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

I'll write this last.
Cite definition of a partition attack from [1].

II. 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 he provided. 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 [3] 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 [4].

III. Web Traffic Censorship

Censorship of Web 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 [5] conducted experiments to infer the mechanics of various countries' approaches to Web censorship and also provided a set of independent sources ranking countries based on the severity of their censorship.

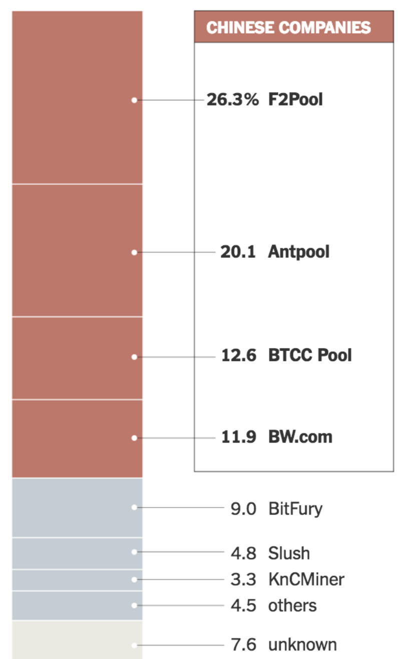

Fig. 1: From [6]: the shares of mined Bitcoin blocks from May 24 to June 24, 2016 by mining pool.

Across our research, four countries were repeatedly identified as the most severe 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 1).

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

IV. The Great Firewall of China

There is no consensus about the precise technical underpinnings of the GFW, as conflicting observations have been made. In particular, there is conflict about whether or not it is stateful – i.e., whether it stores and uses information about the packets it intercepts[1]. However, the basic mechanisms employed are known to be[8]:

- *IP address filtering*: The GFW blocks specific IP addresses from receiving traffic by dropping all packets associated with it. This assures that the GFW's reach extends to all content produced by a host's IP, rather than just the few specified domains.
- *DNS misdirection (hijacking)*: When requesting a blocked host name, there are cases in which the DNS servers under the GFW will return a different IP address than the one that corresponds to the domain name requested. The Chinese government can effectively replace the content with material that is more favorable to their interests.
- *Keyword filtering*: If a banned keyword appears in a URL, after a completed TCP handshake, the GFW will send reset packets to both the source and destination, blocking access to the requested content. Even if a keyword is not explicitly in the URL but appears within the HTML response, the content is also denied. In this particular instance, pages often begin to display but are then truncated after the discovery of a keyword.

A. Impact on Bitcoin

The only direct impact that the GFW has on the Bitcoin network is a minor delay added to every packet. Due to this and normal Bitcoin propagation delays, Chinese miners will hear about blocks mined outside of China later than ones within the country, causing a communication barrier. This also creates an unfair disadvantage to those outside of China since China has majority hash power. This can constrain Bitcoin itself in some ways such as during the controversy surrounding a proposed block size increase. If the size were to increase, Chinese miners would be subject to further delays, potentially jeopardizing profits. (This needs some citations!)

Our initial aim was to produce a Bitcoin block that would be filtered by the GFW. However, in the end we determined that we would need to trick the GFW into interpreting a block as Web traffic of some sort (e.g., DNS or HTTP), which was not feasible. (To all, but especially Andrew: is there anything else we should say here about what we tried / observed?)

References

[1] M. Apostolaki, A. Zohar, and L. Vanbever, "Hijacking bitcoin: Routing attacks on cryptocurrencies," in *CoRR*, vol. abs/1605.07524, 2016.

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

[3] 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.

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

[5] 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.

[6] N. Popper, "How china took center stage in bitcoin's civil war," The New York Times, June 2016.

[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.

[8] 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

[1] The most recent results, in Xu et. al[7], indicate that the GFW does record state