

Cryptocurrency, Bitcoin, and Blockchain Explained

Author : Cat

Date : January 30, 2018

Many people have heard about Bitcoin and cryptocurrency but, like many new technologies, most wave it off as being too complicated to understand. Not so. Given how much I enjoy demystifying tech for others, I've broken it down in a way that even a grade 5 student can understand it. And for reference, I did run this by an actual child in grade 5 who was able to explain it back to me afterwards.

The History of Digital Currency

Currency is an agreed upon system of trade. In the beginning, gold or silver pieces were used to trade for goods and services. This is before the time of locks and safes, meaning security on your currency would have been sketchy at best; Only you knew how many pieces you had, and if they were stolen then they were lost. Then we creating banking systems to act as an agent.

Advantages to centralized banking:

- The bank is responsible for security
- The bank maintains a ledger of what you have
- You can store massive amounts of money (don't have to keep your salary in cash under your mattress)
- Using credit cards or debit cards, you can even pay for purchases without withdrawing your cash

The problems today are that most banks need some of your money to make their profits, governments print money to devalue their debts, and financial markets are too complex for most people to understand. In 2008, after the stock market crash in the US (watch the movie [The Big Short](#) for an entertaining explanation of this event), many people lost their savings. It was at this time that a group of software developers known collectively as Cypherpunks, started seriously throwing around the idea of making a digital currency.

To them, the perceived disadvantages to centralized banking:

- Fees for withdrawing and handling the money
- Fees for exchanging from one currency to another (e.g. US dollars to Euros)
- Fees to the sellers and stores who allow credit card use
- Government-controlled currency value
- Banks making too much profit off people using them
- No access for the billions of adults that don't have a bank account

What is Cryptocurrency?

Digital currency, or Cryptocurrency, is a currency that is not tied to a physical asset, like gold. It is created by computers and the supply is limited by design so there can be no inflation by central banks printing money. When using a digital currency, you make the transaction through computer programs. You request to transfer money from yourself to either a company or a person. The money goes directly without fees. And more importantly, it's global, so no conversion fees either. It is also decentralized, meaning no bank or government controls it. In fact, the system controls itself so its value fluctuates depending on how valuable the world thinks it is.

Each transaction is protected by cryptography, like a secret code, that hides the value unless you have the key. As an owner of cryptocurrency, you are assigned an anonymous userID so there is no record that ties your identity back to your money. Using it is almost exactly the same as your current money but instead of having a digital bank statement that says you have \$1000 USD in your account, you have a digital cryptocurrency statement that says you have 1000 bitcoins (or other currency) in your account.

The first popular and accepted cryptocurrency is called [Bitcoin](#). At the time of this writing, other valuable cryptocurrencies include [Ethereum](#), [Ripple](#), [Litecoin](#), and [Monero](#).

Bitcoin and Blockchain: How digital currency stays safe

Bitcoin was introduced by a programmer (or group of programmers) known as Satoshi Nakamoto. He suggested that instead of one computer keeping a record of transactions, like the database at a bank, many computers would keep the same ledger so there could be no mistakes. Imagine a classroom of students who each had a paper on their desks. Every time a child raises their hand, the entire class marks it down. After a month there may be discrepancies but if there are 30 copies of this ledger then it is simple to see where mistakes are made. In the digital world, there are thousands of copies of this *consensus ledger*, which are verified and public.

For more assurance, we use *Blockchain*. Each transaction is considered a block. As they are made, we add the blocks in like a chain. Example, I give you \$100. Then you give me \$50 back. Then you give me another \$50 back. The end result is that we are back where we started BUT the blockchain will have 3 blocks in it so that we can see each transaction of \$100, \$50, and \$50. You cannot edit or erase the previous blocks.

In order for a computer to be allowed to keep the ledger it has to solve a cryptography problem to show it is trustworthy. Like "what's the password?" at a door, the collective computers are all validating the transactions. If a computer solves certain harder problems then the system will give it a newly created bitcoin. This is called *Mining*. If you are lucky enough to have your computer mine a new coin then it's yours to keep. That's why people are incentivized to dedicate their computers to maintaining these ledgers.

How do you get Bitcoin and where do you store it?

Like traditional currency, you can exchange your cash for bitcoin through a reliable exchange. And yes, there is probably a fee to get it, but once you are in there are no more fees for global exchanges. Numerous websites exist that allow you to buy bitcoin (see references below).

If you don't want to do the exchange, you could sell something online for bitcoin instead of cash. Or ask your employer to pay you in bitcoin (at the going rate) instead of your home currency.

You do need a Bitcoin Wallet to store your bitcoin. That's just an app that runs on your device and/or your computer. Like your current banking app.

Bitcoin Fast facts

- The maximum number of bitcoins that can exist is 21 Million, estimated for 2040, then no more mining will take place
- A single bitcoin can be divided into 100 million pieces, or in increments of 0.00000001, called a Satoshi, or *sat* for short
- The value of one Bitcoin in 2011 was \$0.008 USD, or 0.8 cents. In December 2017, it reached a high of over \$19,000 USD. Which is why we now have Bitcoin Billionaires

- No one actually knows who is behind the name Satoshi Nakamoto (despite [one guy](#) taking credit in 2016, which doesn't fully add up). It is believed to be several people together.

Why don't people like the idea of Cryptocurrency?

Like all things digital, including bank records, the companies that maintain the bitcoin wallets and exchanges are susceptible to hackers and software errors. In 2014, [Mt Gox](#), a Japanese owned Bitcoin Exchange, was handling nearly 70% of bitcoin transactions. They 'lost' over 850,000 bitcoins belonging to users worldwide. It is unclear if it was theft or mismanagement but the Mt Gox software sold off the bitcoins at a fraction of their value and they cannot be reclaimed.

Crime fighters do not like the aspect of the anonymity. When Bitcoin first made the scene, a website was launched called *Silk Road*. They sold every contraband imaginable, from drugs to guns to child pornography. With untraceable Bitcoins, it left police and agents without any clues as to who was selling and buying. Cryptocurrency supporters argued that you can also use cash to buy contraband anonymously in real life, so this is not isolated to digital currency.

If you've read this far down you will also see that though it is teachable, understanding cryptocurrency is not quick to explain. For many people, the thought of 'crypto' and 'digital' is too complicated, making it easier just to avoid it.

References and Links

If you want to read more about Cryptocurrency and Bitcoin, I suggest the following links:

- An in-depth explanation of [Cryptocurrency](#) by people who design it
- Everything you wanted to know about Bitcoin on [Reddit's Bitcoin for Beginners](#)
- White papers and research on cryptocurrency, including Satoshi's original, at the [Satoshi Nakamoto Institute](#)
- A list of places where you can use Bitcoin as a currency at [Spend A Bit](#)
- Complete instruction on [How To Buy Bitcoin](#)

In summary, Bitcoin is the first of several available cryptocurrencies that allow users to seamlessly transfer currency online globally, anonymously, and without fees. Though there is a small risk to owning cryptocurrency, it may also be a valuable investment. Is it the currency of the future? Only time will tell, but it definitely does have an important place in our global and digital world.