BITCOIN MAGAZINE®



THE **HALVING** ISSUE

$21.00US $21.00CAN
42
6 02648 40388 7
MADE IN CANADA

BUY THE NUMBERS sponsored by HIVE NasdaqListed

Pick your poisson

BY JOE RODGERS

Calculated probabilities were calculated by Greg @learnmeabitcoin.com

Block 840,000 is not just another block in the blockchain; it triggers the Bitcoin halving where the block reward is reduced from 6.25 BTC to 3.125 BTC, cutting the amount of BTC mined each day in half. You don't have to be a Princeton economist to understand the impact this will have on the supply and demand dynamics for bitcoin. Beyond the obvious halving of the block reward, a new market has developed around Ordinals which could have a significant impact on what happens to the first block of the halving. Contained within the first block of the halving is an extremely rare "epic sat". While Ordinals have divided some Bitcoiners on their merit, there is no arguing the impact they have had on Bitcoin.and it raises an important question, could Ordinals cause a blockchain reorg? Through this article we will dig into the basics of a reorg, Ordinals demand, how mining probabilities work, and finally who could pull off a successful reorg.

Before we dig into this "epic sat", let's build an understanding of what a reorg is. The Bitcoin blockchain is a slow and dumb database that creates blocks of data every 10 minutes or so. It continues working as intended, but occasionally, things get tense. When two miners find blocks nearly simultaneously, it creates a temporary fork in the blockchain. This moment of overlap leads to a brief period of uncertainty. These forks are resolved by the network through the longest chain rule, which is when the fork tip of the blockchain with more proof-of-work (the longest chain or aka more blocks) will be adopted as the valid chain. Orphaned blocks from the shorter chain are not included in the longer one, and the transactions they contain are returned to the mempool to be included in future blocks. This process of one chain becoming longer than the other and becoming the accepted version is known as a reorganization, or reorg.

Due to the incentive structures built into Bitcoin mining, reorgs are usually resolved as soon as the next block is found and added to the tip of one of the forked chains. This is because finding a block is extremely difficult, and miners are incentivized to work on the longest chain in order to build the next block, and get paid. If they are mining on the short fork, the rest of the network will leave them behind and they will have invalid blocks. The last thing you would want is to build a block that is rejected by the network because you've built a block on a chain and are rejected by the network due to the longest chain rule. During the reorg period of a fork, miners build on whichever chain fork hits their node first and try to build a block to get the longest chain.

Now don't get worried about reorgs. They happen every couple of months (on average) and typically involve one or two blocks. These short reorgs are part of the network's regular operation and quickly resolve without any significant impact on the network and its users. It's worth noting that deep reorgs that consist of many blocks are rare and, correspondingly, more disruptive. They can be triggered by a network split such as what happened in the Blocksize wars, or a new large miner coming to the network, or an attempt to double-spend transactions (this is very rare).

Most Recent Reorgs

Height	Length	Date
829 613	1	09 February 2024
827 853	1	28 January 2024
819 343	1	01 December 2023
818038	1	23 November 2023
815 202	1	04 November 2023
813210	1	21 October 2023
803 389	1	16 August 2023
800 786	1	29 July 2023
792 379	1	01 June 2023
789 147	1	10 May 2023

Source: Learn Me A Bitcoin

The Bitcoin protocol and its incentives are designed so that there's a low likelihood of deep reorgs occurring.

Consensus rules and incentives are meant to keep the network stable and secure. For example, most exchanges and payment processors require that a transaction be confirmed by a set number of times—usually six or more—before a transaction can be considered final, thus greatly reducing the chances of it being unwound by a reorg. Small reorgs happen and are mundane and frequent operations within the Bitcoin blockchain, but large reorgs are notable and very irregular.

About that epic sat

You've probably heard the buzz about Ordinals, that is **"a numbering scheme for satoshis that allows tracking and transferring individual sats"**. Some argue that Ordinals are a scam and they have no place in Bitcoin, but here's the thing, an emerging market is rapidly growing around Ordinals. For now, they are here, and they are getting attention from miners, devs, VC, collectors, scammers, and haters alike.

When it comes to Ordinals, they are classified by their "rarity" and markets determine value.

Ordinals rarity levels:

COMMON	UNCOMMON	RARE	EPIC	LEGENDARY	MYTHIC
ANY SAT THAT IS NOT THE FIRST SAT OF ITS BLOCK	THE FIRST SAT OF EACH BLOCK	THE FIRST SAT OF EACH DIFFICULTY ADJUSTMENT PERIOD	THE FIRST SAT OF EACH HALVING EPOCH	THE FIRST SAT OF EACH CYCLE	THE FIRST SAT OF THE GENESIS BLOCK

If we consider the scenario where all Bitcoin has been mined, which implies that all 21 million bitcoins (or 2.1 quadrillion satoshis) are in circulation, we can calculate the total quantity of each level of Ordinals:

UNCOMMON:	There would be a total of 6,929,999 uncommon satoshis, corresponding to the first satoshi of each block.
RARE:	There would be a total of approximately 3,437 rare satoshis, corresponding to the first satoshi of each difficulty adjustment period.
EPIC:	There would be a total of 32 epic satoshis, corresponding to the first satoshi of each halving epoch.
LEGENDARY:	There would be approximately 5 legendary satoshis, corresponding to the first satoshi of each cycle (noting a slight approximation due to division).
MYTHIC:	There is 1 mythic satoshi, which is the first sat of the genesis block.

These figures give an overview of how the rarity classifications would distribute across the total supply of satoshis once all Bitcoin is mined, showcasing the unique and scarce nature of certain satoshis within the Bitcoin network.

The Ordinals Market and Beyond

Over the past 12 months we've seen rapid development in Ordinals technology and markets. Ordinals markets first emerged in Discord back channels where OTC deals were being made, but as demand has grown, digital marketplaces have developed for buying and selling Ordinals. US Based Magisat.io lists various types of Ordinals and has Rare sats listed for a staggering 3.49 BTC. This valuation has led to the creation of additional inventory of Ordinals beyond the category that was first described in the Ordinals documentation.

Current Market on Magisat.io for standard Ordinals

CATEGORY	FLOOR UNIT PRICE BTC	FLOOR BTC	VOLUME (BTC)	INVENTORY
EPIC	N/A	N/A	N/A	N/A
RARE	3.4906	3.5000	7.59	2
UNCOMMON	0.0034	0.0034	18.5117	246

Stats as of 2-15-2024

This data shows that there is a small but growing demand for Ordinals. You can see the volume for Rare amd Uncommon Ordinals are greater than 26 BTC at the time of writing this. Keep in mind that this is only one marketplace and there are a growing number of OTC deals that are happening between buyers and sellers not to mention demand and business happening in other parts of the world.

Looking beyond Ordinals marketplaces we are now seeing Ordinals make their way to legendary auction house Sotheby's further propelling the phenomenon towards the mainstream. If you look across the Pacific Ocean there is also significant demand for Ordinals and BRC-20 tokens, which would not be possible without Ordinals. So the demand for Ordinals is real and it is growing, not waning.

The last significant item of note that could impact demand for this first block of the halving is the activation of Runes. Runes is another protocol released by the same creator of Ordinals, but the aim of Runes is to make a more efficient token protocol. The kicker on this is that with it going live in the first block of the halving, this alone will cause a significant demand to issue these new tokens as quickly as possible, presumably the first Runes issued will be more valuable than later issued Runes. "Yes there will be reorg incentive for block 840,000, but it's not for epic sat -- it's for the 20btc in fees from Casey's Runes." said Charlie Spears on X. This fee revenue call is speculation but it comes from observation from previous Ordinals and BRC20 activity.

Sifting For Sats

In Bitcoin, "dust" refers to an amount of bitcoin so small that it cannot be spent because the cost of a transaction fee would be higher than the amount itself. The concept of a "dust limit" therefore varies depending on the transaction fee and the type of transaction being made. However, there are general guidelines for what is considered dust, based on the type of Bitcoin script or address being used.

The dust limit is calculated based on the size of the inputs and outputs that make up a transaction. For a transaction to be relayed by most nodes and mined, its outputs must be above the dust limit. The dust limit for a standard P2PKH (Pay-to-Public-Key Hash) transaction output is commonly considered to be 546 satoshis when using the default minimum relay fee of 1 satoshi per byte, but this can vary depending on the network conditions and the policies of individual nodes.

For different script types, the dust limit calculation takes into account the size of the script and therefore can vary:

P2PKH (Pay-to-Public-Key Hash):
This is the most common type, and its dust limit is usually around 546 satoshis.

P2SH (Pay-to-Script Hash):
Outputs for P2SH transactions can have a slightly higher dust limit because the script itself is more complex, requiring more data to be included in a transaction.

P2WPKH (Pay-to-Witness-Public-Key Hash) and P2WSH (Pay-to-Witness-Script Hash):
These SegWit (Segregated Witness) transactions have different weight calculations, leading to lower fees for the same amount of data. Consequently, the dust limit for SegWit transactions can be lower than for traditional P2PKH transactions. For P2WPKH, the dust limit might be closer to 294 satoshis.

MultiSig:
Transactions involving multiple signatures (MultiSig) have higher dust limits due to the increased data size required to accommodate multiple signatures.

The exact dust limit can vary because it depends on the transaction's size and the current fee market. Additionally, changes in Bitcoin's protocol or node policies can affect these thresholds. It's also worth noting that some wallets and services might set their own dust limits based on their operational requirements.

Pools Sifting

Based on the information above we can examine blocks found by pools to see if pools are actively sifting blocks. What we see is 44% of the network is or has sifted for sats in the past year. We have reason to believe that additional pools are in discussions with sifting technology developers in deploying the tech on their pools, but nothing has been made public at this time. Our findings reveal that a very significant percentage of the mining network sees value in sifting for these sats, otherwise this would be a hobbyist endeavor. When this many big players are participating, you know there is some market dynamics happening.

Rank past 6 months	Pool	% Of Network	Sifting	Sifted Blocks
1	Foundry USA	29.02%	FALSE	--
2	AntPool	25.64%	TRUE	830 206
3	F2Pool	12.35%	TRUE	830 208
4	ViaBTC	10.98%	FALSE	--
5	Binance Pool	6.49%	FALSE	--
6	MARA Pool	3.78%	FALSE	--
7	Luxor	2.93%	TRUE	810 020
8	SBI Crypto	1.90%	FALSE	--
9	BTC.com	1.54%	FALSE	--
10	Braiins Pool	1.29%	FALSE	--
11	Unknown	1.27%	FALSE	--

Source: Mempool.space as of 2-12-2024, ranking as of past 6 months

Beyond blockchain investigation outlined above, miners are developing new markets of their own in mining irregular transactions for various projects. Most notably is publicluy traded mining pool Marathon who launched a new service called Slipstream which will mine complex transactions such as 1 sat UTXO which is far below the SEGWIT dust threshold of 546 sats. I bring this up because as they are offering this service, you can't help but assume that Marathon sees or will soon see value in Ordinals of they are willing to invest resources in serving Ordinal or Ordinal adjacent projects with this service. Afterall, the obligation of publicly traded companies is to maximize value for shareholders.

We know more than 40% of hashrate is sifting for sats, but what does that really mean in the grand scheme of things. Afterall, we are talking about one specific sat, the epic sat in block 840,000. We know that Ordinals have value according to the very small market, we also know that this sat will likely be sold for more than a single blocks reward, but the big question is who could forcibly win this block? Proof of Work is all about the longest chain and ethics don't matter when it comes to Bitcoin and the blockchain. The chain is truth, even if you were to reorg. If you are hashing and following consensus and you build a longer chain then you are the victor. Based on the table from the previous section, we can see who the top pools are from the past six months. With that information we can model the probability of these pools forking and causing a reorg of the blockchain in order to win the epic sat but we need to run the numbers. For this we will explore the mining section of the Bitcoin Whitepaper.

Mining Explained in the Whitepaper

Bitcoin mining is a race to find a valid block by solving a cryptographic puzzle, known as proof of work. The difficulty of this puzzle is adjusted by the network so that, on average, a new block is found every 10 minutes, regardless of the total computing power of the network. Now the security of this is where things get interesting. Section 11 of the Bitcoin whitepaper discusses the mathematics behind the security of the blockchain against attackers who try to alter the transaction history.

The paper uses a comparison to a gambler's "ruin problem" to explain how difficult it is for an attacker to catch up with the rest of the network once they fall behind in the race to add new blocks to the chain. Essentially, if honest nodes control more computational power, the probability that an attacker can catch up decreases rapidly as they fall further behind in the blockchain.

The probability that an attacker can catch up becomes almost zero if they do not have a majority of the computational power.

The section outlines the process where transactions become more secure as new blocks are added to the blockchain, using a Poisson distribution to model the likelihood of an attacker catching up from being behind the chain tip. This framework provides the basis for understanding how blockchain achieves security through probabilistic means not absolute guarantees.

In the Bitcoin whitepaper, the Poisson distribution is used to model the security of mining. It's used to quantify the probability that an attacker can catch up with the honest nodes after being z blocks behind, which is vital when considering the risk of a blockchain reorganization. It offers a statistical view of how likely it is for an attacker, with a certain percentage of the total network hash rate, to rewrite the blockchain history.

Converting to C code...

```
#include <math.h>
  double AttackerSuccessProbability(double q, int z)
   {
     double p = 1.0 - q;
     double lambda = z * (q / p);
     double sum = 1.0;
     int i, k;
     for (k = 0; k <= z; k++)
       {
       double poisson = exp(-lambda);
       for (i = 1; i <= k; i++)
       poisson *= lambda / i;
       sum -= poisson * (1 - pow(q / p, z - k));
       }
     return sum;
   }
```

Who Could Pull This Off?

Ordinals introduces a new incentive to reorg. Before Ordinals, the threat of a reorg was focused around a double spend attack, but Ordinals introduced the demand for individual sats, in this case the demand to win a specific block. The question is this, does the value of a single Epic sat or block warrant abandoning the longest chain in hopes of finding a couple quick blocks and winning that epic sat? Pubco mining pools will have a hard time justifying such action to shareholders, it seems negligent. But for private mining pools, they have different incentives and have a bit more freedom in how they pursue revenue.

Looking at the top 10 mining pools by their percent of the network, we can model out who could pull off a reorg. One thing of note, the formulas described in the whitepaper only model catching up with the chain tip, however a reorg would require catching up to the tip +1 block, so our values below show that probability.

RANK PAST 6 MONTHS	POOL	% OF NETWORK	1 BLOCK	2 BLOCKS	3 BLOCKS	4 BLOCKS	5 BLOCKS
1	FOUNDRY USA	29.02%	44.5717%	32.4584%	23.9127%	17.7352%	13.2111%
2	ANTPOOL	25.64%	33.1175%	21.0595%	13.5639%	8.7996%	5.7353%
3	F2POOL	12.35%	7.7912%	2.4780%	0.7999%	0.2603%	0.0851%
4	VIABTC	10.98%	6.1520%	1.7432%	0.5014%	0.1454%	0.0424%
5	BINANCE POOL	6.49%	2.1365%	0.3596%	0.0614%	0.0106%	0.0018%
6	MARA POOL	3.78%	0.7210%	0.0708%	0.0071%	0.0007%	0.0001%
7	LUXOR	2.93%	0.4324%	0.0329%	0.0025%	0.0002%	0.0000%
8	SBI CRYPTO	1.90%	0.1814%	0.0090%	0.0004%	0.0000%	0.0000%
9	BTC.COM	1.54%	0.1190%	0.0048%	0.0002%	0.0000%	0.0000%
10	BRAIINS POOL	1.29%	0.0835%	0.0028%	0.0001%	0.0000%	0.0000%
11	UNKNOWN	1.27%	0.0809%	0.0027%	0.0001%	0.0000%	0.0000%

The first thing I noticed was Foundry and Antpool have a higher % probability of pulling off a reorg from 1 block behind than their own % hashrate of the network. How could this be possible? This is because A miner with 30% of the hashrate being 1 block behind and attempting a reorg is at a disadvantage because the rest of the network (70% hashrate) collectively has a higher probability of extending the current longest chain before the miner can catch up and surpass it. However, due to the randomness captured by the Poisson distribution, there's always a non-zero probability that this miner could, through a streak of good luck, mine enough blocks in a row to take over the longest chain, even from one block behind. This is statistically unlikely but becomes possible with higher hashrate percentages and short reorg depths.

The next key takeaway is how successful reorgs become less likely for each block they are behind. It is remarkable how Foundry could still reorg from 5 blocks behind.

Conclusion

The Bitcoin space is weird (always has been) and bitcoin miners are the longest of long when it comes to outlook on Bitcoin. Based on the reorg probability and the potential value from the additional value on the first block of the halving, the probability of a reorg feels likely. If you take the BTC mined from this block, the epic sat, plus the projected amount of fees that will be earned from the release of Runes, bigger pools would be foolish to not try and make a move to win this block. The only real downside of a reorg would be by working on the old chain and NOT winning the reorg, so you would miss out on possibly winning 1-2 blocks by mining on the original longest chain. I do hope for fireworks. It will be legendary to hear the talk tracks from the new Wall Street financial bros trying to explain this. At the end of the day, miners will have to make a decision, that is to simply build on the longest chain or to try and build the longest chain with heavy amounts of luck. They must consider the tradeoffs and pick their poisson.

DESPITE RISING HASHRATE

AND OPTIMISED HARDWARE



OVER TIME THE PROTOCOL

SEEMS TO BEAR LESS FRUIT