Assignment 3

Problem 1. Scalability of alternate currencies.

All information about transactions in Bitcoin are stored into blocks that are joined together to form the block-chain.

After receiving a new block each node in the network verifies (a) the proof-of-work property; and (b) that all ECDSA signatures corresponding to the transactions are valid. If both checks pass the block is propagated further, otherwise it is rejected.

Currently neither (a) nor (b) pose a CPU bottleneck, because cryptographic operations (SHA256, RIPEMD160 hash computations and ECDSA signature verification) involved in (a) and (b) are very fast.

Some proposed extensions to BitCoin (e.g. ZeroCoin and ZeroCash) would make BitCoin more anonymous, but all make transaction verification in part (b) more expensive. E.g. in ZeroCoin the fast ECDSA signature verification would be replaced by a much slower cryptographic checks.

Suppose that Ben Bitdiddle has invented yet another public-ledger based currency BenCoin, that works just like Bitcoin, but with slower transaction verification times.

(a) The transaction verification time for BenCoin is terrible: 1 second per transaction on a typical computer. What effects does this have on block propagation?

(b) Do dishonest minorities have easier time attacking BenCoin than they would have attacking Bitcoin? Why?

(c) Alyssa suggests to propagate block immediately after proof-of-work checks pass and then discard it (after sending it off to others) if transaction checks fail. Would this suggestion improve the scalability of BenCoin?