Proof of Idle

Feb 11, 2014 • tpd5bf

aka The Crypto-currecny Conservation Reserve Program

I think everyone here is familiar with the "proof of work" idea which started with hashcash and is the underlying way bitcoin forms consensus among mutually untrusted parties. The proof of work blockchain is cool, and it works, but at the same time, doesn't sit well with many people. "It's such a waste!" is a common reaction. Professor shelat mentioned trying to tie the proof of work to something useful rather than mindless SHA256, which has been tried with things like Primecoin. One idea I've had recently, and think may be viable, is something that would allow the Bitcoin (or other equivalent) network to remain safe while greatly reducing the total energy used (which right now is about 20 Peta-hash per second, and who knows how many megawatts). The basic idea is that mining groups can form a type of cartel with only minimal trust needed, and prove that while they have the capacity to work, they are instead idle.

In my simplified example scenario, there are 10 mining agents (A, B, C...), each making up 10% of the total network. 100 bitcoins are mined every day, and on average each group gets 10 per day.

A is paying 6 BTC a day in electrical costs, and so only nets 4BTC per day. A broadcasts a message: "I will turn off my mining center for 5 BTC per day." Were A to shutdown, the remaining 9 miners would each receive 11 BTC per day on average, after the difficulty re-adjustment. While no one miner would find it makes sense to pay off A, if 6 miners got together, they should take A's deal: they would pay the same amount in electrical costs as before, and receive slightly more bitcoin. Through a multi-signature transaction, miners B, C, D etc do not have to trust each other. People only need to trust that A is not mining. A can of course take the money and start back up, and B, C, D will have no recourse; thus the still working miners should only trust A for a limited time. They also must verify that A retains the mining capacity (the threat of mining), so they should also periodically let their agreement lapse, watch as A powers back up, observe the work A does, and adjust their willingness to pay for A to shutdown.

This does not negate the expense of building millions of "wasteful" computer chips (the capital expenses, or capex). This does however, mitigate the "wasted" electricity (operational expenses, or opex). When opex is small compared to capex (which is very likely the case for most miners today as new hardware is coming out at an exponential rate) there is little incentive to participate in the proof of idle system. This is because the capex is a sunk cost

which you must recover through mining. If A paid 40 BTC for his servers, and gained net 4 BTC per day after opex, he can pay off his capex in 10 days, and in 9-ish days with the 5 BTC income for idle hardware. If on the other had, his opex was only 1 BTC per day, and he had paid 90 BTC for the hardware, he would have to charge > 9 BTC per day to idle his equipment. That would require the near-unanimous participation of the competing mining power to buy him off, which is not practical. So, the opex to capex ratio is a good approximation of the portion of the network that needs to co-operate to pay someone to stay idle. This is independent of the potentially idle pool size.

This ratio may fall drastically later this year once mining hardware catches up with moores law, and only 22nm ASICs are used. Once that happens, operational expenses will become primary and a proof of idle system might work with a reasonably small portion of the total network agreeing.

There's all sorts of game-theory / economics stuff I haven't even thought about, like freeloaders (miner X who doesn't participate to pay off A still gets more coins). There's also the issue of what happens when A mines something ELSE, like a competing crypto currency. There's no easy way for A to prove the hardware is actually idle, just that it's not mining bitcoin. The total network also has to be fairly static for this to work on reasonable time scales: if pools are going +/- 5% every day, A going offline would be lost in the noise and unverifiable.

Anyway this might be a neat protocol to write up. The more I've thought of it, the more it seems like this could work, and may address one of the biggest complaints about bitcoin. Then again there could be serious holes in this whole idea, so please point any out, and maybe they can be patched... maybe not!

-Tadge

512 Rice Hall
Charlottesville, VA 22902
434-243-2145
abhi@virginia.edu

abhvious
abhvious