Blockchain Technology

Brief History of Blockchain Technology

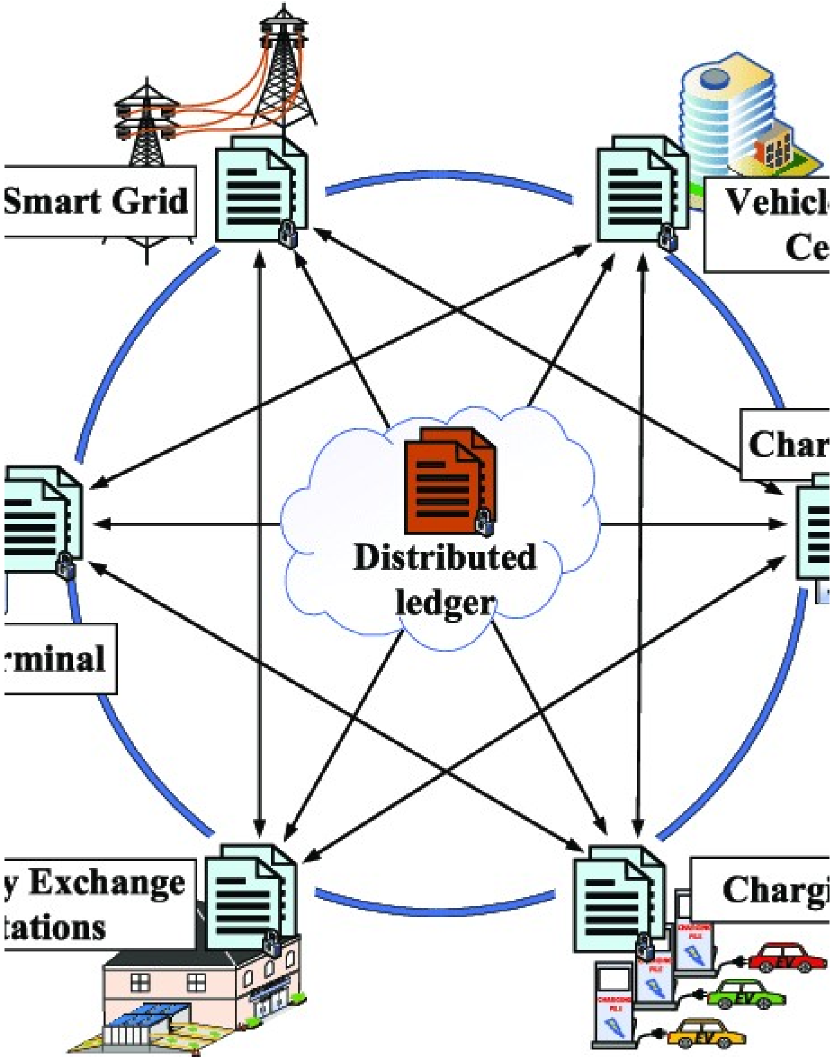
❑ Blockchain started in 1982, when David Chaum proposed the first-ever blockchain-like protocol in his dissertation, Computer Systems Established, Maintained, and Trusted .

❑ This concept was further worked on by Stuart Haber and W Scott Starletta in 1991, where they described the process of a cryptographically secured chain of blocks with timestamps that could not be tampered with .

❑ However, Blockchain was first popularized by Satoshi Nakamoto in 2008 in a paper titled, “Bitcoin: A Peer-to-Peer Electronic Cash System” . The author(s) laid out the framework for blockchain and detailed methods of using a peer-to-peer network to generate a financial database.

❑ Since then, various programmers, cryptographers, and scientists have worked on this concept of blockchain to produce a cryptocurrency network called the bitcoin. The major design goal and the purpose of the blockchain were to solve two major problems. The first is to solve the double spending problem and second was to eliminate the need of central trusted third party.

What Is a Blockchain?



- ❖ A blockchain is a distributed database that is shared among the nodes of a computer network.
- ❖ Blockchains are best known for their crucial role in cryptocurrency systems, such as Bitcoin, for maintaining a secure and decentralized record of transactions.
- ❖ The innovation with a blockchain is that it guarantees the fidelity and security of a record of data and generates trust without the need for a trusted third party.
- ❖ A blockchain collects information together in groups, known as blocks,
- ❖ Blocks have certain storage capacities and, when filled, are closed and linked to the previously filled block, forming a chain of data known as the blockchain

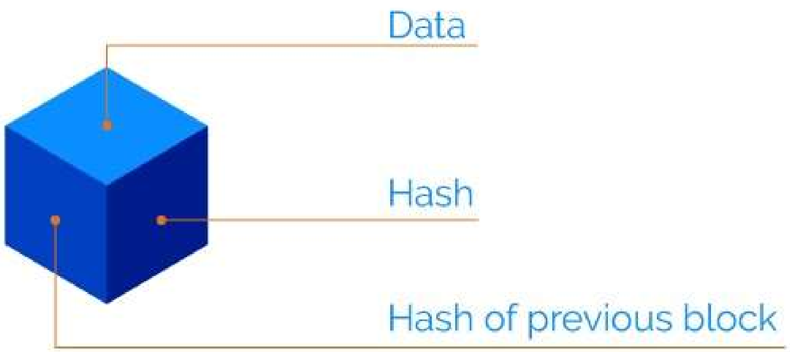
The Block Structure

A block is the building block or the key element of blockchain. A unit of data stored inside a block may be represented by any value depending on the type of blockchain.

For the Bitcoin blockchain. The blocks store number of transactions. For example, blocks are consisted of an average of more than 500 Bitcoin transactions.

A block also stores encrypted details about the parties participating in the network, whose interaction resulted in the data stored in the block.

Each block in blockchain consists of:



The Block Structure(con.)

- Data: Details of all the transactions and the contents that need to take place.
- Hash of the Block: The block details (including the previous hash) are transmitted through a hashing algorithm. This gives a fixed length output which is called the unique hash address. A hash can be compared to a fingerprint, as each hash is unique. Its role is to identify a block and the contents of the block

Hash
000dc75a315c77a1f9c98fb6247d03dd18ac52632d7dc6a9920261d8109b37cf

Figure (5): The hash of the block.

The Block Structure(con.)

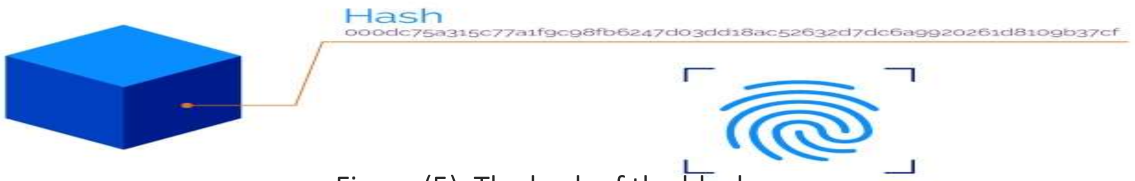
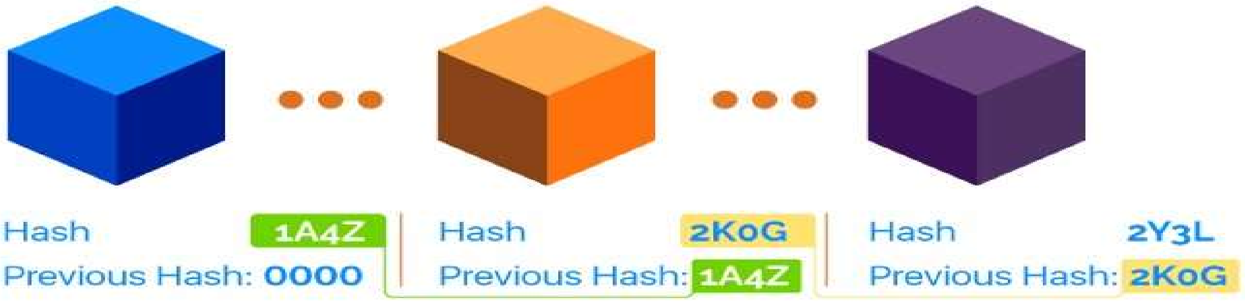

Hash
000dc75a315c77a1f9c98fb6247d03dd18ac52632d7dc6a9920261d8109b37cf

Figure (5): The hash of the block.

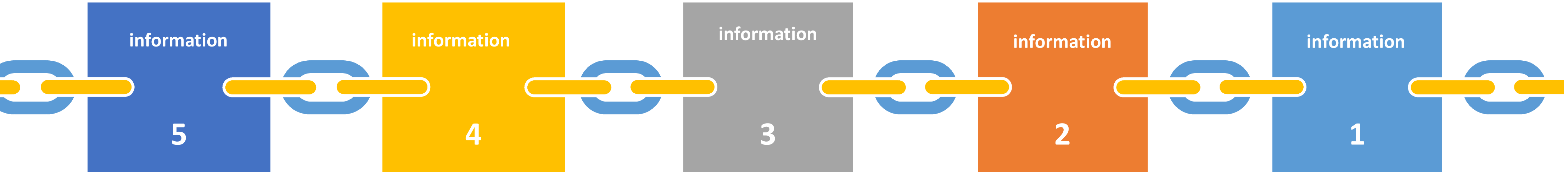
- Previous Hash: The information contained in a block is dependent on and linked to the information in a previous block. Each block contains a hash of the previous block unless it is a genesis block. A genesis block is the first block in the blockchain that is hardcoded at the time the blockchain was first started

For instance, if there are three blocks in a blockchain, block 3 will contain the hash of block 2, and block 2 will contain the hash of block 1. And, over time, forms a chain of blocks. Hence the word blockchain.



The Block Structure(con.)

The hash is dependent on the contents of a block. The slightest change of the contents can drastically change the hash. Because of this dependency property and the fact that the blockchain is distributed, it makes it difficult to hack. This is because if someone were to change the contents of a block for their own favor, it would change the hash and the block in front of it wouldn’t match the same hash. This way, the blockchain can easily recognize changes



The Block Structure(con.)

The hash is dependent on the contents of a block. The slightest change of the contents can drastically change the hash. Because of this dependency property and the fact that the blockchain is distributed, it makes it difficult to hack. This is because if someone were to change the contents of a block for their own favor, it would change the hash and the block in front of it wouldn’t match the same hash. This way, the blockchain can easily recognize changes

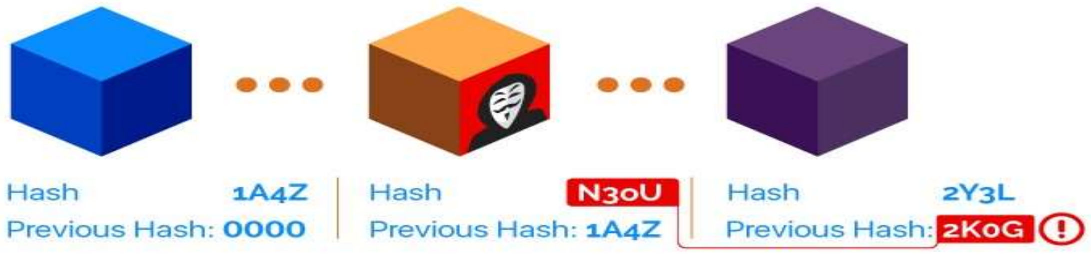


Figure (7): Hash dependency

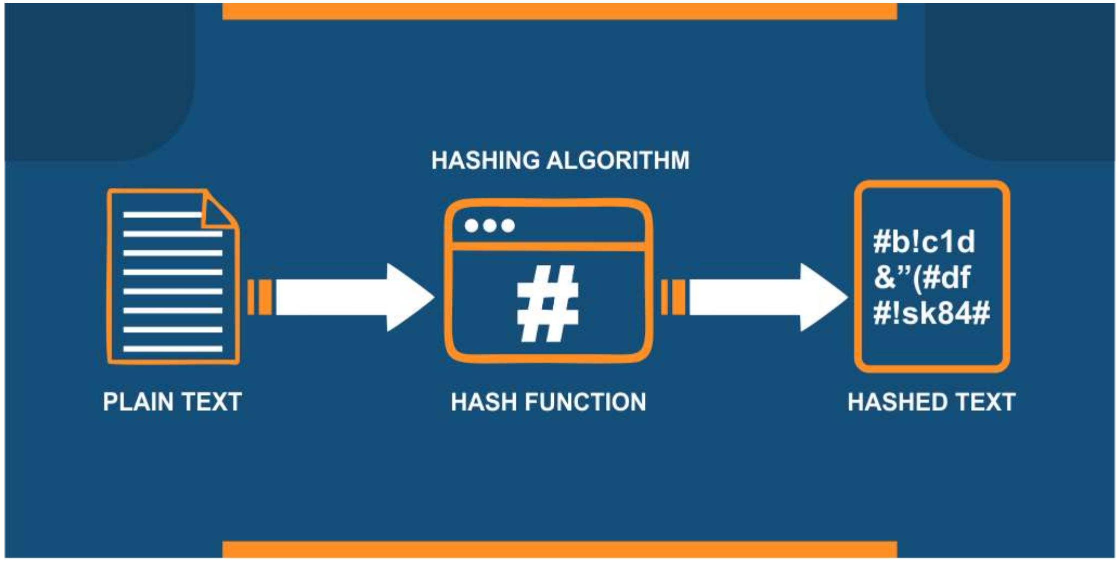
How Blockchain Works?

You should be familiar with :

- Structure of the block
- Cryptographic hash function
- Consensus methods

Cryptographic hashing

Hashing: means taking an input of any length and turn it into a fixed length Structure of the block



Cryptographic hashing

Hash function properties:

- Deterministic
- Quick computation
- Small change in input changes the output

  M =
  01a60e35df88d8b49546cb3f8f4ba4f406870f9b8e1f394c9d48ab73548d748d

  M1 =
  1ae95de4f8f21162fc63203853d9e1d1ce92e755d564164f72cb7c4fff14ec9f
- Collision resistant

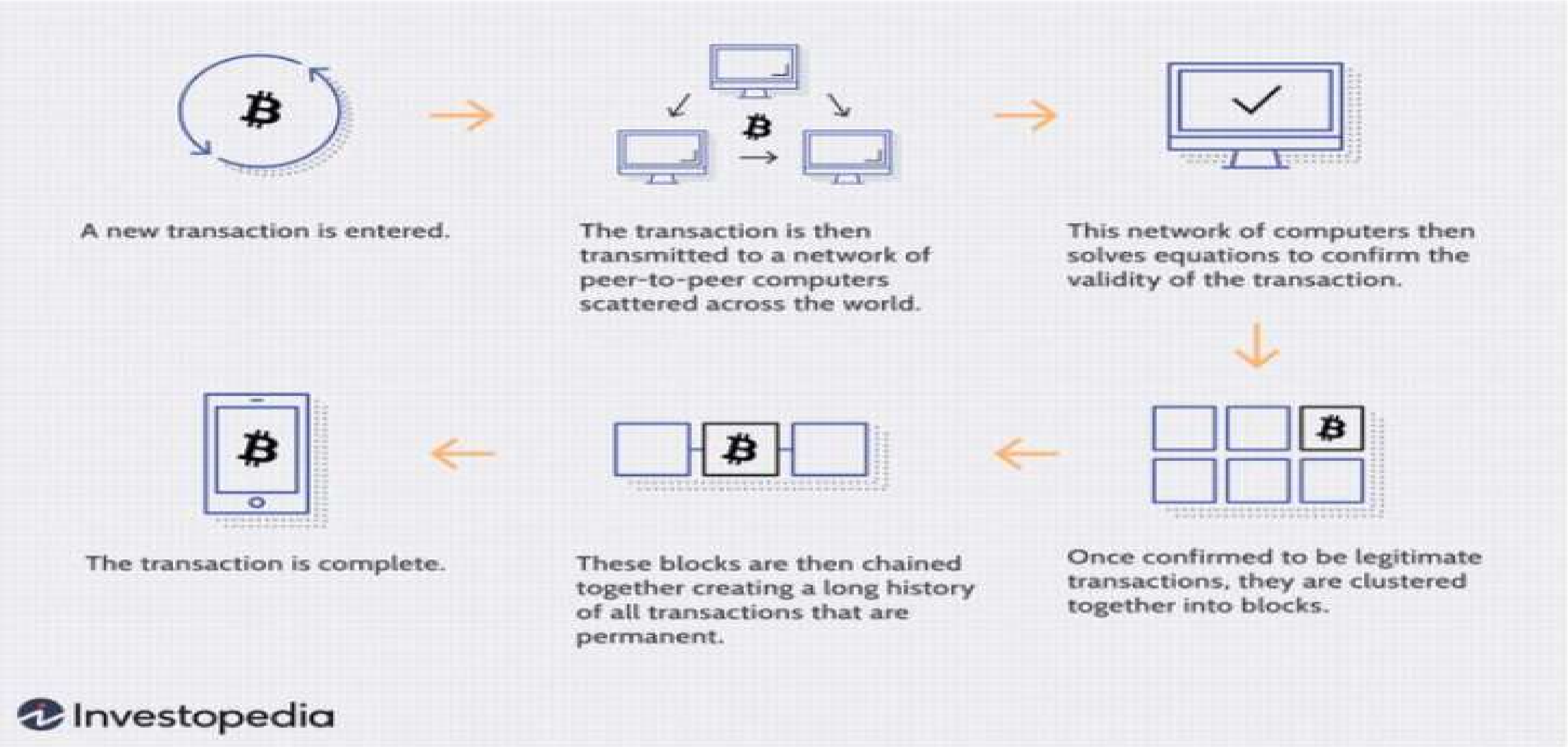
Consensus Mechanism

A consensus Mechanism is a procedure through which all the peers of the Blockchain network reach a common agreement about the present state of the blockchain.

Common consensus algorithms:

- Proof of work (POW)
- Proof of stake (POS)

Transaction Process



A new transaction is entered.

The transaction is then transmitted to a network of peer-to-peer computers scattered across the world.

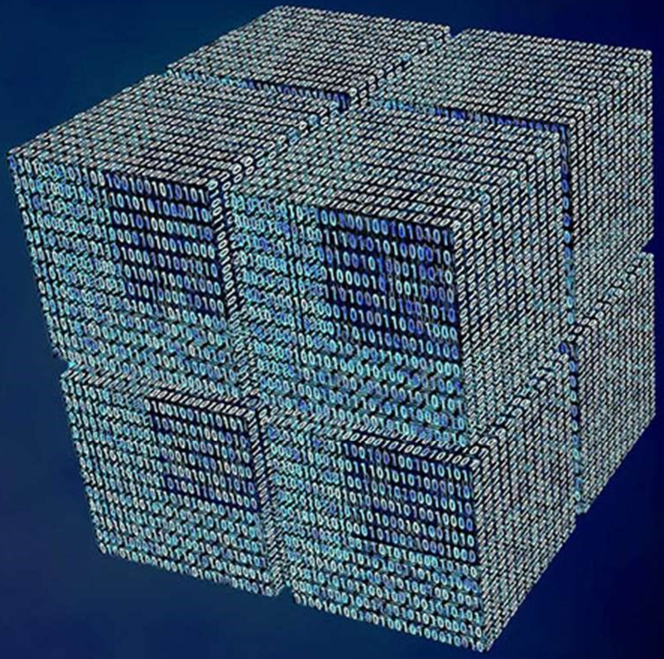
This network of computers then solves equations to confirm the validity of the transaction.

Once confirmed to be legitimate transactions, they are clustered together into blocks.

These blocks are then chained together creating a long history of all transactions that are permanent.

The transaction is complete.

Blockchain Basic Principles



01

peer-to-peer

The blockchain is peer to peer, which means that there is no central controller in the network

02

Distributed

The blockchain is distributed, which simply means that a ledger is spread across the network among all peers in the network

03

Cryptographically-secure

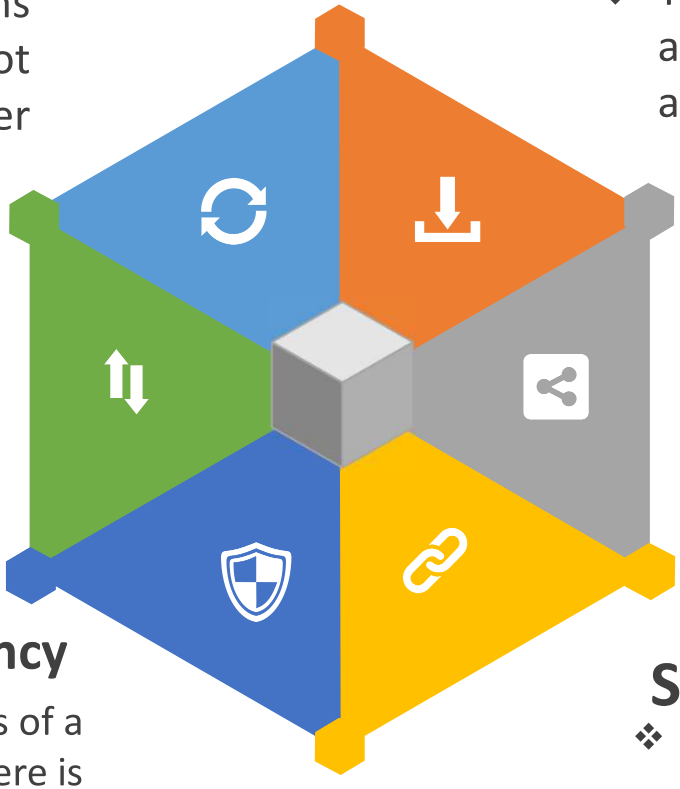
The blockchain is cryptographically-secure, by using hash algorithms to encrypt blocks which make the ledger secure against tampering and misuse.

04

Updateable via consensus

The most critical attribute of a blockchain is that it is updateable only via consensus. This is what gives it the power of decentralization

Advantages of Blockchain



Trust

- The blockchain is immutable and automates trusted transactions between counterparties who do not need to know each other

Decentralized

- No single entity maintains the network. Unlike centralized systems, decisions on the blockchain are made via consensus.

Transparency

- One of the main benefits of a blockchain is the fact that there is a clear record of any transaction or information within a system

Immutability

- You can simply impress your audience and add a unique zing and appeal to your Reports.

Fraud Reduction

- Blockchain could minimize fraud by establishing full transaction histories within a single source of truth

Security

- Due to the cryptographic nature of blockchain networks, it uses a digital signature feature to conduct fraud-free transactions which makes it more secure

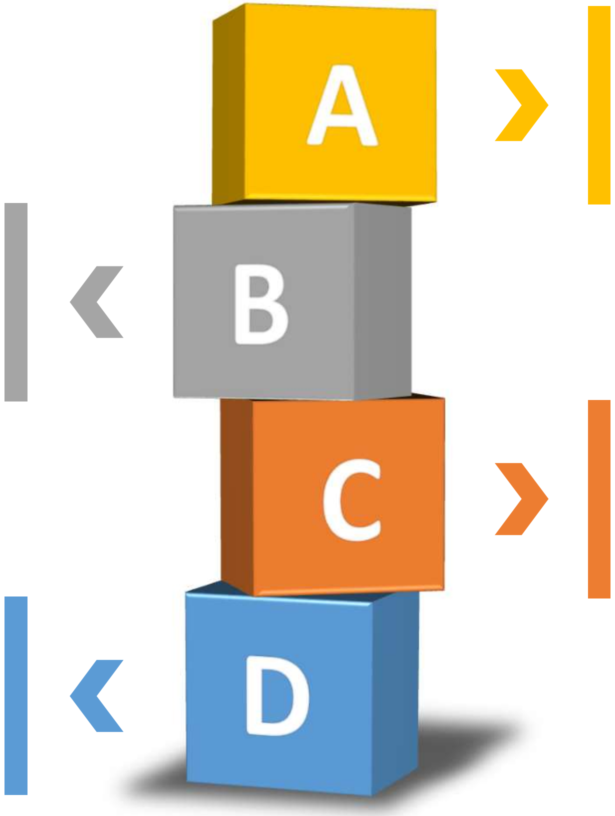
Smart Contracts

> “One of the most attractive features associated with blockchain technology is Smart contracts.”

- Smart contracts, are simply programs stored on a blockchain that run when predetermined conditions are met.

- They typically are used to automate the execution of an agreement so that all participants can be immediately certain of the outcome, without any involvement of third parties or time loss. They can also automate a workflow, triggering the next action when conditions are met

Benefits of Smart Contracts



❖ Accuracy, Speed, and Efficiency.

❖ There is no paperwork to deal with

❖ The information is protected from being tampered with for personal gain because there is no third party engaged.

❖ Eliminate the need for intermediaries to conduct transactions, as well as the time delays and fees that come with them

Types of Blockchain

There are types of blockchains, depending on the scope of its use. They are as follows:

Public Blockchain Networks

❖ As the name suggests, public blockchains are not owned by anyone. They are open to the public, and anyone can participate as a node in the decision-making process. Users may or may not be rewarded for their participation

Private Blockchain Networks

❖ Private blockchains operate on closed networks and have access restrictions, they tend to work well for private businesses and organizations [7]. Companies can use private blockchains to customize their accessibility and authorization preferences, and other important security options. Only one authority manages a private blockchain network.