Measuring Bitcoin's Decentralization

coinmetrics.io/measuring-bitcoins-decentralization

September 15, 2020

By Karim Helmy and the Coin Metrics Team

Key Takeaways

- Bitcoin's decentralization can be quantified in terms of supply dispersion, hashpower distribution, and exchange consolidation, among other metrics.
- Key metrics like the number of active addresses and the network's hashrate continue to rise.
- Bitcoin's supply is becoming more evenly dispersed, and the mining and exchange markets remain competitive.

Introduction

Over the last eleven years, Bitcoin has managed to function relatively seamlessly in the face of a large number of threats, largely due to its lack of a single controlling entity. This trait, known as decentralization, encompasses a large number of loosely-coupled characteristics. Some of these traits are difficult to describe and measure, but others lend themselves well to direct analysis.

One directly observable feature is the dispersion of funds across addresses. The distribution of wealth is a critical factor in any economy, roughly coinciding to the distribution of economic influence. For cryptoassets, which often grant large token allocations to the founding team, it's also a severely underexplored one.

Another characteristic, the distribution of hashpower, is arguably even more important. Bitcoin relies on decentralization at this level in order to meet its goals of sustaining a secure, censorship-resistant payments and savings system.

Bitcoin is also highly exposed to the market share distribution of exchanges, which exercise an outsized influence on the network's economy. The distribution of volume on fiat-quoted spot pairs is particularly important, since these represent on- and off-ramps to and from the world at large.

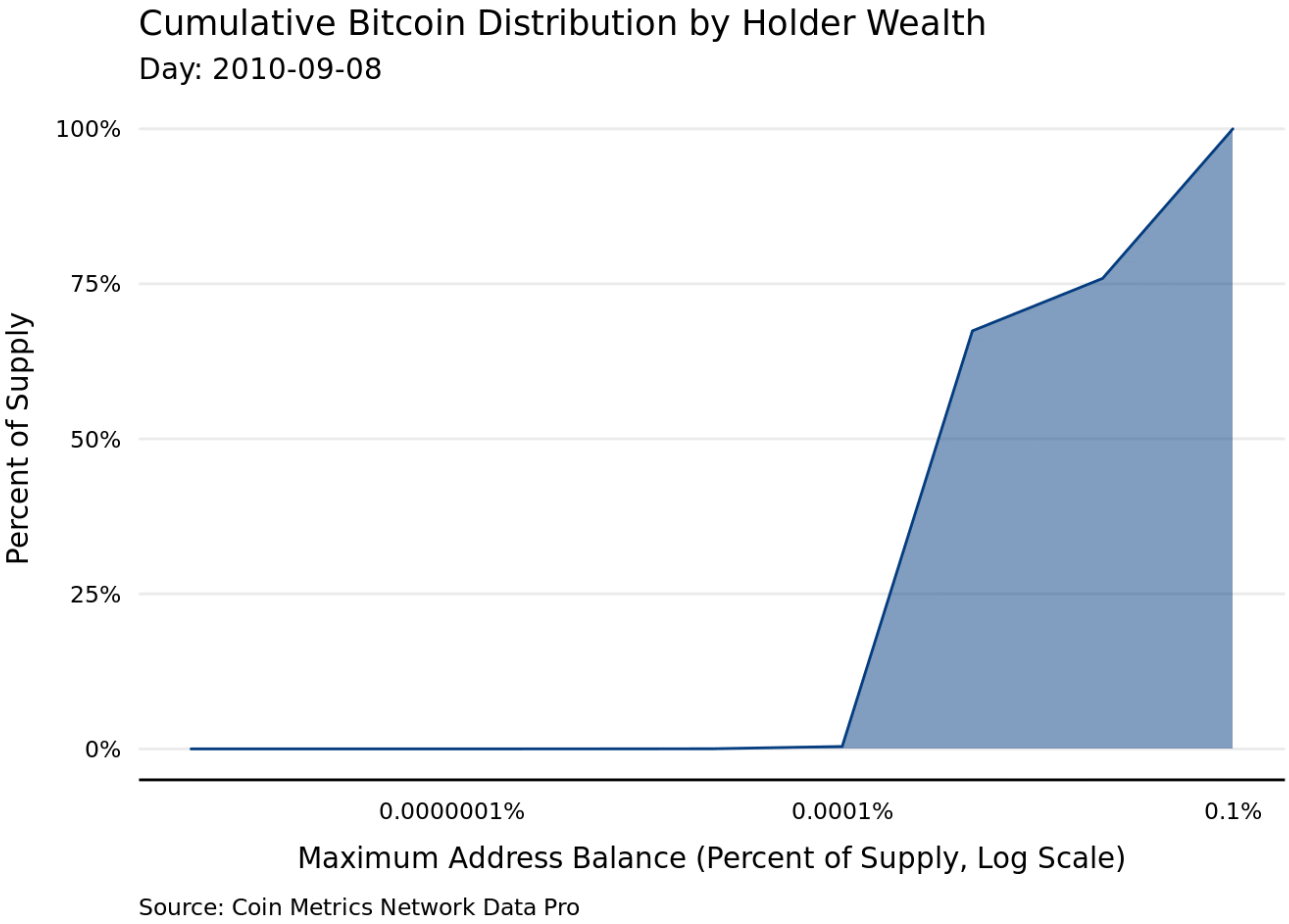
In this week's feature, we'll quantify Bitcoin's decentralization along these three verticals and track how it's progressed over time.

Dispersion

The presence of whales, or users with large quantities of funds held in the asset, is a concern for the viability of many cryptocurrencies. A particularly unequal distribution of funds could grant a small set of users significant influence over the direction of an asset's markets and protocol development and call into question the asset's viability as a store of value or medium of exchange.

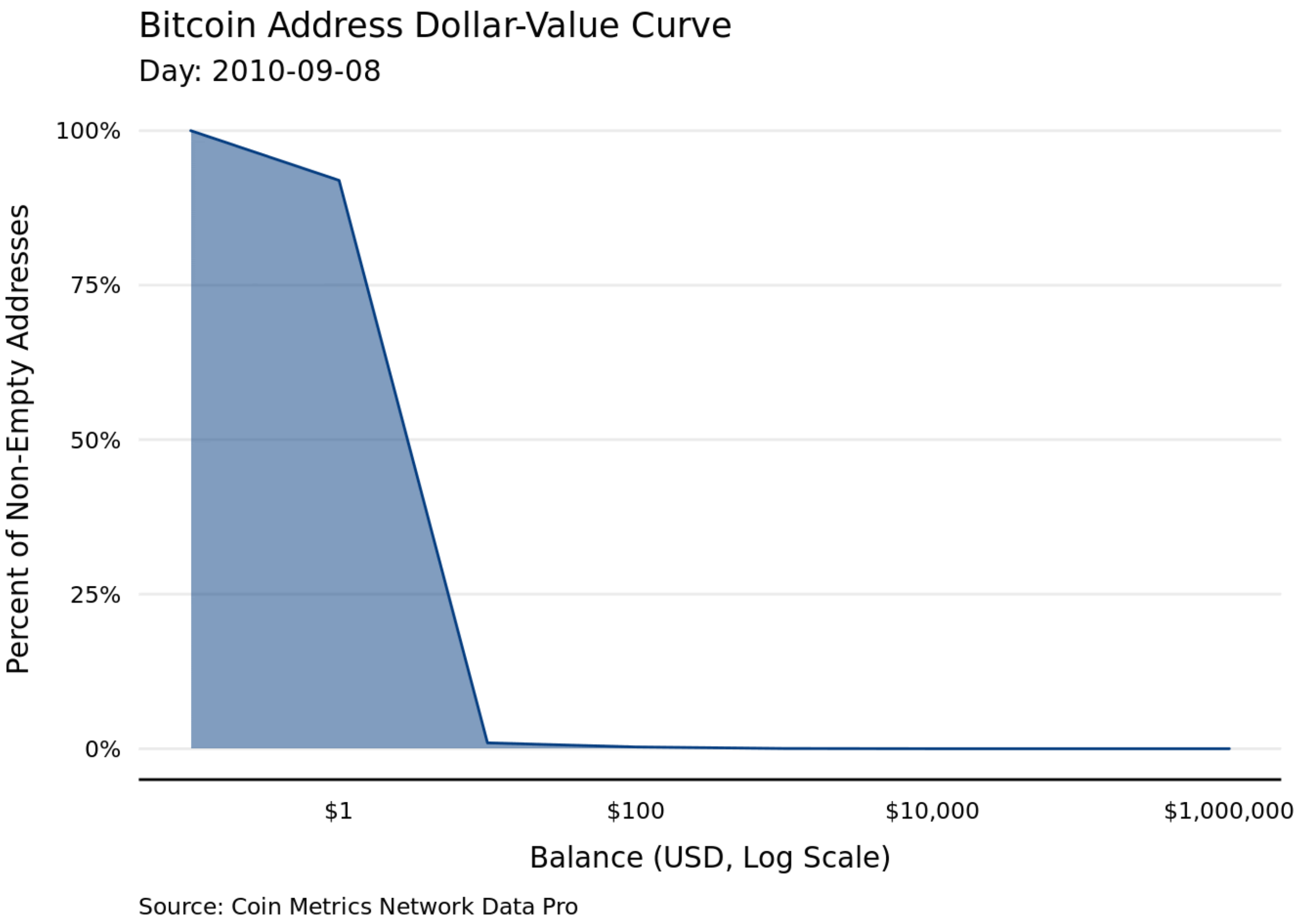
Since Bitcoin balances are easily auditable, dispersion can be assessed with on-chain data. Because funds held by custodians in omnibus accounts cannot be attributed to their owner and address reuse is generally discouraged, these estimates are imperfect. However, the degree of transparency afforded is still unprecedented when compared to the legacy financial system.

Bitcoin still has whales, but since the network's inception, its supply has become more evenly distributed, with smaller accounts comprising an increasing proportion of the aggregate supply.



Source: Coin Metrics Network Data Pro

In addition to controlling an increasing proportion of supply, addresses with smaller balances continue to represent the majority of accounts. In the face of a fluctuating dollar-denominated price, most addresses still control less than $100 worth of Bitcoin.

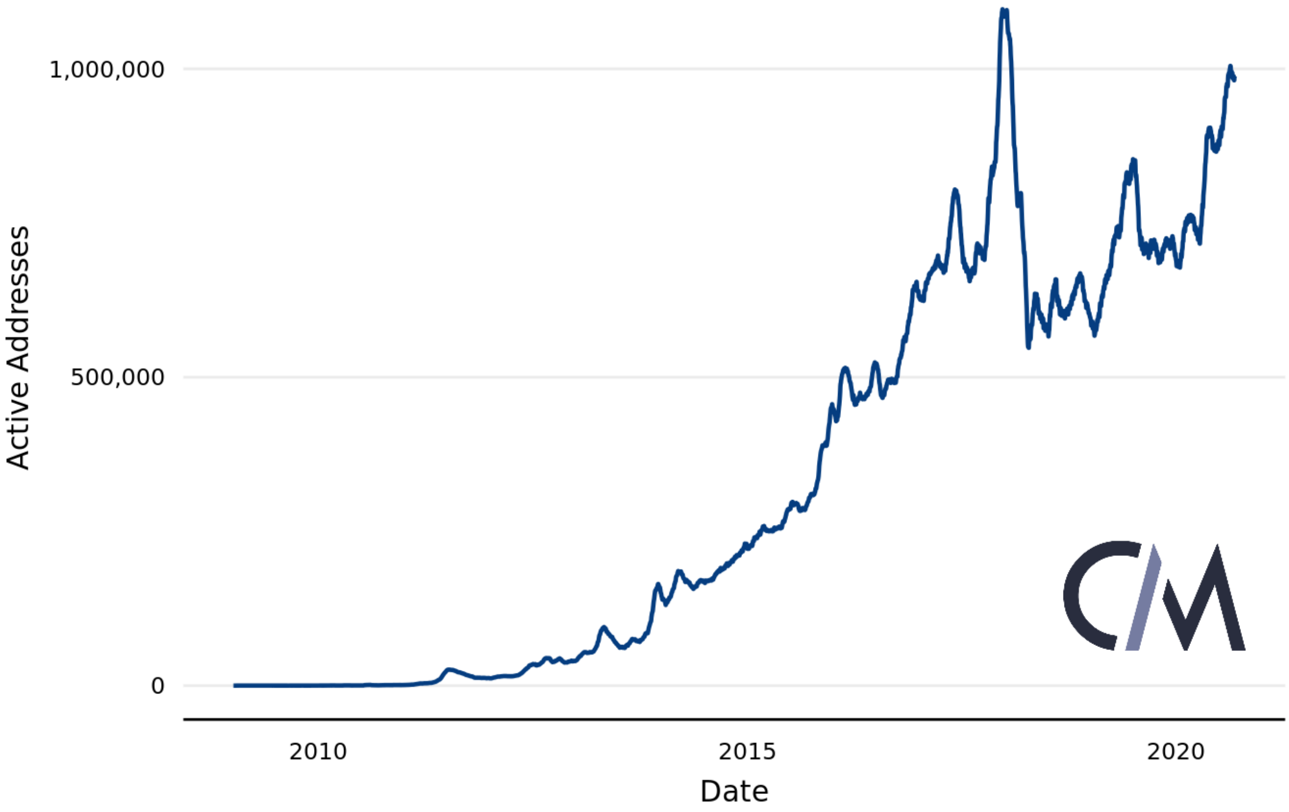


Bitcoin Address Dollar-Value Curve

Day: 2010-09-08

Source: Coin Metrics Network Data Pro

A closely related metric, the number of unique active addresses, also hints at usage by a broader set of network participants. Because a single user can control multiple addresses, this metric is not a perfect proxy for the number of participants, but is generally considered to be correlated. Recently, Bitcoin’s active address count has begun to approach all-time highs.



Active Bitcoin Addresses, 30-Day Moving Average

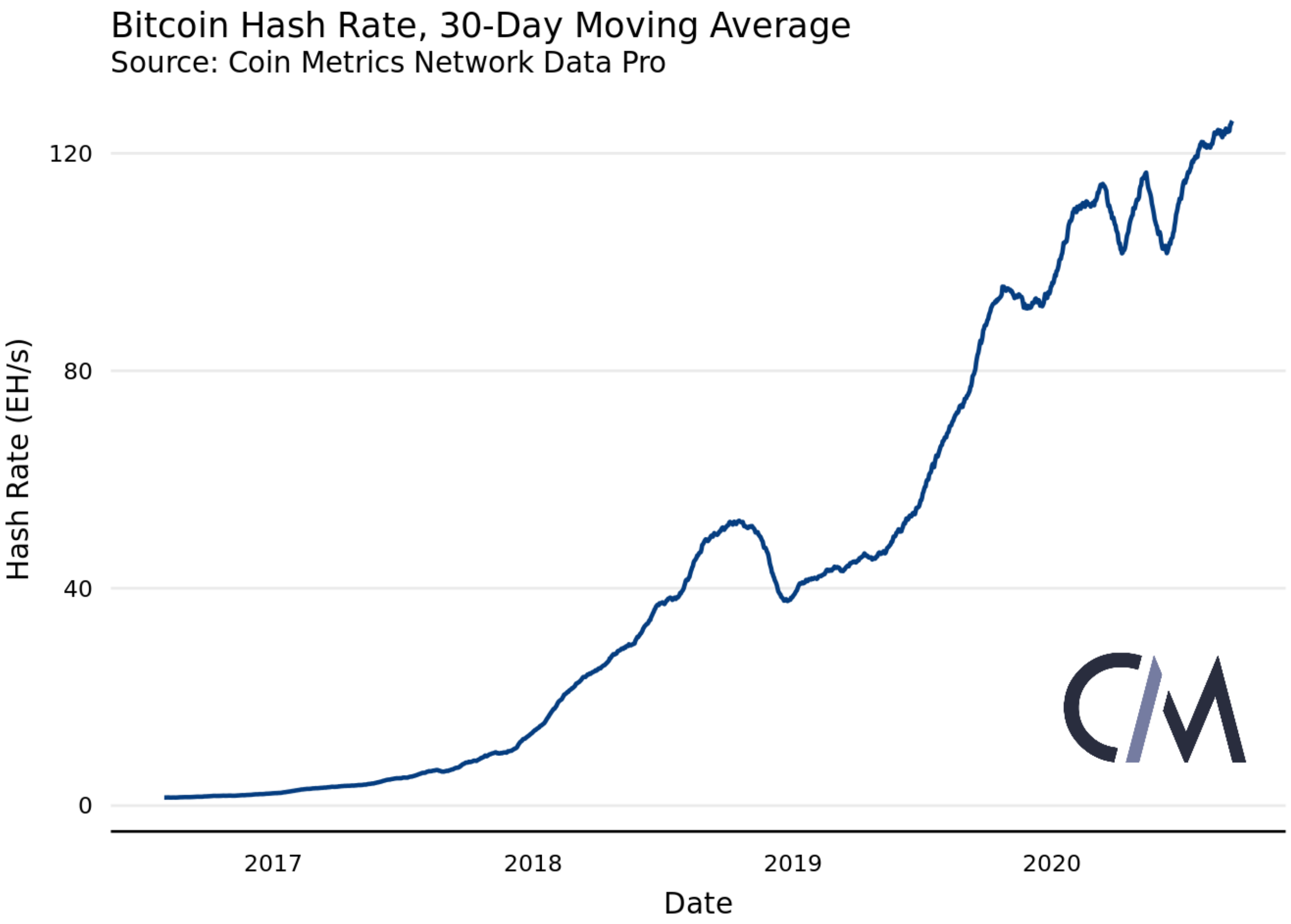
Source: Coin Metrics Network Data Pro

Mining

In addition to on-chain dispersion and activity, Bitcoin's effective decentralization depends on the distribution of computational power, or hashpower, among miners.

Bitcoin relies on miners to secure the network and add new blocks to the blockchain. These miners compete to find the next block by computing a large number of energy-intensive hashes, and often aggregate into loose coalitions known as mining pools.

The amount of hashpower securing the Bitcoin network has generally grown exponentially throughout the network's history.

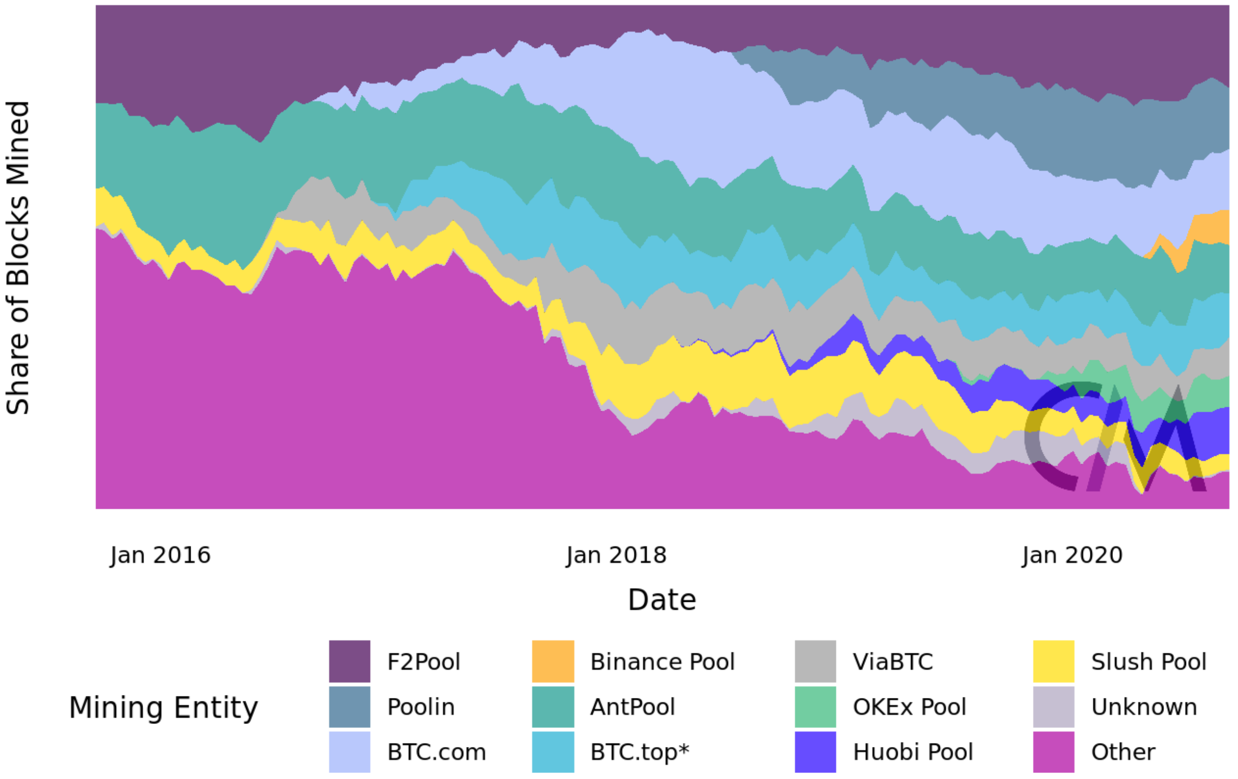


Source: Coin Metrics Network Data Pro

In addition to the amount of raw hashpower securing the network, the distribution of hashpower is also important. A malicious actor who controls more than half of the network's hashpower could 51%-attack the network and perform a double-spend, and an attacker with considerably less resources could censor transactions through feather forks.

An attacker would need to double-spend a large amount of money in order to make a 51%-attack profitable. In majority-hashpower ASIC-mined coins like Bitcoin, which require significant capital expenditure by miners, it would be difficult for a rational miner to perform a 51% attack, though these attacks are made somewhat more feasible by the presence of hashpower marketplaces.

Today, Bitcoin's mining industry is competitive. The plot below, which is subject to a degree of survivorship bias, shows mining to be a thriving, distributed ecosystem.



Bitcoin Miner Dominance by Difficulty Period
Source: Coin Metrics

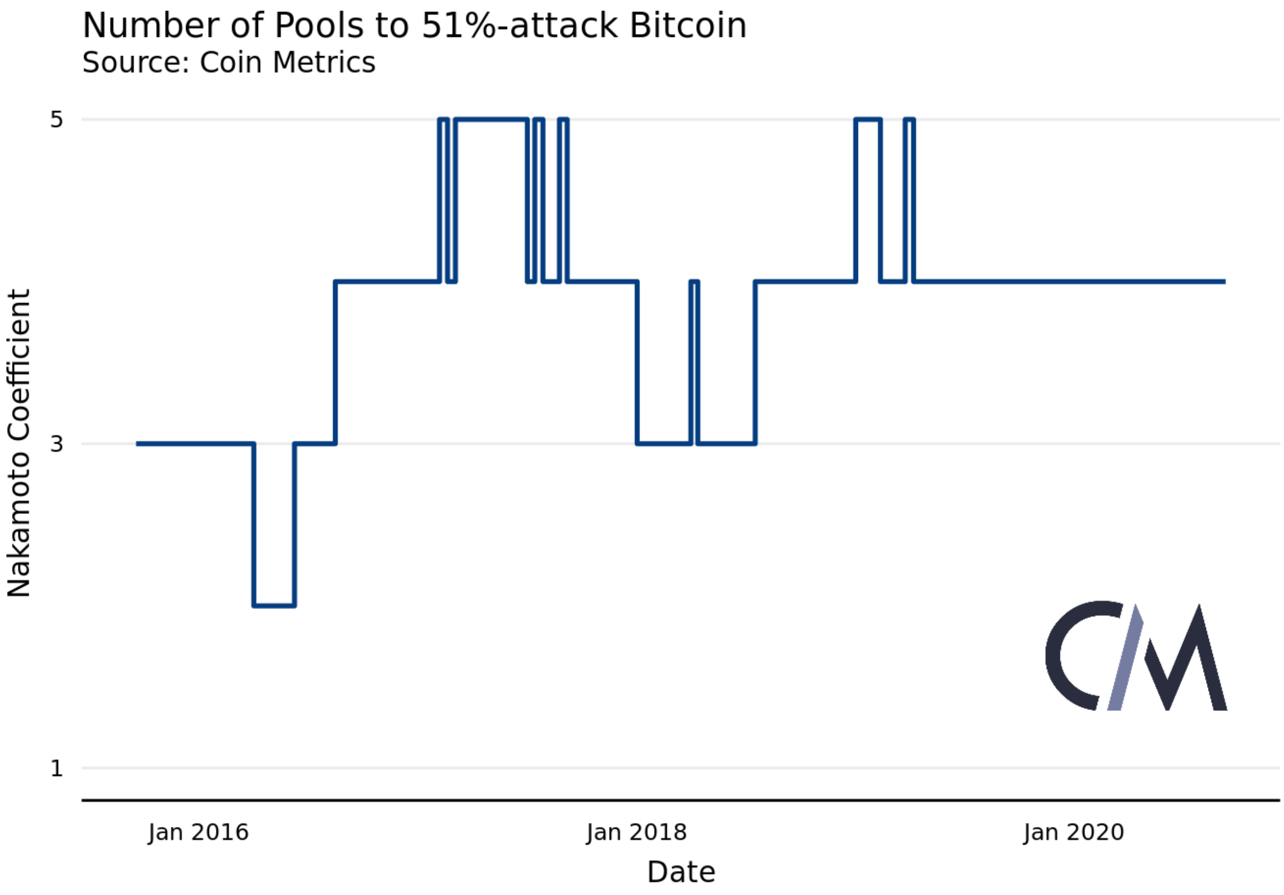
* Also includes 1THash&58Coin, an affiliated pool with shared on-chain custody.

While Bitcoin mining is distributed, it’s still at risk of centralization through state-level coercion and vertical and horizontal integration. Several exchanges, including Binance, OKEx, and Huobi, operate mining pools. BitMAIN, a hardware manufacturer, owns both BTC.com and AntPool, and is the only investor in ViaBTC.

Even a rational, well-resourced mining pool could have difficulty coordinating a 51% attack, since miners could leave the pool if the operator decided to attack the network. New coordination protocols like Stratum V2 may significantly increase the network’s decentralization by shifting control over block composition from pool operators to miners.

One useful metric for gauging the decentralization of hashpower is the Nakamoto coefficient, which measures the number of pools that would need to collude in order to 51%-attack a network. While Bitcoin has never been successfully 51%-attacked, in 2014 the mining pool GHash.io controlled over half of the network’s hashpower for about a day. During this time period, Bitcoin had a Nakamoto coefficient of 1.

Today, Bitcoin has a Nakamoto coefficient of 4, indicating a significant degree of decentralization.



Aggregated by difficulty period.

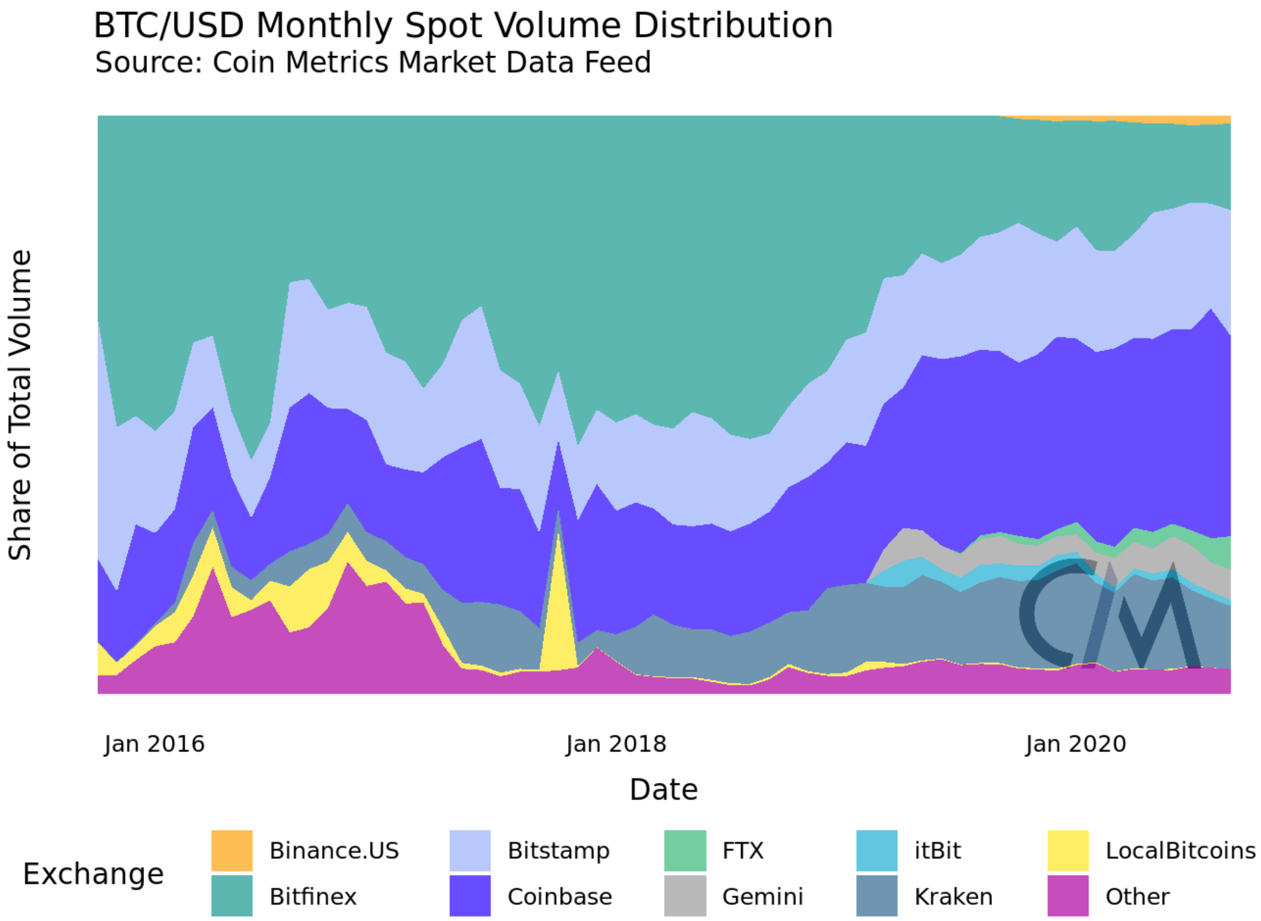
Exchanges

Exchanges have a less direct impact on Bitcoin's decentralization than miners, whose role is embedded in the protocol. As the primary markets on which Bitcoin is acquired and used, however, their influence on the network is significant.

Excessive centralization among exchanges exposes the market to systemic risks in case of insolvency. In the cryptocurrency space, the most well-known example of this is the 2013 Mt. Gox crisis, discussed in depth in SOTN Issue 35.

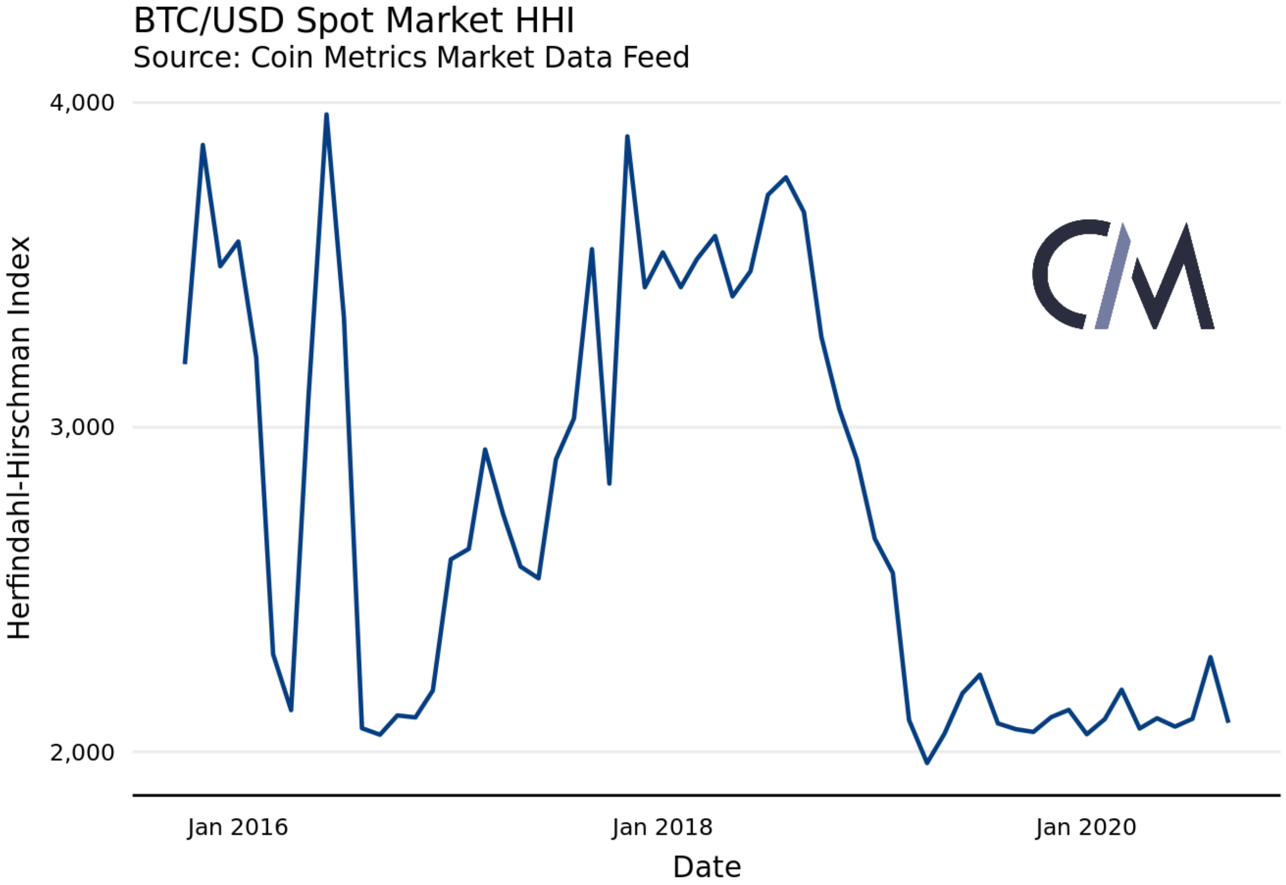
Consolidation would also increase the potential for censorship, negating one of the primary benefits of using Bitcoin. As the primary on-ramp from fiat to Bitcoin, the BTC/USD market is particularly important in this regard. While stablecoins have recently emerged as an alternative quote asset, fiat gateways remain a crucial way for new capital to enter the market.

While several exchanges offer trading on the BTC/USD market, the field is generally dominated by a few large players.



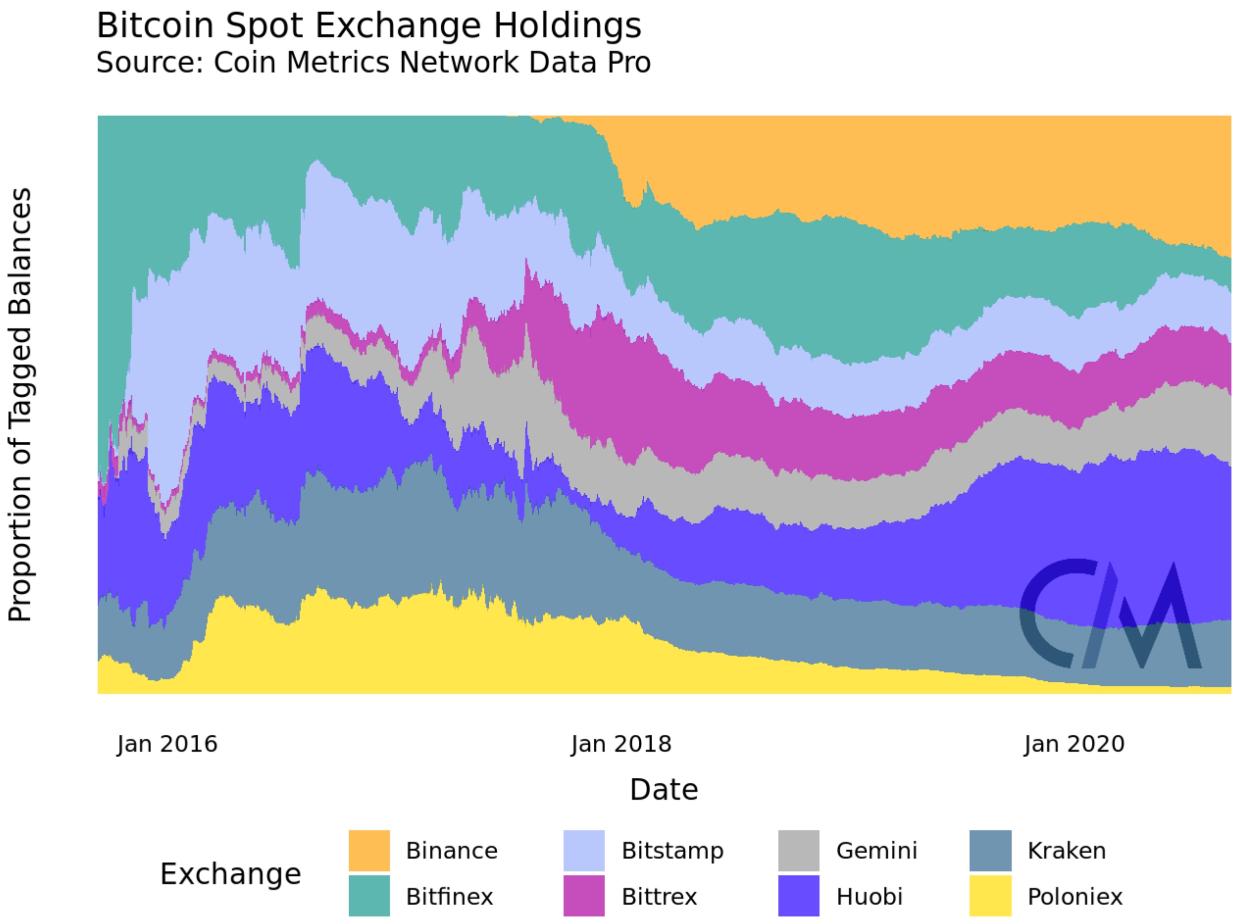
Source: Coin Metrics Market Data Feed

A useful metric for analyzing market concentration is the Herfindahl-Hirschman Index (HHI), which increases as a market becomes more monopolistic. While our estimates are subject to survivorship bias, the HHI of the BTC/USD spot market across Coin Metrics' coverage universe has remained flat over the last year, having dropped significantly prior to that. Currently, the market is considered moderately consolidated according to this metric.



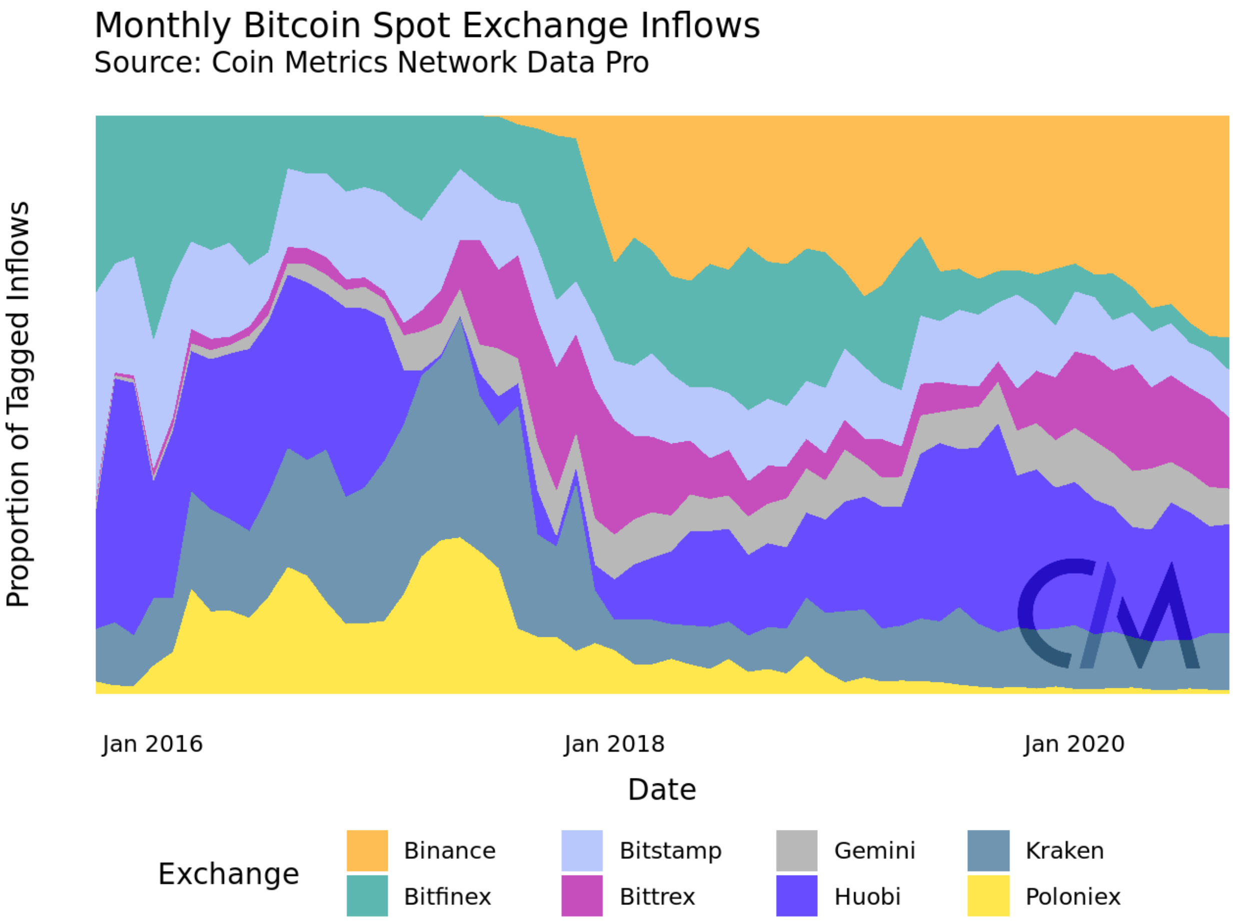
Calculated using monthly dollar volumes across Coin Metrics' coverage universe.

In addition to reported volumes, on-chain holdings offer another glimpse into the state of the industry. The comparative balances of the spot exchanges tracked by Coin Metrics' exchange flows are shown below. Coinbase is notably excluded from these estimates due to the company's avoidance of hot-wallet address reuse.



Source: Coin Metrics Network Data Pro

In a similar vein, tracking exchanges' on-chain flows enables us to form a more complete view of the market and confirm reported activity. These metrics also paint the picture of a relatively competitive marketplace. Inflows for the spot exchanges tracked by Coin Metrics' exchange flows are shown below; the behavior of outflows is very similar.



Monthly Bitcoin Spot Exchange Inflows

Source: Coin Metrics Network Data Pro

Conclusion

Bitcoin is meaningfully decentralized in terms of miner and exchange concentration, and its supply is increasingly evenly-dispersed. This analysis of Bitcoin’s decentralization is far from comprehensive, and various other metrics, such as node count and hardware manufacturer market share, should also be considered in assessing network’s health. On the whole, however, the network’s performance in these key verticals gives reason for cautious optimism.