**Blockchain**

1 – Blockchain is a **distributed public ledger** of immutable transaction, it uses cryptography to secure transactions and block.

Blockchain is a distributed ledger system, there is no central entity that is verifying or validating the transactions. All the participants receive, verify and validate the transactions and log it in system.

**Immutable transactions** make it impossible for any entity (for example, a government or corporation) to manipulate, replace, or falsify data stored on the network. We cannot remove or do alteration in existing transactions.

**Cryptography or cryptology** is the practice and study of techniques for [secure communication](https://en.wikipedia.org/wiki/Secure_communication) in the presence of third parties called [adversaries](https://en.wikipedia.org/wiki/Adversary_(cryptography)). **Cryptography** is about constructing and analyzing [protocols](https://en.wikipedia.org/wiki/Communications_protocol) that prevent third parties or the public from reading private messages.

Cryptography is used to secure the system

**Shaking the system**

Major impact on financial systems

* Banking & Payments
* Supply chain management
* Educational records

It minimizes the impact of middle man e.g. banks in transactions. Blockchain makes the transactions peer to peer.

DApps – Decentralized applications

Web 1.0 – Static pages, we cannot interact with these pages, cannot send messages

Web 2.0 – Facebook, twitter. Social media, we can interact with them, send messages, upload content

Web 3.0 – new era is of web 3.0 – Decentralized applications

**Problem with traditional systems**

* Centrally controlled
* Need to trust
* 3rd party/middleman
* No transparency
* Mutable

**Industries disrupted by blockchain**

* Banking and payments
* Supply chain management
* IOT
* Insurance
* Private transport and ride sharing
* Online data storage
* Charity
* Voting
* Government
* Health care
* Online music
* Retail
* Crowdfunding

**Bitcoin Uses:**

* Secure digital signatures
* Not requiring the use of a third party
* Proof of work
* Hashing the transaction together to form a chain ( transactions should be connected)

**Bitcoin properties**

* Decentralization – peer to peer ledger
* Immutable – cannot be altered, changed
* Fungible – each bitcoin is equal, maintains it value (not like a banana)
* Permission less and without borders
* Divisible (down to 8 decimal)
* Scarcity – 21 million coins ever
* Transferable – can send any amount in seconds, compare to gold

**HASHING Technique**

Unrecognizable 20 digit code to identify the person/transaction

Even a single coma, dot can change entire 20 digit code.

**Flooding/ gossip protocol/ broadcasting - Protocol**

8 node to 8 nodes

Every node picks the transaction from transaction pool and generate the block.

Solves a puzzle. Generate proof of work to generate. It takes 10 minutes to generate it. And any one of the node wins it. And it announce in the network I will. All other nodes **stop working. All node receive the puzzle node from, if valid it will save it.**

Every distributed software sync data before it is ready to use. Ledger will be sync with the network then our node will be ready for the transactions.

**The Blockchain puzzle:**

Why we need a puzzle to solve:

There should be some qualities to generate a hash code. Otherwise it is a matter of seconds to generate a hash code. And every node can generate this hash code within seconds and I can be corrupted easy. So in blockchain, it implements some check, rules, and qualities to generate the hash code. E.g. e.g. hash code should start with 6 zeros.

1 information should have only one hash code.

So if we are going to make a hash code for HELLO, but it does not start with 6 zeros. Here plays the role NONCE – non siniker value – (number only used once) it is a counter that concatenates with HELLO to generate the hash, until it finds to generate the hash code that starts with 6 zeros. It will take time to find a hash code so that starts with 6 zeros.

So difficulty levels sets according to the time taken to generate the hash code by the node.

**Use Old Technologies:**

Accounting ledger

Cryptography

Peer to peer Network

Blockchain use all old technologies that are mentioned above, it defines a new technique/process by using old technologies to use them in an effective way.

**Hashing**

Key concepts: Hashing, public key inscription and mining. By using this blockchain is immutable and unchangeable.

**Hashing:**

It changes any information into a string of alphanumeric strings. It encrypts the data. It is one way encryption. SHA256 – it generates code of 256 bits.

A hash function can take input of any length (even a content of book is passed) it will generate a fixed length code.

It is also called as message digest.

It is also called as digital fingerprint. This is because there is no way this digest can represent any other string.

Hash code is irreversible, it cannot be reversed.

For example, we generate the hash code of word HELLO, it generates a code like

2cf24dba5fb0a30e26e83b2ac5b9e29e1b161e5c1fa7425e73043362938b9824

And now if we enter a coma in the end, entirely a different hash code will be generated:

3d162cb17e6ffe8da81ef3bc00c7862d4df2e330ca6f1178a3a8227e535e6cef

<https://xorbin.com/tools/sha256-hash-calculator>

**Public Key encryption:**

It is simple encrypting technique with keys. A unique encrypted data is generated for an input e.g. HELLO using a private key. This message will only be decrypted using public key.

Public key

Private Key

Message encrypted with private key will be decrypted using public key

and the message encrypted with public key will be decrypted by private key and vice versa.

Example link:

<http://cobweb.cs.uga.edu/~dme/csci6300/Encryption/Crypto.html>

**Mining and understandable block**

As we said, every node solves a puzzle, generate a hash code, with qualities, with some difficulty level so that it takes time. We need to see a demo, how it works;

<https://anders.com/blockchain/>

first block of a blockchain is called a **Genesis Block**

**Bitcoin**

A collection of concepts and currencies, it behaves like conventional currencies, can be purchased, sold and exchanged for other counties at specialized currency rates, they are completely virtual with no physical existence, fast secure and borderless.

Unlike traditional currencies, bitcoin are entirely virtual, the coins are implied in transactions that transfer value, users own keys that proves ownership of bitcoin in the bitcoin network, user sign transaction with keys to unlock the values and spend it by transferring it to a new owner, keys are often stored in a digital wallet, possession of the key is the only prerequisite to spending bitcoin, putting the control entirely in the hands of each user.

Every bitcoin is a transaction. There are no bitcoin in wallets, there are keys. Bitcoin generates through a process called ‘Mining’

The node that wins in generating a block, it gets 12.5 bitcoins and transaction fee. Bitcoin generates in every 10 minutes. After every 4 years, bitcoin generation gets half. Total 21 million bitcoins will be generated in 2140.

**4 Process/ Techniques**

Peer to Peer network, Public ledger, Consensus rules, Proof of work algorithm

**Double Spend Problem**

Why digital currencies do not succeed before, because of below questions:

1 – Is digital currencies authentic?

2 – Is digital currencies send multiple time?

3 – Can digital currencies belong to 2 or more persons?

Bitcoin resolves all these concerns.

**Bitcoin wallets**

Like we have browsers, all these browsers follow protocol (http), so we can see any website in any of these browsers.

Similarly, bitcoin wallet is using protocols

Cold storage – Paper Wallet – Hardware wallets – wallet includes private keys to secure

**Bitcoin Client software**

4 type of bitcoin client software

Reference Client (bitcoin Core) Reference implementations

Full node (include full bitcoin and wallet software)

Lightweight (SPV) wallet (Does not include complete bitcoin, it communicate using internet)

Third party API (do transaction through a server, server communicate to Network)

**Wallets**

Mycelium

Electrum (install it, it give you 2 software, normal – testnet (fake network for transaction learning)

Generate mnemonic (phrase) in case your wallet is lost. You need this 12 word phrase

Wallet listen the transactions. Wallets only have addresses and private keys. Wallet has to confirm the transaction on reading. It is in unconfirmed state. Transaction waiting to include in a block and added to blockchain. In traditional terms it is known as **CLEARING**. Once transaction is confirmed you will get your Bitcoin. Bitcoin address is generated by public/private keys with multiple algorithms, it cannot be reversed.

Bitcoin address generated by wallet is **NOT** known to bitcoin network not it is registered with any bitcoin system. Bitcoin address is simply a number that corresponds to a key that you can use to control access to the funds. Until the moment this address is referenced as the recipient of value in a transaction posted on the bitcoin ledger, the bitcoin address is simply part of the vast number of possible addresses that are valid in bitcoin. Once address has been associated with a transaction, it becomes part of the known addresses in the network.

**How Bitcoin works**

**Transaction Input and output**

Double entry book keeping

Input – 1 bitcoin from my account

Output – 1 bitcoin transfer to other account

Input and output are not exactly the same. It is slight difference called fee.

Input 0.55

Output 0.50

Diff 0.05 (implied Transaction Fee)

**Transaction Chains**

Every transaction output is an input to another transaction

Any transaction amount will remain the same, it cannot be changed, or cannot send partially

E.g. an INPUT transaction to Alice is 0.1000 🡪 output to Alice 0.1000 BTC

0.0005 BTC (Transaction Fee)

INPUT from Alice 0.1000 BTC 🡪 output to Bob’s 0.0150 BTC (spent)

0.0845 BTC (unspent/Returned–Change)

0.0005 BTC (Transaction Fee)

Every transaction is connected with previous transaction. To remain its connectivity, we cannot change the amount of bitcoins in a transaction. For example if I have 2 bitcoins in a transaction, then I have to send 2 bitcoins in next transaction; 1 bitcoin will send to other and 1 bitcoin will be back to myself.

**Making Change**

The amount coming back/reverse in a transaction is called change. This concept is same as in real currency.

The change address does not have to be same address as that of the input address and for privacy reasons it is often a new address from the owner’s wallet.

Some wallets use different strategy for the change transaction amount. They use different address to save the change transaction amount for privacy reasons.

**Common Transaction Forms**

1 – Normal transaction (1 input 🡪 2 outputs)

2 – Aggregation transaction (multiple inputs 🡪 2 outputs)

3 – Common transaction (Single input 🡪 Multiple outputs) wallet facilitates and construct the transaction itself to send 1 transaction to 3 different addresses.