CHAPTER FIVE

Proof-of-Work is Much More Than a Consensus Protocol

CRYPTO CONSENSUS VIEW

Proof-of-Work is a resource-intensive consensus mechanism that can be substituted for other consensus mechanisms, namely Proof-of-Stake, to improve scalability without significant consequences.

UNBOUNDED CAPITAL VIEW

Proof-of-Work is much more than a consensus mechanism and performs other key functions in making Bitcoin trustworthy.

At Unbounded Capital, we think Multicoin Capital and the crypto consensus are mistaken for prioritizing Bitcoin's trustlessness and censorship resistance over its scale. At a more fundamental level, we don't think they truly understand why Bitcoin works. This is evident not only in their evaluation of Bitcoin's scaling potential, but also in their significant investments into systems that have abandoned an essential component of what made Bitcoin successful: its Proof-of-Work protocol (PoW). For anyone unfamiliar with PoW, we recommend reading **this description of PoW** on our website.

The crypto consensus typically describes PoW as a consensus protocol, or a method of reaching consensus on the contents of a blockchain. PoW does serve this function, but it accomplishes much more. By thinking of PoW simply as a consensus protocol, the crypto consensus misses key elements of PoW that make Bitcoin trustworthy. In particular, their significant investments into Proof-of-Stake (PoS) networks – such as **a16z's recent investment in NEAR** – demonstrate this misunderstanding. By examining how PoW makes Bitcoin trustworthy, we can better understand Bitcoin itself and see where firms like Multicoin Capital have erred in their investment into PoS systems. For anyone unfamiliar with PoS, we recommend reading **this description of PoS** on our website.

WHAT IS BITCOIN?

Bitcoin is often thought of as a digital currency. While this is true, it is inseparable from the fact that Bitcoin is also a revolutionary database. Bitcoin's PoW protocol solves a complex coordination problem which, prior to Bitcoin's specific use of PoW, made creating a truly public and immutable database that people are willing to use impossible. The potential applications of this type of database are vast. In fact, when Bitcoin abandoned these other applications in favor of focusing on censorship-resistant digital gold, the widespread excitement around Bitcoin's potential morphed into the "blockchain, not Bitcoin" movement which found the ledger more exciting than the currency. However, in our view the two are not separable, and attempting to divide them has already proven to be as unproductive as limiting the potential of Bitcoin in favor of censorship resistance.

The Bitcoin database is structured as a blockchain. However, blockchains have existed since the 90s. The blockchain outside of the context of Bitcoin's PoW-based protocol has very little value. In fact, many of the modern "blockchains" – which are really attempts at creating an immutable, preferably public database – have abandoned the blockchain as a data structure. They are colloquially called blockchains, but they aren't actually blockchains. This is fine because a scalable, immutable, and public database is the goal, not blockchain. Unfortunately, these other attempts which fundamentally misunderstand Bitcoin are running into issues that Bitcoin has already solved.

For most, the question remains - how does Bitcoin incentivize the creation of this special database in a manner where users can trust it? The challenges of creating a public database that individuals and businesses trust enough to actually use, especially for extremely consequential purposes, are manyfold. The bar to get people looking to get rich quick to invest in these databases is not so high, but the lack of trust is evident in the failure to get significant adoption from enterprises or a large number of individuals. The beauty of Bitcoin's PoW protocol is that it solves these challenges through its own design and by making it easy to interface with other institutions like the law, which help add necessary layers of trust.

WHAT DOES IT TAKE TO TRUST A DATABASE?

As we described in Chapter 3, a trustworthy database is one that functions reliably and has true information. In the case of Bitcoin, proper functioning means that the rules are followed and that the information on Bitcoin is what one would expect based on the inputs and rules of the database. Bitcoin data is also immutable. One can expect that once data is added to Bitcoin through the publication of a block, it will always be a part of Bitcoin and it will be in the same location on Bitcoin. Further, transactions in Bitcoin are ordered, so a location corresponds to an ordering. Finally, these blocks are published widely, so the ordering can serve as a timestamp. If data exists in a block published one year ago, that can serve as legal proof that the data existed in that form at that time.

For a database like the one described above to be trustworthy, one needs to be certain that the rules will be followed, the contents will be maintained, and that it will remain accessible. Further, one may want assurances that operating with this database will be an efficient, cost-effective process. It isn't much good if accessing the database or writing to the database is extremely expensive.

Part of the challenge of a public database is incentivizing the maintenance of it. If the database is valuable, incentivizing people to hold a copy of the database is easy. However, adding to the database is possibly a thankless job. There could be millions or billions of entries a second at scale. Making sure that these follow the rules of the database and adding them accordingly is a task that can scale to a huge magnitude. How can anyone be sure that this will be done, let alone done efficiently?

Consider that a private company cannot necessarily do this. When the rules and contents of a database are public and everyone can coordinate to work on the same version, there is no exclusivity to offering services around that database. For example, it's unlikely that selling access to contents that are public could justify the expense of maintaining a public database. If a private company could have exclusivity to the database then in what sense would it be public? If the database wasn't public then the failure of the company maintaining it would mean the failure of the database. It would be foolish to trust the permanent existence of a company as most individual businesses fail eventually.

The ideal circumstance would be if anyone could maintain the database, but without anyone having to worry about whether the maintainer would follow the rules or not. Further, if the most efficient set of maintainers were always doing the maintenance, that would make the database maximally cost effective. This would also accomplish the issue of maintainers failing. Individual businesses involved in maintaining the database can fail while the system continues.

This is what Bitcoin's PoW protocol accomplishes. It creates a system of incentives that allow anyone to participate in maintaining Bitcoin's database where it can be easily understood that these maintainers will follow the rules of the system and that the most efficient maintainers will ultimately take on that role. This makes Bitcoin's ongoing existence, trustworthiness, and efficiency assured.

HOW DOES PoW MAKE BITCOIN TRUSTWORTHY?

Maintaining Bitcoin has cost, primarily borne through adding data to the database. In Bitcoin, additions come in the form of transactions. Therefore, it makes most sense for individuals to pay a fee per transaction to have their valid transactions added to the database. If one has to pay through traditional means, it poses huge problems. Traditional payment methods have high minimum fees which would make it expensive to use the database. Further, if anyone can participate in database maintenance, it isn't clear to whom the fees will need to be sent. The best solution to these issues is to have a native currency that is kept track of within the database. That currency can be used in extremely small amounts and can be paid instantly to whatever entity ends up processing the transaction. This is why Bitcoin tokens are a necessary part of Bitcoin. Paying for maintenance of Bitcoin's database would not be possible without them. In the future it is possible that a tokenized version of something like USD could be substituted, but this poses extreme challenges in the early going and isn't necessarily competitive longterm with a native currency.

The other benefit to this native currency is that it provides a means for speculation by early maintainers. A database like Bitcoin's is unprecedented. People who see the value in it and understand why it will ultimately become useful and trustworthy can speculate on its native currency. This gives early maintainers an incentive to act. If they can receive native currency for their work, they can either speculate themselves or sell to speculators and get paid in a currently usable currency for providing maintenance.

With the understanding that the database maintenance will be paid for on a transaction-by-transaction basis using a native digital currency, two questions emerge: how is the currency initially allocated, and which maintainer gets paid any given transaction fee? Bitcoin's PoW protocol answers both of these questions. Maintainers, colloquially known as miners and referred to as nodes in the Bitcoin whitepaper, add transactions which follow the rules into the next block. To have a block accepted by the other miners, they must prove that they have solved a problem which can only be solved by brute-force randomness using a hashing algorithm. The first to find a proper hash can broadcast their block to the other miners. If the miners accept that the transactions in the block follow the rules and that the Proof-of-Work was done, the block is accepted and miners begin finding the next block. The longest valid chain is considered the correct chain, so miners are incentivized to add to the longest chain and not try to substitute old blocks for their own since these will be ignored by the public and the other miners.

The value in finding a block is that the miner is given the block reward. The block reward includes the transaction fees for the included transactions and what is called the coinbase, a predetermined number of newly minted Bitcoins. These new Bitcoins are released on a per block schedule. The difficulty of finding a block is variable such that a block is found every 10 minutes on average. The issuance of new Bitcoins decreases by a factor of two every four years in an event now called a halving. Ultimately, 21 million will exist where each of these Bitcoins can be further divided into X number of indivisible units, meaning there are 21 quadrillion individual Bitcoin tokens. These indivisible units are now called satoshis. Through this process, new Bitcoins and transaction fees are both allocated. The manner in which these are allocated has a few important consequences key to the success of the system.

PoW PERFORMS AN IMPORTANT SIGNALING FUNCTION

Proof-of-Work uses a lot of energy. Hashing blocks takes energy. This is a major source of marginal cost in Bitcoin maintenance or transaction processing. Many people in crypto consider this to be wasteful. However, what is considered waste by many in the crypto consensus is actually an extremely important signaling function. Hashing is equivalent to sending a signal of investment in the system. This is because hashes are not free, and the only way to recoup value from these hashes is through earning new Bitcoins and Bitcoin transaction fees. That means that the overall level of hash in Bitcoin corresponds to the total investment in the system and that this investment can only be recouped through maintaining Bitcoin. The more that is invested, the more users can be assured that maintenance will continue.

This signal has another important consequence: exposing the identity of the miners. Setting up a large mining operation is not something that can be done secretly. Large miners need significant facilities to house their hashpower. The visibility of this process exposes miners to their local authorities. This is good, since if mining could be done secretly without any consequences for illegal behavior, the system would be far less trustworthy. The identifiability of miners gives users a “throat to choke” if they aren’t served correctly, resulting in damages. Proof-of-Work is such that if one doesn’t make a significant investment into mining, one will not be able to mine new blocks and get new Bitcoins or fees. If one does make a significant investment, they become exposed to law enforcement and gain accountability.

PoW LEADS TO EFFICIENCY

A final key quality of the allocation by Proof-of-Work is that it incentivizes efficient transaction processing. Database users care that their transactions are processed efficiently and accurately. Miners are incentivized to maximize their profit per hash. Because the coinbase is a fixed quantity, the way to get profit is to be able to hash more cheaply than competitors and/or to be able to add transactions to blocks more cheaply than competitors. Both of these will allow miners to expand their operation relative to competition and start finding a larger share of blocks. Ultimately, the inefficient miners will be driven out of business and economies of scale, specialization, and innovation will dictate what firms are able to engage in database maintenance at any time.

WHY DOES BITCOIN’S POW PROTOCOL RESULT IN SECURITY?

How can we trust miners to be honest and follow the rules of Bitcoin? The main reason is that Bitcoin is public. New blocks will be scrutinized by competing miners for errors. These miners have an incentive to disregard blocks with errors. They know that other miners will also disregard blocks with errors and that the block reward from that block is still available. Erroneous transactions will also be visible to the public and affected parties will sound the alarm. If all the miners fail simultaneously, they will still ultimately be alerted of their error and will have to dismiss those blocks. If miners refuse to process transactions correctly, they could be subject to legal action. This would also harm their business and their investments in maintenance equipment.

Finally, the structure of Bitcoin's blockchain plays an important role. Each block in the chain has a block header. These headers are important because they can be used to prove the existence of a transaction in a block through something called a merkle proof. This merkle proof connects a transaction to the block header proving that the transaction is contained in that block. This becomes very useful as blocks grow to be extremely large. Importantly, there is no way to fake a merkle proof. This means that fake transactions can always be detected.

These block headers are chained together in the PoW process, hence the name blockchain. This means that a block header can't be altered in isolation or else it would no longer fit into the chain. These headers are published with each block and are easy for users to keep track of. Since knowing the headers gives one the ability to assess whether a transaction has been included into a block or not, it is very notable if the block headers suddenly change. The headers are public, so changing them in secret is impossible. Further, these headers are chained together through PoW, meaning that for changing one header one must change all subsequent headers. This is prohibitively expensive. The financial difficulty and lack of secrecy in altering the blockchain provides an ironclad incentive to focus on adding new blocks to the chain instead of rewriting history.

Law is another essential component in keeping miners honest. Since miners are visible due to their investment, they can be held accountable if they violate laws. This includes things like stealing Bitcoin or changing people's data. Miners also have very little incentive to act dishonestly since the value of their investment is tied indelibly to the overall economic value generated by the network. If the price of Bitcoin drops or the revenue available from fees drops, miners can recoup less of their investment in each block. Their incentive is the opposite - make Bitcoin as valuable and useful as possible.

WHY PoS MISSES THE MARK

A lack of understanding about what PoW accomplishes, combined with a suspicion that PoW is somehow unscalable, has led firms like Multicoin Capital to seek other solutions. The most popular alternatives by far are variations on Proof of Stake. Multicoin Capital has invested in at least four PoS blockchains – Algorand, Solana, Dfinity, and Near – and is investing in applications that leverage these chains. They have also written in support of EOS, which is a PoS network, and have invested in applications leveraging Ethereum, which is attempting to transition to PoS.

These PoS networks are purported to have scalability advantages over their PoW alternatives. In our view, this is incorrect. We don't see any theoretical limit on the scalability of either network. This is the focus of Chapter 7, where we will explain why there is no limit to Bitcoin's scalability. In our view, scale is the ability for network maintainers to meet increases in demand. To us, the incentives for miners in a PoW system to rise to the challenge of increased demand is much clearer than in PoS. This forecasts a relative difficulty with scaling before considering other shortcomings with PoS.

The main issue with PoS in regards to meeting the challenge of increased demand is a well known phenomenon: the tragedy of the commons. The incentive for PoS miners to improve the speed at which they can process transactions is much less direct than for PoW miners. In a PoW system, more efficient transaction processing will lead directly to a larger share of the fees. This makes efficiency a long-term certainty. In PoS, miners typically have much less to gain from becoming more efficient unilaterally. PoS miners will want the system to be more efficient, but they have little incentive to invest in scale unless all miners invest in scale. Our expectation is that PoW systems will continue to be far more efficient for this reason. **We are observing that the efficiency of BSV today relative to PoS networks is continuing to grow: there is not a single PoS network or any other blockchain network today besides BSV that is gaining users and transactions without transaction costs skyrocketing. In contrast, on BSV, the increased adoption drives costs down.**

Oligopoly is another issue with PoS networks. Since token ownership correlates with access to block rewards, incumbent miners have an incentive to protect their revenue and not make changes that risk their access to that revenue. These sorts of issues have been made apparent on networks like EOS, which has seen people leave the network over concerns that votes to determine which entities would participate in the mining process **were being traded or bought**. If increasing scale increases miners' costs, this oligopoly has an incentive to resist increased scale unless it is absolutely necessary. If the costs of scaling exceed the benefits to this oligopoly, scaling will not happen. Because all miners are guaranteed work in this system, especially if they can coordinate to stay in power, unilateral improvement is also disincentivized.

This lack of a scaling advantage is problematic for PoS proponents who themselves acknowledge certain PoS shortcomings. Multicoin Capital notes in their essay on **scaling trustless computation** that "PoS schemes are far less battle-tested than PoW schemes in real-world settings. For example, the first PoS implementation, Peercoin, faced nothing-at-stake attacks, among others. As such, PoS schemes should be considered fundamentally riskier." In our view, these security concerns are more of an issue in the early stages. Since all networks go through early stages, these issues are significant, but much of the security in all blockchains is derived from their public nature, which PoS networks share. There are, however, other reasons to be concerned with PoS which suggest to us that they are much less likely to be secure at scale than PoW networks.

Another issue with PoS is the lack of accountability. In PoW, mining requires significant investment in physical infrastructure. In PoS, this is not necessarily the case. PoW miners are necessarily exposed to the public. This brings accountability. Large amounts of cryptocurrency can be owned privately. This is a good feature for ownership, but a worse feature for mining. An attack is much more likely on PoS because miners can be anonymous. On PoW, an attacker will necessarily have an extremely large physical footprint.

Even though there is significant investment in these facilities for PoW miners, PoS can't offer any advantage in terms of economic cost to miners. The economic law that marginal cost equals marginal benefit applies to both protocols. However, PoS does change the nature of the costs in a way that is appealing to environmentalists who see increased use of energy as inherently negative. In our view, however, that energy is being used extremely well. It brings accountability to the miners who maintain the world's public database. We think this will have a positive impact that vastly outweighs any potential environmental cost. You can learn more about this in our second ebook: **Green Bitcoin**.

Bitcoin can and does work just as well with renewable energy sources. The incentive to save money has driven Bitcoin mining to rely heavily on underused renewable resources. Bitcoin's ability to use these sources ultimately **incentivizes the development** of ways to harness energy that **are typically viewed as waste**. In all likelihood, Bitcoin's environmental impact has been, and will continue to be, positive.

A final issue with the current generation of PoS networks is that they are designed with trustlessness and censorship resistance in mind. Bitcoin was designed with efficiency and trustworthiness in mind. In our view, Bitcoin is undoubtedly the gold standard design for creating a trustworthy public database today. Even if a better design could be created, we think that Bitcoin will have enormous staying power due to its network effects. The future is a future built on PoW.

PoS SUFFERS FROM A MINDSET PROBLEM

What is also particularly troublesome with PoS networks is the technocratic mindset that their proponents tend to espouse. Normally, the arrangement is that there exists some sort of governance structure. This structure can alter the rules. Improvements to efficiency are considered a top-down phenomenon and many of these networks have specific foundations or organizations whose explicit task is to improve the network for all.

Even if the incentives are well aligned in these contexts, we don't think this top-down, governance-oriented mindset will be competitive with a network like Bitcoin in the long run. Bitcoin's rules are its greatest asset, but they also represent its greatest failure to this point. That failure was not clearly stating the rules and establishing a culture of keeping those rules constant. Between the original Bitcoin whitepaper, website, codebase, and existing laws, the rules could be understood. However, the line between what is a rule and what is code that could be, and often needed to be, improved was not clear.

This lack of clarity allowed a culture of changing the rules to emerge. Few people would dispute the necessity to improve Bitcoin's code over time. Code, however, is an instantiation of the rules. In fact, multiple versions of code can exist simultaneously in Bitcoin as long as they follow the same rules. Ultimately, having multiple versions of the code is ideal in order to have more competition and innovation.

However, the need to improve the code was equated with a sense that the system should be improved in other ways. As we've already outlined, these "improvements" tended to prioritize censorship resistance at the expense of scale. Beyond the lack of utility in these improvements, the culture of changing the protocol rules created a great deal of instability. This may not be extremely disruptive if one's goal is digital gold which exists outside of existing financial regulations, but for applications trying to build on Bitcoin, the constant rule changing was a big problem. In fact, many other blockchains have inherited this mindset of rule-changes dictated by some form of governance. In our view, this is a mistake for a public database where predictability and consistency across time are paramount.

Issues with this governance came to a head in a recent episode involving PoS network Tron and PoS network Steem. Tron acquired the company which founded Steem, receiving about 40% of the STEEM tokens in that transaction. In what was described as a hostile takeover, **they were accused of colluding with exchanges** who were custodying other users' tokens to limit the power of certain developer accounts. At Unbounded Capital, our view is that political struggles to control the rules of blockchains will hinder their progress. If the rules of the system work, it is better to keep them unchanged and let independent actors compete in provisioning them.

This instability can be removed from Bitcoin much more easily than from PoS systems. Innovation is necessary to compete over the long term, but in Bitcoin this can happen at the level of the miner. Each miner has an incentive to become more efficient. That incentive is much weaker in a PoS system, so some central structure tasked with increasing the efficiency over time is typically a feature. We are betting that the Bitcoin miners will innovate far faster than the governance structures on PoS networks.

In BSV, great lengths are being made to codify the precise nature of the rules and a culture is being set to maintain these rules. The result is that entrepreneurs who grew frustrated with the shifting landscapes of BTC, BCH, and Ethereum have been flocking to BSV for both the additional scale and the certainty that comes with well-defined, unchanging rules.