3. What is a BTC?

TL;DR:

(The abbreviation "TL;DR" stands for "Too Long; Didn't Read." It is commonly used on the Internet to summarize lengthy pieces of text, providing a brief overview or key points for those who do not want to read the entire content.)

- Bitcoin is a cryptocurrency that operates on a decentralized database called blockchain.
- The transactions on the Bitcoin network are recorded on a public ledger and verified by a network of nodes located worldwide.
- Bitcoin is transparent and permissionless, making it a popular alternative to the traditional financial system.

What Is a Bitcoin?

Bitcoin is a digital form of cash. But unlike the government-issued ***fiat currencies*** you're used to, no central bank controls it. Instead, the financial system in Bitcoin is run by thousands of computers distributed around the world. Anyone can participate in the ***ecosystem*** by downloading Bitcoin's open-source software.

Bitcoin was the first cryptocurrency, announced in 2008 (and launched in 2009). It allows users to send and receive digital money called bitcoins (with a lowercase b, or BTC). What makes it highly appealing is its inherent resistance to censorship, the impossibility of double-spending funds, and the ability to conduct transactions anytime and anywhere.

For our students, Bitcoin represents a unique opportunity. Its decentralized nature means it allows students to participate in the global financial system without needing permission from traditional financial institutions. This can be empowering, providing a level playing field where they can engage in economic activities, save, and invest without barriers.

What Makes Bitcoin Unique?

Here are a few of the key features that make Bitcoin unique:

1. Decentralization—Bitcoin operates on a decentralized public ***blockchain***, meaning a central authority doesn't control it. Instead, transactions are verified by the network of computers, known as ***nodes***. In addition, anyone can join the network and help secure it.
2. Permissionless—Bitcoin's permissionless nature means that anyone with an internet connection can participate in the Bitcoin network without authorization or permission from a central authority. Bitcoin allows users to send and receive payments with anyone on the network, regardless of location or identity. This has made bitcoins particularly popular in regions where access to traditional financial systems is limited or non-existent.
3. Limited supply—Bitcoin has a limited supply of 21 million coins hard-coded into the protocol. This means there will never be more than 21 million bitcoins in circulation, which helps prevent inflation.
4. Transparency—All bitcoin transactions are recorded on a ***public ledger*** that is visible to all users. This means that anyone can see the transactions that have taken place, including the amount of bitcoin involved and the addresses of the sender and receiver. In traditional financial systems, transactions are recorded by banks and other financial institutions, and this information is not generally available to the public. Instead, people rely on these institutions to keep accurate records.
5. Divisibility—Bitcoin can be divided into smaller units called ***satoshis***, which are one hundred millionth of a bitcoin. This means that even if the price of a bitcoin becomes very high, people can still use and transact with very small amounts of the currency. This makes bitcoins more accessible to people with limited financial resources and allows for more granular transactions.

How Does Bitcoin Work?

Understanding Bitcoin's blockchain can be particularly empowering for our students. It provides a transparent and secure way to participate in financial transactions without relying on traditional banks, which may have been barriers in the past. Bitcoin's decentralized nature means no single entity can control or restrict access, making it a fair system for everyone involved.

Let's consider a hypothetical scenario involving three people: Alice, Bob, and Carol. When Alice makes a transaction with Bob, she's not sending money in the way

you'd expect. It's not like the digital equivalent of handing him a dollar bill. It's more like she's writing on a piece of paper (that everyone can see) that she's giving Bob a dollar. When Bob goes to send the same funds to Carol, she can see that Bob has them by looking at the sheet of paper.

The sheet is a database called a blockchain. All network participants have an identical copy of it stored on their devices. The participants connect with each other to synchronize new information.

To maintain the security and integrity of the blockchain, Bitcoin uses a consensus mechanism known as ***Proof of Work*** (PoW). When a user makes a payment, they broadcast it to the network, where it is verified by other nodes known as "miners." These miners compete to solve a complex mathematical puzzle and must devote computing power to do so. The first ***miner*** to solve the puzzle gets to add a new block of transactions to the blockchain.

As an incentive, there is a reward available for whoever proposes a valid block. The reward, often referred to as the ***block reward***, is made up of two components: transaction fees from the transactions within the block and the block subsidy. The block fee is the only source of "fresh" bitcoins. With each block mined, it adds a certain amount of coins to the total supply.

Bitcoin's PoW consensus mechanism is designed to make it expensive to create a block, but cheap to verify that it's valid. Suppose someone tries to cheat with an invalid block. In that case, the network immediately rejects it and the miner is unable to recoup the cost of mining.

Anyone in our audience can play the role of Alice, Bob, or Carol. As there are no barriers of entry in cryptocurrency, we believe Bitcoin offers our students a way to gain financial independence, engage in the digital economy, and open up new opportunities for entrepreneurship.

What Is Bitcoin Used For?

Bitcoin is primarily used as a digital currency and store of value. It can be used to make purchases online or in person, just like traditional currencies. Anyone with an internet connection can send and receive it, and its digital presence means that it can be transferred globally.

Bitcoin is sometimes used for more private transactions. The transactions are public, and the addresses (public keys) are pseudonymous, though not completely anonymous. In other words, while the transactions are visible on the blockchain, the users behind them are not easily identifiable.

Some people also buy bitcoins as a long-term investment, expecting their value to increase over time. Like gold or other commodities, bitcoins' limited supply and decentralized nature have made it a viable option for investors looking to diversify their portfolios.

A History of Bitcoin

Bitcoin was first introduced in 2008 when Satoshi Nakamoto published a white paper entitled "Bitcoin: A Peer-to-Peer Electronic Cash System." This white paper introduced a new digital currency that would operate on a decentralized system without relying on governments or the banking system.

In January 2009, the Bitcoin protocol was released, and the first bitcoin transaction took place between Satoshi Nakamoto and a programmer named Hal Finney. The transaction involved sending ten bitcoins from Nakamoto to Finney.

After the first transaction, more people began to discover Bitcoin and join the network. The digital currency gained popularity among a small community of tech enthusiasts by demonstrating that Bitcoin could function without a central authority or intermediary.

Bitcoin Pizza is another important milestone in the history of Bitcoin, as it marked the first time bitcoins were used as a medium of exchange for a real-world transaction. On May 22, 2010, a programmer named Laszlo Hanyecz made history by using 10,000 bitcoins to buy two pizzas. The transaction became known as "Bitcoin Pizza Day" and is now commemorated every year on May 22.

Who created Bitcoin?

Satoshi Nakamoto's identity remains a mystery. Satoshi could be a person or a group of developers anywhere in the world. The name is of Japanese origin, but Satoshi's mastery of English has led many to believe that he or she is from an English-speaking country.

Did Satoshi invent blockchain technology?

Bitcoin combines a number of existing technologies that have been around for a long time, and this includes blockchain technology. The use of such immutable data structures can be traced back to the early 1990s when Stuart Haber and W. Scott Stornetta proposed a system for time-stamping documents. Much like today's blockchains, it relied on cryptographic techniques to secure data and prevent it from being tampered with.

How many bitcoins are there?

The protocol sets the maximum supply of bitcoins at 21 million coins. As of 2023, just over 90% of these have been mined, but it will take over a hundred years to produce the rest. This is due to periodic events known as halving, which gradually reduce the mining reward.

What Is Bitcoin Halving?

Bitcoin's ***halving*** is a process that reduces the rate at which new Bitcoin blocks are created. Specifically, it refers to the periodic halving events that reduce the block rewards offered to miners. The next Bitcoin halving is expected to happen in 2024, roughly four years after the last halving, which took place in May 2020.

Bitcoin halving is at the core of its economic model as it ensures that coins are issued at a steady pace, getting increasingly difficult at a predictable rate. Such a controlled rate of ***monetary inflation*** is one of the key differences between cryptocurrency and traditional fiat currencies, which have an essentially infinite supply.

Is Bitcoin Safe?

One of the main risks associated with Bitcoin is the potential for hacking and theft. For example, in phishing scams, hackers use ***social engineering*** techniques to trick users into revealing their login credentials or private keys. Once the hacker has access to the user's account or crypto wallet, they can transfer the victim's bitcoins to their own wallet.

Another way hackers can steal bitcoins is through malware or ***ransomware*** attacks. Hackers can infect a user's computer or mobile device with malware that

allows them to access the user's Bitcoin wallet. In some cases, hackers can also use ransomware to ***encrypt*** a user's files and demand payment in bitcoins to unlock them.

Because bitcoin transactions are irreversible and not insured by any government agency, users must take precautions to protect their bitcoin holdings. This includes using strong passwords, two-factor authentication, and storing bitcoins in a secure crypto wallet that is inaccessible to hackers. It's also important to only download Bitcoin-related software from trusted sources.

Another risk associated with bitcoin is price volatility. The value of bitcoin can fluctuate highly over short periods of time, making it a risky investment for those who are not prepared for the potential losses.

Closing Thoughts

Bitcoin is a decentralized digital currency that has gained significant attention in recent years. It was created to provide an alternative to traditional financial systems and operates on a peer-to-peer network, allowing users to send and receive payments without intermediaries.

While Bitcoin is still a relatively new technology, it's already revolutionizing the way we think about money. As bitcoin and other cryptocurrencies continue to evolve, it will be interesting to see if they become a part of our everyday lives.

Our team at Prison Professors looks at Bitcoin as more than a digital currency. It also symbolizes a pathway to financial empowerment and independence. Traditional financial systems have often posed significant barriers, making it difficult to access banking services, secure loans, or even open a simple bank account. Bitcoin and other cryptocurrencies offer an alternative—a decentralized financial system that is open to everyone, regardless of their past.

Having spent over a quarter century in prison, I understand the profound disconnect individuals experience when transitioning from incarceration to a world shaped by rapid technological advancements. I encourage our students to invest in themselves by learning about new trends in technology, as demonstrated by our work with Binance. Remember, self-directed education is a powerful tool for overcoming obstacles and seizing opportunities. Our initiative is not just about learning new technologies; it's about empowering justice-impacted individuals to build a better future, both for themselves and their communities.

Critical Thinking Questions

1. How can Bitcoin's decentralized nature empower you to overcome traditional financial barriers?

2. In what ways might the transparency of Bitcoin transactions enhance financial trust and security for you as you re-enter society?

3. How does Bitcoin's limited supply and divisibility affect its potential as a long-term investment for you?

4. What challenges and opportunities might arise from the permissionless nature of Bitcoin for you if you have limited access to traditional financial systems?

5. How can learning about Bitcoin and blockchain technology provide new entrepreneurial opportunities for you?

Glossary

- Block reward (noun): The incentive given to a miner for successfully adding a new block of transactions to the blockchain.
- Blockchain (noun): A decentralized digital ledger that records transactions across many computers in a way that ensures the security and transparency of data.
- Cryptocurrency (noun): A digital or virtual currency that uses cryptography for security and operates independently of a central bank.
- Digital economy (noun): An economy that is based on digital computing technologies, encompassing all economic activities that use digital information and communication technologies.
- Ecosystem (noun): A complex network or interconnected system, in this context, referring to the community of Bitcoin users, miners, and developers.
- Encrypt (verb): To convert information or data into a code, especially to prevent unauthorized access.
- Fiat currency (noun): Government-issued currency that is not backed by a

physical commodity but by the government that issued it.

- Halving (noun): The process by which the reward for mining new blocks is halved, occurring approximately every four years in the Bitcoin network.
- Miner (noun): A participant in a blockchain network who uses computing power to validate and add transactions to the blockchain.
- Monetary inflation (noun): The rate at which the general level of prices for goods and services is rising, leading to a decrease in purchasing power.
- Node (noun): A point in a network, typically a computer, that participates in the communication and validation of transactions in a decentralized network.
- Proof of Work (noun): A consensus mechanism used in blockchain networks where miners solve complex mathematical puzzles to validate transactions and add new blocks to the blockchain.
- Public ledger (noun): A transparent record of all transactions in a blockchain network that is accessible to all participants.
- Ransomware (noun): Malicious software designed to block access to a computer system until a sum of money is paid.
- Satoshi (noun): The smallest unit of Bitcoin, equal to one hundred millionth of a bitcoin.
- Social engineering (noun): The use of deception to manipulate individuals into divulging confidential or personal information that may be used for fraudulent purposes.
- Store of value (noun): An asset that maintains its value without depreciating over time, used as a method to preserve wealth.