On the Power and Execution of Decentralization

Bitcoin Changed the Paradigm of Money

Money is not just money, it is power, it enables access to nearly everything in this world. When a centralized institution (eg. government, bank or anything else) has control over the flow of money there is an opportunity that presents itself to those in control. This ultimately is to take more for oneself than is deserved, according to the social contracts that exist. To put this situation in context, how many people do you know that always follow all the rules? Likely not many, if any. To some extent it is merely a desire to survive, and ensure future survival, that drives people to take actions for the benefit of themselves at the expense of others. This also is foreseeably inevitable without infinite resources.

Therefore the probability of excessive power leading to excessive corruption is relatively high, and we can easily see this in all social power structures, once the corruption has been revealed to the public. Humanity has been trying to combat this problem for hundreds of years. In government there has been a decentralization of power relative to monarchies in the form of democracy, as an example. Religions have been reformed in an effort to remove the access to excessive powers of persuasion. These updated social systems have helped move society to more efficient and more fair structures. Still, while a minority of people retain the majority of power, inevitably the corruption will trickle in. We see this in the private sector and the public sector, the common political argument that one is vulnerable to this, while the other isn't, is always a half truth. The true problem is centralized authority in the hands of a minority of people, that are prone to temptation.

In this context it is not surprising that money is one of the last social tools to be reformed. The invention of Bitcoin has resolved most, if not all of the systematic issues of centralized control technologically. The impact of this invention will inevitably be seen as a turning point in the history e-books of the future.

Proof of Work

Decentralized investment of resources that supports the Bitcoin infrastructure, is achieved through voluntarily incentivizing computational work through reward. This is called Bitcoin mining, and it is a proof of computational work (PoW) that determines eligibility for reward. This method enables a network consensus to be achieved and powered without central approval, or centralized resources. This as intended, has resulted in a vast competition of computational power to achieve the reward first for each given transaction block. The incentivized competition between miners however, has resulted in a consolidation of resources into mining pools to improve the odds of each miner receiving a reward for work. The effect of this has been a centralization of the transaction consensus process. There are numerous ways to address this short coming, and many are being tested and implemented currently. However the centralization of computational power is still a concern, and it is the weakest point of what is the most widely tested system of decentralized control.

On the Power and Execution of Decentralization

Proof of Stake

An alternative approach is called proof of stake (PoS). In PoS, the incentivized reward system is proportional to the percentage of the coin that is owned by a given wallet in the network. The advantage of this method is that there is little to no incentive to pool resources to increase the odds of receiving a reward. Primarily because the reward will always be relative to the total for each wallet. This currently in the case of VeriCoin results in close to half of all the coins continuously being measured for reward, and the largest wallet owned by an exchange, only containing 9% of the total coin. Or approximately 16% of resources on average maximally pooled. Compare this to proof of work coins typically approaching 50% routinely.

Markets, Ownership and Centralized Power Structures

One of the more important and less discussed challenges in preserving decentralization, which is important for both PoW and PoS coins, is ownership. Centralized ownership can have a direct impact on the decentralization of PoS coins, but also has an enormous role in the centralization of power, of PoW coins. In some ways this is an aspect of decentralized currency that is rarely addressed publicly, yet has an enormous effect on the real world decentralization of control.

A simple example is as such, if a coins technology is 100% decentralized yet the ownership is distributed such that 10 people own the largest aggregated share of the coin, then inevitably the market value, coin access, future distribution, application and so on, can be directly controlled by those 10 people. 10 individuals with excess power will more than likely be plagued with excess corruption. In this case the purity of the technology has little effect on the real world decentralization of power and control, and we are immediately back to square one.

This is why VeriCoin's emphasis is two fold. A decentralized, secure, proof of stake transaction core and the most accessible technology possible, for the largest number of individuals all over the world. This is why VeriSMS and VeriBit are so important, they remove entry barriers and improve the odds of decentralized ownership being dominant. Accessibility of use can enable an exponential adoption rate and preserve true decentralization of money, power and control. We plan to engage the world with this approach and believe it is the most efficient path to achieving true decentralization and ultimately enable voluntary access to the many.

Douglas Pike
effectsToCause