Bitcoin is a digital currency known as a crypto currency. It is unlike any money that you may have used before. You can send it to anyone on the network with relatively little fees and virtually no hindrance. It is controlled by yourself in a digital wallet on your PC.

What made Bitcoin truly unique was its decentralised nature. Bitcoin is not controlled or overseen by any one body. It is completely distributed across a network of computers in a peer to peer fashion. Transactions can take place with anonymity between participants. There are no bank accounts linked to an individual's name. This was indeed one of the guiding principles of the creator, Satoshi Nakamoto.

Bitcoin has already revolutionised the way that people think about money and assets. What was once a nascent idea looked at as much of a hobby has transformed the global financial system. There are many people who say that Bitcoin will do to finance what the internet did to the information system.

It may, however, seem relatively complicated to those who are new to the concept. We delve into the underlying principles of Bitcoin in the following post.

# Crypto Currency and Digital Assets

Although Bitcoin is called a "digital" currency, this may be slightly confusing to some people. This is because it is not really an asset in the traditional sense. It is not even a digital asset or file on your computer. It is actually a record of a transaction that shows that someone has sent you something of value previously.

This thing of value is Bitcoin. Bitcoin is a crypto currency that was "mined" by a computer. In essence, this computer devoted resources (electricity and processing power) to solve a complicated cryptographic problem. Similar to classical economic theory, this work by the miner was the labour and capital that was put into the resource (Bitcoin).

This Bitcoin, although not a tangible asset, has value and can therefore be used as a currency. You can send it to anyone across the world just like FIAT money. This is sent to someone else by the way of a transaction from your wallet and public address to the recipients address. This transaction is then confirmed by the miners and place onto the Bitcoin blockchain.

# The Bitcoin Blockchain

The Bitcoin blockchain is a decentralised ledger that contains all of the transactions on the Bitcoin network since the beginning of time. Think of it as a large accounting book with numerous debits and credits. Every single transaction on the Bitcoin network can be traced on the blockchain.

This blockchain is decentralised which means that it is not stored in one particular location. True to the nature of Bitcoin, the blockchain is maintained by all of the network nodes (computers) on the Bitcoin ecosystem. This means that the blockchain is public. Anyone can view transactions that took place on the network. You can view the latest bitcoin the ledger at blockchain.info.
This decentralised ledger is called a “chain” because all of the blocks are linked to the blocks before. Using advanced cryptographic principles, each block will contain data about the prior blocks. This allows these transactions to be immutable, a concept which eliminates the possibility of double spend. We will go over this in more detail below.

# Bitcoin Public Addresses


As mentioned above, Bitcoin is anonymous. There are no Bitcoin accounts where you keep your money. No one can see the identity of the individual who is sending or receiving money. One is able to send Bitcoin to someone else on the network by using their public Bitcoin address. This a string of letters and numbers that is generated from the wallet. An example is this **1PzNiHPM9iVRd2fBpqcMv78m5pgQsag3pn**.

A wallet is merely a collection of files that provide access to a number of public addresses. This is unique to the wallet that you have and can be used continuously or discarded once a payment has been received. When this address is created, you are actually generating a “cryptographic key pair” which is composed of a private key and a public key. The private key is known to only you and the public key is known to the whole network (your unique public address).

When you send Bitcoin to someone else, the transaction needs to be cryptographically “signed” by your private key. The public key allows the network and the miners to verify that the message is indeed signed with the correct private key.

It is important to note that no one can forge your private key. This is because it is linked to your public key using a concept called asymmetric cryptography and hash functions. The exact explanation is beyond this initial introduction but all you need to understand is

that it is impossible to replicate the private key. Even a minute change to a factor in the private key will result in a completely different public key.

Similarly, the hash function that produces the public key from the private key is a one way function. This means that you can calculate the public from the private key but there is no way of calculating it the other way. There is one more stage of algorithmic hashing that occurs on your public key before it is created into a human readable bitcoin address. The hashing function that is used in Bitcoin is a SHA 256 algorithm. You can read more about cryptographic hash functions in depth if it interests you.

# Bitcoin Security

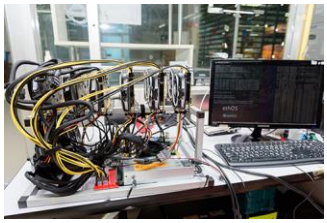
One of the many concerns that Bitcoin new adopters have is how secure the blockchain really is. What is to stop someone from double spending their Bitcoins? What is to stop a hacker from changing a transaction in the blockchain and assigning themselves more money?

Of course, security and trust go hand in hand. You cannot have a decentralised currency without all of the participants having 100% confidence in the network. Theoretically, unless 51% of the network is controlled by one party the blockchain is completely tamper proof. This “rule of 51” is central to the Bitcoin protocol and was addresses in the original whitepaperby Satoshi.
In essence, if ever there is a disagreement of the structure of the blockchain, the network will override and choose the chain that is being presented by the majority of the miners on the network.

With regards to a hacker being able to change a prior transaction and assign more Bitcoin to themselves, this is impossible due to the immutability of the blockchain. All blocks with transactions in them are linked to the blocks prior to them. This link is also through a similar hashing function as described for the private and public key.

Even a minute change to a transaction in a prior block on the chain would result in a completely different blockchain than the established one. Hence, the miners would notice that this is an incorrect blockchain immediately and then revert to the one that the majority of them agree on.

# Bitcoin Mining



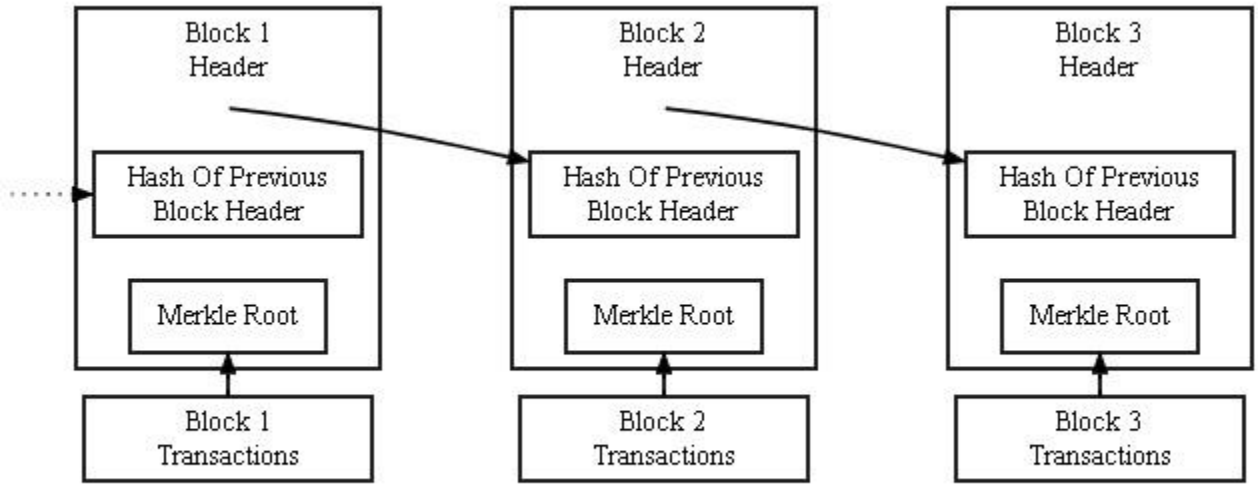
Bitcoin is a digital gold. People view it as a safe haven asset that is limited in supply and hence will always be in demand. Like gold, Bitcoin has to be mined in order to be created. However, this mining is done by computers who solve complicated mathematical problems using brute force computing. Once a

miner has solved this problem, it is rewarded in Bitcoin. This is where new Bitcoin enters the supply.

It is also important to note that there is an upper limit to the amount of Bitcoin that can ever be created. This is capped at 21m BTC. Hence, Bitcoin is naturally deflationary. The network can also regulate the amount of Bitcoin being mined by adjusting the computational difficulty of the problems. As it gets more difficult, it becomes more expensive to solve the problems and hence mine the Bitcoin.

This is why it is quite comparable to mining for a natural resource. For example, when first mining gold it is at the surface and easy to pull up. As more gold is mined they have to dig deeper which will cost more money. Eventually gold supplied to the market will begin to slow down. There is only a certain amount of finite gold on planet earth that can ever be mined.

# What is Inside the Block?




Source: bitcoin.org

Simplified Bitcoin Block Chain

We have been mentioning the blocks in the blockchain without going through an explanation of exactly what the blocks are comprised of. Bitcoin blocks hold a all of the transaction information for a particular time period. They also hold other data such as a timestamp (identifying when it was picked up) and crucially, a hash of the block before. Each block has a block size limit of 1MB.

Given that the current block has a hash of the block before, it is inextricably linked to that block. Hence, there can be no changes to the blocks prior without changing the structure of the hash function. You may also be wondering how the block is able to contain information of all prior blocks and remain within the size limits. This is through a cryptographic discipline called Merkle trees. This is beyond the scope of this post but it

is able to effectively hash together all transactions and efficiently store it under the limits.

When a Bitcoin miner is able to clear a block then they will not only get the payment in Bitcoin for solving the problem but they will also get the transactions fees for all of the transactions. It is important to note that these are Bitoin which are already in circulation and hence won't impact on Bitcoin supply. In terms of the 1MB limit there is currently a proposal to increase the block size limit in November to 4MB. This was all as a result of the SegWit2 scaling implementation.

# Costs of using Bitcoin

Whenever you want to send funds on the Bitcoin network you are required to pay a certain fee in order to incentivise the miner to confirm these transactions. However, unlike with using traditional banking systems and online payment processing, this fee is quite inconsequential. Even with the recently added cost of using the Bitcoin network, these fees are markedly lower.

When it comes to sending money online with an online merchant such as PayPal, your fees are usually about 2-3% of the transaction amount. With Bitcoin, when you send coins you are usually charged about 0.1mBTC (1 thousandth of a Bitcoin) per 1,000 bytes. If one was to consider the average Bitcoin transaction size and number of transactions then one is able to get an idea of the total percentage of all volume is paid in fees. Currently, Bitcoin fees for using network are about 0.760% which is much lower than PayPal.

Then there is of course the question of international payments abroad. If anyone has had to make a SWIFT payment they will know how long it could take as well as how much it costs. There are usually a range of intermediary banks that have to be involved who can facilitate the transactions. Payments can take anywhere from 3-4 business days. In comparison, on the Bitcoin network average confirmation times are currently about 25 minutes.

# What Does the Future Hold

The way in which a decentralised self-governing global currency can change the way we think about the world is truly fascinating. There will be no banks which will charge exorbitant fees. There will be no central government banks which can devalue someone's money with inflation and quantitative easing.

However, when it comes to disruption, it is the underlying block chain technology that has the true potential to really change the world. There are already a number of

companies that are attempting to use a decentralised ledger to manage supply chains, raise funds through crowd funding, improve security, the list goes on.

There have also been a number of other crypto currencies that have been developed that have greatly improved upon the Bitcoin protocol and include could be focused on privacy like Monero or smart contract technology like Ethereum.

Disclaimer: These are the writer's opinions and should not be considered investment advice. Readers should do their own research.