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 [**?**] 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 [**?**] 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 [**?**].

B. Internet Traffic Censorship

Censorship of Internet traffic occurs in a variety of forms all over the world. The most aggressive censorship takes place in countries where citizens' access to the Internet is very limited to begin with (e.g., North Korea and Cuba). Verkamp and Gupta [**?**] conducted experiments to infer the mechanics of various countries' approaches to Internet censorship and also provided a set of independent sources ranking countries based on the severity of their censorship.

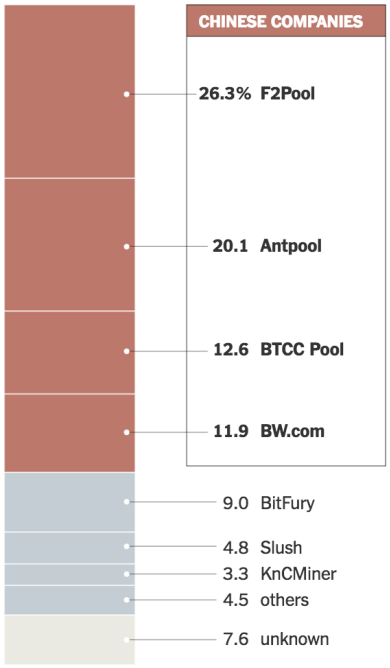

Fig. 1: From [**?**]: the shares of mined Bitcoin blocks from May 24 to June 24, 2016 by mining pool.

Across our research, four countries were repeatedly identified as the most severe Internet censors: North Korea, Cuba, Iran, and China. Of these, China is the most interesting case for our purposes for two reasons: (1) its Internet-connected population far surpasses the others' and (2) it is a hotbed of Bitcoin mining activity, with Chinese-run mining pools accounting for an estimated 70% of all Bitcoin mining power as of June 2016

(Figure **??**). As a collection, China's censorship measures are colloquially referred to as The Great Firewall of China (GFW).

1) The Great Firewall of China: Existing research points to three primary techniques used by the GFW:

- *IP blocking*: blah
- *IP address misdirection*: blah
- *Data filtering*: blah

[**?**] [**?**]

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/

[4] J.-P. Verkamp and M. Gupta, "Inferring mechanics of web censorship around the world," in *Presented as part of the 2nd USENIX Workshop on Free and Open Communications on the Internet*, 2012.

[5] *How China Took Center Stage in Bitcoin's Civil War*, 2016.

[6] M. Hu. (2011, May) The great firewall: a technical perspective. Torfox: A Stanford Project. [Online]. Available: https://cs.stanford.edu/people/eroberts/cs181/projects/2010-11/FreedomOfInformationChina/great-firewall-technical-perspective/index.html

[7] X. Xu, Z. M. Mao, and J. A. Halderman, "Internet censorship in china: Where does the filtering occur?" in *Proceedings of Passive and Active Measurement: 12th International Conference*, 2011.