Portfolio Media. Inc. | 111 West 19th Street, 5th floor | New York, NY 10011 | www.law360.com
Phone: +1 646 783 7100 | Fax: +1 646 783 7161 | customerservice@law360.com

Crypto-Mining Pools, Chips May Prompt Antitrust Concerns

By **Marc Martos-Vila** (September 16, 2019, 3:52 PM EDT)

Marc Martos-Vila

Cryptocurrency mining is a fundamental piece in cryptocurrencies and the blockchain technology.

As Chinese manufacturer Bitmain Technologies Holding Co., one of the largest producers of chipsets used in mining, is reportedly among a handful of notable companies that could **go public** this fall, it is important to understand some of the competitive aspects in cryptocurrency mining. I will focus on Bitcoin mining even though this analysis is relevant to other cryptocurrencies.

Previously, I discussed the views around the notion that cryptocurrencies and their underlying blockchain technologies can modify the payments system toward a more decentralized one, and what that might imply for competition and antitrust.

To review some basic concepts, Bitcoin's technology rests on a decentralized public ledger with the history of all transactions involving this coin. This shared database is decentralized in the sense that no centralized financial institution verifies and stores the transactions in the financial institution's private ledger. In Bitcoin transactions, the verification is done through miners who store transactions in this publicly shared, yet anonymous, ledger.

How does this process work? Miners, using computing power as an input, try to solve a mathematical puzzle involving hashes.[1] The outcome of the puzzle is the verification of a series of transactions that are grouped in a block — hence the term blockchain. After the block is published, other miners offer consent on the block as part of mining a new block.

For Bitcoin and other cryptocurrencies, this process is called proof of work, or POW.[2] To put it in simple terms, when we compare the blockchain system and the traditional banking system, we realize that the traditional system relies on us trusting that our money is safely stored in the bank's ledger. In contrast, Bitcoin provides safety (1) using a process that involves solving a cryptographic puzzle, and (2) logging payments in a permanent and irreversible manner. In addition, the dispersed nature of the public ledger makes tampering more difficult.

Mining Profitability

The supply of mining depends on profitability, which is driven by revenue and cost. Revenue is obtained by whoever successfully mines a block — in essence, only one miner wins the race. If the miner successfully mines a block, the revenue she receives generally consists of two parts: (1) fees associated with the transactions in the block, and (2) a reward of newly created bitcoin determined by Bitcoin's protocol.

In 2018, the reward was 12.5 bitcoins per block mined. Therefore, an increase in Bitcoin's expected value will increase the expected payoff to the miner. Similarly, an increase in the

likelihood of mining a block will also increase the expected value to the miner. Both factors would make mining more attractive, everything else equal.

Given the POW process, it follows that mining costs come mainly from the fact that it takes computing power to successfully mine a block. To give some sense of what computing power means here, the amount of electricity consumed by Bitcoin mining worldwide has been estimated at 61.4 TWh annually in 2018, equivalent to 1.5% of the electricity consumed in the U.S.[3] Better mining technology could, in theory, lower time consumed and cost. However, Bitcoin's protocol keeps adjusting the puzzle's difficulty such that it takes approximately 10 minutes to mine a new block.[4]

The profitability factors listed above and other economic forces are partly behind a host of new products and services, which are reshaping the competitive landscape in cryptocurrency mining. We will focus on two: mining pools and mining chips.

Mining Pools

There are companies that pool the efforts of several miners and share the payoffs received by the pool. These are called mining pools. This arrangement is valued by miners because it reduces the risk of no payoff. In that respect, pooling acts like insurance. Therefore, instead of a high payoff with a small chance, miners obtain a lower payoff with a larger chance as compared to solo mining.

Over time, mining pools have become increasingly relevant compared to solo mining.[5] Mining pools have increased from 5% of all mining power to close to 100% in just four years. This indicates that miners find pooling preferable and beneficial, according to a recent paper.[6]

Pooling could result in recentralization of the blockchain process, which goes against the notion of Bitcoin as a decentralized ledger.[7] In fact, a single pool could potentially dominate mining. This possibility would have implications both for the security of the cryptocurrency, and for competition. In terms of security, industry experts have argued that a mining pool with 51% or more of the mining power could compromise the security of the blockchain.[8]

Some economists suggest that recentralization worries are unwarranted.[9] They argue that miners are free to switch pools whenever they deem appropriate, which limits the emergence of one dominant pool. This is because if risk sharing is the reason miners to participate in a mining pool, they can also do that by participating in several pools at the same time. To achieve the benefits of risk sharing, the pool does not need to be too large. Furthermore, they argue that larger pools tend to charge bigger transaction fees, which slows their growth over time compared to smaller pools.

Drawing a conclusion on pools, there are currently different views regarding the effect of mining pools on competition. There are those that think pools will make mining more centralized and those who think market forces put a limit to the dominance of any particular mining pool.

ASICs and Bitmain

Application-specific integrated circuits, or ASICs, which are chips specifically designed for mining a specific cryptocurrency, can be more efficient and increase the likelihood of success, compared with other forms of mining.[10]

ASICs also contribute to shaping the competitive landscape in cryptocurrency mining, although industry players disagree as to whether ASICs promote mining centralization or not.

Jihan Wu, co-founder of Bitmain, argues that ASICs avoid centralization, while other industry commentators argue the opposite. Wu's argument is that ASICs' specialization in one cryptocurrency makes it costlier for a miner to reach 51% of the power.[11] On the other hand, those who claim ASICs promote mining centralization argue that ASIC manufacturing is in the hands of too few companies.[12]

The case of Bitmain is worth additional commentary. The company holds a 75% market share in mining ASICs, according to the information released during Bitmain's first attempt to go public in Hong Kong's exchange market.[13] This share is large. Furthermore, it also owns two of the largest mining pools: BTC.com and AntPool. The question that might arise in the case of Bitmain is whether the combined market power in ASIC manufacturing and mining pools might pose antitrust concerns.

Bitmain has already been subject to litigation. In 2018, a lawsuit was filed against Bitmain alleging that together with other industry participants, it **conspired to manipulate** a vote on a software update for the blockchain of a cryptocurrency called Bitcoin Cash. The vote was necessary in order to choose between two versions of the update, and would leave "the rejected version incompatible and forced into a new, separate chain." The plaintiff argued this conspiracy favored one software update over the other, causing antitrust harm. In contrast, Bitmain argues the vote was the product of vigorous competition. This case is currently pending.

To conclude, the competitive landscape in cryptocurrency mining is in constant change. Considering that (1) the price of cryptocurrencies, (2) mining difficulty, and (3) underlying mining technologies do all change, so does the level of competition and the need to pay attention to any potential antitrust concerns.

Marc Martos-Vila, Ph.D., is a senior economist at Econ One Research Inc.

[1] For a high-level description of some of these concepts, see Campbell Harvey, Wolfgang Hardle and Raphael Reule, "Understanding Cryptocurrencies." IRTG 1792 Discussion Paper 2018-44. March 26, 2019.

[2] Rainer Böhme, Nicolas Christin, Benjamin Edelman and Tyler Moore, "Bitcoin: Economics, Technology, and Governance," Journal of Economic Perspectives 29 (2), pp. 213-38, Spring 2015.

[3] Sherman Lee, "Bitcoin's Energy Consumption Can Power an Entire Country — But EOS Is Trying to Fix That." Forbes Magazine. April 19, 2018. https://www.forbes.com/sites/shermanlee/2018/04/19/bitcoins-energy-consumption-can-power-an-entire-country-but-eos-is-trying-to-fix-that/.

[4] Böhme et al. (2015).

[5] Lin Cong, Zhiguo He and Jiasun Li, "Decentralized Mining in Centralized Pools," NBER Working Paper No. 25592, February 2019.

[6] Cong et al. (2019).

[7] For a characterization of bitcoin, see Satoshi Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System," https://bitcoin.org/bitcoin.pdf.

[8] Böhme et al. (2015).

[9] Cong et al. (2019).

[10] https://en.bitcoin.it/wiki/ASIC.

[11] Wolfie Zhao, "Bitmain's Jihan Wu: ASICs Are Making Ethereum More Decentralized," CoinDesk, April 17, 2019. Available at https://www.coindesk.com/bitmains-jihan-wu-asics-are-making-ethereum-mining-more-decentralized.

[12] Nathan Reiff, "Why Centralized Crypto Mining Is a Growing Problem," Investopedia, Aug. 13, 2018. Available at https://www.investopedia.com/investing/why-centralized-crypto-mining-growing-problem/.

[13] David Floyd, "Bitmain By the Numbers: An Inside Look at a Bitcoin Mining Empire," CoinDesk, Sept. 28, 2018. Available at https://www.coindesk.com/bitmain-by-the-numbers-an-inside-look-at-a-bitcoin-mining-empire.
