**Bitcoin**

Bitcoin is a virtual currency which blossomed in public consciousness after its price-per-coin rose above $13,000 in early 2018. The cryptocurrency (one of many!) forced a complex intersection of privacy policy, banking regulation, and technological innovation. Some retailers accept bitcoin, for example, while in other jurisdictions, bitcoin is illegal.

**Cryptocurrency Defined**

Cryptocurrencies are just lines of computer code that hold monetary value. Those lines of code are created by electricity and high-performance computers. Cryptocurrency is also known as digital currency. Either way, it is a form of digital public money that is created by painstaking mathematical computations and policed by millions of computer users called miners. Physically, there is nothing to hold although you can exchange crypto for cash.

Crypto comes from the word cryptography, the security process used to protect transactions that send the lines of code for purchases. Cryptography also controls the creation of new coins, the term used to describe specific amounts of code. Hundreds of coin types now dot the crypto markets; only a handful have the potential to become a viable investment.

Governments have no control over the creation of cryptocurrencies, which is what initially made them so popular. Most cryptocurrencies begin with a market cap in mind, which means that their production will decrease over time thus, ideally, making any particular coin more valuable in the future.

**What Are Bitcoins?**

Bitcoin was the first popular cryptocoin. No one knows exactly who created it — most cryptocurrencies are designed for maximum anonymity — but bitcoins first appeared in 2009 from a developer supposedly named Satoshi Nakamoto. He has since disappeared and left behind a Bitcoin fortune

Because bitcoin was the first major cryptocurrency, all digital currencies created since then are called altcoins, or alternative coins. Litecoin, peercoin, feathercoin, ethereum and hundreds of other coins are all altcoins because they are not bitcoin.

One of the advantages of bitcoin is that it can be stored offline on a person's local hardware. That process is called cold storage and it protects the currency from being taken by others. When the currency is stored on the Internet somewhere (hot storage), there is high risk of it being stolen.

On the flip side, if a person loses access to the hardware that contains the bitcoins, the currency is simply gone forever. It's estimated that as much as $30 billion in bitcoins have been lost or misplaced by miners and investors.

**Why Bitcoins Are So Controversial**

Various recent events turned bitcoin into a media sensation.

From 2011-2013, criminal traders made bitcoins famous by buying them in batches of millions of dollars so they could move money outside of the eyes of law enforcement. Subsequently, the value of bitcoins skyrocketed.

Scams, too, are very real in the cryptocurrency world. Naive and savvy investors alike can lose hundreds or thousands of dollars to scams.

Ultimately, though, bitcoins and altcoins are controversial because they take the power of issuing money away from central banks and give it to the general public. Bitcoin accounts cannot be frozen or examined by tax inspectors, and middleman banks are completely unnecessary for bitcoins to move. Law enforcement officials and bankers see bitcoins as "gold nuggets in the wild, wild west," beyond the control of police and financial institutions.

**How Bitcoins Work**

Bitcoins are completely virtual coins designed to be self-contained for their value, with no need for banks to move and store the money. Once you own bitcoins, they behave like physical gold coins: They possess value and trade just as if they were nuggets of gold in your pocket. You can use your bitcoins to purchase goods and services online, or you can tuck them away and hope that their value increases over the years.

Bitcoins are traded from one personal wallet to another. A wallet is a small personal database that you store on your computer drive (i.e cold storage), on your smartphone, on your tablet or somewhere in the cloud (hot storage).

Bitcoins are forgery-resistant. It is so computationally intensive to create a bitcoin, it isn't financially worth it for counterfeiters to manipulate the system.

**Bitcoin Values and Regulations**

A single bitcoin varies in value daily; check places like CoinDesk to check current par rates. There are more than $2 billion dollars’ worth of bitcoins in existence. Bitcoins will stop being created when the total number reaches 21 billion coins, which will be sometime around the year 2040. As of 2017, more than half of those bitcoins had been created.

Bitcoin currency is completely unregulated and completely decentralized. There is no national bank or national mint, and there is no depositor insurance coverage. The currency itself is self-contained and un-collateraled, meaning that there is no precious metal behind the bitcoins; the value of each bitcoin resides within each bitcoin itself.

Bitcoins are stewarded by miners, the massive network of people who contribute their personal computers to the bitcoin network. Miners act as a swarm of ledger keepers and auditors for bitcoin transactions. Miners are paid for their accounting work by earning new bitcoins for each week they contribute to the network.

**How Bitcoins Are Tracked**

A bitcoin holds a very simple data ledger file called a blockchain. Each blockchain is unique to each individual user and his or her personal Bitcoin wallet.

All bitcoin transactions are logged and made available in a public ledger, helping ensure their authenticity and preventing fraud. This process helps to prevent transactions from being duplicated and people from copying bitcoins.

While every bitcoin records the digital address of every wallet it touches, the bitcoin system does not record the names of the people who own wallets. In practical terms, this means that every bitcoin transaction is digitally confirmed but is completely anonymous at the same time.

So, although people cannot easily see your personal identity, they can see the history of your bitcoin wallet. This is a good thing, as a public history adds transparency and security, and helps deter people from using bitcoins for dubious or illegal purposes.

**Banking or Other Fees to Use Bitcoins**

There are very small fees to use bitcoins. However, there are no ongoing banking fees with bitcoin and other cryptocurrencies because there are no banks involved. Instead, you pay small fees to three groups of bitcoin services: the servers (nodes) who support the network of miners, the online exchanges that convert your bitcoins into dollars, and the mining pools you join.

The owners of some server nodes will charge one-time transaction fees of a few cents every time you send money across their nodes, and online exchanges will similarly charge when you cash your bitcoins in for dollars or euros. Additionally, most mining pools will either charge a small 1 percent support fee or ask for a small donation from the people who join their pools.

In the end, while there are nominal costs to use bitcoin, the transaction fees and mining pool donations are much cheaper than conventional banking or wire transfer fees.

**Bitcoin Production Facts**

Bitcoin mining involves commanding your home computer to work around the clock to solve "proof-of-work" problems (computationally intensive math problems). Each bitcoin math problem has a set of possible 64-digit solutions. Your desktop computer, if it works nonstop, might be able to solve one bitcoin problem in two to three days — likely longer.

For a single personal computer mining bitcoins, you may earn perhaps 50 cents to 75 cents USD per day, minus your electricity costs. For a large-scale miner who runs 36 powerful computers simultaneously, that person can earn up to $500 per day, after costs.

Indeed, if you are a small-scale miner with a single consumer-grade computer, you will likely spend more in electricity that you will earn mining bitcoins. Bitcoin mining is only really profitable if you run multiple computers and join a group of miners to combine your hardware power. This prohibitive hardware requirement is one of the biggest security measures that deters people from trying to manipulate the Bitcoin system.

**Bitcoin Security**

Just like holding a bag of gold coins, a person who takes reasonable precautions will be safe from having their personal bitcoin cache stolen by hackers.

More than hacker intrusion, the real loss risk with bitcoins revolves around not backing up your wallet with a failsafe copy. There is an important .dat file that is updated every time you receive or send bitcoins, so this .dat file should be copied and stored as a duplicate backup every day you do bitcoin transactions.

The collapse of the Mt. Gox bitcoin exchange service was not due to any weakness in the bitcoin system. Rather, that organization collapsed because of mismanagement and the company's unwillingness to invest in security measures. Mt. Gox, for all intents and purposes, had a large bank with no security guards and it paid the price.

**Abuse of Bitcoins**

There are currently three known ways that bitcoin currency can be abused.

1) Technical weakness — time delay in confirmation: Bitcoins can be double-spent in some rare instances during the confirmation interval. Because bitcoins travel peer-to-peer, it takes several seconds for a transaction to be confirmed across the P2P swarm of computers. During these few seconds, a dishonest person who employs fast clicking can submit a second payment of the same bitcoins to a different recipient.

While the system will eventually catch the double-spending and negate the dishonest second transaction, if the second recipient transfers goods to the dishonest buyer before they receive confirmation, then that second recipient will lose both the payment and the goods.

2) Human dishonesty — pool organizers taking unfair share slices: Because bitcoin mining is best achieved through pooling (joining a group of thousands of other miners), the organizers of each pool get the privilege of choosing how to divide up any bitcoins that are discovered. Bitcoin mining pool organizers can dishonestly take more bitcoin mining shares for themselves.

3) Human mismanagement — online exchanges: With Mt. Gox being the biggest example, the people running unregulated online exchanges that trade cash for bitcoins can be dishonest or incompetent. This is the same as Fannie Mae and Freddie Mac investment banks going under because of human dishonesty and incompetence. The only difference is that conventional banking losses are partially insured for the bank users, while bitcoin exchanges have no insurance coverage for users.

**Three Reasons Why Bitcoins Are Such a Big Deal**

There is a lot of controversy around bitcoins.

Bitcoins are not created by any central bank, nor regulated by any government. Accordingly, there are no banks logging your money movement and government tax agencies and police cannot track your money. This laxity is bound to change eventually, as unregulated money is a real threat to government control, taxation and policing.

Indeed, bitcoins have become a tool for contraband trade and money laundering, precisely because of the lack of government oversight. The value of bitcoins skyrocketed in the past because wealthy criminals were purchasing bitcoins in large volumes. Because there is no regulation, however, you can lose out immensely as a miner or investor.

Bitcoins completely bypass banks. Bitcoins are transferred through a peer-to-peer network between individuals, with no middleman bank to take a slice.

Bitcoin wallets cannot be seized or frozen or audited by banks and law enforcement. Bitcoin wallets cannot have spending and withdrawal limits imposed on them. Nobody but the owner of the bitcoin wallet decides how their wealth will be managed.

Bitcoin transactions are irreversible. Conventional payment methods — like a credit card charge, bank draft, personal check or wire transfer — benefits from being insured and reversible by the banks involved. In the case of bitcoins, every time bitcoins change hands and change wallets, the result is final. Simultaneously, there is no insurance protection of your bitcoin wallet: If you lose your wallet's hard drive data or even your wallet password, your wallet's contents are gone forever.

**Bitcoin Explained:** https://www.youtube.com/watch?v=kubGCSj5y3k

**BLOCKCHAIN TECHNOLOGY**

Blockchain is a technology that allows for fast, secure and transparent peer-to-peer transfer of digital goods including money and intellectual property. In cryptocoin mining and investing, it's an important topic to understand.

### What Blockchain Is: A Brief Primer

One of the most talked about yet misunderstood topics in recent times, blockchain is completely overhauling the way digital transactions are conducted and could eventually change the way several industries conduct their daily business.

Two words that have rapidly become part of the mainstream vernacular are bitcoin and blockchain, which are often used interchangeably even though they shouldn't be. While they are related in a sense, these terms refer to two very different things.

Bitcoin is a form of virtual currency, more commonly known as cryptocurrency, which is decentralized and allows users to exchange money without the need for a third-party. All bitcoin transactions are logged and made available in a public ledger, helping ensure their authenticity and preventing fraud. The underlying technology that facilitates these transactions and eliminates the need for an intermediary is the blockchain.

**Important:** One of blockchain's main benefits lies in its transparency, as the aforementioned ledger functions as a living, breathing chronicle of all peer-to-peer transactions that occur.

Each time a transaction takes place, such as one party sending bitcoin directly to another, the details of that deal – including its source, destination and date/timestamp – are added to what is referred to as a block.

This block contains the transaction in this example along with other similar types of transactions that have been recently submitted, usually within the past ten minutes or so when you're dealing with bitcoin in particular. Intervals may vary depending on the specific blockchain and its configuration.

**Important:**The validity of the transactions within the cryptographically-protected block is then checked and confirmed by the collective computing power of miners within the network in question.

On an individual basis, these miners are computers which are configured to utilize their GPU and/or CPU cycles to solve complex mathematical problems, passing the block's data through a hashing algorithm until a solution is found. Once solved, the block and all of its respective transactions have been verified as legitimate. Rewards (Bitcoin, in this example, but it could be Litecoin or some other currency) are then divvied up among the computer or computers that contributed to the successful hash.

**Tip:**Now that the transactions within a block are deemed valid it is attached to the most recently verified block in the chain, creating a sequential ledger which is viewable by all who desire.

This process continues in perpetuity, expanding upon the blockchain's contents and providing a public record that can be trusted. In addition to being constantly updated, the chain and all of its blocks are distributed across the network to a large number of machines.

This ensures that the latest version of this decentralized ledger exists virtually everywhere, making it almost impossible to forge.

### Why Blockchain is Needed

Peer-to-peer connectivity over the internet has existed for quite some time in a number of different formats, allowing for the distribution of digital assets directly from one person or business to another.

Since we can already send these bits and bytes to each other, what's the point of using a blockchain?

The behavior of the Bitcoin blockchain is the perfect example to answer this question. Pretend for a moment that there was no blockchain in place and that you had one bitcoin token in your possession with its own unique identifier assigned to it.

Now, let's say you wanted to buy a new television from a business that accepts cryptocurrency, and that shiny new TV happens to cost one bitcoin. Unfortunately, you also need to pay back your friend for the bitcoin which you borrowed from him last month.

In theory, without the blockchain in place, what's to stop you from transferring that same digital token to both your buddy and to the electronics store?

This dishonest practice is called double-spending, and it's one of the main reasons why peer-to-peer digital transactions have never really caught on until now. With blockchain, which not only distributes a public record of all transactions but confirms a block before each of its individual transactions can be finalized, the possibility of this fraudulent activity is essentially wiped out.

While in the past we had no choice but to rely on intermediaries such as banks and payment processors to validate these transactions and make sure that everything was on the up and up, for a nominal fee of course, blockchain technology lets us truly transfer our digital assets from point A to point B taking comfort in the fact that there are reliable checks and balances in place.

### Exploring the Blockchain

As we've already discussed, the ability for anyone to view a public blockchain such as the one associated with virtual currencies like Bitcoin is a key factor in why it works as well as it does. The easiest way to peruse this distributed database is through a block explorer, typically hosted on a free-to-use website such as Blockchain.info.

Most blockchain explorers are heavily indexed and easily searchable, allowing you to locate transactions in a number of different ways including by IP address, block hash or other relevant data points.

### Other Uses for Blockchain

Blockchain has come to the forefront of many discussions because of its role in the distribution of cryptocurrencies like Bitcoin. In the long run, however, these digital cash transactions may end up being a very small part of blockchain technology's overall footprint on the world as a whole and the way we transfer assets online.

The possibilities for blockchain implementation seem endless, as its underlying technology can be leveraged in virtually any field to perform a number of important tasks such as the following.

* Executing contracts
* Safely buying and selling intellectual property
* Distributing important medical information
* Ensuring that voting in elections is incorruptible

We, as a world society, have just begun to scratch the surface here. New potential uses for blockchain are being discovered on a regular basis.

Private blockchains will allow companies to revolutionize their own internal processes while public, open-source variations will continue to change the way we handle business in our daily lives.