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

A citation [1]

II. Background

A. Bitcoin's Networking Protocol

The message transfer protocol that powers Bitcoin is defined abstractly in Nakamoto's original publication [2] 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

References

[1] 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.

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