



# BLOCKCHAIN FAQs - ANSWERED IN 1 HOUR

## FREQUENTLY ASKED QUESTIONS



# BLOCKCHAIN FAQs

## WHAT IS BLOCKCHAIN? WHY IT IS MAKING SO MUCH BUZZ?

- It's a decentralized database (ledger) which stores information in the form of transactions
- It can be public or private and store the data Immutably
- It is highly secure due to decentralization
- Data gets recorded via consensus based algorithms
- Generally exist over peer-to-peer network
- It's a foundational technology of Bitcoin.
- Blockchain use-cases go beyond the online cash transaction systems like Bitcoin.
- It's use cases are revolutionizing the way we look at the technology.
- Application like smart contracts which are built on top of Blockchain are the examples why the whole world is going gaga about Blockchain

# BLOCKCHAIN FAQs

## WHAT ARE THE DIFFERENCES BETWEEN BITCOIN & ETHEREUM?

- Although there are some significant technical differences between the two, the most important distinction to note is that Bitcoin and Ethereum differ substantially in purpose and capability
- Bitcoin offers one particular application of blockchain technology, a peer to peer electronic cash system that enables online Bitcoin payments.
- While the bitcoin blockchain is used to track ownership of digital currency (bitcoins), the Ethereum blockchain focuses on running the programming code of any decentralized application.
- In the Ethereum blockchain, instead of mining for bitcoin, miners work to earn Ether, a type of crypto token that fuels the network.
- Beyond a tradeable [cryptocurrency](#), Ether is also used by application developers to pay for transaction fees and services on the Ethereum network.

# BLOCKCHAIN FAQs

## HOW BLOCKCHAIN IS DIFFERENT FROM MYSQL?

- MySQL is a freely available open source Relational Database Management System (RDBMS) that uses Structured Query Language (SQL).
- It's a centralized technology for storing data in MySQL servers.
- Blockchain can be seen as a decentralized database with key-value pair of data (Meta data)
- More stable & secure due to decentralization
- [Blockchains](#) are essentially databases with some inbuilt pre-agreed technical and business logic criteria, kept in sync via peer-to-peer mechanisms and pre-agreed consensus algorithms. With respect to immutability, the way the data is structured is significant.

# BLOCKCHAIN FAQs

## HOW BLOCKCHAIN IS IMMUTABLE?

- **Immutable** means that something is unchanging over time or unable to be changed.
- So in our context, it means **once data has been written to a blockchain no one, not even a system administrator, can change it.**
- This provides benefits for audit. As a provider of data you can prove that your data hasn't been altered, and as a recipient of data you can be sure that the data hasn't been altered. These benefits are useful for databases of financial transactions.
- Data stored in Blockchain is basically stored in decentralized network through consensus based algorithm. If a server wants to update any existing record he has to ensure that every other server also modify the record.
- In another language it is highly difficult to tamper is recorded data.
- At the same time it will be highly easy to catch any modification because whole network has the original ledger to verify it's authenticity.

# BLOCKCHAIN FAQs

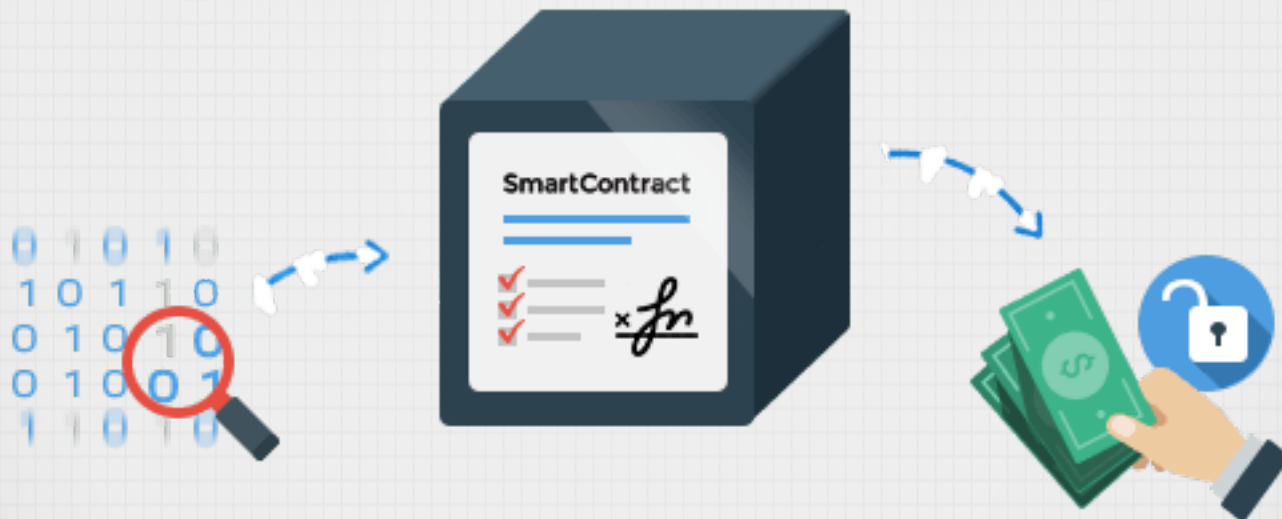
## HOW CAN BLOCKCHAIN BE CONSIDERED SAFE & SECURE THAN THEIR ALTERNATIVES?

- Due to Decentralization
- Due to Immutability of the record
- Proof-of-work
- It will be computationally very expensive to modify the data stored in Blockchain due to proof-of-work

# BLOCKCHAIN FAQs

## WHAT ARE SMART CONTRACTS?

- Smart contracts is a term used to describe computer program code that is capable of facilitating, executing, and enforcing the negotiation or performance of an agreement (i.e. contract) using blockchain technology.
- The entire process is automated can act as a complement, or substitute, for legal contracts, where the terms of the smart contract are recorded in a computer language as a set of instructions.



# BLOCKCHAIN FAQs

## HOW SMART CONTRACTS ARE BETTER THAN PAPER CONTRACTS?

- Traditional physical contracts, such as those created by legal professionals today, contain legal language on a vast amounts of printed documents and heavily rely on third parties for enforcement.
- This type of enforcement is not only very time consuming, but also very ambiguous. If things go astray, contract parties often must rely on the public judicial system to remedy the situation, which can be very costly and time consuming.
- Smart contracts, often created by computer programmers through the help of smart contract development tools, are entirely digital and written using programming code languages such as C++, Go, Python, Java.
- This code defines the rules and consequences in the same way that a traditional legal document would, stating the obligations, benefits and penalties which may be due to either party in various different circumstances. This code can then be automatically executed by a [distributed ledger system](#).



# BLOCKCHAIN FAQs

## WHAT'S WRONG WITH SMART CONTRACTS?

- Still not very stable technology
- Smart contracts are far from perfect.
- What if bugs get in the code?
- Or how should governments regulate such contracts?
- Or, how would governments tax these smart contract transactions?

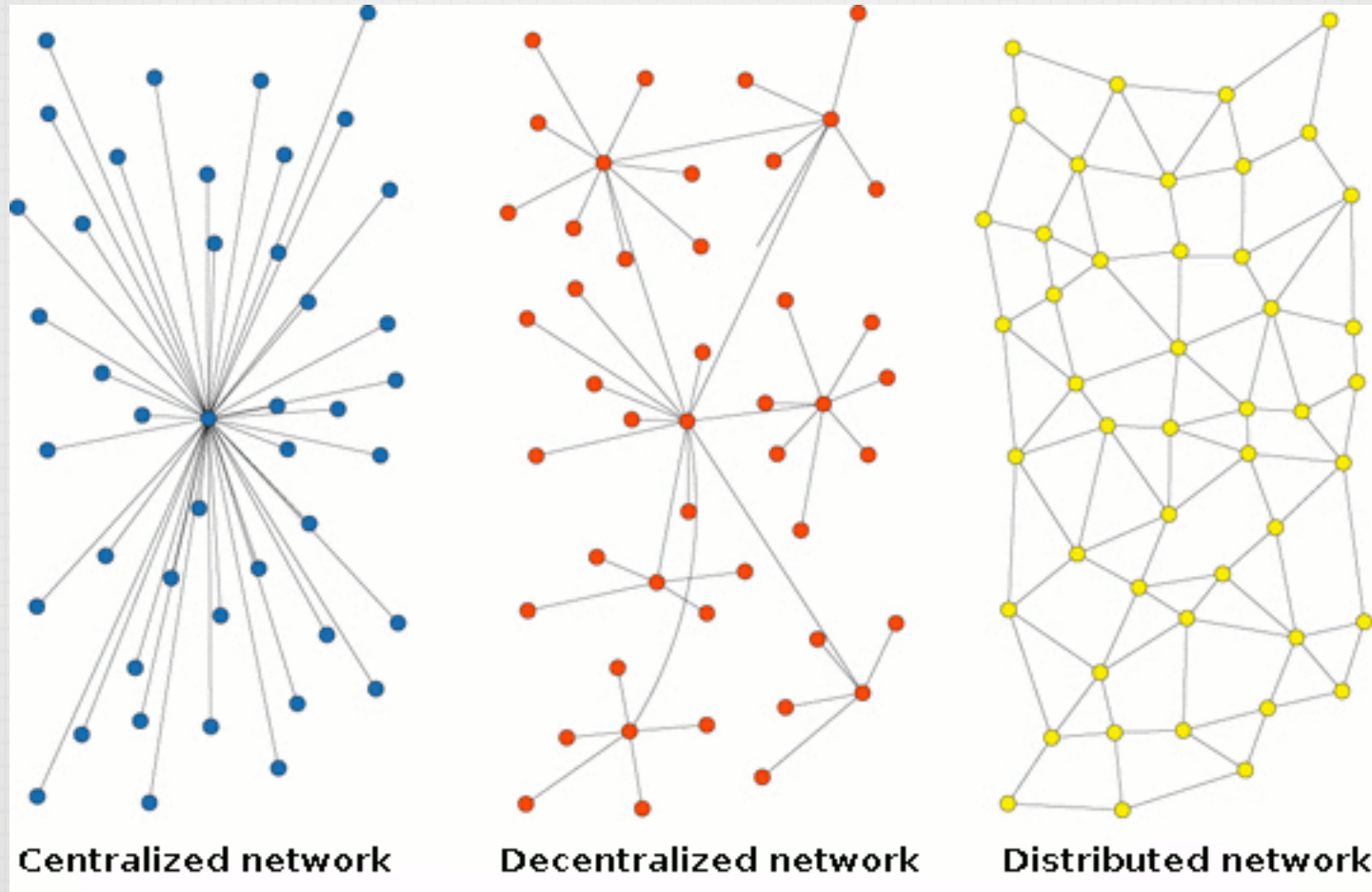
# BLOCKCHAIN FAQs

## WHAT IS DECENTRALIZED LEDGER & WHAT ARE THEIR TYPES?

- A ledger which is stored on decentralized network
- A Blockchain can be considered as a good example
- Decentralized ledger can be broadly of two types:
  - **Private Ledger:** Permissioned Ledger where permission to read & write is controlled by a private entity or a group
  - **Public Ledger:** Permissionless Ledger where anyone can read from or write into the ledger

# BLOCKCHAIN FAQs

## WHAT IS PEER-TO-PEER, CENTRALIZED & DECENTRALIZED NETWORK MEANS?



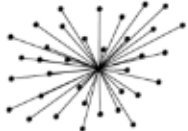

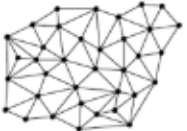






















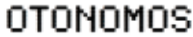





# BLOCKCHAIN FAQs

## WHAT ARE SMART CONTRACTS LANGUAGES?

- Solidity
- Serpent
- LLL
- Viper
- More..

# BLOCKCHAIN FAQs

WHAT ARE PRIMARY USE CASES OF BLOCKCHAIN AND WHY THEY ARE CONSIDERED THE PRIMARY USE CASES?

 PAST	 PRESENT	 FUTURE	<h2>Blockchain Startups</h2> <p>Top Blockchain startups disrupting non-financial markets</p>  Venture Radar
 THE WALL STREET JOURNAL.  THE TIMES  HM Government  Hilton	 facebook  twitter  Dropbox  UBER  airbnb	  Social Networking  synereo  GEMS  Digital Identity  ONENAME  ShoCard  Art & Ownership VERISART  Bitproof.io  MONEGRAPH  colu.	<p>Cloud storage  Filecoin  STORJ.IO  TIERION</p> <p>Smart Contracts  TRUST  EP  appliedblockchain</p> <p>Anti-Counterfeiting  everledger  BLOCKVERIFY</p> <p>Supply Chain  thingchain  Tradle</p> <p>Prediction Markets  augur</p> <p>Governance  OTONOMOS  Swarm  followmyvote  BITNATION</p> <p>Internet of Things  FILAMENT </p> <p>More: <a href="https://www.ventureradar.com/">https://www.ventureradar.com/</a></p>

# BLOCKCHAIN FAQs

## WHAT IS MINING, MINER, MINING REWARD & GENESIS BLOCK?

**Mining:** The process of adding a new Block into the Blockchain by doing some computational work.

**Miner:** The computer which will do the task of mining.

**Mining Reward:** Every miner get some virtual tokens of cryptocurrency in exchange of their service of adding a Block.

**Genesis Block:** This is the very first Block into the Blockchain on top of which every other block is built.

# BLOCKCHAIN FAQs

## WHAT EXACTLY MINER DO FOR THE REWARD?

- Miners are asked to solve a very complex computation problem to identify that next block in the Blockchain.
- In return of doing this computation they are rewarded with some virtual coins like bitcoins, Ethereum etc.
- Miners use CPU power to identify a nonce (number used only once) through which they can create the digest/signature of the next block in the Blockchain which is less than the recently added block. Miner who does it first announces the answer to the entire network & gets the reward (Currently 25 BTC)

# BLOCKCHAIN FAQs

## WHAT IS CONSENSUS ALGORITHM? WHY WE NEED IT?

- Method to resolve a conflict?
- How to resolve certain disputes?
- Who will do the arbitration in case of dispute?



# BLOCKCHAIN FAQs

## WHAT IS MERKEL ROOT? WHAT IS THE USE OF IT?

Root of the binary Tree of hashes of Transactions.

In Bitcoin is uses double SHA-256 hashes

In case of odd number of nodes in a row, last node's digest taken twice to make it even.

Example:

$d1 = \text{dhash}(a)$

$d2 = \text{dhash}(b)$

$d3 = \text{dhash}(c)$

$d4 = \text{dhash}(c)$

# a, b, c are 3. that's an odd number, so we take the c twice

$d5 = \text{dhash}(d1 \text{ concat } d2)$

$d6 = \text{dhash}(d3 \text{ concat } d4)$

$d7 = \text{dhash}(d5 \text{ concat } d6)$

Where  $\text{dhash}(a) = \text{sha256}(\text{sha256}(a))$

It is used to check the integrity of the transactions stored in the Block. All someone has to do is just to calculate the Merkle root & check if it matches the existing root.

# BLOCKCHAIN FAQs

## OPEN PLATFORMS TO BUILD DECENTRALIZED BLOCKCHAIN APPS?

- MultiChain, Checkout our course on MultiChain to setup private Blockchain in AWS.
- OpenChain
- Hyperledger
- Ethereum
- Bitcoin

# BLOCKCHAIN FAQs

## WHAT ARE HARD FORKS IN BLOCKCHAIN? WHY WE NEED IT?

A forceful method to update the core software & it's foundational protocol of the Blockchain to invalidate (or vice-versa) few previously mined Blocks in the Blockchain.

This is generally done to recover the Blockchain from drastic damage or attack.

In private Blockchain this can also be the part of business logic where it is being executed because a company has decided to pivot into some different direction.



# BLOCKCHAIN FAQs

## WHAT ARE SOME EXAMPLE OF BLOCKCHAIN ATTACKS?

- 51% Attack:
  - Often considered a very large flaw in public Blockchain like Bitcoin's Blockchain
  - Let's say if a single entity contributed the majority of the network's mining hashrate, then they would have power to manipulate the public ledger
  - It is theoretically possible because Blockchain is publically open
  - It is likely that confidence in the currency will be lost & price of the currency will decline rapidly
- Eclipse Attack:
  - Cripple a node in such a way that it can not talk to other nodes in the network
  - In that case less %tage owner of network hashrate can launch the attack.
  - Lets say there are 3 nodes with 30%, 30% & 40% network hashrate power.
  - If the node 2 is crippled in such a way that it can not talk to node 1 then node 3 can control the Blockchain's public ledger.

# BLOCKCHAIN FAQs

## WHAT IS HASHRATE & HOW IT CAN AFFECT THE BLOCKCHAIN?

- The hash rate is the **measurement unit of the processing power of the Bitcoin network**.
- The Bitcoin network must make intensive mathematical and cryptography related operations for security purposes.
- For example, when the network reaches a hash rate of 10 Th/s, it meant it could make 10 trillion calculations per second.

# OUR CONTACT DETAILS

**COMPANY:** Tosh Academy

**ADDRESS:** Gurgaon, India

**WEBSITE:** <http://learn.toshendra.com>

**EMAIL:** [learn@toshendra.com](mailto:learn@toshendra.com)



[fb.com/toshendra11](https://fb.com/toshendra11)



[@toshendrasharma](https://twitter.com/toshendrasharma)

THANK YOU FOR YOUR TIME