An In-depth Analysis of Mining Pools Revenue

Stefano **Bistarelli**[1,†], Gianlorenzo **Giuliani**[1,†], Ivan **Mercanti**[1,*,†] and
Francesco **Santini**[1,†]

[1]*University of Perugia, Perugia, Italy*

Abstract

The success of Bitcoin has attracted much attention from both industry and academia. The Bitcoin
network mainly comprises mining pools responsible for network security and performance. While
many measurements are available for the Bitcoin network, more information is needed to understand
the behavior of mining pools, such as their revenue and transaction collection strategies. This paper
aims to explore some of Bitcoin's mining history and compare its performance. We use over 700, 000
blocks mined from 2009 to today, serving as the coin's foundation. We have extracted structured and
explanatory information about the pools' work over the years by analyzing the blockchain data. It
is worth noting that the number of blocks mined by some mining pools only sometimes guarantees
significant gains. Miners' overall earnings have been significantly affected by the fluctuation in Bitcoin's
value over the years.

Keywords
Bitcoin, Mining pool, Halving,

1. Introduction

The word Bitcoin [1] is mistakenly associated with one of many online payment methods or, in
some cases, a risky investment. However, Bitcoin is much more than that. The creator, known
by the pseudonym Satoshi Nakamoto, had in mind a currency revolution, a system that could
decentralize money, removing it from the control of banks and state institutions. For this very
purpose, he created the first cryptocurrency, which has been so successful that it has led to the
birth of more than 25,000 new virtual coins,[1] none of which, however, has had the resonance
that BTC has had. The purpose of this paper is to trace the history of Bitcoin, drawing on more
than 700,000 Blockchain blocks mined from 2009 to the present, the coin's backbone, to infer
which miners contributed most to BTC's success, succeeding in creating virtual capital in the
process. We obtained the required information by extracting data directly from the Blockchain.
We used several scripts to transform the data into statistics and graphs, enabling us to determine
who earned the most from the mining process and identify the factors influencing a miner's
pool selection. Moreover, we analyze mining pools' performance in terms of the rewards they

---

[1]https://coinmarketcap.com/all/views/all/.

have accumulated over the years and their ability to generate new blocks efficiently using their computational power.

The rest of this paper is structured as follows. Section 2 overviews the Bitcoin protocol and hash power. Section 3 reports the stats about mining pools and their gains. Then Section 4 provides information about the mining evolution during the years and the impact of the halving[2] to the mining pools. Section 5 discusses the most important works on mining pools. Finally, Section 6 draws the final conclusions.

2. Background

In this section, we present an overview of the Bitcoin consensus protocol, and we define transactions.

2.1. The Bitcoin Protocol

Bitcoin is a peer-to-peer asynchronous network whose nodes host a ledger recording economic transactions grouped into *blocks*. The ledgers are trees of blocks with a pointer (*handle*) to a *leaf block at maximal depth*; the *blockchain* is the sequence of blocks from the handle to the root block, (*genesis block*). Blocks are created by particular network nodes – the *miners* – and contain information, such as, for example, related to transactions and a pointer to the current handle of the miner's ledger.

Once a block has been mined, the miner (*i*) adds the block to its ledger (therefore, the depth of the ledger increases and the handle is updated); and (*ii*) broadcasts it to all the connected nodes of the network. Every node receiving the new block updates its local copy of the ledger by inserting the block in the correct position, and, if necessary, it also updates its handle. If the block cannot be connected to the ledger (because, due to network delays, a previous block has not been delivered), it is added to the local set of the miner and will be inserted afterward (orphan blocks).

Because of asynchrony, it may happen that two nodes mine and broadcast a block almost concurrently, yielding different ledgers with different handles (and, therefore, with other blockchains). This phenomenon, called *fork*, is at the core of the inconsistencies of Bitcoin, and to overcome this problem, the protocol uses a probabilistic algorithm. In particular, Bitcoin has a technique to regulate the mining of blocks, called *Proof of Work* [2] (PoW). According to PoW, miners can add a block only if they solve a computational problem. Technically, the problem consists of finding a number (a nonce) which is inserted into the block header. The block header is then hashed, and if the numerical value of the hash is less than a predefined condition, which is called target, then the miner is said to have mined the block. The only way to find such a nonce is through an exhaustive search. The finding of suitable nonce values can be modeled as a Bernoulli trial with a probability of $L/2^{256}$ of success, where L is the target. The time needed to mine a new block depends on the PoW's difficulty and the miners' hashing power. The faster miners are, the more computational power they own, the higher the probability of forks and, thus, the more likely the inconsistency between miners. For this reason, the Bitcoin

---

[2]The bitcoin reward that miners receive is halved.

PoW difficulty is determined by a moving average targeting a certain number of blocks per hour. If they are generated too (slowly) rapidly, the difficulty is (decreased) increased, as shown by Nakamoto [1]. The current protocol modulates PoW to have six blocks per hour on average.

To further reduce the probability of inconsistencies, Bitcoin also uses the so-called *eventual consistency* (also known as n-consistency [3]). This is a weak version of consistency, according to which the protocol considers consistent those ledgers with the corresponding blockchains equal up to the last few blocks. In particular, Bitcoin considers both transactions and miner's rewards in blocks at a depth greater than five as confirmed [4].

2.2. Evolution of mining hardware

In the early stages, the competition among miners was low, so the computational energy required to create new blocks and obtain rewards could be quickly processed on CPU-equipped devices such as ordinary personal computers. However, as competition among miners increased, significant developments in Bitcoin mining hardware emerged:

- Mining with GPUs: The first significant step in mining hardware innovation occurred in 2010. Video cards were first used for Bitcoin mining because they are optimized for parallel mathematical calculations, making the mining process much more efficient than CPUs. This made Bitcoin mining about six times more efficient than with CPUs, even though GPUs cost only twice as much.
- Mining with FPGAs: FPGA (Field-Programmable Gate Array) devices were used for Bitcoin mining in 2011. FPGAs could perform the calculations required for mining twice as fast as the best GPUs. However, the configuration of FPGAs required considerable effort at the software and hardware level.
- Mining with ASICs: In 2013, ASIC (Application-Specific Integrated Circuit) technology was introduced. ASICs were designed and optimized for Bitcoin mining and led to a significant increase in computing power, outperforming CPUs, GPUs, and FPGAs.[3]

In Bitcoin mining, the hash rate is the standard measure of a miner's computing power to solve the cryptographic hashes required by proof of work. The hash rate determines how quickly a miner can provide solutions based on a specific hash and is used to estimate the efficiency of the hardware used for mining cryptocurrencies. For example, an ordinary computer can solve a few mega hashes per second (MH/s). At the same time, FPGAs or ASICs can run from hundreds of MH/s to tens of tera hashes per second (trillions of hashes per second). The global hash rate of the Bitcoin network as of March 14, 2023, is 550.85 EH/s[4].

2.3. Transactions

A Bitcoin *wallet* stores a collection of public/private key-pairs of a user, not directly bitcoins. A Bitcoin address is an identifier of 26-35 alphanumeric characters, and it strictly derives from the hash of a generated public key (*pubkey* in the following) [[4]]. A private key is a random 256-bit number, and the corresponding pubkey is generated through an *Elliptic Curve Digital Signature*

---

[3]https://www.coindesk.com/tech/2020/04/26/the-rise-of-asics-a-step-by-step-history-of-bitcoin-mining/.
[4]https://academy.bit2me.com/it/que-es-el-hash-rate/.

Algorithm (*ECDSA*). A transaction *input* must store the proof it belongs to who wants to reuse the money received in a previous transaction. The *output* of a transaction instead describes the destination of bitcoins by providing a challenge to users. Hence, the ownership of the coins is expressed and verified through links to previous transactions. For example, to send three bitcoins (BTC) to Bob, Alice needs to refer to other transactions she has previously received, the amount of which is at least 3 BTC. To lock the coin, a script called *scriptPubKey* is used, while to prove the ownership of a coin, a script called *scriptSig* is used instead. In the following, we will refer to them as "locking script" and "unlocking script".

2.4. Mining pool share and reward systems

A "share" is a potential solution for a block but not necessarily a block solution itself. For instance, if a block solution is a number that ends with ten zeros, a share may be a number with only five zeros at the end. However, eventually, one of the shares will have not only 5 but 10 zeros at the end, and this will be the actual block solution[5].

A common mistake among new miners is to think that they have found a block (or even two) when they see phrases like "Share Found" and "Share accepted" in their mining software. In reality, mining pools need shares to estimate the miner's contribution to the work performed by the pool to find a block. Based on the shares a miner sends to the pool, the pool can plot a miner hash rate graph and determine whether a miner is online, among other things.

There are numerous reward systems, but the majority of mining pools operate with the PPS, FPPS, PPS+, and PPLNS payment models[6]:

- *Pay-Per-Share (PPS)*: in this payment method, a miner receives a fixed payment rate for each completed share. After paying mining pool fees, miners receive a fixed share each day. Therefore, in the PPS method, returns are relatively stable.
- *Pay-Per-Last-N-Shares (PPLNS)*: is closely related to the number of blocks mined. If the mining pool mines more blocks in a day, the miners get a higher profit, calculated according to each one's share; if the mining pool fails to mine a block during the whole day, the miners' profit is zero. The PPLNS model is highly correlated with a pool's luck, the probability of mining a block.
- *Pay Per Share Plus (PPS+)*: combines the previously mentioned methods, PPS and PPLNS. The reward per block is settled according to the PPS model, while the pool and transaction fees are settled according to the PPLNS model.
- *Full Pay Per Share (FPPS)*: in this model, the reward per block and the mining service fee are settled based on theoretical profit. A standard transaction fee is calculated within a certain period and distributed to miners based on their hash power contributions in the pool. With the FPPS method, one gets paid regardless of whether the pool finds a block.
- *Proportional*: in the proportional method, miners earn shares until the pool finds a block. After that, each user receives a reward $R = B \times (n/N)$, where n is the share amount, and N is the total amount of all shares in the cycle.

---

[5]https://2miners.com/blog/what-is-share-and-the-share-difficulty-when-you-are-mining-at-the-pool/.
[6]https://minebest.com/blog/pps-vs-fpps-vs-pplns-vs-pps-mining-pool-payouts-explained.

- *Pooled mining (BPM)*: also known as Slush system because it was initially used in Slush's pool, it uses a system in which the oldest shares from the beginning of a mining cycle have less weight than the newest shares. A new cycle begins when the pool resolves a block, and miners are rewarded proportionally to the quotas submitted.
- *Solo Mining Pool*: in this case, the reward for the block is not distributed among all miners. The entire reward goes to the miner who finds the block.
- *Peer-to-Peer Mining Pool (P2Pool)*: It decentralizes the responsibilities of a pool server. Miners work on a share, mining at a lower difficulty at one share block every 30 seconds. A share block is transmitted and joined to the blockchain when it reaches the network target. Miners are rewarded proportionally to the shares sent before the target block.
- *Geometric method (GM)*: it is based on the same idea as the BPM method: the score assigned for each new share, relative to the existing score and the score of future shares, is always the same, so there is no advantage in mining earlier or later in the cycle.
- *Double Geometric method*: generalized version of the Geometric and PPLNS methods. Introduces a new parameter: o (cross-round leakage). When $o = 0$, this method becomes the Geometric method. When $o = 1$, it becomes a variant of PPLNS with an exponential decrement[7].
- Pay On Target (POT): it is a variant of the PPS model. In this model, payments to miners are not determined by the work provided by the pool but by the difficulty of the work completed by the miners and returned to the pool. This method introduces more significant variability in payments than the traditional PPS model.
- *Pay Per Last N Shifts/Groups (PPLNSG)*: this payment method is similar to PPLNS, but with the difference that dues are grouped into shifts (shifts or groups), and these shifts are paid as a whole.
- *Shared Maximum Pay Per Share (SMPPS)*: is a payment method similar to the Pay Per Share (PPS) model, but with a specific limitation: the reward of all miners is never more than what the mining pool earns.
- *Recent Shared Maximum Pay Per Share (RSMPPS)*: is a payment method similar to the SMPPS method, but gives payment priority to the most recent miners[8].

3. Mining pool stats

To analyze the content of the Blockchain, a sample of $700,000$ blocks of it, mined from January 2009 to March 2023, was saved in a MongoDB database [5]. The first step is to infer from the coinbase and address fields which miner or pool (set of miners) is responsible for mining the block. A JSON [6] file from a GitHub repository updated as of January 2023 and with more than 50 users contributing [9], was used for this purpose. Within the file, each tag or address of a miner is associated with its name and, if it exists, its website. We look for matches between present tags and coinbase/address fields extracted from the Blockchain. If a match is found, the resulting mining pool (or miner) is added to the transaction information in the DB. In this way,

---

[7]https://en.wikipedia.org/wiki/Mining_pool.
[8]https://medium.com/luxor/mining-pool-payment-methods-pps-vs-pplns-ac699f44149f.
[9]https://github.com/blockchain/Blockchain-Known-Pools.

we found the creator of over $550,000$ blocks. Finally, to get a complete overview of the miners' earnings, it is necessary to multiply the value field, the bitcoins received for mining that block, by the value of the bitcoin. We used the dollar value on the date the block was mined. To do this, a daily history of the value of bitcoin was used.[10]
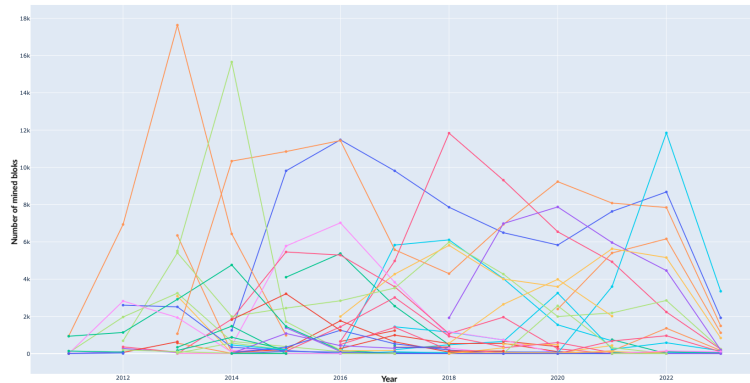

Figure 1: All mining pools ever.

The first attempt to extract a graph that would allow an overview of the number of blocks mined by all the miners in the database over the years, shown in Figure 1, produced a difficult-to-read result because the presence of almost 100 different mining pools. So, we decided to focus
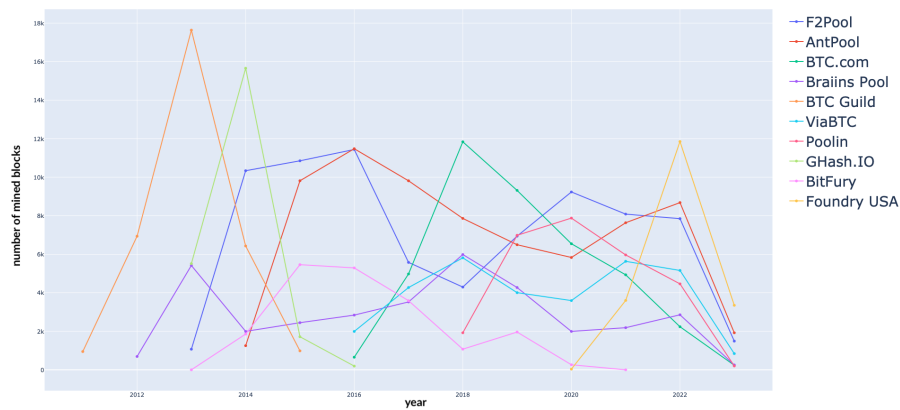

Figure 2: Top ten miner pools by number of blocks over the time

the analysis on some selected miners. The first step is to use the top ten mining pools for the number of mined blocks. The result is shown in Figure 2. At the beginning of Bitcoin, the first mining pool was BTC Guild, which was overtaken in late 2013 by GHash.IO, lasting less than a year to benefit F2Pool. In 2016, the one that mines the most blocks became AntPool, overtaken in late 2017 by BTC.com. In 2019, F2Pool returned to the top, which was then overtaken in mid-2021 by Foundry USA. We can also see that the most long-lived mining pool is the Braiins

---

[10]https://it.investing.com/crypto/bitcoin/historical-data.

pool, followed by F2Pool.

Notice that the greater number of mined blocks does not necessarily correspond to the higher gain; this is due to the significant increase in the value of Bitcoin over the years, e.g., the ViaBTC pool has mined fewer blocks than the BTC Guild pool but having mined them more recently it has earned more: the gain is calculated by multiplying the number of bitcoins received from mining the block by the value of Bitcoin in dollars on the date it was mined.
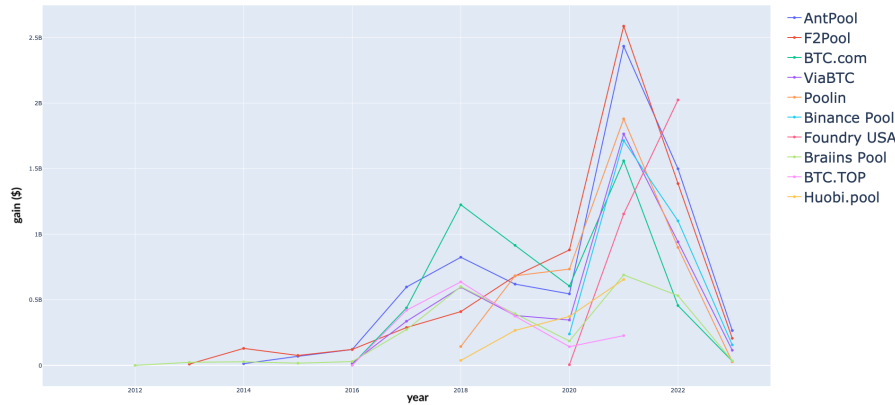

Figure 3: Top ten miners by total gained over time.

Figure 3 represents the top ten mining pools by total earned through mining. Here, it is clear how the miners who have made the most money have all thickened in recent years, thanks to a significantly higher value of Bitcoin. First is F2pool, thanks partly to its longevity, followed by AntPool. Note the significant growth of FoundryUSA in a few years, which is currently the highest-earning mining pool. We can also notice that the top ten miners by number of blocks are different for the aforementioned reason. In particular, BTC.Guild, GHash.IO, and BitFury are replaced by miners who worked in earlier periods: Binance Pool, BTC.TOP, and Huobi.pool.

Mining pool	Mined Block	Gain ($)	Activity period	Reward Method
AntPool	70,798	6,99E+09	2013-present	FPPS
BTC.com	44,051	5,24E+09	2016-present	FPPS
Braiins Pool	34,465	2,81E+09	2012-present	FPPS
BTC Guild	32,935	1,98E+08	2011-2015	PPS
ViaBTC	31,314	4,5E+09	2016-present	PPS+/PPLSN/SOLO
Poolin	24,973	4,37E+09	2018-present	FPPS
F2Pool	77,169	6,77E+09	2013-present	FPPS
Foundry USA	18,841	3,65E+09	2019-present	FPPS
GHash.IO	23,083	2,94E+08	2013-2015	PPLNS
Binance Pool	15,082	3,21E+09	2020-present	FPPS

Table 1
Most important mining pools stats.

Table 1 shows all the information about top mining pools. F2Pool is the one that mined more blocks, but AntPool earned more money. Instead, BTC.com is the second by mined block. On

the other hand, F2Pool is the second for gained dollar.

Mining pool	earned fees($)	earned fees(BTC)
AntPool	374,798,304	36,499
F2Pool	352,529,741	30,602
BTC.com	323,100,643	27,127
ViaBTC	242,439,264	17,891
Poolin	212,224,122	9,921
BTC.TOP	156,725,336	18,033
Braiins Pool	154,238,694	21,324
Binance Pool	154,103,289	4,752
Huobi.pool	98,228,061	4,662
Foundry USA	74,769,139	2,360

Table 2
Mining pools gain from fees.

In addition to the base Bitcoin reward, recognized by the protocol itself and set at 6.25 Bitcoin per mined block, a miner currently chooses the transactions to be validated by looking at the relative fees users offer to be processed. Calculating each reward's fee value was necessary to determine which mining pool has the most efficient block selection algorithm. This was done by subtracting the value of a reward on the day it was mined from the total reward in Bitcoin received by the miner. The results can be found in the table 2. Also, the mining pool that earned the most money was AntPool, and the second was F2Pool. Considering instead the number of bitcoins, the result is the same.

Mining pool	Mined per day	Gain per day ($)
AntPool	21.42	2.11E+06
BTC.com	18.61	2.21E+06
Braiins Pool	9	7.34E+05
BTC Guild	24.82	1.49E+05
ViaBTC	12.83	1,84E+06
Poolin	15.18	2.66E+06
F2Pool	22.72	1.99E+06
Foundry USA	23.40	4,53E+06
GHash.IO	31.66	4.03E+05
Binance Pool	24.32	5,18E+06

Table 3
Most important mining pools normalized stats.

AntPool has been around for long, so it consistently comes out on top. To account for this, we have normalized the results based on the days each mining pool has been active. This helps provide a clearer understanding of which pools have superior algorithms for selecting transactions and fees. For the number of mined blocks and gains, we also use the number of days of each mining pool's life for normalization. Instead, for the fees gained, we use the number of mined blocks to normalize. Table 3 shows the mined blocks and gain per day of the most important mining pools. According to the mined blocks, the most efficient pool is

GHash.IO, followed by BTC Guild. On the other hand, the Binance Pool is the one that gains more per day of activity. The second is Foundry USA.

Mining pool	earned fees per block($)	earned fees per block(BTC)
AntPool	5,293.91	0.515608936
F2Pool	4,568.28	0.395543335
BTC.com	8,653.80	0.615803022
ViaBTC	7,742.20	0.571130239
Poolin	7,742.58	0.397271394
BTC.TOP	8,595,22	0.98902403
Braiins Pool	9,374.75	0.618720931
Binance Pool	10,217.69	0.315347681
Huobi.pool	10,606.64	0.505882432
Foundry USA	3,968.43	0.125264352

Table 4
Mining pools gain per block from fees.

As shown in Table 4, Houbi.pool is the most efficient for selecting transactions with high fees when it creates a block. Binance is the second, followed by Braiins Pool. AntPool and F2Pool, the ones with the highest total amount, are now the last. When considering the block fees in bitcoins, one mining pool stands out from the rest: BTC.TOP. According to the data, BTC.TOP leads the pack with a block fee of nearly one bitcoin per block, making it the most profitable pool. Braiins Pool is the second-best option, with a competitive block fee significantly lower than BTC.TOP's. This information identifies miners looking to maximize their profits.

Mining pool	Mined Block	Mined Tx	Tx per Block
AntPool	70,798	113,836,519	1,608
BTC.com	44,051	72,671,409	1,650
Braiins Pool	34,465	48,683,696	1,413
BTC Guild	32,935	10,960,149	333
ViaBTC	31,314	57,472,790	1,835
Poolin	24,974	50,193,095	2,010
F2Pool	77,169	115,987,897	1,499
Foundry USA	18,841	33,639,215	1,785
GHash.IO	23,083	10,068,049	436
Binance Pool	15,082	28,477,377	1,890

Table 5
Transactions mined by mining pools.

The provided data in Table 5 shows the number of transactions each mining pool has mined. F2Pool is the leading miner as it has mined the most significant number of transactions so far, followed by AntPool, which is quite close behind. When considering the mean of transactions per block, Poolin is the best-performing mining pool, along with Binance Pool. These two mining pools have proven to be highly efficient regarding their block creation rates and the number of transactions processed. On the other hand, the last two mining pools on the list, GHash.IO and BTC Guild, have not been performing as well. However, it is essential to note

that they were active before the massive activity of the Bitcoin network. Overall, these findings provide valuable insight into the performance of different mining pools.

3.1. Miner earnings guidelines

The total hash rate and the number of participants in a pool do not affect the income of a miner who is part of it. In fact, being part of a pool twice as large as another means that the pool can mine double the blocks, so it has twice the frequency of distributing the rewards, but the miner's share is half, as is the reward. In a smaller pool, the miner gets a higher payout but with a lower frequency, given the lower total hash rate and the longer time it takes to mine a block. The calculations vary slightly depending on the payment system offered by the pool. However, the fee types (PPS, PPS+, FPPS) primarily keep the miners in the pool and disadvantage those miners hopping from one pool to another to try to make more money.

The higher gains are where there are lower fees, but it is important to note that a miner does not choose a pool only for maximizing earnings. Often, the quality of customer service, credibility, and nationality of a pool are crucial factors in the miner's ultimate decision.

4. Annual stats

This section analyzes mining pool data by year, starting from January 2011 through March 2023.
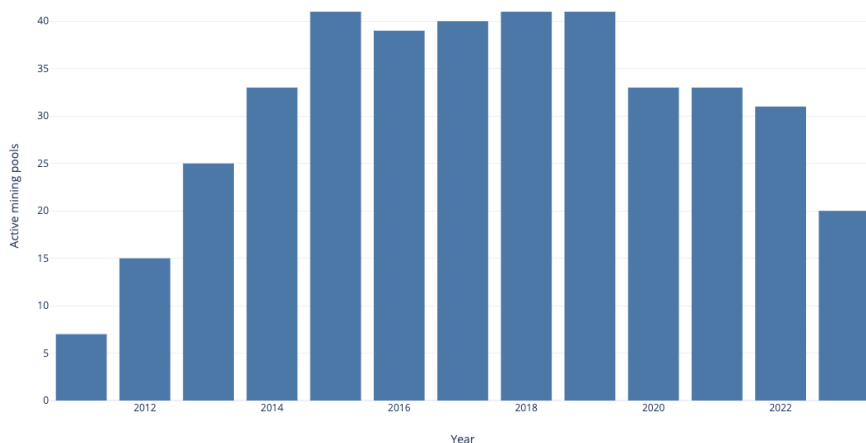

Figure 4: Number of active pools per year.

Figure 4 shows that the number of miners over time has steadily increased except in the years that hosted a halving, namely 2012, 2016, and 2020.

The gains have continuously increased concerning the growth of Bitcoin's value until 2021, as shown in Figure 5.

In 2011, database miners mined 2, 104 blocks, earning a total of 220, 557$. Among the seven operating pools, BTC Guild, Eligius, and yourbtc.net mined and earned the most; despite this, all
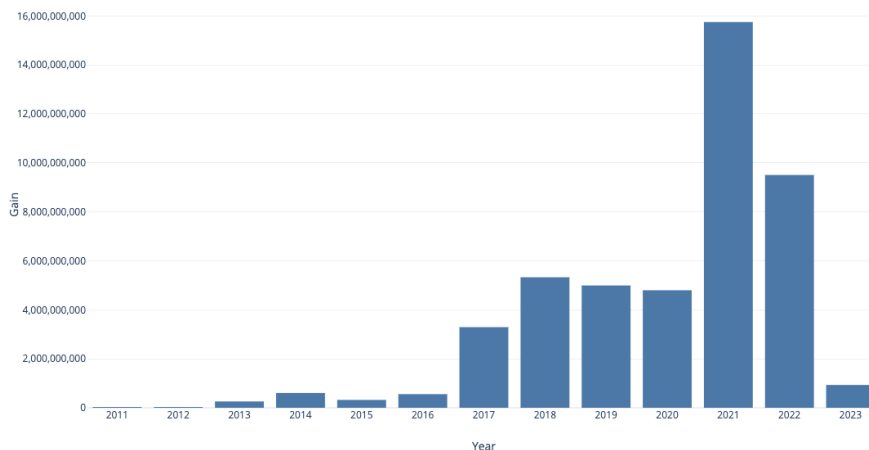
Figure 5: Miner gain (in dollars) per year.

three stopped activity. In 2012, the pools mined $17,310$ blocks, with a total gain of $6,751,084$\$. Active pools have more than doubled from the previous year (15 total), and the BTC guild pool remains at the top of the list for gains and the number of blocks mined. OzCoin and EclipseMC also shut down. In 2013, the database's miners mined $52,481$ blocks, gaining $259,493,456$. The number of active pools increased to 25, and the pools that mined and earned the most were BTC Guild, 50BTC, and GHash.IO, which are now closed. In 2014, they mined $50,549$ blocks, gaining a total of $604,950,230$\$. There were 33 active miners, and the most efficient pools were GHash.IO, BTC Guild, and F2Pool, the latter of which is still alive. In 2015, pools mined $51,041$ blocks, with a total gain of $321,385,158$\$. The number of active miners reached 41, and the most efficient pools were F2Pool, Antpool, a leader in mining even today, and BTCC Pool, which closed in 2018. In 2016, they mined $54,638$ blocks, with a total gain of $556,928,279$\$. The number of active miners dropped to 39, probably due to halving, and the most efficient pools were again F2Pool, Antpool, and BTCC Pool. In 2017, the database's miners mined 55,554 blocks, gaining a total of $3,292,676,723$\$. The number of active miners increased to 40; the most efficient pools were AntPool, F2Pool, and BTC.top. In 2018, mining pools mined $53,281$ blocks, with a total gain of $5,329,510,817$\$. The number of active miners reached 41, and the most efficient pools were BTC.com, which is still active today, Antpool, and BTC.top. In 2019, they mined $52,121$ blocks, with a total gain of $4,993,038,036$\$. There were 41 active miners, and the most efficient pools were BTC.com, F2Pool, and Poolin, which are still active. In 2020, mining pools mined $51,054$ blocks, with a total gain of $4,798,331,807$\$. The number of active miners dropped to 33, aided by halving and the difficulties triggered by the pandemic. The most efficient pools were F2Pool, Poolin, and BTC.com. In 2021, the database miners mined $49,577$ blocks, gaining $15,749,186,536$\$. The number of active miners remained stable at 33; the most efficient pools were AntPool, F2Pool, and Poolin. In 2022, the database's miners mined $53,034$ blocks, gaining a total of $9,505,458,011$. The number of active miners decreased to 31, and the most efficient pool was Foundry USA, which had the fastest growth among all those

analyzed due to the absence of fees, AntPool, and F2Pool. In 2023 (data through March), they mined $10,095$ blocks, with a total gain of $932,182,558\$$. The number of active miners dropped to 20, and the most efficient pools were Foundry USA, AntPool, and F2Pool.
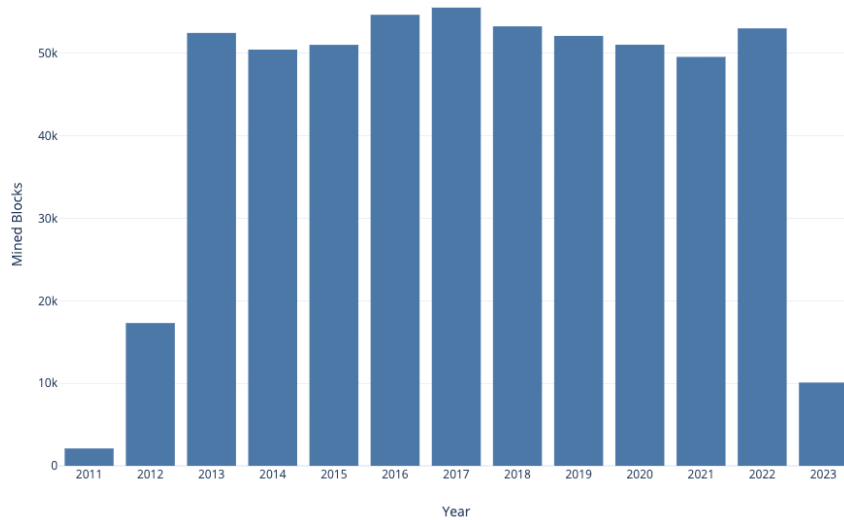

Figure 6: Mined blocks per years).

However, Figure 6 shows the number of mined blocks each year has always been stable at around 50,000 as the protocol increases or decreases the difficulty of mining to keep mining a block for about 10 minutes.

4.1. Halving

Given the decrease in miners over the halving years, we conducted a more detailed analysis to determine how many have closed because of this. The halving event occurs after every $210,000$ blocks mined, about once every four years. During halving, the bitcoin reward that miners receive is halved, which has a significant impact on the supply of new bitcoins and the work of the pools since only the miners with the most efficient hardware and the lowest operating costs can sustain this change while maintaining a gain on the resources spent.

The date of the first halving is November 28, 2012; the next ones were July 9, 2016, and May 11, 2020. The next halving is scheduled for 2024. In particular, in Figure 7, we can see the activity of the miners during the second halving, where 15 pools closed in a few weeks. During the third halving, 12 mining pools stopped working. Figure 8 shows their activity.

5. Related work

The Bitcoin mining and mining pools have been explored in several ways in the literature. In 2014, [7] demonstrated how a mining pool could use a distributed denial-of-service (DDoS)
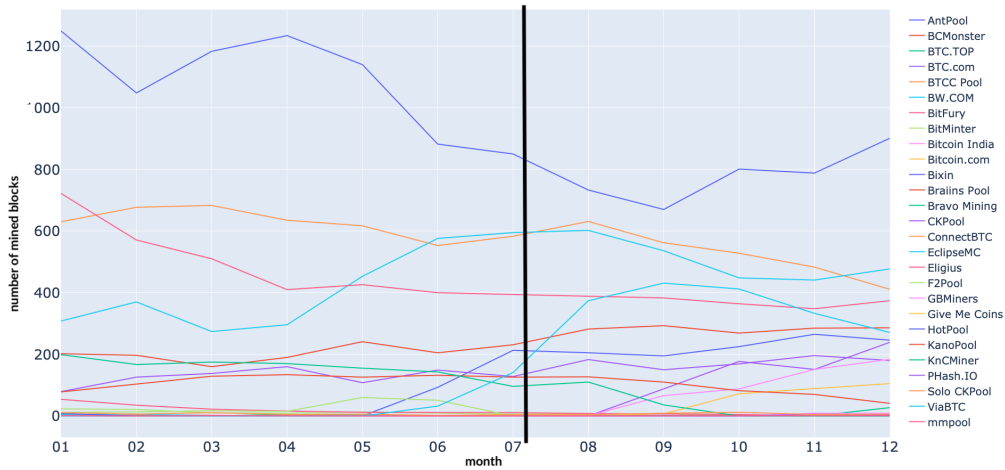
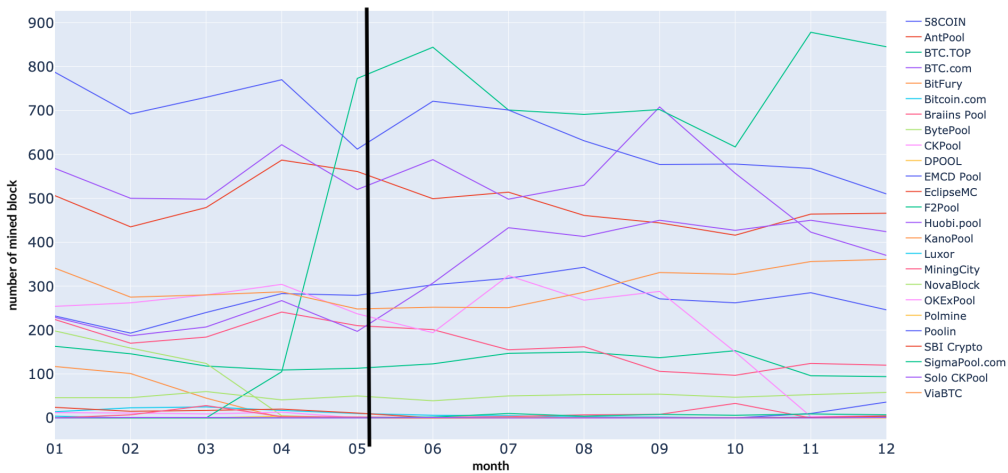**Figure 7:** Active pools during 2016 halving (black line).

Figure 8: Active pools during 2020 halving (black line).

attack to reduce the chances of success of a competing mining pool. The study analyzed the competition between two mining pools of different sizes using game-theoretical models. The researchers considered various factors, such as the cost of investment and attack, as well as the uncertainty of the success of a DDoS attack. The study found that mining pools are more likely to attack larger pools than smaller ones. A few months later, [8] explores alternative methods for Bitcoin mining on non-custom hardware, potentially leading to more efficient mining by utilizing computing resources within machines in mining networks, both legal and illegal.

In 2015, the authors of [9] developed a game-theoretic model that can capture both short-term and long-term impacts of attacks against mining pools. They have used this model to study the conditions under which mining pools have no incentives to launch attacks against each other, known as peaceful equilibria. They have also studied the requirements under which

one mining pool is marginalized by attacks, known as one-sided attack equilibria. The results of this study provide guidelines for ensuring that the Bitcoin ecosystem remains viable and trustworthy in the long run. Instead, [10] discusses the process of pooled mining and how the rewards collected by the pools are shared among the members. The authors use cooperative game-theoretic tools to analyze the reward distribution among the members. They found that it becomes challenging to distribute rewards fairly under certain network parameters, particularly during high transaction loads. As a result, some participants are always motivated to switch between pools.

The year after, [11] presents a game-theoretic model for reward functions in Bitcoin mining pools. The model is based on the history of reported shares and provides miners with a strategy for reporting or delaying the discovery of a share or complete solution. The authors have defined a precise condition for incentive compatibility to ensure that miners' strategy choices optimize the welfare of the pool as a whole. The definition shows that proportional mining rewards are not incentive-compatible in this model. The authors have introduced and analyzed a new reward function that is incentive-compatible in this model.

This 2017 paper [12] proposes an intelligent mining strategy to help a mining pool increase its chances of receiving rewards disproportionate to its computational power. The strategy involves deploying forwarding nodes based on the distribution of Bitcoin nodes. By doing so, the time delay for message propagation can be reduced, and the probability of a new block being appended to the longest blockchain can be increased.

In 2020, the authors of [13] developed an incentive mechanism called the Mining game, which uses a Stackelberg game. They have demonstrated that the Mining game is profitable, individually rational, and has a unique Stackelberg Equilibrium. They have formulated the Budget-feasible Reward Optimization (BFRO) problem for the private cost model to maximize the reward function under the budget constraint. They have also designed a budget-feasible reverse auction to solve the BFRO problem, which is computationally efficient, truthful, individually rational, budget feasible, and constant approximate.

In the last year, the authors of [14] proposed a new approach to decentralize Bitcoin mining pools by introducing an uncertain mining reward system based on transaction fees. The authors have presented a simple model demonstrating how risk-averse Bitcoin miners are more likely to distribute their computational power across multiple mining pools when transaction fees make up a significant portion of the mining reward. Their empirical study has shown a negative correlation between the proportion of transaction fees and the decentralization of Bitcoin mining pools.

6. Conclusion

The paper overviews mining pools activity and the mining process. We have analyzed the information contained within the Blockchain to derive structured and explanatory data about the pools' work over the years and highlight factors that may influence it. In the history of cryptocurrency mining, we have seen a significant increase in the number of pools. This growth has occurred even though many of those established in the early years (2011-2014) have closed as a result of halving, i.e., the reduction in the reward for mining that occurs periodically in

the Bitcoin blockchain, and the increase in the difficulty of mining with consequent hardware evolution. This phenomenon shows how dynamic and competitive the mining industry is, with new players constantly entering the market to get a share of the block rewards. Interestingly, some pools have mined many blocks, but this did not always translate into significant gains. The fluctuation in Bitcoin's value over the years significantly affects the overall earnings of the miners.

Decentralization of mining pools is essential for the health and security of the Bitcoin network. A high concentration of power in the hands of a few pools can pose security risks to the network. Therefore, miners should choose different pools to avoid centralization and contribute to greater network security. In addition to protocol rewards, mining pools receive commissions from the blocks they process. Huobi.pool has proven to be the best at choosing blocks, followed by Binance Pool and Braiins Pool. When the last Bitcoin is mined, which is expected to happen in just over a hundred years, miners will stop receiving block rewards upon completion of each block. Despite this, mining operations should remain profitable in the future, considering that transaction fees will replace block rewards as a source of revenue. Our plan for the future is to expand our analysis of miner efficiency by considering various factors, such as the block and transaction dimensions. By doing so, we can provide a more comprehensive and accurate analysis of the efficiency of miners in selecting and validating blocks. Examining the block and transaction dimensions will provide insights into the miner's ability to handle complex transactions.

Furthermore, it would be valuable to include a discussion on the computational power of each mining pool and its gains. Such an analysis would help us understand how much computational power each mining pool contributes to the network and how much it earns.

References

[1] S. Nakamoto, Bitcoin: A peer-to-peer electronic cash system, Bitcoin project white paper (2009).

[2] S. Bistarelli, R. D. Nicola, L. Galletta, C. Laneve, I. Mercanti, A. Veschetti, Stochastic modeling and analysis of the bitcoin protocol in the presence of block communication delays, Concurr. Comput. Pract. Exp. 35 (2023). doi:10.1002/CPE.6749.

[3] R. Pass, L. Seeman, A. Shelat, Analysis of the blockchain protocol in asynchronous networks, in: J. Coron, J. B. Nielsen (Eds.), Advances in Cryptology - EUROCRYPT 2017 - 36th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Paris, France, April 30 - May 4, 2017, Proceedings, Part II, volume 10211 of *Lecture Notes in Computer Science*, 2017, pp. 643–673. URL: https://doi.org/10.1007/978-3-319-56614-6_22. doi:10.1007/978-3-319-56614-6_22.

[4] A. M. Antonopoulos, Mastering Bitcoin: Programming the Open Blockchain, 2nd ed., O'Reilly Media, Inc., 41 E University Ave, Champaign, USA, 2017.

[5] K. Banker, D. Garrett, P. Bakkum, S. Verch, MongoDB in action: covers MongoDB version 3.0, Simon and Schuster, 2016.

[6] F. Pezoa, J. L. Reutter, F. Suárez, M. Ugarte, D. Vrgoc, Foundations of JSON schema, in: J. Bourdeau, J. Hendler, R. Nkambou, I. Horrocks, B. Y. Zhao (Eds.), Proceedings of the 25th International Conference on World Wide Web, WWW 2016, Montreal, Canada, April 11 - 15, 2016, ACM, 2016, pp. 263–273. URL: https://doi.org/10.1145/2872427.2883029.

[7] B. Johnson, A. Laszek, J. Grossklags, M. Vasek, T. Moore, Game-theoretic analysis of ddos attacks against bitcoin mining pools, in: R. Böhme, M. Brenner, T. Moore, M. Smith (Eds.), Financial Cryptography and Data Security - FC 2014 Workshops, BITCOIN and WAHC 2014, Christ Church, Barbados, March 7, 2014, Revised Selected Papers, volume 8438 of *Lecture Notes in Computer Science*, Springer, 2014, pp. 72–86. URL: https://doi.org/10.1007/978-3-662-44774-1_6.

[8] J. A. Dev, Bitcoin mining acceleration and performance quantification, in: IEEE 27th Canadian Conference on Electrical and Computer Engineering, CCECE 2014, Toronto, ON, Canada, May 4-7, 2014, IEEE, 2014, pp. 1–6. URL: https://doi.org/10.1109/CCECE.2014.6900989.

[9] M. Brenner, N. Christin, B. Johnson, K. Rohloff (Eds.), Financial Cryptography and Data Security - FC 2015 International Workshops, BITCOIN, WAHC, and Wearable, San Juan, Puerto Rico, January 30, 2015, Revised Selected Papers, volume 8976 of *Lecture Notes in Computer Science*, Springer, 2015. URL: https://doi.org/10.1007/978-3-662-48051-9.

[10] Y. Lewenberg, Y. Bachrach, Y. Sompolinsky, A. Zohar, J. S. Rosenschein, Bitcoin mining pools: A cooperative game theoretic analysis, in: G. Weiss, P. Yolum, R. H. Bordini, E. Elkind (Eds.), Proceedings of the 2015 International Conference on Autonomous Agents and Multiagent Systems, AAMAS 2015, Istanbul, Turkey, May 4-8, 2015, ACM, 2015, pp. 919–927. URL: http://dl.acm.org/citation.cfm?id=2773270.

[11] O. Schrijvers, J. Bonneau, D. Boneh, T. Roughgarden, Incentive compatibility of bitcoin mining pool reward functions, in: J. Grossklags, B. Preneel (Eds.), Financial Cryptography and Data Security - 20th International Conference, FC 2016, Christ Church, Barbados, February 22-26, 2016, Revised Selected Papers, volume 9603 of *Lecture Notes in Computer*

Science, Springer, 2016, pp. 477–498. URL: https://doi.org/10.1007/978-3-662-54970-4_28. doi:10.1007/978-3-662-54970-4.

[12] Y. Liu, X. Chen, L. Zhang, C. Tang, H. Kang, An intelligent strategy to gain profit for bitcoin mining pools, in: 10th International Symposium on Computational Intelligence and Design, ISCID 2017, Hangzhou, China, December 9-10, 2017 - Volume 2, IEEE, 2017, pp. 427–430. URL: https://doi.org/10.1109/ISCID.2017.184.

[13] G. Xue, J. Xu, H. Wu, W. Lu, L. Xu, Incentive mechanism for rational miners in bitcoin mining pool, Inf. Syst. Frontiers 23 (2021) 317–327. doi:10.1007/S10796-020-10019-2.

[14] Z. Li, J. Li, K. Zhou, Bitcoin transaction fees and the decentralization of bitcoin mining pools, Finance Research Letters 58 (2023) 104347. URL: https://www.sciencedirect.com/science/article/pii/S1544612323007195.