Bitcoin Blockchain Consensus: Fast and Secure Transactions

UNION COLLEGE

Dae Kwang Lee

Matthew Anderson, Advisor

Introduction

In Bitcoin, miners are incentivized to store transactions in a timestamped object, or a block. Ideally, each user stores a singly linked chain of blocks, or a single blockchain, as a transaction history. When the blockchain has multiple branches, or forks, the longest branch is the only valid history. However, if selfish miners collude to keep mining on top of a shorter branch and make it the longest, they can revert valid transactions and receive dishonest incentives.

Nakamoto Consensus vs. GHOST

The Nakamoto Consensus [1] is the current Bitcoin protocol. It resolves forks by selecting the longest branch as the main chain; the others are discarded.

GHOST [2] is an alternative protocol that instead selects the branch with the most blocks appended to it. The selection process of the protocols is described in Figure 1.

GHOST is faster in transaction processing but produces more forks. Thus, it is more vulnerable to selfish mining activity.

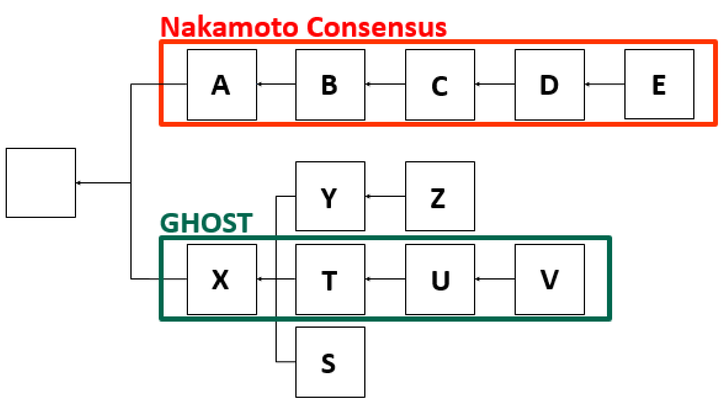

Figure 1. The Nakamoto Consensus selecting the branch rooted at block A, while GHOST choosing the branch rooted at block X

Research Question

Is there a policy that is as fast as GHOST and as secure as the Nakamoto Consensus?

New Protocol: HIRES

We extend GHOST and propose a new protocol, which selects the branch that contains the highest transactions fees, or residuals.

Intuition: Miners attempt to maximize their incentives, and therefore the selfish miners have remaining transactions with low residuals to catch up, results in lower probability of reversion. The protocol is described in Figure 2.

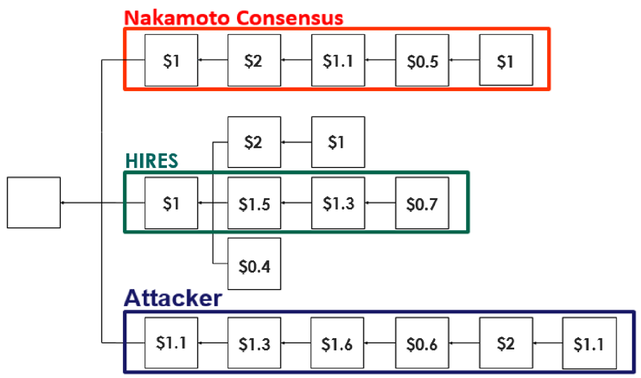

Figure 2. HIRES contains the highest residuals, so the attackers cannot revert the transactions even though their chain is longer

Method

Arthur Gervais's Bitcoin network simulator [3] is a single processor with 16 miner threads that models the Nakamoto Consensus. Our method is:

- Implement the GHOST protocol in the simulator
- Implement our new policy, HIRES
- Run the three protocols under honest mining and selfish mining by passing typical block parameters [4] [5] and extreme block parameters when there are 500 nodes and 100 blocks to be mined (Figure 3)
- Iterate each experiment 100 times
- Compare the efficiency and the security of the three protocols

	Typical		Extreme	
	Block Size	Interval	Block Size	Interval
Nakamoto	1 MB	10 Min	1 MB	6 s
GHOST	1.5 KB	10 – 20 s	1 MB	6 s

Figure 3. The Block parameters inputs for simulation

Result

The simulation result for honest mining is described in Figure 4. The result for selfish mining is described in Figure 5.

	Typical			Extreme		
	Blocks	Fork (%)	Delay (s)	Blocks	Fork (%)	Delay (s)
Nakamoto	94.97	1.93	23.21	57.51	68.05	93.82
GHOST	99.41	4.42	0.82	57.12	67.34	91.77
HIRES	98.12	4.64	0.81	58.23	68.16	93.52

Figure 4. The result for honest mining

	Typical			
	Blocks	Fork (%)	Selfish Blocks	Selfish Miner Profit (%)
Nakamoto	95.74	43.09	48.28	-45.29
GHOST	92.33	41.61	49.07	-29.76
HIRES	94.69	40.48	50.61	-30.17
	Extreme			
	Blocks	Fork (%)	Selfish Blocks	Selfish Miner Profit (%)
Nakamoto	97.96	43.67	49.52	-32.16
GHOST	89.51	40.29	50.17	-18.07
HIRES	88.63	35.68	49.84	-18.20

Figure 5. The result for Selfish mining

Analysis

We can observe that HIRES and GHOST are 30 times faster than the Nakamoto Consensus, but they are less resilient as they incentivize the attackers more than the current Bitcoin protocol does. In this experiment, we conclude that our hypothesis of higher forking rate leading to higher vulnerability is not optimal.

References

[1] Satoshi Nakamoto. Bitcoin: A peer-to-peer electronic cash system. (2008): 28
[2] Yonantan Sompolinsky and Aviv Zohar. Accelerating bitcoin's transaction processing. Fast money grows on trees, not chains. IACR Cryptology ePrint Archive, 2013(881), 2013.
[3] http://arthurgervais.github.io/Bitcoin-Simulator/
[4] Blockchain Charts. https://blockchain.info/charts.
[5] Etherscan. https://etherscan.io/chart/blocktime.