Information Propagation in Blockchains: Analysis, Methods, and Evaluations

515030910588 Yiyan Yang

May 27th, 2018

Abstract

With the development and acknowledgement of Bitcoin, the application of blockchains is attached more attention. Among all the difficulties, information propagation has always been a very important and urgent problem to be solved. This report will combine with bitcoin network to describe in detail how this problem emerges, what consequence the problem leads to and some solutions.

1 Introduction

Blockchain is an emerging decentralized architecture and distributed computing paradigm underlying Bitcoin and other cryptocurrencies, and has recently attracted intensive attention from governments, financial institutions, hightech enterprises, and the capital markets. Blockchain's key advantages include decentralization, time-series data, collective maintenance, programmability and security, and thus is particularly suitable for constructing a programmable monetary system, financial system, and even the macroscopic societal system.

In a bitcoin network, if a transaction happens, it needs to be noted in the blocks and be validated by other nodes using different protocols, for example POW and POS. Then this block can be added to the main link. Transaction information plays a important role in this process. How to make the information propagation fast and secure decides the security of the bitcoin network.

In section 2 & 3, I introduces how the information propagates in bitcoin network and the possible problems. In section 4, I introduces some methods to circumvent the risk to a certain extent. In section 5, I introduces future work.

2 Information Propagation

In bitcoin network, each node receives information from other nodes in its neighborhood and keeps a complete replica of all the information needed to verify the validity of transactions. They each verifies the information independently.

In this case, a node may receives repeating information for many times. If each of the received information contains a complete replica, the propagation of the information would become rather slow and inefficient. So the information propagation in bitcoin network take another way.

As it shows in figure 1, Node A receives a block, verifies it and announces it to its neighbors. Node B receives the inv message which contains the basic information of the block in the form of hash, and if it hasn't received the block yet, it will issue a getdata message. Upon receiving the getdata message, Node A will deliver the block to Node B.

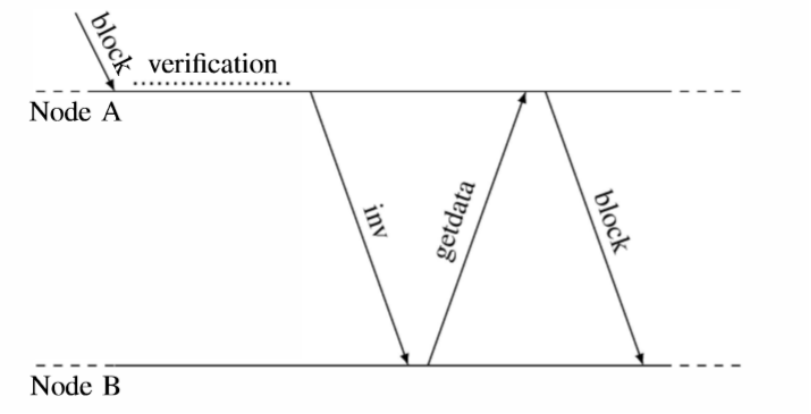

Figure 1: Flow chat of information propagation in bitcoin network

Obviously, this process will still lead to propagation delay, though the inv message and getdata message are only several bit. The propagation delay is the combination of transmission time and the local verification of the block or transaction. This unavoidable delay may result in the following problems.

3 Problems

3.1 Double Spending Attack

Two or more transactions might attempt to transfer the same coins multiple time. This is called a double spending attack. Each node will validate one of the transaction which it first receives and ignore others but the network cannot ensure that all the node receive the same transaction.

By using the protocol of POW, the network will wait until 5 or 6 blocks produce and admit that the longer forking link is the main link. But the problem of double spending attack cannot be avoided completely.

Double spending attack is not very serious and the probability that it happens is about 1.9%.

3.2 Information Eclipsing Attack

The attackers isolate a node from the network. In this way, the attacker can prevent the victim node from obtaining complete information about other parts of the network.

The information eclipsing attack often combines with double spending attack to gain more benefits. As the figure 2 shows.

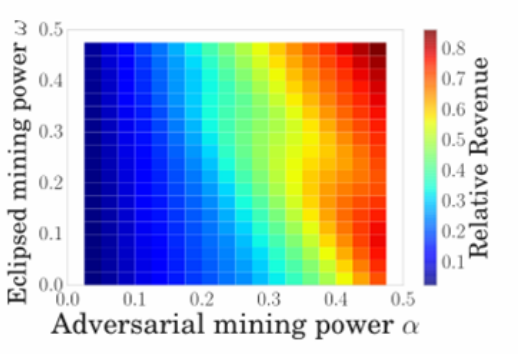

Figure 2: Benefits of eclipse attack

4 Methods

4.1 Incentive and Punishment

The bitcoin network set rewards for those who validate a block and set transection fee to encourage node to note the transaction. However, it never give rewards for those who propagate the information.

Knowledge of a transaction is as precious as its transaction fee. So even a rational participant has an incentive not to share the incoming transaction knowledge with the rest of the network for its own benefits.

In this case, the network should reward for the information propagation to promote the normal operation of the network.

4.2 Routing Mechanisms

In a centralized system, propagation can be handled very efficiently by a predefined routing mechanism because location of the server is known and stable.However, in a decentralized system, as I explained above, a node will receive the same information from different neighboring nodes.

So how to divide the proper neighborhood is a topology question worth studying.

4.3 Speeding Up the Propagation

There are three basic methods of this topic, minimize verification, pipelining block propagation and connectivity increase.

For example, I stated the common methods of how to announce the neighborhood the information. But it may waste extra time in receiving block and verify it. Changes may make it more efficient. Node A receives inv message and if it haven't received this block, it reply a getdata message and send its inv message to Node B. When waiting for B to reply, Node A can receive the block and verify it.

5 Future Work

We should try to build a model about how to reward for information propagation. The rewarding should be attractive enough to encourage people to propagate information but it won't influence the stability of the network.

Then, we should study how to divide the proper neighborhood to decrease the propagation delay.

References

[1] Christian Decker, Roger Wattenhofer. Information Propagation in the Bitcoin Network

[2] Oguzhan Ersoy, Zhijie Ren, Zekeriya Erkin, and Reginald L. Lagendijk. Information Propagation on Permissionless Blockchains

[3] Christian Catalini and Catherine Tucker. Seeding the S-Curve? The Role of Early Adopters in Diffusion