Blockchain Council™

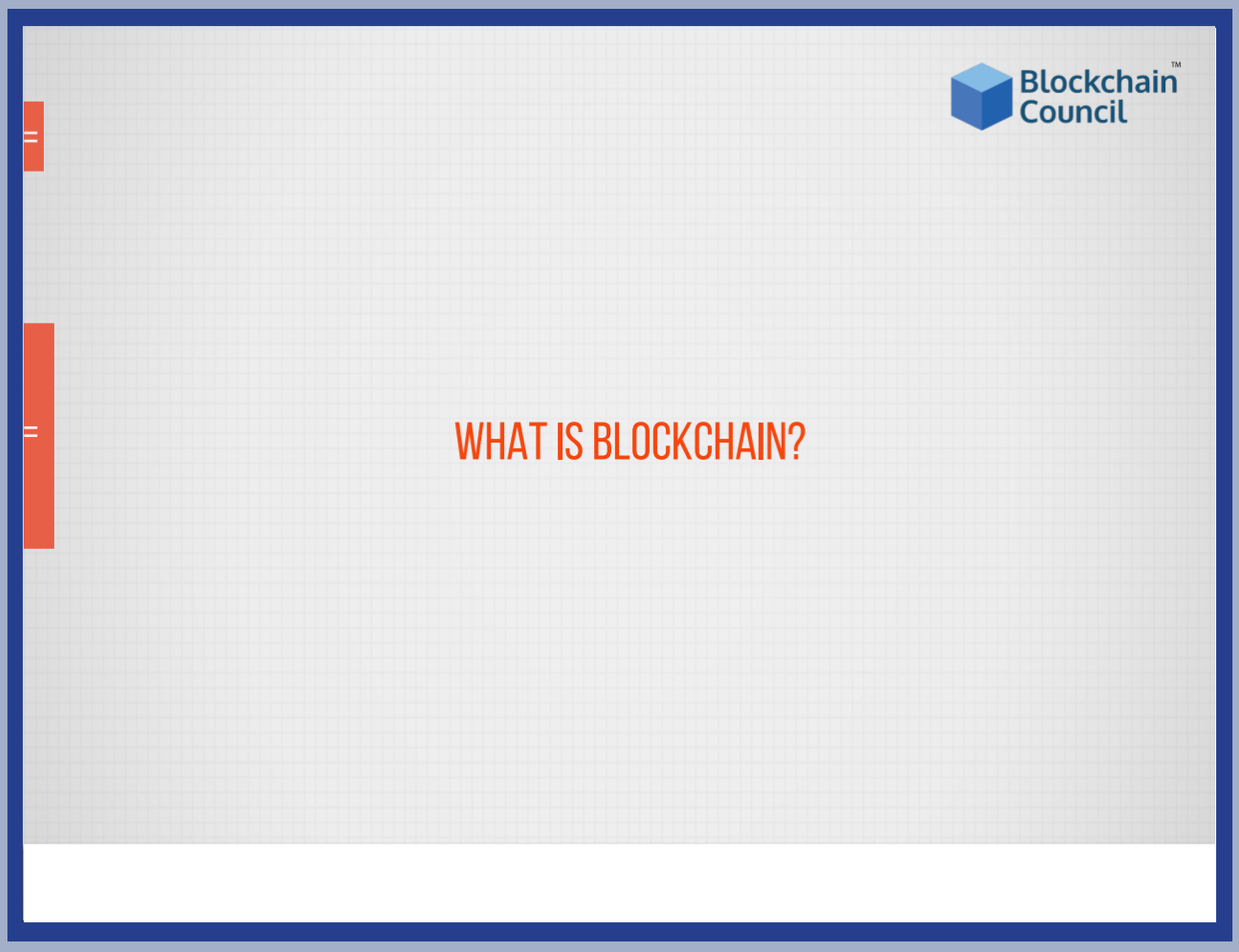
www.blockchain-council.org

CERTIFIED BITCOIN EXPERT™

TOSHENDRA SHARMA

CHAPTER 1

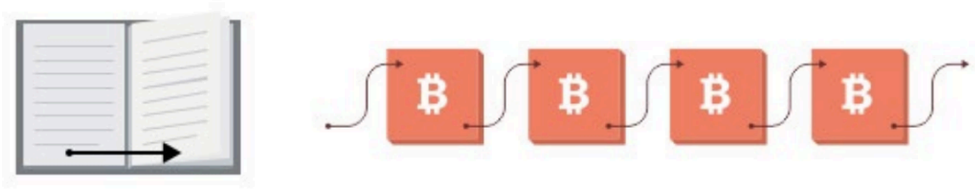
What is Blockchain



WHAT IS BLOCKCHAIN

Blockchain Council™

- A decentralized ledger tracking digital assets on P2P network
- Any real life example?
  - Records of your sales & purchases of raw material
  - Or may be simply your bank account statement
  - An excel sheet tracking all hospital equipments
  - Simply a large size book



Blocks in a chain refer to previous blocks, like page numbers in a book.

Ref: bitsonblocks.net

You might have heard about the Blockchain and the cryptocurrencies or some distributed ledger technology and decentralized technology solution, which is solving people's problem and making money transaction across the borders very swift.

Yes! Blockchain is related to cryptocurrency, but it is not cryptocurrency.

Blockchain is a technology which has the concept of P2P or a distributed ledger shared on a P2P network.

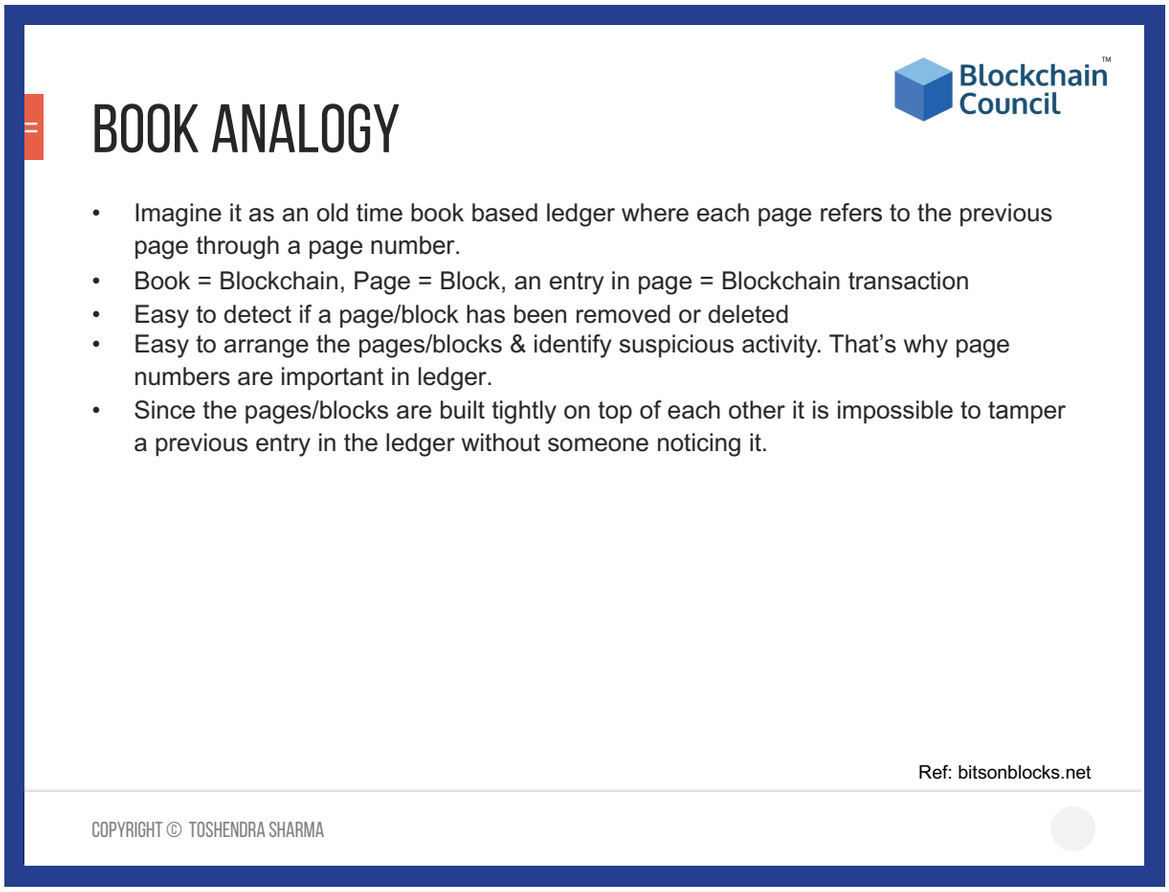
As the name suggests Blockchain is a chain of blocks stored on hundreds or thousands of computers all across the globe or distributed over a geographical location. It is a full ledger which keeps the copy of all the credit and debit of a digital asset. That digital asset can be a representation of a pen, a chair, a virtual number, money or coin etc., so whatever can be represented as a number can also be a considered as a digital asset.

Blockchain is a decentralized ledger tracking of one or more digital assets on a peer-to-peer network. When we say peer-to-peer network, it means a peer-to- peer decentralized network where all the computers are connected in some way and each will have the complete copy of the ledger.

The ledger can also be seen as a bank account statement since day zero. Let's say if you open an account on 1st Jan 2017 then the ledger or the full ledger will keep track of every balance in and out of your account since day zero. So, if you generate a balance statement since day zero that will be called a complete ledger.

Just imagine that full ledger or bank account statement is copied to thousands of machines at the same time in such a way that each machine can verify the individual transaction without involving other machines and announce whether it's a valid transaction or not.

So, now the question is how the block and the chain come into picture and how they are related and connected.



In a typical ledger or a book case, each page contains the lines so you can imagine a book as a Blockchain where pages are nothing but blocks and each page is connected to every other page through a page number. In a book, all pages are in a particular order that's why if someone tampers with a specific page or removes any page, it is easy to identify since the pages are arranged in a particular order.

Now, imagine the book as a Blockchain where each page is connected to another as a block and the lines inside the page as a transaction. And, you have understood the Blockchain already!!

Blockchain is a ledger which stores the credit and debit of every single record in such a way that it cannot be tampered by anyone without getting noticed because each block and page is connected to another.

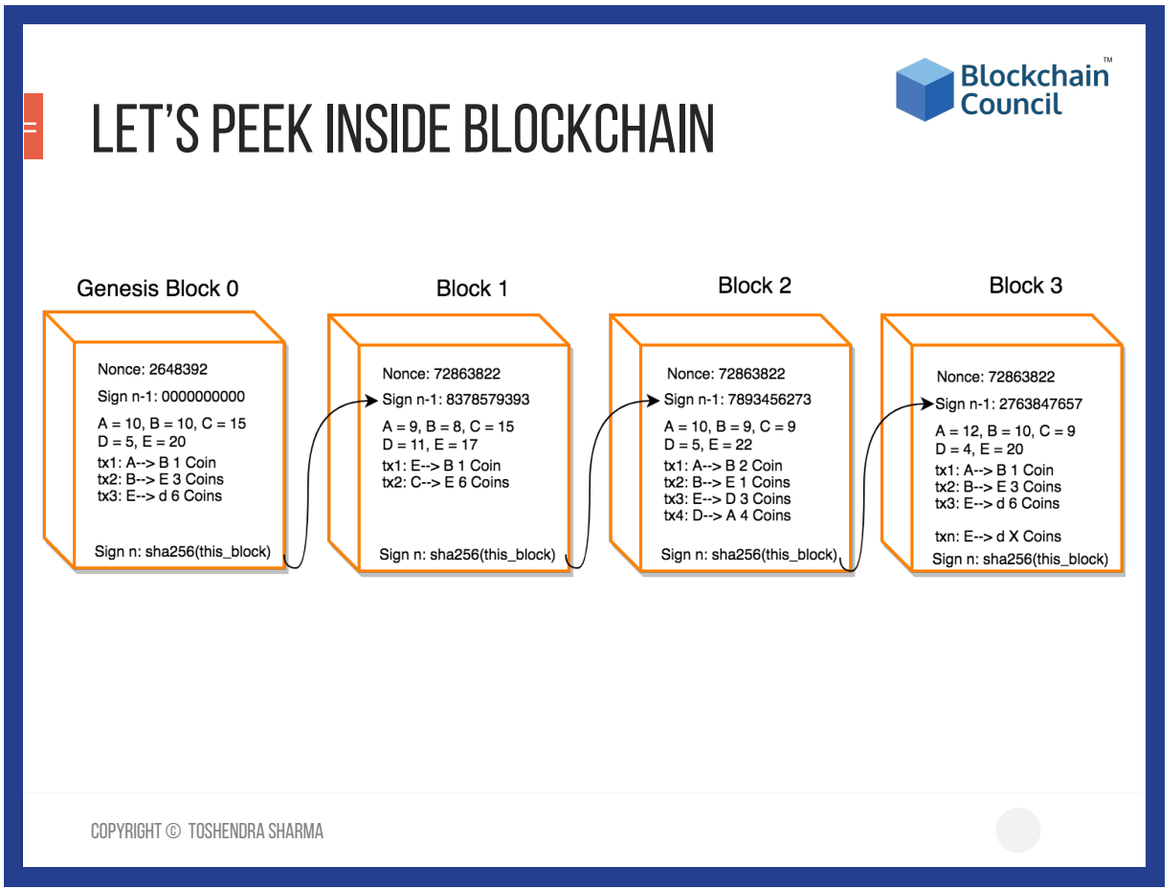
The book analogy given above can be referred where, the book equals to the Blockchain; the page is equal to the block and entry in the page (i.e. a credit or a debit entry) is called a Blockchain transaction. This is how you can connect.

As you have understood that it's easy to detect if a page has been removed or deleted and it is also easy to arrange the pages or the blocks and then identify any suspicious activity. That's why the page numbers are significant in a legal agreement or an MOU because it helps the readers to understand if there is a page missing. It is obvious that changing or removing a page can change the meaning of the whole agreement and that holds true for the ledger as well. Deletion of a page in the ledger can corrupt the entire ledger very easily. Thus it's simple. Let's say you have an account statement that has 100 pages and someone removes the page number 65, then it can be easily identified because the record will not tally itself and corruption can be detected immediately.

Now the question arises that how is it helpful and what's the need to create a cryptocurrency? Cryptocurrency is nothing but a digital token defined as a number in the Blockchain which is tracked since day zero.

So in case of bitcoin, it is just a number which is stored in a Blockchain ledger and is tracked since day zero. The digital number is required because there can be only one copy of it which reflects the fundamental nature of the currency. If I have 100 bitcoins and you have 0 and I transfer 50 bitcoins to you, then I can never have 100 again because the ledger will update. 50 from my balance will be removed and added to your balance, so this will create a single copy maintained securely.

Since everybody needs bitcoin, it has gained a value otherwise it is just a number stored in the Blockchain.



This is how a block looks like! The genesis block is called the day zero block or the block zero. This block contains starting balance, which can even be zero.

So let's say if the Blockchain is not minting new tokens or new balance every single block then the genesis block must have some initial balance otherwise there will be no way to introduce the new balance. As you notice in the genesis block, there is something called nonce which is nothing but a small string based number. Along with nonce there is 'sign n-1' means the signature of the previous block since this is a genesis block we are keeping the signature of 'n-1' to zero.

Let's take an example where A has ten tokens or let's call it Bitcoin if you want to understand it otherwise, it's just a token or only a number.

So, A's balance is 10, B's balance is 10, C's balance is 15, D's is 5 and E's is 20. In this block, there are three transactions that are initiated where A transfers one coin to B, B transfers three coins to E and E transfers six coins to D. As these transactions take place, the new block must reflect the balance according to these transactions. So, when the new block is added into the Blockchain you might notice that there is a 'sign n' which is the signature of this whole current block. You will notice this signature of the block number 0 or 'sign n' is being generated by the digest of the full block. This is just a signature of the full block, which is being calculated by sha256 of the current Block. Here sha256 called simple hash algorithm 256 which is a crunch of any length of data into a fixed length of a unique string. This way if any single digit or letter has been tampered in this block, the signature will completely change and it is not possible to reverse the digest or signature to the original input data or original data.

This is always one-way crunching. Thus the sha256 has crunched the entire block into a fixed length unique string and we call it the signature of the block.

Next, if a new block gets added, the signature of the previous block will go to the 'sign n-1' into the new block as a header and the nonce will be created. This nonce will be created by the miner (a person, computer, the server; or the process) who is adding the block. The miner will guess this number and will update the balance of all the addresses.

Since A had transferred 1 coin to B, so A equals 9, B had transferred 3 but it had also received 1, so it has 8 coins now. Similarly with C, D and E and there are only two new transactions. So, now the transactions will affect the balance of the input and will create the output which will go in the ledger. Here the 'sign n-1' is the signature of the previous block which goes in the ledger and the signature of the whole new block is created through this process which goes back to the next block as a header. Here the nonce is the number which is being generated by the miners. These numbers or the nonce are generated in a particular way, through the mining algorithms. Mostly, it depends on Blockchain to Blockchain, but in general, the nonce should be generated in such a way that this new digest or the new signature of the block should be less than the previous block.

TELL ME EVEN MORE

- In case of real Blockchain, each block is built on top of the recent block and use its previous block's content/signature + nonce (random string).
- Building a block & adding it in the Blockchain is the task of the miner nodes (optional).
- In public Blockchain it is made computationally difficult to add a block to prevent attacks.
- Miners try to guess a number (nonce) in such a way that if it gets crunched with the most recent block's fingerprint then it will create a new fingerprint which will be less than the last/most recent block in the Blockchain.
- It takes time & computational power to add a Block in the Blockchain. Hence there is a reward (12.5 BTC in case of Bitcoin Blockchain, 5 ETH in Ethereum)
- Private Blockchain can chose other methods to add a block as they can trust the miners using a contract etc.

Building a block & adding it into the Blockchain is the task of the miner by guessing the nonce in such a way that the new Block's signature is in particular order. So, technically the miner has to try a millions or trillions of times before coming to this right number. That's why it is called a proof of work. Calculating a nonce in a digest, a million or trillion times is not very easy because the computation takes tremendous efforts, power, and energy. This will generate the proof that this particular block is added after some real work. And since miner put in a lot of work, he will be rewarded by some coins, which are called rewards. Every miner gets a reward to do this. As the newly minted coins have the value, the miners are happy and the entire Blockchain is happy because the new block has been added and is saved.

This way the blocks can go upto 100 thousand, 200 thousand and even to millions, which depends on the algorithm and the technology that how frequently the blocks are being added. The average time of adding a new block in Bitcoin Blockchain is 10 minutes whereas in Ethereum Blockchain it is 15 seconds. So this all depends on Blockchain to Blockchain that how frequently the blocks are being added.

Since there will be 100 thousand or 200 thousand blocks, changing any block will be very difficult for a hacker because if he does changes any of the data; let's say if he decides to change the Block number fifty thousand because he just felt it is very beneficial for him to add balance to his account on that Block. This will tamper the Blockchain and make it smaller but since the whole network is following the longest chain, his corrupted block will be rejected. So, people will reject his modification and continue. If he has replicated all the blocks which are next to fifty thousand's block to ensure his part of the chain is longer, then

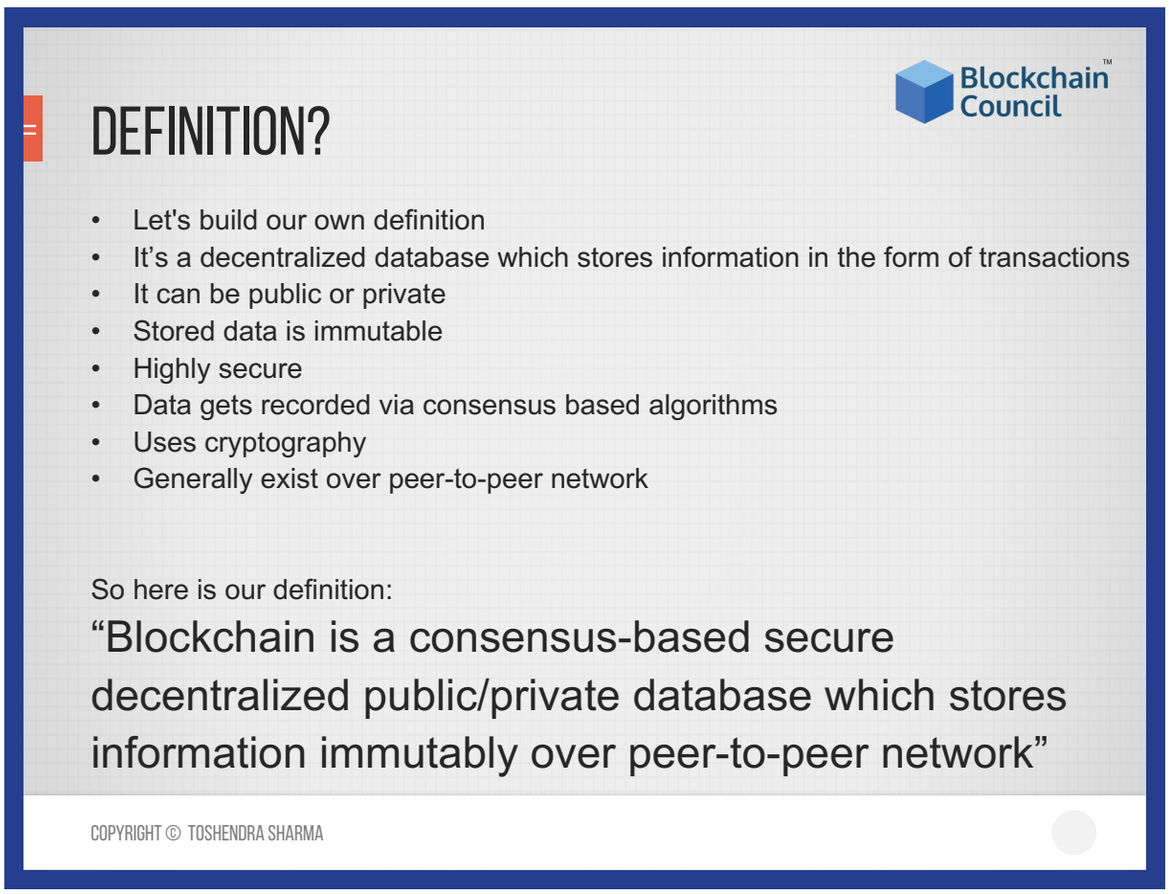
it will be very computationally expensive & time-consuming. That's how the Blockchain is made secure.

As each block is built on the top of the most recent block, so it is very difficult to tamper without affecting all the upcoming blocks. This makes it very safe and secure because even if someone tampers any previous block by a single small bit and because they are all connected to the digest, it is not possible to tamper without someone noticing it. That's a very challenging task.

In case of the public Blockchain, it is intentionally made computationally difficult to add a block, so that a miner has to compete with others to make sure that they get the reward into their wallet to secure the Blockchain. The more complexed the algorithm to add a block would be, the more secure the Blockchain would be, that's called proof of work. They have to prove that they have done some work to add a new block otherwise, if adding a block had been easy then any hacker would have come and replicated the entire Blockchain. He might claim that his Blockchain is valid which is technically not possible if the proof of work is involved.

There is another option, which is 'proof of stake', where the miners have the reputation in terms of number of coins owned or their brand or their recognition in the market. Based on this reputation they are allowed to add a block, which is called 'proof of stake'.

The private Blockchain can choose any method to add a block. They can even trust a miner using some legal agreements and contracts. This is also very interesting to choose the limited miners, so it can be called a 'proof of stake'.



Let's create our definition.

We will not follow any 'xyz' definition which you will never remember. Since we have understood the logic, let's look at the analytical features of the process:

It's a decentralized database that stores information in the form of transactions. It can be public or private. It stores data in an immutable way, i.e. it is tough to tamper and very easy to detect. This is called immutability in the Blockchain. It doesn't mean that data can never be tampered by anyone, it is easy, but it will only affect his local copy and if you are not able to change the entire Blockchain or the entire network, then it is useless. Because of that, it is highly secured. Data is recorded via consensus-based algorithms. Since the consensus is required before adding a new block or adding new transactions, this helps secure the entire Blockchain without involving any trusted third party or a regulator. It uses cryptography, and it exists over a peer-to-peer network.

Hence we can sum it up as:

"Blockchain is a consensus-based secured decentralized public/private database which stores information immutably over peer-to-peer network"

So that's a simple and easy to remember definition!!

SUMMARY

Blockchain Council™

- It is a decentralized distributed ledger (data structure) where data is being stored inside blocks in form of transactions.
- Removes the dependency on the trusted third party for recording the data in Blocks.
- In public Blockchain more complex algorithms required to avoid malicious activities.
- Since each block is built on top of previous block immutability has been achieved.
- Here immutability means, very difficult to fake/alter a block and very easy to detect the alteration.
- This all exist in the memory of the computers and runs as a process.
- Every participant of the Blockchain contains almost same copy of the Blockchain.

Let's summarize, what is a Blockchain?.

It is a decentralized distributed ledger, a data structure where data is being stored inside the blocks in the form of transactions. It removes the dependency on the trusted third party for recording the data. Since people are competing with each other to add a new block or

to achieve the reward, they do it securely. It is very difficult and almost impossible to affect everyone in the world at the same time, that's why it's extremely safe.

In public Blockchains, more complexed algorithms are required to avoid malicious activities.

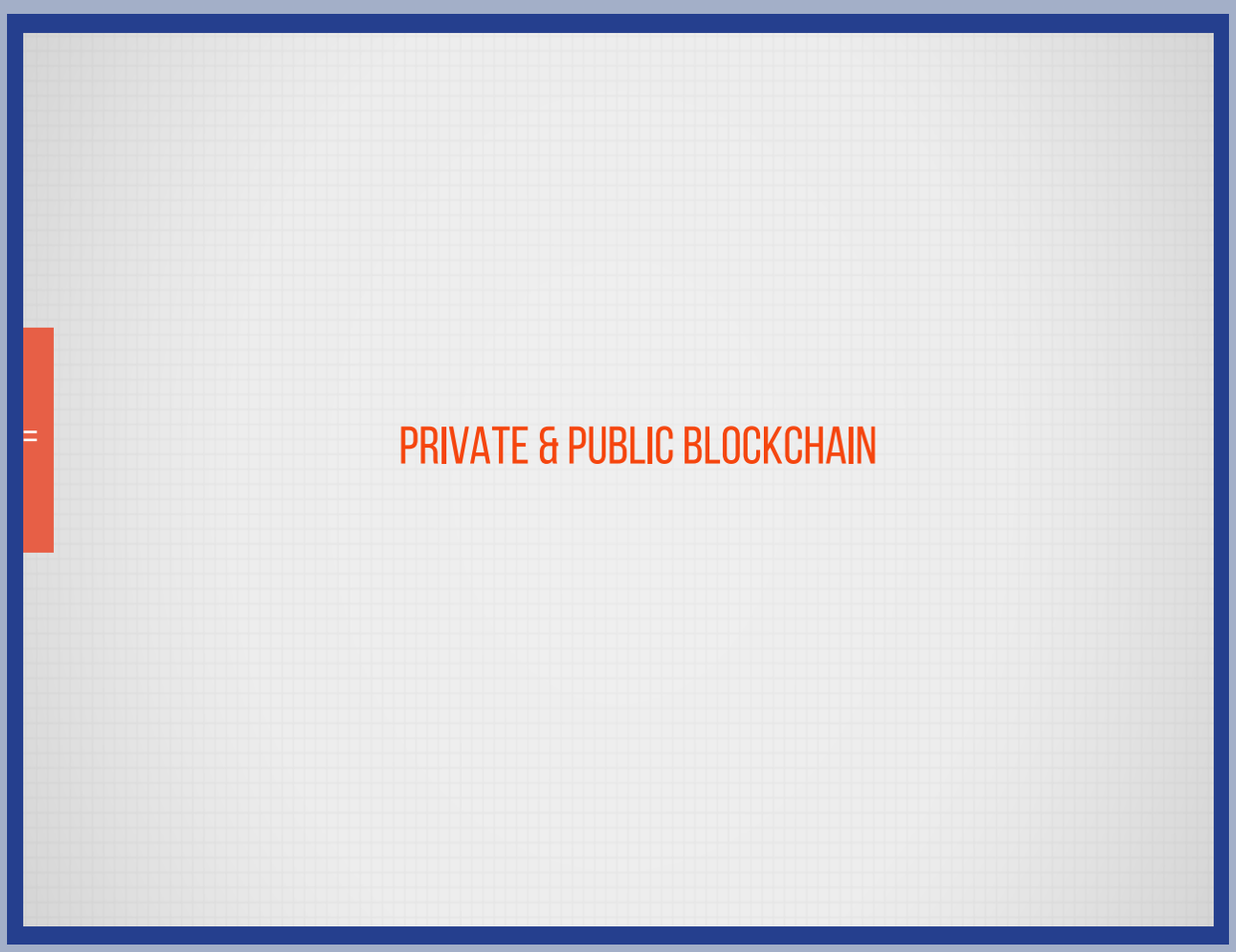
Since each block is built on top of the previous block, the immutability has been achieved.

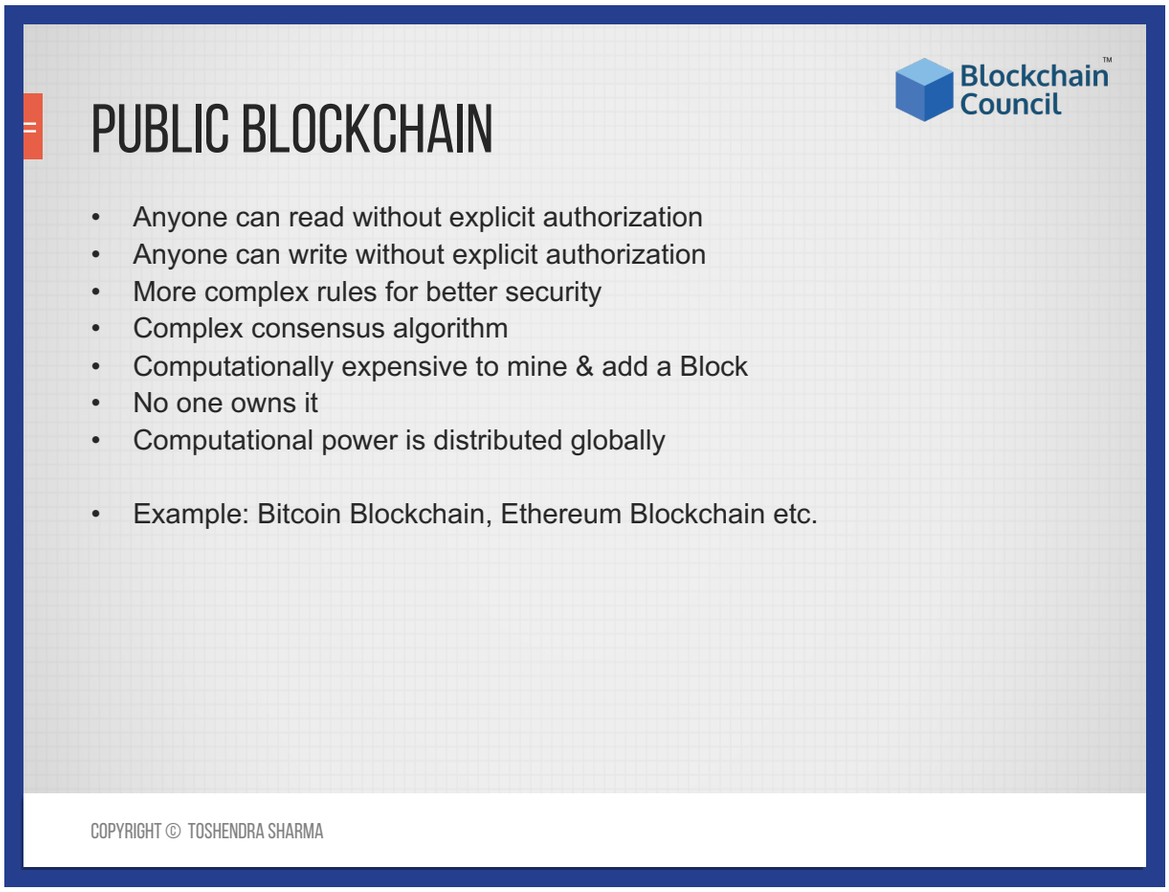
Immutability here means very difficult to fake/alter a block and very easy to detect the tampering.

Every participant of the Blockchain contains almost the same copy of the Blockchain ledger, only the last few blocks might be different based on the geographical location and the communication protocol, but the ultimate ledger is always the same.

CHAPTER 2

Private and Public Blockchain





With respect to access, the Blockchain can be of two types. A public blockchain or a private blockchain.

Let's first talk about a public blockchain.

A Blockchain is called a public blockchain, if the ledger information can be read or written without any explicit authorization or permission. It means that the ledger is fully open for anyone to read or write considering they are paying the transaction cost at their own level.

The type of information which can be written in the blockchain depends on the type of transactions. Any transaction can be initiated by anybody who has an account on that blockchain and all the transaction information can be read by anyone who has the transaction ID. So to read or write the information from the blockchain you don't need anyone's permission that is why it is called a public blockchain.

All the public blockchains require very complexed rules for the increased security. Since it is open for all, the hackers can always come in and flood the blockchain with any bogus information or fake transaction with the intension to turn it down. But since they have the more complex rules to understand the flooding or the DDoS attack, the public blockchain can protect itself automatically. As the blockchain is public, there is no central authority or trusted third party who can protect it easily.

Public Blockchain always requires the complex consensus algorithms to make sure that the whole network is agreeing on a certain transaction with the same decisions, it should not happen that there is no consensus made in the entire network due to some reason.

Due to security, public blockchains are made intentionally expensive to mine; expensive in terms of the energy, computation power and time. This is generally done to make sure that the Blockchain is safe and secure and has enough proof of work invested to create a new block into the Blockchain.

In the public Blockchain, all the nodes together owns it and there is no single owner who claim the ownership of the Blockchain. Though there can be a foundation or an organization which is working as a mediatory or a coordinating group for the entire community but that does not mean the organization owns the Blockchain.

For example, in case of Bitcoin there is a Bitcoin foundation, in case of Ethereum there is an Ethereum foundation who actually coordinates the overall development but they are technically not the owners of the Blockchain.

Also for the public Blockchain it is very important that the computational power is distributed globally without any major focus in any particular geographical location. In case the government sometime decides to shut down all the miners because of any reason or by the act of God, this should not affect the entire network. The idea is that everybody owns the chunk of it and it is distributed all across the globe. Shutting down everything at the same time means the end of the world. Which means we are already doomed and should not be worried about the Blockchain!!.

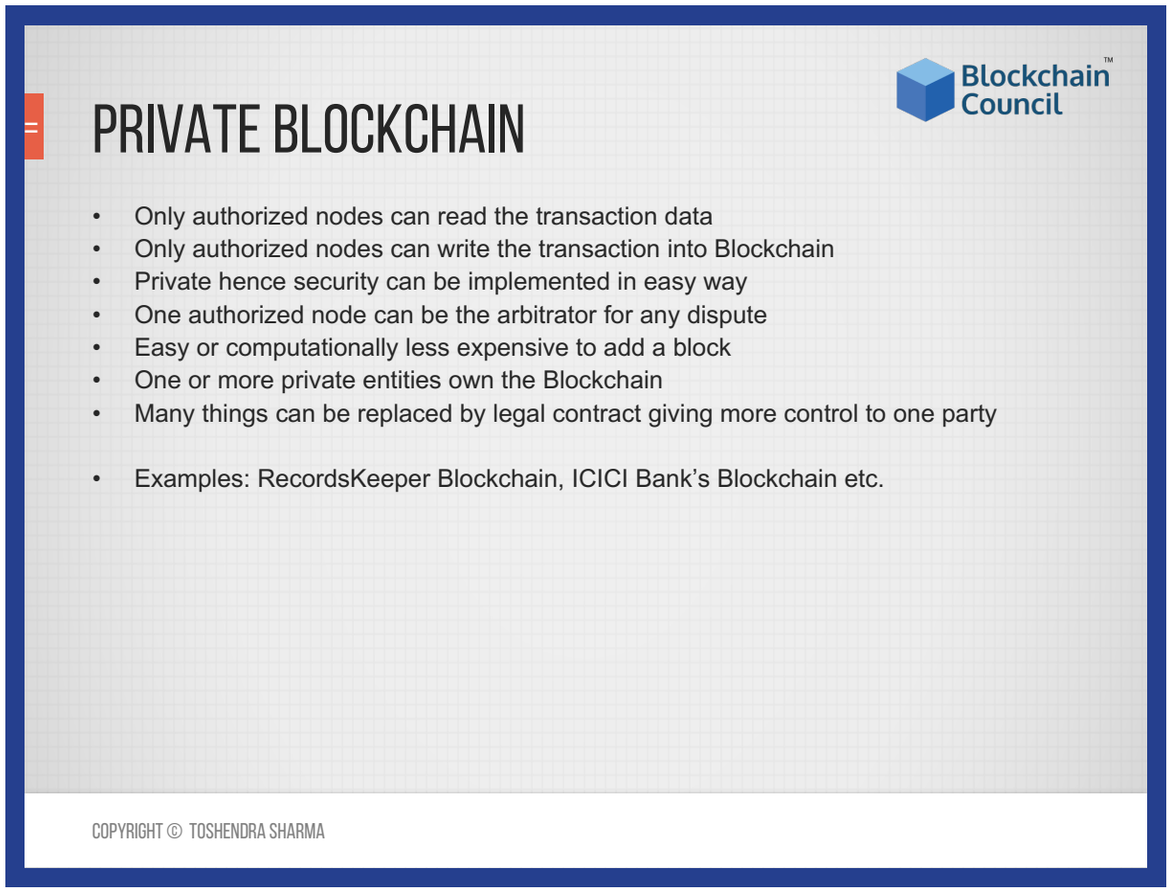
Let us see how a public Blockchain can be read.

For the bitcoin Blockchain you can go to blockchain.info and read the information from the block.

And for the Ethereum Blockchain, the most common explorer is etherscan. Go to etherscan.io and you will be able to read all the Ethereum Blockchain information freely.

You can check the particular block number, transaction or address. This way you can actually explore the entire Blockchain without any restriction or explicit permission requirements from the Blockchain owners because there are no owners.

There are bunch of other Blockchain explorers as well or you can also build your own Blockchain explorer and deploy it anytime.



Now Let's talk about Private Blockchain.

Private Blockchain are the Blockchain where you need explicit authorization from the nodes or admin to read or write the information.

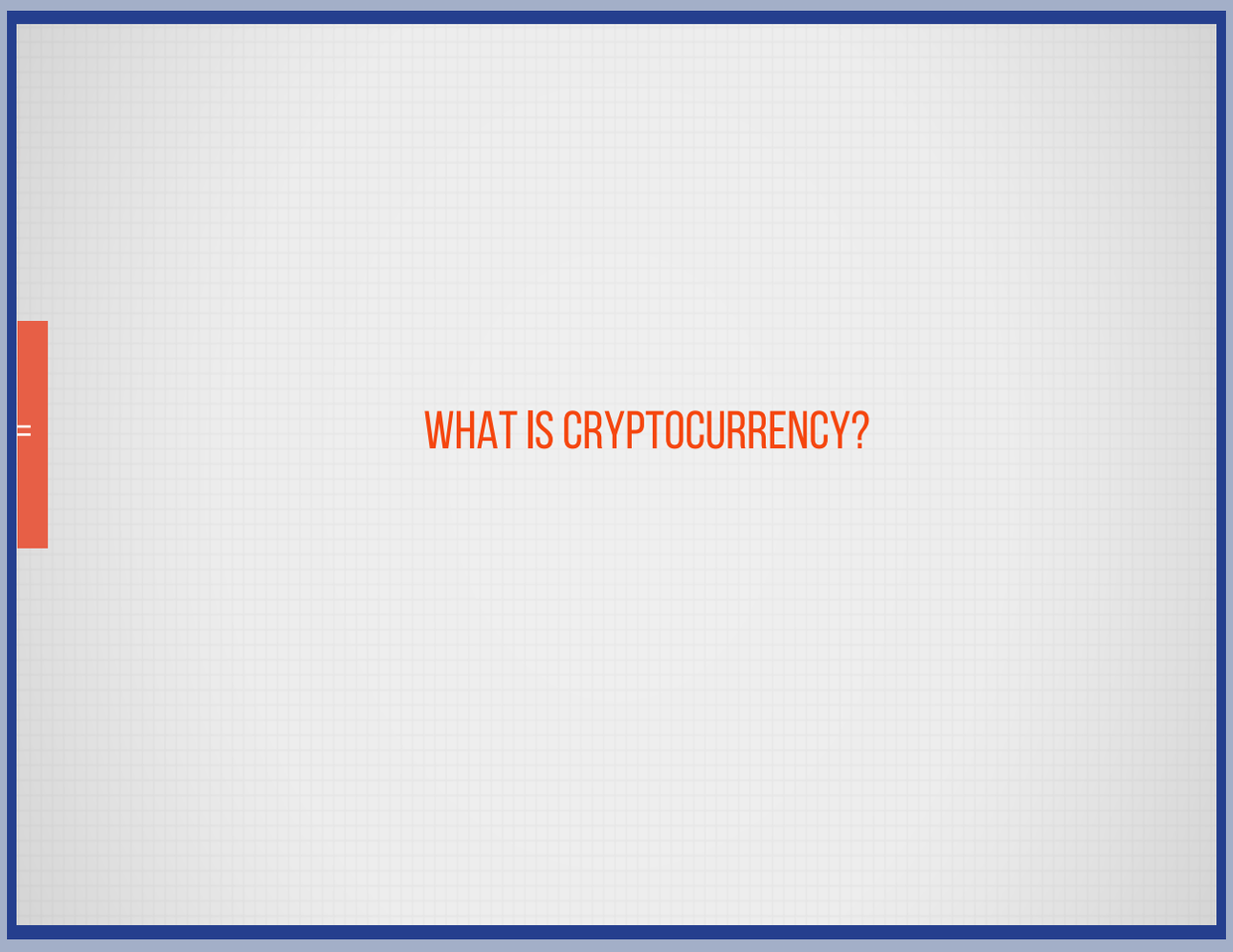
Since it is a private Blockchain it is implemented in a private way by making someone responsible for it. There can be a centralized authority or a trusted third party who is actually maintaining and making sure that the Blockchain is safe. The consensus can also be resolved using the arbitrator which means, we can make one node as the arbitrator to resolve the conflicts. So whenever there is no consensus, we can resolve the conflict through arbitrator node.

Since it is private someone has to own it, which means whoever owns the majority of the nodes will become the owner. This can be a corporate or a private individual, developer, individual authority and so on. There can even be a two nodes private Blockchain. You can make it work even when one node exists in the Blockchain.

In that single node Blockchain case the transaction creator will be the miner and transaction initiator at the same time.

CHAPTER 3

What is Cryptocurrency



WHAT IS CRYPTOCURRENCY?

Blockchain Council™

- A medium of exchange, created and stored electronically in the Blockchain
- An encrypted string of data or a hash, encoded to signify a unit of currency

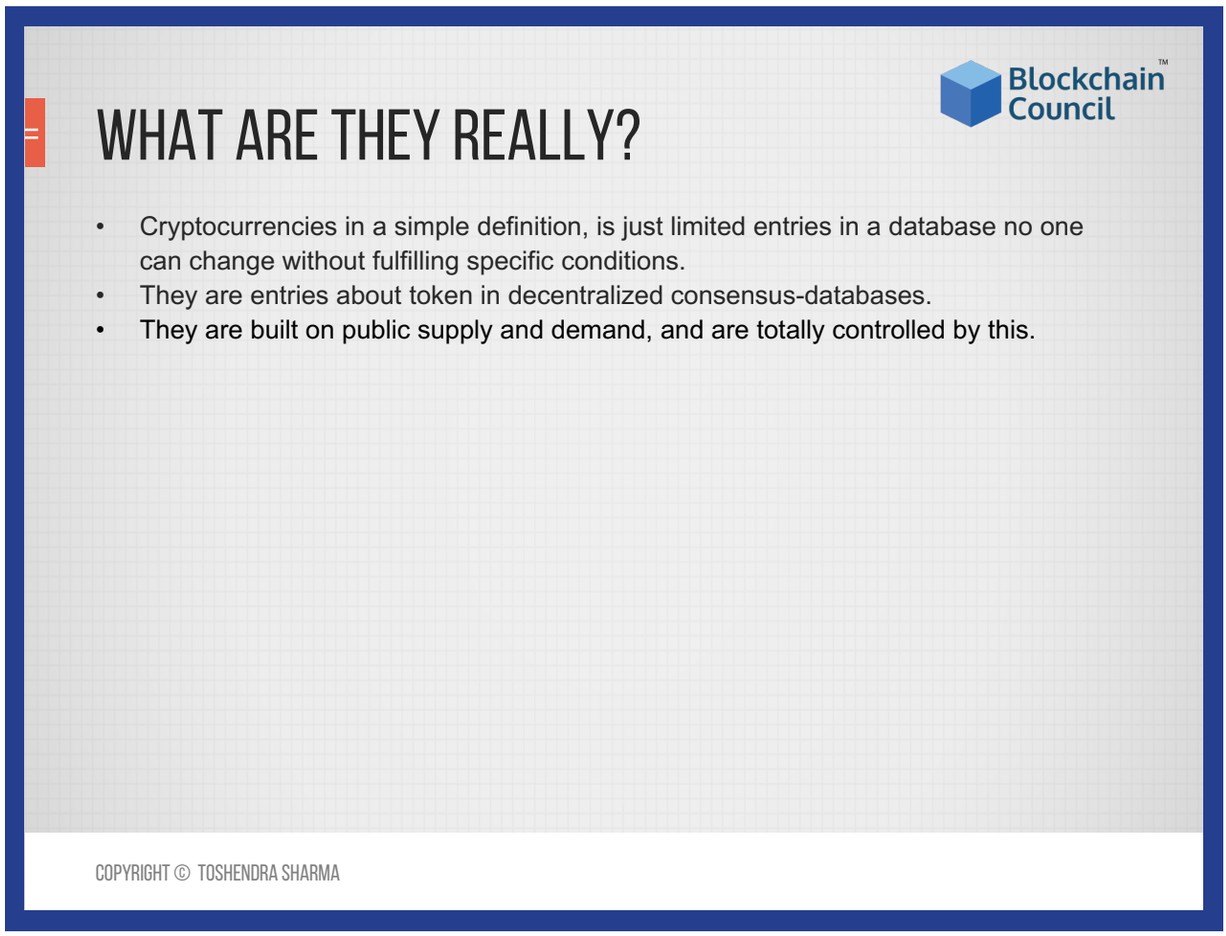
A Cryptocurrency is a medium of exchange of immutable or intangible objects which are created and stored in the Blockchain. It is a digital form of currency that is stored electronically on the Blockchain platform. The reason behind naming it a "Crypto-currency" is the fact that it is an encrypted string of data or a hash that's encoded in a token hence the word crypto. It also shows the characteristics of the currency by being immutable, non-replicable, holding the value and being transferrable in an atomic way. Hence the currency.

BIRTH OF CRYPTOCURRENCY

Blockchain Council™

- Satoshi Nakamoto, the anonymous person or a group of people, inventor of Bitcoin, the first and the most important cryptocurrency, never intended to invent a currency.
- In late 2008,Cryptocurrencies emerged as a side product of “A Peer-to-Peer Electronic Cash System”.
- His major innovation was to achieve consensus without a central authority.

The originator of cryptocurrency is believed to be a name called Satoshi Nakamoto though it is not confirmed whether he is a single person or a group of people. He anonymously invented the currency but had never intended to build one. In late 2008, Cryptocurrencies emerged as a side product of “peer-to-peer” cash system. The single most important part of Satoshi‘s invention was that he found a way to build a decentralized digital cash system in which he achieved consensus without a central authority.



So, now you must be thinking what really are cryptocurrencies?

If you take away all the noise around Cryptocurrencies and reduce it to a simple definition, they are just limited entries in a database which no one can change without fulfilling certain specific conditions. They are entries about a token in a decentralized consensus databases which is called a Blockchain. They are built on public supply and demand and are controlled by this, which is why high volatility comes into the picture.

BASICS OF CRYPTOCURRENCY

Blockchain Council™

- Public Ledgers: Confirmed transactions are stored in a public ledger known as Blockchain. The ledger ensures that corresponding “digital wallets” can calculate an accurate spendable balance.
- Transactions: A transfer of funds between two digital wallets is called a transaction. When a transaction is made, wallets use an encrypted electronic signature to provide a mathematical proof.
- Mining: It is the process of confirming transactions and adding them to a public ledger. The mining process is what gives value to the coins and is known as a proof-of-work system.

Now, we will turn our attention towards the basics of cryptocurrency. What are all the basic things that you must clearly understand before going further into more specific things?

Public ledgers confirm transactions that are stored in a public ledger which are called Blockchain. The ledger ensures that corresponding “digital wallets” can calculate an accurate spendable balance to maintain uniformity in the whole transaction process.

A transaction is a transfer of funds between two digital wallets. When a transaction is made, wallets use an encrypted electronic signature to provide a mathematical proof which is used by miners in the process of mining.

Mining is the process of confirming transactions and adding them to a public ledger. The mining process is what gives value to the coins and is known as a proof-of-work system.

So these are the very basic concepts related to cryptocurrency. We will learn more about the cryptocurrency basics in our upcoming lectures. But for now, we will look out for the characteristics of Cryptocurrencies.

CHARACTERISTICS

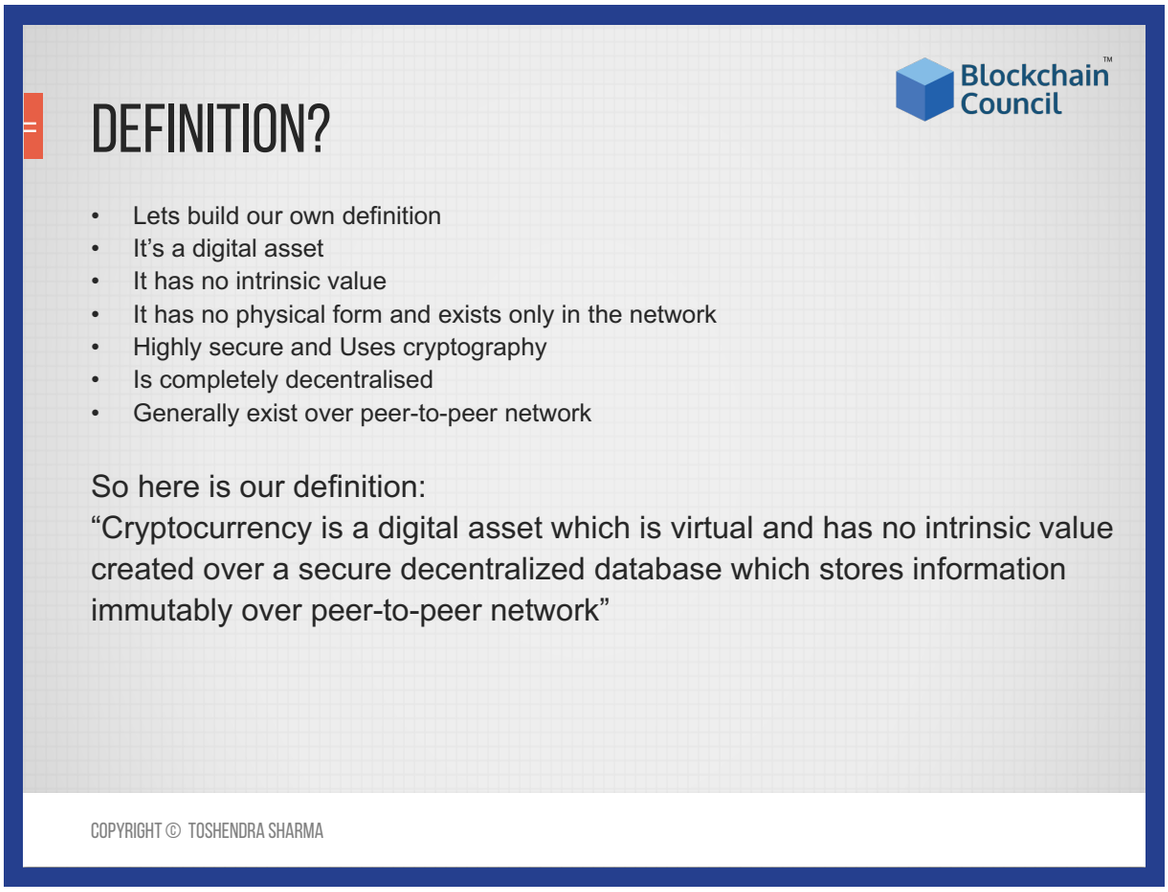
- Irreversible: A transaction can't be reversed, when it is confirmed
- Secure: Cryptocurrency funds are locked in a public key cryptography system, only the owner of the private key can send cryptocurrency
- Permission less: There is no authorization that can prevent you from receiving and sending Cryptocurrencies.
- Fast : Transactions can be propagated instantly and gets confirmed in a couple of minutes.
- Pseudonymous: Identities are not linked with accounts or transactions.

The first thing about cryptocurrency is that it is irreversible that means a transaction can't be reversed once it is confirmed. So you have to be very sure about the receiver's address before making any transaction. The next significant feature of cryptocurrency is it's security that means one who is aware of the private key of the address is the only person who can make transactions.

Permission-less is an important feature related to cryptocurrency which clarifies that there is no authority to deal with.

The transaction is very fast, can be propagated instantly and gets confirmed in a couple of minutes.

Pseudo-anonymity also makes count on these characteristics; it means that our identities are not linked with accounts or transactions.



Now we are well versed with the basic details of cryptocurrency so we will formulate our definition of cryptocurrency just as we did with the Blockchain so that we don't have to learn some xyz definition.

Let's start. It's a digital asset; it has no intrinsic value, it has no physical form and exists only in the network, it is highly secure and uses cryptography, is completely decentralized, generally exists over a peer-to-peer network.

So, here is our definition:

"Cryptocurrency is a digital asset which is virtual and has no intrinsic value, created over a secure decentralized database which stores information immutably over peer-to-peer network."

This will now help you to memorize the definition much easily.

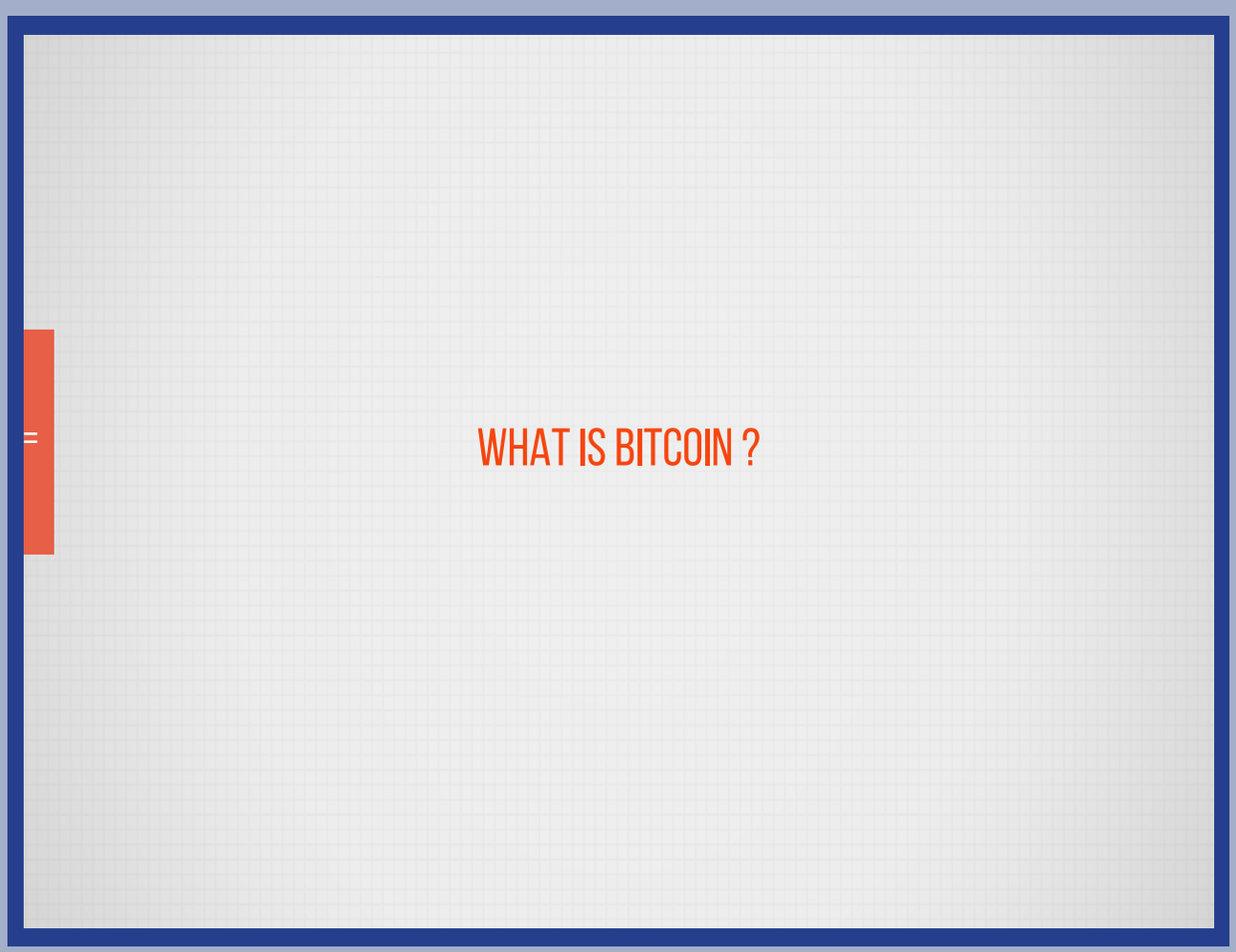
To summarize, Cryptocurrencies are digital gold, sound money that is secure from political influence, so you don’t have to worry about any third party running after your wealth.

It’s the money that promises to preserve and increase its value over time, a person invested in it a few years back have a sure idea about this aspect. They are also a fast and comfortable means of payment with a worldwide scope along with being private and anonymous. They gave birth to an incredibly dynamic, fast-growing market for investors and speculators; mostly everybody is investing in this and is reaping boom-ing benefits from this.

A very important fact related to cryptocurrency is that they don’t represent debts. They just represent themselves. They are money as hard as coins of gold and they open the door for revolutionary technological possibilities in the recent future.

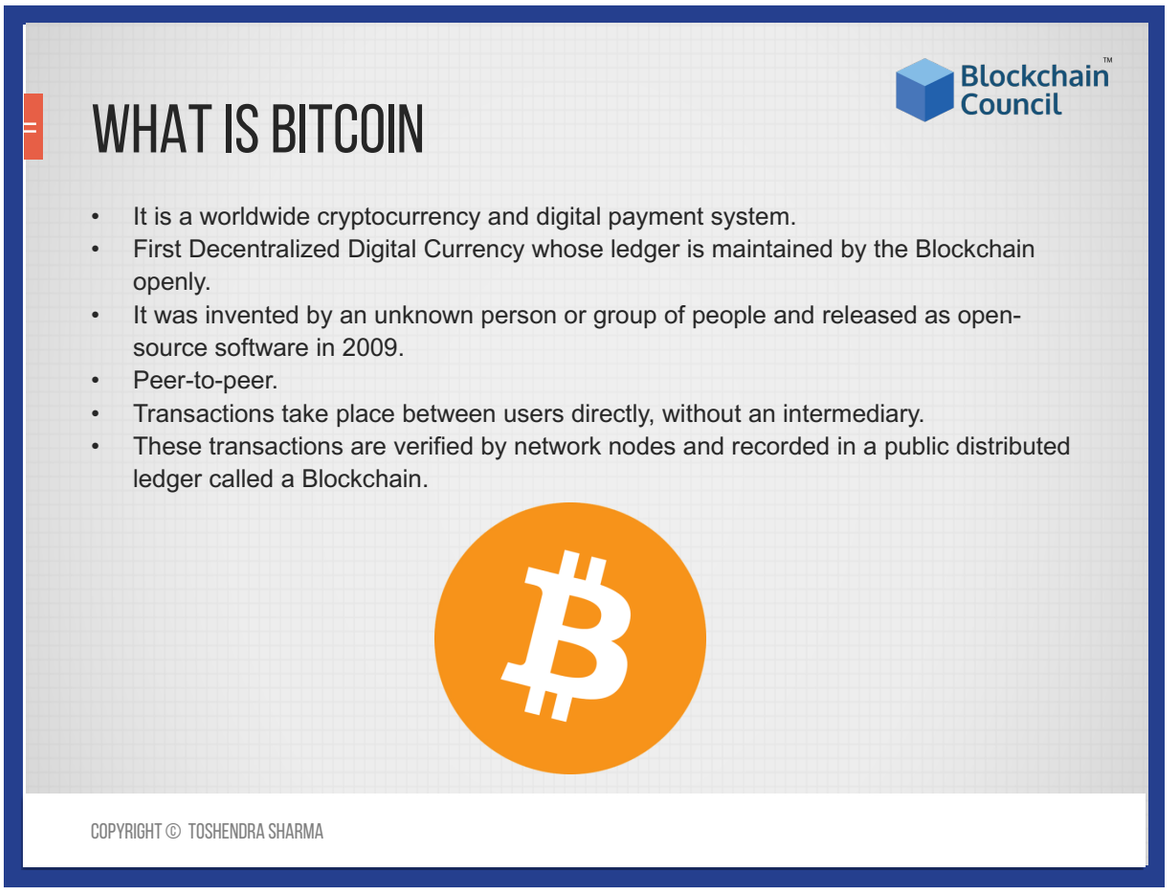
CHAPTER 4

What is Bitcoin



Let's understand what is Bitcoin and why is it getting so popular in the market? Why are people willing to buy Bitcoins, what will they do with them, is it a safe measure to buy them or not?

Starting one by one, this section will cover all the above listed aspects.



Bitcoin is a worldwide cryptocurrency and digital payment system called the first decentralized digital currency, as the system works without a central repository or single administrator. By the term digital currency, we can rectify our concept as of Bitcoin not being available in any physical form (such as bank notes and coins). It exhibits properties similar to physical currencies but allows for instantaneous transactions and borderless transfer-of-ownership.

It was invented by an unknown person or group of people and released as open-source software in 2009.

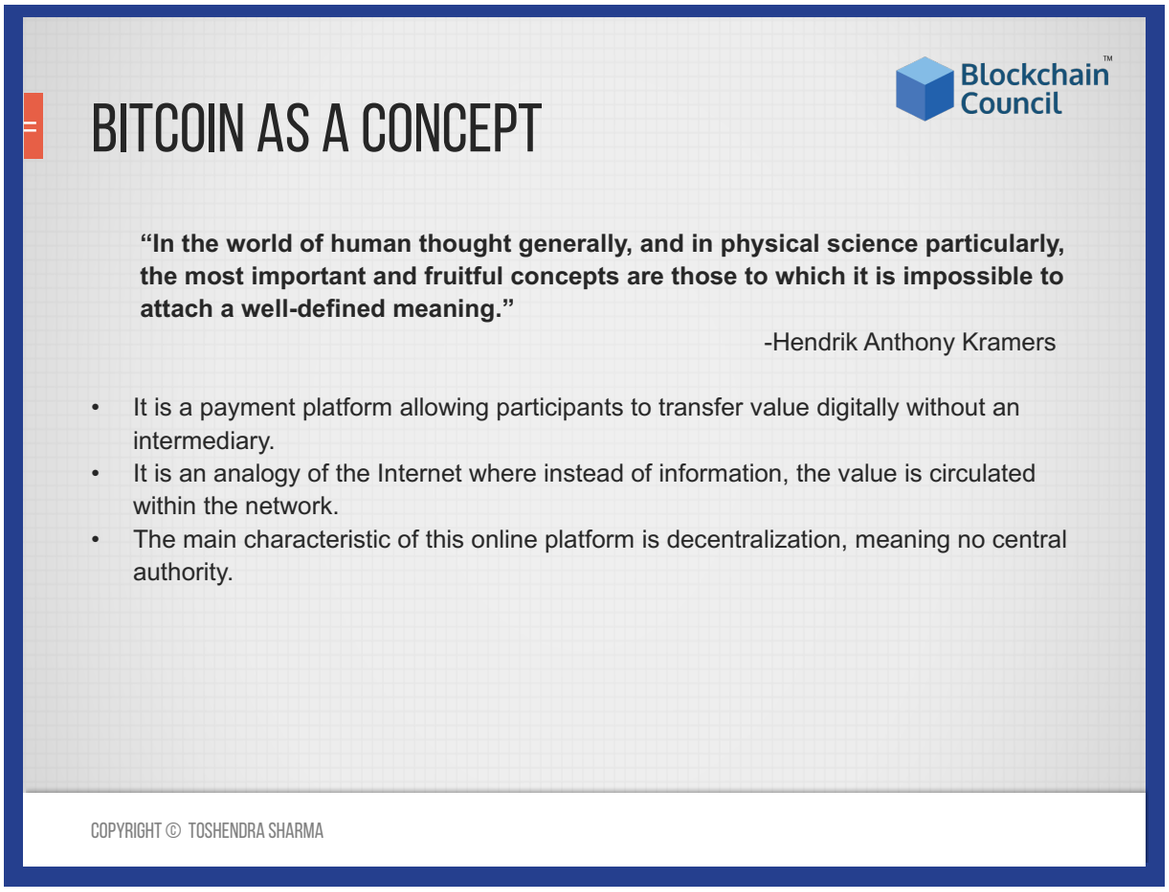
The system is peer-to-peer and transactions take place between users directly, without an intermediary. These transactions are verified by network nodes and recorded in a public distributed ledger called a Blockchain.

WHO CREATED IT?

- A software developer called **Satoshi Nakamoto** proposed Bitcoin, which was an electronic payment system based on mathematical proof.
- It was released as an open source software in 2009.
- The idea was to produce a currency independent of any central authority, transferable electronically, more or less instantly, with very low transaction fees.

Satoshi Nakamoto (Not Verified)

Now, you might be wondering who is behind this amazing concept and who initially worked on it. A software developer called Satoshi Nakamoto proposed Bitcoin, which was an electronic payment system based on mathematical proof. It was released as an open source software in 2009. The idea was to produce a currency independent of any central authority, transferable electronically, more or less instantly, with meagre transaction fees.

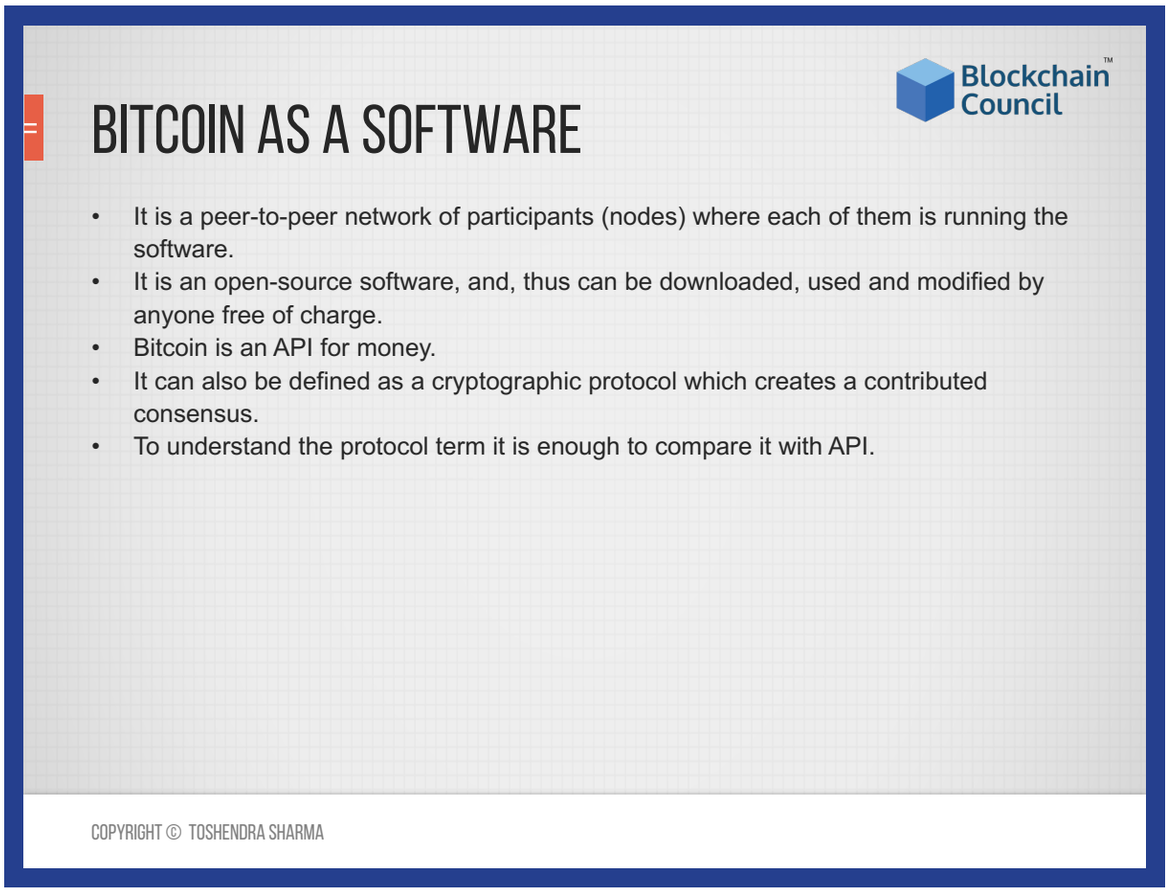


Now we will try to understand Bitcoin in all possible ways.

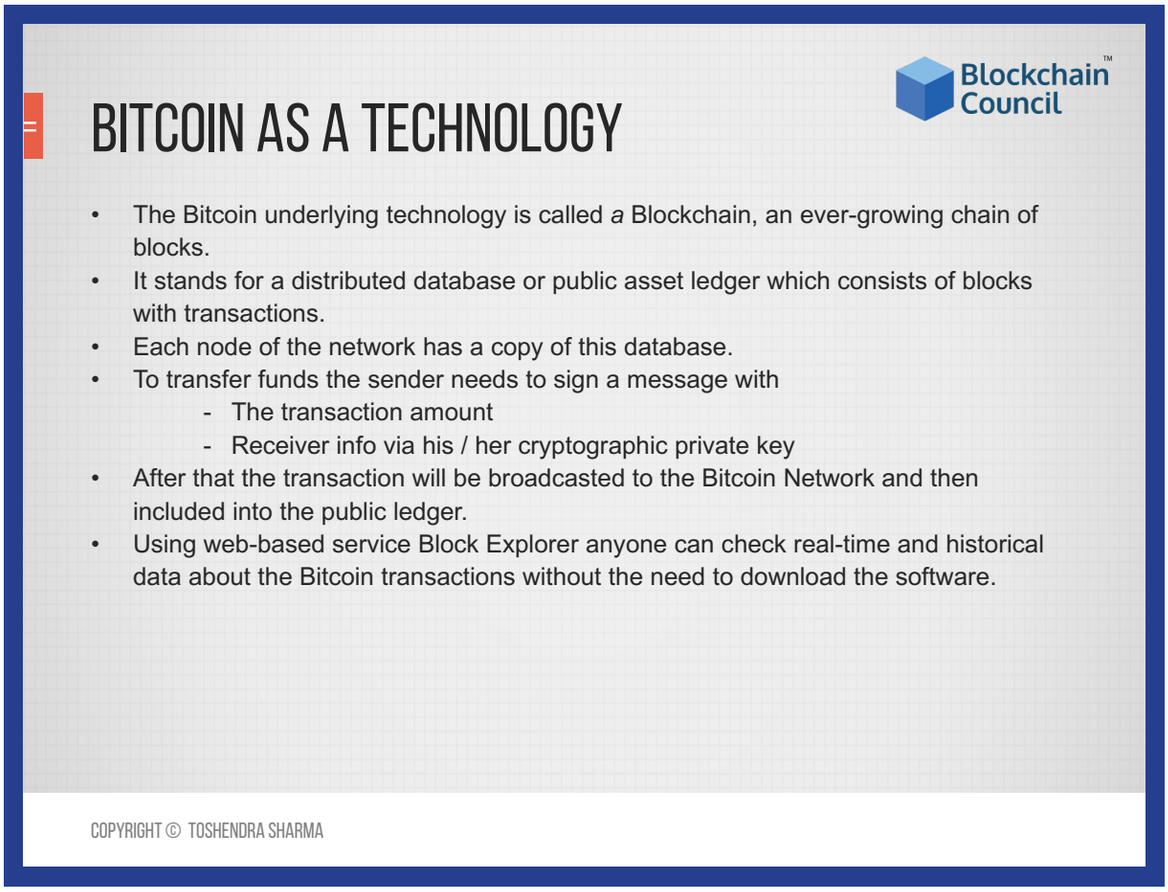
Starting with the concept of Bitcoin, many experts in today's world have shared their views on the concept of Blockchain and Bitcoin.

Hendrick Anthony Kramers, a dutch physicist, once quoted "In the world of human thought generally, and in physical science particularly, the most important and fruitful concepts are those to which it is impossible to attach a well-defined meaning."

Bitcoin is a payment platform allowing participants to transfer value digitally without an intermediary. It is an analogy of the Internet where instead of information, the value is circulated within the network. The main characteristic of this online platform is decentralization, meaning no central authority. Thus, nobody can lose control of the Bitcoin system as nobody owns it.



Continuing with it, we'll now try to understand Bitcoin as a software. Bitcoin is a peer-to-peer network of participants or nodes, where each of them is running the software. The software is open-source and thus can be downloaded, used and modified by anyone free of charge. Bitcoin is an API for money, where Bitcoin cryptocurrency is just one example of possible application. Instead of it, there can be smart contracts. Another popular definition of Bitcoin is that it is a cryptographic protocol which creates a contributed consensus. To understand the protocol term, it is enough to compare it with API.

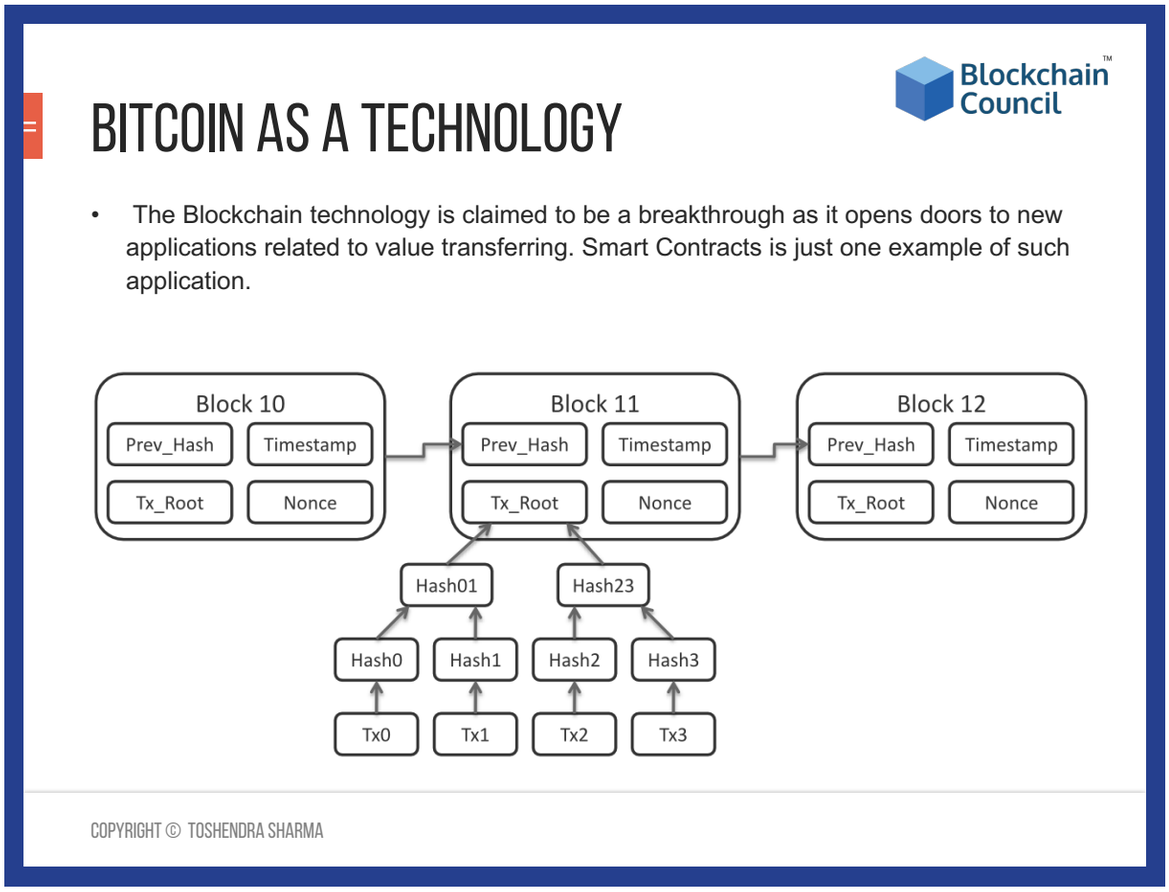


The most important aspect of understanding Bitcoin is it's technology. The Bitcoin underlying technology is called a Blockchain, an ever-growing chain of blocks. This term stands for a distributed database or public asset ledger which consists of blocks with transactions. Each node of the network has a copy of this database. To transfer funds, the sender needs to sign a message with:

- the transaction amount and
- receiver info via his or her cryptographic private key.

After that, the transaction will be broadcasted on the Bitcoin Network and then included into the public ledger.

Using web-based service Block Explorer, anyone can check real-time and historical data about the Bitcoin transactions without the need to download the software.



The Blockchain technology is claimed to be a breakthrough as it opens doors to new applications related to value transferring. Smart Contracts is just one example of such application.

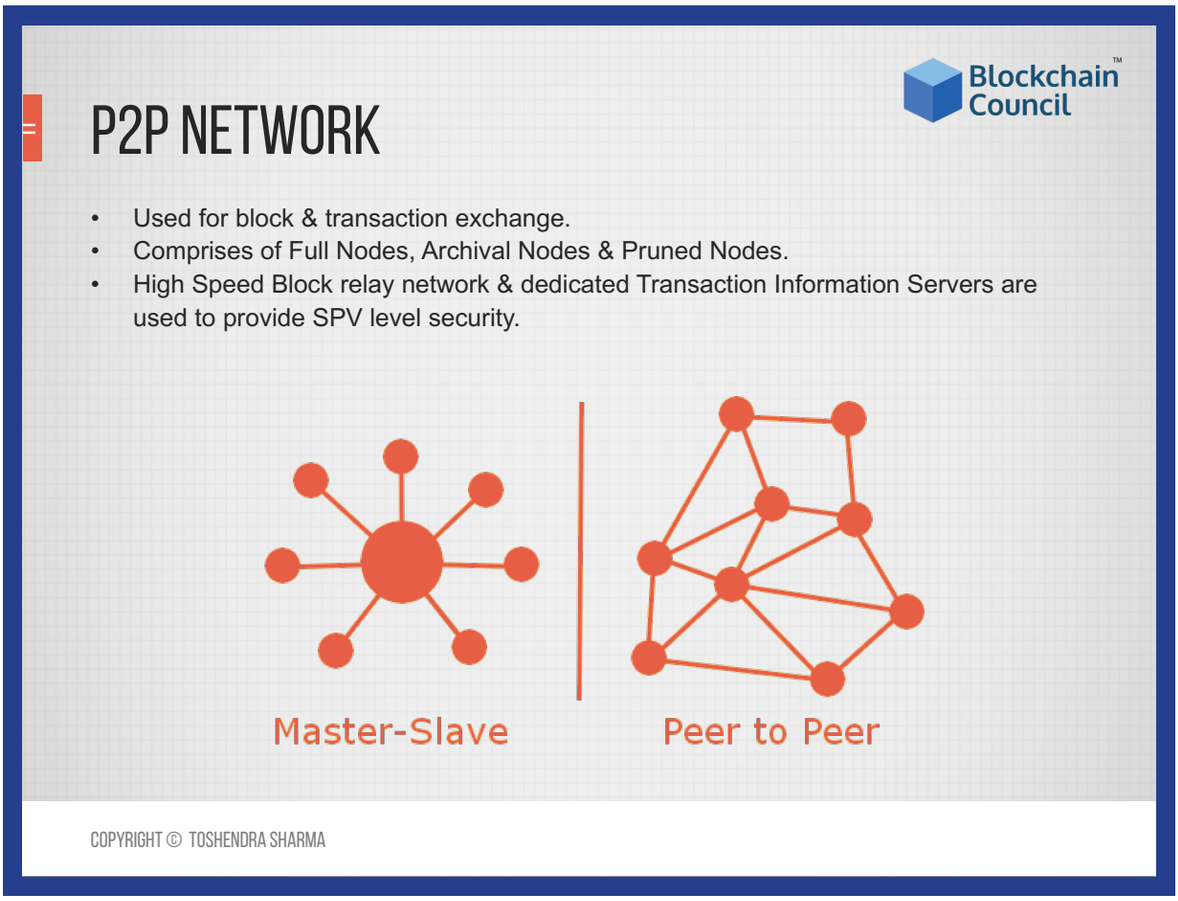
We'll try to understand it with the help of a diagram. It shows the connection of nodes in the network. Block 10 is connected to Block 11 which is connected to Block 12.

Each block header contains Timestamp which is the time when the block was found, reference to parent (Prev_Hash) which is a hash of the previous block header which ties each block to its parent, and therefore by induction to all previous blocks. This chain of references is the eponymy concept for the Blockchain, the Merkle Root (Tx_Root) which is a reduced representation of the set of transactions that are confirmed with this block. The transactions are provided independently forming the body of the block. There must be at least one transaction: the Coinbase which is a special transaction that may create new bitcoins and collects the transaction fees. Other transactions are optional. It also contains a target corresponding to the difficulty of finding a new block. It is updated every 2016 blocks when the difficulty reset occurs.

The block's own hash is a digest of all the above header items except the transaction data which is a proof that the other parts of the header have not been changed and then is used as a reference by the succeeding block.

CHAPTER 5

Peer-to-Peer Network



Bitcoin network nodes are categorized into three types:

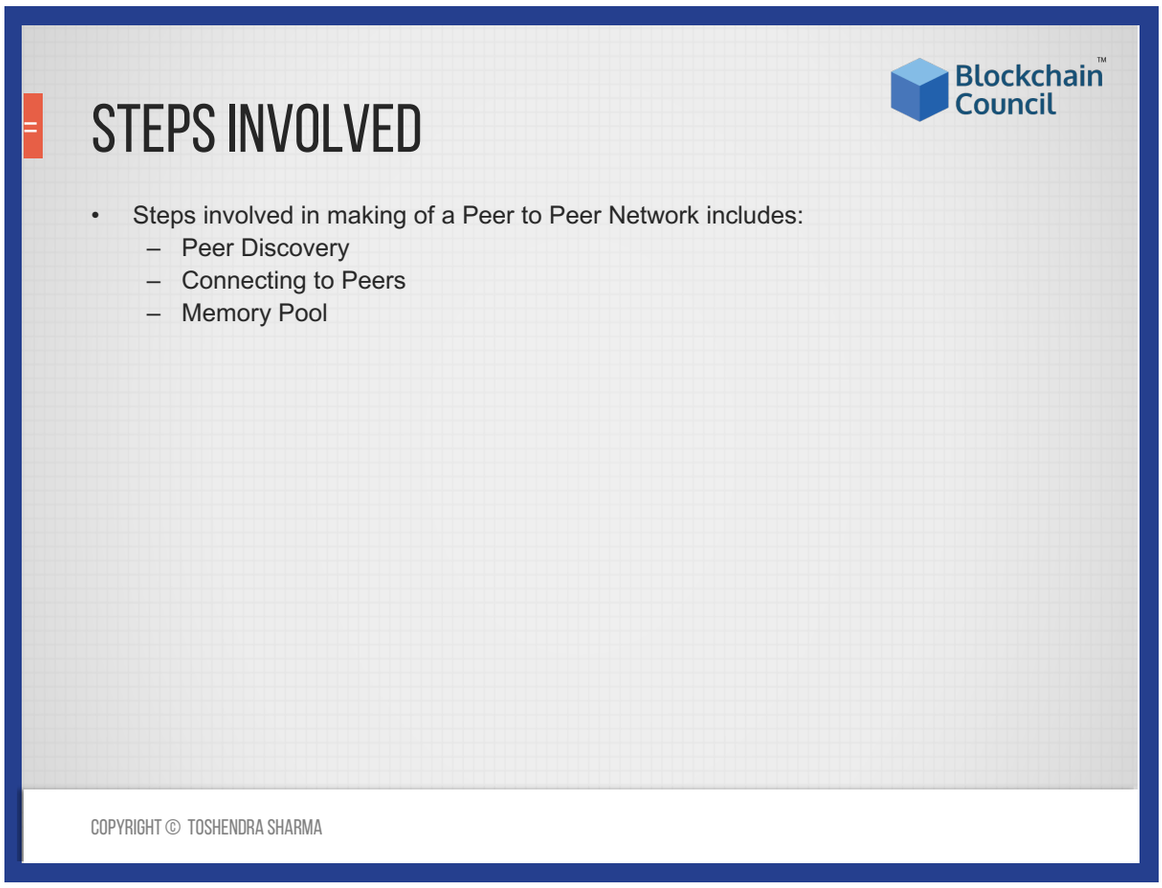
- Full nodes
- Archival nodes
- Pruned nodes

The Bitcoin network protocol allows full nodes (peers) to maintain a peer-to-peer network for block and transaction exchange collaboratively. Full nodes download and verify every block and transaction before relaying them to other nodes.

Archival nodes are full nodes which store the entire Blockchain and can serve historical blocks to other nodes.

Pruned nodes are full nodes which do not store the entire Blockchain. Many SPV clients also using the Bitcoin network protocol to connect to full nodes.

Consensus rules do not cover networking, so Bitcoin programs may use alternative networks and protocols, such as the high-speed block relay network used by some miners and the dedicated transaction information servers used by some wallets that provide SPV-level security.



So, steps involved in making of a peer-to-peer network in Bitcoin are:

Peer Discovery

- When started for the first time, programs don't know the IP addresses of any active full nodes. In order to discover some IP addresses, they query one or more DNS names called DNS seeds. The response to the lookup should include one or more DNS A records with the IP addresses of full nodes that may accept new incoming connections.

Connecting to Peers

- Connecting to a peer is done by sending a version message, which contains your version number, block, and the current time to the remote node. The remote node responds with its version message. Then both nodes send a "verack" message to the other node to indicate the connection has been established.

Once connected, the client can send to the remote node, get address and address messages to gather additional peers.

In order to maintain a connection with a peer, nodes by default will send a message to peers before 30 minutes of inactivity. If 90 minutes pass without a message being received by a peer, the client will assume that connection has closed.

Next Step Involves a Memory Pool

- Full peers may keep track of unconfirmed transactions which are eligible to be included in the next block. It is essential for miners who will mine some or all of those transactions, but it's also useful for any peer who wants to keep track of unconfirmed transactions, such as peers serving unconfirmed transaction information to SPV clients.

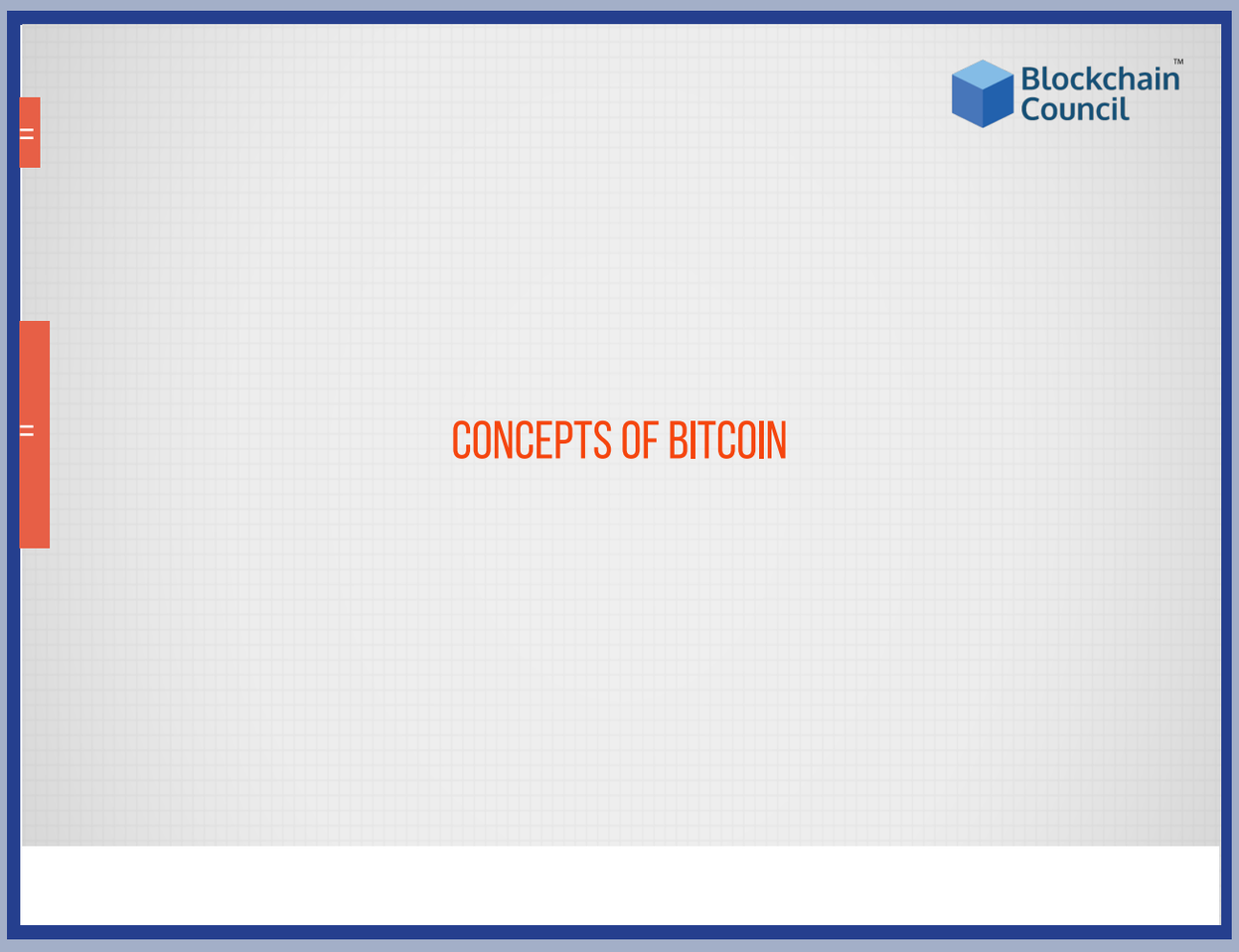
Because unconfirmed transactions have no permanent status in Bitcoin, Bitcoin Core stores them in non-persistent memory, calling it a memory pool or mempool. When a peer shuts down, its memory pool is lost except for any transactions stored by its wallet. It means that never-mined unconfirmed transactions tend to slowly disappear from the network as peers restart or as they purge some transactions to make room in memory for others.

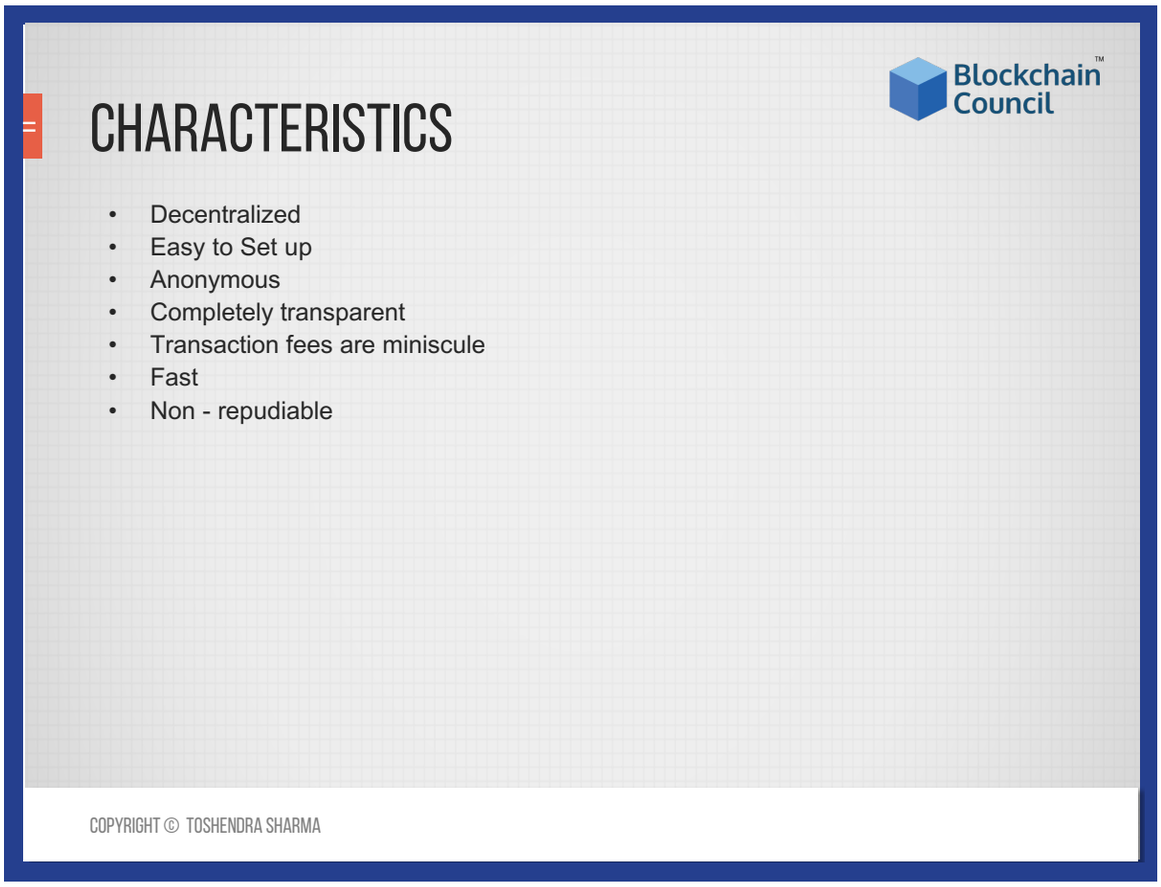
Transactions which are mined into blocks that later become stale blocks may be added back into the memory pool. These re-added transactions may be re-removed from the pool almost immediately if the replacement blocks include them. It is the case in Bitcoin Core, which removes stale blocks from the chain one by one, starting with the tip, the highest block. As each block is removed, its transactions are added back to the memory pool. After all of the stale blocks are removed, the replacement blocks are added to the chain one by one, ending with the new tip. As each block is added, any transactions it confirms are removed from the memory pool.

SPV clients don't have a memory pool for the same reason as they don't relay transactions. They can't independently verify that a transaction hasn't yet been included in a block.

CHAPTER 6

Concepts of Bitcoin





Bitcoins are useful in many ways and has a number of characteristic features that set it apart from government-backed currencies.

1. It's decentralized

The Bitcoin network isn't controlled by one central authority. Every machine that mines Bitcoin and processes transactions make up a part of the network and the machines work together. It means that in theory, one central authority can't tinker with monetary policy and cause a meltdown – or simply decide to take people's Bitcoins away from them, as the Central European Bank decided to do in Cyprus in early 2013. And if some part of the network goes off-line for some reason, the money keeps on flowing.

2. It's easy to set up

Conventional banks make you jump through hoops simply to open a bank account. Set-ting up merchant accounts for payment is another Kafkaesque task, beset by bureaucracy. However, you can set up a Bitcoin address in seconds with no questions asked and no fees payable.

3. It's anonymous

Well, kind of. Users can hold multiple Bitcoin addresses and they aren't linked to names, addresses, or other personally identifying information.

4. It's completely transparent

Bitcoin stores details of every single transaction that ever happened in the network in a huge version of a general ledger called the Blockchain. The Blockchain tells everything.

If you have a publicly used Bitcoin address, anyone can tell how many Bitcoins are stored at that address. They just don't know that it's yours.

Though, there are measures that people can take to make their activities more opaque on the Bitcoin network, such as not using the same Bitcoin addresses consistently and not transferring a lot of Bitcoins to a single address.

5. Transaction fees are miniscule

Your bank may charge you a £10 fee for international transfers. Bitcoin doesn't.

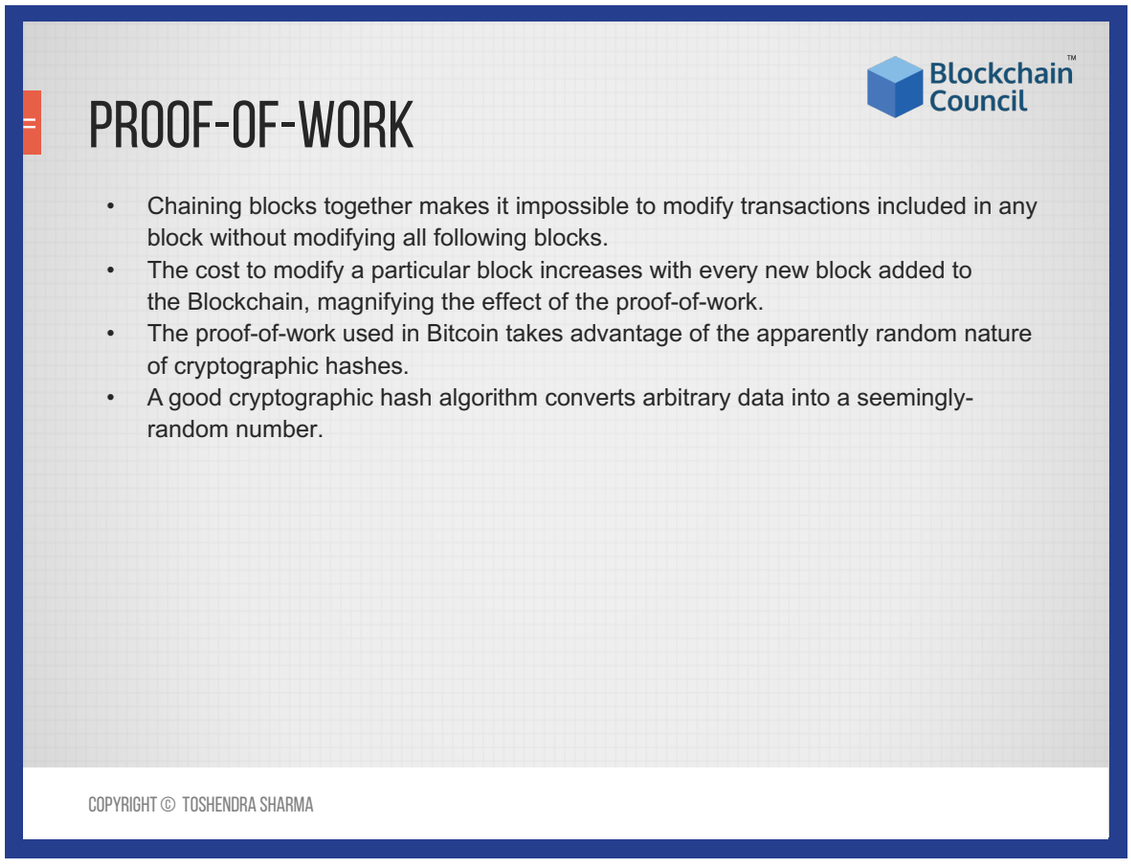
6. It's fast

You can send money anywhere and it will arrive just in minutes, as soon as the Bitcoin network processes the payment.

7. It's non-repudiable

When your Bitcoins are sent, there's no way of getting them back, unless the recipient returns them to you. They're gone forever.

So, Bitcoin has a lot going for it, in theory.



Next, we'll try to understand the concept of Proof-of-Work.

The Blockchain is collaboratively maintained by anonymous peers on the network, so Bitcoin requires to prove that a significant amount of work was invested in its creation to ensure that untrustworthy peer who wants to modify past blocks have to work harder than honest peers who only want to add new blocks to the Blockchain.

Chaining blocks together makes it impossible to modify transactions included in any block without modifying all following blocks.

As a result, the cost to modify particular block increases with every new block added to the Blockchain, magnifying the effect of the proof-of-work.

The proof-of-work used in Bitcoin takes advantage of the apparently random nature of cryptographic hashes.

A good cryptographic hash algorithm converts arbitrary data into a seemingly-random number.

If the data is modified in any way and the hash re-run, a new seemingly-random number is produced, so there is no way to modify the data to make the hash number predictable.

It can also be stated that proof of work is a piece of data which is difficult, costly, time-consuming to produce but easy for others to verify and which satisfies certain requirements. Producing a proof of work can be a random process with low probability where a lot of trial and error is required on an average before a valid proof of work is generated. Bitcoin uses the Hashcash proof of work system.

One application of this idea is using Hashcash as a method of preventing email spam, requiring a proof of work on the email's contents including the "To" address, on every email. Legitimate emails will be able to do the work to generate the proof easily, i.e., not much work is required for a single email, but mass spam emailers will have difficulty generating the necessary proofs requiring huge computational resources.

Hashcash proofs of work are used in Bitcoin for block generation. For a block to be accepted by network participants, miners must complete a proof-of-work which covers all the data in the block. The difficulty of this work is adjusted so as to limit the rate at which new blocks can be generated by the network to one in every 10 minutes. Due to the very low probability of successful generation, this makes it unpredictable which worker computer in the network will be able to generate the next block.

For a block to be valid it must hash to a value less than the current target; this means that each block indicates that work has been done to generate it. Each block contains the hash of the preceding block, thus each block has a chain of blocks that together contain a large amount of work. Changing a block requires regenerating all successors and redoing the work they contain. This protects the block chain from tampering.

The most widely used proof-of-work scheme is based on SHA-256 and was introduced as a part of Bitcoin.

In the next section we will learn about the various legal aspects and the regulations around Bitcoin.

CHAPTER 7

Regulations around Bitcoin

Bitcoin is of interest to law enforcement agencies, tax authorities and legal regulators, all of which are trying to understand how the cryptocurrency fits into existing frameworks. The legality of your Bitcoin activities will depend on who you are, where you live and what you are doing with it.

Bitcoin has proven to be a contentious issue for regulators and law enforcers, both of which have targeted the digital currency in an attempt to control its use.

So let's discuss the concerns about Bitcoin.

As you all might be aware that, Government agencies are increasingly worried about the implications of Bitcoin, as it can be used anonymously and is therefore, a potential instrument for money laundering. In particular, law enforcers seem to be concerned about the decentralized nature of the currency.

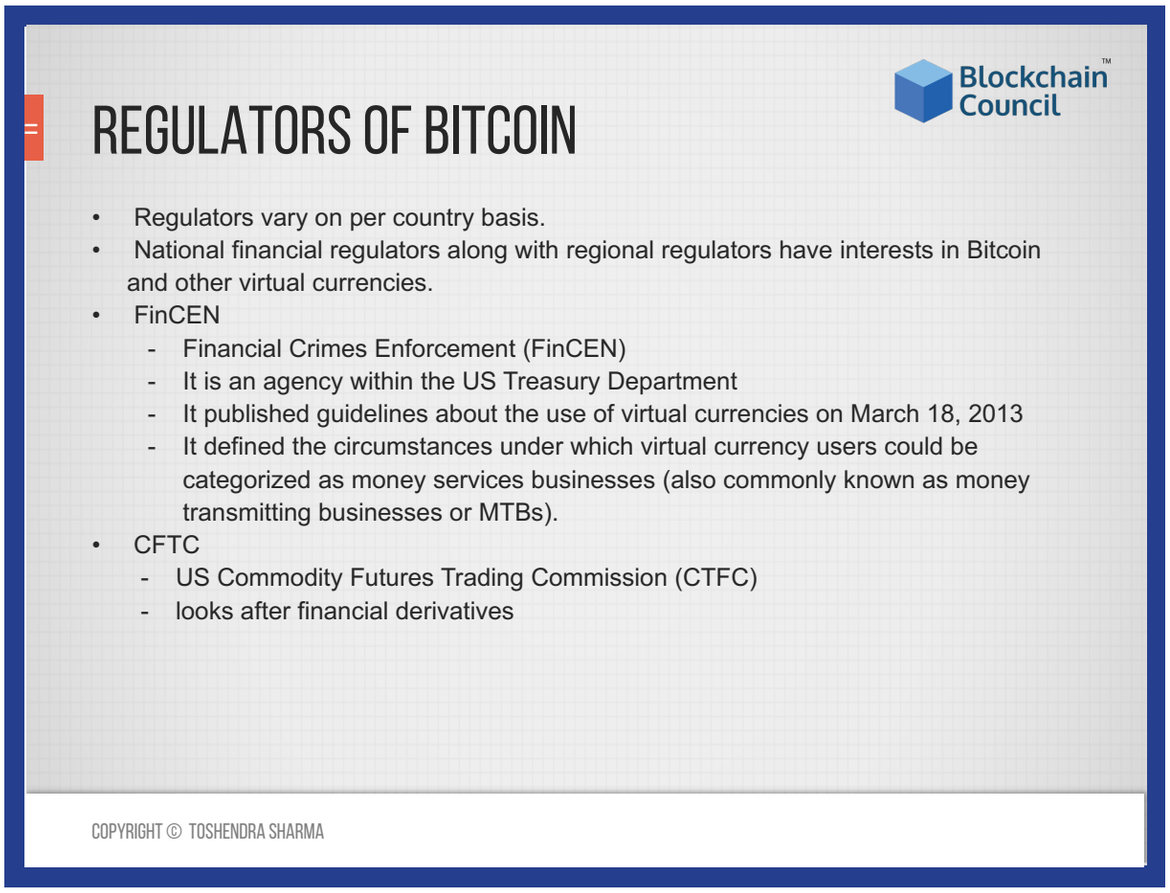
As early as April 2012, the FBI published a document highlighting its fears around Bitcoin specifically, drawing a distinction between it and centralized digital currencies such as eGold and WebMoney.

It voiced concerns that while US-based exchanges are regulated, offshore services may not be and could be a haven for criminals to use Bitcoin for illicit activities without being getting traced.

Bitcoin was the only form of currency accepted on Silk Road, an anonymous marketplace that was only accessible over the TOR anonymous browsing network, which was closed by the FBI in October 2013. It was commonly used to sell goods that are illegal in many countries, including narcotics.

This prompted US Senator Charles Schumer to call for the site to be shut down, explicitly linking it to Bitcoin, which he called a "surrogate currency."

Who is regulating the circulation of Bitcoin?



Who is heading the Bitcoin Community?

Regulators will vary on per-country basis, but one can expect to see national financial regulators interested in Bitcoin and other virtual currencies, potentially along with regional regulators at a sub-country level. Three of the major regulators of Bitcoins in the US are:

FinCEN

FinCEN or the Financial Crimes Enforcement Network is an agency within the US Treasury Department, who took the initiative.

It published guidelines about the use of virtual currencies. FinCEN's March 18, 2013 guidance defined the circumstances under which virtual currency users could be categorized as money services businesses (also commonly known as money transmitting businesses or MTB's).

MTB's must enforce Anti-Money Laundering and Know Your Client measures, identifying the people that they're doing business with.

CFTC

The US Commodity Futures Trading Commission (CTFC), which looks after financial derivatives, hasn't announced any regulation yet but has made it clear that it could if it wanted to.

SEC

The US Securities and Exchange Commission (SEC) hasn't issued solid regulations on virtual currencies, but its Office of Investor Education and Advocacy published an investor alert to warn people about fraudulent investment schemes involving Bitcoin. In particular, it warned of Ponzi schemes, after charging Texas resident Trendon T Shavers also known as 'pirateat40', founder and operator of Bitcoin Savings and Trust, with allegedly raising 700,000 Bitcoins by promising investors up to 7% weekly interest.

The SEC case has also forced the legislative branch of government to consider Bitcoin's legal status. Shavers had claimed that he could not be prosecuted for securities fraud, as Bitcoin wasn't money. However, Judge Amos Mazzant issued a memorandum arguing that Bitcoin can be used as money.

In August 2013, the US Senate wrote to several law enforcement agencies, inquiring about the threats and risks related to virtual currency. The letters included the one to the Department Of Homeland Security, fretting about the lack of a paper trail for regulators and enforcement agencies to follow for virtual currency transactions. It requested policies and

guidance related to the treatment of virtual currencies and information about any ongoing strategic efforts in the area.

November saw responses from the various agencies. The Department of Homeland Security was most worried about the criminal threat from the illicit use of Bitcoin, while the Federal Reserve and the Department of Justice all acknowledged the legitimate uses of virtual currencies. The SEC argued that "any interests issued by entities owning virtual currencies or providing returns based on assets such as virtual currencies" were considered securities and thus fell under its remit.

Consequently, though there were many issues aroused by various authorities concerning about the compromising legal aspects of Bitcoin but were ultimately declined by the society.

So, now we will try to understand the countrywise legality of Bitcoin.

UNITED STATES

Blockchain Council™

- Each US state has their own financial regulators and laws, and each approaches Bitcoin differently.
- California and New York have been particularly aggressive in their pursuit of Bitcoin-related organizations.
- New Mexico, South Carolina, and Montana, don't regulate money transmitting businesses.
- New York's "BitLicense" was the first virtual currency-specific licensing regime to address Bitcoin and digital currencies in the US, released in June, 2015.
- It stands in contrast to decisions by US states to apply existing financial law to the use of the technology.
- There are three main categories of Bitcoin stakeholder :
  - Users
  - Miners
  - Exchangers

Starting with the United States of America, each US state has their financial regulators and laws and each approaches Bitcoin differently. California and New York have been particularly aggressive in their pursuit of Bitcoin-related organizations while others, such as New Mexico, South Carolina and Montana, don't regulate money transmitting businesses.

In May 2013, California's state financial regulator issued a letter to the Bitcoin Foundation, a nonprofit organization designed to promote Bitcoin, warning it that it may be a money transmission business and threatening people there with potential fines and jail time.

In continuation to this, New York's BitLicense was the first virtual currency-specific licensing regime to address Bitcoin and digital currencies in the US.

Developed by the New York State Department of Financial Services and released in June 2015, the regulation stands in contrast to decisions by US states such as Texas and Vermont to apply existing financial law to the use of the technology, as well as efforts in California to amend prior legislation. Several banks have stopped accounts owned by people operating Bitcoin exchanges. The legality of Bitcoin depends on who you are and what you're doing with it.

There are three main categories of Bitcoin stakeholder:

- Users (These are individuals who obtain Bitcoins and either hoard them or spend them. Under the FinCEN guidance, users who simply exchange Bitcoins for goods and services are using it legally.)
- Miners (According to the FinCEN guidance, people creating Bitcoins and exchanging them for fiat currency are not safe.

In contrast, a person who creates units of convertible virtual currency and sells those units to another person for real currency or its equivalent is engaged in transmission to another location and is a money transmitter.

- Exchanger : a person is an exchanger and a money transmitter if a person accepts such de-centralized convertible virtual currency from one person and transmits it to another person, as part of the acceptance and transfer of currency, funds or other value that substitutes for currency.

Someone may fall under more than one of these categories and each category has its legal considerations.

INITIATIVE TAKEN BY INDUSTRIES

Blockchain Council™

- Several companies created a committee to form a self-regulatory body called "DATA", designed to encourage open conversation with regulators.
- The Bitcoin Foundation formed committees to offer legal guidance, steer policy, and liaise with regulators.
- Exchanges have been attempting to secure MTB licenses at the state and federal levels, and some have avoided doing business with US customers until this is resolved.

Now, the question arises, are industries taking any measures to these concerns?

Yes, the industry has responded to the growing regulator concerns in several ways.

- Numerous companies created a committee to form a self-regulatory body called DATA, designed to encourage open conversation with regulators.
- The Bitcoin Foundation formed committees to offer legal guidance, steer policy and liaise with regulators.
- Exchanges have been attempting to secure MTB licenses at the state and federal levels and some have avoided doing business with US customers until this is resolved.

It's not all about the Legal concerns of the USA to Bitcoin, but since Bitcoin is a globally accessible Cryptocurrency, hence we all need to see to the concerns of other countries too.

The European Union's banking regulator and The European Banking Authority issued a statement on 13th December 2013 on warning of investment risk, but focusing mainly on issues of fraud, tax evasion and other crime connected to virtual currency usage.

More recently, in July 2014, the EBA published an 'opinion' warning financial institutions to stay away from digital currencies until the industry is regulated. In the document, which was addressed to the European Union Council, European Commission and European Parliament, the EBA set out new requirements for the regulation of digital currencies and also instructed financial institutions not to buy, hold or sell digital currencies until new rules are in place.

Because of large population in China and India, they also have their legal concerns seeing to the people's growing interest in Bitcoin.

China's authorities had arguably the biggest impact on Bitcoin adoption and values in the past months. In early December 2013, the People's Bank of China (PBoC) issued a statement warning of Bitcoin risks and banning financial institutions from engaging in Bitcoin business themselves or transferring funds to/from Bitcoin exchanges. Another statement just few days later, also blocked third-party payment processors from dealing with exchanges and the price of Bitcoin worldwide crashed from its record high of over $1200 by about 50%. It had a dramatic effect on the market share of large Bitcoin exchanges in the country.

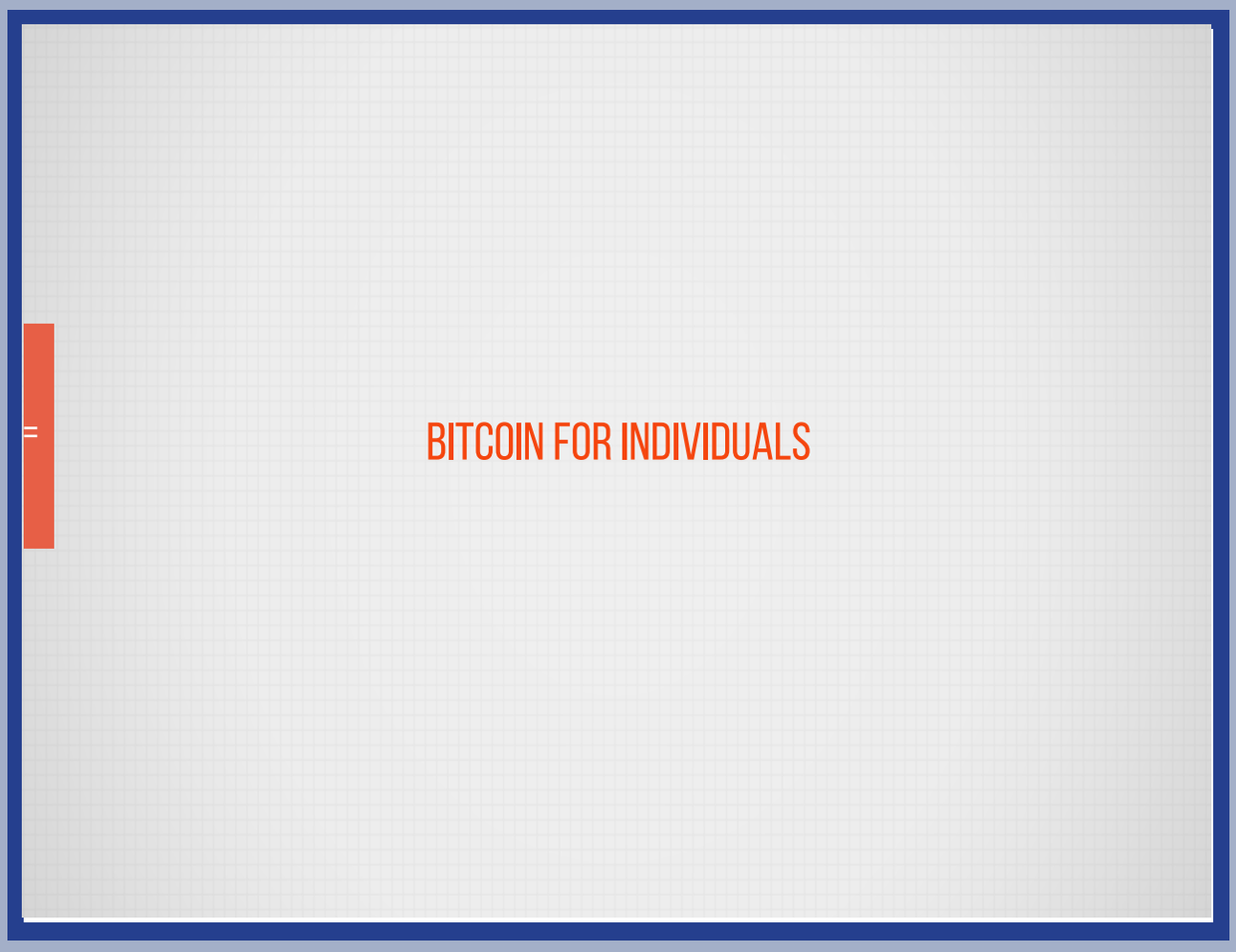
In mid-January, a People's Bank of China official claimed there is no move to suppress or discriminate against Bitcoin in China and exchanges have been allowed to remain open for business.

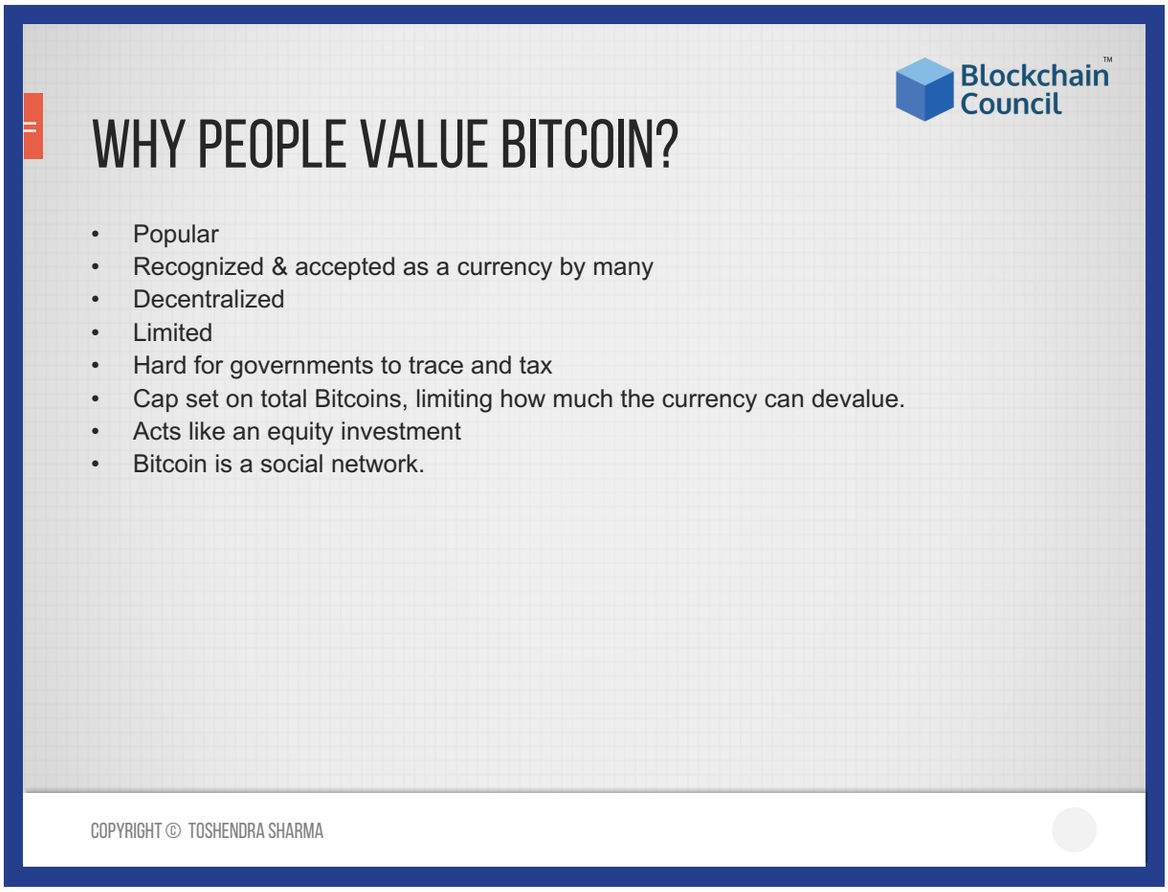
On the other hand, India's central bank is said to be "watching" Bitcoin. In a series of dramatic moves, the Reserve Bank of India (RBI) issued a warning about Bitcoin in late De-cember 2013, which was followed almost immediately by exchanges choosing to suspend operations. One exchange had its premises raided and another was paid a "friendly" visit by tax officials to investigate how digital currencies could be managed and taxed. Since then some exchanges have re-opened for business. It is expected to see Reserve bank of India launching its cryptocurrency very soon.

Next, we'll lead to the necessity of Bitcoin for individuals.

CHAPTER 8

Bitcoin for Individuals





We will start with understanding the fact that why people value Bitcoin?

Bitcoin does not have value as a physical commodity like gold and is not widely accepted as legal tender like dollars. Rather, Bitcoin appears to have value for the following reasons:

It is popular. In short, people accept and trade in Bitcoin because other people accept and trade in Bitcoin.

It is recognized and accepted as a currency by many.

Bitcoin is decentralized and limited. There are roughly only 21 million Bitcoins available across the globe, resulting in high rates due to increased demand. This is a major factor for many Bitcoin users.

Bitcoin is hard for governments to trace and tax.

Unlike fiat money produced by central banks, there is a cap set on total Bitcoin, limiting how much the currency can devalue through inflation.

Bitcoin acts like an equity investment. The market value of Bitcoin has had wild swings in value and even a market cap.

Bitcoin is a social network. The Bitcoin "community" is active and acts like other online social networks.

Hence, all these factors consequently result in increasing the demand and value of Bitcoin.

Now, let's try to understand it's necessity for individuals.

Bitcoin is the simplest way to exchange money at very low cost.

Bitcoin on mobiles allows you to pay with a simple two-step scan-and-pay. No need to sign up, swipe your card, type a PIN, or sign anything. All you need to receive Bitcoin payments is to display the QR code in your Bitcoin wallet app and let your friend scan your mobile or touch the two phones together using NFC radio technology.

Bitcoin transactions are secured by military grade cryptography. Nobody can charge you money or make a payment on your behalf. It gives you control over your money and a strong level of protection against many types of frauds.

It is universally compatible as it uses the same open technology. The Bitcoin network never sleeps, even on holidays!

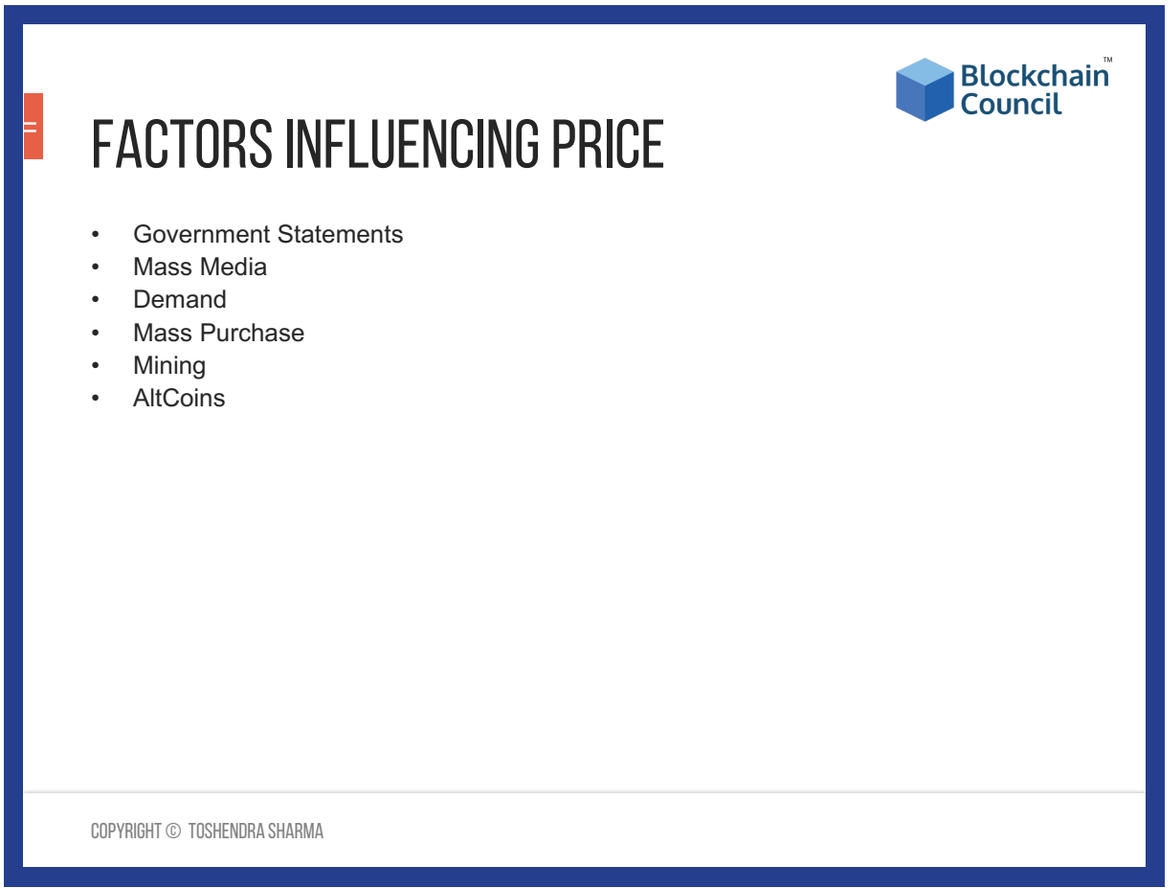
Sending Bitcoin across borders is as easy as sending them across the street. There are no banks to make you wait three business days, no extra fees for making an international transfer and no special limitations on the minimum or maximum amount you can send.

Choose your own fees

This means that there is no fee to receive Bitcoin and many wallets let you control how large a fee to pay when spending. Most wallets have reasonable default fees and higher fees can encourage faster confirmation of your transactions. Fees are unrelated to the amount transferred, so it's possible to send 100,000 Bitcoin for the same fee as required to send 1 Bitcoin.

Protect your identity

With Bitcoin, there is no credit card number that some malicious actor can collect to impersonate you. It is even possible to send a payment without revealing your identity, almost like with physical money. One should, however, take note that some effort can be required to protect your privacy.



The factors influencing the price of Bitcoin are:

Government Statements

The main drivers that make Bitcoin price go up and down are the official government statements regarding the Bitcoin adoption and regulation. The major role belongs to the United States Government as Bitcoin are mainly traded for US dollars.

Mass Media

Mass media provides the essential link between the individuals and the demands of the technological society.

From this heading, it is easy to guess that Bitcoin price movements can coincide with the events covered by the mass media. News that are published by famous FinTech editions or some statements posted on Twitter by opinion leaders influence the Bitcoin price trends as most people are used to reckon upon the influential people's and companies' state of view.

Demand

The more we use it in everyday life - the broader adoption is going to be. While merchants such as Amazon, eBay, Google are adopting Bitcoin, Bitcoin demand is growing, influencing the price growth as a result.

Mining

The mining difficulty, as well as a network hash rate indirectly, impacts the Bitcoin Price. Mining is an investment in the hardware which is required for obtaining Bitcoin. Increasing hash rate with the resulted increased network difficulty influences the number of miners: less and fewer miners are eager to make investments into the hardware as they are not so lucrative as they were used to be. Thereby, they can change the course of their investments from mining to making purchases. Hence, the growing demand can evolve into the price increase.

Altcoins

The Altcoins market also effects Bitcoin price.

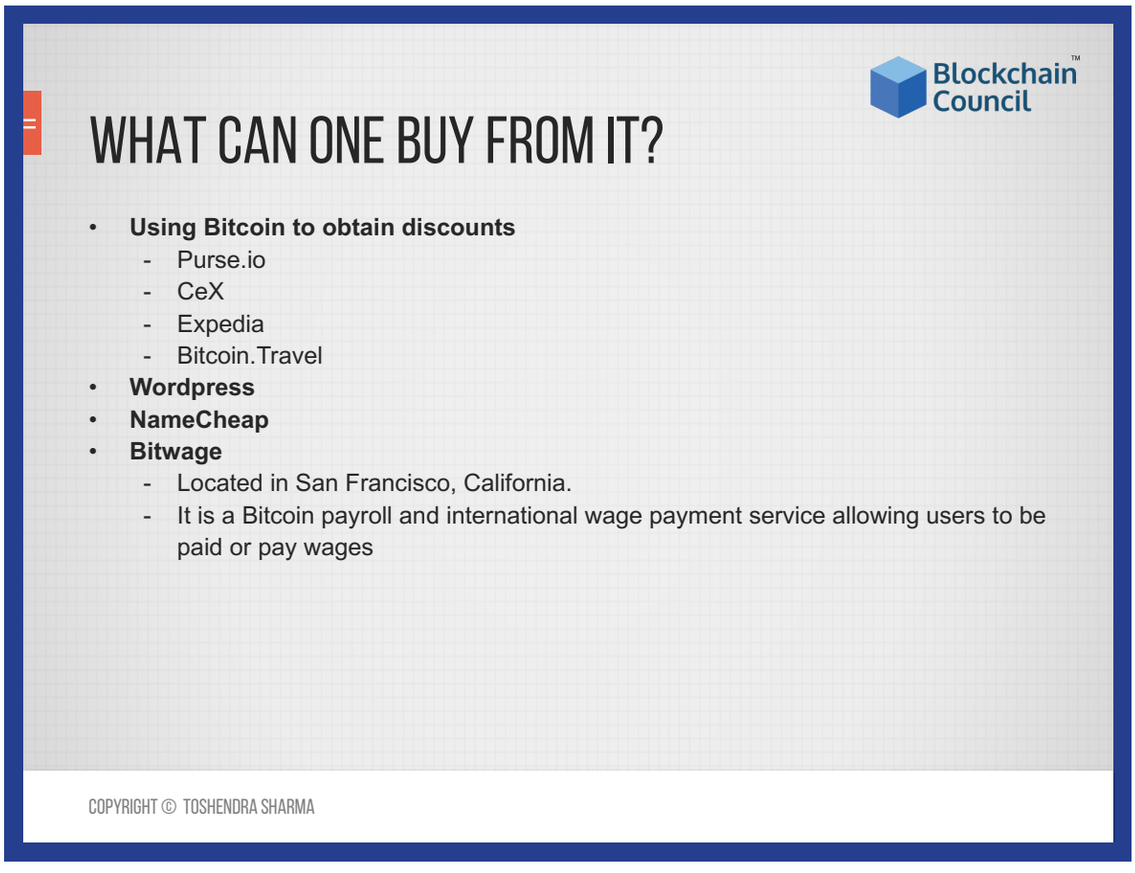
You all might be thinking of what Altcoins are? Altcoins are the alternative cryptocurrencies launched after the success of Bitcoin. Generally, they project themselves as better substitutes to Bitcoin. The success of Bitcoin as the first peer-to-peer digital currency paved the way for many to follow.

The emergence of serious altcoins can distract the attention of Bitcoin audience. A lot of investors, traders, users started to use the altcoins which seem to be more serious and perspective in their point of view in comparison to Bitcoin. Hereby, we will observe the Bitcoin price drop due to the decreasing demand.

So, after considering the pricing strategies and importance of Bitcoin for individuals, let's also see what one can buy from it?

Starting with online e-commerce sites, let's see what all are companies, accepting Bitcoin over market deals.

- Global computing giant "Microsoft" added Bitcoin as a payment option for a variety of digital content across its online platforms in December 2014.
- "Dell," the multinational computer technology specialist, announced in July that it is accepting Bitcoin through a partnership with Coinbase.
- "Overstock" became the first major retailer to accept Bitcoin when it made the announcement back in January 2014.
- "Showroomprive.com" took the crown of the largest European company to start accepting payment in Bitcoin in September 2014. The merchant who sells a variety of products including clothes, fashion accessories, cosmetics and homeware is to accept Bitcoin via European cryptocurrency company Paymium.
- "TigerDirect" the online retailer of computers and consumer electronics, now accepts payments in Bitcoin.
- "Memory Dealers" carries a range of networking hardware equipment and computer memory. It has been a 'Bitcoin believer' from the beginning.
- "BTCTrip" is an online flight and hotel booking service that was one of the first in its industry to serve the Bitcoin community.



Let us now consider the ways of using Bitcoin to receive discounts:

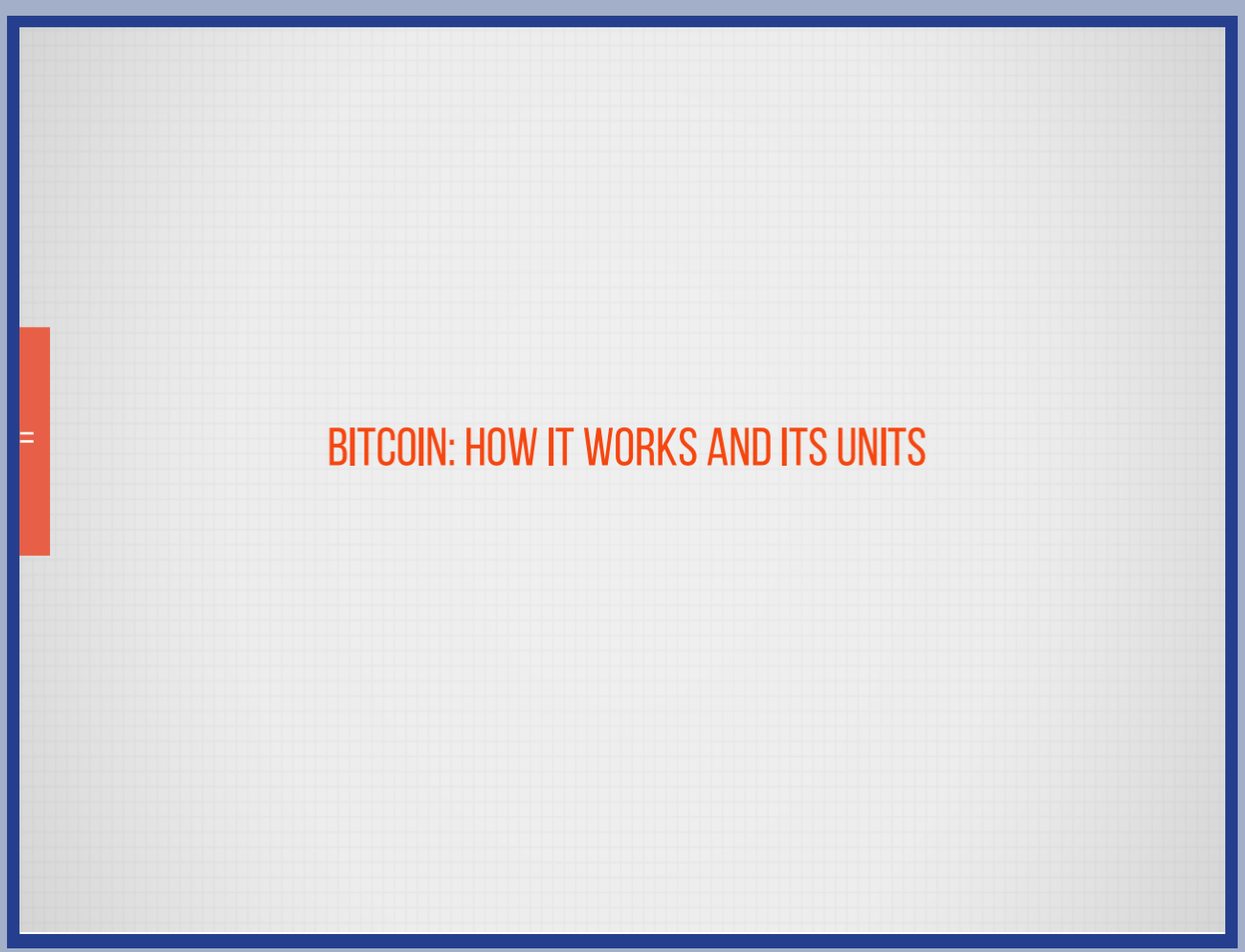
- "Purse.io" is a peer-to-peer marketplace that matches individuals wanting to buy items on Amazon at a discount with others wanting to buy Bitcoin with a credit card or via PayPal.
- "CeX," a UK technology exchange, and retailer, launched a one-store Bitcoin-only payments initiative in Glasgow, as well as Scotland's first Bitcoin ATM.
- "Expedia" has announced that it will now accept Bitcoin for all hotel bookings, making it the first major travel company to accept payments in cryptocurrency.
- "Bitcoin.Travel" is a respected site, offering a mappable list of accommodation, apartments, attractions, bars and beauty salons around the world. Coinmap also maintains a worldwide database of establishments.
- WordPress is among the most visible and popular sites and offers a blogging presence online for payment in cryptocurrency. You can also go to BitcoinCodes to buy credits for Steam, Spotify, XBoxLive, PlayStation Network and AirVPN. Namecheap accepts Bitcoin directly as payment for domain services. If you want a little more privacy online, several VPN (virtual private network) providers now accept only Bitcoin after being blocked by credit card companies and PayPal.
- Bitwage is a Bitcoin payroll and international wage payment service allowing users to be paid or pay wages in Bitcoin, local currencies and commodities.

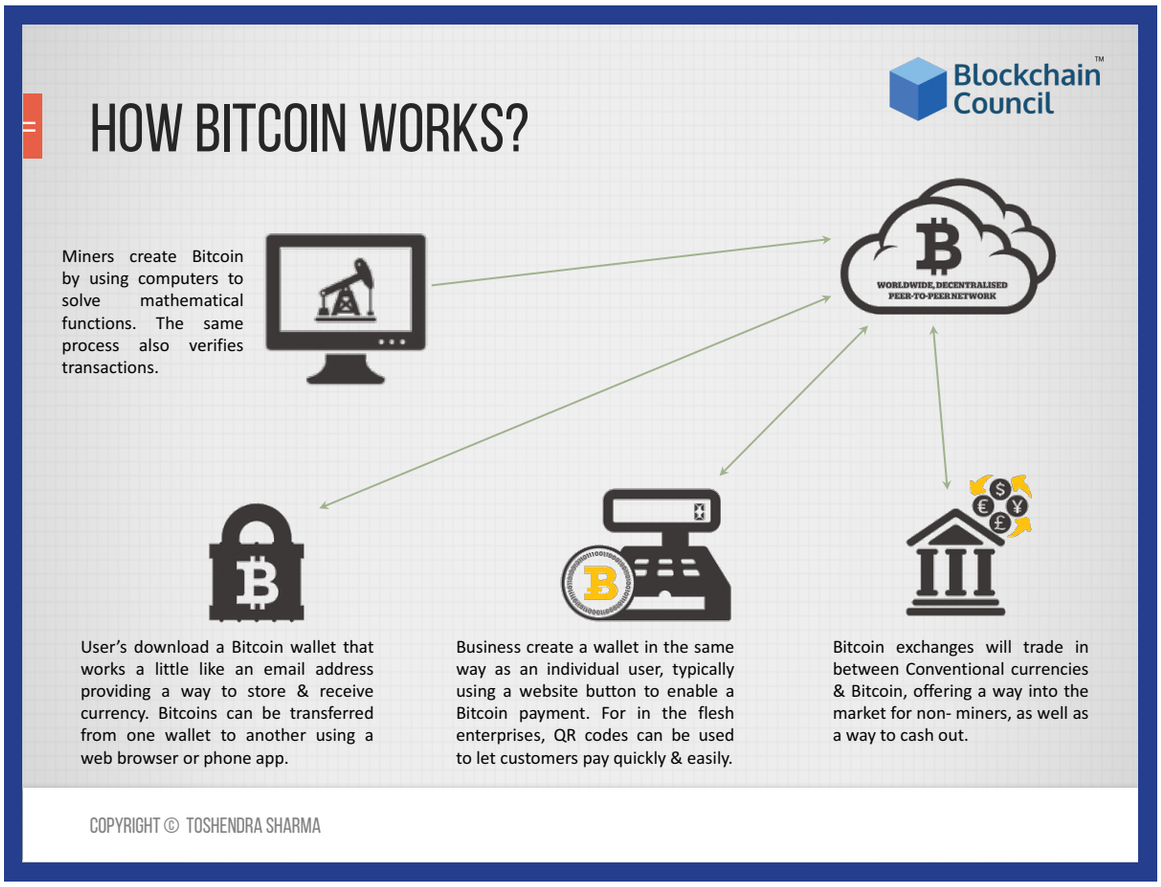
Employees and employers can use Bitwage to reduce costs, increase visibility into the payment process and increase the speed of international wage payments. Bitwage is located in San Francisco, California.

In our following section, we'll try to understand the working of Bitcoin and the units used for calculating the price of Bitcoin.

CHAPTER 9

Bitcoin Working and it's Units





Firstly, Bitcoin can receive or send any amount of money. It can be from anyone and anywhere across the globe at a very minimal cost. Secondly, Bitcoin creates a wallet, which can be installed on mobile phone or computer. It is accessible and easy to operate.

It has two essential ingredients called an address and a key. The address is a public part of a Bitcoin. It is normally 27 to 34 characters where money is either received or sent. The key is the private part, which is cryptographed and is used to sign a transaction. The key also prevents the transaction to be altered once initiated.

Let's try to understand it with the help of the previous diagram.

Bitcoin is a worldwide acceptable and a decentralized peer-to-peer network or a trending cryptocurrency. It is created by miners who are computers or processing units or person solving a mathematical puzzle which is hard enough, to generate Bitcoins and to get it circulated in the market.

It also verifies previous transactions.

Now, these generated Bitcoins are available for circulation in the market for buying, selling, making other payments for business or trading, etc.

Here comes the role of Bitcoin wallets and Bitcoin trading exchanges.

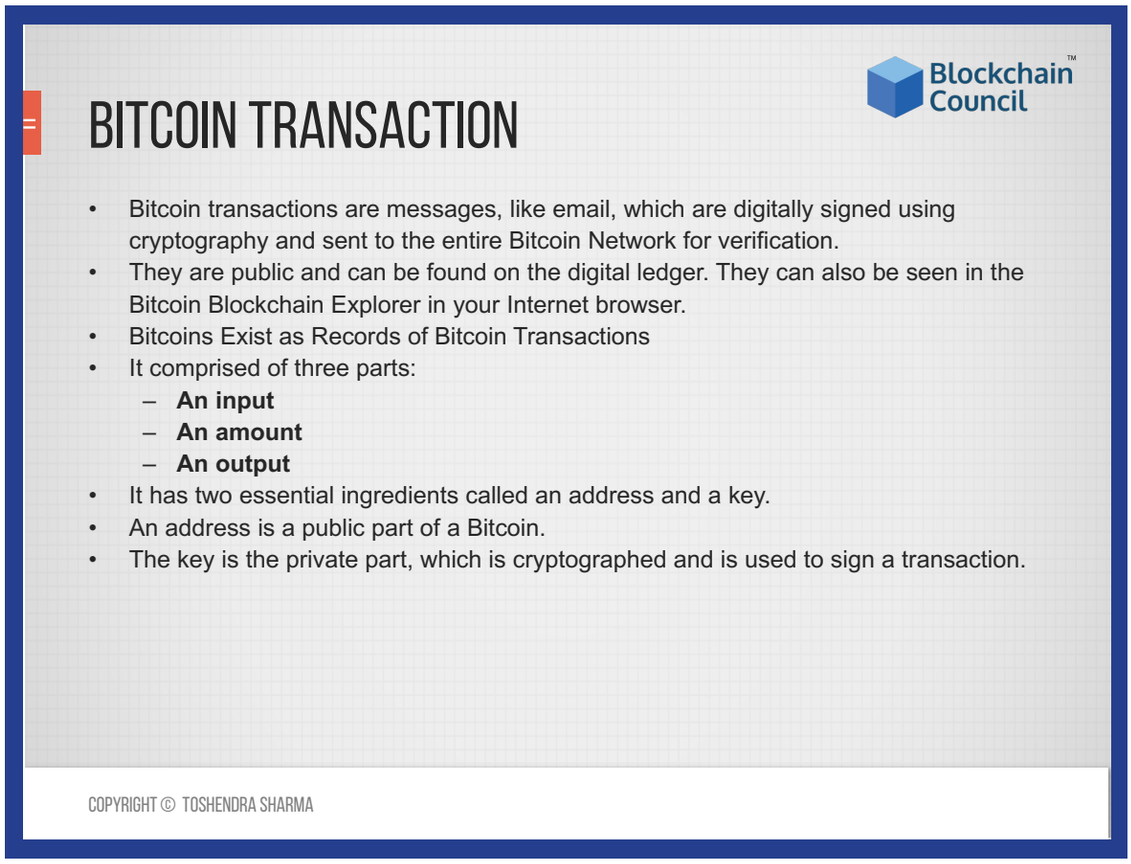
Users download a Bitcoin wallet that works like an email address providing a way to store and receive currency. Bitcoins can be transferred from one wallet to another using a web browser or phone app.

Another way involves Business to create a wallet in the same way as an individual user, typically using a website button to enable a Bitcoin payment. For in the flesh enterprises, QR codes can be used to let customers pay quickly and easily.

Lastly, there are Bitcoin Exchanges trading in between conventional currencies and Bitcoin, offering a way into the market for non-miners, as well as a way to cash out.

Thus, to make a successful transaction, a sender's address, a receiver's address, money and a key is required. Every new transaction is called a block, which is added to the public ledger forming a Blockchain. Every computer that writes a block or performs the transaction is called a miner.

Thus, Bitcoin is a new way of making payments. It has paved a new platform for a cashless economy. It can be rightly called as digital revolution.



Coming up to Bitcoin Transaction

According to Satoshi Nakamoto's, Bitcoin Whitepaper

"Bitcoins Exist as Records of Bitcoin Transactions".

We define a Bitcoin as a chain of digital signatures. Each owner transfers Bitcoin to the next by digitally signing a hash of the previous transaction and the public key of the next owner and adding these to the end of the coin. A payee can verify the signatures to confirm the chain of ownership.

It's worth mentioning here that Bitcoins do not "exist" per se. That's right! Those BTC in your wallet does not explicitly exist the way cash, coins or even stocks do. There are no physical Bitcoins anywhere—not on a hard-drive or a spreadsheet or a bank account and not even on a server anywhere.

Think of the Blockchain as a record of the transactions between various Bitcoin addresses. These transaction records are updated by the Bitcoin network and shared across each of its nodes as balances increase and decrease. You can even use one of our Bitcoin.com tools if you want to see the history as well as the current balance of any given Bitcoin address. Simply enter a Bitcoin address to explore its entire history.

So, let's understand the Bitcoin transactions with the help of an example. Suppose Mark wants to send some Bitcoin to Jessica. Essentially, a Bitcoin transaction is comprised of three parts:

"an input" which is a record of the Bitcoin address from which Mark initially received the Bitcoin and wishes to send to Jessica.

"an amount" which is the specific amount of BTC, Mark wants to send Jessica and

"an output" which is Jessica's public key; also known as her 'Bitcoin address'.

How does a Bitcoin transaction work?

Sending Bitcoin requires having an access to the public and private keys associated with that amount of Bitcoin.

When we talk about someone "having Bitcoins" what we mean is that person has an access to a key-pair comprised of a public key to which some amount of Bitcoin was previously sent and the corresponding unique private key which authorizes the BTC previously sent to the above pub-key to be sent elsewhere.

Public keys, also called as Bitcoin addresses, are random sequences of letters and numbers that function similarly to an email address or a social-media site username. They are public so you are safe sharing it with others. In fact, you must give your Bitcoin address to others whenever you want them to send you BTC.

The private key is another sequence of letters and numbers. However, private keys—like passwords to email or other accounts, are to be kept secret. Never share your private key with anyone whom you do not trust. Also, remember to backup private keys with pen and paper and store them somewhere safe.

Your Bitcoin address is basically a transparent safe. Others can see what's inside, but only those with the private key can unlock the safe to access the funds within.

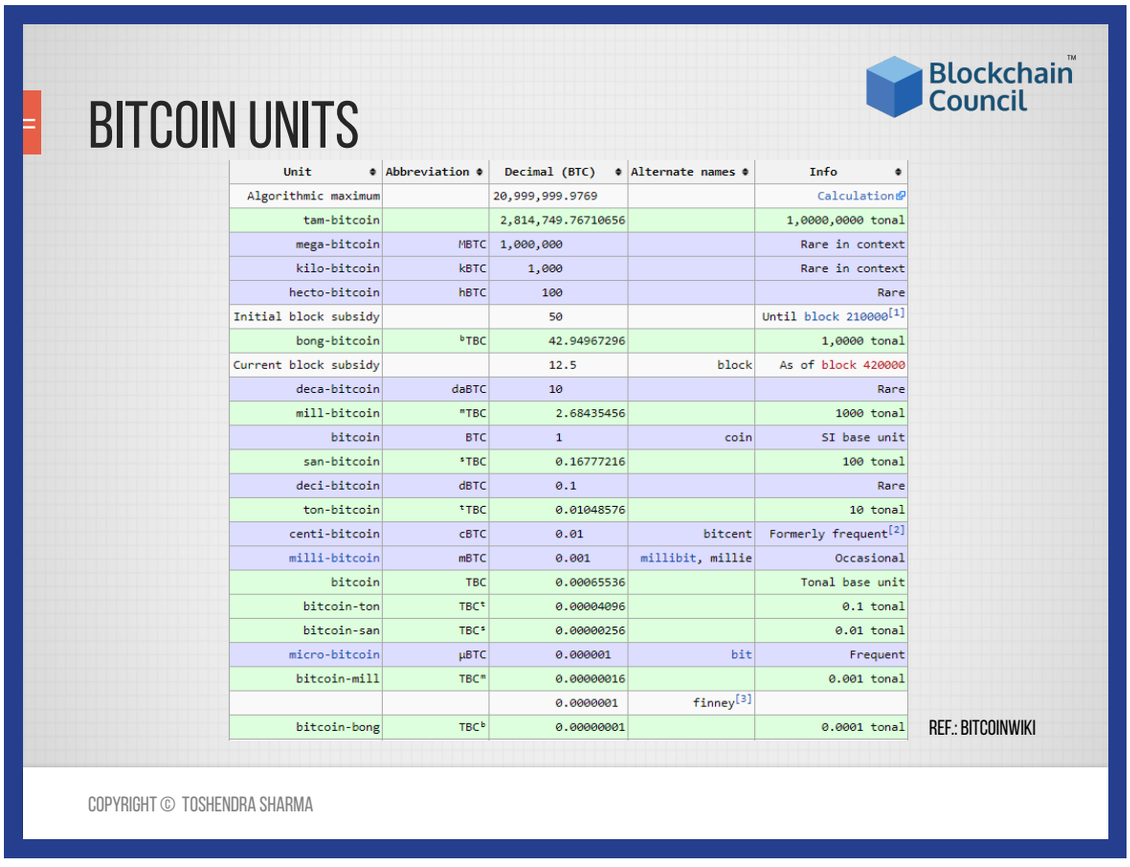
In the above example transaction, Mark wants to send some Bitcoins to Jessica. To do this, he uses his private key to sign a message with the transaction-specific details. This message is then sent to the Blockchain and contains, firstly, an input which is the source transaction of the coins previously sent to Mark's address, secondly, some amount of BTC to be sent from Mark to Jessica and for last an output which is Jessica's public address.

This transaction is then broadcasted to the Bitcoin network where miners verify that Mark's keys are able to access the inputs, i.e., the address from where he previously received BTC he claims to control. This confirmation process is known as mining because it requires resource-intensive computational labor and rewards miners, in BTC, per block solved. This is also the process by which new Bitcoins are 'created.'

You must be wondering that why some Bitcoin transaction confirmations take so long?

To answer that we need to understand that all Bitcoin transactions must be verified by miners on the Blockchain. Note, miners don't mine transactions; they mine blocks which are collections of transactions. Sometimes your transaction gets left out of the current block and gets put on hold until the next one is assembled. The Bitcoin protocol dynamically adjusts requirements to have each block take approximately 10 minutes to mine.

Another reason for long confirmation time is that blocks are limited to 1MB by the current Bitcoin protocol. This arbitrary limit can be increased, but for the present, it limits the amount of transactions that may enter a block which effectively slows down confirmation time and by extension of the entire Bitcoin network.



Unit	Abbreviation	Decimal (BTC)	Alternate names	Info
Algorithmic maximum		20,999,999.9769		Calculation
tam-bitcoin		2,814,749.76710656		1,0000,0000 tonal
mega-bitcoin	MBTC	1,000,000		Rare in context
kilo-bitcoin	kBTC	1,000		Rare in context
hecto-bitcoin	hBTC	100		Rare
Initial block subsidy		50		Until block 210000[1]
bong-bitcoin	ᵇTBC	42.94967296		1,0000 tonal
Current block subsidy		12.5	block	As of block 420000
deca-bitcoin	daBTC	10		Rare
mill-bitcoin	ᵐTBC	2.68435456		1000 tonal
bitcoin	BTC	1	coin	SI base unit
san-bitcoin	ˢTBC	0.16777216		100 tonal
deci-bitcoin	dBTC	0.1		Rare
ton-bitcoin	ᵗTBC	0.01048576		10 tonal
centi-bitcoin	cBTC	0.01	bitcent	Formerly frequent[2]
milli-bitcoin	mBTC	0.001	millibit, millie	Occasional
bitcoin	TBC	0.00065536		Tonal base unit
bitcoin-ton	TBCᵗ	0.00004096		0.1 tonal
bitcoin-san	TBCˢ	0.00000256		0.01 tonal
micro-bitcoin	µBTC	0.000001	bit	Frequent
bitcoin-mill	TBCᵐ	0.00000016		0.001 tonal
		0.0000001	finney[3]	
bitcoin-bong	TBCᵇ	0.00000001		0.0001 tonal

Now we will learn about units used for measuring Bitcoins.

Most commonly, units of Bitcoin are expressed in decimal exponents such as BTC ("Bitcoins"), mBTC ("milliBitcoins") and µBTC ("bits").

The BTC unit was chosen to represent a value of 10 to the power of 8, to give sub-unit precision rather than large whole numbers. It allows for divisions of 1/10th (deci-Bitcoins, dBTC), 1/100th (centi-Bitcoins, cBTC), 1/1 000th (milli-Bitcoins, mBTC), and 1/1 000 000 (micro-Bitcoins, µBTC).

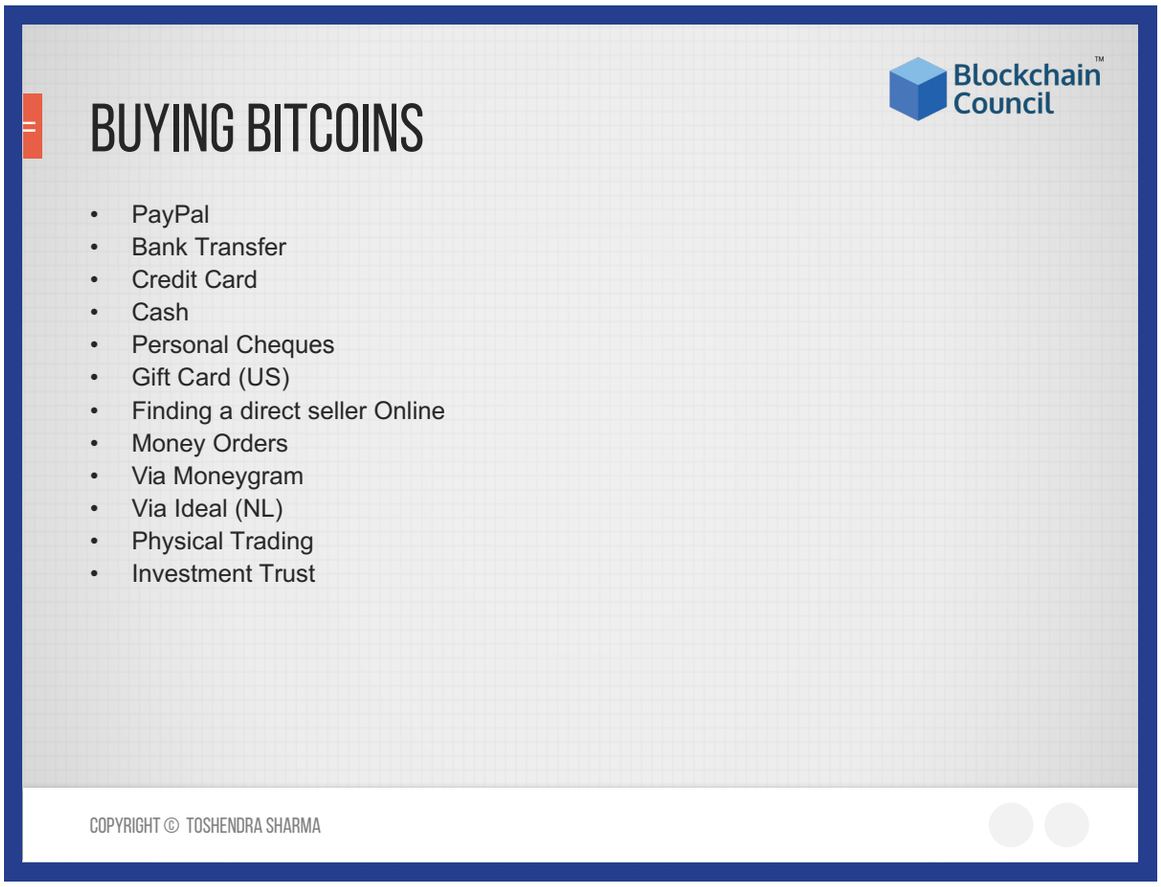
As shown in the chart above, one milli-Bitcoin is the one by thousandth part of 1 Bitcoin while one micro-Bitcoin is equivalent to ten to the power of minus six value of a single Bitcoin.

Hence, these units are designed to give exact precision to the value of Bitcoin and so it can be bought even in small or decimal values as per the need. It is created to make easy trading and payments possible through Bitcoins.

In the next chapter we will understand how to buy Bitcoins.

CHAPTER 10

How to Buy Bitcoins?



For starting with trading or making payments through Bitcoins, you initially need to own one. One can buy Bitcoins from many exchanges present all over the globe through various ways.

Some ways through which one can buy Bitcoins are :

- PayPal

One can't directly buy Bitcoins using PayPal, because it is risky for the seller and therefore few sellers will offer this. There are basically three reasons for that:

The buyer of Bitcoins can always perform a chargeback, and there is no way for the seller to contest that.

Second, there are many hacked accounts and when PayPal realizes that such an account has been fraudulently used, they will also perform a chargeback.

And thirdly, PayPal doesn't like Bitcoins, as the Bitcoins network is in direct competition to it. They will ban accounts that have anything to do with Bitcoins and freeze their balance.

Through bank transfers, personal cheques (as expresscoin.com allows customers to buy Bitcoins with a personal cheque), through cash as Local Bitcoins allows sellers and buy-ers who are located nearby to meet and exchange Bitcoins through various methods including cash, wire transfer, money bookers, skrill and more. Local Bitcoins offers a Bitcoins escrow service that holds the funds until the transaction is complete, therefore reducing fraud.

- one can also use credit card to buy Bitcoins.

Cubits is an all-inclusive platform to buy, sell and accept Bitcoins.

Their easy-to-use interface allows users to buy and sell Bitcoins instantly with 17 supported currencies. Visa and Mastercard are also accepted.

VirWox: The Virtual World Exchange accepts all major credit cards via Paypal or Skrill and allows one to buy Second Life Lindens which one can then trade to Bitcoins. Using this method is faster than most options but has larger transaction fee involved.

One can also buy through gift card, by finding a direct seller online, by money orders, via Moneygram, via Ideal, through physical trading and investment trust.

Buying Bitcoins involve a major step of finalizing the exchanges according to one's choice. Hence, now we'll see some of the major Bitcoins Exchanges.

Some famous exchanges are Coinbase, Coinmama, Bitpanda and CEX.io.

Many other exchanges are also present in the market, but these are the most famous and have gained people's trust over time. So, let's have a detailed look at them.

Starting with Coinbase, it is the world's largest Bitcoins broker. At Coinbase one can buy up to $150 or €150 of Bitcoins per week instantly with a credit or debit card in:

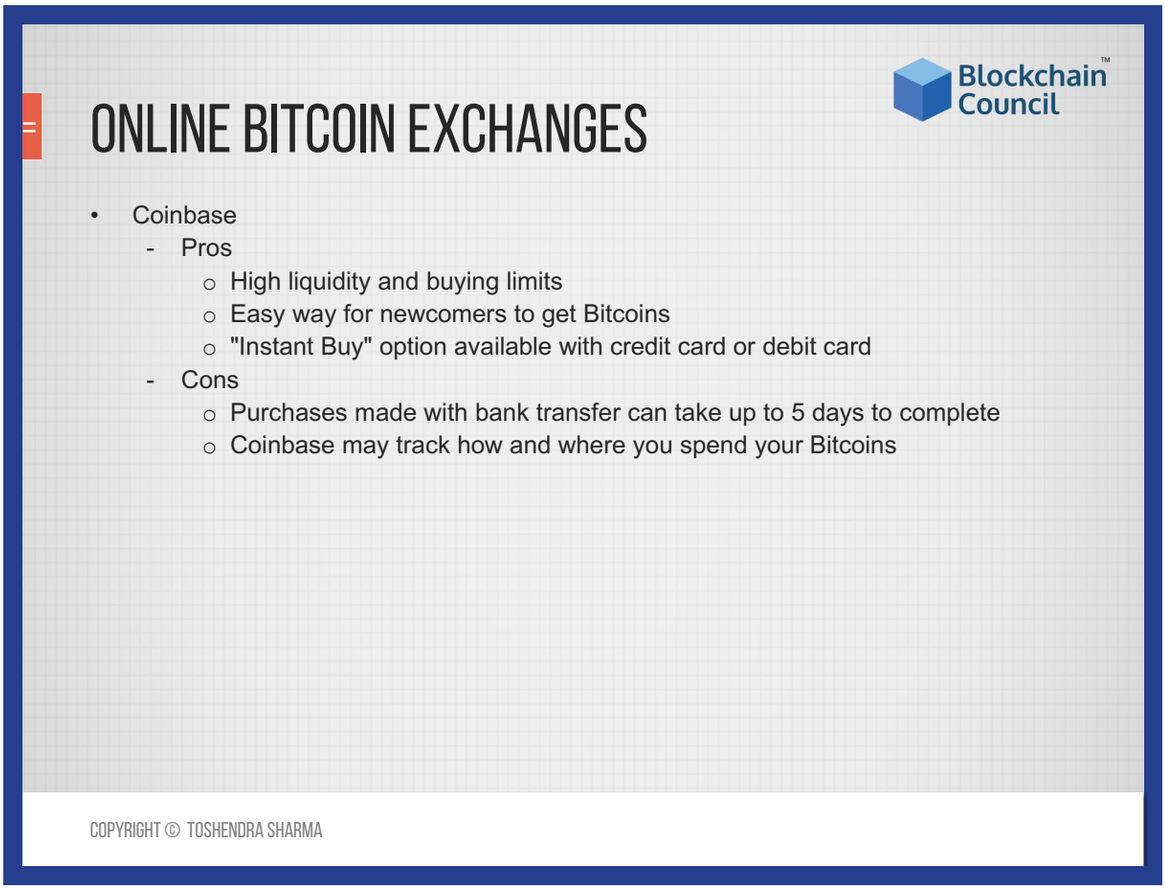
- The United States
- Canada

- Europe
- United Kingdom
- Australia
- Singapore

Coinbase charges a flat 3.99% fee on all purchases via credit or debit card, which is among the lowest for European and US customers.

Here's, a quick step-by-step guide on how to buy Bitcoins with a credit card on Coinbase:

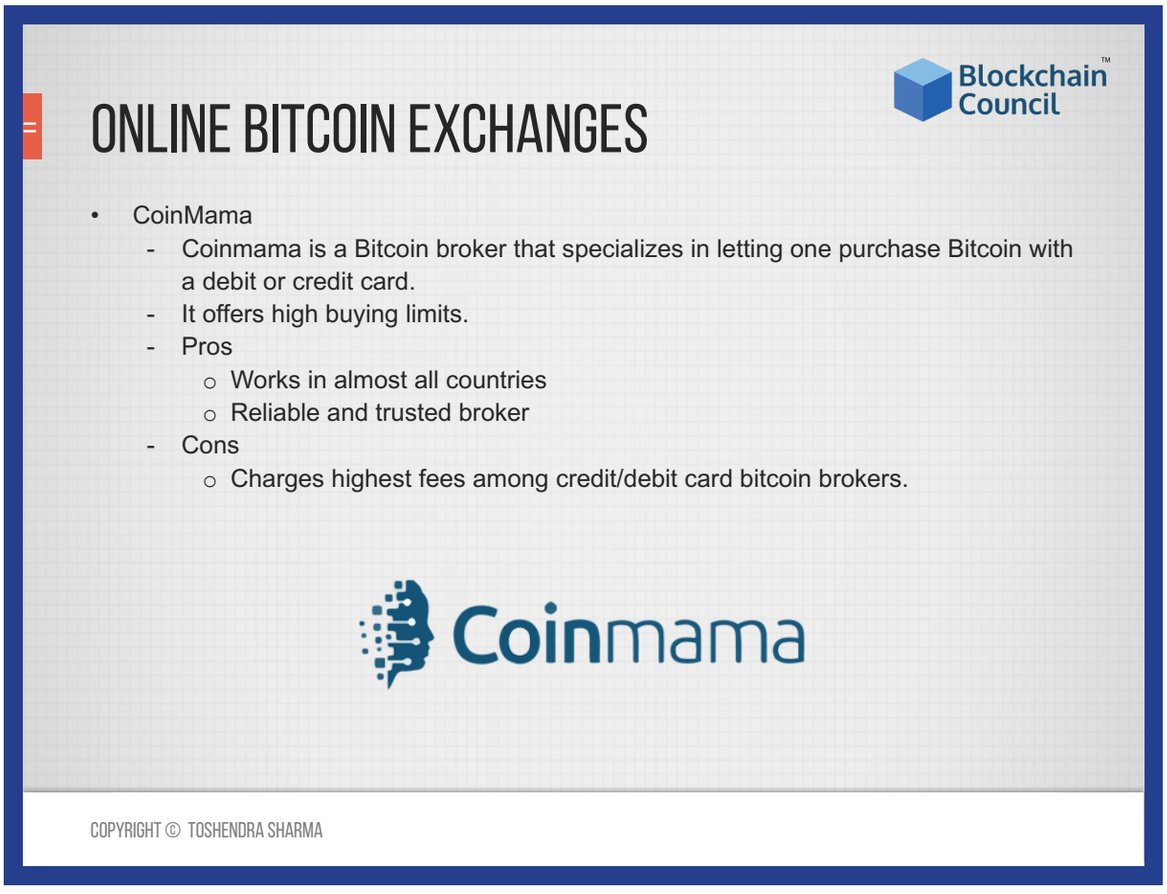
1. Create your account on Coinbase.
2. Add your credit card to your Coinbase profile
3. Verify your ID with Coinbase.
4. Start buying Bitcoins using your credit card.



Everything has certain pros and cons associated with it. Coinbase has high liquidity and buying limits, has easy way for newcomers to get Bitcoins and an "instant buy" option is available with credit or debit card.

Whereas on the other hand, there are some limitations as well:

Purchases made with bank transfer can take up to 5 days to complete and Coinbase can also track how and where you spend your Bitcoins.



Let's see the aspects behind Coinmama.

Coinmama is a Bitcoin's broker that specializes in letting one purchase Bitcoins with a debit or credit card.

You'll be charged 6% fee due to the risks and processing fees that comes with credit card payments.

Coinmama offers high limits. One can buy up to:

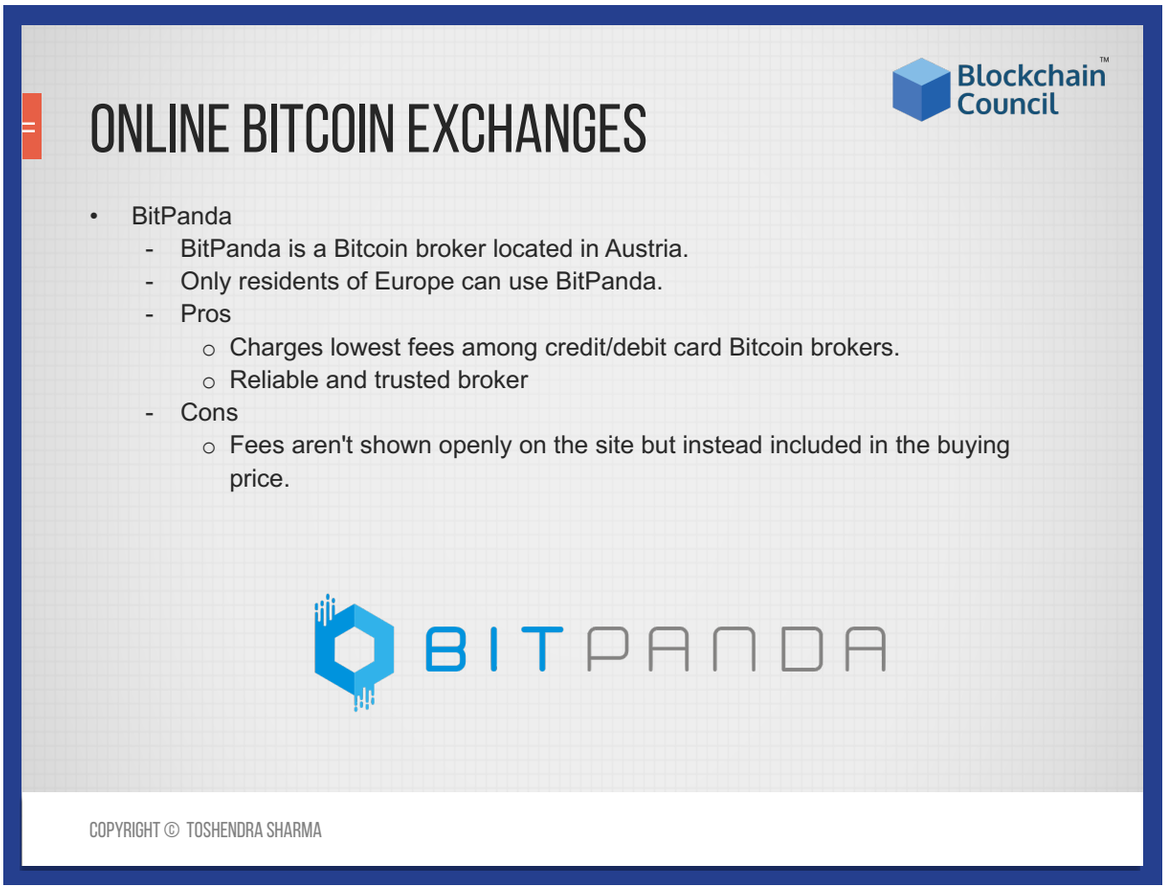
- $5,000 worth of Bitcoins per day and
- $20,000 worth of Bitcoins per month

PROS associated with Coinmama are:

- It works in almost all countries
- Has highest limits for buying Bitcoins with a credit card and is a reliable and trusted broker.

CONS associated with Coinmama are:

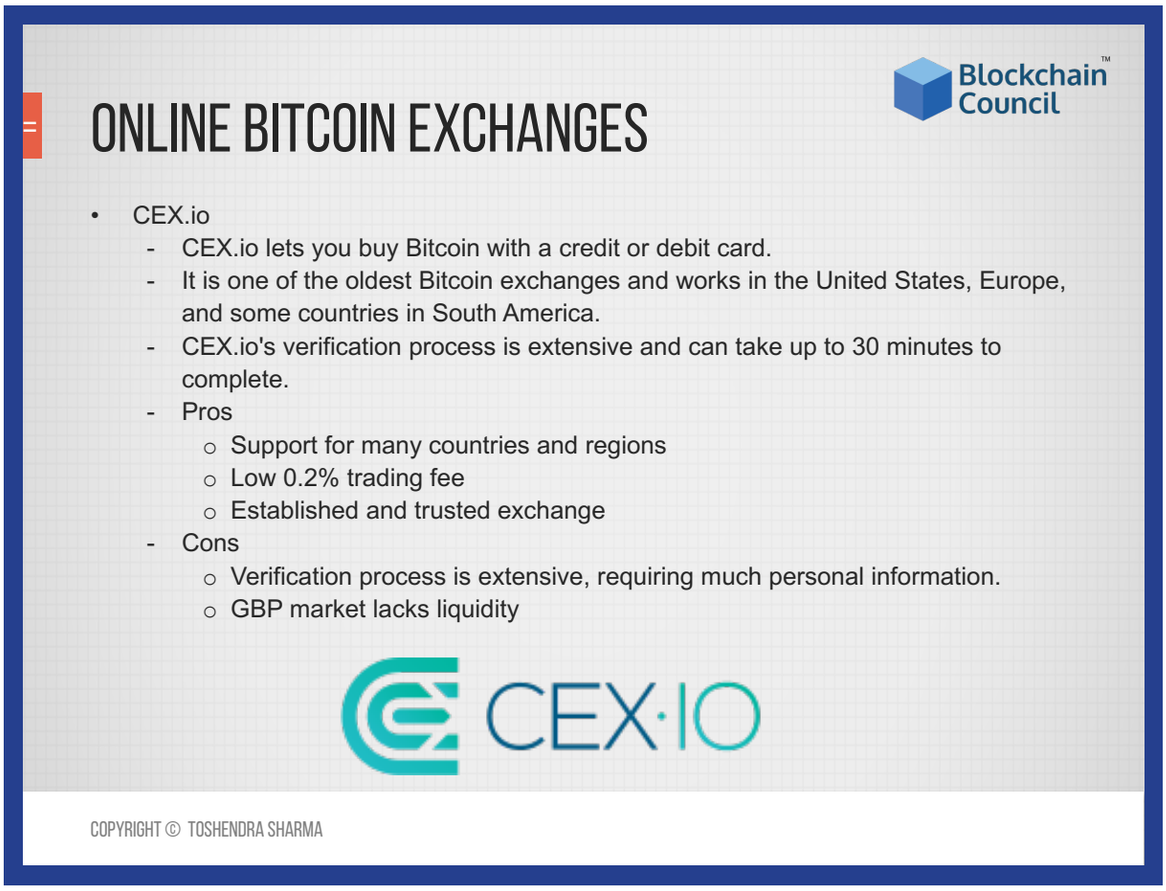
- It has the highest fees among credit or debit card Bitcoins brokers.



Let's know more about BitPanda.

BitPanda is a Bitcoin's broker located in Austria allowing one to purchase coins with a credit or debit card for 3-4% fees. Only residents of Europe can use BitPanda.

- It offers a low fees for buying Bitcoins with credit or debit card and is also a reliable and trusted broker though its fees aren't shown openly on the site but are included in the buying price.



Switching to CEX.io:

It lets you buy Bitcoins with a credit or debit card and is one of the oldest Bitcoins exchanges and works in the United States, Europe and some countries in South America.

CEX.io's verification process is extensive and can take up to 30 minutes to complete.

Its PROS includes support to many countries and regions with as Low as 0.2% trading fee and is an established and trusted exchange.

But to list a few cons, its verification process is extensive, requiring much personal information (including a photo) and incurs a long delay. Its GBP market also lacks liquidity.

LOCALBITCOINS.COM

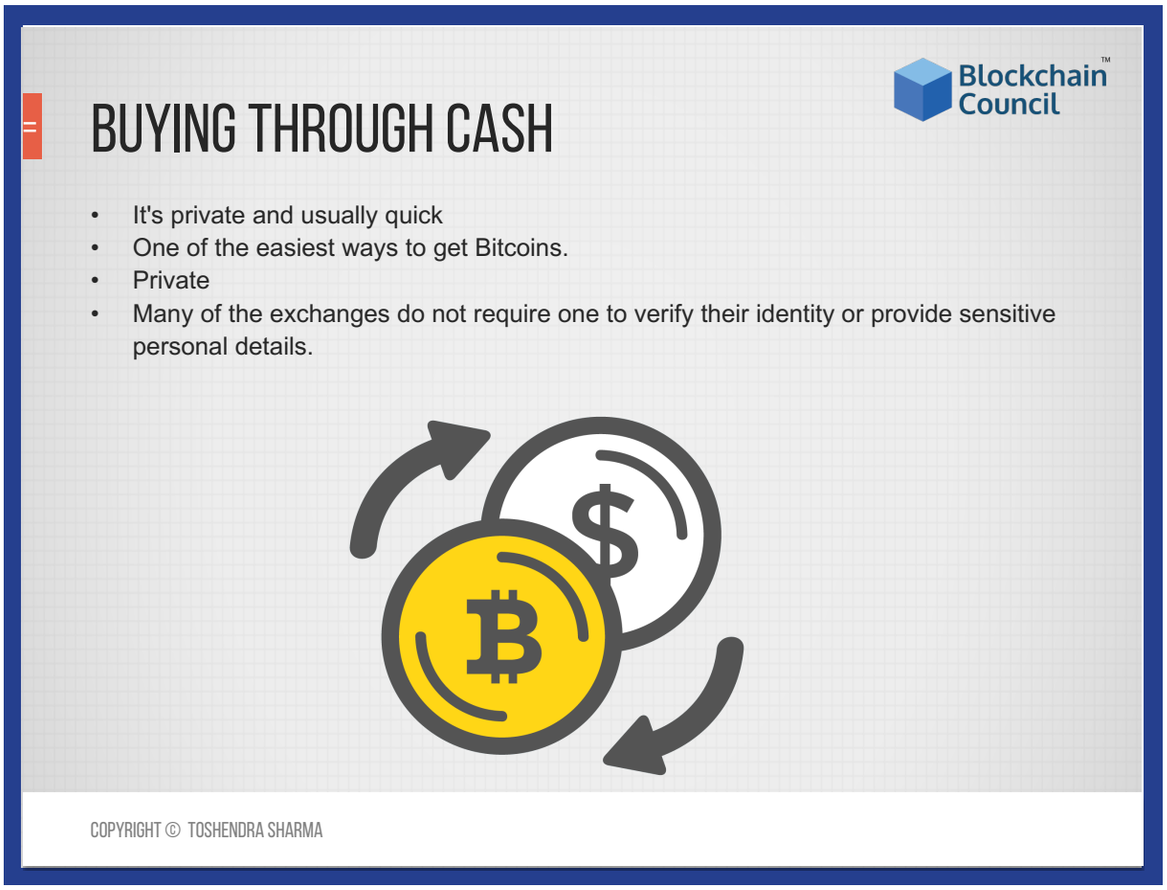
Blockchain Council™

- LocalBitcoins is a Bitcoin start-up company based in Helsinki, Finland founded in June, 2012.
- Its service facilitates over-the-counter trading of local currency for Bitcoins.
- Users post advertisements on the website, where they state exchange rates and payment methods for buying or selling Bitcoins.
- Other users reply to these advertisements and agree to meet the person to buy Bitcoins with cash or pay with online banking.
- The website offers a service to facilitate the locating of other Bitcoin users can meet others for person to person trading of Bitcoin.
- Suggested for casual traders seeking more privacy.

LocalBitcoins.com
Bringing Bitcoin Everywhere

Local Bitcoins is another very trending way of buying Bitcoins, apart from credit or debit cards.

LocalBitcoins is a startup company based in Helsinki, Finland. Its service facilitates "over-the-counter" trading of local currency for Bitcoins. Users post advertisements on the website, where they state exchange rates and payment methods for buying or selling Bitcoins. Other users reply to these advertisements and agree to meet the person to buy Bitcoins with cash or online banking. LocalBitcoins has a reputation and feedback mechanism for users and an escrow and conflict-resolution service. As of December 2013, LocalBitcoins has around 110,000 active traders with a trading volume of 1400–3000 Bitcoins per day. The website offers the service to facilitate the location, where bitcoin users can meet and carry on the trading of Bitcoins.The site is suggested for casual traders seeking more privacy and uses an escrow system and the transfer of Bitcoins is made after funds are received in the seller's account.



Let's have a quick overview on buying Bitcoins through cash.

Why one should buy Bitcoins through cash?

First of all, It is private and usually quick and secondly, it is one of the easiest ways to get Bitcoins.

For real, converting your cash to Bitcoins can get you Bitcoins within a couple of hours. Buying Bitcoins with cash is also private.

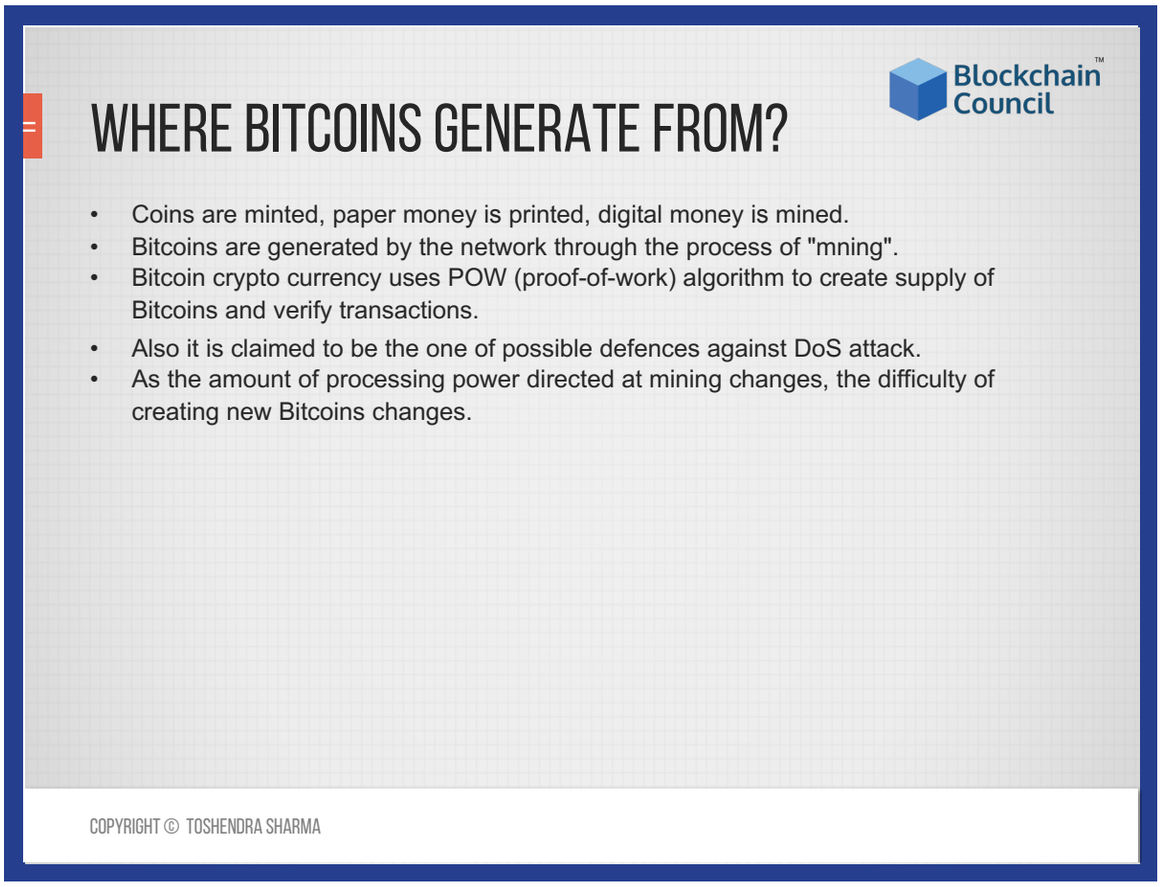
Many of the exchanges do not even require you to verify your identity or provide sensitive personal details.

Make sure you have a Bitcoins wallet before you buy since it's a prerequisite by some of the exchanges like, LocalBitcoins.com, BitQuick, Wall of Coins, LibertyX and Bitcoins ATM's.

Next, we'll learn about Bitcoins mining – what is it and what miner's do?

CHAPTER 11

Bitcoin Mining



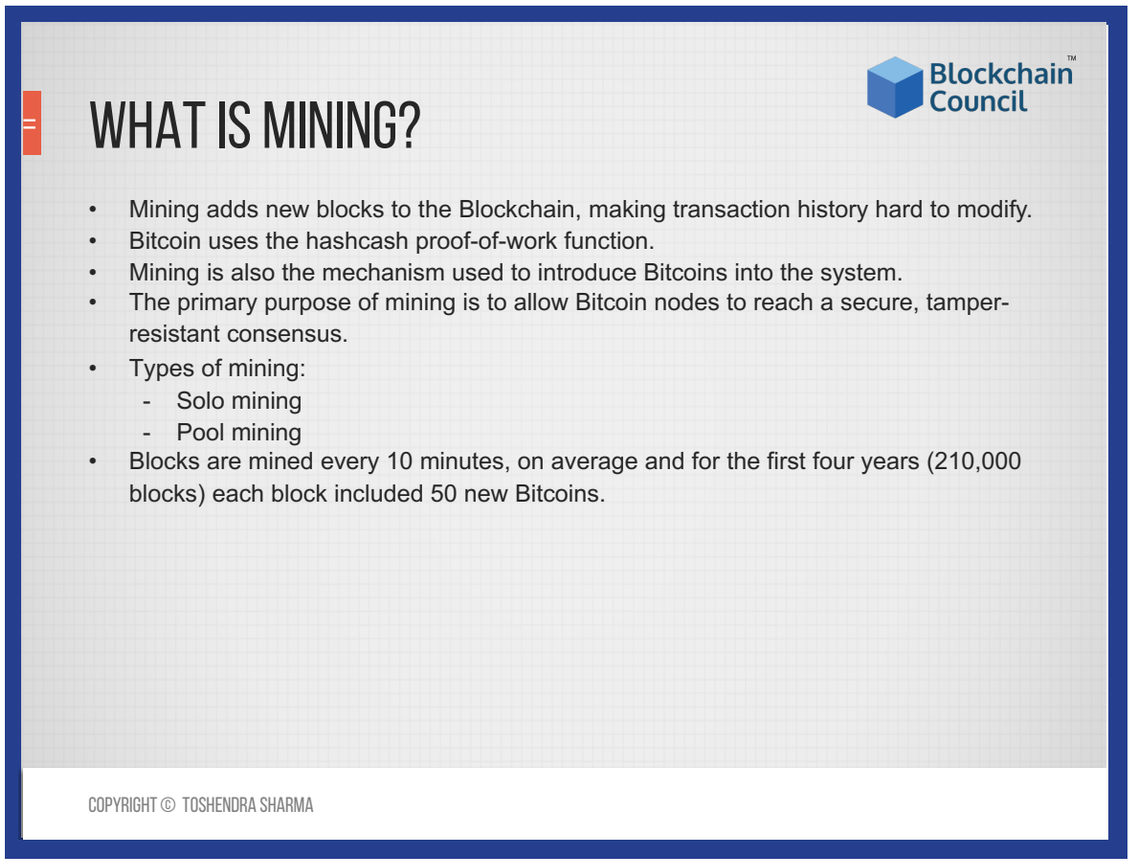
Let's start with knowing from where do Bitcoins generate?

Like coins are minted, paper money is printed, digital money is mined. The rules of how Bitcoin mining works are defined by the Bitcoin protocol and implemented in its software. Bitcoin cryptocurrency uses proof-of-work algorithm to create a supply of Bitcoins and verify transactions. Also, it is claimed to be one of the possible defence against DoS attack.

You'll be thinking, what is a DoS attack? In computing, a denial-of-service attack or DoS attack is a cyber-attack where the perpetrator seeks to make a machine or network resource unavailable to its intended users by temporarily or indefinitely disrupting services of a host connected to the Internet. Denial of service is typically accomplished by flooding the targeted machine or resource with superfluous requests in an attempt to overload systems and prevent some or all legitimate requests from being fulfilled.

Thus, to prevent it, the network demands from miners to prove that some work has been done by them, hence, the name, proof-of-work. The network gives a mathematical puzzle to miners which is difficult to solve but easy to verify computationally. The miner uses computational power to solve the stated math problem and to produce the valid block. After the challenge is completed, miner submits his work to other nodes' for validation to which in return the miner who found a block first gets a block reward and transaction fees included in this block.

Slide 3



What is Mining?

Mining adds new blocks to the Blockchain, making transaction history hard to modify. Mining is intentionally designed to be resource-intensive and difficult so that the number of blocks found each day by miners remains steady.

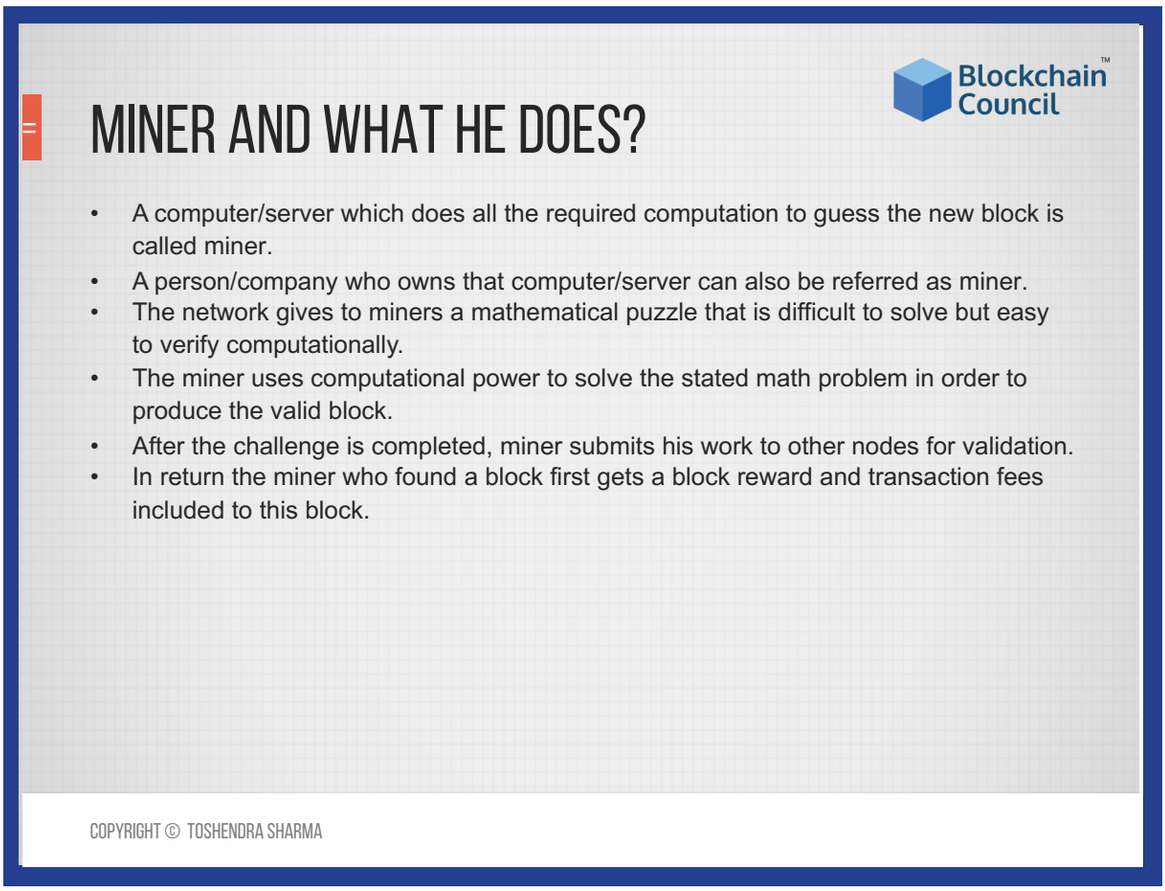
Individual blocks must contain a proof-of-work to be considered valid. This proof of work is verified by other Bitcoin nodes each time they receive a block. Bitcoin uses the "hashcash proof-of-work" function. The primary purpose of mining is to allow Bitcoin nodes to reach a secure, tamper-resistant consensus.

Mining is also the mechanism used to introduce Bitcoins into the system as Miners are paid transaction fees as well as a "subsidy" of newly created coins.

This both serves the purpose of disseminating new coins in a decentralized manner as well as motivating people to provide security for the system.

Mining today takes on two forms namely solo mining and pooled Mining.

Blocks are mined every 10 minutes on an average and for the first four years, i.e., 210,000 blocks, each block included 50 new Bitcoins.



Who is a miner and what he does?

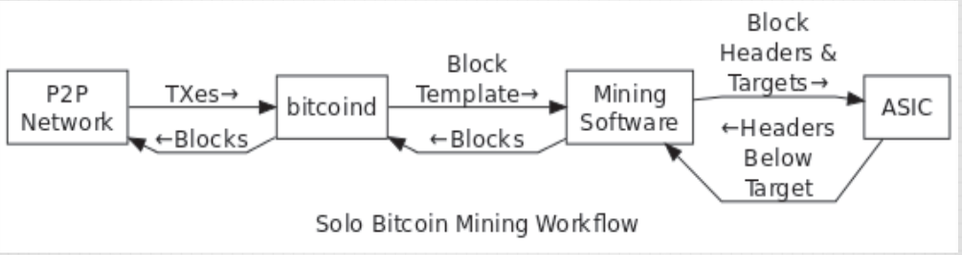
A computer or a server which does all the required computation to guess the new block is called miner. It can also be stated as a person or company who owns that computer/server. The Bitcoin cryptocurrency is the puzzle that miners need to solve which has a cryptographic proof-of-work hash function, i.e., SHA 256d.

It is a standard mathematical algorithm that converts input into output. Usually, it is really computationally-easy to get the output by putting the input into the function. For e.g., from 1+2+3+4 we get 10. But if we set the challenge vice versa knowing only the output we will have a number of different variants of inputs: 9+1, 8+2, 7+3, 6+4, 5+5, etc. The challenge in a mathematical puzzle is that miner needs to find such input that will satisfy the specific output. For solving the puzzle, a miner searches a block nonce. The one who finds it first is a winner.

The efficiency of miner depends on its speed in searching the right nonce.

SOLO MINING

- Miner attempts to generate new blocks on his own, with the proceeds from the block reward and transaction fees going entirely to himself, allowing him to receive large payments with a higher variance.
- Solo miners typically use ”bitcoind” to get new transactions from the network.



Solo Bitcoin Mining Workflow

Let’s discuss types of mining.

Solo mining, where the miner attempts to generate new blocks on his own, with the proceeds from the block reward and transaction fees going entirely to himself, allowing him to receive large payments with a higher variance, i.e., longer time between payments.

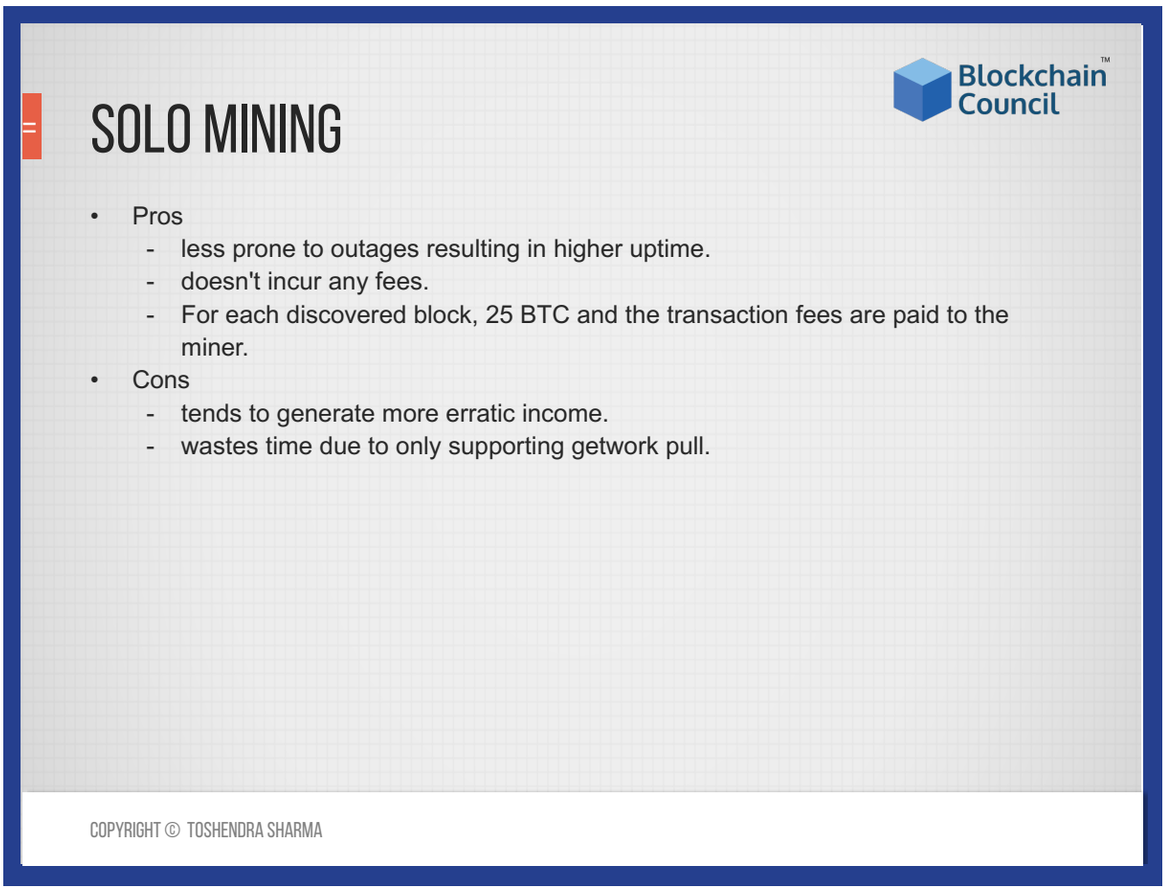
As illustrated in the diagram, solo miners typically use “Bitcoind” to get new transactions from the network. Their mining software periodically polls Bitcoind for new transactions using the getblocktemplate RPC, which provides the list of new transactions plus the public key to which the coinbase transaction should be sent.

The mining software constructs a block using the template and creates a block header. It then sends the 80-byte block header to its mining hardware along with a target threshold or the difficulty setting. The mining hardware iterates through every possible value for the block header nonce and generates the corresponding hash.

If none of the hash is the threshold, the mining hardware gets an updated block header with a new Merkle root from the mining software; this new block header is created by adding extra nonce data to the coinbase field of the coinbase transaction.

On the other hand, if a hash is found below the target threshold, the mining hardware returns the block header with the successful nonce to the mining software.

The mining software combines the header with the block and sends the completed block to Bitcoind to be broadcasted to the network for addition to the Blockchain.



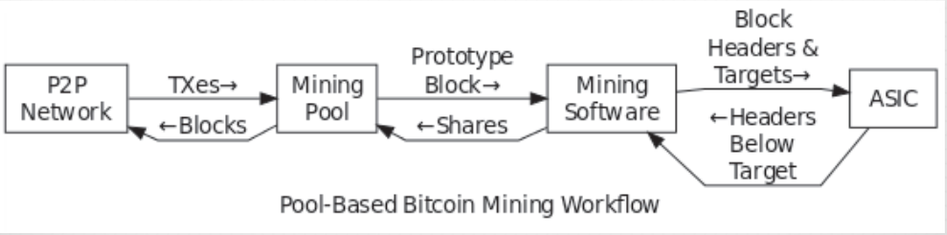
Features of Solo Mining are listed as following:

It is less prone to outages resulting in higher uptime and doesn't even incur any fees. For each discovered block, 25 BTC and the transaction fees are paid to the miner.

Solo Mining also has its associated cons with it. It tends to generate more erratic income and also wastes time due to only supporting get-work pull.

POOL MINING

- Miner pools resources with other miners to find blocks more often, with the proceeds being shared among the pool miners in rough correlation to the amount of hashing power they each contributed, allowing the miner to receive small payments with a lower variance.
- It allows mining pool operators to pay miners based on their share of the work done.



Pool-Based Bitcoin Mining Workflow

Coming to Pool mining, miner pools resources with other miners to find blocks more often, with the proceeds being shared among the pool miners in rough correlation to the amount of hashing power they each contributed, allowing the miner to receive small payments with a lower variance.

It allows mining pool operators to pay miners based on their share of the work done.

Pool miners follow a similar workflow, illustrated below, which allows mining pool operators to pay miners based on their share of the work done.

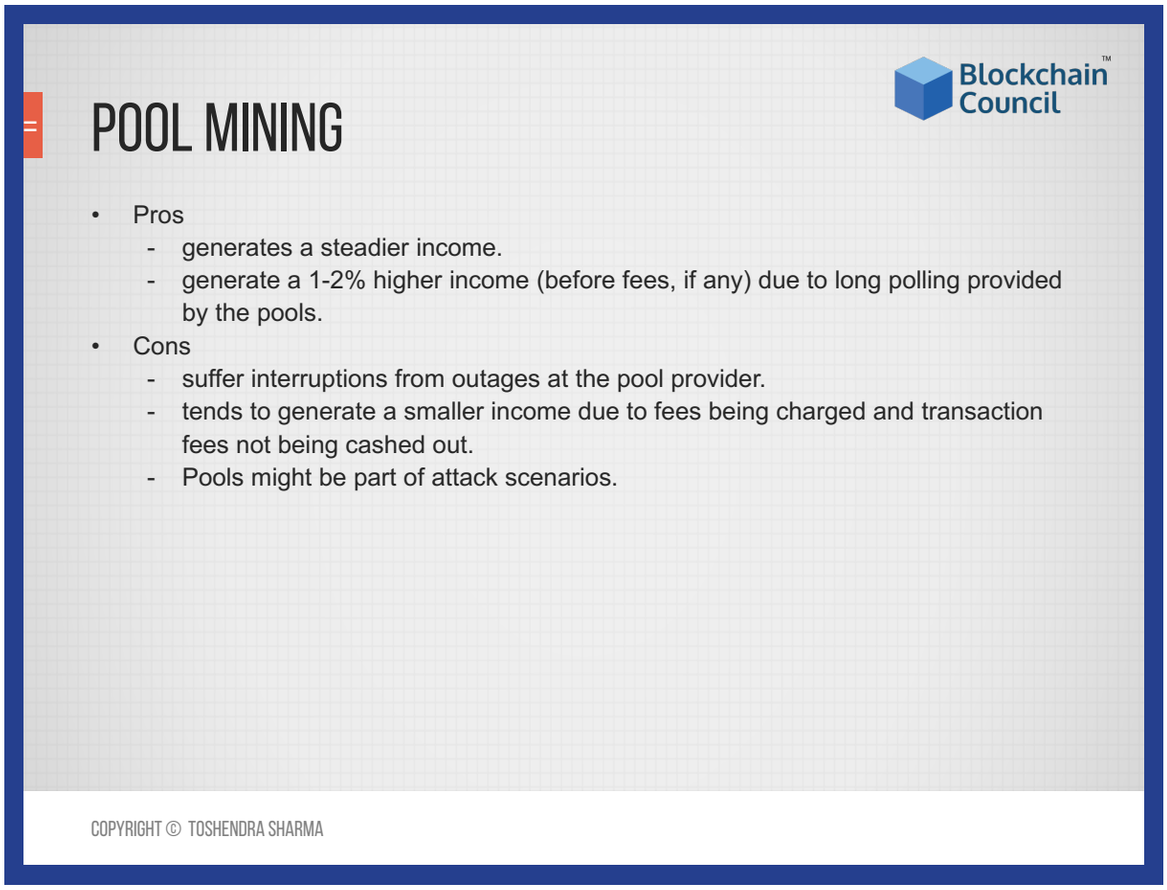
The mining pool gets new transactions from the network using Bitcoind. Each miner's mining software connects to the pool and requests the information it needs to construct block headers. In pooled mining, the mining pool sets the target threshold a few orders of magnitude higher which is less difficult than the network difficulty.

This causes the mining hardware to return many block headers which don't hash to a value eligible for inclusion on the Blockchain but which do hash below the pool's target, proving on average that the miner checked a percentage of the possible hash values.

The miner then sends to the pool a copy of the information the pool needs to validate that the header will hash below the target and that the block of transactions referred to by the header Merkle root field is valid for the pool's purposes. The information the miner sends to the pool is called a share because it proves the miner did a share of the work.

By chance, some shares the pool receives will also be below the network target; the mining pool sends these to the network to be added to the Blockchain. The block reward and transaction fees that come from mining that block are paid to the mining pool. The mining pool pays out a portion of these proceeds to individual miners based on how many shares they generated.

Different mining pools use different reward distribution systems based on this basic share system.



Pool mining has its own plus points.

- Pooled mining generates a steadier income and can generate a 1 to 2% higher income due to long polling provided by the pools.

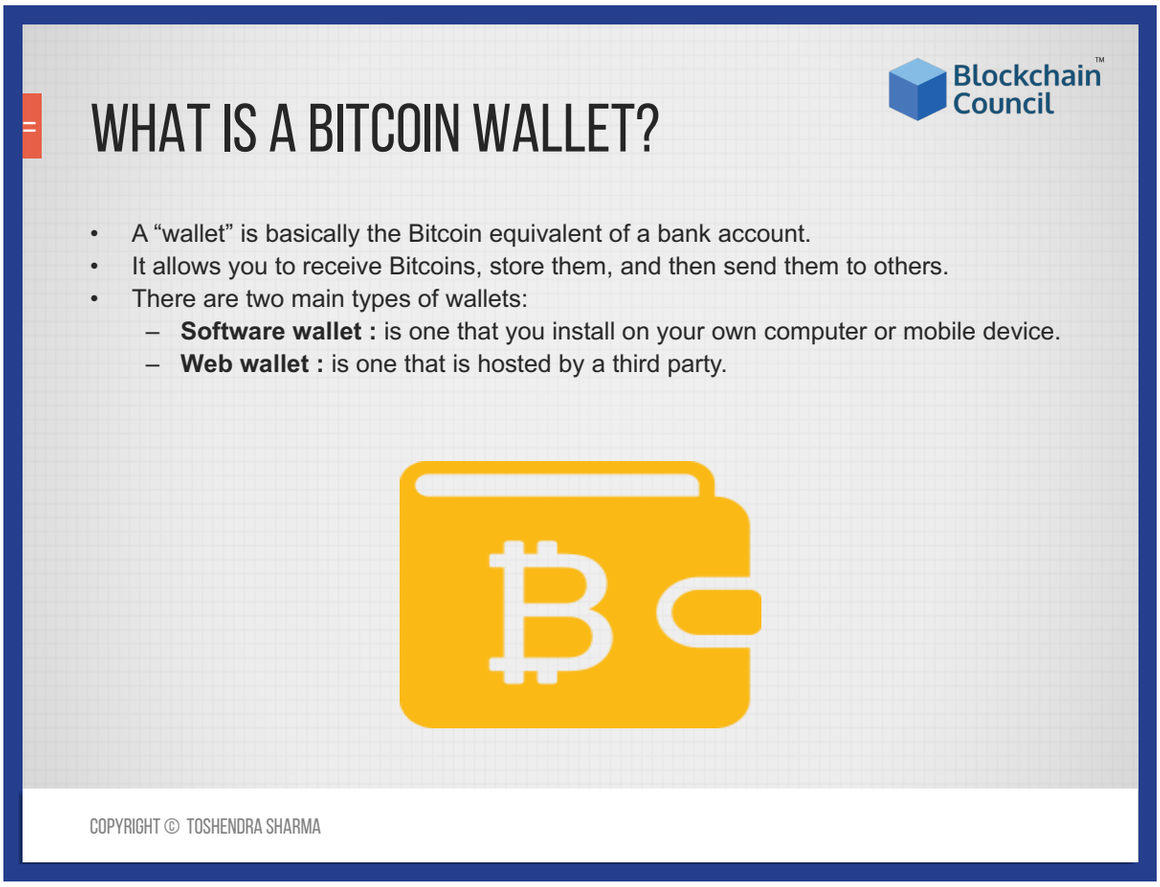
Pool mining cons includes:

- Pool mining can suffer interruptions from outages at the pool provider. Pools are subject to DOS attacks and have other downtimes, too. Backup pools and solo mining can be configured for these cases.
- Pooled mining tends to generate a smaller income due to fees being charged and transaction fees not being cashed out.
- There are zero fee pools. Until now, transaction fees are not cashed out by any pool.
- Pools might be a part of attack scenario.

Next, we will be learning about the various types of Bitcoin wallets and how to create your own wallet.

CHAPTER 12

Bitcoin Wallets



Let's understand what is a Bitcoin wallet?

A "wallet" is basically the Bitcoin equivalent of a bank account.

It allows you to receive Bitcoins, store them and send them to others. To be technically accurate, Bitcoins are not stored anywhere; there is a private key or a secret number for every Bitcoin address that is saved in the Bitcoin wallet of the person who owns the balance. So, basically, there are two main types of wallets.

A **software wallet** is one that you install on your own computer or mobile device. You are in complete control over the security of your coins, but they can sometimes be tricky to install and maintain.

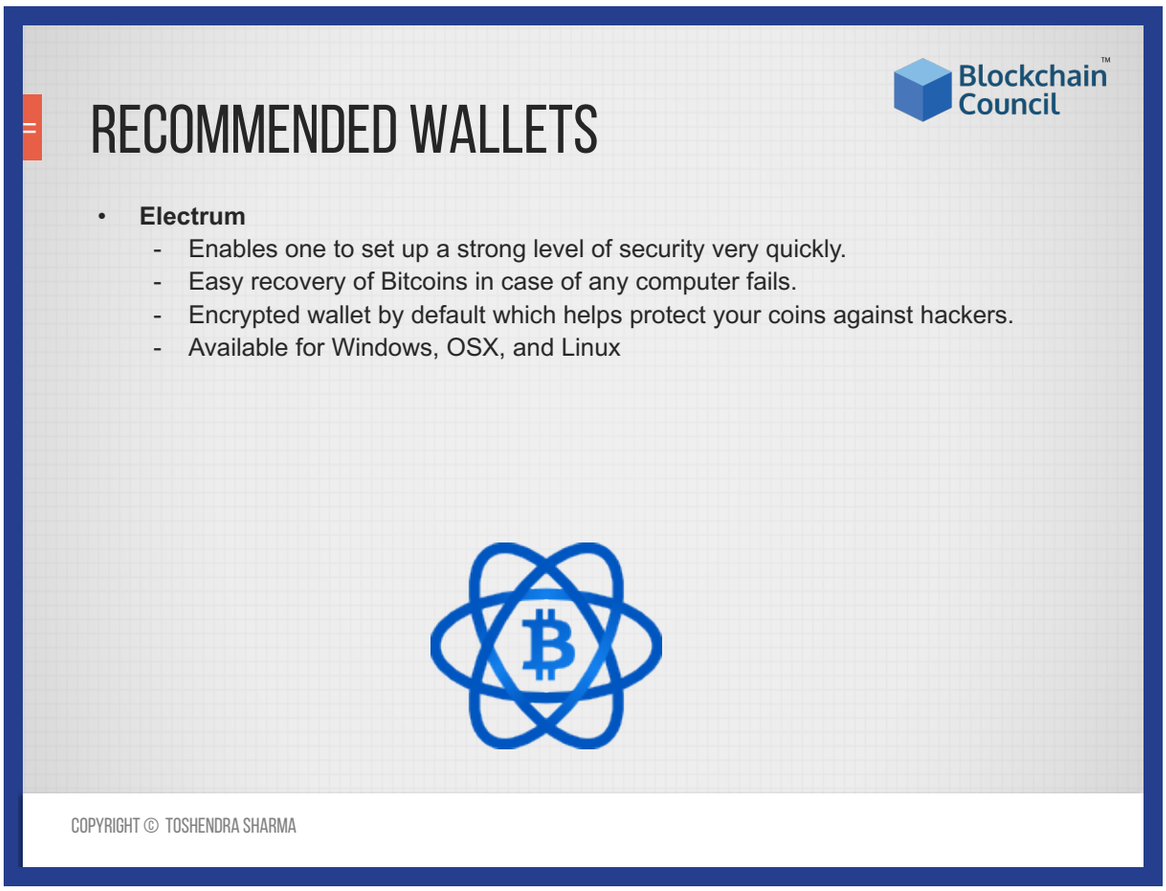
A **web wallet** or hosted wallet is one that is hosted by a third party. They are often much easier to use, but you have to trust the provider to maintain high levels of security to protect your coins.

Considering the fact of popularity and being user-friendly, there are four main wallets that are recommended:

Starting with Coinbase, which is the popular Bitcoin Wallet in the market and also is trusted by a lot of users. Coinbase is a web wallet with a simple design and some very useful features that makes it excellent for beginners. One can send and receive Bitcoins via email and buy and sell Bitcoins directly from Coinbase. A full-featured Android app enables access to all account functions on the go.

It's founders have a proven startup track record and have raised money from very prominent venture capitalists. This gives Coinbase a level of legitimacy unparalleled in the Bitcoin space.

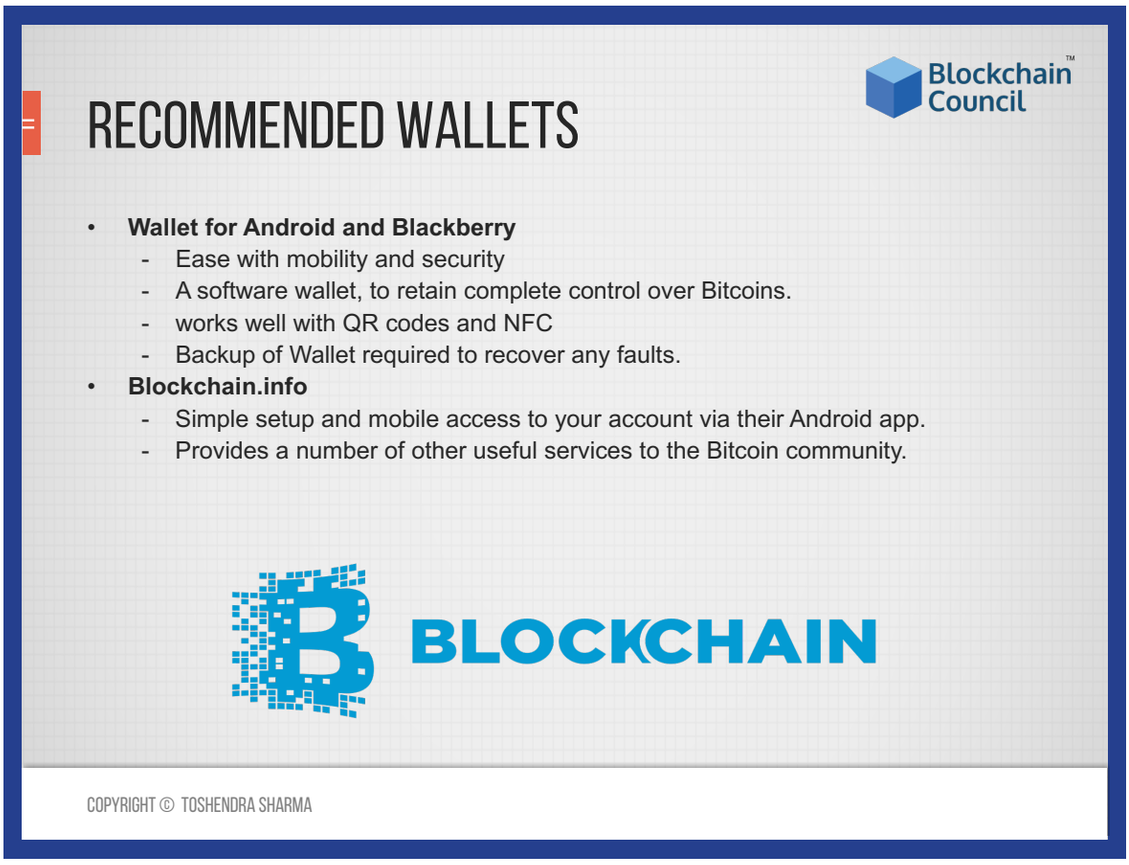
They are also one of the only large Bitcoin companies never to suffer a major hack.



Next in the list is Electrum. Electrum is a software wallet that enables you to set up a strong level of security very quickly.

During the simple installation process, you are given a twelve-word phrase that will allow you to recover all of your Bitcoins if your computer fails. Your wallet is also encrypted by default which helps protect your coins against hackers.

Electrum is available for Windows, OSX, and Linux.



Now let's consider Bitcoin wallets for Android and Blackberry.

For those looking for mobility and security, the simply-titled Bitcoin wallet mobile app is recommended. There is a version for both Android and BlackBerry OS. It is a software wallet and helps you to retain complete control over your Bitcoins.

It also works well with QR codes and NFC, making transferring coins to someone else's phone easier than writing a cheque.

But at the same time, be sure to backup your wallet with the included "Backup Wallet" feature or else you might risk losing all your coins the next time you get too close to a pool.

Another beautiful name in Bitcoin wallet is Blockchain.info.

It is another web wallet like Coinbase and provides a simple setup and mobile access to your account via their Android app.

They also provide some other useful services to the Bitcoin community.

Some other Bitcoin wallets are Armory which is a good choice for those requiring the high-est possible security, and the original Bitcoin-Qt client is also trusted and worth learning how to use.

PAPER WALLET

Blockchain Council

- Contains copies of the public and private keys that make up a wallet.
- The benefit of a paper wallet is that the keys are not stored digitally anywhere.
- Not subjected to cyber-attacks or hardware failures.
- Due to relative fragility of paper and easy degradation it can also seem disadvantageous to some.

Apart from software wallets, there is also an option available for maintaining paper wallets. A paper wallet is a document that contains copies of the public and private keys that make up a wallet. Often it will have QR codes so that you can quickly scan them and add the keys into a software wallet to make a transaction.

The benefit of a paper wallet is that the keys are not stored digitally anywhere and are therefore not subject to cyber-attacks or hardware failures.

The disadvantage of a paper wallet is that paper and ink can degrade and paper is relatively fragile, which is worth keeping well away from fire and water for obvious reasons. Furthermore, if you lose a paper wallet, you'll never be able to access the Bitcoins sent to its address.

For users of the Blockchain.info website, there is a basic paper wallet option. Click on the 'import/export' option, and look for the 'paper wallet' link on the left-hand side menu. A much more sophisticated option for your paper wallet can be found at Bitcoinpaperwallet.com. It offers a tamper-resistant design of paper wallet. It is also possible to order holographic labels to demonstrate that the wallet hasn't been tampered with. It also supplies a live-boot Ubuntu CD with paper-wallet software pre-installed.

Along with all its implications and way of using, you should always keep in mind of not allowing anyone to see you create your wallet.

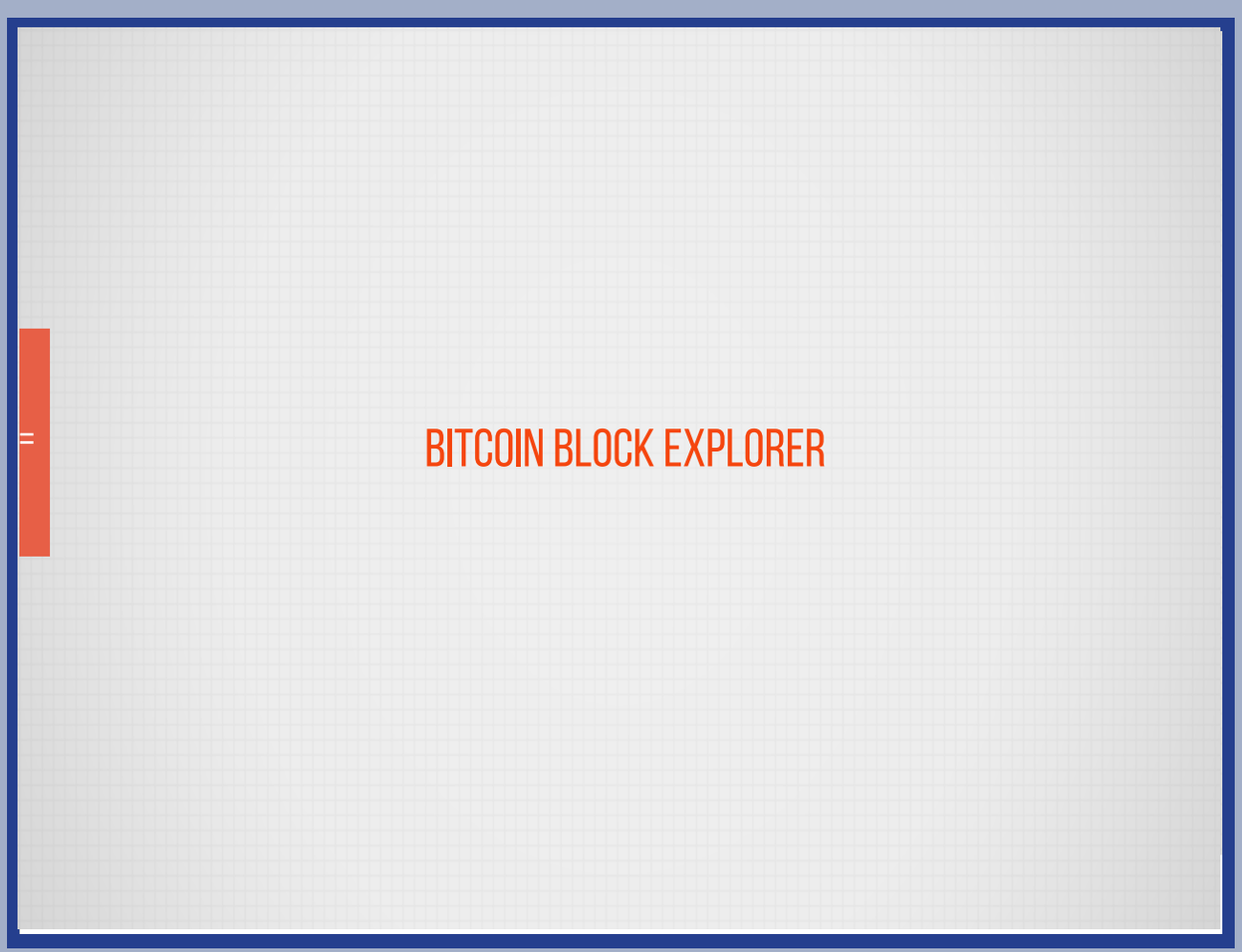
To rule out the risk of any spyware monitoring your activity, you should use a clean operating system. A good way to achieve this would be to create a USB flash drive or DVD with

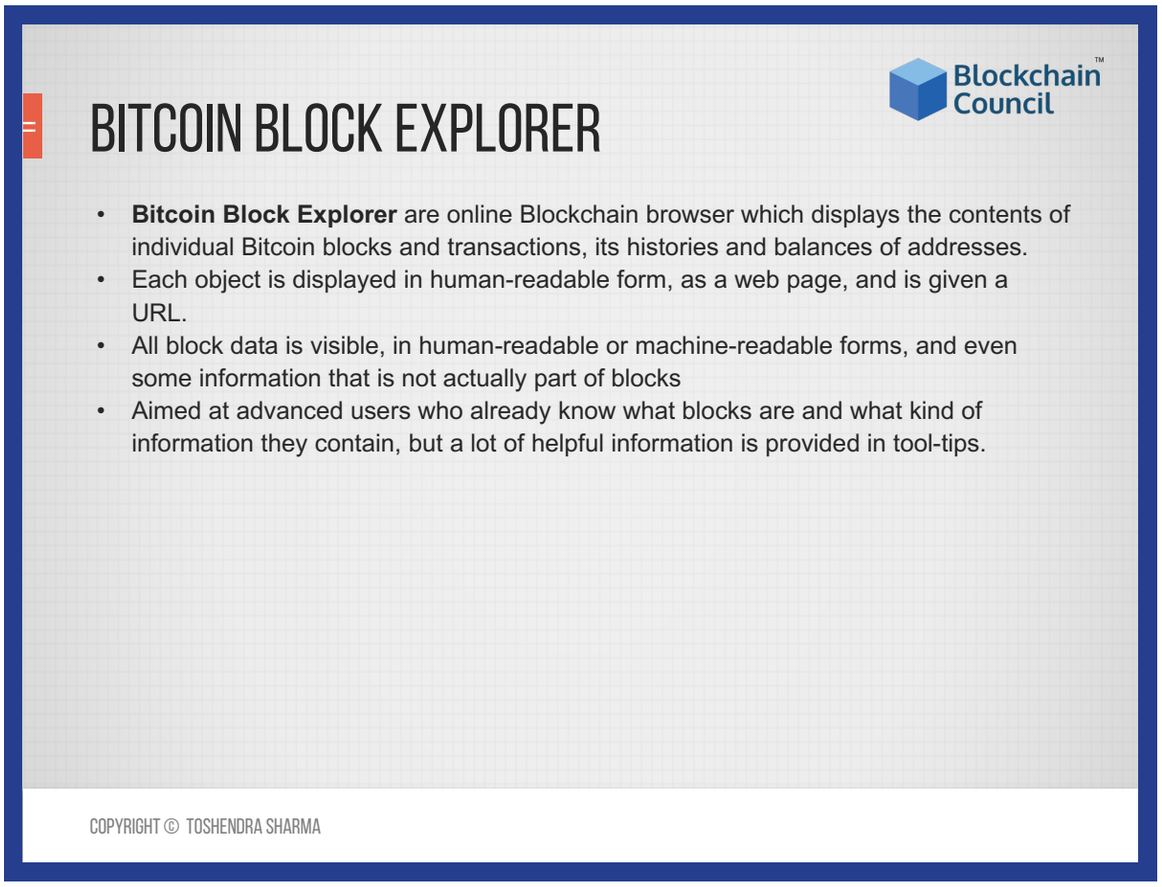
a ‘LiveCD’ Linux distribution, such as Ubuntu. Furthermore, once a paper-wallet has been set up via a website, it should be possible for the website code to run offline. Therefore, before creating the private and public keys, take your computer offline. Even for an ultra-tight security, print the paper wallet from a printer that is not connected to a network.

Next, we’ll be checking about Bitcoin Block Explorers.

CHAPTER 13

Bitcoin Block Explorer





You can view your transactions with all the details of it on your web browser through a Block Explorer. Bitcoin Block Explorer is an online Blockchain browser which displays the contents of individual Bitcoin blocks and transactions and the transaction histories and balances of addresses.

BitcoinBlockExplorer.com allowing such features was originally written by Theymos, but now it is operated by Liraz Siri.

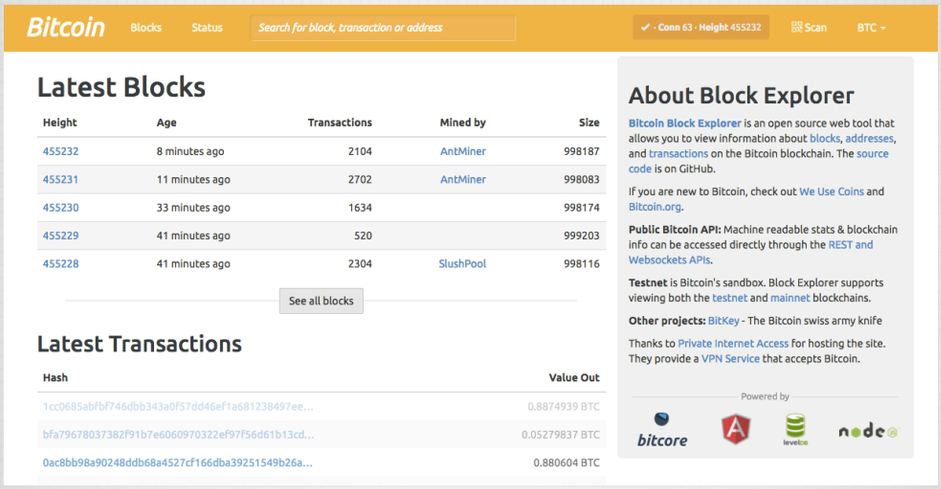
Each object is displayed in the human-readable form, as a web page and is given a URL. By using hyperlinks, it allows users to switch from seeing one piece of data to a related one, with a single click. Clicking on the hash of an object will move to the page that displays its data. This way, for instance, one can switch from looking at a transaction to looking at the previous transaction which gave this transaction its inputs. All block data is visible, in human-readable or machine-readable forms and even some information that is not actually part of blocks.

It is mainly aimed at advanced users who already know what blocks are and what kind of information they contain, but a lot of helpful information is provided in tool-tips.

A listing of “strange transactions” is displayed on the main page along with listings of the latest and largest transactions.

Bitcoin Block Explorer can also display information from the Testnet which is a test network for development purposes.

BITCOIN BLOCK EXPLORER



FAMOUS BITCOIN EXPLORER

- Blockcypher
- Bitcoinchain
- Blockr
- BTC.com
- Blockchain.info
- TradeBlock

Some of the famous and most popular Bitcoin Explorers are mentioned below.

Blockcypher: The **Blockcypher** Bitcoin block explorer is quite pleasing to the eyes with its warm colors. When one looks up a wallet address, they will immediately see the QR code for that address, as well as the total amount of money received and sent.

BitcoinChain: The **BitcoinChain** block explorer crams a lot of information into a browser window. Everything is well-organized and it even mentions which mining pool mined indi-vidual blocks on the network. The platform also keeps track of Bitcoin markets, pools and network nodes.

Blockr: People active in the world of Bitcoin and cryptocurrency will know the name **Blockr**. The company's block explorer is one of the complete solutions, as it shows a lot of information in a convenient format.

BTC.com: Depending on what type of Bitcoin network information one is looking for, the **BTC.com** block explorer is well worth checking out. On the front page, one can see the real-time hash rate of all mining pools, as well as real-time network information. BTC.com also keeps track of network congestion, which is a very attractive feature.

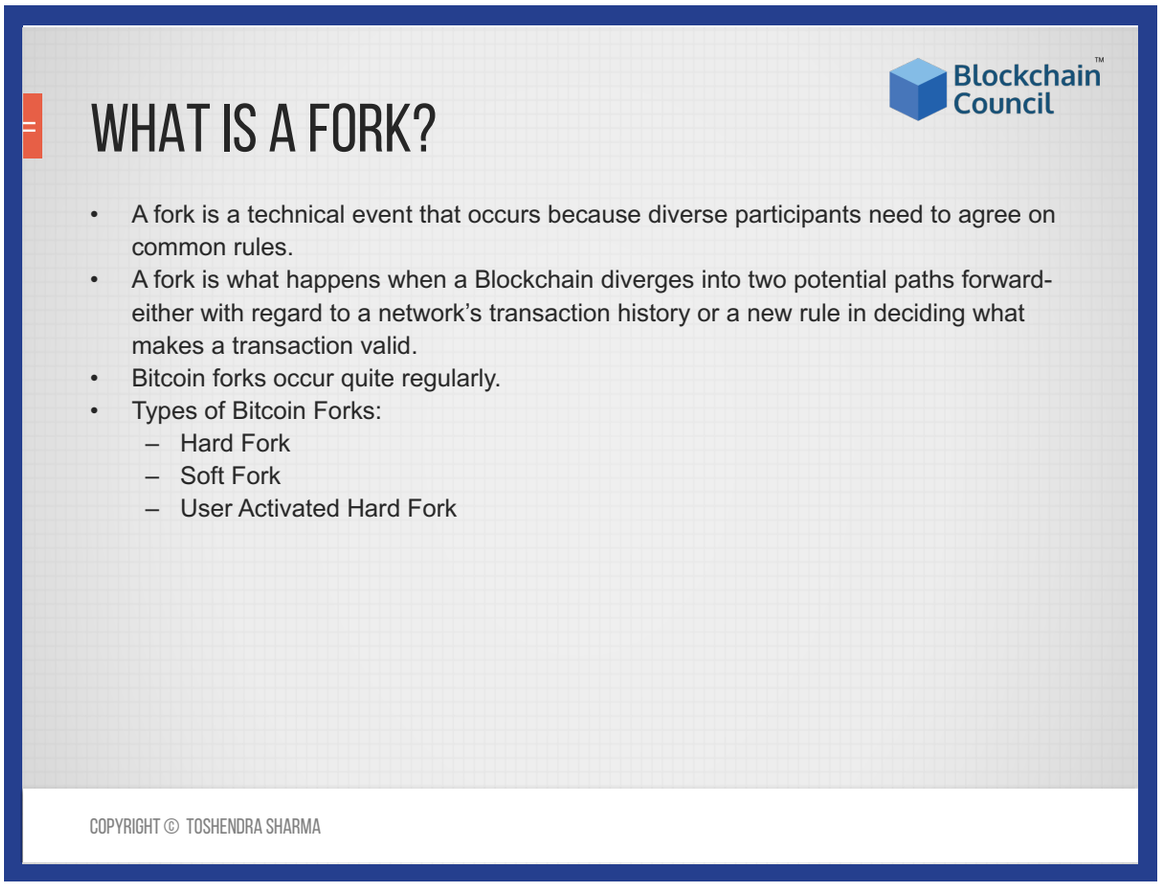
Blockchain.info (Most people use this solution as the go-to platform to look up Bitcoin wallet addresses and transactions. Moreover, the company provides plenty of statistics and charts pertaining to the Bitcoin network itself)

TradeBlock (TradeBlock is a bit of a dark horse when it comes to Bitcoin block explorers. The explorer itself offers all of the functionality one would expect, yet presents it in a slightly different manner. All data is formatted nicely with external links to individual traction hashes).

In the next chapter we'll try to understand what a fork is in Bitcoin and the number of forks introduced in it.

CHAPTER 14

Bitcoin Forks



A fork occurs when two miners find a valid hash within a short span of time.

They both spread the solution for verification to their neighbours. As the process continues, the network will split into two, where one half of the network believes one block is the next to be included in the Blockchain ledger, while the other half of the network believes in a different block.

Mostly, this problem gets resolved quickly or within one block, i.e., the probability of two blocks being found within two seconds of each other, for two block rewards consecutively is very low. A one block fork occurs roughly once a week, while a two block fork occurrence is extremely rare.

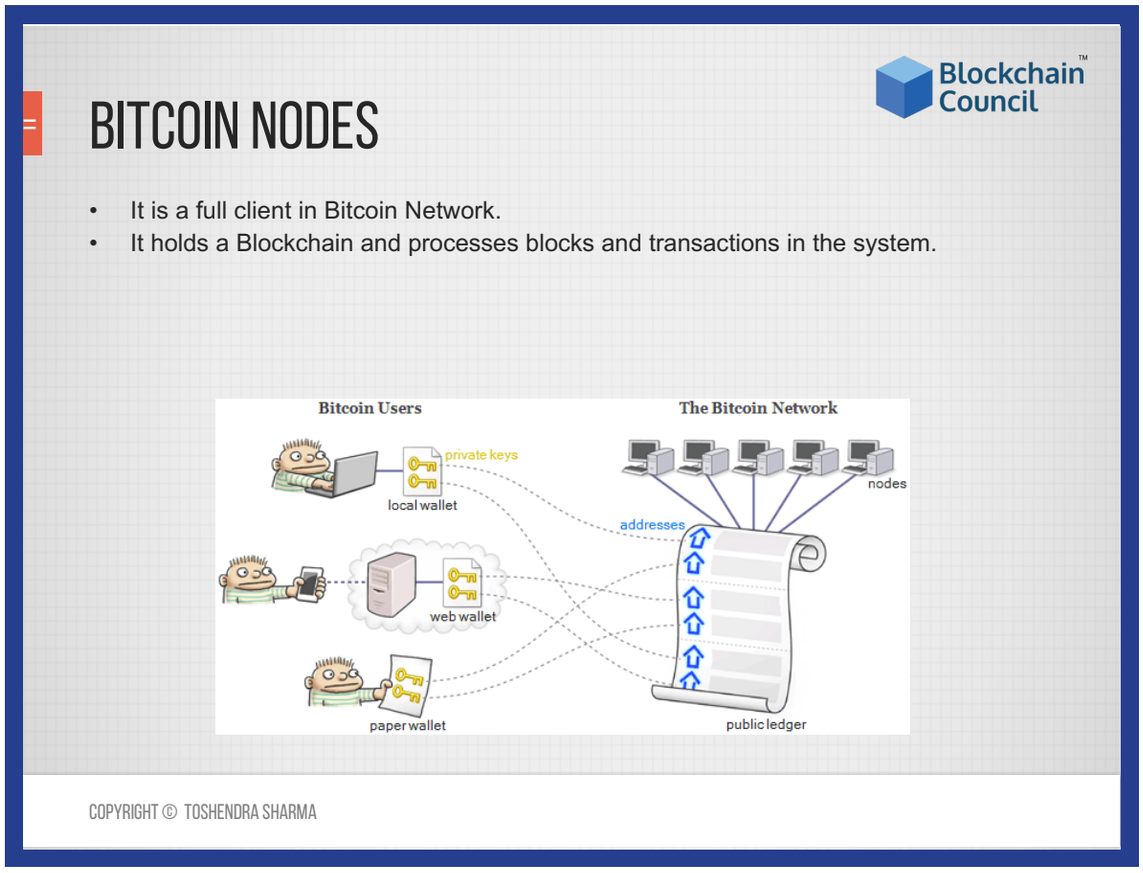
A Bitcoin fork happens when someone modifies the source code so that it is sufficiently different from the original, thereby creating a unique version of the software. So, overall a fork is a technical event that occurs because diverse participants need to agree on common rules and happens when a Blockchain diverges into two potential paths forward-either about a network's transaction history or a new rule in deciding what makes a transaction valid.

Since Bitcoin forks occur quite regularly, they can be classified into two general types which are a hard fork and a soft fork.

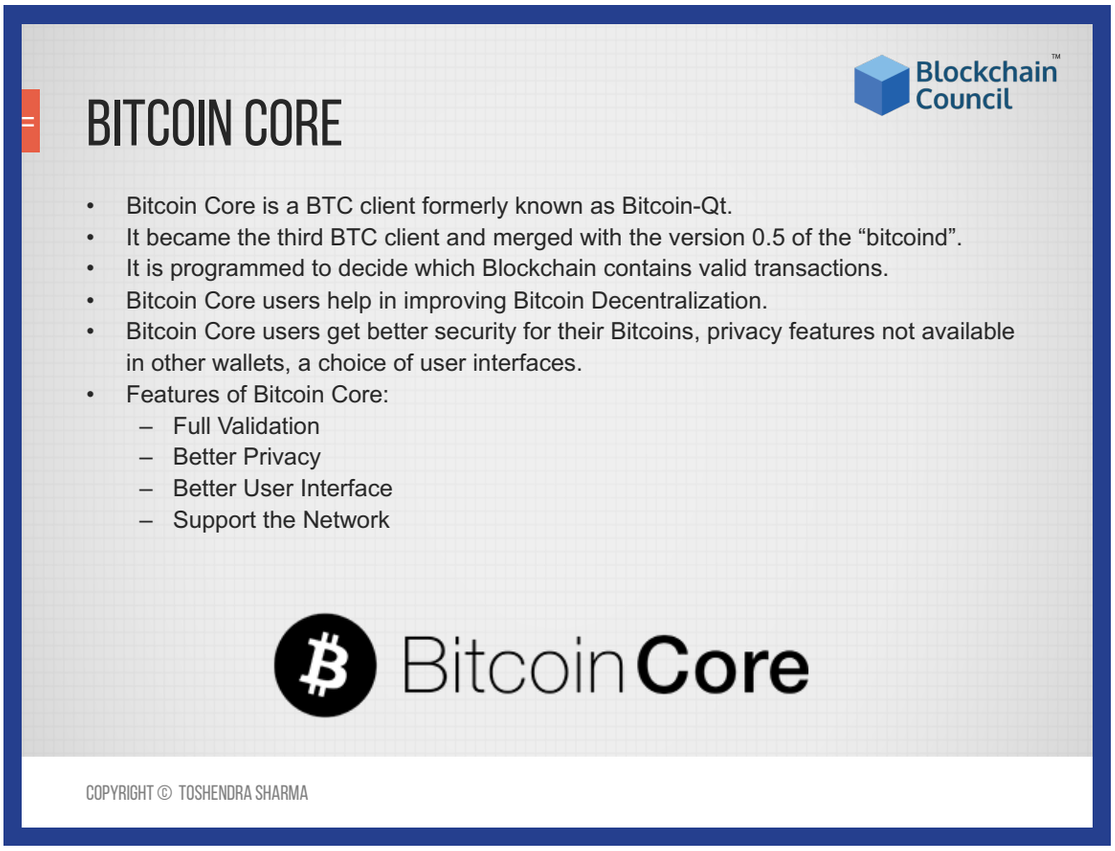
A hard fork is a software upgrade that introduces a new rule to the network that isn't compatible with the older software. You can think of a hard fork as an expansion of the rules. You might be thinking what happens in a hard fork?

Nodes that continue running the old version of the software will see the new transactions as invalid. So, to switch over to the new chain and to continue to mine valid blocks, all the nodes in the network need to upgrade to the new rules.

On the other hand, a soft fork, in contrast is any change that's backward compatible. Non-upgraded nodes will still see the new transactions as valid. However, if non-upgraded nodes continue to mine blocks, the blocks they mine will be rejected by the upgraded nodes. This is why soft forks need a majority of hash power in the network.



Let's understand about Bitcoin nodes. There are "full" and lightweight clients in the Bitcoin network. A Bitcoin node is a full client, which means that it holds a Blockchain and processes blocks and transactions in the system. A full node is basically an electronic bookkeeper and anybody in the world can set up and run one. Each node has a complete copy of the public ledger. Any computer either mining or just running a Bitcoin client supports the chosen node and the system in general. The stakeholders can support the preferred node by running the corresponding software. Bitcoin network uses a client to client network infrastructure, so there is no difference between a mining client and a non-mining client, they don't have any privileges.



Let's move to various forks that occurred in Bitcoin, starting with Bitcoin Core. Bitcoin Core is a BTC client formerly known as Bitcoin-Qt. It became the third BTC client and merged with the version 0.5 of the Bitcoind. According to the main goals of stable Bitcoin network, the client validates transactions in the Blockchain, prevents double spending and contrib-utes to the secure decentralized ecosystem.

Bitcoin Core is programmed to decide which Blockchain contains valid transactions. The users of Bitcoin Core only accept transactions for that Blockchain, making it the Bitcoin Blockchain that everyone else wants to use. These users keep Bitcoin decentralized. They individually run their own Bitcoin Core full nodes and each of those full nodes separately follows the same rules to decide which Blockchain is valid. There's no voting or other corruptible process involved, there's just individual software following identical rules of "math"—to evaluate identical blocks and coming to identical conclusions about which Blockchain is valid. In addition to improving Bitcoin's decentralization, Bitcoin Core users get better security for their Bitcoins, privacy features which are not available in other wallets, a choice of user interfaces and several other powerful features.

So, features of Bitcoin Core are :

- Full Validation as Bitcoin Core ensures every block and transaction it accepts is valid, increasing not only your security but also helping prevent miners and banks from taking control of Bitcoin.
- Better privacy

Bitcoin Core provides exclusive privacy features that can make it hard for anyone to link you to your transactions, so, to warn you in advance, better security has costs.

- A better user interface

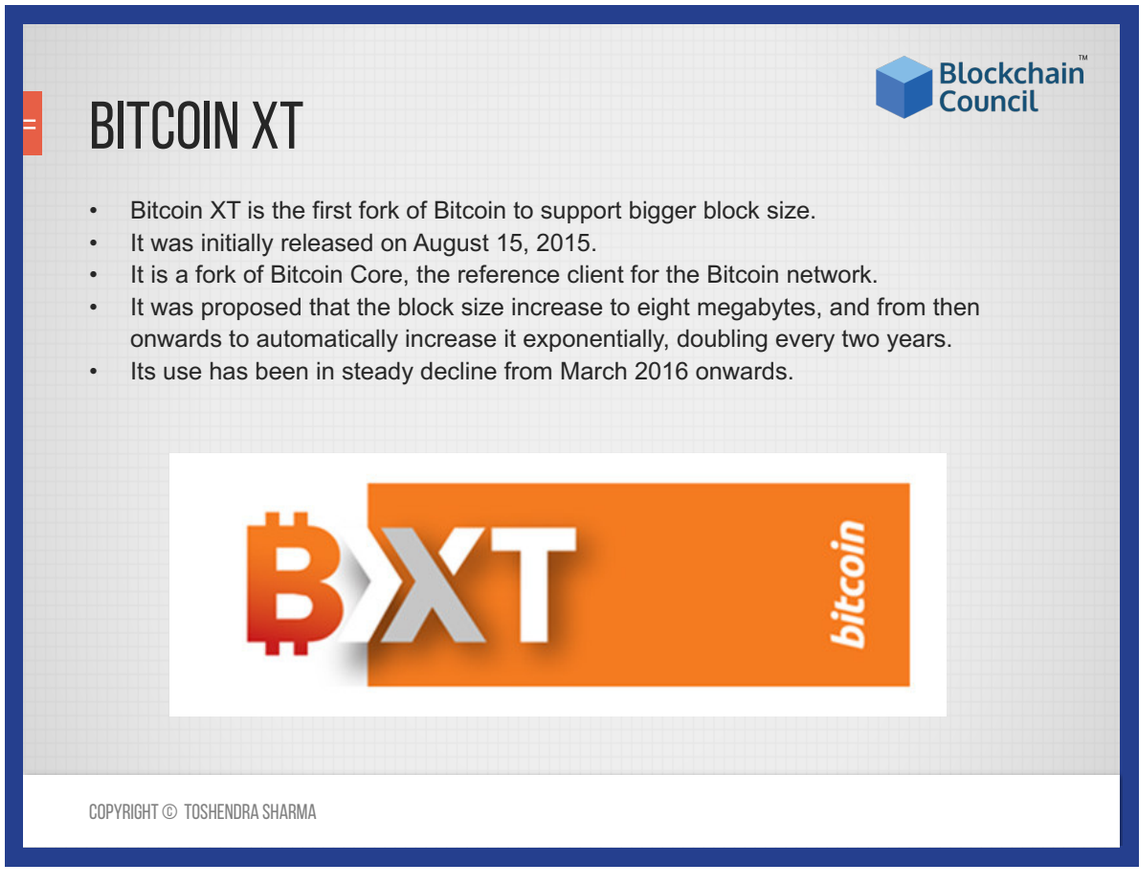
By this, it means that Bitcoin Core wallet has features most other wallets don't have. But if you don't need them, you can use several other wallets on top of Bitcoin Core without losing Bitcoin Core's security and privacy benefits.

- Support the network

Bitcoin Core helps support other peers. This isn't as useful as helping to keep Bitcoin decentralized, but it's an easy way for broadband users to contribute to less well-connected users.

Next, explaining about Bitcoin Classic, it is a fork of Bitcoin Core with a larger BTC block size and contributes to a healthier and more capable network. The software is adaptable to their needs. Larger blocks make the network more stable and serve as a stronger protection against the double spending of the digital currency. Blocks, which contain transaction data, form the basic structure of the immutable Blockchain. Bitcoin Classic started out as similar to, though less aggressive than, the Bitcoin XT fork, which never managed to get the support it needed. Bitcoin Classic in its first eight months promoted a single increase of the maximum block size from one megabyte to two megabytes. In November 2016 this changed and the project moved to a solution that moved the limit out of the software rules into the hands of the miners and nodes. Bitcoin Classic is also an attempt to move the technical governance of this decentralized and independent Bitcoin project from the developers of the original

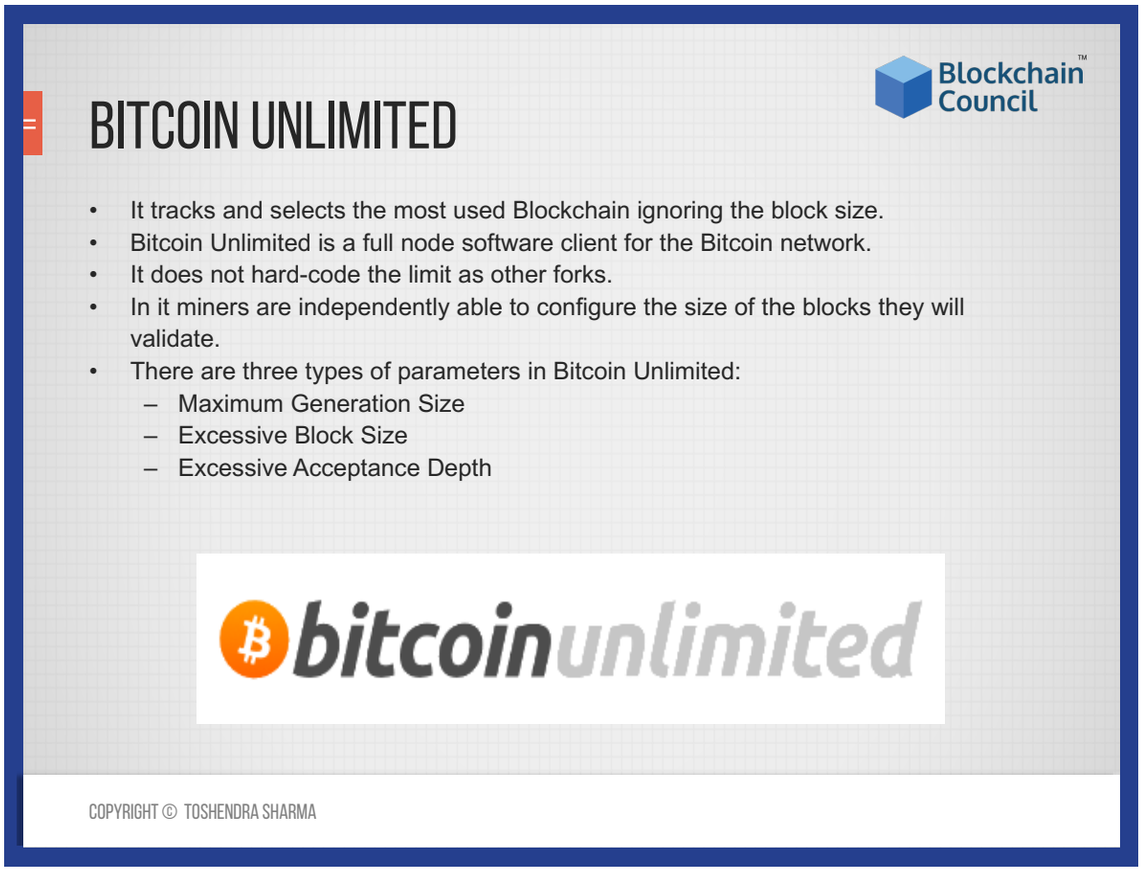
Bitcoin to a voting process involving a larger community of miners, businesses, developers and users. There is no formal activation method for the software, but due to the nature of Bitcoin, a supermajority needs to support it. In Bitcoin, transactions are collected into blocks and each block is produced by the Bitcoin network on average every ten minutes. With Bitcoin's current limit of one megabyte, this capacity translates to an estimated average of three transactions per second. With Bitcoin Classic's proposed doubling of the block size limit to two megabytes, the maximum transaction rate would also roughly double and If deployed, Bitcoin Classic would render current Bitcoin software obsolete as it changes protocol parameters, namely increasing the maximum block size from one megabyte to two megabytes. Most implementations of Bitcoin software would require small modifications to the block size limit in order to continue to work.



Moving on to Bitcoin XT, Bitcoin XT is the first fork of Bitcoin to support bigger block size. BTC transactions are assembled into blocks every 10 minutes because of the continuous development of the currency.

Bitcoin XT is a fork of Bitcoin Core, the reference client for the Bitcoin network. In mid-2015, the concept achieved significant attention within the Bitcoin community amid a contentious debate among core developers over increasing the block size cap. The current reference implementation for Bitcoin contains a computational bottleneck. This brings it to a daily average of around 300,000 transactions at max. It was proposed that the block size increases to eight megabytes and more automatically, increasing it exponentially and almost doubling up every two years. The proposal did not gain the necessary support to go into effect on

the Bitcoin network by early 2016, the earliest possible switchover date. Its use has been in steady decline from March 2016 onwards.

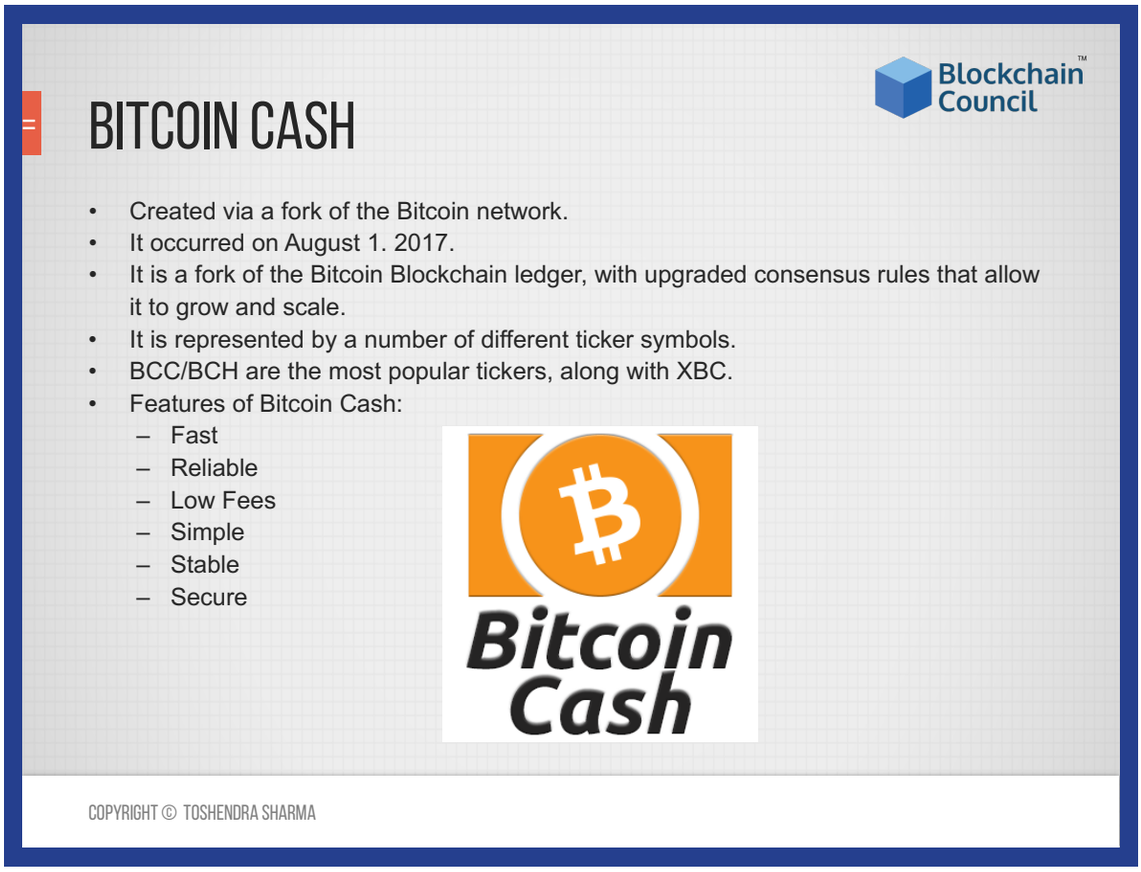


Bitcoin Unlimited

The distinctive feature of Bitcoin Unlimited client is freedom for all members of the Bitcoin system to have a say about the block size. It tracks and selects the most used Blockchain ignoring the block size. At the same time, the adopters can choose a cap for the blocks they consider redundantly large. Bitcoin Unlimited is a full node software client for the Bitcoin network. Compared to the Bitcoin Core client hard-coding the block size limit to 1 megabyte, from which it is forked. Bitcoin Unlimited does not hard-code the limit thereby allowing the users to signal which block size limit they prefer, find the limit having a majority consensus and set their block size limit to that value.

Bitcoin Unlimited is an attempt to upgrade Bitcoin Core into a client that processes Bitcoin transactions into blocks with a potential maximum size greater than the Core's hard-coded limit of one megabyte. The one-megabyte block size limit was added in 2010 by Satoshi Nakamoto as a temporary anti-spam measure. This limited the maximum network capacity to about three transactions per second. As per the advocates of the change, a block size increase is needed to avoid a workflow bottleneck due to the number of transactions made as Bitcoin adoption increase. With Bitcoin Unlimited, miners are independently able to con-figure the size of the blocks they will validate. Maximum generation size also referred to as MG is a new parameter which by default is set to one megabyte.

The software allows the users to adjust it and select the size of blocks they produce. Excessive Block Size or EB parameter allows nodes to choose the size of the block they accept. By default, this is set at 16 megabytes. The third new parameter allows a user to select the Excessive Acceptance Depth or AD. This implements a consensus strategy by retroactively accepting larger blocks if a majority of other miners have done so. Miners using Bitcoin Unlimited continue to process regular-sized blocks but as soon as a block larger than 1 MB is mined, they will follow the chain containing the most work.



Another fork of Bitcoin is Bitcoin Cash

Bitcoin Cash (BCC) is a cryptocurrency created via a fork of the Bitcoin network. This means that any user who held Bitcoin at the time of the fork (August 1st, 2017), now has an equivalent amount of Bitcoin Cash on the forked Bitcoin Cash Blockchain.

Bitcoin Cash is a token that may exist in the near future due to a user-activated hard fork that will bifurcate the Bitcoin Blockchain into two branches. The UAHF was initially a contingency plan against the user-activated soft fork (UASF) announced by the Bitcoin company Bitmain Technologies.

Some of it's features are:

- Fast, i.e. transact in seconds and get confirmed in minutes.
- Reliable- a network that runs without congestion.
- Low fees- send money globally for pennies.

- Simple- easy to use. No hassles.
- Stable- a payment system that's a proven store of value.
- Secure- World's most robust Blockchain technology.

Is Bitcoin Cash different from 'Bitcoin'?

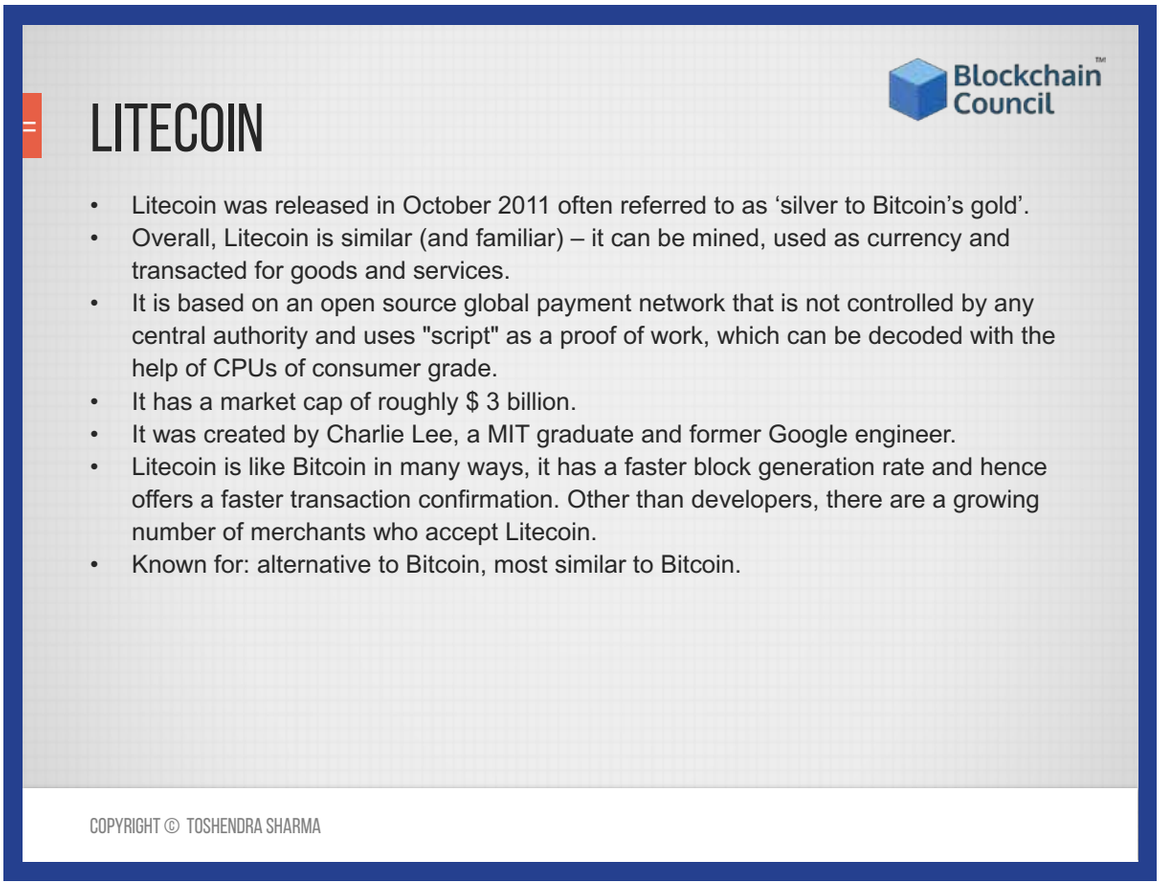
The answer is Yes. Bitcoin Cash is the continuation of the Bitcoin project as peer-to-peer digital cash. It is a fork of the Bitcoin Blockchain ledger with upgraded consensus rules that allows it to grow and scale. Bitcoin Cash is represented by a number of different ticker symbols depending on the service or wallet. BCC/BCH are the most popular tickers with XBC being used to meet the International Standard for currency codes.

After having an idea of what Bitcoin forks are, we will try to understand the variations in Bitcoin in our next section.

CHAPTER 15

Bitcoin Variations

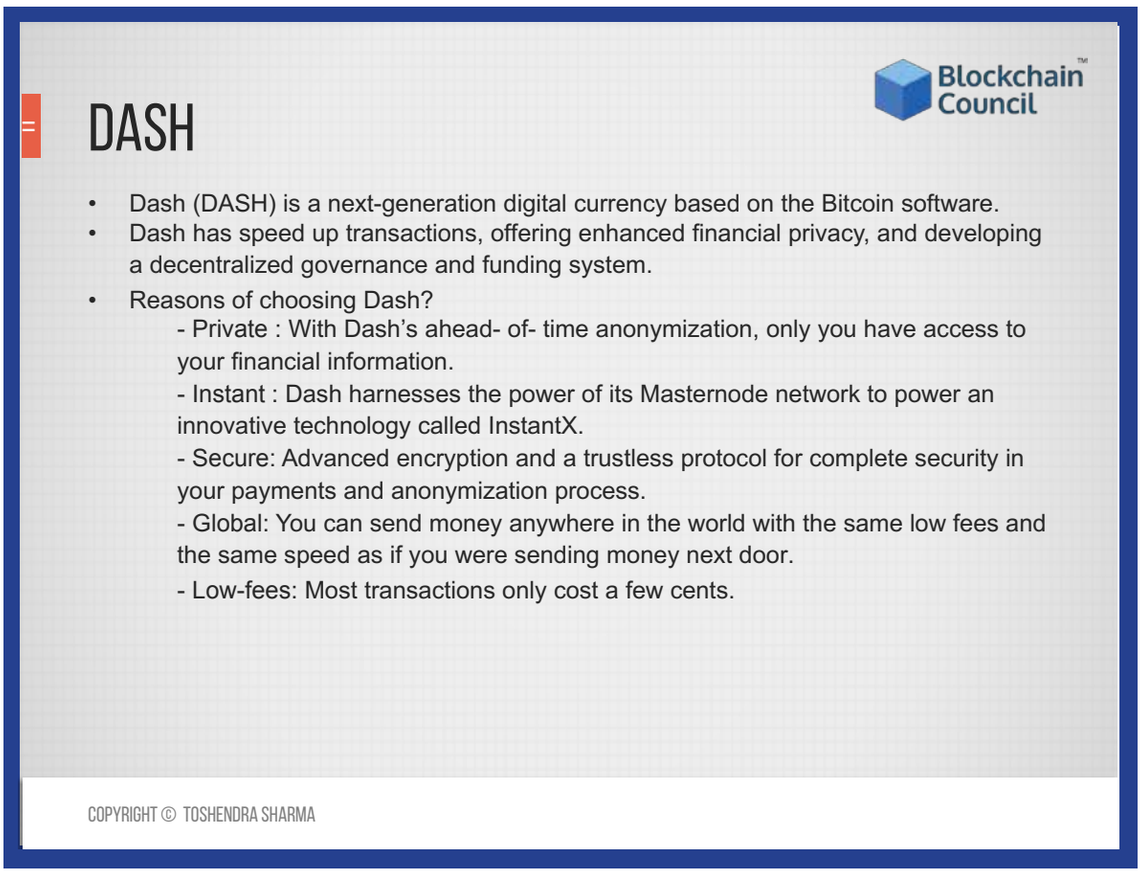
This section will give you an overview about some famous Cryptocurrencies. At present there are already 1241 Cryptocurrencies in the market. But here, we will only focus on some of these like Litecoin, Zcash, Dash etc.



Apart from Bitcoin, another big name in the market is Litecoin which was released in October 2011 and is often referred to as silver to Bitcoin Gold. Overall, Litecoin is similar to Bitcoin – it can be mined, used as currency and transacted for goods and services. It is based on an open source global payment network that is not controlled by any central authority and uses "scrypt algorithm" as a proof of work, which can be decoded with the help of CPUs of consumer grade. It facilitated the emergence of several other Cryptocurrencies which used its codebase but made it even more light. Examples are Dogecoin or Feathercoin. It has a market cap of around $ 3 billion.

It was created by Charlie Lee, an MIT graduate and former Google engineer. Litecoin is like Bitcoin in many ways; it has a faster block generation rate and hence offers a faster transaction confirmation. Other than developers, there are a growing number of merchants who accept Litecoin.

While Litecoin failed to find a real use case and lost its second place after Bitcoin, it is still actively developed and traded and is hoarded as a backup if Bitcoin fails. Known for: alternative to Bitcoin and is pretty similar to Bitcoin.



Dash (DASH) is a next-generation digital currency based on the Bitcoin software. Dash has speed up transactions, offering enhanced financial privacy and developing decentralized governance and funding system. Reasons to choose Dash are that.

It is private: With Dash's ahead- of- time anonymization, only you have access to your financial information.

It is instant: Dash harnesses the power of its masternode network to power an innovative technology called InstantX.

It is secure: Advanced encryption and a trustworthy protocol for complete security for your payments.

It is global: You can send money anywhere in the world with the speed as if you are sending money next door.

It has low-fees: Mostly transactions only cost a few cents.

In addition to traditional proof- of- work rewards for mining Dash, users are also rewarded for running and maintaining special servers called Masternodes which enables additional features such as instant transactions (InstantX), private transactions (Darksend), and decentralized governance and budgeting.

Anyone can run a masternode but in order to do so, the user must prove that they own 1000 Dash.

This is to prevent so-called Sybil attacks on the network.

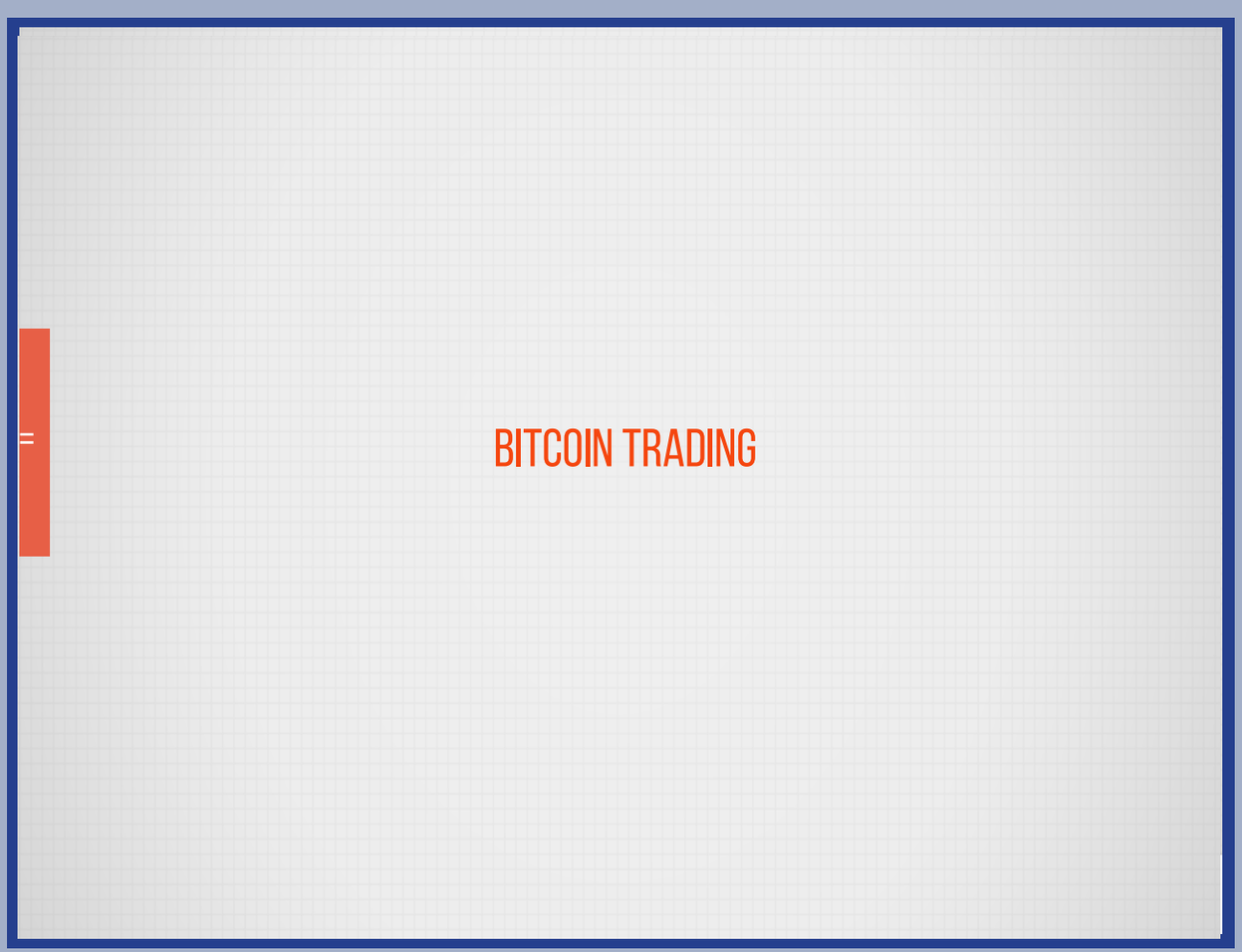
Zcash: A decentralized and open-source cryptocurrency launched in 2016. If Bitcoin is like http for money, Zcash is "https" is how Zcash defines itself. This is because many digital currency transactions rely on the use of private keys which are strings of letters and numbers that identify a user. An address can become attached to several transactions over time which makes it easy for friends, family, marketers or even government authorities to learn more about a person's purchasing trends. And if a user's private key is attached to certain transactions, some parties may refuse to accept his or her money. This is where Zcash comes in. Zcash offers privacy and selective transparency of transactions where all transactions are recorded and published on a Blockchain but details such as the sender, recipient and amount remain private. Zcash is a cryptocurrency that grew out of the Zerocoin project aimed at improving anonymity for Bitcoin users. The Zerocoin protocol was initially improved and transformed into Zerocash which thus yielded the Zcash cryptocurrency in 2016.

Zcash offers its users the choice of shielded transactions, which allows for content to be encrypted using advanced cryptographic technique or zero-knowledge proof construction called a zk-SNARK developed by its team.

The Zcash Blockchain went live on October 28, 2016 and is currently hovering around $540 million.

CHAPTER 16

Bitcoin Trading



We will now learn about Bitcoin Trading as it is the most important part for every person to understand and to have a general idea of why people have so much of interest in Bitcoins and other cryptocurrencies and through it, how can one gain large amount of profits, if invested and traded wisely. It has high risks too associated with it. Here, we'll provide you with a general understanding of trading in Bitcoin and what is trading.

Starting with Bitcoin trading, Bitcoin trading can be extremely profitable for professionals or beginners. The market is new and is highly fragmented with huge spreads. Arbitrage and margin trading are widely available. Many people can make money trading Bitcoins. Bitcoin's history of bubbles and volatility has perhaps done more to bring in new users and investors than any other aspect of the cryptocurrency. Each Bitcoin bubble creates hype that puts Bitcoin's name in the news. The media attention causes more to become interested and the price rises until the hype fades.

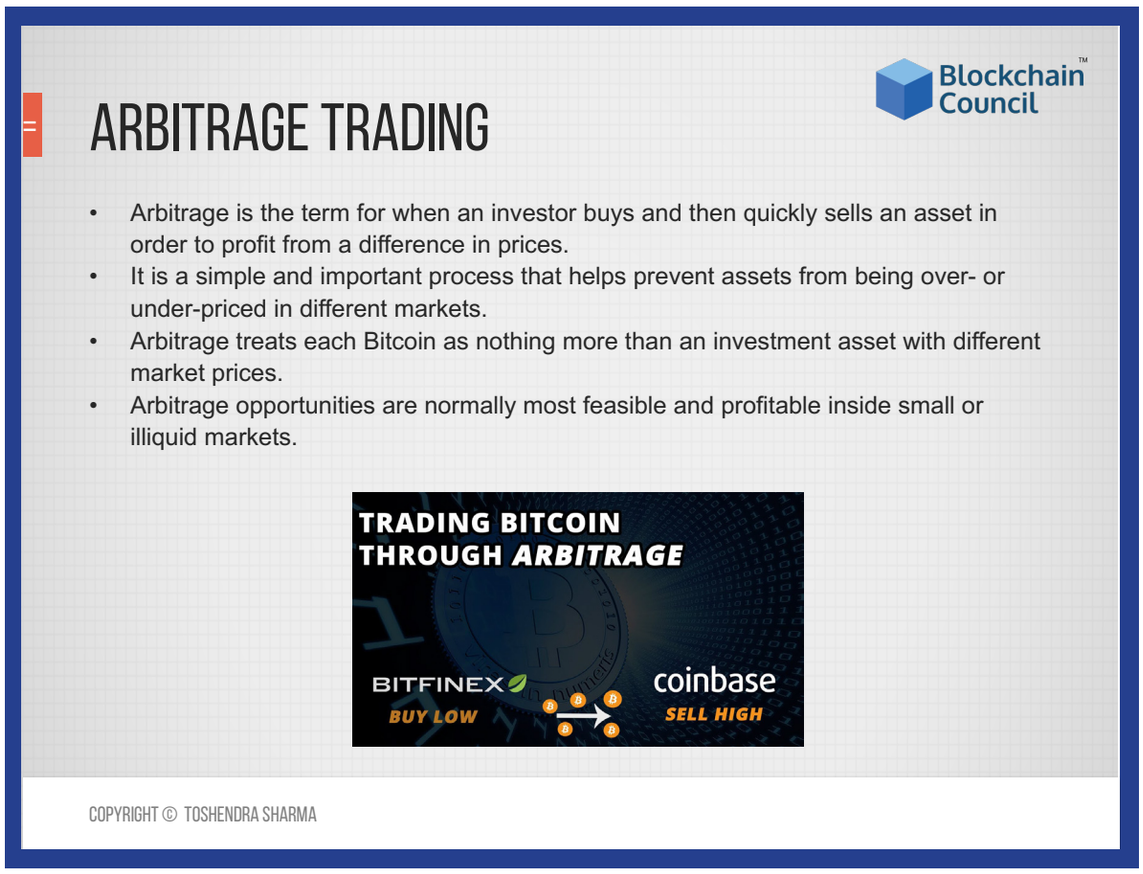
Each time Bitcoin's price rises, new investors and speculators want their share of profits because Bitcoin is global and easy to send anywhere making trading Bitcoin simple. If you are interested in trading Bitcoin then there are many online trading companies offering this product usually as a contract for difference or CFD.

Why trade Bitcoin?

Before learning how to trade Bitcoin, it's important to understand why Bitcoin trading is both exciting and unique.

- Bitcoin Is Global: Bitcoin isn't fiat currency, i.e. its price isn't directly related to the economy or policies of any single country. Throughout its history, Bitcoin's prices have reacted to a wide range of events, from China's devaluation of the Yuan to Greek capital controls.
- Bitcoin Trades 24/7: Unlike stock markets, there are no official Bitcoin exchanges. Instead, there are hundreds of exchanges around the world that operate 24/7. Because there is no official Bitcoin exchange, there is also no official Bitcoin price. This can create arbitrage opportunities, but most of the time exchanges stay within the same general price range.
- Bitcoin is Volatile: Bitcoin is known for its rapid and frequent price movements. Looking at this daily chart from the CoinDesk BPI, it's easy to spot multiple days with swings of 5% or more.

So, before starting with how to trade Bitcoins let's understand what is arbitrage and margin trading.

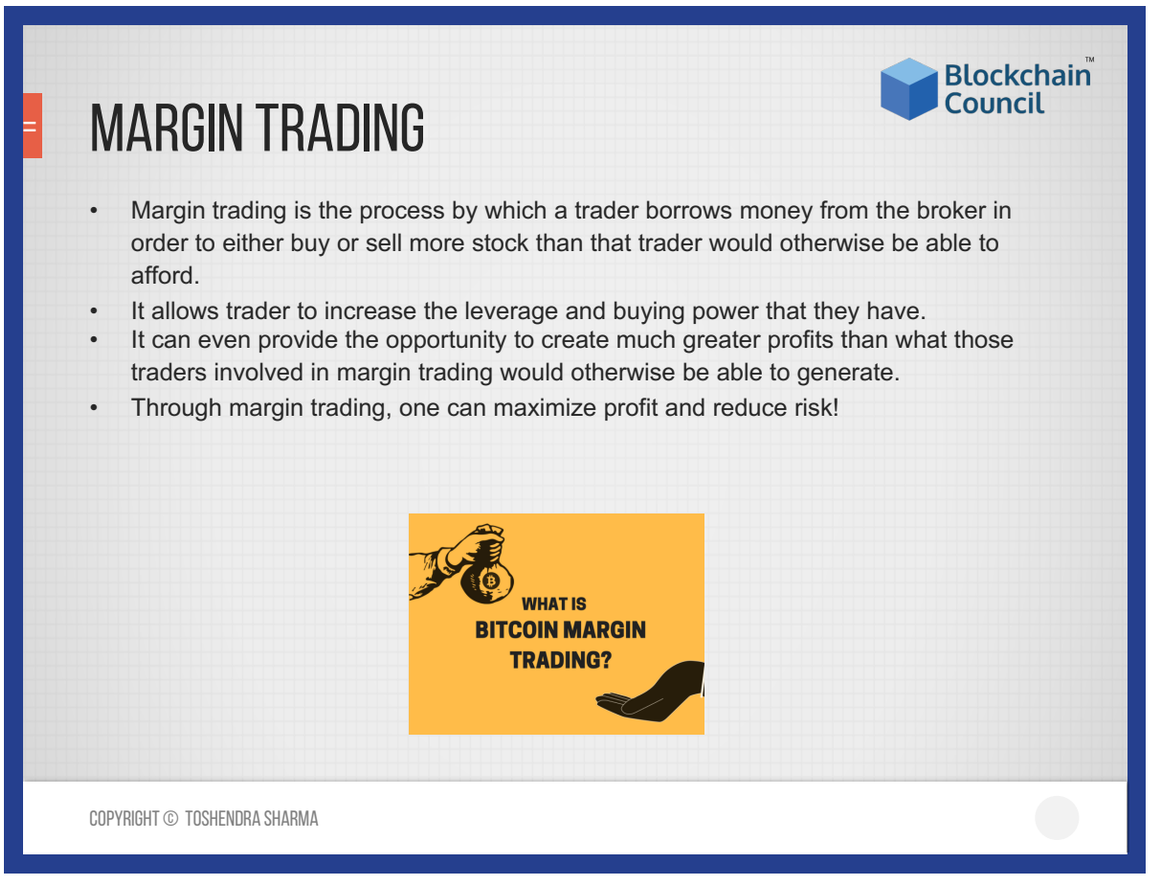


Starting with Arbitrage trading, Bitcoin arbitrage is the buying of Bitcoins on an exchange where the price is very low and selling it at an exchange where the price is relatively higher. The prices of Bitcoin vary on various exchanges because the markets are not directly linked and the trading volume on many exchanges is low enough that the price does not adjust to the average right away. Bitcoin arbitrage trading is a way to make money with less risk than speculative Bitcoin trading or day trading.

It is true that trading Bitcoin is a risky business. The price can swing wildly and nobody knows for certain what the price will vary from day to day. If you know the Bitcoin market, it is possible to read the market signals and make trade based on what you think might happen. In this entire speculation you might gain or loose your money. In nut shell, its a gamble.

Bitcoin arbitrage trading is one of the best ways to make money without having to worry much about sudden price movements that could lose you money. It is a quick and safe way to trade than establishing trade on what the chart is.

Hence, It is a simple and important process that helps preventing assets from being over- or under-priced in different markets. Arbitrage treats each Bitcoin as nothing more than an investment asset with different market prices. Arbitrage opportunities are normally most feasible and profitable in small or illiquid markets.



Margin trading allows a trader to open a position with leverage. Margin Trading is the process by which a trader borrows money from the broker in order to either buy or sell more stock than that trader would otherwise be able to afford. Margin trading is possible due to the existence of the lending market. Lenders provide loans to traders so they can invest in larger amount of coins and lenders benefit from inter-est on the loans. In some exchanges, like Poloniex, users provide the loans for the margin markets and in others the exchange itself provides them. It allows a trader to increase the leverage and buying power that they have.

It can even provide the opportunity to create much higher profits than what those traders involved in margin trading would otherwise be able to generate. Through margin trading, one can maximize profit and reduce risk!

Let's see how to trade Bitcoins. The initial phase involves choosing a Bitcoin Exchange.

When you decide to trade Bitcoins the first and foremost requirement is to figure out where you are going to trade. Though this is supposed to be a decentralized, P2P currency yet it's currently impossible to do high-frequency trading without the help of a centralized server. These centralized servers have been known as a point of weakness for the Bitcoin market as a whole, but improvements in security have slowly been rolled out to various exchanges over time. If you're going to trade Bitcoins on a regular basis, then you'll need to have some deposits at one or two Bitcoin exchanges at all times. While platform features and unique trading options may be the most important aspects of exchanges in other markets but security is the most important feature to think about when trading Bitcoins in a hot wallet. Factors such as longevity, two-factor authentication and proof-of-reserve are going to be the most important features to look at while choosing an exchange.

Longevity and two-factor authentication are two factors that probably should be at the back of mind for traditional exchanges, but proof-of-reserve is a new feature for Bitcoin exchanges that should be viewed with the utmost importance.

Bitcoin exchanges can prove that they actually have the Bitcoins they say they have by signing messages from Bitcoin addresses containing large amounts of Bitcoins, so this should

calm some of the fears when it comes to the possibility of an exchange running a Ponzi scheme. Based on those factors, the following exchanges dominate the Bitcoin exchange market:

- Bitfinex: Bitfinex is the world's ranked one Bitcoin exchange regarding USD trading volume, with about 25,000 BTC traded per day. Customers can trade with no verification if cryptocurrency is used as the deposit method.
- Bitstamp: Bitstamp was founded in 2011 making it one of Bitcoin's oldest exchanges. It's currently the world's second-largest exchange based on USD volume, with a little under 10,000 BTC traded per day.
- OKCoin: Bitcoin exchange based in China but trades in USD.

Coinbase Exchange was the first regulated Bitcoin exchange in the United States. With about 8,000 BTC traded daily, it's the world's 4th largest exchange based on USD volume.

- Kraken: Kraken is the ranked one exchange regarding EUR trading volume at 6,000 BTC per day. It's currently a top-15 exchange in terms of USD volume.

The second phase involves buying and holding Bitcoins.

Once you've signed up for a Bitcoin exchange and verified your account, you can then start to think about your own trading strategy. There are plenty of traders who try to time the market on a daily basis, but the reality is that the buying and holding strategy is the one that has paid off for the largest number of Bitcoin holders in the past. It's usually a good idea to throw your emotions out of the window and simply purchase Bitcoins on a regular basis. One never knows when a piece of regulatory news out of China or a newly announced killer app could cause a huge price swing one way or the other. This will be weekly for some traders, while others will decide to pick up a few Bitcoins on the first of every month. Attempting to trade Bitcoins without understanding why you purchased them in the first place can also be a huge issue. Bitcoin has been known to drop in price by as much as 50% in a single day, so one cannot be tempted to exit the market at a loss when these kinds of events take place. Trading Bitcoins without a view that the price will eventually go higher as the price increases can be problematic because one will probably end up buying high and selling low. So, act smartly while buying and selling of Bitcoins so as to avoid huge losses.

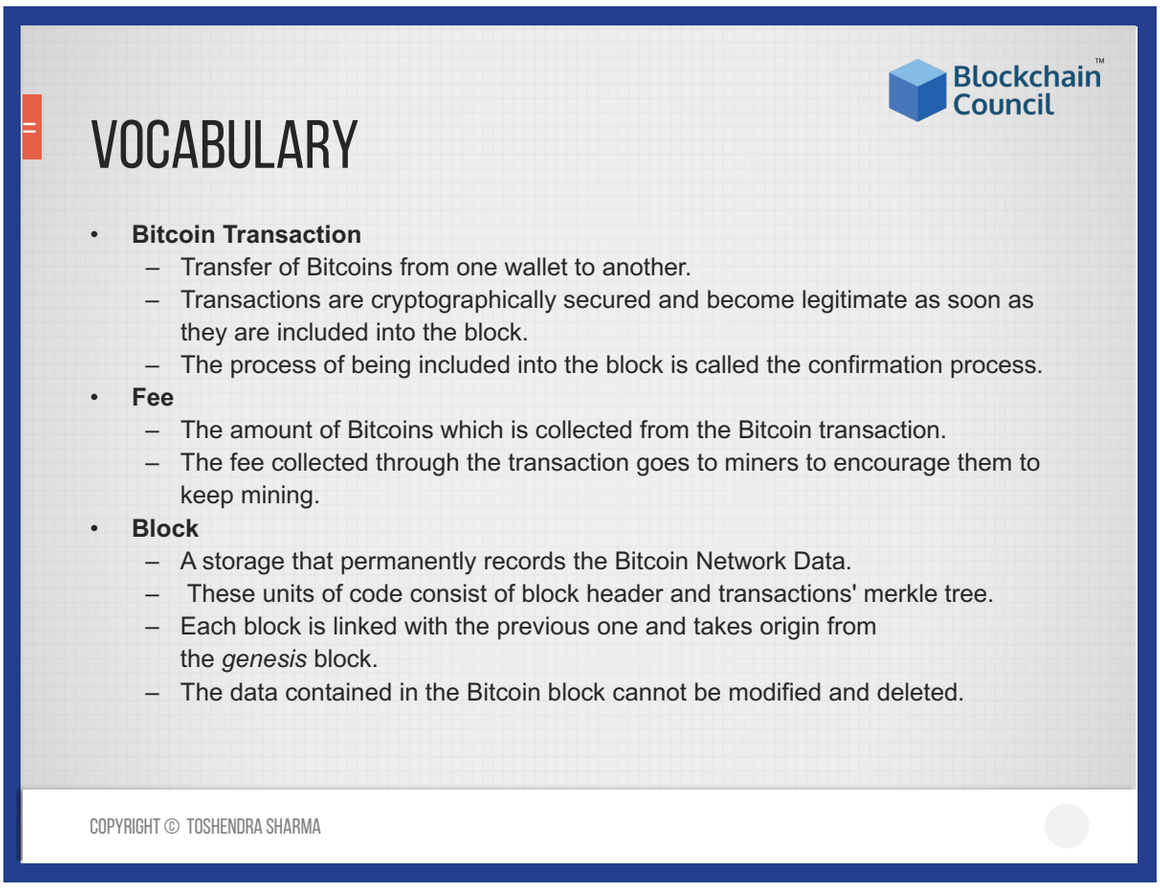
The last step involves reporting your profits

One last thing to remember when it comes to trading Bitcoins is that this currency is not really anonymous when you're using a centralized exchange. After all, the exchange knows all about your true identity due to the various AML and KYC regulations that are required to be followed. Having your Bitcoins increase in value in terms of dollars is not something that will be easy to hide from your local government during tax season. These earnings are viewed as capital gains in most countries, so you should remember to fill out your yearly tax return with that fact in mind.

CHAPTER 17

Bitcoin Vocabulary

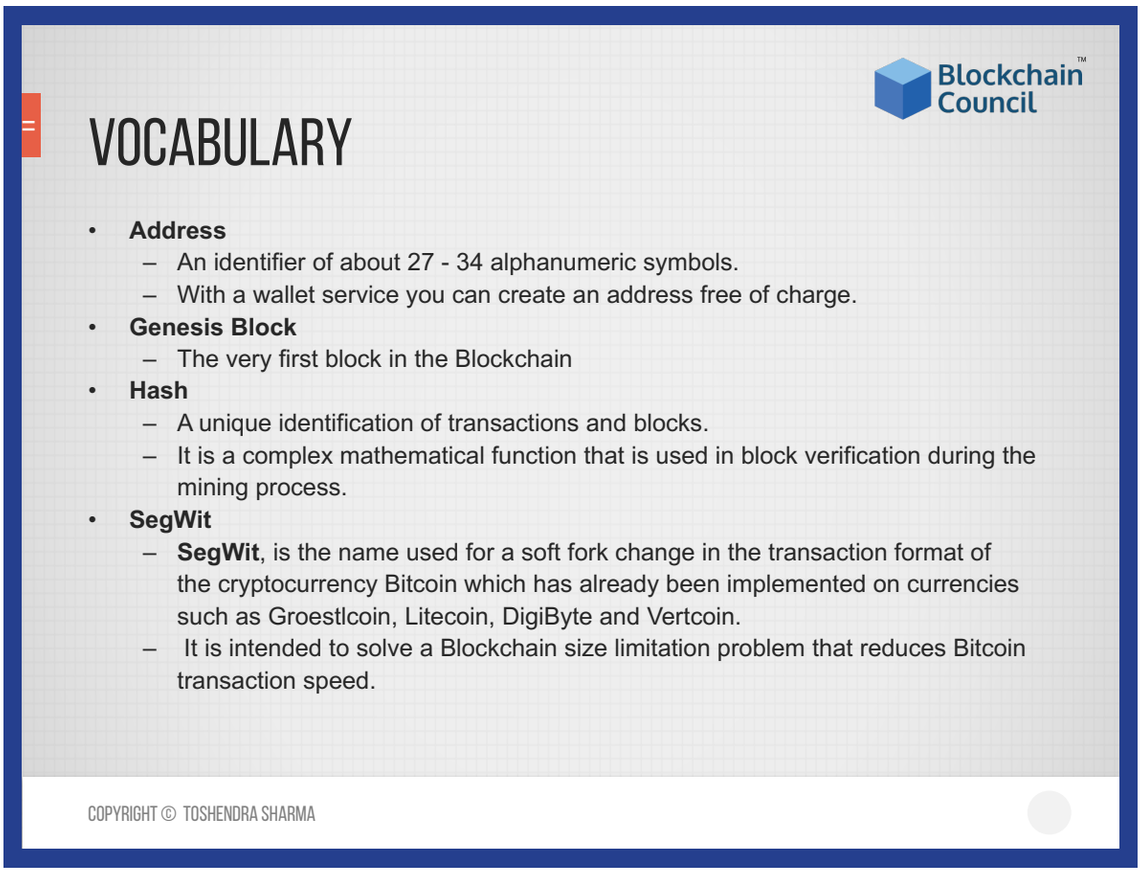
There are some terms which are more frequently used and must be comprehended in an effortless and precise way.



So, one such term is Bitcoin transaction. It is the transfer of Bitcoins from one wallet to another. Transactions are cryptographically secured and become legitimate as soon as they are included in block. The process of being included in the block is called the confirmation process.

Next is Fees. It is the number of Bitcoins which is collected from the Bitcoin transaction. The fee collected through the transaction goes to miners to encourage them to keep mining.

Block. Storage that permanently records the Bitcoin Network Data. These units of code consist of the block header and transactions' Merkle tree. Each block is linked with the previous one and takes origin from the genesis block. The data contained in the Bitcoin block cannot be modified and deleted.



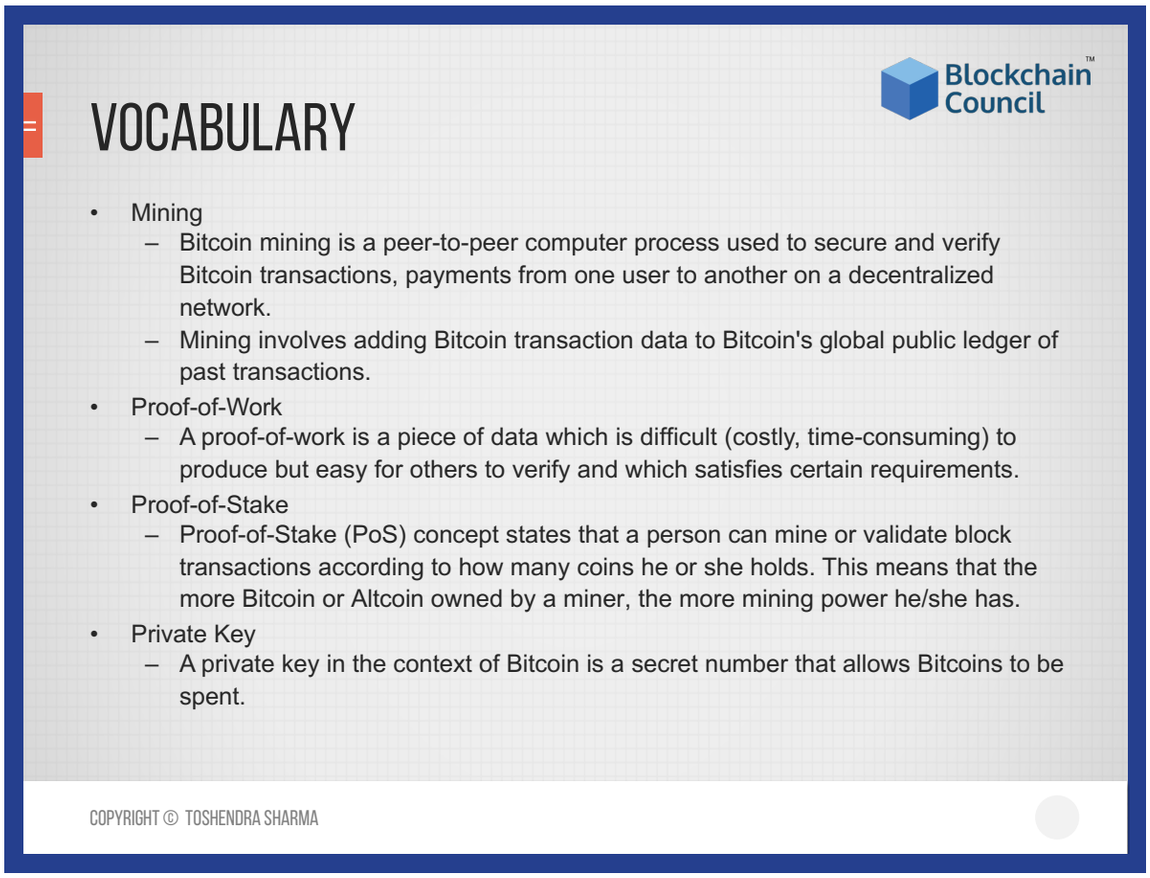
A very important term always used in Blockchain is address.

It is an identifier of about 27 - 34 alphanumeric symbols. With a wallet service, one can create an address free of charge.

The very first block in the Blockchain is called a Genesis Block.

A Hash is a unique identification of transactions and blocks. It is a complex mathematical function that is used in block verification during the mining process.

Next is a SegWit, which if you'll start studying in deep is a very important concept in Bitcoin. SegWit is the name used for a soft fork change in the transaction format of the cryptocurrency Bitcoin which has already been implemented on currencies such as Groestlcoin, Litecoin, DigiByte, and Vertcoin. It is intended to solve a Blockchain size limitation problem that reduces Bitcoin transaction speed.



Mining is a peer-to-peer computer process used to secure and verify Bitcoin transactions or payments from one user to another on a decentralized network. It also includes adding Bitcoin transaction data to bitcoins public ledger of past transactions.

Proof-of-Work is a piece of data which is difficult, costly and time con-suming to produce but easy for others to verify and satisfies certain requirements.

Proof-of-stake concept states that a person can mine or validate block transactions according to how many coins he or she holds. This means that the more Bitcoin or Altcoin owned by a miner, the more mining power he or she has.

A private key in the context of Bitcoin is a secret number that allows Bitcoins to be spent.

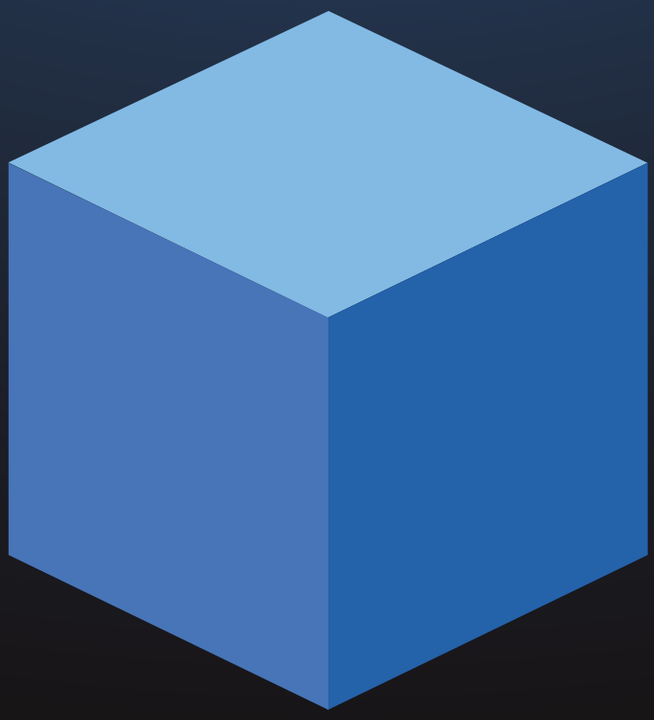
The public key is used to ensure that you are the owner of the address that can receive funds. The public key is also mathematically derived from your private key.

As studied earlier, a “wallet” is basically the Bitcoin equivalent of a bank account. It allows one to receive Bitcoins, store them and send them to others.

Next is Market Cap. Market Capitalization is one way to rank the relative size of a crypto-currency. It is calculated by multiplying the price to the circulating supply.

Trade Volume

The total volume is the sum of the transactions, including buying and selling. Here you can see more detailed info on volume by an exchange.



The Blockchain Council is a de-facto standard body for Blockchain Education & Certifications.

To Purchase Certifications Please visit https://www.blockchain-council.org

Blockchain Council™

www.blockchain-council.org