CHAPTER SEVEN

Why "Bitcoin Can't Scale" is Wrong

CRYPTO CONSENSUS VIEW	UNBOUNDED CAPITAL VIEW
Bitcoin can't scale at all or can't scale while remaining secure/valuable.	Bitcoin has no fundamental limits on its scale and can scale to meet any level of demand.

It is key to the crypto consensus that Bitcoin can't scale. So much has been invested in protocols developed to remedy Bitcoin's lack of scalability that a scalable Bitcoin is an enormous black swan to these portfolios. In one fell swoop, the assumptions girding these protocols would crumble just as a new competitor emerges that could potentially eclipse what these platforms can offer. In our view, this black swan is already here in the form of BSV, and other black swans could develop in the shape of a new blockchain focused on scale. To the crypto consensus, this is as distant a threat as one can imagine. To them, if there is one certainty in all of blockchain, it's that Bitcoin doesn't scale.

WHY IS IT THOUGHT THAT BITCOIN CAN'T SCALE?

It's easy to understand how the narrative that Bitcoin can't scale has survived for so long. That perception is rooted in the fact that BTC, the dominant version of Bitcoin by visibility and market cap, has been defined by its lack of scale. Further, because the majority of

people most involved in Bitcoin assume that decentralization is a requirement for Bitcoin, paths to scale which threaten that decentralization are dismissed. Bitcoin is also thought not to need scale in order to be valuable. It's believed that Bitcoin's scarcity combined with its decentralization is all that is necessary to take on the digital gold store of value function, the only application of Bitcoin that BTC seeks to fill. In BTC, these beliefs and priorities manifest in a version of Bitcoin that doesn't scale and has no concrete plan or strong desire to scale. The assumption that Bitcoin simply can't scale follows naturally.

This assumption is backed up by an intuition that something about Bitcoin is clearly inefficient. Because of the lack of scale, many miners are still small, home-based operations. PoW is thought to be wasteful. How could such a decentralized network of electricity burners be efficient? It is even thought that inefficiency is an essential part of Bitcoin. As we already noted in Chapter 4, Multicoin Capital paraphrases Nick Szabo's description of how lack of scalability leads to trustlessness in their "**Models for Scaling Trustless Computation**:"

> *But first, we need to establish context for the term "trustless." Nick Szabo frames trustlessness as an inverse function of technical efficiency. Basically, the less efficient the computer, the more difficult it is to manipulate. The more difficult it is to manipulate, the more you can trust it, therefore making it trustless.*

The idea that Bitcoin is severely inefficient – but that its limitations facilitate trustlessness and censorship resistance, which ultimately give Bitcoin value – makes sense on the surface. It helps that this goes unquestioned by the crypto consensus. The idea that Bitcoin has wasted a decade functioning far below its capabilities for lackluster reasons seems much less plausible. Experts who embrace the supposed limitations are considered pragmatic and believable. Those who say Bitcoin can replace the internet sound fanciful given the lack of scale to this point.

THERE IS NO BARRIER TO SCALE IN BITCOIN

Vitalik Buterin, a creator of Ethereum and a crypto consensus authority, is confident **that BSV can't scale**. But, how would one actually go about proving that Bitcoin cannot scale? There would have to be some fundamental barrier or an asymptotic expense which could not reasonably be assumed.

Maybe something about the algorithm described by the protocol does not scale. Perhaps there is a fundamental limitation to what can be transmitted between the miners. Maybe there is an economic incentive not to scale which can't be overcome.

Virtually no one actually goes through this process of trying to identify the barrier to scale. The barrier is assumed to be the risk of centralization. We have already established that centralization does not pose a risk to the network outside of bringing it into the scope of law. So, what other barriers to scale may exist, and what is the mechanism for scale if these barriers do not exist?

WHAT IS SCALE IN BITCOIN?

Increased scale is the ability for Bitcoin to include more data and more transactions overall and to accept the same transactions and data at lower fees. Layer two solutions like the lightning network are not actually scaling solutions because they are not solutions that provide the full feature set of Bitcoin, which includes having ownership tracked on the blockchain. These also don't work for technical, economic, and legal reasons that are well articulated **in these resources**.

More transactions and data leads to larger block sizes. In BTC, there is a block size limit. This is the barrier to scale imposed to increase decentralization. It is important to recognize that scaling isn't something that happens by removing a block size limit. Real scaling is a two-sided process. On the one side, users must demand greater scale by generating more transactions and paying the associated fees. On the other side, miners and other service providers must respond to increased demand by investing in greater capacity. Scale happens first and block size increases follow, not the other way around. There is no maximum block size on BSV today, but there is still a long way to go in terms of scaling.

BITCOIN IS HIGHLY FLEXIBLE

To understand Bitcoin's scalability, it is important to realize that the system has a lot of built in economic flexibility. There are two main variables that create this flexibility: the mining difficulties and variable fees.

Bitcoin blocks are supposed to be discovered every 10 minutes on average. The rate of block discovery is a function of hashrate and the mining difficulty. Hashrate, the total hashing volume of miners on the network, can increase or decrease over time depending on the efficiency of hashing and the available revenue to miners. Mining difficulty resets to keep the average block time consistent at 10 minutes. This difficulty resets approximately every two weeks. Since mining difficulty resets to keep average block-time constant, there is no hash-based limitation to scale. If increased scale makes hashing more difficult, the mining difficulty can adjust to facilitate that scale. Therefore, the hashing necessary from PoW cannot be the limiting factor in Bitcoin's scale.

Bitcoin transaction fees are also adjustable. There is no set fee rate in Bitcoin. Users are free to offer whatever fee they like, although there is no guarantee that transactions will be included if fees are too low. If a situation emerged where fees started to increase because current capacities were being reached, miners would be incentivized to invest to accommodate greater scale and earn these higher fees. This is the mechanism that leads to scale. If capacity is reached, fees increase, creating an incentive for miners to invest in greater scale. On BTC, fees regularly increase, but since scale is prohibited no investment occurs towards being able to process more transactions.

BITCOIN'S ALGORITHM IS EFFICIENT

An easy place to look for possible scaling bottlenecks is Bitcoin's algorithm. Bitcoin miners accept transactions, verify them, send them to other miners, include them in a block, solve the PoW puzzle, and then propagate their block to other miners. Which of these steps would be the scaling bottleneck? We know that finding a valid hash can't be the bottleneck, since mining difficulty is variable. An easy place to look for a theoretical bottleneck would be in transaction verification. As of 2022, miners can meet peak demand by verifying many thousands of transactions a second on BSV, but is there an algorithmic limit? Are millions or billions a second possible?

The key to understanding the scalability of transaction verification is realizing that Bitcoin is fully parallelizable. This means miners can validate new transactions independently. Other than in edge cases which can be handled easily, Bitcoin miners can validate multiple transactions simultaneously. This means that a miner can scale horizontally by adding additional computers that work in parallel rather than simply trying to invest in the fastest,

most powerful computer. This horizontal method is extremely common in large professional data centers. The BTC code has not taken advantage of Bitcoin's initial built-in parallelizability for obvious reasons. Since BTC and BSV have shared origins, BSV inherited mining software that was optimized for single-thread processing, not parallel processing. Fortunately, multiple parties are currently building parallelized implementations of Bitcoin mining software to accommodate the future needs of BSV, most notably **Teranode**.

Parallelizability exposes flaws with competing blockchain technology. Platforms like Ethereum have a state which changes on a per-transaction basis. Validators must all evaluate transactions in the same order to determine if a block is valid. This means that only one processor can be used. This limitation has been crippling to Ethereum's scalability and has played a role in their plan to switch to a PoS network that leverages sharding. This plan has been in the works for several years, showing the difficulty of such a task, and many application developers oppose sharding because of added complexity. Many other platforms have this same problem of not being parallelizable. These sorts of mistakes come from protocol developers who haven't properly thought through what it takes to achieve massive scale. This isn't surprising since massive scale is not the goal of most of these projects. Censorship resistance, trustlessness, and in some cases acquiring retail or private financing through ICOs or venture capital are more pressing concerns than building for long-term success.

Some developers in BSV have actually gone through the process of formally evaluating the efficiency of Bitcoin algorithms using Big O notation. Prominent examples are Attila Aros of MatterCloud and Nithin Mani of Xoken Labs. Nithin has **published several pieces** on the scalability of Bitcoin and surrounding algorithms.

MINER BEHAVIORS CAN CHANGE AT SCALE

Other possible bottlenecks on scale have to do with components of the protocol that directly relate to miner behavior. These components include accepting transactions, sharing transactions with other miners, including transactions in blocks, and sending those blocks to other miners. There are no fixed rules for any of these actions. Miners act according to their own interests, as they weigh costs and benefits.

As Bitcoin has worked in a certain way for so long, with most miners simply running the main Bitcoin Core software with default settings, people don't think about the flexibility with these processes. Miners are set up in a peer-to-peer network with other miners and

the default is typically to treat these other miners equally. Ultimately, miners can be more selective about their peers. They can be selective about who they accept transactions from, with whom they share transactions, what they include in blocks, and to whom they send blocks. Users navigate these considerations by having relationships with one or more miners and by adjusting fees to provide more incentive to have transactions included.

It is worth acknowledging that existing systems outside of blockchain have achieved massive scale. Companies like Amazon, Google, Facebook, and Netflix have helped drive innovations in sending massive amounts of data around the world. Internet speeds have increased 100-fold every ten years. Today, **fiber-optic cables are being researched** which can transmit over a Petabyte per second. That means 1,073,741,824 BTC blocks will soon be able to be sent across a fiber-optic cable every second. There is very little reason to think that bandwidth will be the prohibiting factor for Bitcoin's success.

INVESTMENT LEADS TO SCALE

Ultimately, miners are incentivized to find blocks and include transactions. This is how they make money. Miners will always be incentivized to include transactions if it is profitable. Further, miners are incentivized to make investments that increase their profitability. This can be investing in hardware or software to verify transactions. It could be investing in greater bandwidth to send and receive data more easily. Coalitions of miners can invest in greater connectivity or invest in processes which make coordination easier. Ultimately, the miners who make the best investments will earn an outsized proportion of the available fees by offering a more efficient system. That efficiency leads to greater profits, allowing miners to invest in more hashpower. More hashpower raises the mining difficulty and squeezes less efficient competitors out of the network. The only thing necessary to facilitate this process is demand for using Bitcoin expressed by fee-paying transactions and the elimination of artificial barriers.

THE REAL BARRIER TO SCALE

In BTC the barrier to scale is self-imposed, but this has already been eliminated in BSV. In BSV today, the real barriers are much more mundane, including typical business challenges such as PR, marketing, and sales. The narrative and branding around Bitcoin

today is not conducive to adoption. It is hard to get individuals and businesses to adopt a system they believe is highly inefficient, unstable, and possibly illegal. Because of this perception, people don't think to use Bitcoin the way they think to use other blockchains like Ethereum. Unfortunately, the failures of chains like Ethereum have further poisoned the well of blockchains generally, including BSV, to the extent that a scalable blockchain is not considered by many to be possible without significant tradeoffs.

The lack of scale and usability on public blockchains have driven some companies to consider using private blockchains. However, to the astute reader, the notion of a private blockchain will seem very strange since the point of systems like Bitcoin is to be public. In our view, private blockchains have no advantage over existing database solutions. They are most likely being adopted by companies that are more preoccupied with being perceived as innovative than with actually engaging in real innovation. With the public options having dropped the ball to such an extreme degree in relation to the hype around blockchain, who can blame them?

Ultimately, the misunderstandings surrounding Bitcoin's scale and the value of decentralization will be resolved. Telling a better, more accurate story about Bitcoin and driving adoption is the next great business opportunity for the world. Entrepreneurs are flocking to BSV for this exact reason. Bitcoin is almost certainly too useful to fail. However, the faster that adoption can be driven, the more likely its success is. We chose the name Unbounded Capital because we believe that Bitcoin has unbounded scale and potential. We are working tirelessly to help accelerate that scale and the adoption which drives it. We hope that this ebook inspires others to join us on that mission.