Alishan Hassan
December 7, 2015
Cryptocurrency Cabal

Encrypted, Anonymous, Network with Bandwidth Derived Cryptocurrency Rewards and Transactions

Formerly: A Bandwidth Based "Proof of Work"

Introduction

In this paper, I will attempt to describe a potential encrypted, anonymous, peer to peer, network that keeps track of bandwidth usage and rewards nodes for expending bandwidth necessary to keep the network running. The rewards are effectively a form of currency that can be used for transactions within the network by using the public address of each of the nodes in the network.

Motivation

In circles not familiar with cryptocurrencies, there is often resentment with the wasteful nature of Bitcoin's proof of work. People wonder, why should so many processing cycles, and therefore energy, be spent doing useless hashing? Why can't Bitcoin mining computations be used for something that's beneficial to humanity, such as protein folding or endeavors such as SETI@home? The reasoning is largely because the act of wasting energy is spent on making sure the Bitcoin network is secure and stable and provides a massive barrier of entry for any nefarious users willing to attack the network. The wasteful nature of the proof of work is intrinsic to the Bitcoin protocol. Running other computations compromises the integrity of the network.

Regardless, the motivation behind this project was to find some mathematical operation that could serve as an alternative proof of work. Some endeavors already attempt this, such as Gridcoin[1] which is linked to the Berkeley Open Infrastructure for Network Computing (BOINC). BOINC allows volunteers to contribute their computer's processing power to solve larger, usually research orientated, problems such as gene mapping. Gridcoin offers a cryptocurrency payment for those who mine by contributing to BOINC. So how does this work? Gridcoin still has a proof of work system that is run side by side with the BOINC computations. Anyone who runs just the proof of work system gets a small number of coins, and anyone who runs both the proof of work and BOINC receives significantly more coins. The problem inherent here is that security is weaker than in Bitcoin. It does not possess the same level of protection against double spend attacks that Bitcoin has. Furthermore, the idea behind Gridcoin is that they don't want to waste energy simply doing hashes, but the system, nevertheless, has to do a normal proof of work on the side, anyway. The result is an unreliable currency, wasted resources to keep the

[1] http://www.gridcoin.us/

unreliable currency running, and BOINC not receiving all the available computing power of the miners.

There have been other attempts at similar, more altruistic, alt-coins such as CureCoin, but they all suffer from the same drawbacks. My initial goal was to try and find some sort of function that could provide benefits similar to SHA-256. My thoughts revolved around atmospheric calculations as a basis, however the best ideas I could come up with would have the predictability benefit of SHA-256. Bitcoin miners, on average, add a new block to the blockchain every 10 minutes. This is very consistent and the difficulty can be adjusted to keep it this way. Any of my attempts would have had no predictability at all, which would be deeply problematic for a stable currency.

Thus, it was suggested that I investigate wasting other resources, besides energy. Storage was the first suggestion. In a way, one could be rewarded for opening up the extra storage on their hard drives for a cloud storage solution. This could be an excellent way to share files and store backups on the cloud, while rewarding people for providing storage (as opposed to paying a cloud storage service separately). There are a couple attempts at this already, such as PermaCoin[2] and storej. The former, however, acknowledges the importance of Bitcoin's proof of work and, instead, is supposed to be a modification of Bitcoin rather than alt-coin. It could potentially add decentralized storage to Bitcoin while maintaining Bitcoin's underlying incentives. Implementing a functionality on top of Bitcoin is certainly a way this project can go.

Ultimately, I chose to pursue the usage of bandwidth as opposed to energy. There are certainly some interesting things to consider about bandwidth. Some Internet Service Providers, such as Comcast, have begun to treat bandwidth like a limited resource. In some markets, users are limited to 300 GB of bandwidth per month in consumer applications. Thus, could bandwidth be used to back a currency? And, if it could be, how exactly would the bandwidth be expended by users?

Background

Let's consider an anonymous, encrypted, peer to peer, network. We can say it's similar to Tor (although Tor, technically, isn't strictly P2P) with encrypted data being sent from one node to a couple random relays before reaching an exit node that connects to a destination. The relays and the exit node are expending bandwidth to keep the Tor network running.

[2] Miller, et. al. "Permacoin: Repurposing Bitcoin Work for Data Preservation"