The first mention of a product called bitcoin was in August 2008 when two programmers using the names Satoshi Nakamoto and Martti Malmi registered a new domain, bitcoin.org. In October of the same year, Nakamoto released a document, called a white paper, entitled “Bitcoin: A Peer-to-Peer Electronic Cash System.” In the preceding months, Nakamoto and a group of volunteer researchers had proposed different versions of the concept in forums and email threads. It was in 2008 that it all came together.

The Bitcoin White Paper
Source: Satoshi Nakamoto

This paper laid out principles of Bitcoin, an electronic payment system that would eliminate the need for any central authority while ensuring secure, verifiable transactions. In short, the document described a new form of currency, one that allowed for trustless payments on the web – that is, they require a minimal amount or even no trust between parties.

In other words, the system allowed two users who didn’t know or trust each other to exchange money in the same way they could pass cash back and forth. The system also allowed users to confirm messages, transactions and data using a tool called public key encryption, eliminating any need to disclose their identities to transaction partners or third parties. Pseudonymity, in this case, was a byproduct but not a primary feature.

In January 2009, the first bitcoin currency transaction occurred between two computers owned by Nakamoto and the late Hal Finney, a developer and an early cryptocurrency enthusiast.

To this day, no one knows who Satoshi Nakamoto really is. Even a man named Dorian Nakamoto was erroneously named as Bitcoin’s creator by a Newsweek reporter in 2014.

Dorian Nakamoto wasn't Satoshi.
Source: Newsweeklied.com

In the end, however, because of the decentralized nature of the platform, it is not considered important to know who Satoshi Nakamoto is.

Bitcoin Up Close

Bitcoins aren't printed, like dollars or euros – they're produced by computers all around the world using free software and held electronically in programs called wallets. The smallest unit of a bitcoin is called a satoshi. It is one hundred millionth of a bitcoin (0.00000001). This enables microtransactions that traditional electronic money cannot perform.

Bitcoin, often abbreviated by the ticker symbol BTC, was the first example of what we now call a cryptocurrency. Cryptocurrencies are a growing asset class that shares some characteristics with traditional currencies except they are purely digital, and creation and ownership verification is based on cryptography.

Generally the term "bitcoin" has two possible interpretations. There's bitcoin the token, which refers to the keys to a unit of the digital currency that users own and trade. A bitcoin token is held in a bitcoin wallet that is identified by a string of numbers and letters such as "1A1zP1eP5QGefi2DMPTfTL5SLmv7DivfNa." When someone wants to send you bitcoin, that person will send it to your particular, public wallet address, and you will access it via your private keys.

Then there's Bitcoin the protocol, a distributed ledger that maintains the balances of all token trading. These ledgers are massive files stored on thousands of computers around the world. The network records each transaction onto these ledgers and then propagates them to all of the other ledgers on the network. Once all of the networks agree that they have recorded all of the correct information – including additional data added to a transaction that allows the network to store data immutably – the network permanently confirms the transaction.

Bitcoin can be used to pay for things electronically, if both parties are willing. In that sense it's like conventional dollars, euros or yen, which can also be traded digitally using ledgers owned by centralized banks. Unlike payment services such as PayPal or credit cards, however, once you send a bitcoin, the transaction is irreversible – it cannot be called back.

That said, bitcoin does not depend on a centralized system of banking. Because each node on the network is owned by a private entity, the entire network is responsible for maintaining the accuracy of the ledger. When you send a bitcoin – or a fraction of a bitcoin – to another person, the entire network takes part.

This process is called **decentralization**, one of the Bitcoin network's most important characteristics. No single institution controls the bitcoin network. The protocol is maintained by a group of volunteer coders, and run by an open network of dedicated computers around the world.

Since there is no central validator in this network, users do not need to identify themselves when sending bitcoin to others. When a sender initiates a transaction, the protocol checks all previous transactions to confirm the sender has the necessary bitcoin as well as the authority to send them. Put another way, bitcoin users theoretically operate in semi-anonymity and the network is self-policing, ensuring that bad actors cannot be rewarded.

Bitcoin is also **pseudo-anonymous.** In practice, each user is identified by the address of his or her wallet, which can be used to track transactions. Law enforcement has also developed methods to identify users if necessary. Most exchanges are required by law to perform identity checks on their customers before they are allowed to buy or sell bitcoin. This means an exchange-assigned wallet address is most likely connected to a particular user. However, cryptocurrency wallets are not limited to exchanges or other online services, and a wallet generated by an anonymous user on a single computer is fairly difficult to trace. Further, every transaction on the network is fully transparent, a fact that concerns some privacy advocates. Ultimately, tracing a bitcoin transaction to a specific person is difficult but not impossible, and any statements describing the "anonymity" of bitcoin are inaccurate.

Since the network is transparent, the progress of a particular transaction is visible to all. Once that transaction is confirmed, it cannot be reversed. This means any transaction on the bitcoin network cannot be tampered with, making it immune to hackers. Most bitcoin hacks happen at the wallet level, with hackers stealing the keys to hoards of bitcoins rather than affecting the Bitcoin protocol itself.

Another attribute of bitcoin that takes away the need for central banks is that its supply is tightly controlled by the underlying algorithm. With fiat currencies (dollars, euros, yen, etc.), central banks can issue as many currency units as they want and can attempt to manipulate a currency's value relative to others. Holders of the currency, especially citizens with little alternative, bear the cost.

With bitcoin, a small number of new coins trickle out every hour, and will continue to do so at a diminishing rate until a maximum of 21 million has been reached. This makes bitcoin more attractive as an asset: in theory, if demand grows and the supply remains the same, the value will increase.

Generally, the value of bitcoin has risen greatly since its inception, peaking in December 2017 at a price of $19,783.06 (in U.S. dollars). On Nov. 30, 2020, the price briefly rose above that mark to $19,850.11. The actual price of a decentralized asset like bitcoin isn't strictly defined. Different services and exchanges may quote different prices for bitcoin at any given time, accounted for by discrepancies in asset liquidity, slippage and other factors. CoinDesk uses its own Bitcoin Price Index (BPI), which represents an average of bitcoin prices across leading global exchanges.

Roughly every four years, the amount of bitcoin that miners can earn in the network will be halved, potentially driving up the asset’s price. Such an event is called bitcoin halving (the most recent one happened in May 2020).
By Noelle Acheson, John Biggs and Hoa Nguyen