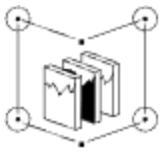

Digital Assets Academy[23]

Lecture 02 — Cryptocurrency: A closer look at Bitcoin

Transcript

Bitcoin is a cryptocurrency that is built using its own blockchain. Bitcoin is decentralized, meaning there is no singular authority that controls it. Instead, it uses encryption based on blockchain technology, calculated by multiple parties on the network, to verify transactions and maintain the protocol.

Bitcoin, with a capital “B”, often refers to the network, the system, or the concept, while bitcoin, with a lower-case “b”, typically refers to the asset BTC.

Transactions are ordered and added to the blockchain through Bitcoin’s Proof-of-Work consensus mechanism, which rewards cryptocurrency miners for validating transactions. In other words, by extending the blockchain with new transactions, bitcoin miners are compensated in two ways. First, they receive newly minted issuance, as in supply inflation, and second, they receive transaction fees included by spenders seeking to have their transactions added to the blockchain more quickly.

Bitcoin is governed by three groups of stakeholders: miners, nodes, and developers. Together, these groups reach a balance that we call the governance triumvirate, with each group possessing checks and balances against the other two.

Developers are essential for writing and deploying code, whether to fix bugs or add new features, but developers cannot force nodes and miners to run that code.

Nodes can choose which code to run, and they validate blocks and transactions, but nodes do not write code and cannot append new transactions to the ledger.

Miners can pick and choose which transactions to add to the ledger, and in which order, but they don’t write code and their blocks can be rejected by nodes. There are drawbacks to this type of system design, but this dynamic results in a decentralized balance of power that keeps Bitcoin credibly neutral in a way that no other system can achieve.

Bitcoin itself was first proposed on October 31st, 2008, when Satoshi Nakamoto, an anonymous developer, published the first version of the Bitcoin whitepaper. Later, Satoshi mined the first block, block #0, also known as the “Genesis Block”, on January 3rd, 2009, and famously inscribed the words “Chancellor on brink of second bailout for banks,” a headline from that

day's London Times, in the first transaction.

Satoshi's reference had a dual meaning. First, holding up today's newspaper to provide a timestamp and proving to the world that he did not selfishly begin mining the coin earlier than he had stated, and second, to reference Bitcoin's positioning as an alternative to the traditional banking system.

Bitcoin is a digital monetary asset. Although it has no industrial use, it is scarce, durable, portable, divisible, verifiable, fungible, scalable, and salable, and recognized across borders, and therefore has the properties of money.

Bitcoin already has several uses today, but the core of what makes BTC valuable in the marketplace is defined by supply and demand.

Scarcity: Bitcoin's protocol limits it to 21 million coins in total, which gives it both scarcity and a predictable issuance schedule.

As with other commodities, Bitcoin's defined, limited, and crucially inelastic supply support its value as its demand increases. There is no central authority that can unilaterally change that limit; Satoshi Nakamoto himself couldn't add more coins to the Bitcoin protocol if they wanted to.

The inelasticity of Bitcoin's supply is a significant factor here. While gold is widely considered a scarce commodity, increases in demand still incentivize gold miners to produce more gold. In contrast, no matter how much incentive there is for Bitcoin miners to produce more bitcoin, they can never alter the supply dynamics.

These coins are divisible into 100 million units each, like fractions of an ounce of gold. This smallest fraction of a bitcoin is called one satoshi. And today, there are currently 19.431 million BTC in existence. That's 92.5% of Bitcoin's terminal supply of 21 million, or 1,943,158,600,000,000 satoshis.

Another way that Bitcoin devices value is its fundamental utility. While Bitcoin's scarcity helps make BTC's exchange rate increase along with usage, several of Bitcoin's properties help drive demand for bitcoin, its underlying asset. The network is censorship resistant, meaning it's extremely difficult for any party, including a nation state, to prevent a user from sending a transaction or a miner from mining a block.

It is permissionless, and that nature allows the network to be accessed, used, mined, or validated by users and nodes around the world. Its decentralization brings credible neutrality to the network and also makes the network resilient to disruptions or downtime. Bitcoin transactions are extremely programmable and are likely to become more so in the future, with the ability to add features without the use of an intermediary.

Network effects are also important to consider. A network effect is an attribute of a network system. As more people use the network, a network becomes exponentially more valuable for each user. Bitcoin's network effect refers to the idea that as more people use and accept Bitcoin, its demand, value, and utility increase.

Bitcoin's network is protected in several ways. Its high hashrate – the measurement of computational power expended per-second by miners – makes it difficult or impossible for bad actors to disrupt the growth of the blockchain through attacks on Bitcoin's proof-of-work consensus process.

Adversarial nodes, which validate blocks transactions, make it difficult or impossible to alter Bitcoin's code. A developer ecosystem that is widely distributed and operates in a completely transparent way increases the security of bitcoin's code and decreases the likelihood that malicious upgrades are introduced or implemented.

These three factors Scarcity, Functionality, combined with Network Effect, help give Bitcoin its value.

What is Bitcoin Mining?

Mining is the process by which new blocks are created and new transactions are added to the blockchain ledger. In Proof of Work mining, the process Bitcoin utilizes, miners compete to solve a simple but difficult mathematical puzzle that requires significant amounts of computational work. Upon identifying a valid solution to the puzzle, Bitcoin miners submit their proof, a new block, to the rest of the network and, upon acceptance of that block, the network issues a reward to the miner, resulting in the creation of newly minted bitcoin.

Miners also receive the transaction fees appended by spenders to all the transactions in the block they create and publish. Together, the newly minted issuance, called a reward, or "block subsidy", and the transaction fees comprise a miner's revenue. Each block, miners submit proof of their computational work to the network, and that proof is validated by network nodes, hence the name "Proof of Work."

To maintain the hard cap supply of 21 million coins, as well as keep Bitcoin's network block time, the average interval between blocks added to the blockchain, at 10 minutes, the Bitcoin network periodically adjusts the difficulty of the puzzle. This adjustment happens every 2016 blocks or approximately every two weeks. If the average time between blocks is greater than 10 minutes during one of these 2016-block periods, also known as a "difficulty epochs", which would mean that the cumulative mining hashrate during that period had reduced, the Bitcoin network will then reduce the puzzle's difficulty. Alternatively, if the cumulative mining hashrate increases during the difficulty epoch, resulting in an average block time that is less than 10 minutes, the Bitcoin network will increase the puzzle's difficulty.

I know this sounds complicated, but this is known as the “Difficulty Adjustment” and it’s an important part of Bitcoin.

While the term “miner” typically refers to an entity that participates in block production on a Proof-of-Work network, the term “validator” typically refers to an entity that participates in block production on a Proof-of-Stake network, which we will explain more in our Ethereum lecture.

What is the Halving Cycle?

When Satoshi mined the Genesis Block on January 3rd, 2009, they received 50 BTC in compensation from the network, which were the first 50 BTC in Bitcoin’s supply. Over the next 210,000 blocks, each new block that was mined resulted in the creation of 50 new BTC, which were paid to miners as compensation for producing that new block.

However, the protocol is programmed so that this amount of new coins per block decreases over time, once a certain number of blocks are added to the blockchain. These events are called “halvings”.

Every 210,000 blocks, which is approximately every four years, the first portion of Bitcoin miner revenue, the “reward” or “block subsidy”, reduces by 50% in an event known as a “halving.”

There have been three halvings in Bitcoin’s history so far and the current block subsidy is 6.25 BTC per block, resulting in approximately 900 new bitcoins issued per day.

Bitcoin’s 4th halving will occur at block height 840,000 which is currently expected sometime in April 2024 and will reduce the block subsidy to 3.125 BTC per block.

Bitcoin has transformed from a relatively obscure digital currency into a globally recognized asset, and we believe today Bitcoin stands as a legitimate macro asset. At the time of this recording, Bitcoin has a market capitalization of over $570 billion dollars, approximately half a million daily transactions, and hundreds of millions of users globally.

Consider the difference in scarcity between dollars, euro, yen, and other fiat currencies and their unrestricted supplies vs. inherently scarce commodities like gold and silver and the perfectly scarce Bitcoin. In a time of rising challenges for our monetary system, you could consider it a hedge, both because of its scarcity and its global nature.

With the global banking system rocked by rising interest rates, attention has turned once again to Bitcoin. Over the past year, Bitcoin has been one of the best-performing assets when compared to a range of securities, both equities and fixed income, indices, and commodities. Over longer time frames, Bitcoin’s outperformance only improves. However, past performance is no guarantee for future performance.

Bitcoin’s disinflationary nature, meaning its programmatically declining inflation leading to its fixed supply, could make it a more inflation-resistant asset and therefore a good store of value over longer timeframes.

The next halving is expected to occur around April 2024. Historically, Bitcoin has performed well in the years following halving events. However, with a sample size of only three halvings, which all occurred in low interest rate environments, it does remain to be seen how the next halving will play out.

Addressing the common misconceptions of Bitcoin.

One misconception is that bitcoin has no intrinsic value. While Bitcoin might not be backed by a physical asset like gold, neither is the US dollar or virtually any other modern fiat currency. As mentioned before, most fiat currencies derive their value from a centralized authority and its supply and demand. Unlike the USD or other fiat currencies, bitcoin is fully decentralized, scarce, and mathematically verifiable. Due to its limited supply, functionality, and network effects, it has established a robust belief system around the world. The more people that use bitcoin, the more people it attracts. And because its supply is completely inelastic, this self-reinforcing virtuous network effect should make it more and more valuable over time.

Another misconception is that a better cryptocurrency could come along, which would decrease the value of bitcoin. Through a combination of first-mover advantage and smart design, Bitcoin’s network effect of security and user adoption is very hard for other cryptocurrencies to catch up with at this point. Bitcoin's dominance is currently around 48% of the cryptocurrency market, and much higher if you remove stablecoins and low-liquidity coins from the calculation, despite a full decade of alternative coin launches. That being said, Bitcoin is a young technology and other digital assets, like infrastructure tokens could gain more market share in the future.

Another misconception is that Bitcoin mining consumes too much energy. Bitcoin mining’s competitive nature makes it an energy-intensive process at scale. But determining the environmental impact is hard. For one, all aspects of the digital economy require energy. Already a significant portion of bitcoin mining is powered by renewable energy sources, or energy surplus. Bitcoin mining will gravitate towards the cheapest form of energy, which is increasingly renewable energy.

And lastly, Bitcoin’s energy consumption is undeniable, but critical in preserving the security of the network. Bitcoin’s environmental footprint currently remains relatively small. As of 2022, electricity generation powering bitcoin mining is estimated to be responsible for 0.1% of world greenhouse gas emissions. We will go into more detail, in our “ESG” lecture as part of this academy series.

We also hear that Bitcoin is too volatile. The inelasticity of Bitcoin’s supply is one of the network’s most prominent features, and it also contributes to the volatility of bitcoin’s

exchange rate. However, as more and more people have used Bitcoin over the years, its exchange rate volatility has consistently declined. That being said, it is important to state that bitcoin remains a risky growth asset, but that doesn't mean it shouldn't be included in your portfolio. The common way to deal with volatile assets in a portfolio is with proper position sizing.

We don't hear it often, but some people ask if Bitcoin is secure. Since BTC has had any exchangeable value, the Bitcoin network has never been hacked. Bitcoin's core protocol has functioned securely with 99.9% uptime since its creation in 2009.[1] A vast amount of computing power secures the network. The miners that power the network are distributed throughout the world and while some mining pools control between 20 and 30% of the hash rate, Bitcoin is unlikely to suffer from a so-called 51% attack due to the prohibitive cost of acquiring that much hashing power. But even in the case of a successful 51% attack, a malicious actor can only disrupt the chain or attempt double-spend attacks with new transactions, but they cannot seize bitcoin from existing wallets.

In Summary:

Bitcoin is the first decentralized and censorship-resistant, verifiable, scarce digital asset. It introduced the concept of digital private property on the Internet.

Bitcoin's protocol limits it to 21 million coins. It's scarcity and fundamental transactional properties combine with its network effect to give it value.

Bitcoin combines the scarcity of gold with the portability and fungibility of fiat currencies. This makes it ideal for a global digital age.

Bitcoin uses a proof-of-work consensus mechanism. Mining is the process by which new blocks are created and new transactions are added to the blockchain ledger.

Bitcoin mining requires computational work, which consumes electricity, and is estimated to contribute about 0.1% to the world's greenhouse gas emissions as of today.

Bitcoin has been one of the best-performing assets and we believe it deserves consideration in an investor's portfolio.

[1] Bitcoinuptime.org