Analyzing the Possibility of Bitcoin Network Partitions Caused by Internet Censorship

Jorge Coll, Andrew Fasano, Benjamin Kaiser, Lucy Qin
MIT 6.805: Shared Public Ledgers – Final Project
jorge.coll@ll.mit.edu, *andrew.fasano@ll.mit.edu*, *benjamin.kaiser@ll.mit.edu*, *ziyuan.qin@ll.mit.edu*

***Abstract*—Abstract goes here.**

I. Introduction

Blah blah blah.

II. Background

A. Bitcoin's networking protocol

The message transfer protocol that powers Bitcoin is defined abstractly in Nakamoto's original publication [1] and further fleshed out in bitcoind, the reference implementation written by Nakamoto that still serves as the default and most popular Bitcoin client. In this section, we will provide a high-level overview of the portion of the protocol relevant to our work. In particular, because we focus on a partitioning attack that severs existing connections, we will not discuss how new clients are bootstrapped, how initial blocks are downloaded, or how further peer connections are established. This leaves the standard relay protocol, which consists of four message types:

- *inv*: when a transaction or block has been verified by a node, the node announces that the transaction or block is available by sending an *inv* message to all of their neighbors.
- *getdata*: when a node receives an *inv* message for a transaction or block that it does not already have a local copy of, it responds with a *getdata* message asking for that block.
- *tx*: when a node receives a *getdata* request for a given transaction, it responds with a *tx* message containing the transaction
- *block* when a node receives a *getdata* request for a given block, it responds with a *block* message containing the block

A node will only propagate a block or transaction to its neighbors if it can verify it. Unverified transactions or blocks are not propagated.

By itself, Bitcoin does not attempt to detect or mitigate partitions. If a partition appears, both portions will continue operating independently and their state will diverge. If the divergence results in subnetworks that produce incompatible transaction histories, they will be unable to merge if the partition is later removed. Decker and Wattenhofer [2] observe that detection of network partitions may not be challenging and could be achieved through simple monitoring of the observed aggregate computational power in the network. As Bitcoin has grown in size and influence, such monitoring has begun to take place, and as of this writing it is possible to easily view the total network hashing rate via public websites [3].

Talk about approximate current state of network (num nodes, avg connectivity, total hash power, geographic distribution if possible)

B. Internet traffic censorship

1) China:

2) Cuba:

3) Iran:

4) ...:

References

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

[2] C. Decker and R. Wattenhofer, “Information propagation in the bitcoin network,” in *Proceedings of the 13th IEEE International Conference on Peer-to-Peer Computing*, 2013.

[3] [Online]. Available: http://bitcoin.sipa.be/