Problem Set 2	**6.857**	# 2-3 Scalability of Alternate Currencies
Ben Bitdiddle, Alyssa P. Hacker		April 11, 2014

(a) Block Propagation

Bencoin's transaction verification time of 1s per trasaction would have a drastic effect on block propagation. Since blocks must be verified for both their proof of work property and their transaction correctness before being passed onwards, the cost of verification will be done per node. For Bitcoin, this is quite fast: the mean time for 50% of nodes to see a new block in Bitcoin is between 4 and 6 seconds[1].

If Bencoin is used instead, then each transaction must be verified before the block is passed onwards. There are usually several hundred transactions per block, in order to fit the number of transactions in the targetted 10 min between blocks. This means that several hundred computation seconds must be spent verifying the transactions if we use a model of 1 s per transaction verification. This cost is spent per node, and several orders of magnitude above the estimated 11.37 seconds that is spent verifying the block by the entire network currently[2]. Even if the node can parrallelize this cost, it would still take longer than the Bitcoin average.

(b) Dishonesty & Bencoin

Bencoin would be a huge advantage to attackers. The reason for this is that Bitcoin is designed to have a average Block mining time of 10 minutes, which is much larger than the propagation delay of Bitcoin. If the propagation delay is longer, avenues for attack are opened for an attacker.

First, the miner of a block gets a head start on mining the next block while the other nodes are stuck validating the block. This means that group of malicious nodes would need less than the 50% that is traditionally cited as being the minimum percentage of malicious actors to allow a doublespending attack. Let's assume that a block is mined in 600 seconds of the Bencoin network's power, and that a block has 100 transactions which take 100 seconds per node to verify. For now, let's assume that propagation times are negliable. The effective computational power of the rest of the network is down by 100s/600s for mining blocks, to 83.3% after a block is found compared to the finder. This means that an attacker only needs 41.6% of the network's power to simultaneously mine a separate chain and double spend their coins.

If the propagation times aren't neglected, then the minority attacker would need even less of the computing power. An average propagation delay of 20s on top of the 100s verification

[1] $http://bitcoinstats.com/network/propagation/$

[2] $http://www.tik.ee.ethz.ch/file/49318d3f56c1d525aabf7fda78b23fc0/P2P2013_041.pdf$

time would drive down the effective computing power to 80%.

(c) Block & Transaction Verification

If we implement Alyssa's suggestion that we forward blocks before completing the transaction checks, it does improve the scalability of Bencoin, while still maintaining the protection scheme of bitcoin. This is because it is just as hard to mine an invalid block as it is to mine a valid block, so checking just block proof of work allows you to be sure that the block miner has done the necessary amount of work.

Since the work is necessary, it would make no sense for the attacker to add invalid transactions to their block, as they could have mined a valid block with those computing resources and gotten paid for it.

This proposal is interesting in that it has been proposed for Bitcoin, Bitcoin's propagation times are enough that only 49.1%[3] of the Bitcoin network is needed to mount a 50% attack.

[3] $http://www.tik.ee.ethz.ch/file/49318d3f56c1d525aabf7fda78b23fc0/P2P2013_041.pdf$

6.857 Network and Computer Security

Spring 2014