods of time with moderate and heavy workload conditions respectively. The plots support the intuition that, when the load is moderate, there is a lower



(a) Arrival rate and fee per byte as functions of the time.

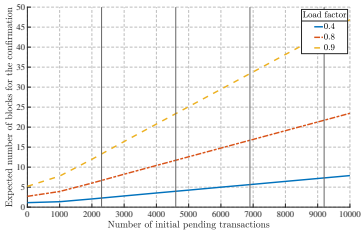


(b) Empirical probability density function of fee per byte in moderate workload conditions.

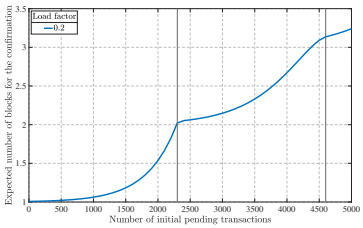


(c) Empirical probability density function of fee per byte in heavy workload conditions.

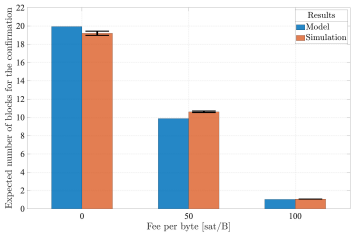
Figure 1: Data retrieved from the BTC blockchain analysis.



(a) Expected number of blocks for the confirmation as a function of number of initially pending transactions for different load factors.



(b) Expected number of blocks for the confirmation as a function of number of initially pending transactions for $\rho = 0.2$.



(c) Expected number of blocks for the confirmation as function of fee per byte for model and simulation results with $Y = 6,000$ and $\lambda = 3.21$ transactions per second.

Figure 2: Experiment results.

competition for accessing the new blocks, hence the fee-per-byte ratio tends to be as small as possible.

3. Results

In this section, we show some numerical experiments with our model and comment on the insights that they reveal on the system under study.

Impact of the initial Mempool state on the expected confirmation time. The Mempool state at the tagged transaction arrival is of great importance for transaction fee estimation. This observation is even more evident thanks to the plots of Figure 2a. It is interesting to observe that the function describing the expected confirmation delay given the initial number of pending transactions has abrupt changes in its growth for values corresponding to integer multiples of the block size. This is clearly shown by Figure 2b and, if we assume the limiting case $\lambda \to 0$, this function becomes a step function with unit increase at B, $2B$, $3B$ and so on.

Comparison with trace-driven simulation. In this paragraph, we evaluate the accuracy of the model prediction by resorting to trace-driven Monte Carlo simulation.

The experiment is done by measuring $\lambda = 3.21$ transactions per second, i.e., $\rho \simeq 0.85$. In this case, transactions offering 0 sat/B are almost sure to be confirmed. We assume that the Mempool contains $6,000$ transactions. Figure 2c shows the model predictions and the simulation estimates assuming that fees of 0, 50 or 100 sat/B are offered. We can see that, in these cases, there is an excellent agreement among the data.

According to our experiments, even in heavier load, the model manages to maintain a relative error below 20%. Moreover, we believe that the accuracy can be further increased with appropriate techniques of workload predictions.

4. Conclusion

In this talk, we discuss a transient analysis of a $M/M^B/1$ queueing model that allows the definition of a new method for estimating the expected transaction confirmation time in blockchain based on PoW. The model uses three key parameters: the observed state of the Mempool, the current arrival intensity and the distribution of the offered fees. With respect to the queueing models proposed at the state of the art, we take into account the initial state of the Mempool and the numerical experiments have shown that this has a strong impact on the estimations.

Although the model was studied on the Bitcoin network, it can be applied for any kind of PoW-driven blockchains where transactions are confirmed according to an auction on the fees.

The results of the models have been compared with trace-driven simulations under heavy and very heavy workloads. The accuracy is generally very good, although it may deteriorate for long-term predictions in very heavy load.

Acknowledgements

This work is partially supported by the Project PRIN 2020 “Nirvana - Noninterference and Reversibility Analysis in Private Blockchains”, and by the project SERICS (PE00000014) under the MUR National Recovery and Resilience Plan funded by the European Union - NextGenerationEU.

References

[1] D. Easley, M. O'Hara, S. Basu, From mining to markets: The evolution of bitcoin transaction fees, J. of Financial Economics 134 (1) (2019) 91–109.

[2] G. Huberman, J. Leshno, C. Moallemi, Monopoly without a monopolist: An economic analysis of the bitcoin payment system, Review of Economic Studies 0 (2021) 1–30.

[3] H. Qiu, T. Li, Auction method to prevent bid-rigging strategies in mobile blockchain edge computing resource allocation, Future Gener. Comput. Syst. 128 (2022) 1–15.

[4] S. Nakamoto, Bitcoin: A peer-to-peer electronic cash system (2009). URL `http://www.bitcoin.org/bitcoin.pdf`

[5] L. Kleinrock, Queueing Systems Volume 1: Theory, Wiley, 1975.

[6] P. G. Harrison, A. Marin, Product-forms in multi-way synchronizations, Comput. J. 57 (11) (2014) 1693–1710.