NYDIG

MARCH 2022

Bitcoin **Mining**

BUILDING THE BLOCKCHAIN

TABLE OF CONTENTS

Introduction

Bitcoin is a decentralized network. No single entity is trusted to update the blockchain.[1] Instead, a subset of network participants, called **miners**, collectively take on this responsibility. This isn't to say that miners run the network. Bitcoin's history proves that they don't.[2] Instead, you can think of miners as security guards who are paid by the network for their labor.

Miners secure the network so that the same bitcoin can't be spent multiple times by the same user. They do so by ordering the network's transactions into blocks, or batches of transactions, which is akin to time-stamping them.

1 The blockchain is the history of transactions made on the network.

2 Between 2015 and 2017, a faction of Bitcoin developers proposed changing the code to increase the block size beyond one megabyte. The largest miners at the time were in favor of this modification, yet the proposal never gained consensus among node operators and ultimately failed to be implemented.

For providing this valuable service, miners are incentivized to bring computing power to the network with new bitcoins. Miners receive 6.25 new bitcoins[3] — as of May 11, 2020 — for each block they add to the blockchain plus the associated fees from the transactions within that block.

Bitcoin's pseudonymous creator Satoshi Nakamoto understood the temptation miners would have to break the rules to enrich themselves. So to discourage malicious behavior, he designed a system where miners have skin in the game.

Adding blocks comes at a cost. In what is known as "proof-of-work," miners have to make an incredible number of simple computations to have a chance at winning a block (it is a competition, after all). Running so many calculations requires real-world energy consumption, and lots of it. In this way, mining connects the physical and digital worlds. A miner who would try to submit a block with invalid transactions does so at their peril. Other network participants would reject an invalid block, thereby wasting the miner's own time and money in the process.

Miners' Role

When a person sends bitcoin from one address to another, computers running the Bitcoin software (known as nodes) that maintain copies of the ledger (known as the blockchain) jump into action. The nodes check that the data is formatted correctly, is less than the block limit of 4 million weight units, and conforms to a host of other technical parameters.

If the transaction passes this initial test, it's added to what is known as the mempool. The mempool is simply a repository of valid transactions not yet included on the Bitcoin ledger.

Here's where miners come in. Nodes don't add groups of transactions, known as blocks, to the blockchain. Miners do. When a miner discovers a new block, the competition for the next one immediately starts. Miners begin aggregating mempool transactions based on priority. Factors such as how long they've been in the mempool and the fees attached to them determine if they'll get included in the next block.

3 The amount of bitcoin miners receive for discovering blocks is cut in half approximately every four years in what is known as a halving. This regular event is programmed into the protocol. Halvings occur, arguably, for two reasons: 1) Satoshi anticipated that with the rising value of bitcoin it would take less of a reward (in bitcoin terms) to incentivize miners to participate and 2) halvings limit the supply of new bitcoin resulting in a decreasing rate of inflation.

Proof-of-Work

While aggregating the transactions into a potential block is simple enough, mining is computationally cumbersome because of the proof-of-work required by the protocol. Consequently, for a valid block to get added to the chain, a miner has a task that, at first glance, might seem unnecessary.

At a high level, bitcoin mining is a lottery. Miners that do the most computations get the most tickets, which increases their odds of winning a block, but there's no guarantee. Like the lottery, finding a block is purely probabilistic.

This extra step serves an essential purpose. By imposing a cost for adding new blocks, proof-of-work discourages miners from including invalid entries like double-spends (using the same bitcoin in multiple transactions). If miners included double-spends, faith in the system would be lost.

However, it is possible, albeit unlikely, for a miner or group of miners to include invalid transactions in a block. In order to do this, miners would need to control more than half of the network computational power in what is known as a "51% attack." By controlling over half the network computational power, these malicious actors could insert transactions that would not be recognized by the rest of the network participants, potentially spending the same bitcoin multiple times. A 51% attack on the Bitcoin network is exceedingly improbable given the amount of processing power it would require. Still, it has happened on other blockchains[4] that have far fewer miners. With these facts in mind, you can think of a blockchain's security as a function of the amount and distribution of its processing power.

Contrary to popular belief, mining doesn't require solving a complicated mathematical problem. In reality, miners are just playing a guessing game with incredibly long odds. The first miner to generate a lower number than the current target set by the network wins. The catch is that, unlike a lottery, miners don't get to choose their numbers.

4 In August 2021, Bitcoin SV endured such an attack.

Hashes

The numbers they play in the Bitcoin lottery come from what is known as a hash function. A hash function is an algorithm that takes a data input of any size and turns it into a numerical value. For example, Bitcoin uses the SHA-256 hash function, which the U.S. National Security Agency created in 2001. For data of any length, SHA-256 returns a value in hexadecimal format (a 64 character long string of numbers and letters that is just another way to write out what you'd think of as a typical number). It's worth noting that the hexadecimal number doesn't store the data used to create it. So knowing the number doesn't mean the SHA-256 algorithm knows what went into making it. You can quickly transform data with SHA-256, but the only way to discover the input is to guess.

The magic of SHA-256 is that the same input will always result in the same output, and each different input yields a unique output. So running "Satoshi" through SHA-256 will always produce the same result. But "Satoshi1" results in an entirely different value.

Satoshi Result

fdd4d9893b23aa6cdb357e1606907c6909
a1231595549e698f779a141d4534c7

Satoshi1 Result

c80273983144ed7509366a59e2b3706f18795
c4ff52b13f02729c83618f38f83

And how "Satoshi1" differs from "Satoshi" is unpredictable: the only way to determine how the two will vary is to run the SHA-256 computation.

Rules of the Game

The rules of the Bitcoin lottery are deceptively simple. Miners compete to be the first to find a hash that has a numeric value that is lower than the target number. The data they input to create the hash isn't arbitrary,

however. If it was, miners could recycle prior hashes with known values. As such, hash inputs must obey a set of rules.

You can think of the inputs used to create a hash as falling into two buckets for simplicity. First, there are constant components. Each input for a hash must include the hash of the previous block and the current target value, among other requirements. The second component type is variable. This part of the entry is known as the nonce.[5] The only limitation set upon what the miner uses for a nonce is that it must be a 32-bit positive number.

Essentially, miners keep entering combinations of these constant and variable components. They change the nonce value with each attempt until someone produces a hash with a value that is lower than the current target. Because there's no formula for the SHA-256 algorithm, miners don't know what nonce value will result in a winning ticket when added to the required components. Just like the lottery, the only way to see if you'll win is to play the game. In the case of bitcoin mining, that means creating as many hashes as you can, as quickly as you can.

Theoretically, a miner could hit on their first try. Still, on average, it takes quadrillions of hashes to find a sufficient one. These minuscule odds are intentional. The protocol's design tries to have blocks mined approximately every ten minutes. There are two reasons for this: to allow nodes enough time to acknowledge changes to the blockchain and to keep new bitcoin issuance on its predetermined supply schedule.

Since the discovery rate varies with the network's hashrate, the target value is modified every 2,016 blocks, or roughly every two weeks. This modification is what is known as the difficulty adjustment. For example, the protocol will lower the target value automatically if miners produce blocks quicker than the desired ten-minute pace. Conversely, if the average block creation time were above ten minutes, the target would increase, creating more winning hash values, and making it easier for a miner to “win” the game.

For a sense of how the difficulty adjustment works, consider the example of rolling a pair of dice. If the target is 12, any roll other than two sixes would be a winner. That works out to a probability of success of 97.2%. But if the target drops to 3, only one combination works, and the success rate plummets to less than 3%. The higher the target, the easier mining becomes.

5 In practice, other components of the hash input can be slightly changed as well, but for this overview we'll only consider the nonce.

In this way, the network constantly adapts to the number of miners on the system and advancements in processing power. No matter how fast the network grows, miners can't add blocks to the chain much quicker or slower than every ten minutes. And because of that fact, miners can't create all 21 million bitcoins until about 2140.

While it takes quadrillions of guesses to find a winning hash, once found, it only takes one computation to confirm it. The miner who first discovers a good hash sends out the inputs they used to the network. Other miners and nodes can then run a single computation to verify its validity.

Mining Pools

After the rest of the network verifies the winning hash, the miner has the right to add the new block to the chain and receive the block reward and associated transaction fees via a coinbase[6] transaction.

Because mining is quite literally a numbers game, it's become economically infeasible for individuals or even small companies to go at it independently. But that doesn't mean mining is only for industrial-sized operators. Smaller miners can join pools, essentially mining collectives, to increase their odds of success.

Pools distribute the mining rewards they earn to their members based on the proportion of hashrate each contributes. So, for example, a miner that makes up 10% of the pool's computing power would get a 10% share of the pool's bitcoin rewards whether their machine was the one to find the block or not.

Key Takeaways

01 Bitcoin mining's purpose is to secure the network & group transactions.

6 Coinbase here refers to an element of the Bitcoin protocol, not the popular exchange. A coinbase transaction is the first transaction in a block and it's how miners reward themselves for finding a new block. The coinbase transaction creates new bitcoin.

02

Miners are essentially playing a lottery where each computation they make is akin to buying a ticket.

03

As an incentive to participate in the validation process, miners who create a new block (which requires winning the lottery) receive the block reward of 6.25 new bitcoins plus the associated transaction fees.

04

Mining difficulty is adjusted approximately every two weeks to keep new bitcoin issuance on schedule and allow for ten minutes between every new block.

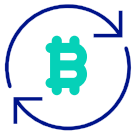
05

Mining is a numbers game. Because of this, individuals and small mining companies band together in pools to increase their odds of success.

A BRIEF NOTE ON BITCOIN MINING & ENERGY USAGE:

Bitcoin mining is undoubtedly energy-intensive. But because energy is the primary cost of doing business, miners are incentivized to find the cheapest sources of electricity they can. This hunt for cheap electricity often means using unconventional energy sources like waste gas from oil wells, stranded or excess energy. Since Bitcoin miners are mobile, wherever there's energy, a bitcoin miner can find a home. Miners can capture potential clean energy that has gone untapped due to its lack of proximity to population centers. Because of bitcoin miners' mobility, the industry encourages the development of clean energy and grid stability. The general public can then use that clean energy when populations move closer to the source. Miners also can serve as buyers of last resort for excess energy capacity. Energy providers produce more power than their customers typically consume. This extra energy usually isn't stored because doing so is economically unviable. Bitcoin miners, however, can turn themselves on when this excess power is available and off when there's a shortage. The result is that bitcoin miners can buy energy that would otherwise go unused (and unpaid for), which lowers the overall cost of production.

Mining Process



Transactions are signed by senders

Signed transactions are then broadcast to other nodes

Miners collect validated transactions into a block

Miners search for a valid proof-of-work. Proof-of-work is a snippet of code showing that miners spent real world resources to derive their solution

Once a valid proof-of-work is found, the block is broadcast to other nodes

These nodes verify transactions in the block are valid

Miners then express their acceptance by building the next block in the chain

DISCLOSURES

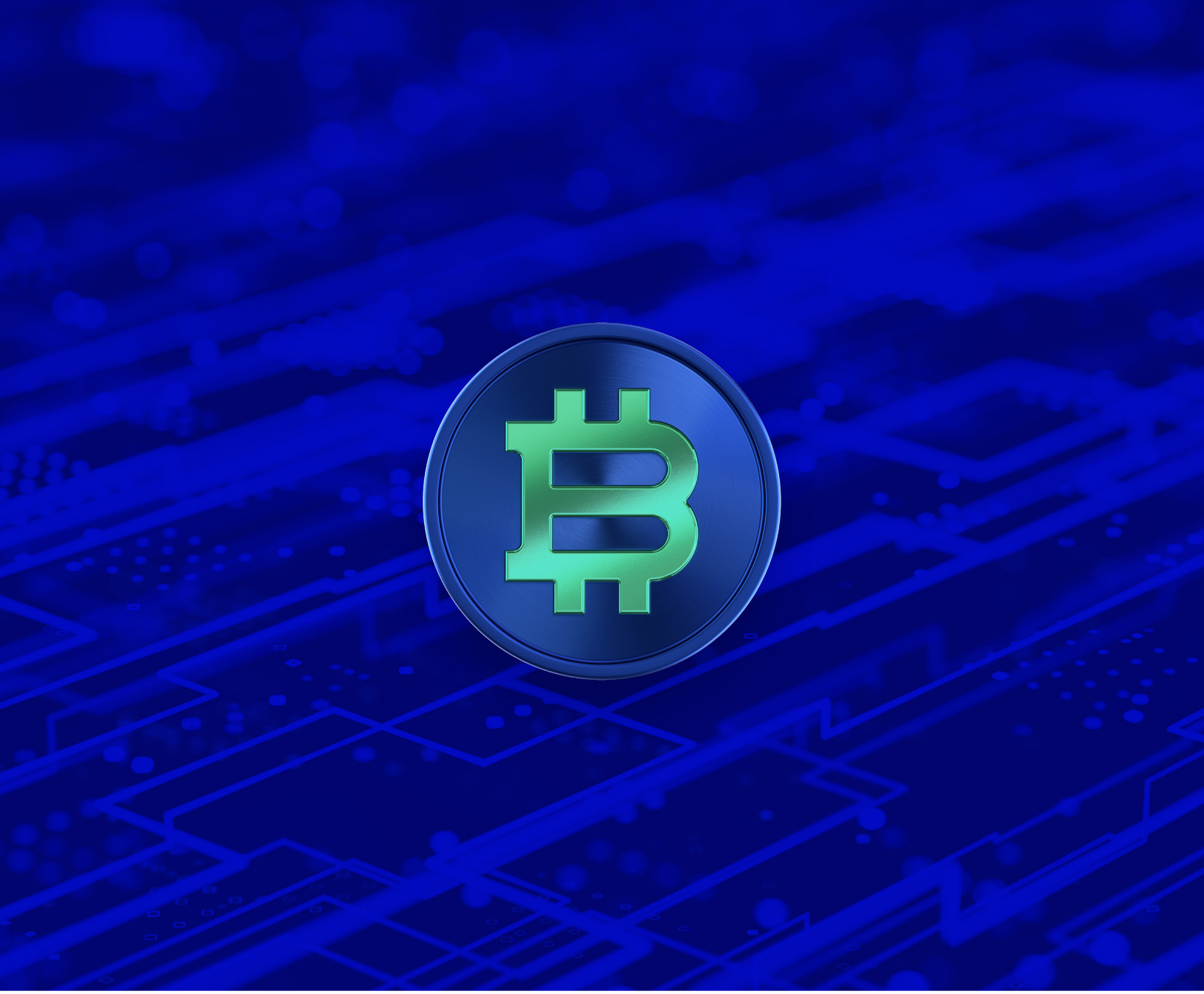
This report has been prepared solely for informational purposes and does not represent investment advice or provide an opinion regarding the fairness of any transaction to any and all parties nor does it constitute an offer, solicitation or a recommendation to buy or sell any particular security or instrument or to adopt any investment strategy. Charts and graphs provided herein are for illustrative purposes only. This report does not represent valuation judgments with respect to any financial instrument, issuer, security or sector that may be described or referenced herein and does not represent a formal or official view of New York Digital Investment Group or its affiliates (collectively, "NYDIG").

It should not be assumed that NYDIG will make investment recommendations in the future that are consistent with the views expressed herein, or use any or all of the techniques or methods of analysis described herein in managing client accounts. NYDIG may have positions (long or short) or engage in securities transactions that are not consistent with the information and views expressed in this report.

The information provided herein is valid only for the purpose stated herein and as of the date hereof (or such other date as may be indicated herein) and no undertaking has been made to update the information, which may be superseded by subsequent market events or for other reasons. The information in this report may contain projections or other forward-looking statements regarding future events, targets, forecasts or expectations regarding the strategies, techniques or investment philosophies described herein. NYDIG neither assumes any duty to nor undertakes to update any forward-looking statements. There is no assurance that any forward-looking events or targets will be achieved, and actual outcomes may be significantly different from those shown herein. The information in this report, including statements concerning financial market trends, is based on current market conditions, which will fluctuate and may be superseded by subsequent market events or for other reasons.

Information furnished by others, upon which all or portions of this report are based, are from sources believed to be reliable. However, NYDIG makes no representation as to the accuracy, adequacy or completeness of such information and has accepted the information without further verification. No warranty is given as to the accuracy, adequacy or completeness of such information. No responsibility is taken for changes in market conditions or laws or regulations and no obligation is assumed to revise this report to reflect changes, events or conditions that occur subsequent to the date hereof.

Nothing contained herein constitutes investment, legal, tax or other advice nor is it to be relied on in making an investment or other decision. Legal advice can only be provided by legal counsel. NYDIG shall have no liability to any third party in respect of this report or any actions taken or decisions made as a consequence of the information set forth herein. By accepting this report in its entirety, the recipient acknowledges its understanding and acceptance of the foregoing terms.



NYDIG

Interested In Learning More?

NYDIG.COM/RESEARCH