International Journal of Research
Available at https://journals.pen2print.org/index.php/ijr/
e-ISSN: 2348-6848
p-ISSN: 2348-795X
Volume 06 Issue 09
August 2019

# A Novel Approach to The Blockchain Technology Overview

**Amos R[1], Anakh K A [2], Chandana M[3]**

[1]Assistant Professor, Department of MCA, MIT Mysore, seeamos@gmail.com
[2] Project Manager, ARCCOM, Bangalore, anakh.k@ar-ms.in
[3] Trainee, Hash Foundry Pvt Ltd, Mysuru, chandu.mistigowda@gmail.com

A **Block Chain** is a block of chains that contains information. **Block Chain** Refers to a Data Structure. **Block Chain** is a Distributed Ledger that is completely open to anyone.

In Year 1991, group of researcher and scientists were intended to work on timestamp digital document. Their main motive was not possible to backdate and tamper with them.

The most important property or feature of **Block Chain -** Once some Data has been recorded inside a **Block Chain**, it becomes very difficult to change it or It is impossible to change it.

## Blockchain – Introduction:

In recent years, there is a lot of buzz on Blockchain. Many have described this as a most disruptive technology of the decade. Especially, the financial markets could be the most affected ones.

The technology is being adapted into many verticals like Healthcare, Medicines, Insurance, Smart Properties, Automobiles, and even Governments.

However, so far the most successful implementation of Blockchain is the Bitcoin - A Peer-to-Peer Electronic Cash System, which incidentally is also the first implementation of blockchain technology. Thus, to understand blockchain technology, it is best to understand how Bitcoin System is designed and implemented.

In this article, you will learn what is Blockchain, its architecture, how it is implemented and its various features. I will site Bitcoin implementation while describing the intricacies of blockchain.

The blockchain architecture is not so trivial and many have written good articles, tutorials including several videos. These range audience from Novice to Professionals. In this tutorial, I will focus on the conceptual understanding of blockchain architecture, keeping both Novice and Professionals on mind. Before delving into the blockchain, it is important to know why the need for this new technology emerged? The answer to this question lies in what is known as **Double − Spending**.

### How Block Chain Works?

**Block Chain** Contains:

1. Data
2. Hash
3. Previous Hash

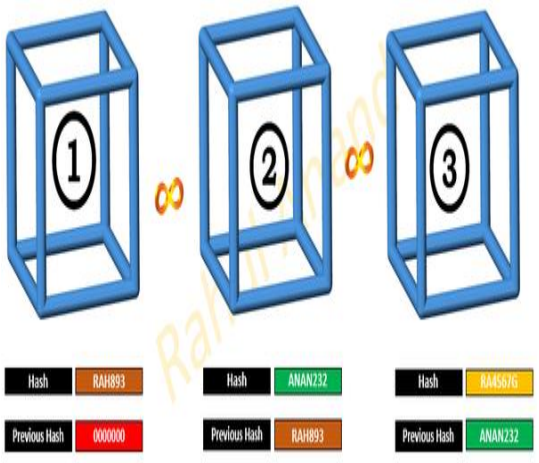
**Data:** The data stored inside a **Block**

**Chain** depends on the type of **Block Chain**.

International Journal of Research
Available at https://journals.pen2print.org/index.php/ijr/
e-ISSN: 2348-6848
p-ISSN: 2348-795X
Volume 06 Issue 09
August 2019

**Hash:** Every block will have Hash. Hash is unique. You can compare hash with a finger print. Hash identifies a block and its content. When block is created, it's Hash value is also created. Changing or Altering inside a block will create a new block and will create new Hash value. Hashes are very useful, if you want to detect any changes in the block. If finger print changes - it's no longer the same block.

Previous Hash: The third element inside a block is the Hash of previous block. This efficiency creates a chain of blocks and it's this technique only that makes a **Block Chain** so secure.




n above diagram - I am showing you three blocks, Say Block-1, Block-2, Block-3. For Block-2 Previous Hash value is similar to Hash value of Block-1. For Block-3 Previous Hash value is similar to Hash value of Block-2. We can find that all blocks are inter-linked to each other and forming a chain.

But Block-1, Hash Value is 0000000 and it being the first block - it is called as Genesis Block.

If anyone tampers Block-2, then Hash Value ANAN232 will change and will create new Hash Value and Say RAHULANAND2299. Then Previous Hash of Block-3 will be invalid. So all the Blocks in the chain will be invalid.

So tampering a single Block in Block Chain will invalid all the blocks. This concludes - How Secure is Block Chain.

**Bitcoin** is one of the example of **Block Chain.** The data in Bitcoin **Block Chain**stores transaction such as Sender Address, Receiver Address and Amount of coins. **Block Chain**are being targeted to use in different domains such as - Financial, Government, Medical, Stocks, Industries etc.

## Blockchain Categories:

Blockchains has many variations depending on how they are configured. The information stored on the blocks and activities performed by various individuals on the networks of Blockchain can be controlled with these variations.

### Private Blockchain

A private Blockchain allows entry for only selected individuals of verified participants, which is similar to private business, one can choose for implementation of private Blockchain. The participant needs a verified invitation or a validation done by the network operators to join a private network. Basically, a private blockchain is not decentralized, and it operates as a closed distributed ledger, it is a secure database based on cryptography concepts.

### Public Blockchain:

This is open to everyone, anyone can join and participate in activities involved in establishing a Blockchain network. It operates on a scheme of providing incentives that encourage new individuals in keeping the network agile. These

blockchains provide a valuable solution from the perspective of a truly democratized, decentralized and authority-free operation.

**Permissioned Blockchain:**

Permissioned Blockchain allows a combination of public and private blockchains with many customizations. These type of blockchains have some set of instructions which include allowing anyone to participate in permissioned network with secured identity verification. The verified candidates have the choice of specific functions like reading, write and access information on the blockchain. Enterprises and Businesses are more interested in implementing permissioned blockchain networks as they can imply necessary restrictions while configuring networks.

## Features of Blockchain:

Below are the most important features of Blockchain technology that has made it a revolutionary technology:

- SHA256 Hash Function
- Public Key Cryptography
- Distributed Ledger & Peer to Peer Network
- Proof of Work
- Incentives for Validation
- Lets try to understand each one of them one by one.

- **SHA256 Hash Function**

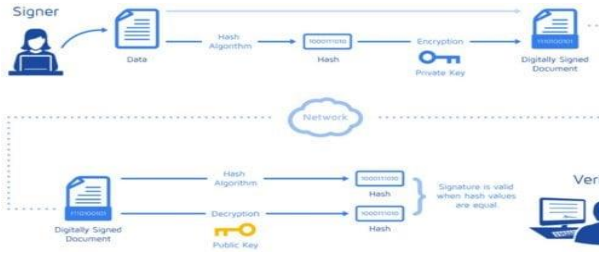
The core hash alogorithm used in blockchain technology is the SHA256. The purpose of using a hash is because the output is not 'encryption' i.e it cannot be decrypted back to the original text. It is a 'one-way' cryptographic function, and is a fixed size for any size of source text. To get a better understanding, let us look at an example below:


- If you look at the first example, we are feeding the input as "Hello World" and getting an output as "a591a6d40bf420404a011733cfb7 b190d62c65bf0bcda32b57b277d9a d9f146e". However, by just adding an "!" at the end, the output completely changes to "7f83b1657ff1fc53b92dc18148a1d 65dfc2d4b1fa3d677284addd20012 6d9069". If we change "H" to "h" and "W" to "w", then the output value changes to "7509e5bda0c762d2bac7f90d758b 5b2263fa01ccbc542ab5e3df163be0 8e6ca9".
- I hope with this example you have understood how complex the algorithm is as even the slightest change in the input can cause a massive change in the output.

**Public Key Cryptography**

This cryptographic technique helps the user by creating a set of keys referred as Public key and Private key. Here the Public key is shared with others whereas the Private key is kept as a secret by the user. To understand the roles of these keys, Let us look at the example below to get a better understanding:

International Journal of Research
Available at https://journals.pen2print.org/index.php/ijr/
e-ISSN: 2348-6848
p-ISSN: 2348-795X
Volume 06 Issue 09
August 2019




If Chandler sends some bitcoins to Joey, that transaction will have three pieces of information:

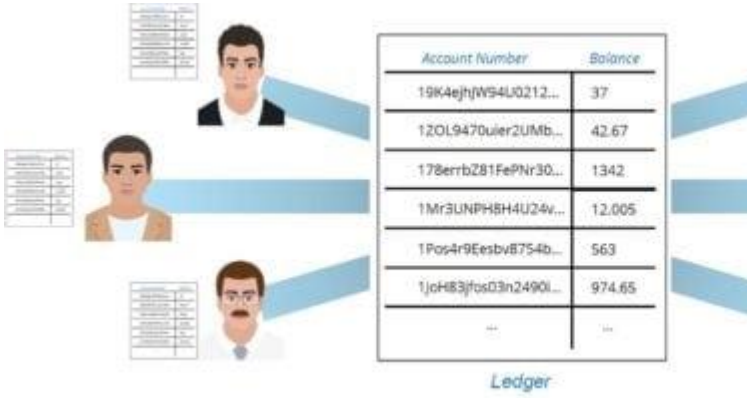
- Joey's bitcoin address.(Joey's Public key)
- The amount of bitcoins that Chandler is sending to Joey.
- Chandler's bitcoin address.(Chandler's Public key)

Now all this data along with an encrypted digital signature is sent through the network for verification. The Digital signature is again a hash value achieved by the combination of the Chandler's bitcoin address and the amount he is sending to joey. This digital signature is encrypted by the private key. Once this data is received by a miner who has to verify this transaction, there are 2 process he does simultaneously:

1. He takes all the un-encrypted data like transaction amount and public keys of both Joey and Chandler, and feeds it to a hash algorithm to get a hash value which we shall call Hash1
2. He takes the digital signature and decrypts it using chandler's public key to get a hash value which we will call as Hash2

If both Hash1 and Hash2 are the same then it means that this a valid transaction.

**Distributed Ledger and P2P Network:**

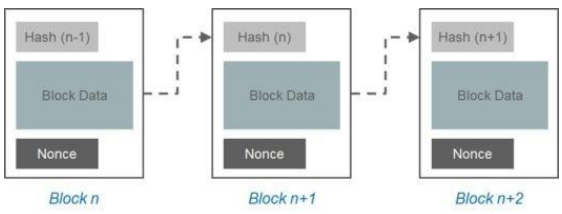



Every single person on the network has a copy of the ledger. There is no single centralized copy. Let me help in you understanding what a ledger is with the following example: Suppose you need to send 10 Bitcoins to your friend John where your Bitcoin balance is 974.65 and John here with a balance of 37. Your balance will be deducted by 10 BTC and credited into John's account.

Blockchain has a unique way to implement this. There are no accounts and balances in the Bitcoin Blockchain ledger. Every transaction from the first one is stored on a continuous growing database called Blockchain. There are blocks averaging around 2050 transactions and as of today, there are 484,000 blocks in the Blockchain with around 250 million transactions.

This ledger is distributed across all users of Bitcoin Blockchain, i.e., the ledger has no central location where it is stored. Everyone on the network owns a copy of the ledger and the true copy is the collection of all the distributed ledgers.

**Proof Of Work:**



e-ISSN: 2348-6848
p-ISSN: 2348-795X
Volume 06 Issue 09
August 2019

You might be wondering if everyone equally owns the ledger, who adds blocks to the Blockchain? How can people trust this person?

For this, we have the concept of proof of work. It is basically like solving a very big puzzle. It requires lots of computational effort. This work is done by people in the Bitcoin network we call miners. The work of these miners is to verify the transactions and solve a complex mathematical puzzle associated with the block being created. The difficulty of the problem is adjusted so that on average a block is solved in 10 minutes. Miners search for a specific nonce(mathematical value) which gives the desired hash which is predetermined. The current difficulty level is such that you need to try about 20.6 quadrillion nonce to get the correct hash.

Each block has a hash value which is the combination of the previous block's final hash, transaction data's hash value and the nonce. The final resulting hash for the block must start with a specified number of trailing zeroes. It is this computation to find the nonce which satisfies the condition that makes mining so computationally expensive.

So the person who finds this nonce is the successful miner and he/she can add their block to the blockchain. Through our P2P distributed network, he/she broadcasts their block and everyone verifies if hashes match, updates their blockchain and moves on to solving the next block immediately.

**Incentives for Validation**

The last step of a Bitcoin transaction is to giving a reward to the miner who has created the latest block. This rewards is provided by the Blockchain system for validating the transactions and maintaining the Blockchain. Currently the reward per block is 12.5 BTC (Rs **3,427,850**/- or **$ 53,390**). This is the most interesting part of Bitcoin Mining.

Bitcoin incentives is the only way to generate new currency into the system and it is believed that by 2140, all 21 million bitcoins will be mined.

With this, I hope you now have more understanding and appreciation towards the Blockchain technology. Blockchain is much more than Bitcoin. Finance is just one of the many industries Blockchain aims to disrupt. Moving ahead with our Blockchain tutorial, let us now look at one such example of IBM and Maersk, to understand how the Supply Chain Industry is disrupted by blockchain.

**Challenges:**

Today, 90% of the goods in global trade are carried by the shipping industry. This supply chain is flowed by the complexity

and sheer volume of point-to-point communication. These communications are across a loosely coupled web of land transportation providers .freight forwarders, customs, brokers, government's ports and ocean carriers processing. Documents and information for a container shipment is estimated to cost more than twice that of the actual physical transportation.

**Solution:**

IBM and Maersk are addressing this problem with a distributed permission platform accessible by the supply chain ecosystem designed to exchange event data and handled document workflows.

Merck and IBM are employing Blockchain technology to create a global tamper proof system by the digitizing trade workflow and tracking shipments end-to-end. This eliminates frictions including costly point-to-point communications. The collaboration will launch with potential ability to track millions of container journeys per year and integrate with customs authorities on selected trade lanes.

**Results:**

- Provided a secure **Data Exchange** platform for all the stakeholders involved in the supply chain system.
- Established a **Tamper proof repository** to store all the documents involved as part of the process.
- Regular shipping events help reduce significant **Delays and Frauds**, saving Billions of dollars annually.
- **Reduced the barrier** between trade organisations thereby increasing worldwide GDP by 3%.
- Helped **increase the overall trade volume** by 12%.

This is how Blockchain technology helped Maersk and has been helping many other companies worldwide. Finally as part of this Blockchain tutorial, we will look at a demo as to how you set up a private autonomous Blockchain on your system.

**Blockchain Alternatives**

The Blockchain is not created for companies to build applications and processes. But many other companies like Ethereum, Hyperledger, R3, IBM and Ripple have created blockchain platforms to support firms interested in the technology build processes.

**Ethereum**

Ethereum is primarily a Blockchain platform that is specialized in handling smart contracts, it has a virtual coin named as ether-linked to it. Ether is the world's second-largest cryptocurrency by value and is similar to the functioning of bitcoin.

**Ripple**

Ripple is a type of Blockchain created specifically for cross-border transactions. The transfer of money by changing currency across the world, mainly for large businesses, is highly expensive and takes more time. This process involves many third party entities from banks to clearing houses. Ripple's blockchain system is named as xCurrent, helps to remove

intermediaries, reducing time by seconds for cross-currency transactions.

**Applications of Blockchain:**

The stream of blocks on the Blockchain store information about monetary transactions. But the Blockchain is very reliable as it stores other types of transactions, as well. Indeed the Blockchain technology is used to store information like stops in supply chain, property exchanges, and even candidate votes.

Deloitte, a professional services network recently surveyed 1,000 companies across different countries regarding the integration of Blockchain into their business operations. The survey results tell that 34% of total companies already had Blockchain systems in production today, while others are likely to deploy a Blockchain application in the next 12 months.

**The following are few of the most popular Blockchain applications being explored today:**

**Cryptocurrency**

Blockchain is the most essential technology for cryptocurrencies like bitcoin. The foreign currencies like the US dollar are verified and regulated under the control of central authority. With the control of central authority system, the value of the individuals currency may be at risk if the bank in which he has invested loses the currency value.

To overcome this problem the bitcoin came into existence and has widespread. By spreading the bitcoin operations across a wide network of computers, Blockchain enables all the cryptocurrencies to work without the need of central authority. This eliminates the transaction, processing fees and reduces the risks involved.

**Banks**

Apart from banking sector no other industry benefits from integrating Blockchain into their business. If a person transfers money or issues a check, it takes 3 days to reflect the bank account, Blockchain, on the other hand, never sleeps. By deploying Blockchain into banks, individuals can see transactions processed in a very little amount of time. With the help of Blockchain, banks also have the opportunity to exchange funds among the institutions more securely and quickly.

**Healthcare**

Healthcare management can leverage Blockchain to safely place their patients' medical records. As soon as the medical record is produced and signed, the information can be stored in the Blockchain, this gives patients the confidence and proof that the records cannot be manipulated. These health records can be secured by encoding and storing them on the blockchain with a private key, so that they can only be accessed by management or certain individuals to ensure privacy.

**Supply Chains**

The use of Blockchain in supply chain helps suppliers to record the origins of materials that they have bought. With this the companies will have the right to verify the authenticity of their products, along with genuine labels like "**Local**", "**Fair Trade**" and "**Organic**".

**Smart Contracts**

A smart contract is a computer code that is built into Blockchain to facilitate, negotiate or verify a contract agreement. It helps you to exchange money, shares,

property or anything of value without any disputes while avoiding the services of middlemen. Smart contracts run with a set of rules that users agree to. When those rules are obeyed , the terms of the agreement are accomplished. This saves the middleman fees that are accompanied with a third-party mediator or notary.

**Voting**

Use of Blockchain in voting eliminates the election fraud and increases the number of people who show up to vote, this procedure was tested in the midterm decentralized elections held in West Virginia. Every vote would be stored as a block, making the act of tampering impossible. With Blockchain the need of personnel to conduct elections is reduced and maintains transparency in the electoral procedure giving way for instant results.

**Advantages of Blockchain**

- Real-time transactions are effective and take very little time.
- All the processes become transparent with proper tracking and creation of records.
- Increased security with decentralized, cryptographic protocols.
- Security risks reduced such as frauds, cybercrimes, and tampering.
- Direct transactions remove the overheads and eliminate the middleman costs.

**Conclusion:**

In this short tutorial you were introduced to several concepts of Blockchain by taking Bitcoin as a case study. The Bitcoin is the first successful implementation of blockchain. Today, the world has found applications of blockchain technology in several industries, where the trust without the involvement of a centralized authority is desired. So welcome to the world of Blockchain.

**References:**

[1] Clarke, A.C., "Hazards of Prophecy: The Failure of Imagination," from Profiles of the Future: An Inquiry into the Limits of the Possible, 1962.

[2] Lamport, Leslie. "The Part-Time Parliament." ACM Transactions on Computer Systems, vol. 16, no. 2, Jan. 1998, pp. 133–169., https://dl.acm.org/citation.cfm?doid=279227.279229.

[3] Narayanan, A., Bonneau, J., Felten, E., Miller, A., and Goldfede, S., Bitcoin and Cryptocurrency Technologies: A Comprehensive Introduction, Princeton University Press, 2016.

[4] Nakamoto, S., "Bitcoin: A Peer-to-Peer Electronic Cash System," 2008. https://bitcoin.org/bitcoin.pdf

[5] National Institute of Standards and Technology, Secure Hash Standard (SHS), Federal Information Processing Standards (FIPS) Publication 180-4, August 2015. https://doi.org/10.6028/NIST.FIPS.180-4

[6] National Institute of Standards and Technology (NIST), Secure Hashing website, https://csrc.nist.gov/projects/hash-functions

[7] "Hash per Second." Bitcoin Wiki, http://en.bitcoin.it/wiki/Hash_per_second.

[8] National Institute of Standards and Technology, SHA-3 Standard: PermutationBased Hash and Extendable-Output Functions, Federal Information Processing Standards (FIPS) Publication 202, August 2015. https://doi.org/10.6028/NIST.FIPS.202

[9] National Institute of Standards and Technology (NIST), Digital Signature Standard, Federal Information Processing

e-ISSN: 2348-6848
p-ISSN: 2348-795X
Volume 06 Issue 09
August 2019

Standards (FIPS) Publication 186-4, July 2013. https://doi.org/10.6028/NIST.FIPS.186-4 [10] "LDAP.com." LDAP.com, https://www.ldap.com.

[11] "How Is the Address of an Ethereum Contract Computed?" Ethereum Stack Exchange, 29 Jan. 2016, 22:14, https://ethereum.stackexchange.com/questions/760/how-is-the-address-of-anethereum-contract-computed.