Measurements, Analysis and Modeling of Hyperledger Fabric

Abstract—Bitcoin network

Index Terms—Bitcoin Network, Mining Pools, Malthusian Trap, Incentive Mechanism

1 Introduction

BITCOIN [1] is a decentralized peer to peer (P2P) cryptocurrency that was first proposed by Satoshi Nakamoto in 2008. Without resorting to any trusted third party, Bitcoin adapts a cryptographic proof mechanism that enables anonymous peers to complete transactions through the P2P network. Blockchain is the core mechanism of the Bitcoin system. It not only records historical transactions from Bitcoin clients, but also prevents the Bitcoin network from double spending attacks [2]. The Bitcoin network participants, who maintain and update the ongoing chain of blocks, are called miners. These miners compete in a mining race driven by an incentive mechanism [3], [4], where the one who first solves the Bitcoin cryptographic puzzle [5] has the right to collect unconfirmed transactions into a new block, append the new block to the main chain, i.e., the longest chain of blocks, and gain some BTCs [6] as a mining reward.

2 Environment

Hyperledger Fabric version 1.4
Fabric SDK v1.0.0
Jmeter

3 BlockTime Solo Orderer Mode

3.1 Model of Orderer's Configuration

The configuration file, i.e., configtx.yaml, configures the orderer service as follows.

```
BatchTimeout: 2s
BatchSize:
    MaxMessageCount: 10
    AbsoluteMaxBytes: 98 MB
    PreferredMaxBytes: 512 KB
```

Case 1 without considering block size, we have the following model,

$$BlockTime = \begin{cases} \infty & TAR = 0 \\ BatchTimeout & 0 < TAR \le \frac{MaxMessageCount}{BatchTimeout} \\ \sigma & \frac{MaxMessageCount}{BatchTimeout} < TAR \end{cases} \tag{1}$$

If $TAR = 0$, then $BlockTime = \infty$. It means that if there are no transactions, there are no blocks.

If $0 < TAR \le \frac{MaxMessageCount}{BatchTimeout}$. It means that the number of transactions are less than MaxMessageCount given a BatchTimeout. Therefore, blocks are created for each BatchTimeout.

If $\frac{MaxMessageCount}{BatchTimeout} < TAR$. It means that the number of transactions are larger than MaxMessageCount in each BatchTimeout. Therefore, blocks are created as soon as possible and σ is a small value.

3.1.1 Experiment 1: Uniform Random Distribution of TAR

TABLE 1
Different Configuration of BatchTimeout

BatchTimeout (s)	0.1	0.5	1	2	5	10	30
BlockTime (s)	a	a	a	a	a	a	a

Table shows how different configuration of BatchTimeout affect BlockTime. Following our model, and the experiments, we can have a comparison results as follows,

Here we need a figure with a comparison of the model result and the experimental results.

See more about Uniform Random Timer $http : //2min2code.com/articles/jmeter_intro/random_timer$

3.1.2 Experiment 2: Poisson Distribution of TAR

TABLE 2
Different Configuration of BatchTimeout

BatchTimeout (s)	0.1	0.5	1	2	5	10	30
BlockTime (s)	a	a	a	a	a	a	a

Table shows how different configuration of BatchTimeout affect BlockTime. Following our model, and the experiments, we can have a comparison results as follows,

Jmeter Poisson Distribution of TAR: $https : //www.blazemeter.com/blog/comprehensive - guide - using - jmeter - timers/$

3.1.3 Experiment 3: Constant Distribution of TAR

Jmeter Constant Distribution of TAR: $https : //www.blazemeter.com/blog/comprehensive - guide - using - jmeter - timers/$

Table shows how different configuration of BatchTimeout affect BlockTime. Following our model, and the experiments, we can have a comparison results as follows,

TABLE 3
Different Configuration of BatchTimeout

BatchTimeout (s)	0.1	0.5	1	2	5	10	30
BlockTime (s)	a	a	a	a	a	a	a

3.2 Transaction Delay (For Peer)

Here we need to discuss something about transaction delay in this section.

3.2.1 Transaction Size

How transaction size affects transaction delay, transaction loss

3.2.2 Experiment 1: Transaction Size 1 byte

3.2.3 Experiment 2: Transaction Size 300 byte

3.2.4 Experiment 3: Transaction Size 10 Mbyte

3.2.5 Endorsement Policy

3.2.6 Experiment 1: Policy a

3.2.7 Experiment 2: Policy b

3.2.8 Experiment 3: Policy c

Here we need to know how endorsement policy affect transaction delay

4 Kafka Orderer Mode

4.1 Model of Kafka Orderer's Configuration

The configuration file of Kafka

References

[1] S. Nakamoto, "Bitcoin: A peer-to-peer electronic cash system," 2008.

[2] G. O. Karame, E. Androulaki, M. Roeschlin, A. Gervais, and S. Čapkun, "Misbehavior in bitcoin: A study of double-spending and accountability," *ACM Transactions on Information and System Security (TISSEC)*, vol. 18, no. 1, p. 2, 2015.

[3] Y. Lewenberg, Y. Bachrach, Y. Sompolinsky, A. Zohar, and J. S. Rosenschein, "Bitcoin mining pools: A cooperative game theoretic analysis," in *Proceedings of the 2015 International Conference on Autonomous Agents and Multiagent Systems*. International Foundation for Autonomous Agents and Multiagent Systems, 2015, pp. 919–927.

[4] O. Schrijvers, J. Bonneau, D. Boneh, and T. Roughgarden, "Incentive compatibility of bitcoin mining pool reward functions," in *International Conference on Financial Cryptography and Data Security*. Springer, 2016, pp. 477–498.

[5] I. Giechaskiel, C. Cremers, and K. B. Rasmussen, "On bitcoin security in the presence of broken cryptographic primitives," in *European Symposium on Research in Computer Security*. Springer, 2016, pp. 201–222.

[6] BTC. [Online]. Available: https://en.bitcoin.it/wiki/Bitcoin, Accessed on 31 January 2019.