Bitcoin Suisse | Decrypt

November 5, 2019 | Season 1 Episode 16

The Benefits of Decentralization

Operating a decentralized, peer-to-peer electronic cash network such as Bitcoin comes with a great deal of complexity compared to centralized alternatives. Why should one care about decentralization? And how is decentralization measurable?

Written by Dr. Raffael Huber from Bitcoin Suisse Research
and Demelza Kelso Hays and Mark J. Valek from incrementum

Last week, the cryptocurrency community celebrated the eleventh anniversary of the Bitcoin whitepaper originally published by Satoshi Nakamoto on October 31, 2008. One of the drivers for the development of a trustless peer-to-peer electronic cash system was the failure of digital currencies that relied on a central authority to verify payments, such as *e-gold*.[1] Only a system devoid of a single point of failure – a *decentralized* system – could resist adversaries trying to take it down.

Today, decentralization is widely accepted as one of the key value propositions of cryptocurrencies. In a decentralized world, game-theoretical incentives take over the role of a central, governing authority. Economics of cryptocurrency protocols need to ensure that the network is stable if every participant acts in their self-interest.

> *"Decentralization is what allows Bitcoin to substitute an army of computers for an army of accountants, investigators, and lawyers."*
> *– Nick Szabo*

A decentralized network run and secured by thousands of computers around the world can guarantee availability – in fact, **Bitcoin has achieved more than 99.98% uptime since its inception** and 100% over the last six years.[2] Failure of one computer does not impact the network overall. Bitcoin is also uniquely **censorship resistant** – miners have no incentive not to include a transaction in a block. Even if one miner decided to block a certain transaction, others would step in, include it in a block they mined and collect the transaction fee. An additional advantage of decentralized systems is their improved collusion resistance: Coordination in a distributed network is harder than in centralized ones. This reduces the chance that a group of network participants (e.g. miners) is able to work together to gain a competitive advantage (e.g. through selfish mining[3]).

In view of the benefits of decentralization, trying to maximize it should be a priority for public blockchains. To do that, some methods of quantifying decentralization are required. Common measures of decentralization include node and miner distribution: Where are they located geographically? Who controls them? What software do the nodes run?

The last question brings up another aspect of

1. https://www.bitcoinsuisse.com/research/decrypt/the-recipe-for-trustlessness
2. http://bitcoinuptime.com/
3. https://arxiv.org/abs/1311.0243

decentralization – who is developing the code to operate the network? A look at currently active Bitcoin nodes shows that about 97% are running Bitcoin Core software.[4] Over the years, the Bitcoin Core github repository had 669 contributors,[5] with 15 individuals being responsible for at least 1% of the total commits. This indicates that developers have a relatively large influence on the network overall, potentially marking a bottleneck for network decentralization.

The high percentage of nodes running the same software also means that errors in the code will lead to significant disruptions of the network. The only two instances of Bitcoin "downtime" in 2010[6] and 2013[7] were related to such issues. To counteract this, multiple client implementations are required. In networks with proof-of-stake based consensus algorithms and *slashing* for faulty behavior,[8] running the same software as a large majority of the network bears additional economic risks – for Ethereum 2.0, eight different clients are being developed.[9]

China's Impact on Bitcoin

Recent news of The People's Bank of China's plans to release a digital currency has prompted investors to question the security of the Bitcoin network. If the central bank issues their own digital currency, will Chinese regulators still allow Bitcoin miners to mine in the Sichuan providence?

Measuring decentralization of the Bitcoin network by calculating the geographic dispersion of Bitcoin mining pools reveals that the lion's share, or 82.5%, of Bitcoin's hash rate is controlled by mining pools that are headquartered in China.[10] However, the actual miners contributing to these pools may be more globally distributed – mining outfits exist, for example, in North America and Iceland in addition to China.

Luckily, Bitcoin will survive even if China shuts down mining and mining pools within the country. Even if Bitcoin lost all of its mining power coming from China, the Bitcoin network would still have more than triple the hashrate of the next largest coin with the same hashing algorithm, SHA-256, namely Bitcoin Cash. However, Bitcoin Cash is also predominately mined in China and would also lose a significant amount of mining power if China outlawed mining.

Table 1: Bitcoin Mining Pool Statistics November 5, 2019.

Mining Pool	Hash Rate (EH/s)	% Total	Country
Poolin	19.07	20.98%	China
BTC.com	12.20	13.41%	China
AntPool	11.75	12.93%	China
F2Pool	11.75	12.93%	China
Unknown or <1%	8.64	9.5%	Unknown
Huobi.pool	5.10	5.61%	China
ViaBTC	4.88	5.37%	China
SlushPool	3.77	4.15%	Czech Republic
1THash&58Coin	3.55	3.90%	China
BitFury	3.55	3.90%	Georgia
BytePool	2.44	2.68%	China
BTC.TOP	2.22	2.44%	China
NovaBlock	2.00	2.20%	China

Source: BTC.com, Incrementum AG.

A theoretical risk to Bitcoin is that Chinese mining pool operators could mine on a secret chain that contains a double spend, and the miners that are in that pool would not even know that their mining pool operator is directing their hash rate towards a secret chain instead of the original chain. Once the mining pool has mined a longer chain, they could release the secret chain to the network, and force a chain reorganization. This is why Matt Corallo and other Bitcoin developers propose to change the way Bitcoin mining pools interact with Bitcoin miners. For example, Betterhash is a protocol that gives Bitcoin miners control over what transactions are included in the blocks that they mine for mining pools.

Despite this theoretical risk, the practical risk is very low because a successful double spend attack would decrease the confidence in Bitcoin's security model, and the potential negative impact on the price of the cryptocurrency would damage the business model and profitability of the miner in the long run. Also, a mining pool operator that shows this sort of malicious behavior would quickly lose support by individual miners. Miners would switch to a different pool by redirecting their hashrate towards the new pool.

4. https://coin.dance/nodes
5. https://github.com/bitcoin/bitcoin/
6. https://bitcointalk.org/index.php?topic=822.0
7. https://github.com/bitcoin/bips/blob/master/bip-0050.mediawiki
8. https://www.bitcoinsuisse.com/research/decrypt/staking-on-chains
9. https://docs.ethhub.io/other/ethereum-2.0-ama/
10. https://btc.com/stats/pool?pool_mode=month

Additionally, such an endeavor would require a fair amount of coordination between miners. Despite their geographical co-location, such collusion in decentralized systems is still hard and a prerequisite for it would be the perfect alignment of incentives.

How much decentralization is enough for real-life purposes can only be proven in practice. The current architecture of major cryptocurrencies seems sufficient to provide many of the benefits of decentralization, such as high network availability and censorship resistance. In the future however, as adoption grows and regulatory frameworks solidify, we might get a better idea which models actually prevail under the test of time.

> *"Gradually, decentralized trust will be accepted as a new and effective trust model. We have seen this evolution of understanding before – on the Internet."*
> *– Andreas Antonopoulos*

Bitcoin Suisse AG
CH-6300 Zug
bitcoinsuisse.com

in collaboration with

incrementum