Introduction to Blockchain
Yogesh Kulkarni

Introduction

Introduction to Blockchain

What on earth is Blockchain?

- A blockchain is a digital concept to store data, in form of blocks, chained one after another.
- Its public and immutable (non changeable)
- Anything can be stored as data (to name some: property rights, identities, money balances, medical records), without being at risk of someone tampering with those records.

And there is an addition of one more word, which is a must in every talk...and that is?

Bitcoin

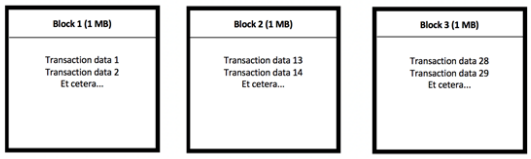
How Bitcoin Works?

Background

- Bitcoin blockchain is a giant track record of all the Bitcoin transactions that have ever occurred, all the way back to the very first Bitcoin transaction.

Step 1 — Transaction data

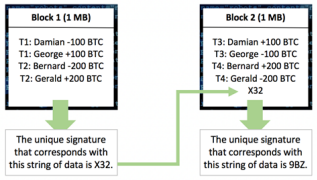
- The blocks on the Bitcoin blockchain consist of approximately 1 MB of data each
- The data is about Bitcoin transactions



(Ref: "How does blockchain work in 7 steps — A clear and simple explanation." - Jimi S, Good Audience)

Step 2 — Chaining the blocks (with a hash)

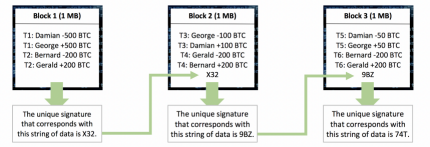
- Let's say block 1 registers two transactions, transaction 1 and transaction 2
- Assume these fill up 1MB data limit.
- This block of data now gets a signature for this specific string of data. Let's say the signature is 'X32'.
- Similarly next set of transactions go to Block 2 with a signature '9BZ'.
- Block 2 gets appended to the existing chain (ie Block 1)
- The signatures link the blocks to each other



(Ref: "How does blockchain work in 7 steps — A clear and simple explanation." - Jimi S, Good Audience)

Step 2 — Chaining the blocks (with a hash)

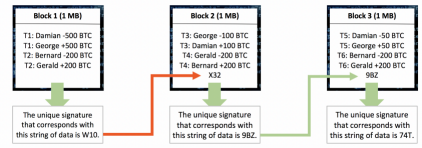
- One more block comes (ie Block 3), it gets appended in a similar manner.
- Now imagine if the data in block 1 is altered.
- Damian now supposedly sent 500 Bitcoin to George instead of 100 Bitcoin.
- Block 1's signature now changes, say it is now 'W10'



(Ref: "How does blockchain work in 7 steps — A clear and simple explanation." - Jimi S, Good Audience)

Step 2 — Chaining the blocks (with a hash)

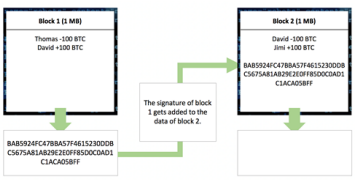
- The signature W10 does not match the signature that was previously added to block 2 anymore.
- Block 1 and 2 are now considered no longer chained to each other.
- Blockchain rejects this change by shifting back to their previous record of the blockchain where all the blocks are still chained together (the record where Damian sent 100 BTC to George).
- If you try to change pointer in Block 2, its data changes, this signature changes and so on
- This means that altering a single block requires a new signature for every other block that comes after it all the way to the end of the chain. This is considered to be near impossible.



(Ref: "How does blockchain work in 7 steps — A clear and simple explanation." - Jimi S, Good Audience)

Step 3 — How the signature (hash) is created

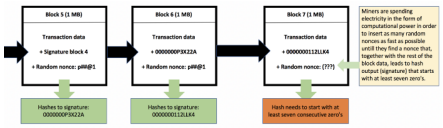
- Signature is created by a cryptographic hash function.
- Takes any string of input and turns it into a unique 64-digit string of output.
- e.g. "761A7DD9CAFE34C7CDE6C1270E17F773025A61E511A56F700D
- If a single digit of the input changes, including a space, changing a capital letter or adding a period for example, the hash will be totally different.
- But same string 'guarantees' same hash.



(Ref: "How does blockchain work in 7 steps — A clear and simple explanation." - Jimi S, Good Audience)

Step 4 — When does the signature qualify, and who signs a block?

- A block will only be accepted on the blockchain if its digital signature starts with — for example — a consecutive number of zeroes, Say, 10.
- String of data of a block needs to be changed repeatedly until that specific string of data leads to a signature starting with ten zeroes.
- Because the transaction data and metadata (block number, timestamp, et cetera) need to stay the way they are, a small specific piece of data, called 'nonce' is added to every block that has no purpose except for being changed repeatedly in order to find an eligible signature.
- This is called mining and is what miners do. More compute you have (and luck), faster the process would be.



(Ref: "How does blockchain work in 7 steps — A clear and simple explanation." - Jimi S, Good Audience)

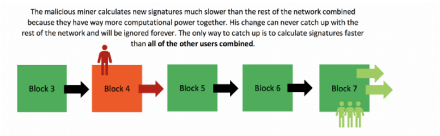
Step 4 — When does the signature qualify, and who signs a block?

- Any user on a blockchain network can participate in this process by downloading and starting the according mining software for that specific blockchain.
- When a user does this, they will simply put their computational power to work in order to try to solve the nonce for a block.
- As you can see, the hash (signature) of this block and the hash of the previous block both start with a number of zeroes.

(Ref: "How does blockchain work in 7 steps — A clear and simple explanation." - Jimi S, Good Audience)

Step 5 — How does this make the blockchain immutable?

- Let's say a corrupt miner has altered a block of transactions and is now trying to calculate new signatures for the subsequent blocks in order to have the rest of the network accept his change.
- The problem for him is, the rest of the network is also calculating new signatures for new blocks.
- The corrupt miner will have to calculate new signatures for these blocks too as they are being added to the end of the chain.
- Unless the miner has more computational power than the rest of the network combined, he will never catch up with the rest of the network finding signatures.



(Ref: "How does blockchain work in 7 steps — A clear and simple explanation." - Jimi S, Good Audience)

Step 5 — How does this make the blockchain immutable?

- What if a bad actor has more computational power than the rest of the network combined? Theoretically yes, this is possible.
- It is called a 51% attack
- It would not just require an immense amount of hardware, cooling equipment and storage space for the computational power, but also involves the risk of prosecution and, more importantly, would dramatically harm the ecosystem of the corresponding blockchain, rendering the potential returns in Bitcoin to drop significantly in value.
- This is also the reason that the more users participate in the mining process, the more secure a blockchain becomes.

Step 6 — How is the blockchain governed? Who determines the rules?

- A governance model of democracy, so Majority wins.
- It requires the majority of the computational power to create the longest version of the blockchain.
- This is also how an altered block is automatically rejected by the majority of the network.
- On the Bitcoin blockchain, all transaction history and wallet balances are public (blockchain.info).
- Anyone can look up any wallet or transaction that has ever occurred all the way back to the first transaction that was ever made (on January 3rd, 2009).
- Although wallet balances can be checked by anyone publicly, the owners of those wallets remain largely unknown.

Final step, step 7 — Where does this leave cryptocurrencies?

- Most cryptocurrencies are built upon their own blockchain protocol that may have different rules from the Bitcoin blockchain.
- Cryptocurrencies can however be given any kind of value, depending on their issuer. They could be referred to as 'tokens'.
- Any sort of value can be attached to a 'cryptocurrency' token.
- All these cryptocurrency transactions are registered on various blockchains and can be exchanged online through cryptocurrency exchanges such as Binance.

Ethereum

How Ethereum Works?

References

References

Many publicly available resources have been refereed for making this presentation. Some of the notable ones are:

- "How does blockchain work in 7 steps — A clear and simple explanation." - Jimi S, Good Audience

Copyleft ⓒ Send suggestions to yogeshkulkarni@yahoo.com