Decentralised Cryptocurrency Mining

A brief discussion about the ever increasing centralisation of cryptocurrency security and creation of wealth. A possible solution to the problem i.e. what can be done about it.

By Macca Spacca (Cryptocurrency Enthusiast)

BM-2cWn8aEqt11rruL6LeuS3MQ1Lho2w3nPq8

Date: 29th November 2015

Problem Overview

Cryptocurrency is intended to be decentralised in nature. Despite the original intentions and ideals of peer to peer cryptocurrency creators, there is an increase in tendency towards centralisation as cryptocurrency becomes more popular and more valuable. This has certainly held true for currencies that generate security and new coins using the traditional proof of work (POW) mechanism to secure the blockchain (e.g. Bitcoin, Litecoin et al). As the popularity and value of any particular cryptocurrency increases there is a tendency for POW mining to become increasingly more expensive, more specialised, consume larger amounts of energy and become more centralised as larger mining organisations mine against an ever smaller number of large mining pools. The end result is that the creation of new coins and therefore new wealth ends up in the hands of those who can afford to mine or operate large mining pools and not in the hands of ordinary cryptocurrency users (who have to buy their coins from the rich few rather than create new coins for themselves).

The tendency to centralisation is also increasingly true for currencies that use proof of stake (POS) mechanisms to secure the blockchain although this is a slower process and tends towards invididuals rather that mining groups or corporations. A quick examination of richlists of POS currencies shows small numbers of addresses owning large percentages of available coins and therefore capable of staking more often and in larger amounts. The net result is similar where only those who can afford to buy coins can accumulate a higher stake to produce new wealth effectively.

The end point in both scenarios (and even with hybrid POS/POW coins) is centralisation and the rich owning most of the wealth as well as most of the capability to create more wealth – just like the fiat currency mechanism that it is supposed to replace or be an alternative for.

When Gavin Andresen was explaining what Bitcoin was in December 2010 he stated "Bitcoin is the first peer-to-peer currency - it is money created by people instead of by a central bank or government."

(http://readwrite.com/2010/12/29/interview-bitcoin)

Note that Andresen clearly used the word "people" in his statement not "a few rich people" or "a few private companies". Here Andresen is reflecting a vision of peer to peer cryptocurrency as being fully decentralised and being created by individuals and not centralised organisations (that can easily be manipulated by governments or central banking bodies).

Below I have tried to propose a possible solution to the problem of centralisation of cryptocurrency wealth creation. I am not a developer and I am not outlining the technical solution to the problem. I am merely offering a mechanism by which centralisation can be reduced or discouraged enough to allow "people" to create currency as was originally intended.

The Possible Solution

The Aim

To provide a scenario where securing of a cryptocurrency blockchain and transactions is undertaken using an adapted proof of work methodology that encourages decentralised mining. This new methodology (as yet to be created, tested and developed) includes the requirement that mining rewards (creation of new coins and wealth) remains in the hands of individual people and users of the currency and not centralised mining pools and large mining operations.

The Scenario

The proposed scenario is that all mining for the as yet unknown / unnamed cryptocurrency will take place between wallet peers only. The wallet and coin code is constructed in such a way that mining can only take place using the built-in wallet mining software and the wallet of a peer on the network. In other words a wallet will only accept a single remote mining connection from the built-in miner of a suitable peer.

So, how does it work?

1. The wallet of the cryptocurrency is a normal wallet with built-in mining software. The algorithm for the coin is deliberately gpu / asic resistant, a mining connection only lasts for one block and can only take place between the built-in wallet miner and a remote peer wallet on a different external IP address. External RPC requests are only allowed for a mining connection and on a port chosen by the wallet receiving the connection (different from the normal RPC port).
2. When mining is enabled (setgenerate true) then the wallet receives a token or key from the network to allow it to mine (consensus from a set number of peers). The wallet will only receive a token if it complies with certain conditions that proves it is actually a valid wallet. The token also allows the wallet to receive a mining request from another wallet miner on the network.
3. Once the token is received the wallet then advertises or requests work across the peer to peer network. This is responded to by another wallet (which also has a token to mine on the network) and mining takes place.
4. Mining continues until a block is found. The reward for the new block is split between the miner and the wallet being mined against (80% to the miner and 20% to the wallet being mined against – or some other suitable proportion).
5. The mining connection is broken after a block is found and all parties then repeat the process to make new mining connections with different peers.

DN: email=maccaspacca@virginmedia.com
Date: 2015.11.29 19:57:49 Z