Introduction

Blockchain- Despite the inherent 'Block' in it, the name has traversed more miles than any other technical term in the recent past. It is echoing in almost all existing IT infrastructures; posing a potential threat to the very existence of the present establishments. The blockchain is said to be the technology of future. Here we are trying to simplify the things for all those who wish to understand the technology. As we indicated in the preface, the book is meant for anyone who wishes to start with blockchain technology.

We have organized the book into two major sections, while the first section provides the basics of Blockchain and related terminologies, the second section is purely dedicated to different tools and technologies that emerged along with blockchain.

First section is further divided into six major topics. Blockchain, Cryptocurrency, Bitcoin, Ethereum, Hyperledger and Tokens which covers all the basic ingredients for starting with the blockchain technology. In the first part, which is about blockchain, we have discussed what blockchain, its working principles, the historical developments, the technical implementations, its application areas and the possible future of Blockchain. The second topic is about Cryptocurrencies, which is an essential topic that must be learned before going deep into the famous blockchain protocol Bitcoin. A general overview of cryptocurrencies as well as their working principles is discussed here. The third topic is about the most popular blockchain platform- Bitcoin. Here we discussed the topics like bitcoin and its background, bitcoin working, bitcoin mining, the value of bitcoin etc. In the next topic which is about Ethereum, we have included the details of another popular blockchain platform – Ethereum. The reader will get an overview of the second most popular blockchain platform from this section.
Ethereum related terms and terminologies like the smart contract, Solidity, DApp, Etherscripter, Ether etc. are also simplified here. The fifth topic is about the

ambitious open source project Hyperledger. The project, its objectives, and the products that have developed under the project etc. are discussed in this section. We have alsoincluded a comparative study of all of these technologies to give a better understanding. The final topic is exclusively dedicated to -Tokens, which is a thriving application area of blockchain technology.

Second section of this book doesn't need much introductory comments, all the topics in the second section is more or less independent. The section provides information about different blockchain related tools like wallets, Programming languages and IDEs, Blockchain platforms and development frameworks.

To simplify the things further we have tried to include images, infographics, tips and quick info bars wherever possible. Moreover, most of the terms and terminologies we used are explained in the beginning of the book. Make use of all these extra information provided while going through the book and have a good read.

Terms and Terminologies

Some of the terms and terminologies you may encounter while going through this book is described here.

Use it as a quick reference.

Block

- Block is used to store the transaction along with their hash value and data

Transaction

- Any state change occurred in a blockchain

Smart contract

- self executing contract with terms and conditions written in lines of codes

Ledger

- Blockchain ledger is used to record the transactions in a blockchain

Token

- Digital asset

Cryptocurrency

- Digital asset

Bitcoin

- Most popular cryptocurrency

Hash

- The encrypted value of the data in the block.

SHA256

- Hashing Algorithm

Node

- Each computer connected to the blockchain network

Solidity

- Programming language for writing smart contracts in Ethereum

Hyperledger

- Blockchain platform

Ethereum

- blockchain platform

Baas

- Blockchain as a service

ERC20

- Ethereum token standard

ICO

- Initial coin offering

DApp

- Decentralized applications

IoT

- Internet of things

PoW

- Proof of work

PoS

- Proof of stake

Mining

- The validation process in a blockchain (in Bitcoin and Ethereum)

Miner

- The nodes which perform mining

Wallets

- Digital wallet to store, send and receive cryptocurrencies and other digital assets.

Testnet

- Test blockchain networks for development and testing purpose

BFT

- Byzantine fault tolerance principle.

BIP

- Bitcoin improvement proposal

Genesis block

- First block in the blockchain

Composer

- blockchain development framework in hyperledger fabric

Participants

- Those who have an account in the blockchain and performing any transactions.

Peer2Peer(P2P)

- Decentralized network architecture. There is no dedicated server in this case

Consensus

- General agreement between the participants in the blockchain

An Introduction to Blockchain

The Beginning

Before going into the details of working principles and other aspects of blockchain; let's look into the genesis of the technology itself. The conceptual framework behind blockchain was first put forward by a group of researchers in 1991. The idea was initially intended for time-stamping digital documents such that backdating them will not be possible thereafter. However, the idea went mostly unused until it was again mentioned by Satoshi Nakamoto in his white paper
"Bitcoin: A Peer-to-Peer Electronic Cash System".

It may be the first time in history that the inventor of a game-changing technology has completely gone anonymous. Satoshi Nakamoto; an anonymous person/group is said to be behind the first blockchain, which is Bitcoin. Bitcoin is the first blockchain came into existence and it was in 2009. In the following years, the bitcoin became popular, and the underlying technology became even more popular. **So the confusion and lack of clarity among people start from the origin itself; a product and its related terminologies went viral before the technology behind it. And when the blockchain displayed its real potential, people were trying to relate it with the bitcoin terminologies; the result was total misconception and confusion.** But it is the other way; start from blockchain and then try to understand bitcoin.

Why Blockchain

It is another question that must be addressed first before going into the details of the technology. To say technology is revolutionary; obviously, it must have a lot of advantage over existing technologies. Here are some advantages of blockchain over existing systems of different domains. Blockchain is:

- **Decentralized**
- **Distributed**
- **Secure and Faster**
- **Transparent and Immutable**

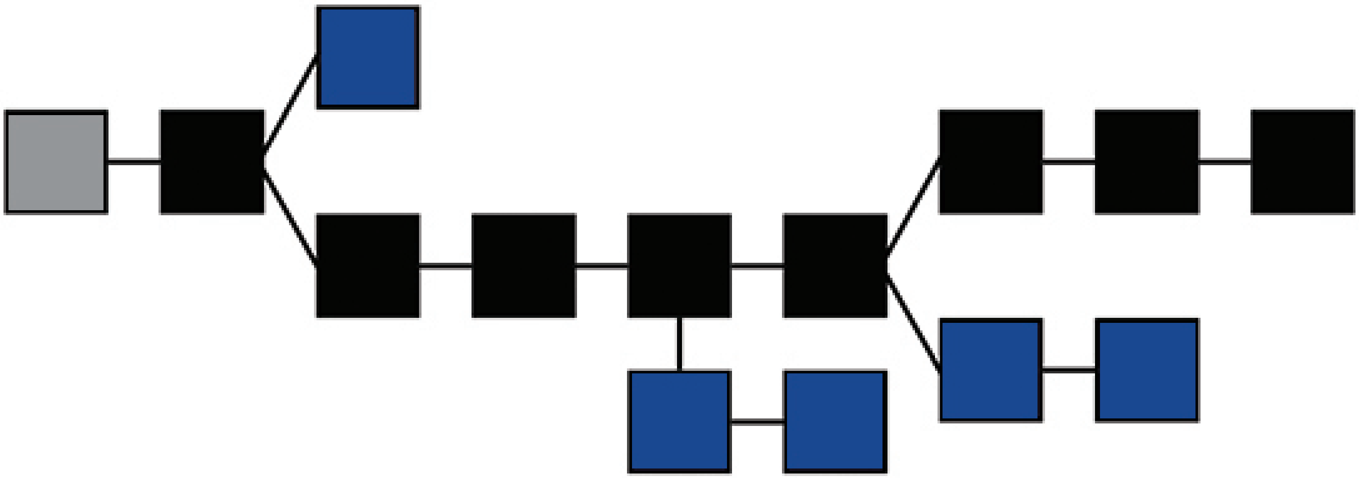
The features can be understood well if we look the data structure, data distribution, data validation (Authentication of a piece of data in blockchain) and other related terminologies of blockchain.

The Structure of Blockchain

According to IBM, blockchain is a shared, distributed ledger that facilitates the process of recording transactions and tracking assets in a network. The asset may be a tangible asset like property, house, vehicle or an intangible asset like digital currency, intellectual property rights, etc. Basically, it stores Data, and records its movements in a distributed environment. Let's look into its details.

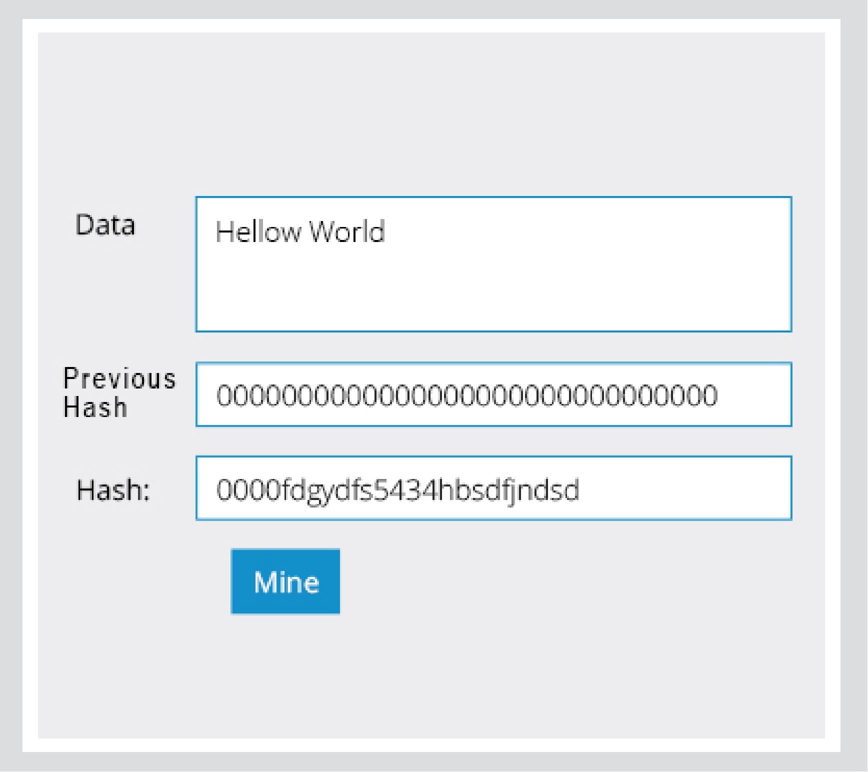
It is a distributed database or a public registry that keeps details of assets and its movements/transactions across a P2P network. Each transaction will be secured through cryptography and later all the transaction history will be grouped and stored as blocks of data. Then the blocks are linked together with cryptography and secured from modification. The whole process will
create an unforgeable, and immutable record of the transactions that happened across the network. Additionally, this blocks of records are copied to every participating computer in the network, so everyone will have access to it. The great advantage of blockchain is that it can store any kind of asset, its ownership details, history of the ownership and location of assets in the network. Whether it is the digital currency bitcoin, or any other digital assets like a certificate, personal information, a contract, title of ownership of IP, even the real-world objects.

The powerful feature of Blockchain is that we can create a shared reality across non-trusting entities. That is all of these participating nodes in the network do not need to know each other or trust each other because each has the ability to monitor and validate chain for themselves. The irony is that the mutual distrust among participant is the thing which keeps the blockchain secure and verified.



Data Structure of Blockchain

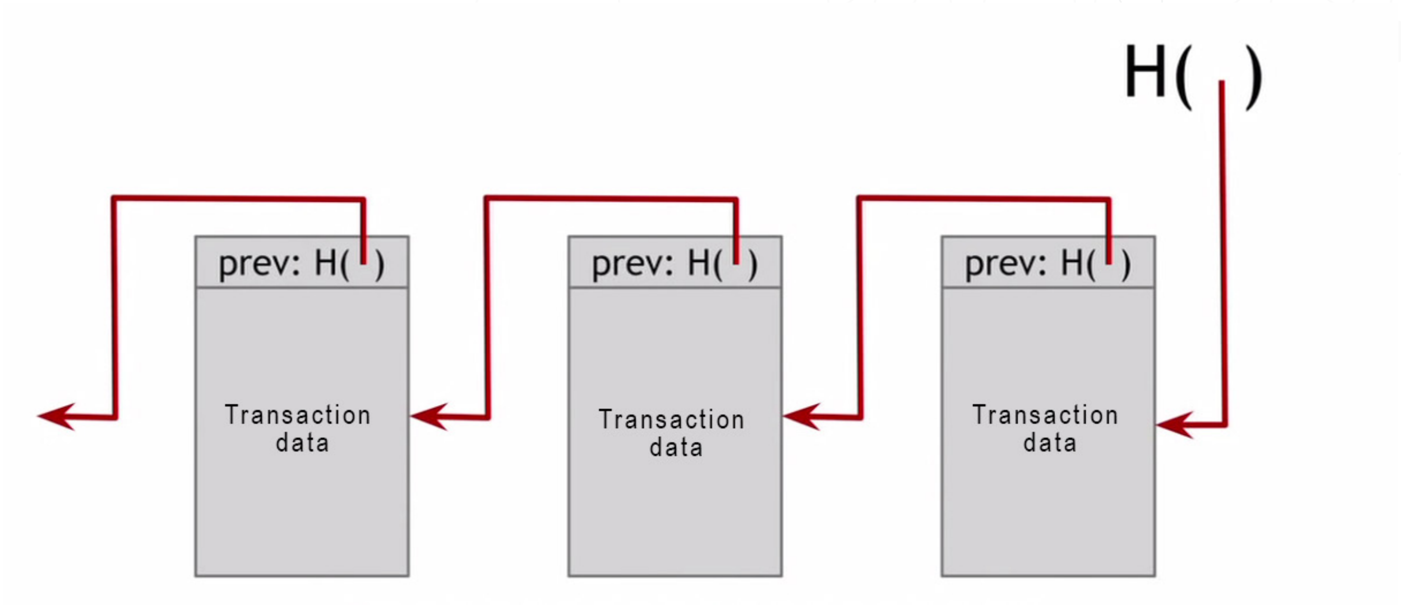
The data in blockchain is stored as individual blocks, that's why it is called Blockchain. Just like a linked list, the Blockchain is a collection of blocks linked together. So what does the block actually contain? Each block in a blockchain will have the following fields.



Data	Hellow World
Previous Hash	00000000000000000000000000000000
Hash:	0000fdgydfs5434hbsdfjndsd

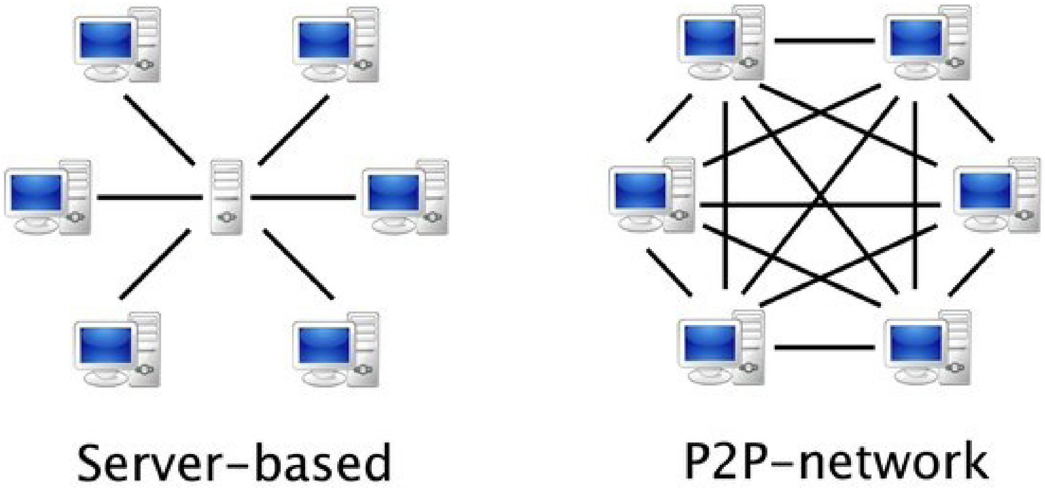
1) Data: Stores the data
2) Previous hash: Stores the hash of the previous block
3) Hash: Hash value for the current block which can be used to refer this block

As far as the user is concerned the Data field is the most important thing. The actual data (like transaction details, asset details etc.) are stored in this field. Previous hash will store the hash values of the previous block (consider it as a link to the previous block), the blocks are connected through this value.



Data Distribution in Blockchain

We saw that blockchain has its own unique Data storage structure, the data distribution in a blockchain has also a different approach. **They don't follow the widely adopted client server model rather the Peer to Peer model. The peer to peer data distribution approach gives the reason behind unfettered nature of Blockchain; there is no central authority to control.**



Unlike the client-server model, In P2P network the data is stored in all the participant nodes in the network. All the individual nodes will have the copy of the entire 'Blocks' and a single change in a particular block will be updated in all the nodes.

But here is the problem, in Client-Server model the data is stored in DB after verification of a central authority; but in P2P network there is no central authority, then how does the authenticity of data assured? The answer is the validation process and consensus mechanism of the blockchain network

Block Validation

As we described above; the asset and its transactions are stored as connected blocks in blockchain. Only the valid transactions are added to the blockchain. Technically saying, Blockchain validation is simply the process of finding the block hash. In a blockchain, all the blocks are added to the blockchain after validation only. Whenever a transaction takes place in the blockchain it will be added to a block; sometimes one transaction per block and sometimes several transactions per block. It depends on the block size and the nature of the network. When a transaction is added to the block, it must undergo a validation process before it is being added to the blockchain as a valid block. The hash value for the block can be calculated using some algorithms (like sha 256). The hash value has certain properties too. The main thing is that the hash value should be collision-free i.e. no two blocks should have the same hash value. Since each block is represented using the hash value it should be identical. The second property is that the hash values should be irreversible. This means the block data could not be retrievable from the hash value

Block Validators

Block validators are the nodes which participates in the process of block validation. The validators are rewarded for their effort, (In fact they are rewarded for the computational power they spent). Different blockchain protocols adopt different methodologies for selecting the validator from available pool of nodes. Some of the methods are described below.

PoW (Proof of Work)

In PoW, the mining challenge is open to all. All the miners compete each other to add the next block. A fixed reward is given to the miner who finds the solution first. In fact, the node with more computational power usually wins the race. Bitcoin uses the PoW algorithm.

PoS (Proof of Stake)

It is a common alternative of PoW. Here, the validators are chosen based on the fraction of coins they own in the system. The nodes with more number of coins have more chance to be selected than the node with lesser number of coins. In PoS the reward is in the form of transaction fee, new coins are not created for paying the validators. Presently, Blackcoin, NXT and Peercoin blockchains uses the PoS algorithm. Ethereum is also planning to shift to this method by 2018.

Proof of Activity

PoA is a hybrid approach and it is introduced to overcome some of the problems in PoS and PoW. In this method, the mining begins with PoW and at some point the process is switched PoS. Presently, 'Decred' is the only coin that is using a variation of proof of activity.

Proof of Elapsed Time

In this method, the network uses a lottery functions for implementing consensus. A lottery algorithm is used for finding the leaders from a set of nodes. So the validators are selected randomly from the pool. Hyperledger Sawtooth blockchain uses PoET method. .

Proof of Burn

In this method, the aspiring validators increase their stake in the system by sending their coins to an irretrievable location (thus the name burn). The validators are selected randomly, but those who has more stake in the system has high probability to get selected. Over the time the earned stake decays and the nodes has to burn more currency to increase their stake. The only coin that uses proof of burn mechanism is slimcoin.

At this stage we can't say which method is more efficient. Each method has its own advantages and disadvantages. Many other methods are also being introduced to attain maximum productivity on a blockchain.

Blockchain So far

Initially, it was about Bitcoin; following the trend, many other cryptocurrencies also came into the market. While some of them found their fortune, some other cryptocurrencies lagged behind. However, soon the blockchain technology found its real potential and spread to many other unpredicted domains. Healthcare Industry, Enterprise software development, financial domains like Banking, Insurance and so on; today the blockchain is drastically changing existing technology frameworks of almost all domains. According to prominent statistics websites, the blockchain market is expected to grow $20 billion by 2024.

Banking and payments

All the banking and payment systems are now moving towards blockchain. Bitcoin-like cryptocurrencies can control the payment systems without any geopolitical restrictions. ABRA is an example of bitcoin-based remittance.

Cyber Security

In blockchain, data is verified and secured using cryptography. This will restrict all unauthorized changes and hacks in the system. It removes the middlemen from the system so no one can make any unauthorized changes.

Supply chain

The blockchain can revolutionize the supply chain by providing better transparency, accountability and feedback mechanism along the supply chain. Any product can be tracked completely using the blockchain supply chain management. Each and every movement, as well as the condition of a product, can be recorded in the blockchain with IoT sensors. Blockverify and Provenance is a blockchain based supply chain management system.

Online Data Storage

Data on the centralized server like Onedrive, Google Drive etc. are vulnerable to the single point of failure. Blockchain allows distributed data storage in a more secure and robust way. Storj is such an encrypted cloud storage facility

Networking and IoT

The blockchain technology can be applied in Networking and IoT to create a decentralized network of IoT devices. This eliminates the need for a central location to handle the IoT devices.

Insurance

The global insurance market is based on trust management. Blockchain is the new way of managing the trust. Blockchain ensures trust by mutual distrust between participants. 'Aeternity' is an example of blockchain based insurance management system.

Government

Applying blockchain technology in government systems will reduce bureaucratic hurdles, red-tapism, and increases efficiency and transparency of government operations. Dubai government has already started to implement the technology.

Crowdfunding

It is a popular method of fundraising, for new startups and projects. In blockchain based crowdfunding platforms trust is built through smart contracts and online reputation systems, which eliminates the need for a central party who charges high fees for this service. New projects can release their own tokens that can later be exchanged for products, services or cash.

Multimedia and entertainment

Now blockchain has entered into the entertainment field where the third party interference is too much. The blockchain implementation in this fields will remove the middleman from the scenario. Online music is one of the entertainment areas where blockchain has already started their implementation
Eg; Mycelia & Ujo music

Real estate

It another important area where blockchain implementation will make a drastic change. The current real estate system is facing a lot of ownership and transfer issues. The blockchain implementation of this field can control the entire real estate systems with shared ledgers.

E.g; In India, the Andhra Pradesh state government has started implementing the complete land registration through blockchain.

There are much more other areas on the list. Like Voting, Healthcare, Forecasting, Transportation, Energy management, etc. Not only blockchain applied solutions but industry-specific blockchain development frameworks, blockchain management software, DApp and Digital Asset management software etc. also emerged along with blockchain. And many more tools are being introduced as it grows. All these tools and frameworks are making blockchain development and management easier than before. So the development and deployment of blockchain applied solution have become easier than before. In the upcoming chapters, we will discuss some of the prominent blockchain development frameworks, Blockchain development projects, Management tools and other related tools.