# CHAPTER SIX
# Why Decentralization Has No Value in Bitcoin

| CRYPTO CONSENSUS VIEW | UNBOUNDED CAPITAL VIEW |
| --- | --- |
| Decentralization is necessary to achieve trustlessness and censorship resistance. Decentralization also is necessary for Bitcoin's security. This makes decentralization essential to Bitcoin's value. | Decentralization is not necessary for Bitcoin's security or proper functioning. Bitcoin's security is economic and not dependent on decentralization. |

In the opening sentence of their essay "**New Models for Token Distribution**," Multicoin Capital states that "Crypto networks are supposed to be decentralized". At Unbounded Capital, we would argue that decentralization is not needed or even important for Bitcoin to be successful. In light of the magnitude of this statement, it is necessary to closely examine what value decentralization has to Bitcoin. We have already identified trustlessness and censorship resistance as unnecessary or even poor goals for Bitcoin, so promoting decentralization to achieve these qualities cannot be the justification. However, are there other ways in which centralization of mining would negatively impact Bitcoin's reliability, security, and general proper functioning?

To consider this question, we decided to pose a thought experiment. Since centralization is typically discussed within the context of mining and efforts to promote

decentralization impact the mining process, it is interesting to consider what Bitcoin would be like under a mining monopoly. We can consider the mining monopolist condition to be a situation where anyone can mine, but only one company engages in mining. What would the problem be with the monopolist miner? The answer to that question makes the value of decentralization very clear. How could a monopolist miner use its position to harm or destroy the value of Bitcoin, and would it?

## WHAT CONSTRAINS THE MONOPOLIST MINER AT SCALE?

Before diving into what risks a monopolist miner poses, it is worth examining what forces constrain the monopolist miner. In the history of Bitcoin, technical restrictions on miner power have been given the most attention. In actuality, there is little to no technical restraint on the monopolist miner. A miner willing and able to ignore the protocol can do anything. While cryptography can prevent a miner from signing a valid transaction stealing coins, the miner can just accept an invalid transaction stealing coins instead. If the monopolist miner wants to mint 1,000 new Bitcoins per block, there is no technical limitation that prevents this. This malleability of code is what makes reassigning coins per court order a possibility. The restraints are not technical.

So what restrains the monopolist miner? Many things, but in general, self-interest. To be more specific, economic loss to competition, economic loss from a reduction in business, and economic loss due to legal action are the major constraints on the monopolist miner. The beauty of Bitcoin mining is that upfront investment is required proportional to the revenue available to miners. If Bitcoin mining revenue is $100 billion dollars annually, some amount on the order of $100 billion dollars will be invested annually by that miner. This means significant losses are possible if one loses business to competitors or reduces the overall revenue available.

## WHAT RISKS DOES A MONOPOLIST MINER POSE?

With the economic constraints on the monopolist miner, what threat would it pose to the important qualities of Bitcoin – cheap transactions, fast transactions, secure transactions, reliability, scarcity, and service availability?

The classic argument against monopolies is that they raise prices and reduce supply. That is a justifiable fear when a monopoly is enforced by law, but a naturally occurring monopoly is a function of economies of scale. In other words, this mining monopoly occurred because it was able to produce output and process transactions at a cheaper unit price than any other competitor. This also assumes that the monopolist miner has an advantage in any possible specialization of transaction processing. It also isn't necessarily true that a monopolist is incentivized to limit supply and raise prices. Rather, the monopolist is incentivized to maximize profits, which could easily occur at a price below the level which any competitor could offer. Further, the monopolist has incentive to choose a price which doesn't bait possible competitors to invest in a competing entity. Due to these factors, it is highly unlikely that a mining monopolist would adversely affect the affordability of transactions given that the monopoly was formed naturally.

Why might a monopolist miner choose to adversely affect the security of Bitcoin? The typical threat cited is the double spend. A double spend would entail the monopolist miner replacing a transaction that sent money to someone else with another transaction that sends the money back to the monopolist miner. The monopolist miner could also coordinate with some other party to offer this double-spend service. This can pose serious issues if there is no legal recourse. However, in practice this attack would be highly unlikely for many reasons. For one, it would be illegal, and there is no way to accomplish this without leaving a trail of evidence which would make reclaiming the stolen funds through legal action exceptionally easy. This monopolist miner is likely among the most visible and sueable companies in the world with data centers across the globe. Additionally, even if the monopolist miner could get away with it, they would be destroying their own credit and driving business away from the system. Stealing $1000 worth of Bitcoin isn't likely to be worth it to the mining monopolist. Stealing $1 million isn't going to be possible from a legal standpoint. This is the 51% attack vector so many people are worried about in the crypto consensus: **it simply isn't economically incentivized at scale**.

The reason why the monopolist miner has trouble altering the security of Bitcoin is the public nature of the system. A monopolist miner is forced to make the blockchain public, or competitors will. Further, the system doesn't work without the blockchain being public, as one would have no way of knowing if they had been paid or not without being able to see. In BSV, many are using the blockchain as a database for all kinds of applications. These also depend on a publicly viewable blockchain. Because a miner can only steal or change what is already public, doing so alerts the world to that alteration.

How about the reliability of the system? The monopolist miner clearly has a strong incentive to guarantee uptime. Further, the monopolist miner will be incentivized to distribute data to avoid any data loss and remove central points of failure. Distribution is probably a better word to describe the value of decentralization, and it can be accomplished by a single operator in the same manner as a service like AWS would distribute data.

A far more salient threat to reliability would be changing the rules of the system. This may be the biggest threat from the monopolist, although a strong argument is currently being made that changing the rules would be illegal. In fairness, the allegedly decentralized BTC has undergone many rule changes which negatively affected the reliability of the system. Therefore, it isn't clear that the monopolist miner poses a greater threat than the status quo of achieving changes through "social consensus," perhaps more accurately described as the will of the BTC core developers. What can be assumed about changes made by a monopolist miner is that these changes would result in greater profits to the miner. This may actually be a benefit to the system if these changes increase revenues or lower costs. Profit to miners is certainly a much better signal for making changes to the system than the whims of protocol developers, the primary change agents to this point in Bitcoin's history, are. Further, if one's expectation is that reliability is economically beneficial, it is unlikely that changes will be made that disrupt this reliability. And, the law also exists as a final preventative measure and backstop.

The defined scarcity of Bitcoin is another element that would likely be protected by law but is irrelevant. Using Bitcoin for saving is a function which gives an outsized contribution to the price of Bitcoin. Since there are so many substitute goods for saving value, a miner would jeopardize their source of revenue by altering the planned issuance of new Bitcoin.

What about denial of service? Again, a strong legal argument can be made that a miner is not allowed to prohibit service, sort of like an internet service provider. It is unlikely this miner would be able to freeze users' funds at their own discretion from a legal standpoint. However, even if that case could not be made, there are still major barriers to a monopolist miner censoring their customers. First, the miner would not necessarily know what to censor. Transactions are pseudonymous and the data in those transactions can be encrypted. Among the thousands, millions, or billions of transactions processed every second, what effort can be afforded in an attempt to censor? Further, if one is successful at denying service, that may drive other customers away. If it is known that your Bitcoin can be trapped through arbitrary censorship by a service provider, it makes it much less valuable. This is in contrast to knowing that money can be frozen or reassigned by a

legal authority, since these types of denial of service have extreme benefits in addition to drawbacks.

With so many factors ensuring the monopolist preserves the valuable qualities of Bitcoin, censorship resistance becomes the obvious reason to preserve decentralization. When censorship resistance is defined as existing outside of law, the degree to which it can be achieved through the status quo is unclear, as is its desirability. Many have alleged that mining is already centralized to the point where a coordinated intervention by governments is possible on BTC. This would not be surprising due to economies of scale. Liberty Reserve, a pre-Bitcoin attempt at globally decentralized extralegal online money, was ultimately shut down through the cooperation of more than a dozen nations led by the United States Justice and State Departments. Their failure serves as precedent for such an intervention despite the effective decentralization of the operation. In fact, Multicoin Capital makes reference to the current centralization of networks like BTC and Ethereum in their essay **Why Decentralization Matters: A Response**, where it is noted that there are likely around 20 miners that comprise the vast majority of hashrate on BTC and Ethereum respectively. In that piece this is described as the natural result of cartelization, although we would have probably used the term economies of scale.

Bitcoin's potential has been severely stunted by efforts to preserve decentralization. The major quality that can be preserved through decentralization is what Multicoin Capital calls "sovereign-grade" censorship resistance – in other words, having extralegal status, although it isn't clear that networks like BTC have achieved this due to the inevitabilities of economies of scale. Further, the value of this censorship resistance is not clearly positive, as we outlined in Chapter 4. If you are a Bitcoin user, investor, or enthusiast today, an important question exists: what is the value of decentralization, and what will you give up for it? For the crypto consensus, the answer may be everything.