COTW: Bitcoin Mining Part 1 of 4: Overview of a Transaction

In our first multi-part Chart of the Week, we dive deep into Bitcoin mining over four distinct pieces. This initial piece covers how mining works and the role miners play in the network, while subsequent pieces examine the infrastructure used, business model and value drivers, competitive environment and strategies employed, and impact on the climate.

Anatomy of a Transaction

To understand Bitcoin mining, one must have a basic sense of how the Bitcoin network works in general. At a high level, the Bitcoin blockchain can be thought of as a decentralized database or distributed ledger comprised of a network of computers, often called nodes and miners. To send a bitcoin, an individual uses a software application that takes the transaction information, the recipient's public key, and their own private and public keys to generate, digitally sign, and broadcast the transaction to the network. Once the network receives the transaction, nodes process it by running validation tasks like checking that the signature is valid and miners organize valid transactions into blocks. To ensure all nodes/miners have the same valid copy of the distributed ledger, a consensus mechanism is used to determine which miner gets to post their block to the blockchain. Bitcoin uses a proof-of-work consensus mechanism, where miners work to be the first to solve a puzzle, with the winner earning the right to post the block and receive the block reward and transaction fees. The distributed ledger then stores the data in a chained format using hash pointers to make the blockchain easily searchable and tamper-evident.

Exhibit 1: Anatomy of a Bitcoin Transaction

Step	Party	Action
1)	User	An individual uses a software app such as a digital wallet to take transaction info, the recipient's public key, and their own private and public key to generate, digitally sign, and broadcast the transaction to the network
2)	Nodes	Nodes receive, validate, and relay the transaction to other nodes on the network via a gossip protocol
3)	Miners	Miners organize transactions into blocks, work to solve the mining puzzle, and once done, broadcast the winning block/puzzle solution to the network before its verified and added to the blockchain
4)	Nodes	A copy of the blockchain is maintained and continuously updated on thousands of computers around the world. A transaction will be considered final once several transactions have occurred on top of it

Source: GSR

Hash Functions

One key mechanism used not only in bitcoin mining but also in many other areas such as digital signatures and blockchain construction is that of cryptographic hash functions. A hash function is an algorithm that converts an arbitrary amount of input data into a fixed length, numeric output, known as a hash, such as 256 bits (ones and zeros) or 64 hexadecimal (hex) characters. A hash can be thought of as some input data's digital fingerprint. To create this unique identifier for the input data, the hash function splits the data into pieces and runs many rounds of local operations on them like AND, OR, and XOR, losing information as it goes. Hash functions should be one-way (the only way to know the input from a given output is to try all possible inputs), deterministic (returns the same output for a given input), easy to compute (but not so easy that one can quickly cycle through all potential inputs to solve), and produce few collisions (two different inputs should be very unlikely to produce the same output).

Hashes have several benefits, such as improving efficiency and allowing for data verification without revealing the contents of the data. For example, rather than store passwords in a database that could potentially be hacked, a website can store hashed passwords. Then, when a user enters his or her password upon log-in, the website can simply take a hash of the entered password and compare it to its database of hashed passwords, materially enhancing security by not storing the passwords themselves (most websites add further security modifying this in what's called a salted hash).

Bitcoin uses a specific hash algorithm called SHA-256, which can be explored in this online SHA-256 hash calculator. SHA-256 produces an unfathomably large number of potential hashes. The function generates 256-bit hash values, meaning the output space equals 2^{256}, or equivalently 16^{64}, which is approximately 1.158×10^{77}. To contextualize the magnitude of this output space, the number of atoms in the observable universe is estimated to be in the realm of 1×10^{80}. SHA-256 hashes are expressed as a

64-digit hex number, where each character represents a number between 0 and 15. We show several inputs and outputs in the exhibit below. Notice the high avalanche effect, where making one small change to the input data completely and unpredictably changes the resulting hash.

Exhibit 2: SHA-256 Example Hashes

Input		SHA-256 Hash (Output)
Hello, World	hash →	03675ac53ff9cd1535ccc7dfcdfa2c458c5218371f418dc136f2d19ac1fbe8a5
Hello World!	hash →	7f83b1657ff1fc53b92dc18148a1d65dfc2d4b1fa3d677284addd200126d9069
Four score and seven years ago our fathers brought forth, upon this continent, a new nation, conceived in liberty, and dedicated to the proposition that all men are created equal.	hash →	711126a836a33364a6fac8e473ca1590402547d33fa4f3e7455e14199a482bcd

Source: GSR

Mining

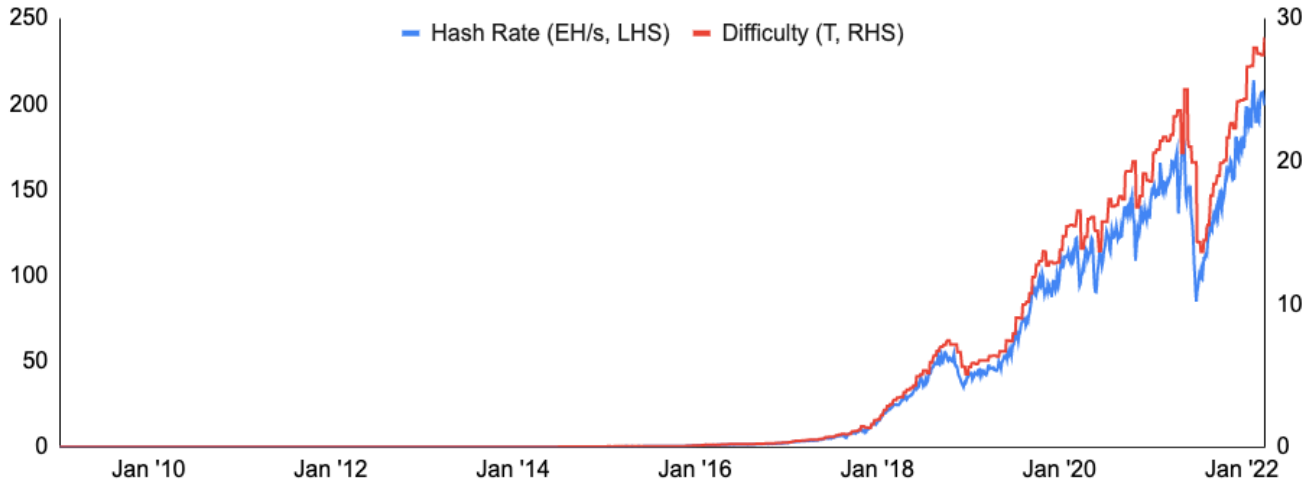
To mine bitcoin, a miner will work to solve the Bitcoin mining puzzle. First, transactions are generated, signed, and broadcasted to the network by users, and these transactions are then received, validated, and relayed to other nodes before going into a pending transactions queue known as the mempool. Given the inherent latency in networks where information propagates from peer-to-peer, each node has their own copy of the mempool. Miners then start the mining process by selecting the desired transactions from their mempool to include in their proposed block, or candidate block, typically prioritizing the transactions with the highest fees. The miner then attaches a random number called a nonce, and takes a hash of this proposed block in an attempt to produce a hash that is lower than the current “target”, which when successful yields a valid solution to the puzzle, known as a proof-of-work. Miner’s that can compute hashes more quickly than others are more likely to find a solution to the puzzle first; this concept is known as hashrate which measures the speed in which miners can compute hashes each second. For context, the total Bitcoin network hashrate today is about 200 exahash per second (EH/s), this means that all miners in aggregate are calculating about 200 quintillion hashes per second.

Simply put, the process of mining can be thought of as computers quickly iterating input data through the SHA 256 cryptographic hash function. Each iteration returns a hash which is simply a number, and if that number is a sufficiently small number based on the current network difficulty, that hash will be

deemed a valid proof-of-work. Assuming all other network rules are followed, the miner that first distributes a new block with a valid proof-of-work will receive the mining rewards. In essence, miners are participating in a lottery where their probability of 'winning' each lottery is equal to their hashrate as a proportion of the total network's hashrate. Given the mathematical properties underpinning cryptographic hash functions like SHA 256 (deterministic, one-way function with a high avalanche effect), there are no techniques to quickly find a proof-of-work beyond brute force computation, hence the name. There are some techniques to slightly expedite the process but they are largely commoditized today (i.e., AsicBoost) so the mining process is a work-based lottery.

As more mining rigs come online and the chip technology improves, the odds increase that the mining puzzle will be solved faster. However, the Bitcoin network automatically changes the difficulty required to solve the puzzle as the network hashrate changes such that it takes roughly ten minutes for the network to produce a new block on average. For example, if more miners join the network and the network hashrate rises significantly, the network will increase the difficulty by lowering the mining puzzle target, decreasing the probability that any given hash will be lower than the target. This adjustment to mining difficulty occurs every 2,016 blocks, or roughly every two weeks on average. The total network hashrate has generally increased over time, with the most noticeable decline in both hashrate and difficulty occurring in May to June of last year when China cracked down on mining. Network hashrate subsequently recovered as Chinese miners relocated and as new and existing miners added new rigs.

Exhibit 3: Bitcoin Mining Difficulty & Total Network Hashrate



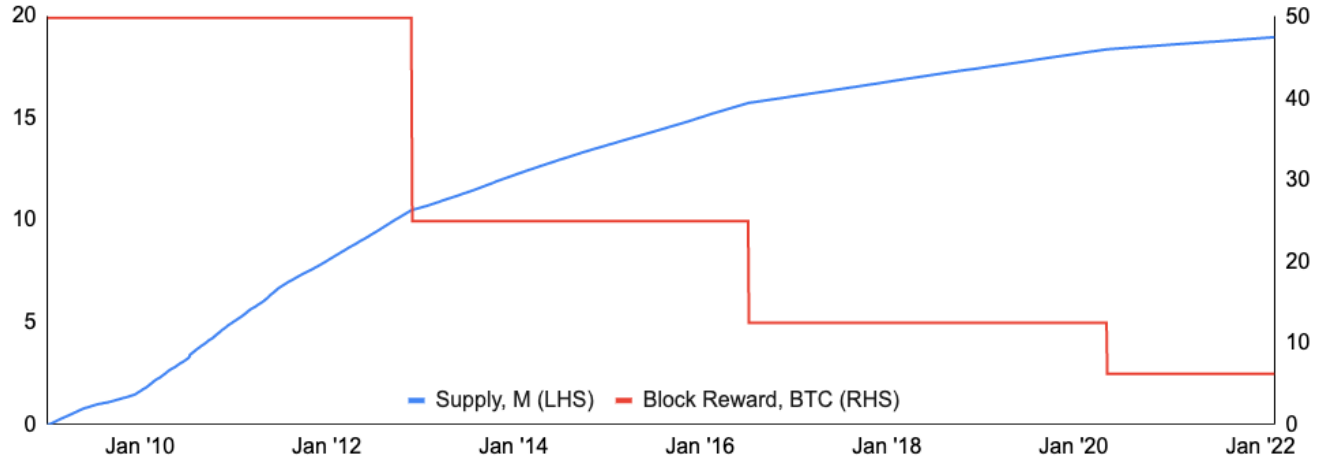
Source: Blockchain.com, GSR

Mining Rewards

Bitcoin miners secure the network by making it prohibitively expensive to manipulate historical transactions, providing a sense of finality for transactions. Miner's are compensated for this service through block rewards and transaction fees, which in aggregate can be viewed as the security budget protecting Bitcoin's value. The first miner that generates a proof-of-work and distributes a valid block will be rewarded the block reward and all the transaction fees inside the newly mined block. Nodes in

the network will validate this newly received block, and if valid, they will append it to their copy of the blockchain and extend it. Block rewards are currently set at 6.25 bitcoin per block, but they are cut in half every 210,000 blocks, or roughly every four years. The halving process makes bitcoin's monetary policy disinflationary, reducing the rate of inflation by 50% every four years on average. With inflation halving every 210,000 blocks, eventually you get to a point where the block reward would be theoretically halved to a unit of bitcoin less than one satoshi – the smallest unit of bitcoin equal to 0.00000001 bitcoin – but given bitcoin cannot be divided beyond this, the block reward cannot be halved any further and it ceases to exist. This will bring the inflation rate down to zero just shy of 21m bitcoin being produced. This is expected to occur around the year 2140 based on average block times. However, we would note that given improvements in computational power, halvings have been occurring slightly faster than every four years which could pull this timeline forward by a few years.

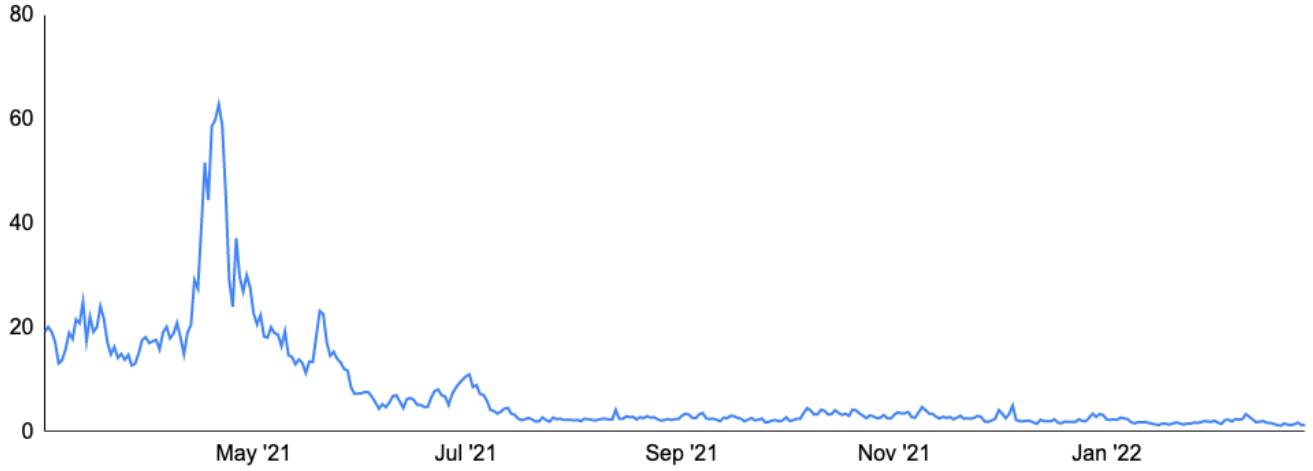
Exhibit 4: Bitcoin Supply & Block Rewards



Source: Blockchain.com, GSR

In addition to the block reward, miners are entitled to transaction fees in the block they mined. Transaction fees are a "voluntary" fee paid by users of the network to incentivize miners to include their transaction in a block. In reality, these fees are only voluntary if you are mining your own transaction, as nodes will not relay zero-fee transactions by default. Given the limited size and frequency of blocks, transaction fees are a direct outcome of the supply versus the demand for blockspace. Consequently, transaction fees tend to increase significantly during times of high network usage as users try to entice miners to include their transaction in a block. While high transaction fees, low throughput / slow finality, and price volatility has limited bitcoin's use as a payment mechanism so far, such fees act as another incentive for miners and are thought to be one key component sustaining miner profitability as block rewards move down over time through halvings. BitOoda research estimates that the value generated from transaction fees will begin to flip the value generated from block rewards around the 2028 halving. However, the vast majority of miner revenue today comes from the block reward, with transaction fees representing only 1-5% of the total payout depending on the time period observed. In recent months transaction fees have been particularly low averaging about 1% of the total reward.

Exhibit 5: Average Fee per Transaction (USD), Last 12 Months



Source: Blockchain.com, GSR

In addition to transaction fees, other items may sustain bitcoin mining long after the last block reward, such as a falling price of electricity or mining equipment, as well as a rising price of bitcoin. While it is true that the amount of bitcoin given out as a block reward has fallen over time, the rising price of bitcoin has made the value of such block rewards generally increase in USD terms historically. With enough price appreciation, the same may be true going forward.

Mining Pools

As the network hashrate has risen over time and difficulty has increased, it has become more and more difficult for many miners to consistently produce blocks and generate consistent revenue. This is particularly true for small miners, but even the largest miners control just a low-single-digit percentage of the global hashrate. As such, mining pools were formed to help smooth out future revenue. In mining pools, miners pool together compute resources to mine blocks as a group, sharing processing power over a network and splitting the rewards. The concept is no different than an office lottery pool, and pools can simply be thought of as a diversification tool to decrease the swings that luck will have on realized outcomes. Participating in a pool does not increase a miner's expected return, but they are simply changing the distribution around the mean outcome. Participation in a mining pool actually decreases expected returns by the fees charged by the pool operator which may range from about 0% to 4% of the rewards generated. In this sense, pools can be thought of as an insurance mechanism, paying a small premium to smooth out returns and hedge the risk of ruin in the event of bad luck.

Mining pools utilize multiple different types of payout structures today with varying risk assumptions amongst them. Different variations of pay per share (PPS) models tend to be the most popular today. Most notably, PPS models provide a regular payout based on work done, irrespective of the mining pool's results. As an extreme example, imagine a PPS pool possessing 10% of the network's hash rate and assume they had a very unlucky day and did not mine any bitcoin. Based on the daily bitcoin emissions currently (900), the pool operator would need to pay out 90 bitcoin to its miner constituents

based on each of their respective percentages of the contributed hash rate, even though the pool did not mine any bitcoin that day. In a PPS model, the risk of bad luck is assumed and managed by the pool operator, and therefore these tend to be the most expensive pool payout structures. There are also further variations in PPS models with nuances for how transaction fees are incorporated. Another common model is the pay per last n shares (PPLNS) approach. In this approach, miners assume the risk of bad luck and they are only compensated for the work contributed after a block is mined. Once a block is mined, this model looks back in time and compensates miners based on the amount of work contributed to that block. This model still provides risk reduction benefits over solo mining, however the risk of bad luck is not removed entirely. PPLNS models tend to be the cheapest as the pool operator is not backstopping the risk of bad luck.

Exhibit 6: Considerations Amongst the Common Options for Pool Payouts

	Pay Per Share (PPS)	Pay Per Share Plus (PPS+)	Full Pay Per Share Plus (FPPS+)	Pay Per Last N Shares (PPLNS)
Block Rewards	Expected Value	Expected Value	Expected Value	Actual Value
Transaction Fees	None	Actual Value	Expected Value	Actual Value
Luck Factor	None	Low	None	High
Regular Payout	Yes	Yes	Yes	No
Fees	Medium	High	Highest	Low

Source: GSR, Nicehash, Minebest

Lastly, mining pools help keep mining decentralized by making it feasible for small miners to operate profitability on a daily basis. If an at-home miner wanted to invest in one currently top-of-the-line ASIC, they would pay about $10-15k for a rig with a hashrate of 110 TH/s. Given the Bitcoin network hashrate is about 200 EH/s, this at-home miner would have roughly a 1 in 1.82 million chance of mining each block. With an average block time of 10 minutes, this miner would not be expected to win a block for nearly 35 years mining on his own. This implicitly assumes hashrates remain constant which is certainly a false assumption, but this picture would look even worse for the at-home miner if this was accounted for. However, if the miner has access to sufficiently cheap electricity, they can enter their one mining rig into a pool and generate a small profit on a daily basis, a proposition that may make the investment more palatable. This ability helps keep small miners in business and helps prevent the network of Bitcoin miners from becoming too top heavy.

Exhibit 7: Mining Pool Distribution, Last One Month

Rank	Network	Hash Rate Share	Blocks Mined	Empty Blocks Count	Empty Blocks	Avg. Block Size (Bytes)	Avg. Tsx Fee per Block	Tx Fees of Block Reward
1	Foundry USA	19.64 %	866	1	0.12 %	1,153,916	0.074	1.18 %
2	AntPool	13.88 %	612	2	0.33 %	1,208,756	0.076	1.22 %
3	F2Pool	13.22 %	583	6	1.03 %	1,171,507	0.074	1.19 %
4	Binance Pool	11.86 %	523	2	0.38 %	1,180,275	0.076	1.22 %
5	Poolin	11.72 %	517	0	0.00 %	1,134,351	0.067	1.07 %
6	ViaBTC	10.18 %	449	5	1.11 %	1,134,896	0.071	1.13 %
7	SlushPool	6.33 %	279	3	1.08 %	1,170,376	0.078	1.25 %
8	BTC.com	5.51 %	243	0	0.00 %	1,101,697	0.065	1.04 %
9	SBI Crypto	2.31 %	102	1	0.98 %	1,057,552	0.062	0.99 %
10	Luxor	2.27 %	100	0	0.00 %	1,210,599	0.073	1.16 %

Source: BTC.com, GSR.

Authors:
Brian Rudick, Senior Strategist
Matt Kunke, Junior Strategist

Sources

University of Michigan: Blockchain & Cryptocurrency Explained
Duke University: Blockchain Business Models
Antonopoulos: Mastering Bitcoin
BitOoda

About GSR

GSR is a global leader in digital asset trading, market making, OTC derivatives, and investments. We operate in a culture of excellence and leverage our first-rate reputation, deep relationships and proprietary trading technology to move swiftly and capitalize on market opportunities.

GSR's experienced team brings together decades of institutional trading expertise, while our industry-leading proprietary technology stack anchors everything we do.

Our main service areas are: market making; proprietary and algorithmic trading; client execution; structured products; risk management solutions; and portfolio investments.

For more information or if we can help with anything, please see gsr.io or contact us at gsr@gsr.io.

Required Disclosures

This material is a product of the GSR Sales and Trading Department. It is not a product of a Research Department, not a research report, and not subject to all of the independence and disclosure standards applicable to research reports prepared pursuant to FINRA or CFTC research rules. This material is not independent of the Firm's proprietary interests, which may conflict with your interests. The Firm trades instruments discussed in this material for its own account. The author may have consulted with the Firm's traders and other personnel, who may have already traded based on the views expressed in this material, may trade contrary to the views expressed in this material, and may have positions in other instruments discussed herein. This material is intended only for institutional investors. Solely for purposes of the CFTC's rules and to the extent this material discusses derivatives, this material is a solicitation for entering into a derivatives transaction and should not be considered to be a derivatives research report.

This material is provided solely for informational purposes, is intended for your use only and does not constitute an offer or commitment, a solicitation of an offer or comment (except as noted for CFTC purposes), or any advice or recommendation, to enter into or conclude any transaction (whether on the indicative terms shown or otherwise), or to provide investment services in any state or country where such an offer or solicitation or provision would be illegal.

Information is based on sources considered to be reliable, but not guaranteed to be accurate or complete. Any opinions or estimates expressed herein reflect a judgment made as of the date of publication, and are subject to change without notice. Trading and investing in digital assets involves significant risks including price volatility and illiquidity and may not be suitable for all investors. GSR will not be liable whatsoever for any direct or consequential loss arising from the use of this Information. Copyright of this Information belongs to GSR. Neither this Information nor any copy thereof may be taken or rented or redistributed, directly or indirectly, without prior written permission of GSR. Not a solicitation to U.S. Entities or individuals for securities in any form. If you are such an entity, you must close this page.