

## The unseen economic forces that govern the Bitcoin protocol.

BY YONATAN SOMPOLINSKY AND AVIV ZOHAR

# Bitcoin's Underlying Incentives

BEYOND ITS ROLE as a protocol for managing and transferring money, the Bitcoin protocol creates a complex system of economic incentives that govern its inner workings. These incentives strongly impact the protocol's capabilities and security guarantees, and the path of its future development. This article explores these economic undercurrents, their strengths and flaws, and how they influence the protocol.

Bitcoin, which continues to enjoy growing popularity, is built upon an open peer-to-peer (P2P) network of nodes.<sup>9</sup> The Bitcoin system is “permissionless”—anyone can choose to join the network, transfer money, and even participate in the authorization of transactions. Key to Bitcoin's security is its resilience to manipulations by attackers who may choose to join the system under multiple false identities. After all, anyone can download the open-source code for a Bitcoin node and add as many computers to this network as they like, without having to identify themselves to others. To counter

this, the protocol requires nodes that participate in the system to show proof that they exerted computational effort to solve hard cryptographic puzzles (proof-of-work) in order to participate actively in the protocol.

Nodes that engage in such work are called *miners*. The system rewards miners with bitcoins for generating proof-of-work, and thus sets the incentives for such investment of efforts.

The first and most obvious effect of participants getting paid in bitcoins for



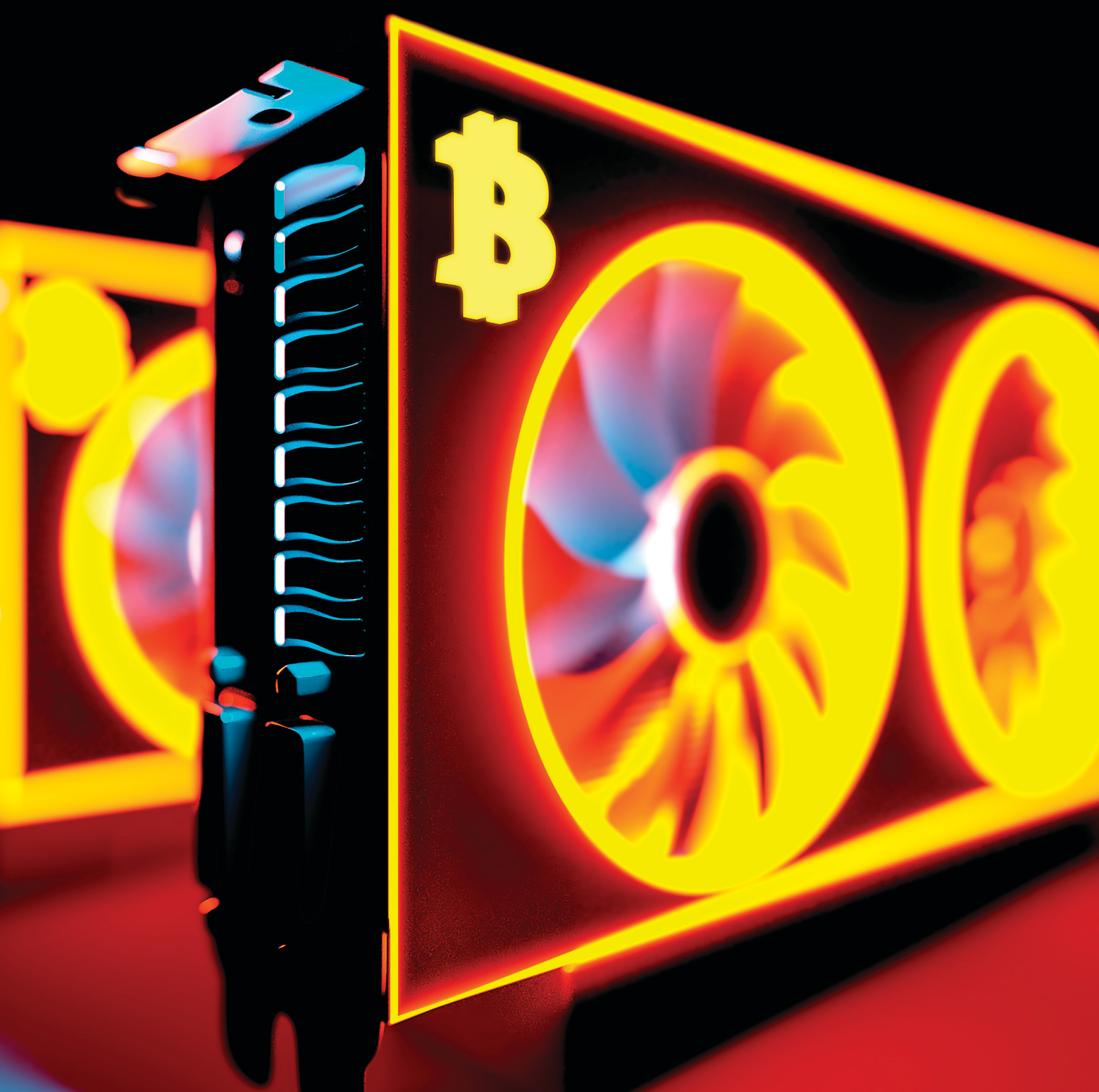


IMAGE BY SERGEY ILVASOV

running software on their computers was that, once bitcoins had sufficient value, people started mining quite a lot. In fact, efforts to mine intensified to such a degree that most mining quickly transitioned to dedicated computer farms that used specialized gear for this purpose: first, GPUs that were used to massively parallelize the work; and later, custom-designed chips, or ASICs (application-specific integrated circuits), tailored for the specific computation at the core of

the protocol (machines with current ASICs are about a million times faster than regular PCs when performing this work). The Bitcoin network quickly grew and became more secure, and competition for the payments given out periodically by the protocol became fierce.

Before discussing the interplay between Bitcoin's security and its economics, let's quickly look at the rules of the protocol itself; these give birth to this complex interplay.

### **A Quick Primer on the Bitcoin Protocol**

Users who hold bitcoins and wish to transfer them send transaction messages (via software installed on their computer or smartphone) to one of the nodes on the Bitcoin network. Active nodes collect such transactions from users and spread them out to their peers in the network, each node informing other nodes it is connected to about the requested transfer. Transactions are then aggregated in batches called *blocks*.

Blocks, in turn, are chained together to create the *blockchain*, a record of all accepted bitcoin transactions. Each block in the chain references its predecessor block by including a cryptographic hash of that block—effectively a unique identifier of that predecessor. A complete copy of the blockchain is kept at every node in the Bitcoin network. The process of block creation is called *mining*. One of its outcomes (among others) is the printing of fresh coins, which we call *minting*.

The rules of the protocol make block creation extremely difficult; a block is considered legal only if it contains the answer to a hard cryptographic puzzle. As compensation, whenever miners manage to create blocks they are rewarded with bitcoins. Their reward is partly made up of newly minted bitcoins and partly of mining fees collected from all of the transactions embedded in their blocks. The rate of minting is currently 12.5 bitcoins per block. This amount is halved approximately every four years. As this amount decreases, Bitcoin begins to rely more and more on transaction fees to pay the miners.

The key to Bitcoin's operation is to get all nodes to agree on the contents of the blockchain, which serves as the record of all transfers in the system. Blocks are thus propagated quickly to all nodes in the network. Still, it is sometimes possible for nodes to receive two different versions of the blockchain. For example, if two nodes manage to create a block at the same time, they may hold two different extensions to the blockchain. These blocks might contain different sets of payments, and so a decision must be made on which version to accept.

The Bitcoin protocol dictates that nodes accept only the longest chain as the correct version of events, as shown in the accompanying figure. (To be more precise, nodes select the chain that contains the most accumulated computational work. This is usually the longest chain.) This rule, often called the “longest chain rule,” provides Bitcoin with its security. An attacker who wishes to dupe nodes into believing that a different set of payments has occurred will need to produce a longer chain than that of the rest of the network—a task that is incredibly dif-



**The key to Bitcoin's operation is to get all nodes to agree on the contents of the blockchain, which serves as the record of all transfers in the system.**



icult because of the proof-of-work required for each block's creation. In fact, as long as the attacker has less computational power than the entire Bitcoin network put together, blocks and transactions in the blockchain become increasingly harder to replace as the chain above them grows.

This difficulty in replacing the chain implies that it takes many attempts before an attacker can succeed in doing so. These failed attempts supposedly impose a cost on attackers—mining blocks off of the longest chain without getting the associated mining rewards. Naïve attacks are indeed costly for attackers (more sophisticated attacks are discussed later).

The accompanying figure on page 49 shows the evolution of the blockchain: forks appear and are resolved as one of the branches becomes longer than the other. Blocks that are off the longest chain are eventually abandoned. They are no longer extended, their contents (transactions colored in red) are ignored, and the miners that created them receive no reward. At point 1 there are two alternative chains resulting from the creation of a block that did not reference the latest tip of the blockchain. At point 2 the fork is resolved, as one chain is longer than the other. At point 3 there is another fork that lasted longer, and at point 4 the second fork is resolved.

### **Bitcoin Economics 101: Difficulty Adjustment and the Economic Equilibrium of Mining**

Bitcoin's rate of block creation is kept roughly constant by the protocol: Blocks are created at random intervals of roughly 10 minutes in expectation. The difficulty of the proof-of-work required to generate blocks increases automatically if blocks are created too quickly. This mechanism has been put in place to ensure that blocks do not flood nodes as more computational power is added to the system. The system thus provides payments to miners at a relatively constant rate, regardless of the amount of computational power invested in mining.

Clearly, as the value (in U.S. dollars) of bitcoins rises, the mining business (which yields payments that are denominated in bitcoins) becomes more



lucrative. More participants then find it profitable to join the group of miners, and, as a consequence, the difficulty of block creation increases. With this increase in difficulty, mining blocks slowly becomes more expensive. In the ideal case, the system reaches equilibrium when the cost of block creation equals the amount of extracted rewards. In fact, mining will always be slightly profitable—mining is risky, and also requires an initial investment in equipment, and some surplus in the rewards must compensate for this. Hence, Bitcoin's security effectively adjusts itself to match its value: A higher value also implies higher security for the protocol.

As mining rewards continue to decline (as per the protocol's mining schedule), the incentive to create blocks is expected to rely more on transaction fees. If a sudden drop in bitcoin transaction volume occurs, these fees might be insufficient to compensate miners for their computational resources. Some miners might then halt their block creation process, temporarily. This may compromise the system, as the security of transactions depends on all honest miners actively participating. (For additional work on the incentives in Bitcoin after mining declines, see Carlsten et al.<sup>3)</sup>

Many complain that the computation required to create blocks wastes resources (especially electricity) and has no economic goal other than imposing large costs on would-be attackers of the system. The proof-of-work is indeed a solution to a useless cryptographic puzzle—except, of course, that this “useless” work secures the Bitcoin network. But what if some of the work could be useful? Or could be produced more efficiently? If mining does not entail a waste of resources for each node, then it also costs nothing for attackers to attack the system. In fact, if the proof-of-work is less costly to solve, more honest participants join mining (to collect the rewards), and soon the difficulty adjustment mechanism raises the difficulty again. Hence, in a sense, the Bitcoin proof-of-work is built to spend a certain amount of resources no matter how efficient an individual miner becomes. To derive substantial benefits from mining without an offsetting increase in costs re-

quires a proof-of-work that is useful to society at large but cannot provide value to the individual miner. (For some attempts at using other problems as a basis for proof-of-work, see Ball et al.,<sup>2</sup> Miller et al.,<sup>8</sup> and Zhang et al.<sup>13)</sup>

### Mining Decentralization

The key aspect of the Bitcoin protocol is its decentralization: no single entity has a priori more authority or control over the system than others. This promotes both the resilience of the system, which does not have a single anchor of trust or single point of failure, and competition among the different participants for mining fees.

To maintain this decentralization, it is important that mining activity in Bitcoin be done by many small entities and that no single miner significantly outweigh the others. Ideally, the rewards that are given to miners should reflect the amount of effort they put in: a miner who contributes an  $\alpha$ -fraction of the computational resources should create an  $\alpha$ -fraction of the blocks on average, and as a consequence extract a proportional  $\alpha$ -fraction of all allocated fees and block rewards.

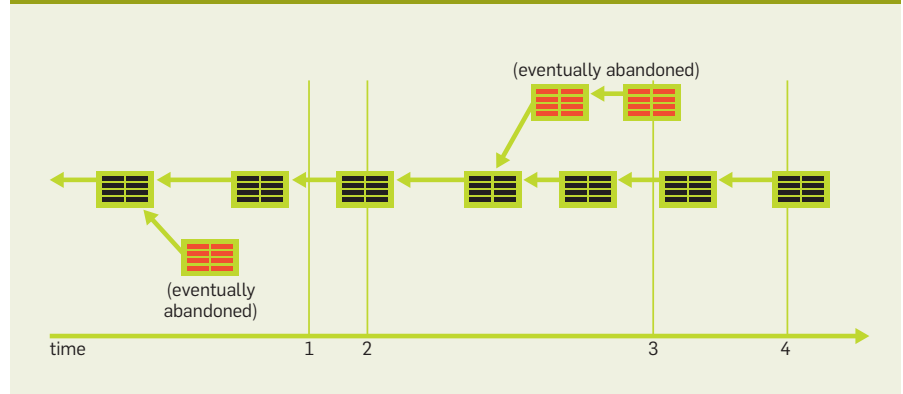
In practice, some participants can benefit disproportionately from mining, for several different reasons. An unbalanced reward allocation of this sort creates a bias in favor of larger miners with more computational power, making them more profitable than their smaller counterparts and creating a constant economic undercurrent toward the centralization of the system. Even slight advantages can endanger the system, as the miner can use additional returns to purchase more and more computational power, raising the difficulty of mining as the

miner grows and pushing the other smaller (and, hence, less profitable) miners out of the game. The resulting winner-takes-all dynamic inevitably leads to centralization within the system, which is then at the mercy of the prevailing miner, and no security properties can be guaranteed.

**ASICs mining.** The appearance of ASICs initially alarmed the Bitcoin community. ASICs were orders of magnitude more efficient at mining bitcoins than previous systems. As this special hardware was not initially easy to acquire, it provided its owners with a great advantage over other miners—they could mine at a much lower cost. Those with this advantage would add ASIC-based proof-of-work to the system until the difficulty level would be so high that everyone else would quit mining. The risk was then that a single large miner would have sole access to ASICs and would come to dominate the Bitcoin system. Concerns subsided after some time, as ASICs became commercially available and more widely distributed.

In fact, ASIC mining actually introduces long-term effects that contribute to security. Later this article looks at how a miner can carry out profitable double spending and selfish mining attacks. One can argue, however, that even selfish and strategic miners are better off avoiding such attacks. Indeed, a miner who invested millions of dollars in mining equipment such as ASICs is heavily invested in the future value of Bitcoin: the miner's equipment is expected to yield payments of bitcoins over a long period in the future. Should the miner then use this gear to attack the system, confidence in the currency would drop, and with

### The evolution of the blockchain.



it the value of bitcoins and future rewards. The interests of miners are thus, in some sense, aligned with the overall health of the system.

All in all, ASIC mining introduces a *barrier-to-entry* to the system, as ordinary people cannot simply join the mining efforts; it thus reduces decentralization. On the other hand, it introduces a form of *barrier-to-exit*, as miners cannot repurpose their equipment to other economic activities; it therefore contributes to security.

The appearance of competing cryptocurrencies (for example, Litecoin, which essentially cloned Bitcoin), some of which use the same proof-of-work as Bitcoin, offers alternatives for miners who wish to divert their mining power elsewhere. This introduces complex market dynamics. For example, when a specific currency loses some value, miners will divert their mining power to another cryptocurrency until the difficulty readjusts. This can cause fluctuations in block creation that destabilize smaller cryptocurrencies.

**Alternative systems with no ASIC mining.** Interestingly, some cryptocurrencies use different proof-of-work puzzles that are thought to be more resistant to ASIC mining, that is, they choose puzzles for which it is difficult to design specialized hardware; for example, Ethereum uses the Ethash puzzle (<https://github.com/ethereum/wiki/wiki/Ethash>). This is often achieved by designing algorithmic problems that require heavy access to other resources, such as memory, and that can be solved efficiently by commercially available hardware.

These alternative systems are in principle more decentralized, but on the flip side they lack the barrier-to-exit effect and its contribution to security.

A similar effect occurs when cloud mining becomes highly available. Some mining entities offer their equipment for rental over the cloud. The clients of these businesses are effectively miners who do not have a long-term stake in the system. As such services become cheaper and more accessible, anyone can easily become a temporary miner, with similar effects on security.

**ASICBoost.** Recall that creating a block requires solving a cryptographic puzzle unique to that block. This involves guessing inputs to a crypto-

graphic hash function. Solving the puzzle is mostly done via brute-force enumeration of different inputs.

A miner can gain an advantage by creating blocks using more efficient methods than his or her counterparts. In addition to better hardware, an advantage can take a more algorithmic form. In fact, an algorithmic “trick” nicknamed ASICBoost has recently made headlines. ASICBoost enables the miner to reuse some of the computational work performed during the evaluation of one input for the evaluation of another. This algorithm is proprietary, patent pending, and it is unclear who is and who is not using it. Such an algorithmic advantage can be translated to lower power consumption per hash. Bitmain, a large manufacturer of ASICs for bitcoin mining that also operates some mining pools, was recently accused by some of secretly deploying a hardware variant of ASICBoost to increase its profits. Allegations were made that this company was politically blocking some protocol improvements that would coincidentally remove their ability to use ASICBoost.

**Communication.** Yet another method for a miner to become more efficient is to invest in communication infrastructure. By propagating blocks faster, and by receiving others’ blocks faster, a miner can reduce the chances that their blocks will not belong to the longest chain and will be discarded (“orphaned”). As off-chain blocks receive no rewards, a better connection to the network translates to reduced losses. Admittedly, with Bitcoin’s current block creation rate, this advantage is rather marginal; blocks are created infrequently, and speeding up delivery by just a few seconds yields relatively little advantage. Nonetheless, better connectivity is a relatively cheap way to become more profitable.

Furthermore, the effects of communication become much more pronounced when the protocol is scaled up and transaction processing is accelerated. Today, Bitcoin clears three to seven transactions per second on average. Changing the parameters of Bitcoin to process more transactions per second would increase the rate of orphan blocks and would amplify the advantage of well-connected miners.

**Economies of scale.** As with any

large entity, professional miners may enjoy the economic benefits of size. With a larger mining operation, such miners are much more likely to invest in different optimizations, such as finding sources of somewhat cheaper electricity, or placing their equipment in cooler regions to provide more efficient cooling to their machines (mining usually consumes a great deal of electricity, and cooling the machines presents a real challenge). Large miners can also purchase ASICs in bulk for better prices. All of this translates to natural advantages to size, a phenomenon that is not specific to Bitcoin but in fact appears in many industries. These effects give large miners an advantage and slowly pull the system toward a centralized one.

Many have raised concerns that most of today’s Bitcoin mining is done by Chinese miners. They enjoy better access to ASICs, cheaper electricity, and somewhat lower regulation than similar operations in other locations. The Chinese government, which tightly controls Internet traffic in and out of China, could choose to disrupt the system or even seize the mining equipment that is within its borders.

### Mining Pools and Risk Aversion

Bitcoin’s mining process yields very high reward but with very low probability for each small miner. A single ASIC that is running full time may have less than a 1-in-600,000 chance of mining the next block, which implies that years can go by without finding a single block. This sort of high-risk/high-reward payoff is not suitable for most. Many would prefer a small, constant rate of income over long periods of time (this is essentially risk aversion).<sup>6</sup> A constant income stream can be used, for example, to pay the electric bills for mining.

**The formation of pools.** Mining pools are coalitions of miners that combine their computational resources to create blocks together and share the rewards among members of the pool. Since the pool’s workers together find blocks much more often than each miner alone, they are able to provide small continuous payments to each worker on a more regular basis.

From the perspective of the Bitcoin network, the pool is just a single min-

ing node. Pool participants interact with the pool's server, which sends the next block header that the pool is working on to all workers. Each member tries to solve the cryptographic puzzle corresponding to this block (in fact, they use small variants of the same block and work on slightly different proof-of-work puzzles to avoid duplicating work). Whenever a worker finds a solution, it is sent to the pool manager, who in turn publishes the block to the network. The block provides a reward to the pool, which the manager then distributes among all of the pool's workers (minus some small fee).

**Reward distribution within pools and possible manipulations.** Many pools are public and open to any willing participant. Obviously, such pools must take measures to ensure that only members who truly contribute to the pool's mining efforts enjoy a portion of the rewards. To that end, every pool member sends *partial solutions* of the proof-of-work to the pool—these are solutions that came “close” to being full blocks. Partial solutions are much more common than full solutions, and anyone working on the problem can present a steady stream of such attempts that fall short of the target. This indicates that the worker is indeed engaged in work, and can be used to assess the amount of computational power each worker dedicates to the pool. Pools thus reward workers in some proportion to the number of shares that they earn (a share is granted for every partial solution that is submitted).

Fortunately, a pool member who has found a valid solution to the puzzle cannot steal the rewards. The cryptographic puzzle depends on the block header, which is under the control of the pool's manager. It encodes a commitment to the contents of the block itself (via a cryptographic hash), including the recipient of the block's rewards. After finding a valid solution for a specific block header, one cannot tamper with the header without invalidating the solution.

Nonetheless, pools are susceptible to some manipulations by strategic miners:

*Pool hopping.* In the early days of Bitcoin, mining pools would simply divide the reward from the latest block



**Mining pools are coalitions of miners that combine their computational resources to create blocks together and share the rewards among members of the pool.**



among all workers in proportion to the number of partial solutions each worker submitted. The number of shares was measured from the previous block created by the same pool.

Some workers came up with a way to improve their rewards: if a pool was unlucky and did not find a block for a while, many partial solutions (shares) would accumulate. If a block was then found by the pool, its reward would be split among many shares. Working to generate additional shares is just as costly as before but yields low expected rewards for this very reason. Instead, the worker could just switch to another pool in which a block had been found more recently, and in which each additional share granted a higher expected reward. If many adopt this behavior, a pool that is temporarily unsuccessful should, in fact, be completely abandoned by all rational miners. Pool-hopping-resistant reward schemes were quickly developed and adopted by most mining pools.<sup>10</sup>

*Block-withholding attacks.* While a miner cannot steal the block reward of a successful solution, he or she can still deny the rewards from the rest of the miners in the pool. The miner can choose to submit only partial solutions to the pool's manager but discard all successful solutions. The miner thus receives a share of the rewards when others find a solution, without providing any actual contribution to the pool. Discarding the successful solution sabotages the pool, and causes a small loss of income to the attacker.

In spite of the losses to an attacker, in some situations it is worthwhile for mining pools to devote some of their own mining power to sabotage their competitors: the attacker pool infiltrates the victim pool by registering some of its miners as workers in the victim pool. These workers then execute a block-withholding attack. Careful calculations of the costs and rewards show that, in some scenarios (depending on the sizes of the attacker and victim pools), the attack is profitable.<sup>4</sup> To prevent such schemes, a slight modification of the mining protocol has been proposed. In the modified version, workers would not be able to discern between partial and full solutions to the proof-of-work puzzle and would not be able to selectively withhold full solutions.


*Eliminating pools.* While pools are good for small miners, mitigating their risk and uncertainty, they introduce some centralization to the system. The pool operator is essentially controlling the combined computational resources of many miners and is therefore quite powerful. Some researchers proposed a technical modification to the mining protocol that undermines the existence of public pools altogether.<sup>7</sup> Under this scheme, after finding a valid solution to the block, the pool member who mined it would still be able to redirect the rewards to themselves (without invalidating the solution). Assuming many miners would claim the rewards for themselves, pools would not be profitable and would therefore dissolve.

### The Economics of Attacks and Deviations from the Rules


Earlier, this article described methods by which a miner can become more dominant within the protocol—both to profit more than his or her fair share and to generate more of the blocks in the chain. The methods discussed thus far do not violate any of the protocol's rules; in some sense, miners are *expected* to make the most of their hardware and infrastructure. This section discusses direct violations of the rules of the protocol that allow miners to profit at the expense of others. In a sense, the existence of such strategies implies that there is something fundamentally broken in the protocol's incentive structure: rational profit-maximizing participants will not follow it.

Informally, the protocol instructs any node to: validate every new message it receives (block/transaction); propagate all valid messages to its peers; broadcast its own new blocks immediately upon creation; and, build its new blocks on top of the longest chain known to that node. Attacks on the protocol correspond to deviations from one or more of these instructions.

**Validation.** A miner who does not validate incoming messages is vulnerable—the next block might include an invalid transaction that he or she did not verify, or reference an invalid predecessor block. Other nodes will then consider this new block as invalid and ignore it. This sets a clear incentive for miners to embed in their blocks only



**The existence of selfish mining strategies implies that there is something fundamentally broken in the protocol's incentive structure: rational profit-maximizing participants will not follow it.**



valid transactions and to validate every new block before accepting it.

Interestingly, despite this logic, sometimes miners mine on top of a block without fully validating it. This practice is known as *SPV mining* (simplified payment verification usually refers to the use of thin clients that do not read the full contents of blocks).

Why would miners engage in building on top of an unvalidated block? The answer again lies in incentives. Some miners apply methods to learn about the hash ID of a newly created block even before receiving its entire contents. One such method, known as spy-mining, involves joining another mining pool as a worker to detect block creation events. Even when the block is received, it takes time to validate the transactions it contains. During this time, the miner is aware that the blockchain is already longer by one block. Therefore, rather than letting the mining equipment lie idle until the block is validated, the miner decides to mine on top of it, under the assumption that it will most likely be valid. To avoid the risk that the next block will contain conflicts with the transactions of the unverified block, the miner does not embed new transactions in the next block, hoping still to collect the block reward.

There is indeed evidence that miners are taking this approach. First, some fraction of the blocks being mined is empty (even when many transactions are waiting to be approved). Another piece of evidence is related to an unfortunate incident that took place in July 2015. An invalid block was (unintentionally) mined due to a bug, and SPV miners added five additional blocks on top of it without validating. Of course, other validating miners rejected that block and any block that referenced it, resulting in a six-block-long fork in the network. Blocks that were discarded in the fork could have contained double-spent transactions.

This event shows the dangers of SPV mining: it lowers the security of Bitcoin and may trigger forks in the blockchain. Fortunately, miners have vastly improved the propagation and validation time of blocks, so SPV mining has less and less effect. The planned decline in the mined reward given to



empty blocks will also lower the incentive to engage in such behavior.

**Transaction propagation.** A second important aspect of the Bitcoin protocol pertains to information propagation: new transactions and blocks should be sent to all peers in the network. Here the incentive to comply with the protocol is not so clear. Miners may even have a disincentive to share unconfirmed transactions that have yet to be included in blocks, especially transactions that offer high fees.<sup>1</sup> Miners have strong incentive to keep such transactions to themselves until they manage to create a block. Sending a transaction to others allows them to snatch the reward it offers first. Thus far, most transaction fees have been relatively low, and there is no evidence that transactions with high fees are being withheld in this way.

Next, let's turn our attention to deviations from the mining protocol intended explicitly to manipulate the blockchain.

**Selfish mining.** Whenever a miner creates a new block, the protocol says it should be created on top of the longest chain the miner observes (that is, to reference the tip of the longest chain as its predecessor) and that the miner should send the new block immediately to network peers.

Unfortunately, a miner can benefit by deviating from these rules and acting strategically.<sup>5,11</sup> The miner's general strategy is to withhold the blocks' publication and keep the extension of the public chain secret. Meanwhile, the public chain is extended by other (honest) nodes. The strategic miner publishes the chain only when the risk that it will not prevail as the longest chain is too high. When the miner does so, all nodes adopt the longer extension that the miner suddenly released, as dictated by the protocol, and they discard the previous public extension.

Importantly, this behavior increases the miner's *share* in the longest chain—meaning, it increases the *percentage* of blocks on the eventual longest chain that the miner generates. Recall that Bitcoin automatically adjusts the difficulty of the proof-of-work so as to keep the block creation rate constant. Thus, in the long run, a larger relative share of blocks in the chain translates to an increase in the miner's absolute rewards.

There is no definite method to verify whether miners are engaging in selfish mining or not. Given that very few blocks are orphaned, it seems like this practice has not been taken up, at least not by large miners (who would also have the most to gain from it). One way to explain this is that miners who attempt such manipulation over the long term may suffer loss to their reputation and provoke outrage by the community. Another explanation is that this scheme initially requires losing some of the selfish miner's own blocks, and it becomes profitable only in the long run (it takes around two weeks for the protocol to readjust the difficulty level).


**Double spending** is the basic attack against Bitcoin users: the attacker publishes a legitimate payment to the network, waits for it to be embedded in the blockchain and for the victim to confirm it, and then publishes a longer chain of blocks mined in secret that do not contain this payment. The payment is then no longer part of the longest chain and, effectively, “never happened.”

This attack incurs a risk: the attacker could lose the rewards for his or her blocks if they do not end up in the longest chain. Surprisingly, and unfortunately, a persistent attacker can eliminate this risk by following more sophisticated attack schemes.<sup>12</sup> The idea is to abandon the attack frequently, publish the secret attack chain, and collect rewards for its blocks. By resetting the attack whenever the risk of losing block rewards is too high, the attacker can eliminate the attack cost and even be profitable in the long term. These schemes are in essence a combination of selfish mining and double-spending attacks.

Currently, double spending is not observed often in the network. This could be because executing a successful double spend is difficult, or because the very miners who could execute such attacks successfully also have a heavy stake in the system's reputation.

## Conclusion

Incentives do indeed play a big role in the Bitcoin protocol. They are crucial for its security and effectively drive its daily operation. As argued here, miners go to extreme lengths to maximize their revenue and often find creative ways to do so that are sometimes at odds with the protocol.

Cryptocurrency protocols should be placed on stronger foundations of incentives. There are many areas left to improve, ranging from the very basics of mining rewards and how they interact with the consensus mechanism, through the rewards in mining pools, and all the way to the transaction fee market itself. 

## Related articles on queue.acm.org

### Research for Practice: Cryptocurrencies, Blockchains, and Smart Contracts

Arvind Narayanan and Andrew Miller

<http://queue.acm.org/detail.cfm?id=3043967>

### Bitcoin's Academic Pedigree

Arvind Narayanan and Jeremy Clark

<http://queue.acm.org/detail.cfm?id=3136559>

### Certificate Transparency

Ben Laurie

<http://queue.acm.org/detail.cfm?id=2668154>

## References

1. Babaioff, M. et al. On Bitcoin and red balloons. In *Proceedings of the 13th ACM Conference on Electronic Commerce*, 2012, 56–73.
2. Ball, M. et al. Proofs of Useful Work. IACR Cryptology ePrint Archive, 2017, 203.
3. Carlsten, M. et al. On the instability of Bitcoin without the block reward. In *Proceedings of the ACM SIGSAC Conference on Computer and Communications Security*, 2016, 154–167.
4. Eyal, I. The Miner's dilemma. In *Proceedings of the IEEE Symposium on Security and Privacy*, 2015.
5. Eyal, I. and Sirer, E.G. Majority is not Enough: Bitcoin mining is vulnerable. In *Proceedings of the International Conference on Financial Cryptography and Data Security*. Springer, Berlin, 2014.
6. Fisch, B.A., Pass, R., Shelat, A. Socially Optimal Mining Pools. arXiv preprint, 2017.
7. Miller, A. et al. Nonoutsourcable scratch-off puzzles to discourage Bitcoin mining coalitions. In *Proceedings of the 22nd ACM SIGSAC Conference on Computer and Communications Security*, 2015.
8. Miller, A. et al. Permacoin: Repurposing Bitcoin work for data preservation. In *Proceedings of the IEEE Symposium on Security and Privacy*, 2014.
9. Nakamoto, S. Bitcoin: A peer-to-peer electronic cash system. Bitcoin.org, 2008; <https://bitcoin.org/bitcoin.pdf>.
10. Rosenfeld, M. Analysis of Bitcoin Pooled Mining Reward Systems. arXiv preprint, 2011.
11. Sapirshstein, A., Sompolsky, Y. and Zohar, A. Optimal selfish mining strategies in Bitcoin. In *Proceedings of the International Conference on Financial Cryptography and Data Security*. Springer, Berlin, 2016.
12. Sompolsky, Y. and Zohar, A. Bitcoin's security model revisited. In *Proceedings of the International Joint Conference on Artificial Intelligence, Workshop on A.I. in Security*, 2017. Melbourne.
13. Zhang, F. et al. REM: Resource-Efficient Mining for Blockchains. Cryptology ePrint Archive. <https://eprint.iacr.org/2017/179>.

Yonatan Sompolsky is a Ph.D. student at the School of Computer Science and Engineering at the Hebrew University of Jerusalem. He is founding scientist of DAGlabs.

Aviv Zohar is a faculty member at the School of Computer Science and Engineering at the Hebrew University of Jerusalem, and a cofounder and chief scientist of QED-it. He has been researching the scalability, security, and underlying incentives of cryptocurrencies for several years.

Copyright held by authors/owners.  
Publication rights licensed to ACM. \$15.00.