A free and open-source Bitcoin course by Area Bitcoin

Table of Contents - Bitcoin 4 All -

Inside Bitcoin Part II: how does Bitcoin work?

(mining, halving and cycles)

5.3 The Emergence of Mining Pools
5.4 Solo Mining vs Pooled Mining
5.5 Can Mining Pools Centralize the Network?

---

6. The Halving Mechanism

6.1 What Is a Halving and Why It Matters
6.2 History of Bitcoin's Halvings (2012–2024)
6.3 Halvings as a Built-In Supply Schedule
6.4 Transparent, Predictable Monetary Policy
6.5 The Final Bitcoin: Year 2140

---

7. Impact of Halvings on Scarcity and Price

7.1 Supply Shock: Fewer New Bitcoin, Same Demand
7.2 The Role of Hodlers in Price Dynamics
7.3 Cycles of Appreciation Triggered by Halvings

---

8. Bitcoin Market Cycles

8.1 The Four Phases of the Cycle
  – Bear Market
  – Accumulation Phase
  – Expansion Phase
  – Bull Run
8.2 Fear & Greed Index: Market Psychology
8.3 Halvings and Price Peaks: Historical Patterns
8.4 Higher Lows: Long-Term Price Floor Trend

---

9. Final Reflections

9.1 Will Bitcoin Appreciate Forever?
9.2 Preview of the Next Lesson

Bitcoin 4 All - Full Text

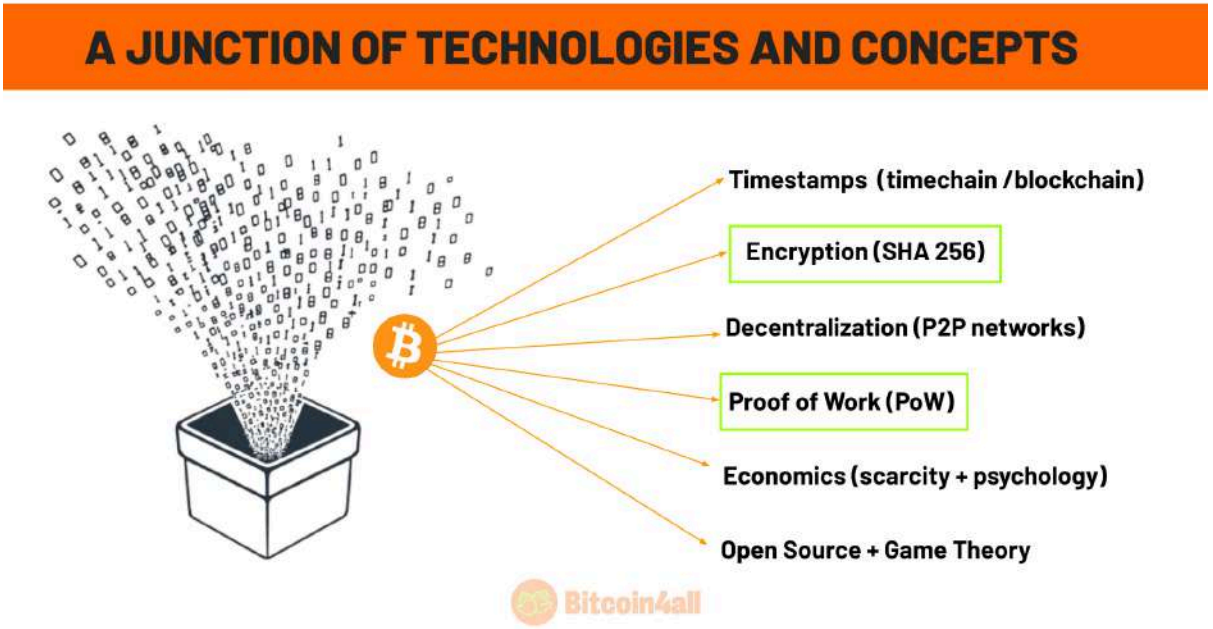
Bitcoin 4 All is a free and open source course created by Area Bitcoin. The goal is to help more people to understand Bitcoin and inspire anyone to be a multiplier of Bitcoin education.

About this eBook

Published by Area Bitcoin – 2025

Inside Bitcoin Part II: how does Bitcoin work?

(mining, halving and cycles)



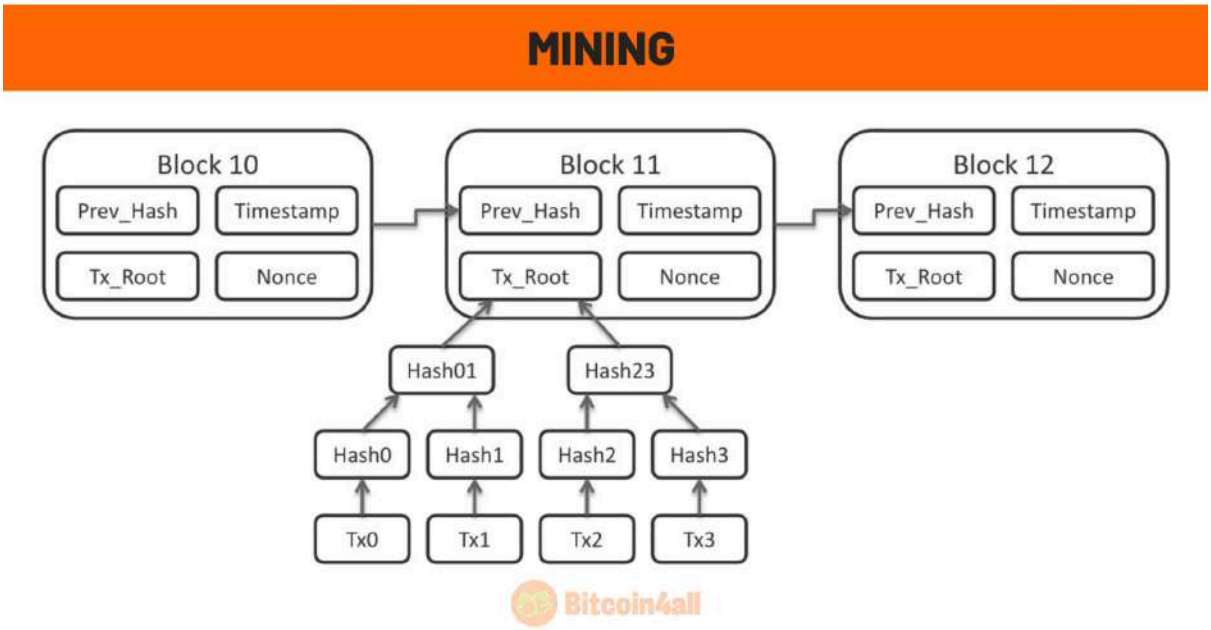
(slide 109) - Bitcoin 4 All

Now that you've understood how the Bitcoin blockchain works and that it needs consensus from the participants for decentralized coordination, let's understand how the network agrees with each other through a mechanism called Proof of Work (PoW).

(slide 110) - Bitcoin 4 All

Bitcoin "mining" is an analogy for the process of searching for something precious, like gold, except that in the Bitcoin network that something precious is the hash of each block. When it comes to gold, miners keep digging until they find the precious metal. Once they do, they have something scarce and valuable in their hands. Gold is scarce; over time, it becomes harder and more expensive to mine it, since digging deeper and deeper into the ground is needed. Gold mining requires increasingly modern and efficient equipment to access the deepest and most complex deposits.

Something very similar happens with Bitcoin. In the Bitcoin network, miners compete with each other, through trial and error, to see who gets to the hash that closes each block of information first.



(slide 111) - Bitcoin 4 All

Remember that a block is made up of several components? The hash of the previous block, a timestamp and all the transaction data?

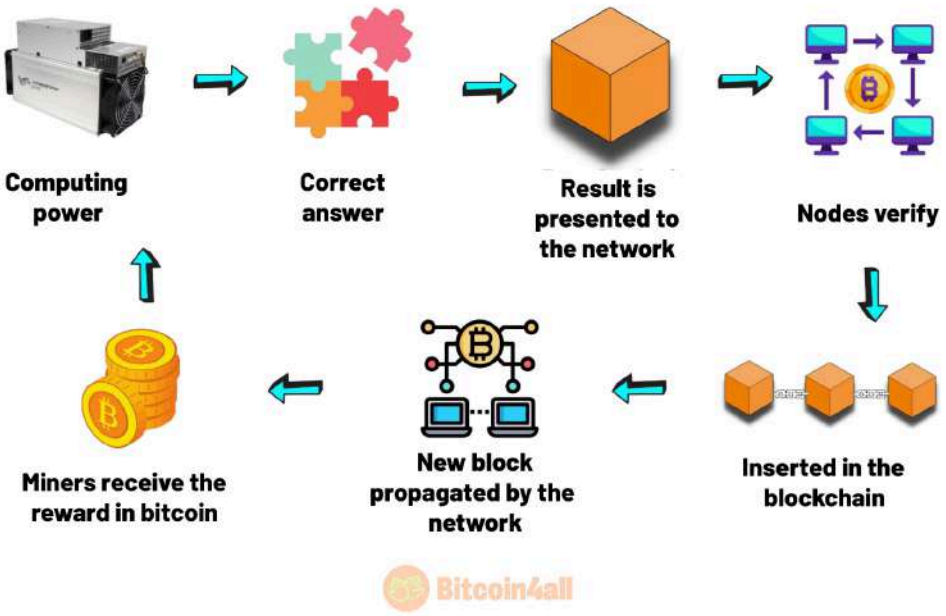
Along with this information, there is also a piece of information called a "nonce". Nonce stands for "number used only once". When miners use computing power to mine the block, it means that they are, at an absurd computational speed, trying to find that number that can only be used once by the network. That's the number that all the miners are competing to find.

The block header contains the hash that mixes several components: the hash of the previous block, the timestamp, the root transaction that summarizes all the transactions that entered the block and the nonce.

(slide 112) - Bitcoin 4 All

Everyone is looking for the right piece within all the possibilities and whoever finds it first tries to fit it into the picture. When the miner finds the missing piece, it's very easy for everyone to see if it fits. Just look at the picture and see if the piece was correct or not.

This means that mining is a process that is difficult to defraud and at the same time very easy to verify, just like a piece in a giant jigsaw puzzle: it's difficult to find the correct piece, but easy to check whether it was the missing piece or not. Bitcoin is like a global puzzle in which the whole world participates and follows the results in real time.

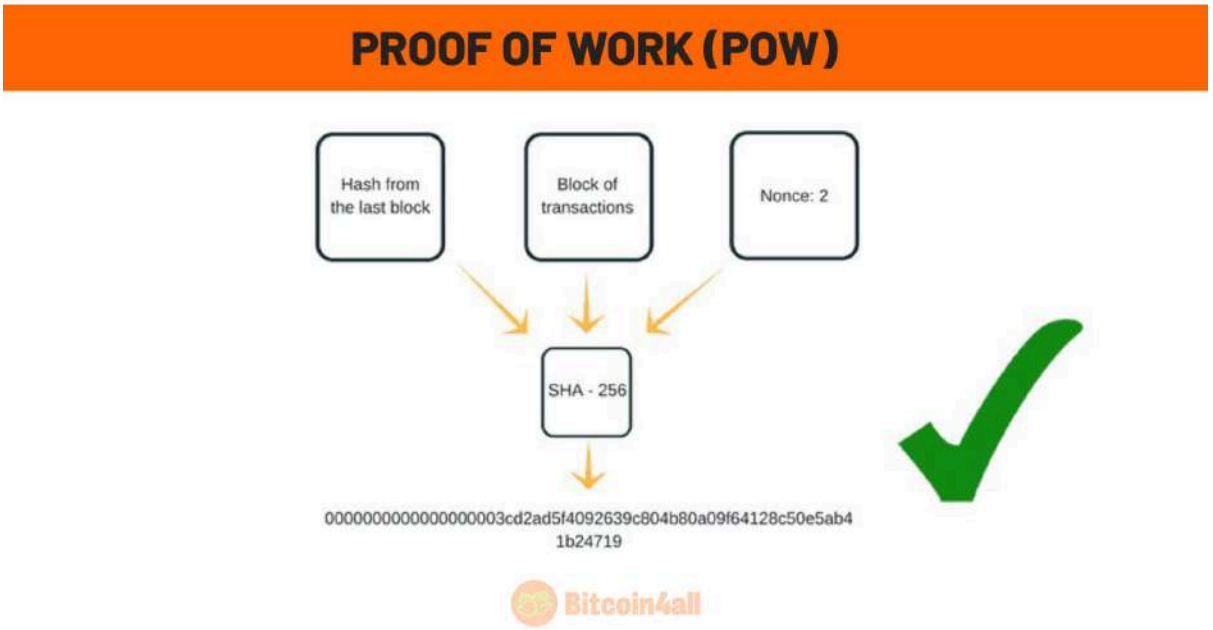


(slide 113) - Bitcoin 4 All

The entire mining and consensus process when registering the Bitcoin blockchain works like this:

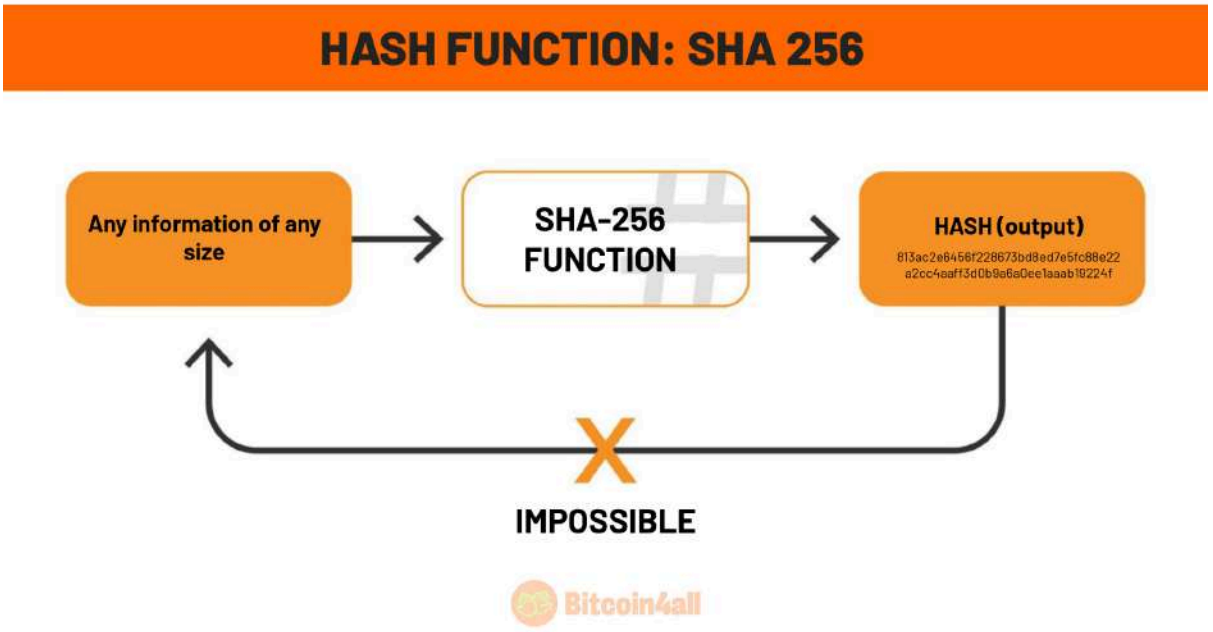
Miners use computing power, buying powerful machines with huge computing power to try and find the nonce of the block as quickly as possible. When they find it, they create the hash, show it to the network, and the nodes check that the proposed block is following the rules. If everything is OK, the block is added into the blockchain and propagated through the network; the block is inserted into all participants' copies of the blockchain (timechain). Afterwards, the miners receive Bitcoin as a reward for completing the task.

This whole process is known as proof of work.



(slide 114) - Bitcoin 4 All

Proof of work means that the miner has followed the rules, found the nonce, created the block hash, and provided a computational service to the network. When all the information in the block is found, it goes through the encryption process of turning the information into a cryptographic puzzle using SHA-256. The result is this huge number, which represents the hash of the block, the result of all the miner's work.



(slide 115) - Bitcoin 4 All

This process is not exclusive to Bitcoin, but to anything that can be encrypted. SHA-256 is the algorithm that does this. The SHA-256 takes information of any length and creates a 256-bit sequence: a series of 256 zeros and ones. From this huge number full of zeros and ones, the algorithm creates a hexadecimal sequence made up of 64 digits -- both letters and numbers -- that is easier to write down. In other words, it's easy to check that the sequence is correct, but it's practically impossible to forge the encrypted information.

Trying to randomly match a hash and break SHA-256 encryption is practically impossible. It involves an absurdly high number of possible combinations, more numbers than the number of atoms in the observable universe! This would require so, so many attempts, that it would take a normal computer billions of years to do it.

That's where the story of the quantum computer comes in! People always ask us if a quantum computer could break Bitcoin's encryption. This is one of the great hopes of Bitcoin haters, but the truth is that no quantum computer would be able to kill Bitcoin.

I will leave an article that better explains whether quantum computers are a threat here in the description of this class.

Now it's time to show you a very cool site. It's this one, called Code Beautify. This site allows you to experiment and convert any information into a SHA-256 function.

Let's type Bitcoin4All here. See how the code in the box below changes with every letter, space or punctuation mark. This is what happens to the Bitcoin network's block hash if any information is modified. Note how fast it happened: it didn't require mega computing power to find this hash. If it was that easy to create a hash right here on this site, why does it take 10

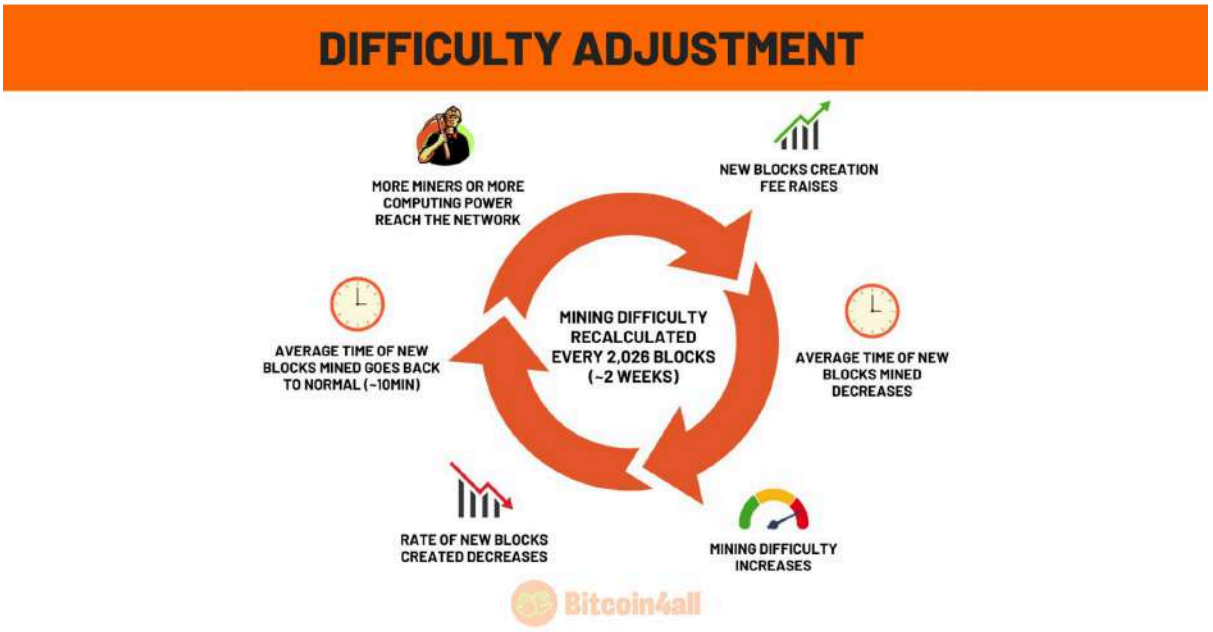
minutes on the Bitcoin network? And why is it no longer possible to mine from your home computer?

(slide 116) - Bitcoin 4 All

This has to do with a mechanism called difficulty adjustment.

The difficulty adjustment has the role of regulating the issuance of new bitcoin. It is this adjustment that ensures that the average time taken to create new blocks, followed by the reward delivered by the network, is 10 minutes. This is because every 2016 blocks mined, about 15 days on average, there is an algorithm that will analyze the amount of computing power in the network and increase or decrease the difficulty of finding the block hash.

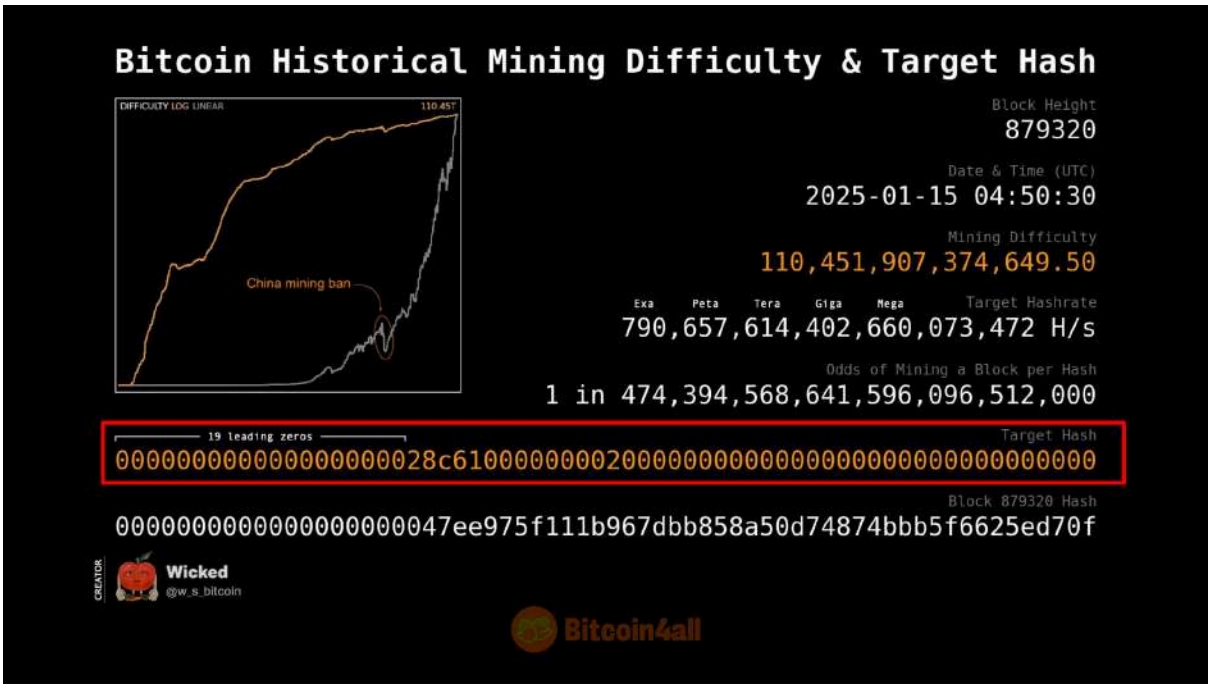
If the number of miners suddenly increases, the network will regulate itself to increase the difficulty of mining so as not to speed up the rate at which new blocks are created and consequently not speed up the rate at which new bitcoin are created.



(slide 117) - Bitcoin 4 All

It works like this: as more miners join the network and the hashrate increases (the rate at which new blocks are created), miners start to find blocks more easily and the average mining time between one block and the next becomes faster. The network realizes this through its algorithms and increases the difficulty of mining. As a result, the speed of creating new blocks drops (since it has become more difficult for miners to find blocks) until it stabilizes at an average of 10 minutes between one block and another.

This is how the network regulates itself as demand increases so that it never loses its predictability.



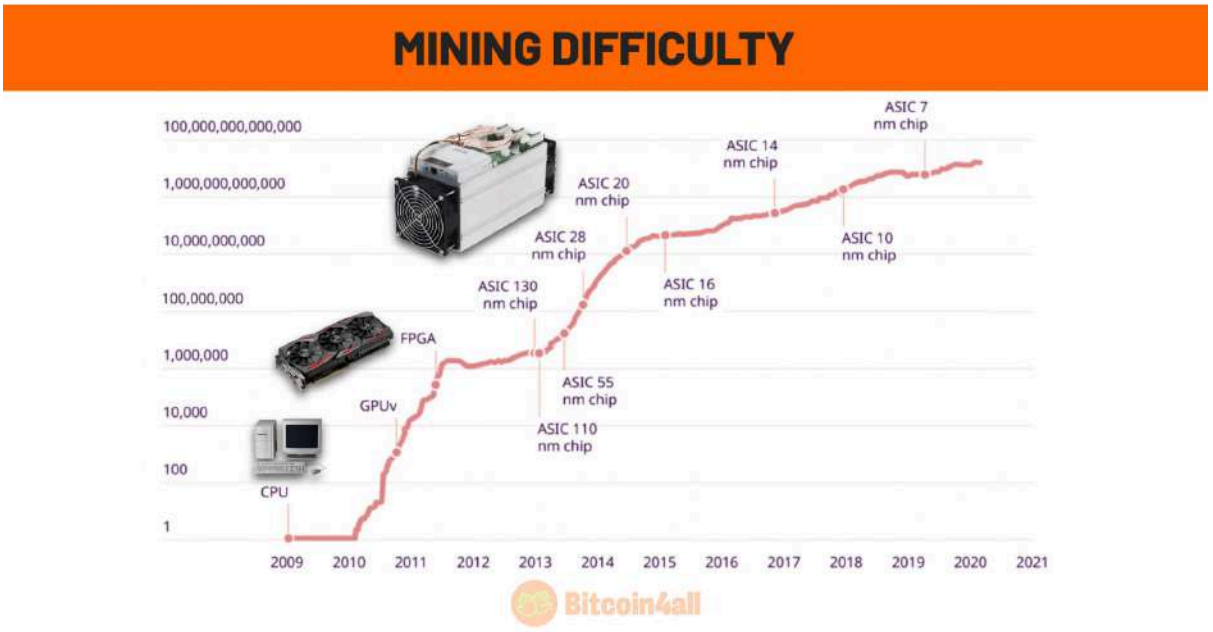
(slide 118) - Bitcoin 4 All

You can tell the difficulty level of mining each block by the number of zeros that appear before the block's hash number. This block, for example, has 24 zeros in front of the hash code. It was mined in October 2022, being one of the most difficult blocks to mine at the time.

The miner's goal is to assemble a block where the hash code is smaller than the current target. The smaller the target, the harder it is to find a valid block. The more miners on the network, the harder this search gets.

(slide 119) - Bitcoin 4 All

In other words, the more zeros leading a hash, the harder it is to mine, requiring more effort for a miner to search and find a block's nonce.



(slide 120) - Bitcoin 4 All

It's because of the difficulty setting that mining has evolved and it's no longer so easy to mine from your home PC from a CPU. Today, Bitcoin is mined using specific machines called ASICS. As the price of Bitcoin rose, it ended up attracting more and more people, with more computing power being employed in the network. With it, the difficulty adjustment algorithm was increased to maintain an average of one block mined every 10 minutes.

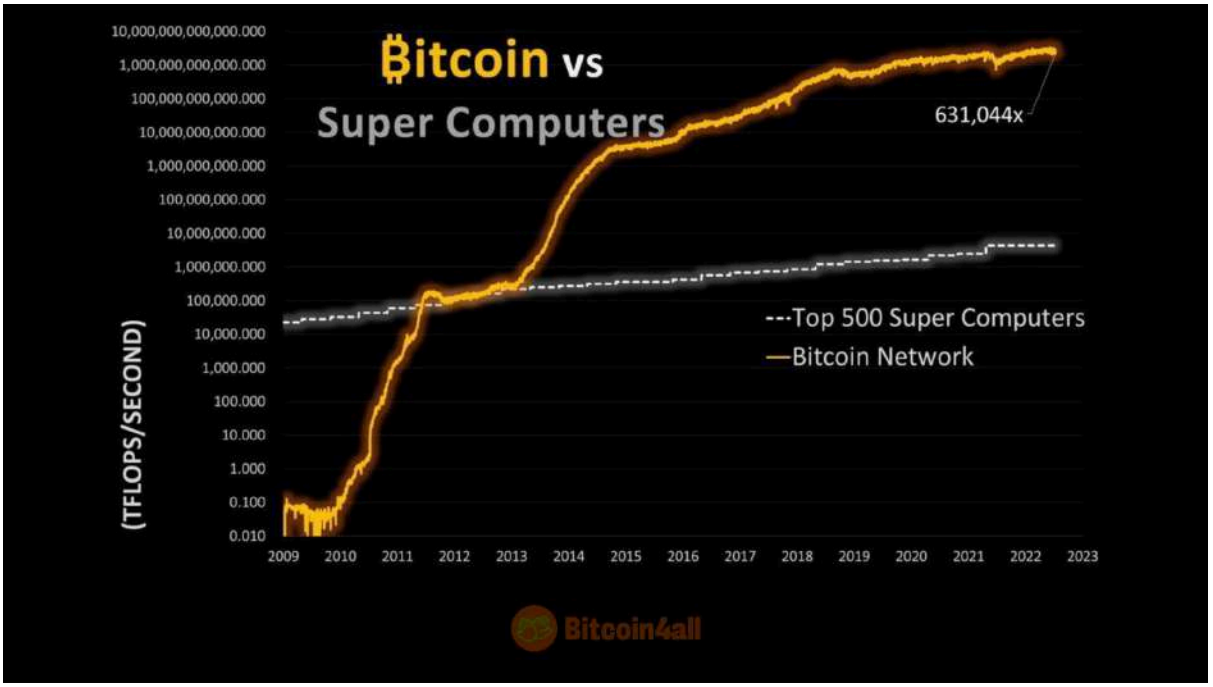
As the level of difficulty increased, more tech savvy people began to use more powerful machines: GPUs, which are widely used in gaming computers. Bitcoin continued to attract more and more people wanting to mine, until a machine was created with this specific purpose: ASICs.

This type of machine is much more powerful and beats CPUs and GPUs at the speed of finding the block's hash. Mining has become a giant and dedicated industry, tirelessly seeking efficiency. In other words, it aims to produce as many bitcoin as possible with as little or as little energy as possible.

That's why the price doesn't matter in this case. Bitcoin could reach 10 billion dollars. The speed at which new bitcoin are issued does not change. Even an increase in the power of the hashrate cannot lead to more bitcoin being issued than is planned for each halving cycle. Bringing more miners into the network doesn't produce more bitcoin, but it does make the network more secure and decentralized.

(slide 121) - Bitcoin 4 All

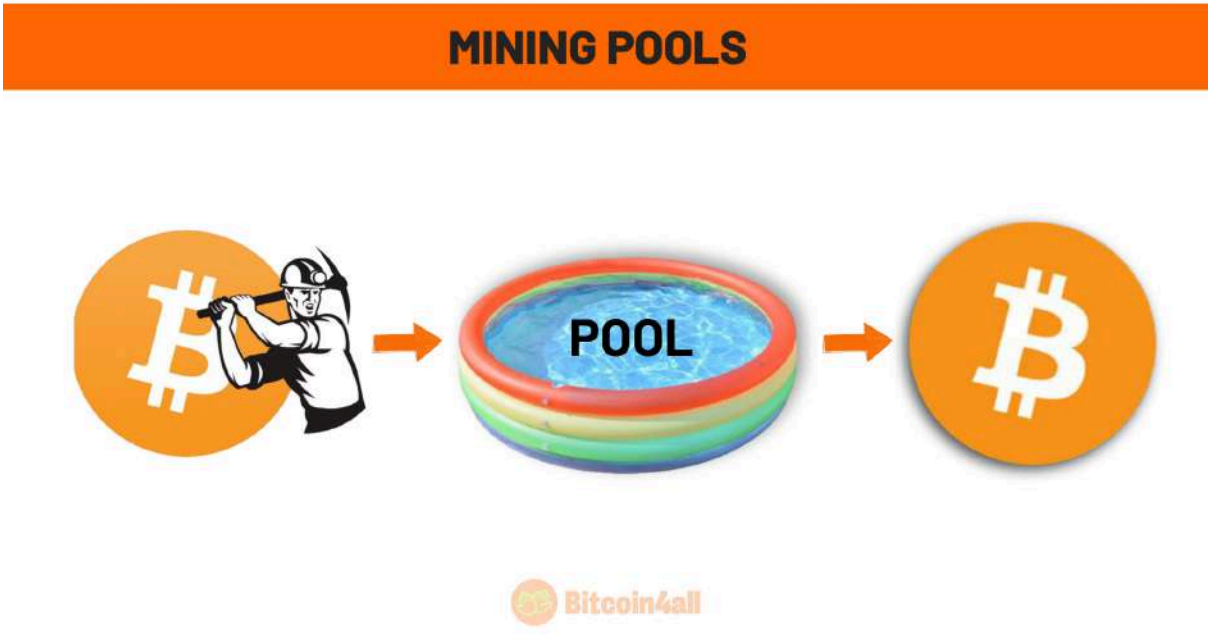
And why does this mechanism make the network more secure? Well, because the greater the computing power, the harder it is to attack the network. In this graph, the line represents the hashrate, the computing power, and the redder colors represent the difficulty of mining each block. The difficulty and hashrate have increased exponentially since the Bitcoin network started hashing. As the line turns orange, the harder it is to mine a block. The greater the computing power, the more the network has adapted to protect Bitcoin's properties. That's why Bitcoin has no competitor in mining: it's the protocol with the most miners distributed around the planet and the most computing power of all.



(slide 122) - Bitcoin 4 All

Bitcoin is 631 times more powerful than the world's 500 largest supercomputers combined, represented in the white line -- Bitcoin is shown in the orange line. Bitcoin has the most attack-resistant computer network, 600x stronger than any centralized computer system or data center.

But the advance of mining hasn't stopped at ASICs. Over time, even with an extremely powerful machine, it became harder and harder to find blocks. As a response, the miners ended up grouping together in pools. They pool their computing power to have a better chance of finding blocks and sharing the reward.

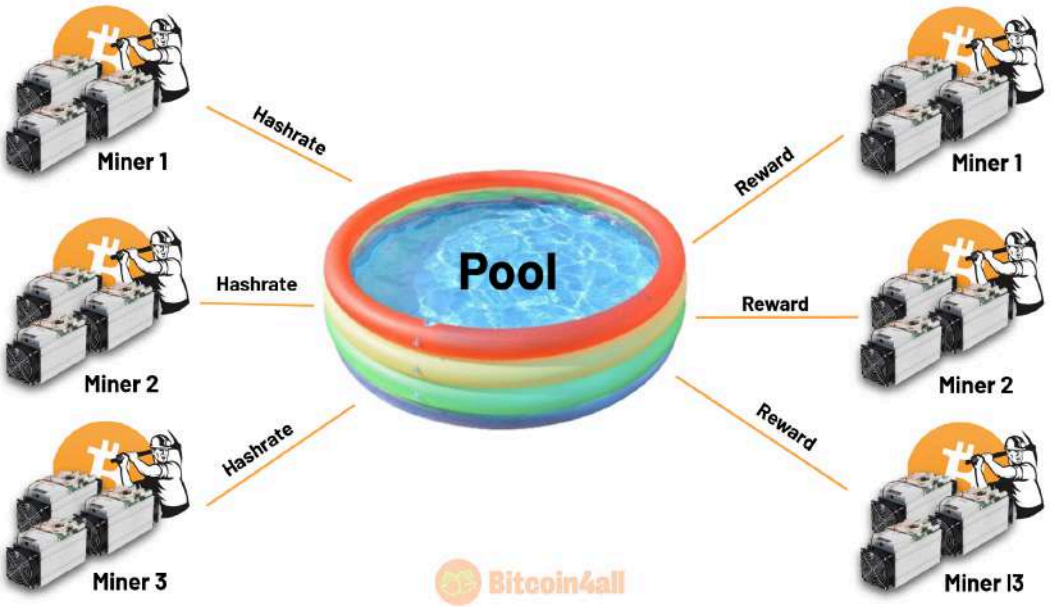


(slide 123) - Bitcoin 4 All

Mining pools work between Bitcoin software and the miners, allowing miners to pool the computing power of their machines and have a better chance of finding a block. The term "pool" designates a pool of computing power.

(slide 124) - Bitcoin 4 All

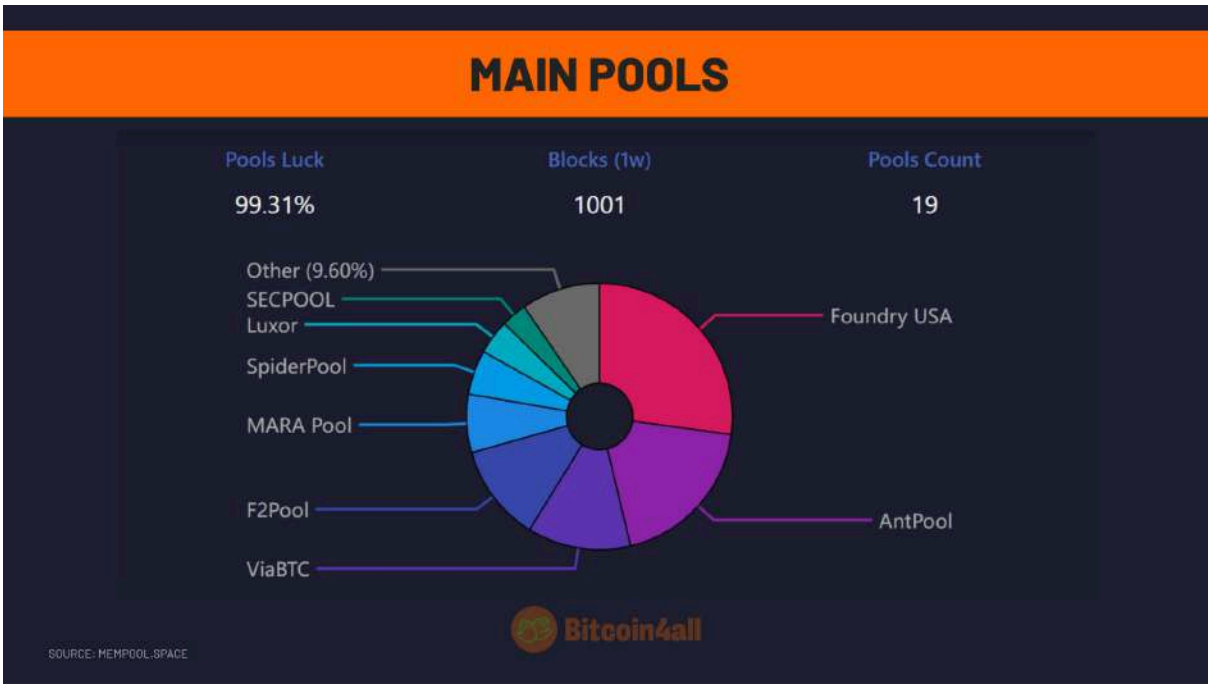
To give you an idea of how difficult it is to mine outside a pool -- to mine solo --, an S19JPRO, which is one of the most modern ASIC machines, has a 0.000000208% chance of mining a Bitcoin block. That's one chance in almost 4.8 billion attempts over the entire lifetime of the machine, which lasts an average of 5 to 8 years. This probability will continue to decrease over time as more miners arrive, the hashrate rises and the difficulty increases.



(slide 125) - Bitcoin 4 All

That's why pools work like a system where everyone chips in with computing power: whenever someone finds the block, everyone shares the reward in Bitcoin in proportion to

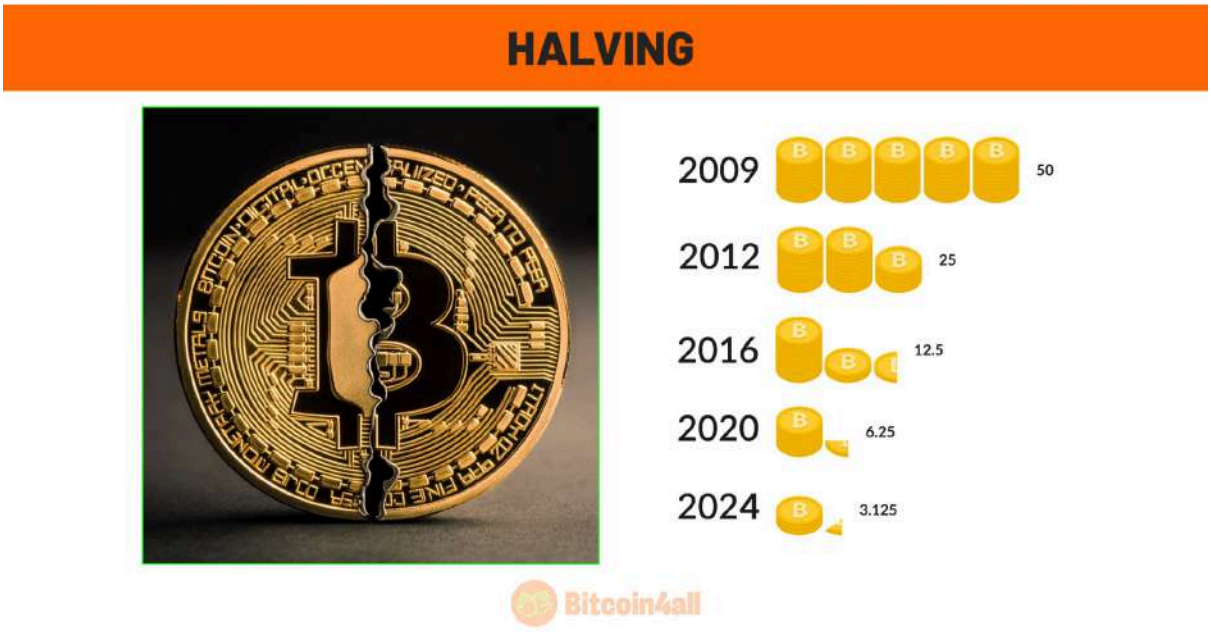
their hashing power. This way, miners can earn a frequent income instead of hoping to find a block on their own, which can take years and is not guaranteed to happen at all.



(slide 126) - Bitcoin 4 All

Nowadays the Bitcoin network has dozens of pools, but five of them are the largest and aggregate most of the hashrate: Foundry, Antpool, F2Pool, ViaBTC and Mara. Although many people say that this could be classified as a centralization mechanism, in reality miners can leave the pool at any time and go to another one. They can even mine solo if they want to try their luck. The concentration in these five largest pools was a natural market movement of the miners' will to stay in pools with greater odds of finding blocks and share the rewards. The pools don't rule the network, since it's the nodes that check and decide whether the mined blocks are valid or not.

Another essential point in the functioning of Bitcoin is the halving, which has everything to do with mining. As time goes by, Bitcoin becomes more and more scarce. Growing scarcity coupled with growing demand is what has caused Bitcoin's parabolic upward price movements. It is the halving that causes Bitcoin to gradually become scarcer and at the same time creates cycles of appreciation that have been repeated.



(slide 127) - Bitcoin 4 All

Halving comes from the word "halfing". The Bitcoin halving means that, for every 210,000 blocks mined (every 4 years on average), the protocol cuts the reward given to miners in half.

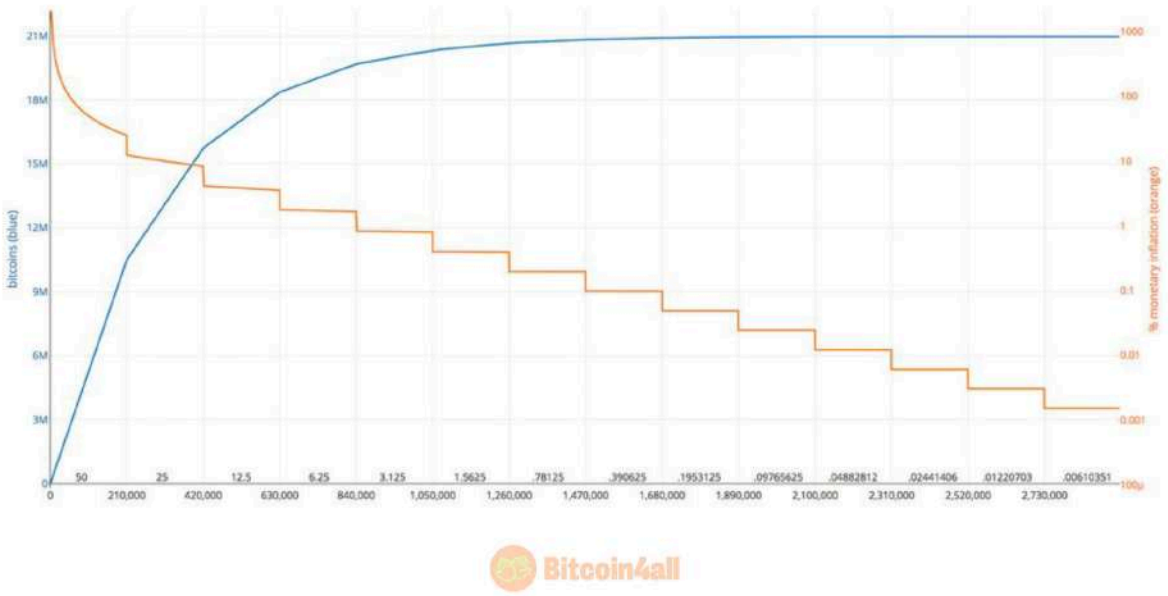
Halving	Estimated Date	Block height	Block reward (BTC)
0	N/A	0	50
1	28/11/2012	210.000	25
2	09/07/2016	420.000	12,5
3	11/05/2020	630.000	6,25
4	2024	840.000	3,125
5	2028	1.050.000	1,5625

(slide 128) - Bitcoin 4 All

The first halving took place on November 28, 2012, at the very beginning of the network. At the time, the Bitcoin network produced 50 bitcoin per block of information processed. In other words, for every 10 minutes on average at that time, miners received 50 bitcoin as a reward. With the 2012 halving, miners were paid 25 bitcoin per mined block.

In 2016, the second halving took place, in the 420,000 block, and the emission was halved again. Instead of receiving 25 bitcoin per block, each miner now receives 12.5 bitcoin per mined block. The third halving took place in 2020, on May 11, in block 630,000. From then on, miners received 6.25 bitcoin per block until the next halving.

The last recorded halving, the fourth, took place in April 2024 at block 840,000. The next one will be in 2028. The best thing about all this is that we know in advance which block it's going to be: at the time of the 1.50 million block. The new reward will be 1.5625 bitcoin for miners.



(slide 129) - Bitcoin 4 All

This image shows how, at each halving -- a step upwards of the orange line --, Bitcoin is slowly becoming scarcer and approaching the unit supply limit in the blue line.

That's quite an amazing image: it illustrates how Bitcoin is transparent, programmable and has a predictable monetary policy that cannot be expanded or modified. These aspects are very different from other assets or currencies that change their rules or monetary policies at any given time.

The last satoshi will be mined in the year 2140: that's when the issuance of new bitcoin will end. Network fees will be the only source of revenue for miners to pay for operating costs.

Years	Years since inception	Total # of Blocks	Block Reward (BTC)	Total Mined BTC	% of Total Mined
2008 - 2012	0 - 4	210,000	50.00000000	10,500,000.000	50.00000000%
2012 - 2016	4 - 8	420,000	25.00000000	15,750,000.000	75.00000000%
2016 - 2020	8 - 12	630,000	12.50000000	18,375,000.000	87.50000000%
2020 - 2024	12 - 16	840,000	6.25000000	19,687,500.000	93.75000000%
2024 - 2028	16 - 20	1,050,000	3.12500000	20,343,750.000	96.87500000%
2028 - 2032	20 - 24	1,260,000	1.56250000	20,671,875.000	98.43750000%
2032 - 2036	24 - 28	1,470,000	0.78125000	20,835,937.500	99.21875000%
2036 - 2040	28 - 32	1,680,000	0.39062500	20,917,968.750	99.60937500%
2040 - 2044	32 - 36	1,890,000	0.19531250	20,958,984.375	99.80468750%
2044 - 2048	36 - 40	2,100,000	0.09765625	20,979,492.188	99.90234375%
2048 - 2052	40 - 44	2,310,000	0.04882813	20,989,746.094	99.95117188%
2052 - 2056	44 - 48	2,520,000	0.02441406	20,994,873.047	99.97558594%
2056 - 2060	48 - 52	2,730,000	0.01220703	20,997,436.523	99.98779297%
2060 - 2064	52 - 56	2,940,000	0.00610352	20,998,718.262	99.99389648%
2064 - 2068	56 - 60	3,150,000	0.00305176	20,999,359.131	99.99694824%
2068 - 2072	60 - 64	3,360,000	0.00152588	20,999,679.565	99.99847412%
2072 - 2076	64 - 68	3,570,000	0.00076294	20,999,839.783	99.99923706%
2076 - 2080	68 - 72	3,780,000	0.00038147	20,999,919.891	99.99961853%
2080 - 2084	72 - 76	3,990,000	0.00019073	20,999,959.946	99.99980927%
2084 - 2088	76 - 80	4,200,000	0.00009537	20,999,979.973	99.99990463%
2088 - 2092	80 - 84	4,410,000	0.00004768	20,999,989.986	99.99995232%
2092 - 2096	84 - 88	4,620,000	0.00002384	20,999,994.993	99.99997616%
2096 - 2100	88 - 92	4,830,000	0.00001192	20,999,997.497	99.99998808%
2100 - 2104	92 - 96	5,040,000	0.00000596	20,999,998.748	99.99999404%
2104 - 2108	96 - 100	5,250,000	0.00000298	20,999,999.374	99.99999702%
2108 - 2112	100 - 104	5,460,000	0.00000149	20,999,999.687	99.99999851%
2112 - 2116	104 - 108	5,670,000	0.00000075	20,999,999.844	99.99999925%
2116 - 2120	108 - 112	5,880,000	0.00000037	20,999,999.922	99.99999963%
2120 - 2124	112 - 116	6,090,000	0.00000019	20,999,999.961	99.99999981%
2124 - 2128	116 - 120	6,300,000	0.00000009	20,999,999.980	99.99999991%
2128 - 2132	120 - 124	6,510,000	0.00000005	20,999,999.990	99.99999995%
2132 - 2136	124 - 128	6,720,000	0.00000002	20,999,999.995	99.99999998%
2136 - 2140	128 - 132	6,930,000	0.00000001	20,999,999.998	99.99999999%

(slide 130) - Bitcoin 4 All

This table here is another way of showing the same thing. This table shows Bitcoin's entire monetary policy: from the first satoshi and the first halving to the last halving in 2140.

We can see that more than 90% of bitcoin have already been issued and that, by the year 2036, 99% of all bitcoin to ever exist will have been mined. The rest, the final 1%, will be created between 2036 and 2140. It takes 110 years to mine 1% of the remaining Bitcoin supply!

The year 2030 is probably when the biggest source of income for miners will be fees. At this point, Bitcoin's demand should be very high, to the point where the fees charged by miners sustain their operation, including machine maintenance and energy costs, instead of depending on the block reward.

(slide 131) - Bitcoin 4 All

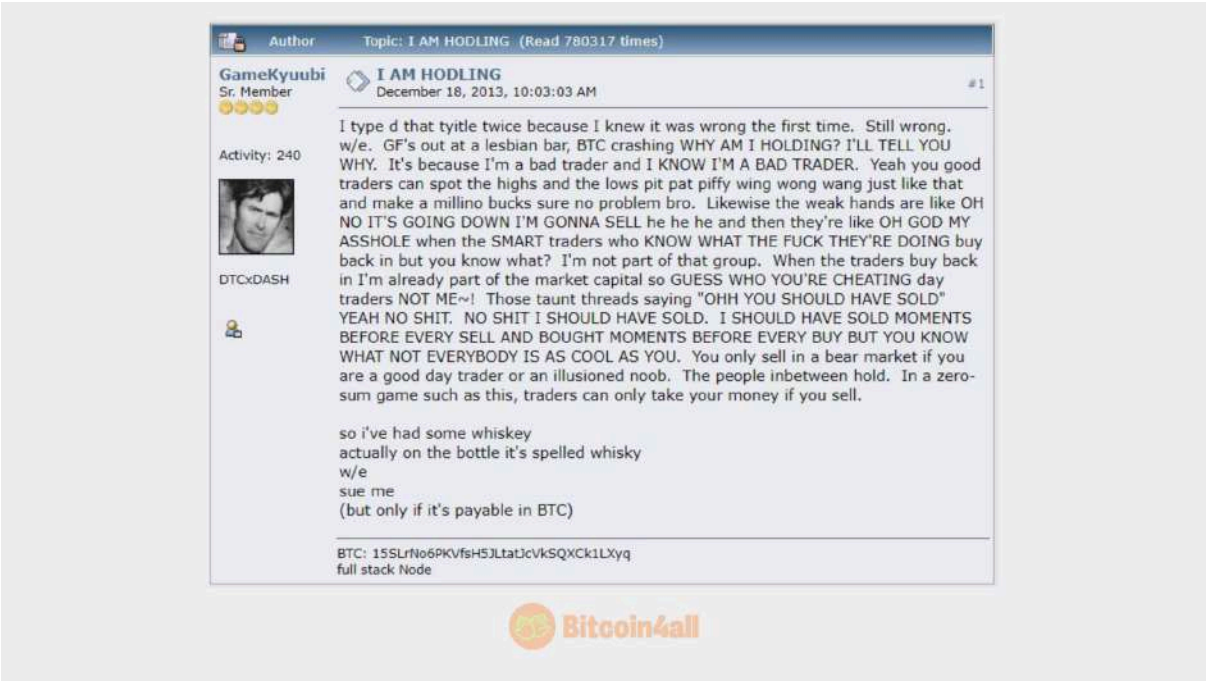
When we talk about 2140, there's fear of the unknown and doubt: "What happens when the last bitcoin is mined?"

The answer is: nothing. This great change begins much earlier. By 2030, fees will tend to be the main source of income for miners. By the time 2140 arrives, miners will probably be receiving much more in fees than the few satoshis offered by the network due to the increasing scarcity of the currency, the rising price of fiat and the increased use of the network.

And why is the halving so important?

(slide 132) - Bitcoin 4 All

Halvings create a "supply shock": fewer bitcoin become available while demand remains the same. With each halving, the number of bitcoin mined per block is cut in half. This reduces supply, which pushes up the price. If a lot of people want to buy bitcoin and you can't create more units, the only way to convince hodlers to sell is to offer a higher price.



(slide 133) - Bitcoin 4 All

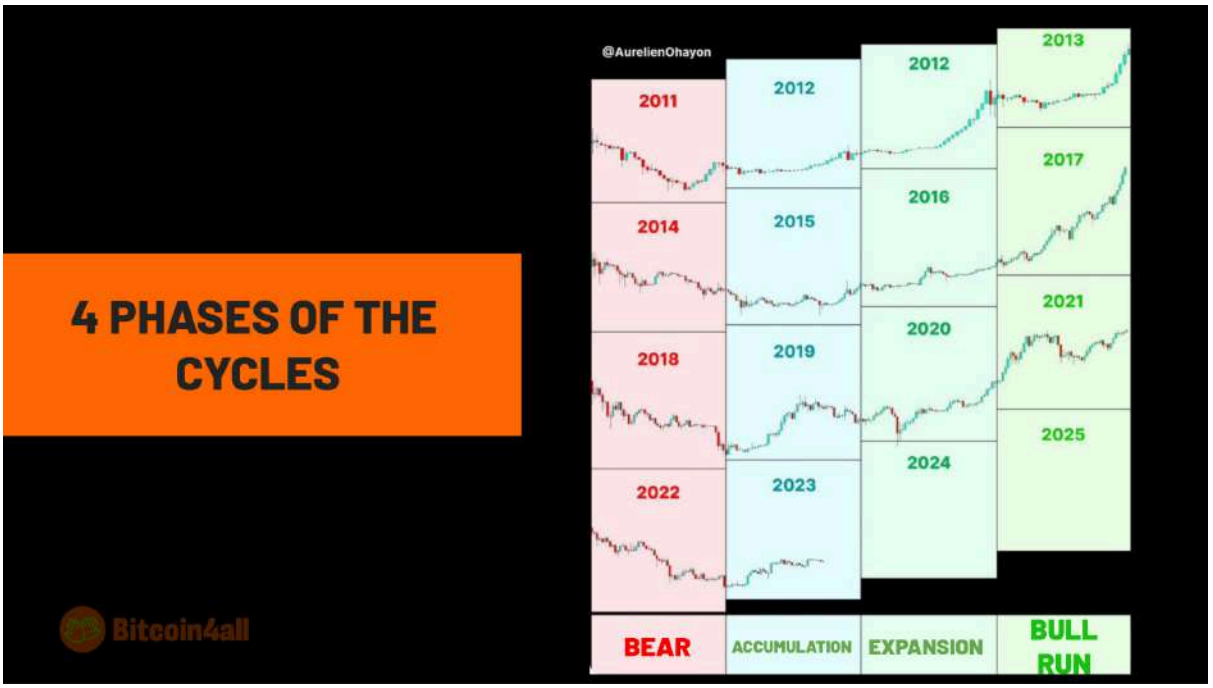
"Hodlers" are bitcoiners who accumulate bitcoin for the long term and don't sell even in the biggest short-term falls. The term hodler became a meme because a guy on Bitcoin Talk, a famous bitcoin forum, misspelled it and people adopted the slang to differentiate it from the

traditional stock market crowd. This image is a screenshot of the post that gave hodlers their name: bitcoiners who hold bitcoin tightly and don't sell at all.

This rise forms parabolic movements and attracts everyone's attention: Bitcoin makes the news, further increasing demand. That's when the hallucinatory euphoria of the bull run begins.

This is because the only way to have the same liquidity to satisfy new buyers is to increase the premium so that those who have Bitcoin change their minds and want to sell. It's the simplest law of economics: the law of supply and demand. If there is too much demand and supply is reduced, prices rise. As the number of Bitcoin is limited to 21 million units and there is no way to issue more, when demand increases, the only way for supply to meet demand is for the price to go up.

Halvings cause supply shocks that make Bitcoin's price to rise until a new price breakthrough. This whole process creates cyclical movements of appreciation and contraction until the new price is set.



(slide 134) - Bitcoin 4 All

Bitcoin cycles are made up of four phases. The first phase is the BEAR, when the market is bearish. This is when the price falls sharply after a period of highs and those who joined the boom leave. 2011, 2014, 2018 and 2022 were Bitcoin's bear years. That's when only negative news comes out and those who were tourists in Bitcoin leave.

Following the bear comes a VERY agonizing phase, which is the accumulation phase. Which is when Bitcoin goes sideways for a whole year. Nothing happens. It's pure boredom and it never seems to end.

The next phase is the expansion, or growth, phase. That's when Bitcoin starts to rise slowly, without a peep. This is the phase in which the haters attack because they don't believe in a new rise and bitcoiners begin to renew their hopes that a new bull run is on the horizon. 2012, 2016, 2020 and 2024 were years of expansion.

And -- finally -- comes the bull run. That's the Bitcoin reaches the peak of the cycle and runs like an unbridled bull. Nothing can hold it back. This phase is pure joy and euphoria -- even the haters disappear! Bitcoin is the talk of the town, attracting everyone's attention and reaching new price levels. When the euphoria wears off, the fall comes. A new price floor is established, and so it all goes back to the beginning, to the bear phase. It's a mental (and emotional) rollercoaster.

(slide 135) - Bitcoin 4 All

So much so that the fear and greed index was created just to measure the emotional state of the market. The closer to 0 it gets, the closer the sentiment is to "Extreme Fear", while approaching to 100 represents approaching "Extreme Greed".

(slide 136) - Bitcoin 4 All

People generally want Bitcoin to appreciate in a straight line, but Bitcoin's biggest rises took a year to reach the apex of the movement. Let's take a closer look to analyze Bitcoin's price following the halvings. From the halving to the top of the cycle, it has taken about a year to hit an ATH (all-time high), but it doesn't happen in a straight line. The chart fluctuates a lot, but with an average upward rise in value. Bitcoin appreciated 11,000 percent after the first halving, 2,500 percent after the second halving and 1,000 percent after the third halving in 2020, when it reached the last ATH at 69,000 dollars. The fourth halving took place in 2024, Bitcoin has already hit $100k and those who live to see it will know how far the price can go in this cycle.

(slide 137) - Bitcoin 4 All

But everything that goes up has to come down. Although Bitcoin's great rises in value have diminished their intensity over the years, the same has happened with the falls.

In 2012 Bitcoin had a brutal drop of 93%. After the first halving, it dropped 84%. In the second halving, it fell 84% again. In the last halving, the drop was 77%, lower than in the previous bears. This means that over time Bitcoin is becoming less volatile. Of course, it's a long way from moving in a straight line, but we can already notice this trend.

(slide 138) - Bitcoin 4 All

What can also be observed is that Bitcoin has had increasingly higher lows throughout the cycles. In 2012, one bitcoin was worth less than a dollar. By 2014 the minimum was already ten dollars. In 2016, it was worth a hundred dollars, in 2019 a thousand dollars and, in 2022, ten thousand dollars.

In other words, as much as Bitcoin falls a lot, it has maintained higher and higher minimum prices over time. But will it always be like this? Will Bitcoin continue to appreciate forever?

This is the subject of the next lesson. Now that you've learned how Bitcoin works and the history of Bitcoin's cycles, it's time to understand why it tends to keep growing in the long term. See you there.