



BITCOIN

MAGAZINE®



DISPLAY UNTIL APRIL 15, 2023



THE **BROKE** ISSUE



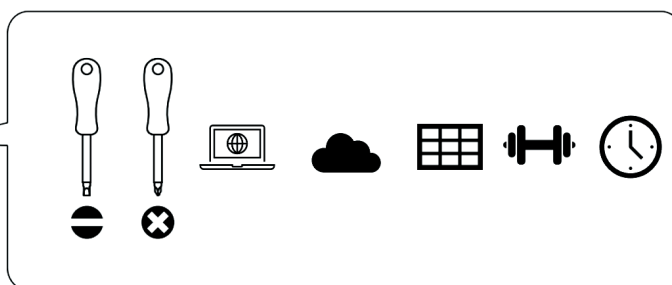
sponsored by
HIVE

BUY THE NUMBERS: BUILDING BLOCKS

BY JOE RODGERS

Welcome to Bitcoin, a peer-to-peer electronic cash system that prevents double-spending with a decentralized network where new coins are made from proof-of-work without a centralized mint or trusted third parties.

This guide helps you discover how miners build blocks for the Bitcoin blockchain, optimize for revenue, and how this incentive helps dissolve censorship.



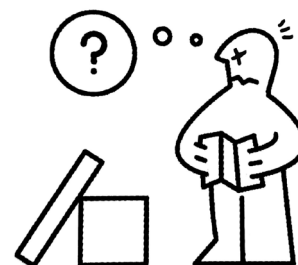
GETTING STARTED

Before we begin building blocks, there are two key pieces of information you need to understand; how bitcoin is mined and by whom.

The computers that mine bitcoin are application-specific integrated circuits, or ASICs. ASICs are specially built and can only perform one operation; hashing SHA-256. They can effectively only mine bitcoin. This means that ASICs cannot be used for anything else. You cannot install a regular computer operating system on them or any other computation except use them for mining bitcoin. Perhaps you could use them as a large paperweight. It is also important to note that ASICs do not build the blocks or broadcast blocks to the greater Bitcoin network. ASICs only mine bitcoin.

The next piece of the puzzle is the bitcoin mining operators who are the people and/or companies that run the ASICs. Mining operators come in many shapes and sizes from pleb home miners with a single ASIC to industrial-scale miners who operate thousands of ASICs across many locations. Mining operators also do not build blocks; they simply operate ASICs, which mine bitcoin.

In order to increase revenue flow and probability of mining a block, mining operators join bitcoin mining pools, which are organizations that coordinate multiple mining operators' efforts. By participating in a mining pool, mining operators are rewarded for their proportional contribution to the entire pool. In other words, mining operators receive their fair share of revenue based on their ASICs' contribution in doing work to find blocks. Mining pools are responsible for building the blocks and broadcasting them to the network. Once blocks are broadcast, they are verified by Bitcoin nodes on the Bitcoin network and further propagated to their peers until these newly mined blocks are received by all nodes, which usually takes around 10 seconds.



→ To summarize, bitcoin mining is performed by mining operators who run ASICs to mine bitcoin. Bitcoin ASICs and mining operators do not build blocks, they simply mine for blocks. Mining operators often participate in mining pools responsible for building and broadcasting blocks to the Bitcoin network.

BUILDING CANDIDATE BLOCKS

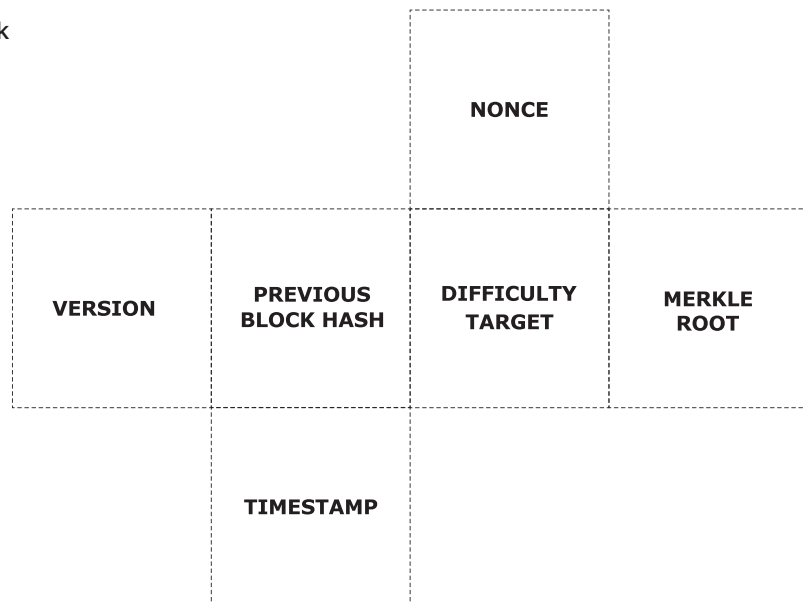
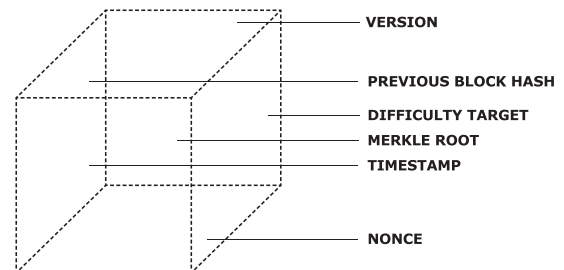
Before a block is added to the blockchain, it begins its journey as a candidate block. A candidate block is a potential, successive block that a mining pool intends on adding to the blockchain upon finding an appropriate nonce. More on the nonce later. Effectively, all confirmed blocks on the blockchain start as candidate blocks.

Blocks are containers that hold bitcoin transactions and are added to the blockchain on average every **10 minutes**. Transactions are selected from a mempool; a list of unconfirmed bitcoin transactions received by your node. Bitcoin transactions are not instantaneous, yet do achieve settlement finality once confirmed by the nodes on the Bitcoin network.

Blocks also have a maximum block size, or block weight, of around **4 MB**. Along with a time constraint, this block size limit introduces a market dynamic where transactions with higher fees will be prioritized and included in blocks before those with low transaction fees. The fee market helps fight censorship by incentivizing inclusion of transactions.

Candidate blocks are constructed by mining pools and meet a set of requirements for miners to include them in a block for the blockchain, specifically the information included in the block header.

- ❑ Version clarifies which kind of block it is. Since there have been several changes to the Bitcoin protocol, there are different versions to be demarcated. This space can also be used to flag for soft forks.
- ❑ Previous block number is an identification number that tells in which order this block was added to the blockchain. Our miner is hoping to add his candidate block on top of the previous block.
- ❑ Transactions selected from the mempool are hashed into a single line of text in the form of a Merkle root.
- ❑ Timestamp, or the time it was added to the blockchain displayed in UNIX.
- ❑ Difficulty Target is the minimum mining difficulty requirement for adding a block to the blockchain.



SIZE	FIELD	DESCRIPTION
4 byte	Version	The Bitcoin Version Number.
32 bytes	Previous Block Hash	The previous block header hash.
32 bytes	Merkle Root	A hash of the root of the Merkle tree of this block's transactions.
4 bytes	Timestamp	The timestamp of the block in UNIX.
4 bytes	Difficulty Target	The difficulty target for the block.
4 bytes	Nonce	The counter used by miners to generate a correct hash.

WHAT ARE WE HASHING?

Once a mining pool has built a candidate block, it is broadcast to mining operators' ASICs who immediately begin mining for that candidate block. Here's an often confusing secret; technically, we are not mining. We are hashing. Yes, ASICs are actually hashing — a trapdoor function that transforms information. The entire Bitcoin mining network is actually hashing, but the meme of mining is easier to understand.

To mine a block, you take a block header and add a nonce (literally a random number). We take the output of the blockheader with nonce and hash it using the **SHA-256** algorithm. Together, they spit out a **256-bit**, or **32-byte** number. If that number is lower than the mining target as outlined in the block header, you have met consensus and have earned the right to add the block to the blockchain. If you do not meet the mining target, you pick another nonce to run through the hashing algorithm again.

Modern ASICs are measured in how many times they can perform the hash function described every second; how many times a second the machine can run a candidate block header with nonce through SHA-256. The current network hash rate of all bitcoin miners is around **260 exahash per second**, or **260,000,000,000,000,000**.

With mining pools coordinating the efforts of thousands of mining operator and even more ASICs, mining pools tell mining operator's ASICs where in the nonce field to begin hashing in order to prevent ASICs duplicating work. All parties want to increase efficiency as much as possible in order to increase the probability of finding a block.

DYNAMIC CANDIDATE BLOCKS

It's important to understand that candidate blocks are fluid.

Transactions are constantly being added to the mempool and miners want to include transactions with the highest fees possible in order to maximize revenue.

Miners scan the mempool for higher-fee transactions and rebuild candidate blocks multiple times during the on-average **10-minute** window of hashing a block.

This means that if a Bitcoin user needs to urgently send his bitcoin transaction, he can include a large fee to ensure a mining pool will include it in the next block. Of course, there is a chance that the transaction might not be seen by a mining pool and included in a candidate block in time. In this event, it would likely be included in the following block.

Transactions vary in size depending on how simple or complex they are. For example, a multisig transaction with many transaction inputs will be much larger in byte space than a standard **1 input, 1 output** transaction. It is also important to note that transaction fees are calculated by the byte size of the transaction, not by the transactional value in satoshis. Remember, there is a limit on the overall size of the block, so users usually must pay a fee to be included.

WHAT ABOUT EMPTY BLOCKS?

Occasionally blocks will get added to the blockchain with no transactions. We call these empty blocks. If miners are incentivized to maximize their blocks for transaction fees, then why do we occasionally see empty blocks?

At block height **761,173**, we have seen **13 (0.27%) empty blocks** over the previous **30 days**. This is a small fraction of the overall blocks that have been mined, but begs the question why. In most cases, an empty block occurs when a miner finds back-to-back blocks. When a miner finds a block, he broadcasts it to the network and immediately begins mining for the next block. Because of basic internet latency, he can have a couple second head start on his peers on the other side of the Earth. In the event he finds his next block shortly after the first block, he might not have time to include transactions in a candidate block. He is incentivized to begin mining right away, and in this scenario, he could mine an empty block.

WHAT HAVE WE LEARNED

There are three key actors in the building block process; mining pools, mining operators, and the ASICs.

ASICs are special computers run by mining operators who participate in mining pools. ASICs and mining operators do not build blocks; they simply hash. Mining pools build candidate blocks and broadcast mined blocks. Blocks are containers for bitcoin transactions that hold up to **4 MB** worth of transactions and are found on average every **10 minutes**. Before a block is actually confirmed on the blockchain, it is a candidate block — a potential block that contains prospective transactions and required information in the block header. Miners optimize for revenue by prioritizing the inclusion of transactions with higher fees in their blocks. 🐼