# CHAPTER 1

# INTRODUCTION

The Blockchain technology will promise us the bright future. It can help to make the business, government and logistic systems more reliable, trusty and safety. This technology has very strong benefits, because it can help to achieve the goals in different systems. Certainly, the Blockchain technology has some disadvantages, mostly they relate to the costs and the implementation process of the technology. The successful implementation of the technology is depending on many different factors, such as government and legislative support. Certainly, the Blockchain is the new type of a database. This technology is very interesting for people, because it can solve one of the big problems, which is connected with finance. This problem is a double spending without middleman. How does the Blockchain technology work and solve this problem? The Blockchain creates the blocks with different information. Each of these blocks relates to others blocks in this blockchain. The proof-of-work is used for the Blockchain’s secure and safety. When the new block is connected to the Blockchain, it is almost impossible to change or delete these blocks. For the hacking of the Blockchain it is necessary to have very huge processing power. The miners are the people, who calculate the hash value for the new blocks. The Blockchain technology always relates to the cryptocurrency, because this technology is the basis of cryptocurrency’s work, but these are different things.



Fig.1.1: Blockchain

The Blockchain technology also is used in another areas, such as the logistics systems or medicine institutions and others. The application of this technology improves the quality of the system’s working process. The main advantages of the Blockchain technology are decentralized network, transparency, trusty chain, unalterable and indestructible technology. In turn, the main disadvantages of the Blockchain are the high energy dependence, the difficult process of integration and the implementation’s high costs.

# CHAPTER 2 BLOCKCHAIN

2.1 What is Blockchain?

A blockchain is a constantly growing ledger which keeps a permanent record of all the transactions that have taken place in a secure, chronological, and immutable way.

Let's breakdown the definition,

* **Ledger:** It is a file that is constantly growing.
* **Permanent:** It means once the transaction goes inside a blockchain, you can put up it permanently in the ledger.
* **Secure:** Blockchain placed information in a secure way. It uses very advanced cryptography to make sure that the information is locked inside the blockchain.
* **Chronological:** Chronological means every transaction happens after the previous one.
* **Immutable:** It means as you build all the transaction onto the blockchain, this ledger can never be changed.

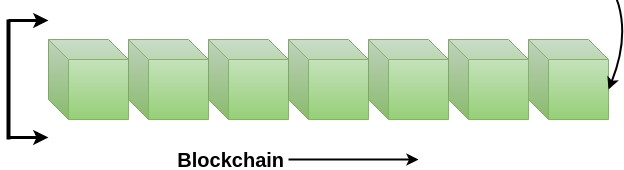


Fig 2.1: Structure of Blockchain

A blockchain is a chain of blocks which contain information. Each block records all of the recent transactions, and once completed goes into the blockchain as a permanent database. Each time a block gets completed, a new block is generated. In simple words, Blockchain can be defined as a chain of the block that contains information. The technique is intended to timestamp digital documents so that it's not possible to backdate them or temper them. The blockchain is used for the secure transfer of items like money, property, contracts, etc. without requiring a third-party intermediary like bank or government. Once a data is recorded inside a blockchain, it is very difficult to change it.

The blockchain is a software protocol (like SMTP is for email). However, Blockchains could not be run without the Internet. It is also called meta-technology as it affects other technologies. It is comprised of several pieces: a database, software application, some connected computers, etc.

* Blockchain is not Bitcoin, but it is the technology behind Bitcoin
* Bitcoin is the digital token and blockchain is the ledger to keep track of who owns the digital tokens
* You can't have Bitcoin without blockchain, but you can have blockchain without Bitcoin.

“Blockchain is a decentralized, distributed public ledger system”

Blockchain is based on P2P i.e. peer to peer network. A distributed ledger is a type of database that is consensually shared, replicated, and synchronized among the members of a decentralized network. All the information on this ledger is securely and accurately stored using cryptography. This information can be accessed by using keys and cryptographic signatures. The distributed ledger allows transactions to have public witnesses, which makes cyberattack more difficult. It records the transactions such as the exchange of assets or data, among the participants in the network.

All the participants in the network govern and agreed-upon consensus on the updates to the records in the ledger. There is no central authority, or third-party mediators such as a financial institution or government agencies are involved. Every record in the distributed ledger has a timestamp and unique cryptographic signature. It makes the ledger an auditable, and immutable history of all transactions in the network. Further, if any alterations made to the ledger, they are reflected and copied to all participants in seconds or minutes. In other words, when any modifications or updates happen in the ledger, each node constructs the new transaction, and then the nodes vote by consensus algorithm on which copy is correct. Once a consensus algorithm has been determined, all the other nodes update themselves with the new and correct copy of the ledger.

The primary advantage of the distributed ledger is the lack of central authority. As we know that centralized ledgers are prone to cyber-attack, distributed ledgers are inherently very hard to attack. It is because all the distributed copies need to be attacked simultaneously for an attack to be successful.

2.2 Versions-

2.2.1 Blockchain 1.0: Currency

The idea of creating money through solving computational puzzles was first introduced in 2005 by Hal Finney, who created the first concept for cryptocurrencies (The implementation of distributed ledger technology). This ledger allows financial transactions based on blockchain technology or DLT to be executed with [Bitcoin.](https://www.javatpoint.com/bitcoin) Bitcoin is the most prominent example in this segment. It is being used as cash for the Internet and seen as the enabler of an Internet of Money.

2.2.2 Blockchain 2.0: Smart Contracts

The main issues that came with Bitcoin are wasteful mining and lack of network scalability. To overcome these issues, this version extends the concept of Bitcoin beyond currency. The new key concepts are Smart Contracts. It is small computer programs that "live" in the [blockchain.](https://www.javatpoint.com/blockchain-tutorial) They are free computer programs which executed automatically and checked conditions which are defined earlier like facilitation, verification or enforcement. The big advantage of this technology that blockchain offers, making it impossible to tamper or hack Smart Contracts. A most prominent example is the Ethereum Blockchain, which provides a platform where the developer community can build distributed applications for the Blockchain network. Quickly, the blockchain 2.0 version is successfully processing a high number of daily transactions on a public network, where millions were raised through ICO (Initial Coin Offerings), and the market cap increased rapidly.

2.2.3 Blockchain 3.0: DApps

DApps is also known as a decentralized application. It uses decentralized storage and communication. Its backend code is running on a decentralized peer-to-peer network. A DApp can have frontend code hosted on decentralized storages such as Ethereum Swarm and user interfaces written in any language that can make a call to its backend like a traditional App.

2.3 Blockchain vs Database-

|  |  |  |
| --- | --- | --- |
| **SN** | **Blockchain** | **Database** |
| 1. | It is decentralized because there is no admin or in-charge. | It is centralized because it has admins and in-charge. |
| 2. | It is permissionless because anyone can access it. | It required permission bcoz it can be accessed only by entities who have rights |
| 3. | Blockchains are slow. | Databases are fast. |
| 4. | It has a history of records and ownership of digital records. | It has no history of records and ownership of records. |
| 5. | Blockchain is fully confidential. | The database is not fully confidential. |
| 6. | Blockchain has only Insert operation. | It has Create, Read, Update, Delete option. |
| 7. | It is a fully robust technology. | It is not entirely robust technology. |
| 8. | Disintermediation is allowed with It. | Disintermediation is not allowed with It. |
| 9. | Anyone with the right proof of work can write on the blockchain. | Only entities entitled to read or write can do so. |
| 10. | Blockchain is not recursive. Here, we cannot go back to repeat a task on any record. | The database is recursive. Here, we can go back to repeat a task on a particular record. |

# CHAPTER 3 HISTORY

* The blockchain technology was described in 1991 by the research scientist *Stuart Haber and W. Scott Stornetta.* They wanted to introduce a computationally practical solution for time-stamping digital documents so that they could not be backdated or tampered. They develop a system using the concept of cryptographically secured chain of blocks to store the time-stamped documents.

* In 1992, Merkle Trees were incorporated into the design, which makes [blockchain](https://www.javatpoint.com/blockchain-tutorial) more efficient by allowing several documents to be collected into one block. Merkle Trees are used to create a 'secured chain of blocks.' It stored a series of data records, and each data records connected to the one before it. The newest record in this chain contains the history of the entire chain. However, this technology went unused, and the patent lapsed in 2004.

* In 2004, computer scientist and cryptographic activist *Hal Finney* introduced a system called Reusable Proof of Work (RPoW) as a prototype for digital cash. It was a significant early step in the history of cryptocurrencies. The RPoW system worked by receiving a non-exchangeable or a non-fungible Hashcash based proof of work token in return, created an RSA-signed token that further could be transferred from person to person. RPoW solved the double-spending problem by keeping the ownership of tokens registered on a trusted server. This server was designed to allow users throughout the world to verify its correctness and integrity in real-time.

* Further, in 2008, *Satoshi Nakamoto* conceptualized the theory of distributed blockchains. He improves the design in a unique way to add blocks to the initial chain without requiring them to be signed by trusted parties. The modified trees would contain a secure history of data exchanges. It utilizes a peer-to-peer network for timestamping and verifying each exchange. It could be managed autonomously without requiring a central authority. These improvements were so beneficial that makes blockchains as the backbone of cryptocurrencies. Today, the design serves as the public ledger for all transactions in the [cryptocurrency](https://www.javatpoint.com/blockchain-cryptocurrency) space.

# CHAPTER 4

# BITCOIN : FIRST BLOCKCHAIN

# IMPLEMENTATION

4.1 What is Bitcoin?

It is Blockchain based digital currency. Satoshi Nakamoto introduced the bitcoin in the year 2008. Bitcoin is a cryptocurrency (virtual currency), or a digital currency that uses rules of cryptography for regulation and generation of units of currency. A Bitcoin fell under the scope of [cryptocurrency](https://www.javatpoint.com/blockchain-cryptocurrency) and became the first and most valuable among them. It is commonly called decentralized digital currency.



Fig 4.1: Bitcoin

4.2 Transaction-

How mining works and transactions are processed in seven steps in Bitcoin application of blockchain:

* **Step 1**: A user signs off on a transaction from their wallet application, attempting to send a certain crypto or token from them to someone else.
* **Step 2**: The transaction is broadcasted by the wallet application and is now waiting to be picked up by a miner on the according blockchain. As long as it is not picked up, it hovers in a ‘pool of unconfirmed transactions’. This pool is a collection of unconfirmed transactions on the network that are waiting to be processed. These unconfirmed transactions are usually not collected in one giant pool, but more often in small subdivided local pools.
* **Step 3**: Miners on the network (sometimes referred to as [nodes,](https://medium.com/coinmonks/blockchain-what-is-a-node-or-masternode-and-what-does-it-do-4d9a4200938f) but not [quite the same!](https://medium.com/@JimiS/blockchain-what-is-a-node-or-masternode-and-what-does-it-do-4d9a4200938f)) select transactions from these pools and form them into a ‘block’. A block is basically a collection of transactions (at this moment in time, still unconfirmed transactions), in addition to some extra metadata. Every miner constructs their own *block of transactions.* Multiple miners can select the same transaction to be included in their block.

Example: two miners, miner A and miner B. Both miner A and miner B can decide to include transaction X into their block. Each blockchain has its own maximum block size. On the Bitcoin blockchain, the maximum block size is 1 MB of data. Before adding a transaction to their block, a miner needs to check if the transaction is eligible to be executed according to the blockchain history. If the sender’s wallet balance has sufficient funds according to the existing blockchain history, the transaction is considered valid and can be added to the block. Miners will usually prioritise transactions that have a high transaction fee set, because this provides them a higher reward.

* **Step 4**: By selecting transactions and adding them to their block, miners create a block of transactions. To add this block of transactions to the blockchain (to have all other miners and nodes register the transactions), the block first needs a signature (also referred to as a proof of work). This signature is created by solving a very complex mathematical problem that is unique to each block of transactions. Each block has a different mathematical problem, so every miner will work on a different problem unique to the block they built. All of these problems are equally hard to solve. In order to solve this mathematical problem, a lot of computational power is used (and thus a lot of electricity). You could compare it to running a calculation on a calculator, only much heavier and on a desktop. This is the process referred to as mining.
* **Step 5**: The miner that finds an eligible signature for its block first, broadcasts this block and its signature to all the other miners.
* **Step 6**: Other miners now verify the signature’s legitimacy by taking the string of data of the broadcasted block, and hashing it to see if the output hash indeed matches the included signature. If it is valid, the other miners will confirm its validity and agree that the block can be added to the blockchain (they reach *consensus*, aka they all agree with each other, hence the term consensus algorithm). This is also where the definition ‘proof of work’ comes from. The signature is the ‘proof’ of the work performed (the computational power that was spent). The block can now be added to the blockchain, and is spread across all other nodes on the network. The other nodes will accept the block and save it to their transaction data as long as the transactions inside the block correspond correctly with the current wallet balances (transaction history) at that point in time.

4.3 Blockchain Double Spending-

Double spending means spending the same money twice. As we know, any

transaction can be processed only in two ways. One is offline, and another is online. In a physical currency, the double-spending problem can never arise. But in digital cash-like bitcoin, the double-spending problem can arise. Hence, bitcoin transactions have a possibility of being copied and rebroadcasted. It opens up the possibility that the same BTC could be spent twice by its owner.

How Bitcoin handles the Double Spending Problem?

Bitcoin handles the double-spending problem by implementing a confirmation mechanism and maintaining a universal ledger called blockchain.

Let us suppose you have 1 BTC and try to spend it twice. You made the 1 BTC transaction to Alice. Again, you sign and send the same 1 BTC transaction to Bob. Both transactions go into the pool of unconfirmed transactions where many unconfirmed transactions are stored already. The unconfirmed transactions are transactions which do not pick by anyone. Now, whichever transaction first got confirmations and was verified by miners, will be valid. Another transaction which could not get enough confirmations will be pulled out from the network. In this example, transaction T1 is valid, and Alice will receive the bitcoin.

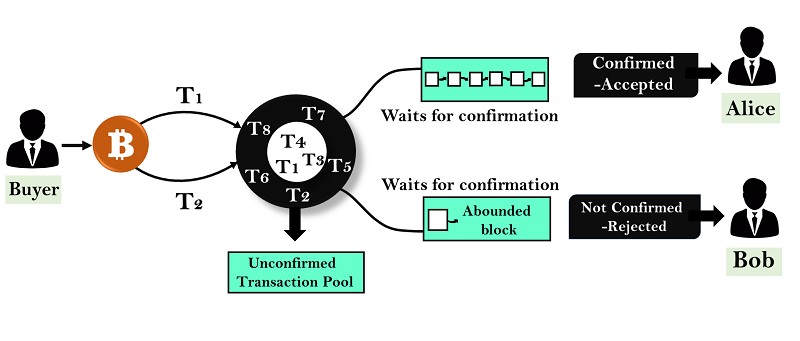


Fig 4.3 double spending

What happened if both the transactions are taken simultaneously by the miners?

Suppose two different miners will pick both transactions at the same time and start creating a block. Now, when the block is confirmed, both Alice and Bob will wait for confirmation on their transaction. Whichever transaction first got confirmations will be validated first, and another transaction will be pulled out from the network.

Now suppose if both Alice and Bob received the first confirmation at the same time, then there is a race will be started between Alice and Bob. So, whichever transaction gets the maximum number of confirmations from the network will be included in the blockchain, and the other one will be discarded.

# CHAPTER 5

# LOGICAL ARCHITECTURE

The architectural components of Blockchain have been generalized and then modified by various companies, leading to different blockchain projects like Bitcoin, [Ethereum,](https://www.edureka.co/blog/what-is-ethereum/) [Hyperledger](https://www.edureka.co/blog/what-is-hyperledger/) etc. To keep things simpler, Let us discuss the bitcoin blockchain architecture.

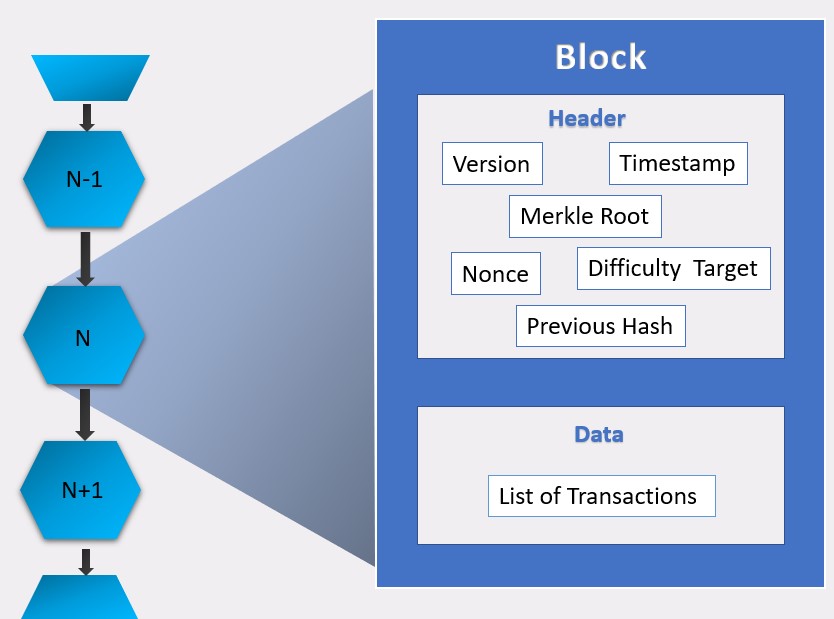


Fig 5.1: Architecture

5.1 P2P-

The blockchain is a peer to peer (P2P) network working on the IP protocol. A P2P network is a flat topology with no centralized node. All nodes equally provide and can consume services while collaborating via a consensus algorithm. Peers contribute to the computing power and storage that is required for the upkeep of the network. P2P networks are generally more secure because they do not have a single point of attack or failure as in case of a centralized network.

A blockchain network can be a permission-based network as well as a permissionless network. A *permissionless* network is also known as public blockchain because anyone can join the network, while a permission-based blockchain is called a consortium blockchain. A *permission-based* blockchain or private blockchain requires pre-verification of the participants within the network and these parties are usually known to each other. In a typical blockchain architecture, every individual node in a network maintains a local copy of blockchain. The decentralisation of blockchain architecture is the sole credit of the P2P network that it is built on.

5.2 Block–

Block contains the information as a block header and transactions. Blocks are data structures whose purpose is to bundles sets of transactions and are replicated to all nodes in the network. Blocks in blockchain are created by miners. Mining is the process to create a valid block that will be accepted by the rest of the network. Nodes take pending transactions, verify that they are cryptographically accurate, and package them into blocks to be stored on the blockchain. Block header is the metadata that helps in verifying the validity of a block.

The rest of a block contains transactions. It can be any number of transactions bundled in a block depending on the choice of a miner.

Types of Blocks :

1. Most blocks simply extend the current main blockchain which is also the longest chain in the network. These blocks are called *“main branch blocks”.*
2. Some blocks reference a parent block that is not at the longest blockchain. These blocks are called *“side branch blocks”.*
3. Some blocks reference a parent block that is not known to the node processing the block. These are called *“orphan blocks”.*

Side branch blocks might not currently a part of the main branch, but if more blocks are mined that reference them as a parent, there is the possibility that a particular side branch will be restructured into the main branch. This brings in the concept of forking.

# CHAPTER 6

# FEATURES OF BLOCKCHAIN

6.1 Asymmetric Cryptography-

Cryptography is a method of using advanced mathematical principles in storing and transmitting data in a particular form so that only those for whom it is intended can read and process it. Encryption is a key concept in cryptography — It is a process whereby a message is encoded in a format that cannot be read or understood by an eavesdropper. Two types are,

6.1.1 Symmetric cryptography:

Symmetric cryptography is which uses a single key to encrypt and decrypt data.

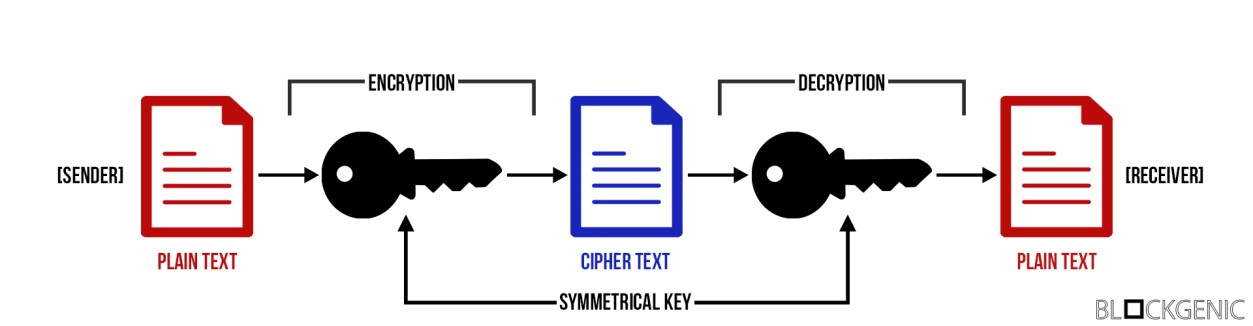


Fig 6.1: symmetric cryptography

6.1.2 Asymmetric cryptography:

Asymmetric cryptography is similar to symmetric cryptography, but is a bit more complex and also has a solution to the main downside of symmetric cryptography. The main distinction from symmetric cryptography is the usage of keypairs. Asymmetric cryptography uses keypairs, instead of a shared key, in order to encrypt and decrypt data. Keypairs consist of 2 parts, a public key and a private key.

A public key can be seen as a username, it is available to everyone, can be shared with everyone, and everyone can view the history of the account with that username. The username is tied to a password (private key), but there is absolutely no way to derive the password (private key) from a username. It is also not possible to authorize any action on the account with just the username. A private key can be seen as a password to an account with a certain username. It is not publicly available and should not be shared with anyone. The private key is used to authorize actions on the accounts. Unlike with ‘normal accounts’, to access the account, or to authorize any action on the account, only the private key is needed.

First of all, the sender encrypts the message with the public key of the receiver, the sender can then send the (encrypted) message safely, as the only way to view the message is to decrypt it with the corresponding private key which only the receiver has. The receiver then receives the message and is able to decrypt it using the private key.

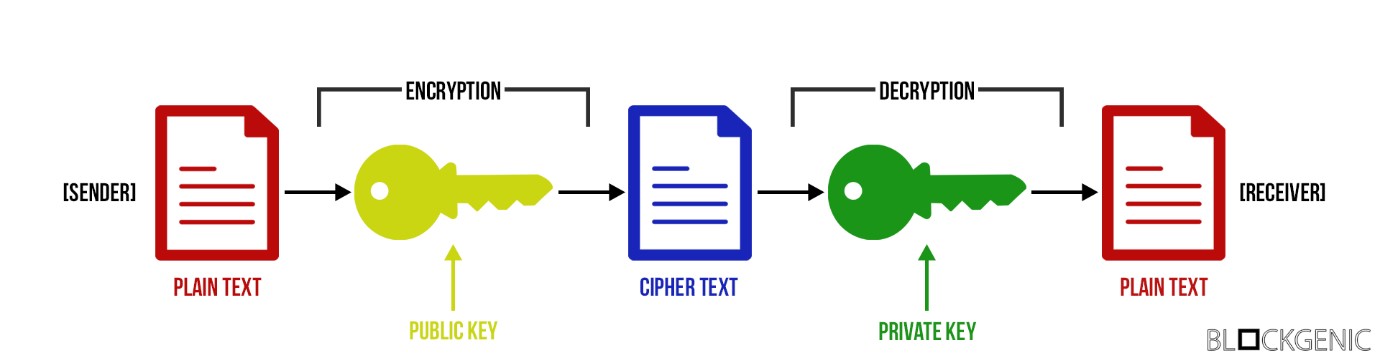


Fig 6.1.2

Due to the usage of keypairs asymmetric cryptography is a (much) safer way to encrypt data and make sure only those who are supposed to receive it are able to receive it. These keypairs also allow themselves to be used for authentication purposes.

## 6.2 Digital Signature-

Digital signatures are one of the main aspects of ensuring the security and integrity of the data that is recorded onto a blockchain. They are a standard part a blockchain protocols, mainly used for securing transactions and blocks of transactions, transferral of information, contract management and any other cases where detecting and preventing any external tampering is important. Digital signatures utilize asymmetric cryptography, meaning that information can be shared with anyone, through the use of a public key. In many parts of the world, digital signatures are as legally binding as a regular signature.

Digital signatures provide three key advantages of storing and transferring information on a blockchain. First of all, they guarantee integrity. Theoretically, data that is being sent can be altered without necessarily even being seen by a hacker. However, if this does happen in the case of data that is accompanied by a digital signature, the signature would become invalid. Therefore, digitally signed data, that is encrypted, is not only safe from being seen but will also reveal if it has been tampered with, cementing its incorruptibility. Digital signatures not only secure data but also the identity of the individual sending it. Ownership of a digital signature is always bound to a certain user and as such, one can be sure that they are communicating with whom they intend to.

For example, even the most proficient hacker could not fake another’s digital signature as a means of convincing someone else to send money, it is simply mathematically not within the realms of possibility. Therefore, digital signatures not only guarantee the data that is being communicated, but also the identity of the individual communicating it.

When using blockchain technology a user has a public key and a private key, both of which appear as strings of random numbers and letters. The public key can be compared to an email address and private key to password. It is very important to never share a private key with anyone. It is equally important to have the private key written down and stored in a safe and secure place. Ideally on a piece of paper or a hardware wallet, as these two are near impossible to hack. Storing private keys in text documents or notes is not advised as these can be hacked relatively easily. There is no “I Forgot My Private Key” option. If a private key is lost, everything that is controlled by the key is lost too.

Finally, the fact that private keys are linked to individual users gives digital signatures a quality of non-repudiation. This means that if something is digitally signed by a user, it can be legally binding and entirely associated with that individual. As indicated earlier, this is heavily dependent on there being no doubt that the private key that signed the data was not compromised, used or seen by anyone other than its owner.

Digital signatures are unique to the signer and are created by utilising three algorithms:

* A key generation algorithm, providing a private and public key.
* A signing algorithm that combines data and private key to make a signature.
* An algorithm that verifies signatures and determines whether the message is authentic or not based on the message, the public key and signature.

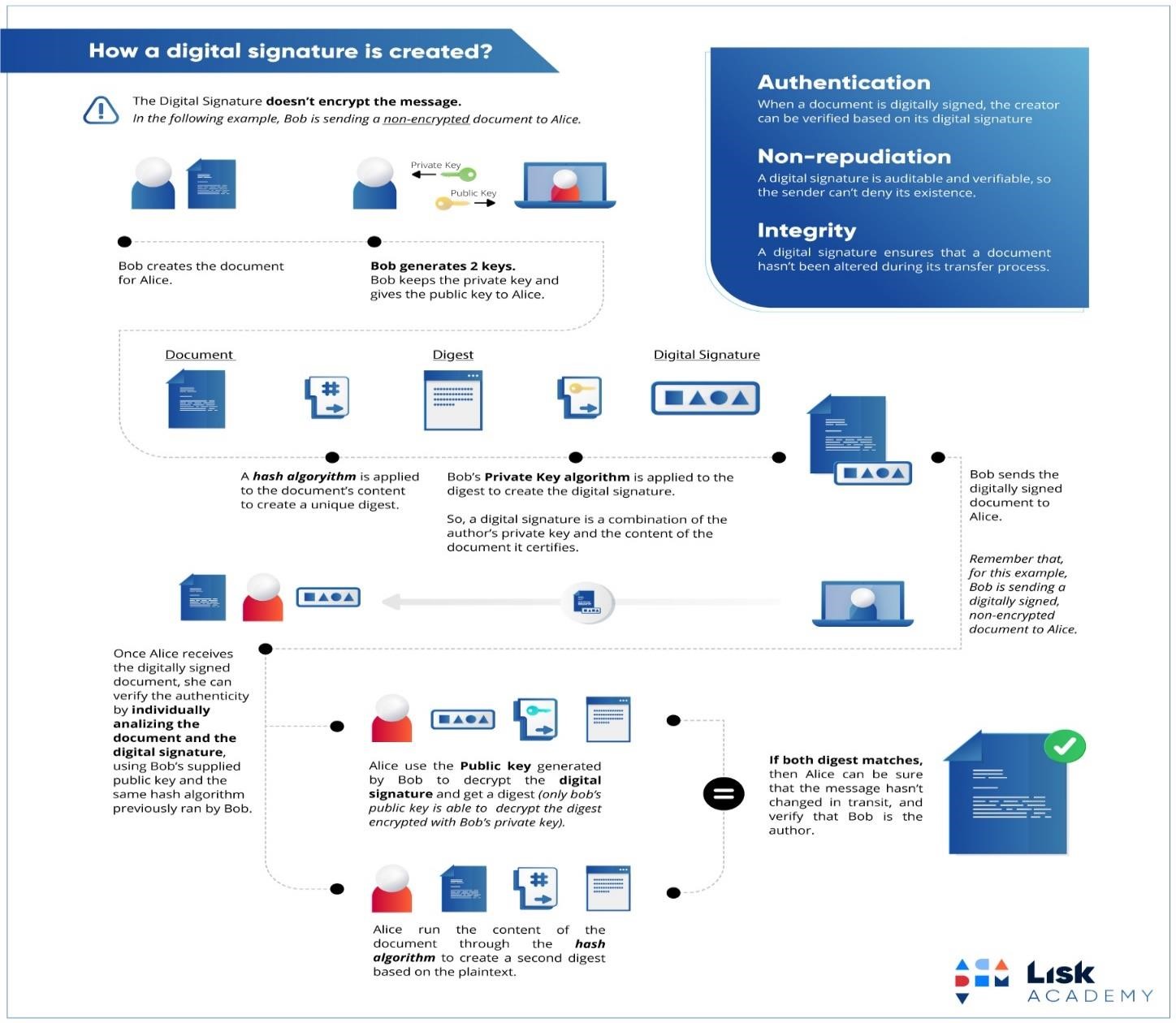


Fig 6.2.1: digital signature

**The key features of these algorithms are:**

* Making it absolutely impossible to work out the private key based on the public key or data that it has encrypted.
* Ensuring the authenticity of a signature based on the message and the private key, verified through the public key.

## 6.3 Hashing –



Fig 6.3.1: hash function

A hash function takes an input string (numbers, alphabets, media files) of any length and transforms it into a fixed length. The fixed bit length can vary (like 32-bit or 64-bit or 128-bit or 256-bit) depending on the hash function which is being used. The fixed-length output is called a hash. This hash is also the cryptographic by-product of a hash algorithm. We can understand it from the following diagram.

The hash algorithm has certain unique properties:

1. It produces a unique output (or hash).
2. It is a one-way function.

In the context of cryptocurrencies like [*Bitcoin,*](https://www.javatpoint.com/bitcoin) *the blockchain uses cryptographic hash function's properties in its consensus mechanism.* A cryptographic hash is a digest or digital fingerprints of a certain amount of data. In cryptographic hash functions, the transactions are taken as an input and run through a hashing algorithm which gives an output of a fixed size.

*A Bitcoin's blockchain uses SHA-256 (Secure Hash Algorithm) hashing algorithm.* In 2001, SHA-256 Hashing algorithm was developed by the National Security Agency (NSA) in the USA.

If we write the same text again in a data section, it will always give the same output. It is because you are creating a message digest of that one's specific amount of data. Since the Hash function is a one-way function, there is no way to get back entire text from the generated hash. This is different from traditional cryptographic functions like encryption where you can encrypt something using the key and by using decryption, you can decrypt the message to its original form.

6.3.1 Blockchain Block Hashing:

In this section, we are going to learn how SHA-256 applies to build a block within a blockchain. We will see here in the context of the Bitcoin blockchain and understand how this tie into the role of miners. The miners are actually in the process of building blocks, and these blocks are added to a blockchain to build out what the Bitcoin blockchain will be. Block is composed of a block number, data field, cryptographic hash associated with it and a Nonce.



In the above image, the generated hash would look like 00001acbm010gfh1010xxx. I'd like to point out that this hash has four leading zeros. The four leading zeros describes whether the block is valid or not. For practical purposes, you will see that this hash is corresponding to the nonce, and the block number is corresponding to the available data. Since the hash has four leading zeroes, therefore, it is a valid block. If we make any change in the data section, it will give the completely different hash that can be shown in the below image.

If the newly generating hash does not have four leading zeroes, then it will not a valid block.

To make the block valid, we will do it by using the field called nonce. Nonce stands for a Number Used Once in a cryptographic communication such that the block's hash meets a certain criterion. This criterion could be generated a hash that must have its leading four digits to be zero. Thus, the generated hash would look like *00001acbm010gfh1010xxx*.

A nonce is basically a random number which figures out how you can actually make this specific block provide you with a valid hash. The way you can do this is by changing the nonce manually. Generally, the miner starts with a Nonce value of 1 and keeps on incrementing it until the generated hash meets the specified criterion. Thus, it may take several iterations until the desired hash with four leading zeros is generated. The expected time for generating a block in the [bitcoin](https://www.javatpoint.com/bitcoin) system is 10 minutes. Once the miner successfully mines the block, he releases that block in the system and making it the last block in the chain.

6.4 Merkle Tree and Merkle Root-

Merkle tree is a fundamental part of blockchain technology. It is a mathematical data structure composed of hashes of different blocks of data, and which serves as a summary of all the transactions in a block. It also allows for efficient and secure verification of content in a large body of data. It also helps to verify the consistency and content of the data. Both Bitcoin and Ethereum use Merkle Trees structure. Merkle Tree is also known as Hash Tree.

The concept of Merkle Tree is named after Ralph Merkle, who patented the idea in 1979. Fundamentally, it is a data structure tree in which every leaf node labelled with the hash of a data block, and the non-leaf node labelled with the cryptographic hash of the labels of its child nodes. The leaf nodes are the lowest node in the tree.

How do Merkle trees work?

A Merkle tree stores all the transactions in a block by producing a digital fingerprint of the entire set of transactions. It allows the user to verify whether a transaction can be included in a block or not. Merkle trees are created by repeatedly calculating hashing pairs of nodes until there is only one hash left. This hash is called the Merkle Root, or the Root Hash. The Merkle Trees are constructed in a bottom-up approach. Every leaf node is a hash of transactional data, and the non-leaf node is a hash of its previous hashes. Merkle trees are in a binary tree, so it requires an even number of leaf nodes. If there is an odd number of transactions, the last hash will be duplicated once to create an even number of leaf nodes.

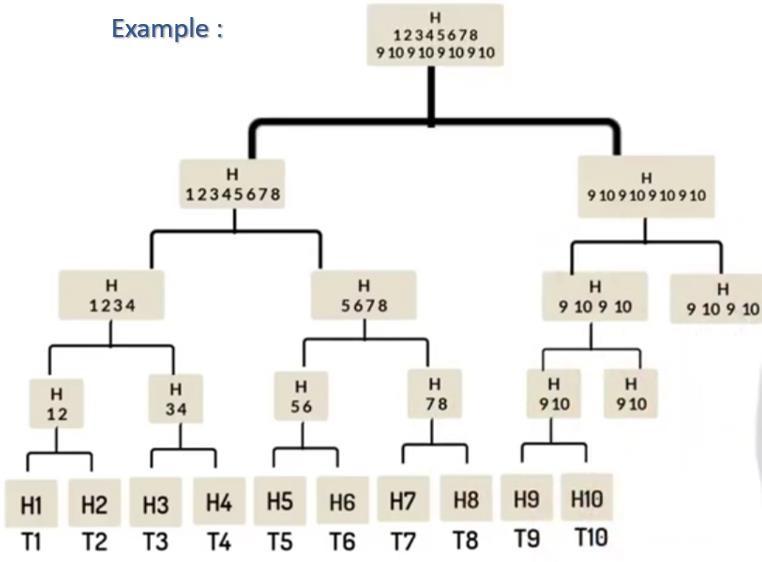


Fig 6.4.1: Merkle tree

Merkle Root is stored in the block header. The block header is the part of the bitcoin block which gets hash in the process of mining. It contains the hash of the previous block, a Nonce, and the Root Hash of all the transactions in the current block in a Merkle Tree. So, having the Merkle root in block header makes the transaction tamper-proof. As this Root Hash includes the hashes of all the transactions within the block, these transactions may result in saving the disk space.

The Merkle Tree maintains the integrity of the data. If any single detail of transactions or order of the transaction's changes, then these changes reflected in the hash of that transaction. This change would cascade up the Merkle Tree to the Merkle Root, changing the value of the Merkle root and thus invalidating the block. So, everyone can see that Merkle tree allows for a quick and simple test of whether a specific transaction is included in the set or not.

Merkle trees have three benefits:

* It provides a means to maintain the integrity and validity of data. o It helps in saving the memory or disk space as the proofs, computationally easy and fast.
* Their proofs and management require tiny amounts of information to be transmitted across networks

6.5 Consensus in Blockchain-

The way all these copies of a single ledger is synchronized is due to a consensus algorithm. The consensus mechanism ensures that whatever local copy every individual party has, they are consistent with each other and is the most updated one. The copy that every individual node has are identical or similar to each other. It could be arguably stated that the consensus algorithm forms the core of every blockchain architecture. Some of the consensus algorithms are discussed below:

6.5.1 Proof-of-Work (POW):



6.5.1:

PoW

Proof of Work (PoW) is the *original consensus algorithm* in a blockchain network. The algorithm is used to confirm the transaction and creates a new block to the chain. In this algorithm, miners (a group of people) compete against each other to complete the transaction on the network. The process of competing against each other is called mining. As soon as a miner successfully created a valid block, he gets rewarded. The most famous application of Proof of Work (PoW) is Bitcoin. Producing proof of work can be a random process with low probability. In this, a lot of *trial and error* is required before a valid proof of work is generated. The main working principle of proof of work is a mathematical puzzle which can easily prove the solution. Proof of work can be implemented in a [blockchain](https://www.javatpoint.com/blockchain-tutorial) by the Hashcash proof of work system. It basically involves guessing the string that produces a 256-bit hash, produced by the popular hashing algorithm SHA256. The fact that hashing algorithms are irreversible stands as the fundamental pillar of such an approach to consensus achievement. Since someone has to go through a million guesses to verify the hash, the process gets its name ‘proof-of-work’.

6.5.1.1 Coinbase Transaction:

A coinbase transaction is the first transaction in a block. It is a unique type of bitcoin transaction that can be created by a miner. The miners use it to collect the block reward for their work and any other transaction fees collected by the miner are also sent in this transaction. Each transaction executed on the [bitcoin](https://www.javatpoint.com/bitcoin) network is combined together to form a block. When a block is formed, immediately, it will be added in the blockchain. Now, these blocks are immutable and tamper-proof for all transactions that are made on the bitcoin network. Each block must contain one or more transactions, and the first transaction in the block is called the coinbase transaction. There is one important feature of a coinbase transaction is that bitcoins involved in the transaction cannot be spent until they have received at least 100 block confirmations in the blockchain.

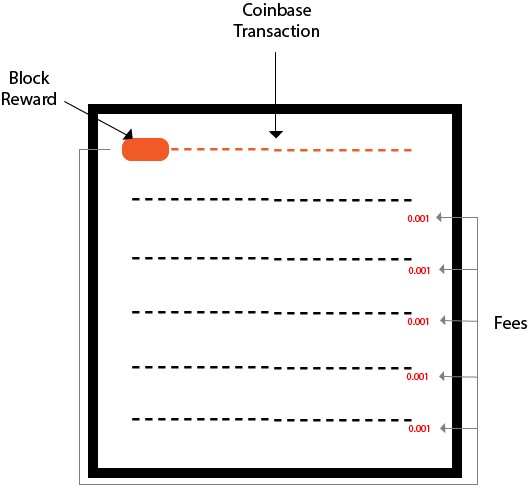


Fig 6.5.1.1 coinbase transaction

6.5.1.2 Mining (Gaming Theory)-

Miners are users who involved in a gaming theory because bitcoin is truly a game which is run by these miners around the world. In the above, we have seen that the first component is **software for bitcoin** that issues a cryptography challenge in every 10 minutes. The cryptography challenge involves in trying to find a Nonce which will make the hash for a specific block valid. All the hashes and validations are done by these miners. After successful creation of the block, the new block is added to the blockchain.

**Let's see how gaming theory works!**

* Bitcoin software creates a challenge. Now, there is a game begins, and there is a race that goes off. The race involves all these miners competing against each other to solve the challenges.
* This task or challenge will take approximately 10 minutes to be completed.
* Every single miner starts trying to find the solution to that one Nonce that will satisfy the hash for the block. o At some specific point, one of those miners in the global community with higher speed and great hardware specs will solve the cryptography challenge and be the winner of that race. o Now, the rest of the community will start verifying that block which is mined by the winner. This makes Bitcoin so strong, because in one stage of this cycle, the miners are competing against each other, and in the next stage of the cycle, the rest of the community rallies together to ensure that that solution is correct. o If the Nonce is correct, it will end up with the new block which will be added to the blockchain.
* For this task or challenge, the winner will earn a reward. That reward is currently 12.5 bitcoins.

**CHAPTER 7**

# TYPES OF BLOCKCHAIN

7.1 Public Blockchain-



Fig 7.1: public blockchain

As the name suggests, Public Blockchain is publicly accessible and has no restriction on who can participate or be a Validator. In Public Blockchains, no one has complete control over the network. This ensures data security and helps immutability because a single person cannot manipulate the Blockchain. The authority on the Blockchain is equally divided among each node in the network, and due to this, Public Blockchains are known to be fully distributed. Public Blockchains are mainly used for cryptocurrencies like Bitcoin, Ethereum, and Litecoin.

7.2 Private Blockchain-



Fig 7.2: private blockchain

A Private Blockchain (also known as Permissioned Blockchain) has restrictions on who can access it and participate in transaction and validation. Only pre-chosen entities have permissions to access the Blockchain. These entities are chosen by the respective authority and are given permission by the Blockchain developers while building the Blockchain application. Suppose there is a need to give permissions to new users or revoke permissions from an existing user, the Network Administrator can take care of it.

Private Blockchains are mainly used in private organizations to store sensitive information that should be available only to certain people in the organization. Because Private Blockchain is a **Closed** Blockchain, the data is within the organization and out of reach from any external entities.

7.3 Consortium Blockchain:



Fig 7.3: consortium blockchain

In Consortium Blockchain, some nodes control the consensus process, and some other nodes may be allowed to participate in the transactions. Consortium Blockchain is like a hybrid of Public and Private Blockchain. It is public because the Blockchain is being shared by different nodes, and it is private because the nodes that can access the Blockchain is restricted. Hence, it is partly public and partly private. There are two types of users here: First, the users who have control over the Blockchain and decide who should have permission to access the Blockchain and second, the users who can access the Blockchain.

This type of Blockchain can be used when organizations are ready to share the Blockchain, but restrict data access to themselves, and keep it secure from public access.

**CHAPTER 8**

# ETHEREUM AND HYPERLEDGER

8.1 Ethereum-



Fig 8.1: Ethereum

Ethereum is an open-source & public blockchain based distributed computing platform for building decentralized applications. So, Before the creation of Ethereum, blockchain applications were designed to do a very limited set of operations. Bitcoin and other cryptocurrencies, for example, were developed exclusively to operate as peer-to-peer digital currencies.

[***Vitalik Buterin***](https://www.youtube.com/watch?v=TDGq4aeevgY&t=1s) envisioned Ethereum as a platform for developers to write programs on the blockchain. To accomplish his goal, he used similar Blockchain designs & protocols as that of Bitcoin’s and improvised it to support applications beyond currency issuance. Anyone across the globe can connect with Ethereum blockchain to develop a program and can maintain the current state of the network, hence the term ***“World Computer”.***

8.1.1 Smart Contracts:

A contract that self-executes, and handles the enforcement, the management, performance, & payment.

Simply put, it can be defined as a contract that self-executes, and handles the enforcement, the management, performance, & payment. You would require tokens for executing a smart contract as well as for trading. So basically, *Ethereum is incomplete without cryptocurrency.*

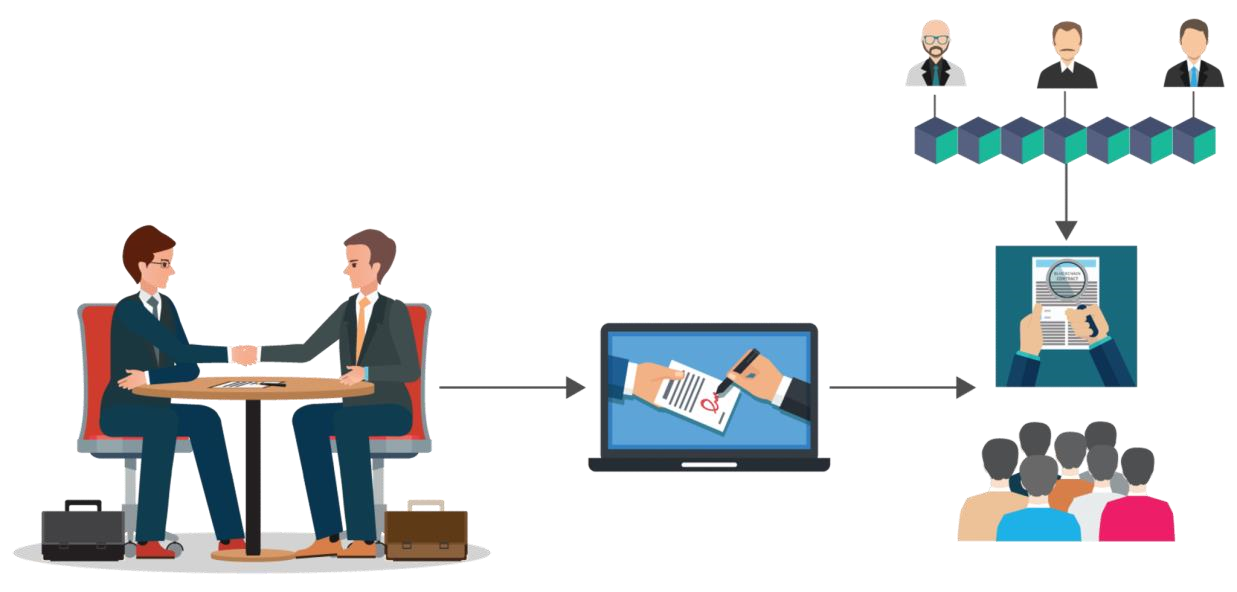


Fig 8.1.1: smart contract

8.1.2 Ethereum Cryptocurrency:

Ethereum runs on its native token which serves two main purposes:

1. Ether payment is required for applications to perform any operation so that broken and malicious programs are kept under control
2. Ether is rewarded as an incentive to the miners who contribute to the Ethereum network with their resources- much like bitcoin’s structure.

Every time a contract is executed, Ethereum consumes token which is termed as ‘gas’ to run the computations.

8.1.3 Gas in Ethereum:

[Gas](https://kb.myetherwallet.com/gas/what-is-gas-ethereum.html) is required to be paid for every operation performed on the Ethereum blockchain. Its price is expressed in ether and it’s decided by the miners, which can refuse to process the transaction with less than a certain gas price.

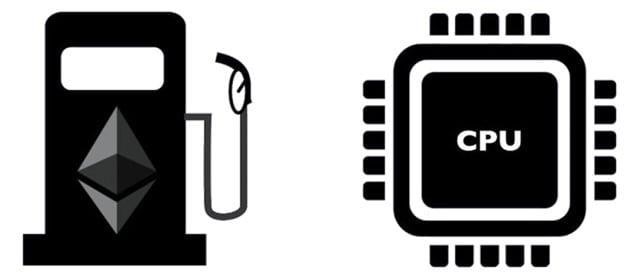


Fig 8.1.3: Ether buys gas to fuel up the E.V.M.

8.1.4 Decentralized Autonomous Organization (DAO):

A DAO is an organization which is represented by rules encoded as a computer program that is transparent, controlled by shareholders, and not influenced by the central government. A DAO is the most complex form of a **smart contract**. A smart contract is a computer program that autonomously exists on the internet, but at the same time, it needs people to perform a task that it can't do by itself.

* DAO are organizations that exist entirely on a blockchain and are governed by its protocols

It is designed to hold onto assets and use a kind of voting system to manage their distribution

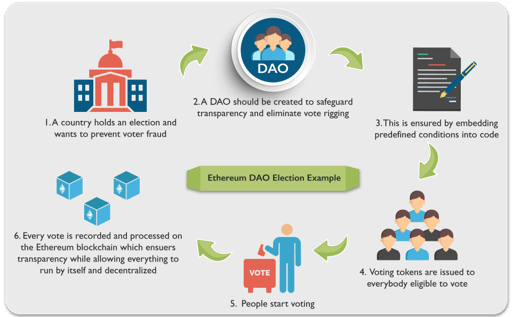


Fig 8.1.4: DAO

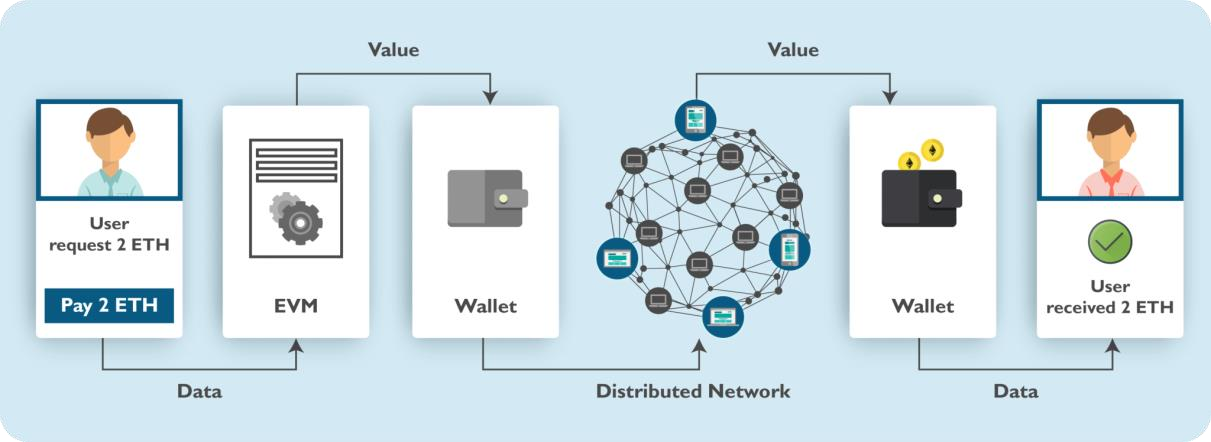
* + 1. Ethereum Virtual Machine (EVM) : 

Fig 8.1.5: EVM

The Ethereum virtual machine is the engine in which transaction code gets executed. E.V.M. enables the development of potentially thousands of different applications all on one platform .Contracts written in a smart contract-specific programming language are compiled into ‘bytecode’, which an EVM can read and execute .

It actually handles the internal state and computation in Ethereum. Practically, EVM can be thought of as a large decentralized computer with millions of objects called “accounts” which have the ability to maintain an internal database, execute code and also, they can talk to each other. With EVM at its heart, Ethereum enables the development of potentially thousands of unstoppable applications. Wondering what can be built on Ethereum? Well, Ethereum can be used to build some really cool applications called DApps.

8.1.6 Decentralized Applications (DApps):

* DApps are computer applications that operate over a blockchain enabling direct interaction between end users and providers
* It can be comprised of single DAO or even a series of DAO that work together to create an application

A user may need to exchange Ether as a way to settle a contract with another user, using the network’s distributed computer nodes as a way to facilitate the distribution of this data.

8.1.7 What is Being Built on Ethereum?

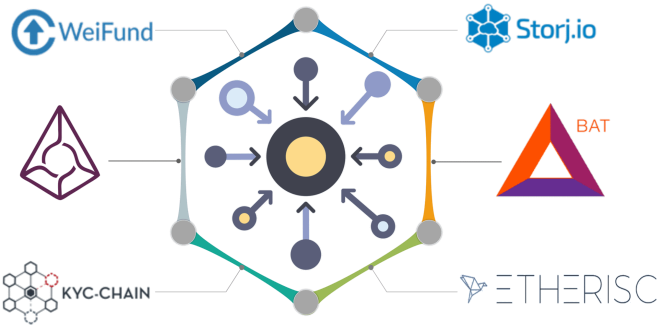


Fig 8.1.7 Dapps built on Ethereum

8.1.8 Bitcoin vs Ethereum-

Both Bitcoin and [Ethereum](https://www.edureka.co/blog/ethereum-tutorial-with-smart-contracts/) are often compared to each other, but, the two were designed with different vision and goals. Bitcoin is an established cryptocurrency used for trading, Ethereum is a multipurpose platform with its digital currency as the fuel for [*smart contracts*](https://www.edureka.co/blog/smart-contracts/) functionality.

|  |  |  |
| --- | --- | --- |
| **Merits** | **Bitcoin** | **Ethereum** |
| Concept | Digital Money | World Computer |
| Founder | Satoshi Nakamoto (Mysterious) | Vitalik Buterin & Team |
| Scripting Language | Turing Incomplete | Turing Complete |
| Release Date | Jan 2009 | July 2015 |
| Coin Release Method | Early Mining | Through ICO |
| Average Block Time | ~10 minutes | ~12-15 seconds |
| Purpose | Alternative to Regular Money | Peer to peer Contracts |

8.2 Hyperledger-

“Hyperledger is an open sourced community of communities to benefit an ecosystem of Hyperledger based solution providers and users focused on blockchain related use cases that will work across a variety of industrial sectors.“ – Brian Behlendorf, Executive Director of Hyperledger.

Hyperledger is an umbrella project, under the Linux Foundation. NodeJs, Alljoyn, Dronecode are some example projects that have adopted the “Linux Way”, i.e. to weave a community of developers who work on open source projects thus maintaining a cycle where a piece of code is constantly getting modified and redistributed.

Hyperledger project began with a small number of developers in late 2015. These developers came from various sectors like data science, manufacturing, banking etc., and had one common goal in mind, i.e. to make blockchain as a technology more accessible to developers and industries.

8.2.1 Notable changes in Hyperledger-

Due to Hyperledger’s modular architecture which makes properties like consensus a plug-and-play feature. In this architecture, the most notable changes are seen in the peers of a network. The peers have been divided into two separate runtimes and three distinct roles namely,

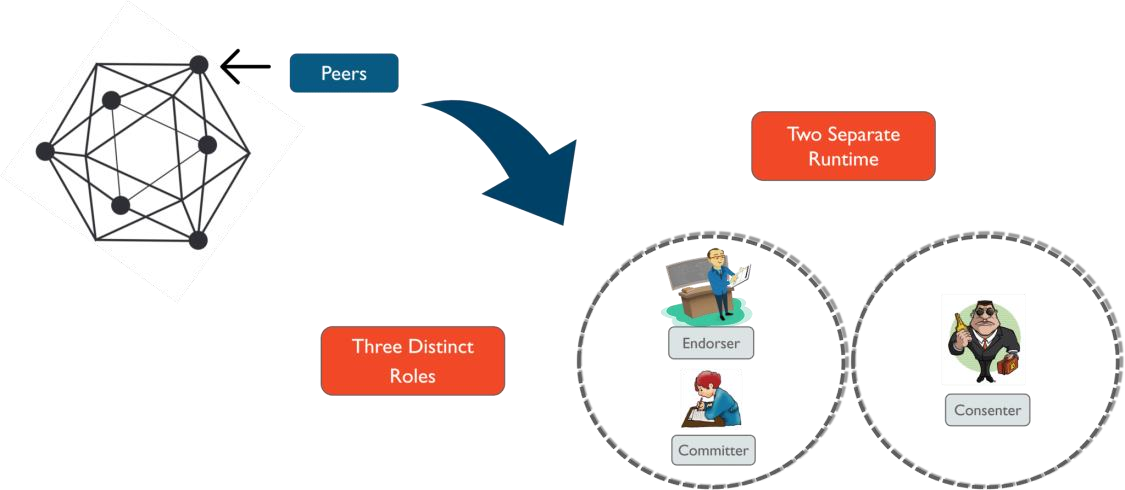


Fig 8.2.1 Hyperledger architecture

* + - Committer:

These peers only write validated transactions returned from the consensus mechanism to the respective ledgers. Committer nodes can act as Endorsers on networks with fewer restrictions. But, as restrictions are increased, this condition is completely avoided

* + - Endorser:

These nodes are responsible for simulating transactions specific to their network and prevent non-deterministic and unreliable transactions. While committers may or may not be endorsers depending on network restrictions, all endorsers act as committers

* + - Consenters:

These nodes are responsible for running the consensus of the network. They run on a completely different run-time, unlike endorsers and committers which run on the same runtime. Consenters are responsible for validating transactions and deciding which ledger the transaction be committed to.

8.2.2 Hyperledger Projects:

Hyperledger is an umbrella project. This means that there are numerous projects under Hyperledger itself. These include projects such as:

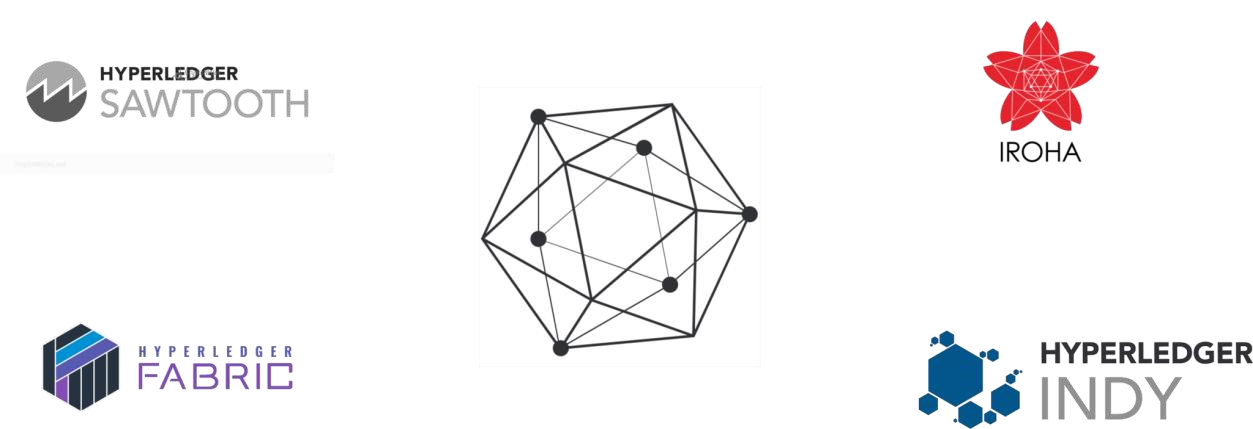


Fig 8.2.2: Hyperledger Projects

* + - 1. *Hyperledger Fabric,* used extensively in supply-chain networks
      2. *Hyperledger Sawtooth,* is being used in the fishing industry to track the journey of fishes
      3. *Hyperledger Burrow,* which is being used to run Ethereum smart contracts in a Hyperledger network
      4. *Hyperledger Iroha,* finds usage in mobile application optimization with the help of blockchain
      5. *Hyperledger Indy,* is being used as a decentralized identity database service for bus

# CHAPTER 9

# PROS AND CONS OF BLOCKCHAIN

9.1 Advantages-

9.1.1 Distributed:

Since blockchain data is often stored in thousands of devices on a distributed network of nodes, the system and the data are highly resistant to technical failures and malicious attacks. Each network node is able to replicate and store a copy of the database and, because of this, there is no single point of failure: a single node going offline does not affect the availability or security of the network.

In contrast, many conventional databases rely on a single or a few servers and are more vulnerable to technical failures and cyber-attacks.

9.1.2 Stability:

Confirmed blocks are very unlikely to be reversed, meaning that once data has been registered into the blockchain, it is extremely difficult to remove or change it. This makes blockchain a great technology for storing financial records or any other data where an audit trail is required because every change is tracked and permanently recorded on a distributed and public ledger.

For example, a business could use blockchain technology to prevent fraudulent behaviour from its employees. In this scenario, the blockchain could provide a secure and stable record of all financial transactions that take place within the company. This would make it much harder for an employee to hide suspicious transactions.

9.1.3 Trust less system:

In most traditional payment systems, transactions are not only dependent on the two parties involved, but also on an intermediary - such as a bank, credit card company, or payment provider. When using blockchain technology, this is no longer necessary because the distributed network of nodes verify the transactions through a process known as [mining.](https://www.binance.vision/blockchain/what-is-cryptocurrency-mining) For this reason, Blockchain is often referred to as a 'trust less' system.

Therefore, a blockchain system negates the risk of trusting a single organization and also reduces the overall costs and transactions fees by cutting out intermediaries and third parties.

9.2 Disadvantages-

9.2.1 51% Attacks:

The [Proof of Work](https://www.binance.vision/blockchain/proof-of-work-explained) [consensus algorithm](https://www.binance.vision/blockchain/what-is-a-blockchain-consensus-algorithm) that protects the [Bitcoin](https://www.binance.vision/blockchain/what-is-bitcoin) blockchain has proven to be very efficient over the years. However, there are a few potential attacks that can be performed against blockchain networks and [51% attacks](https://www.binance.vision/security/what-is-a-51-percent-attack) are among the most discussed.

Such an attack may happen if one entity manages to control more than 50% of the network hashing power, which would eventually allow them to disrupt the network by intentionally excluding or modifying the ordering of transactions.

Despite being theoretically possible, there was never a successful 51% attack on the Bitcoin blockchain. As the network grows larger the security increases and it is quite unlikely that miners will invest large amounts of money and resources to attack Bitcoin as they are better rewarded for acting honestly. Other than that, a successful 51% attack would only be able to modify the most recent transactions for a short period of time because blocks are linked through cryptographic proofs (changing older blocks would require intangible levels of computing power). Also, the Bitcoin blockchain is very resilient and would quickly adapt as a response to an attack.

9.2.2 Data modification:

Another downside of blockchain systems is that once data has been added to the blockchain it is very difficult to modify it. While stability is one of blockchain’s advantages, it is not always good. Changing blockchain data or code is usually very demanding and often requires a [hard fork,](https://www.binance.vision/blockchain/hard-forks-and-soft-forks) where one chain is abandoned, and a new one is taken up.

9.2.3 Private keys:

Blockchain uses public-key (or asymmetric) [cryptography](https://www.binance.vision/glossary/cryptography) to give users ownership over their cryptocurrency units (or any other blockchain data). Each blockchain address has a corresponding private key. While the address can be shared, the private key should be kept secret. Users need their private key to access their funds, meaning that they act as their own bank. If a user loses their private key, the money is effectively lost, and there is nothing they can do about it.

9.2.4 Inefficient:

Blockchains, especially those using [Proof of Work,](https://www.binance.vision/blockchain/proof-of-work-explained) are highly inefficient. Since mining is highly competitive and there is just one winner every ten minutes, the work of every other miner is wasted. As miners are continually trying to increase their computational power, so they have a greater chance of finding a valid block hash, the resources used by the Bitcoin network has increased significantly in the last few years, and it currently consumes more energy than many countries, such as Denmark, Ireland, and Nigeria.

9.2.5 Storage:

Blockchain ledgers can grow very large over time. The Bitcoin blockchain currently requires around 200 GB of storage. The current growth in blockchain size appears to be outstripping the growth in hard drives and the network risks losing nodes if the ledger becomes too large for individuals to download and store.

# CHAPTER 10

# FUTURE SCOPE

10.1 Financial Services-

Traditional systems tend to be cumbersome, error-prone and maddeningly slow. Intermediaries are often needed to mediate the process and resolve conflicts. Naturally, this costs stress, time, and money. In contrast, users find the blockchain cheaper, more transparent, and more effective. Small wonder that a growing number of financial services are using this system to introduce innovations, such as [smart bonds](http://smartbonds.co/) and [smart contracts.](https://blockgeeks.com/guides/smart-contracts/) The former automatically pays bondholders their coupons once certain preprogramed terms are met. The latter are digital contracts that self-execute and self-maintain, again when terms are met.

Examples of blockchain financial services applications:

1. Asset Management:Trade Processing and Settlement

Traditional trade processes within asset management (where parties trade and manage assets) can be expensive and risky, particularly when it comes to cross-border transactions. Each party in the process, such as broker, custodian, or the settlement manager, keeps their own records which create significant inefficiencies and room for error. The blockchain ledger reduces error by encrypting the records. At the same time, the ledger simplifies the process, while cancelling the need for intermediaries.

1. Insurance: Claims processing

Claims processing can be a frustrating and thankless procedure. Insurance processors have to wade through fraudulent claims, fragmented data sources, or abandoned policies for users to state a few and process these forms manually. Room for error is huge. The blockchain provides a perfect system for risk-free management and transparency. Its encryption properties allow insurers to capture the ownership of assets to be insured.

1. Payments: Cross-Border Payments

The global payments sector is error-prone, costly, and open to money laundering. It takes days if not longer for money to cross the world. The blockchain is already providing solutions with remittance companies such as [Abra,](https://www.goabra.com/) [Align Commerce](https://www.aligncommerce.com/?cid=3050&kid=3052&gclid=CjwKEAiAjvrBBRDxm_nRusW3q1QSJAAzRI1tS7bbm_853D8KBmM0Oo0ICLotxGrFYT9TEyap2SZtARoCagbw_wcB) and [Bitspark](https://bitspark.io/) that offer end-to-end blockchain powered remittance services. In 2004, Santander became one of the first banks to merge blockchain to a payment’s app, enabling customers to make international payments 24 hours a day, while clearing the next day.

10.2 Smart Property-

A tangible or intangible property, such as cars, houses, or cookers, on the one hand, or patents, property titles, or company shares, on the other, can have smart technology embedded in them. Such registration can be stored on the ledger along with contractual details of others who are allowed ownership in this property. Smart keys could be used to facilitate access to the permitted party. The ledger stores and allows the exchange of these smart keys once the contract is verified.

The decentralized ledger also becomes a system for recording and managing property rights as well as enabling the [smart contracts](https://blockgeeks.com/guides/smart-contracts/) to be duplicated if records or the smart key is lost.

Making property smart decreases your risks of running into fraud, mediation fees, and questionable business situations. At the same time, it increases trust and efficiency.

Examples of Blockchain Smart Property Applications:

1. Unconventional money lenders/ hard money lending:

Smart contracts can revolutionize the traditional lending system. For instance, unconventional money lenders (e.g. hard money lenders) service borrowers who have poor credit with needed loans while charging two to ten percent of the loan amount and claiming their property as collateral. Too many borrowers fall into bankruptcy and lose homes. The blockchain can undercut this by allowing a stranger to loan you money and taking your smart property as collateral. No need to show the lender credit or work history. No need to manually process the numerous documents. The property’s encoded on the blockchain for all to see.

1. Your car/ smartphone:

Primitive forms of smart property exist. Your [car-key,](https://blockgeeks.com/blockchain-car-wallet/) for instance, may be outfitted with an immobilizer, where the car can only be activated once you tap the right protocol on the key. Your smartphone too will only function once you type in the right PIN code. Both work on cryptography to protect your ownership.

The problem with primitive forms of smart property is that the key is usually held in a physical container, such as the car key or SIM card, and can’t be easily transferred or copied. The blockchain ledger solves this problem by allowing blockchain miners to replace and replicate a lost protocol.

10.3 Blockchain Internet-of-Things (IoT)-

Any material object is a ‘thing.’ It becomes an [internet of things (IoT) wh](https://blockgeeks.com/blockchain-and-iot-a-perfect-match/)en it has an on/ off switch that connects it to the internet and to each other. By being connected to a computer network, the object, such as a car, become more than just an object. It is now peoplepeople, people-things, and things-things. The analyst firm [Gartner](http://www.forbes.com/companies/gartner/) says that by 2020 there will be over 26 billion connected devices. Others raise that number to over 100! How does the IoT affect you? Your printer can automatically order cartridges from Amazon when it runs low. Your alarm clock will change your time for brewing coffee, while your oven will produce an immaculately timed turkey for Thanksgiving. These are just some examples. On a larger scale, cities and governments can use IoT to develop cleaner environments, more efficient energy use and so-called ‘smart cities,’ to improve how we live and work.

Where the blockchain comes in as in all cases, the blockchain ledger provides security to this Internet of things. With billions of devices linked together, cybersecurity experts worry how to make sure this distributed information stays secure.

* What can companies do to protect their systems from being invaded?
* How can inventors shield their ideas?
* How should governments protect their secret information from spies and potential terrorists?

Then, there’s the problem of how to organize and analyse this massive amount of data that’s coming from these related devices. Enter the blockchain ledger system that ensures that information is only accepted and released to trusted parties. The ledger grants parties a management platform for analysing the vast amounts of data.

Examples of Blockchain Internet-of-Things (IoT) Applications,

1. Smart Appliances:

A smart appliance is a device that connects to the internet and gives you more information and control than before. For instance, a code connected to your appliance can be linked to the internet and alert you when your cookies are ready or if your laundry has stopped. These alerts keep your appliances in good condition, they save you money regarding energy efficiency and help you control your devices when away from home, among other benefits. Encrypting these appliances on the blockchain protects your ownership and enables transferability.

2. Supply Chain Sensors:

Sensors give companies end-to-end visibility of their supply chain by providing data on the location and condition of the supplies as they are transported around the globe. As of 2016, a Deloitte and MHI report [surveyed](https://www2.deloitte.com/us/en/pages/about-deloitte/articles/press-releases/deloitte-mhi-annual-report.html) 99 leading supply chain companies and found that sensors were used by 44% of these respondents. Eighty-seven percent of these industries said they plan to use the technology by 2020. The technology is expected to grow to 1 trillion by 2022 and to 10 trillion sensors by 2030, according to this same Deloitte and MHI report. The blockchain stores, manages, protects and transfers this smart information.

10.4 Smart Contracts-

Smart contracts are digital which are embedded with an if-this-then-that (IFTTT) code, which gives them self-execution. In real life, an intermediary ensures that all parties follow through on terms. The blockchain not only waives the need for third parties, but also ensures that all ledger participants know the contract details and that contractual terms implement automatically once conditions are met. You can use smart contracts for all sort of situations, such as financial derivatives, insurance premiums, property law, and crowd funding agreements, among others.

Examples of Blockchain Smart Contracts Applications,

* + 1. Blockchain Healthcare:

Personal health records could be encoded and stored on the blockchain with a private key which would grant access only to specific individuals. The same strategy could be used to ensure that research is conducted via [HIPAA laws](https://www.hhs.gov/hipaa/for-professionals/privacy/) (in a secure and confidential way). Receipts of surgeries could be stored on a blockchain and automatically sent to insurance providers as proof-of-delivery. The ledger, too, could be used for general health care management, such as supervising drugs, regulation compliance, testing results, and managing healthcare supplies.

* + 1. Blockchain music:

Key problems in the music industry include ownership rights, royalty distribution, and transparency. The digital music industry focuses on monetizing productions, while ownership rights are often overlooked. The blockchain and smart contracts technology can circuit this problem by creating a comprehensive and accurate decentralized database of music rights. At the same time, the ledger and provide transparent transmission of artist royalties and real time distributions to all involved with the labels. Players would be paid with digital currency according to the specified terms of the contract.

10.5 Blockchain Government-

In the 2016 election, Democrats and Republicans questioned the security of the voting system. The [Green Party called for a recount](http://www.usatoday.com/story/news/politics/onpolitics/2016/11/28/recount-need-to-know/94547368/) in Wisconsin, Pennsylvania, and Michigan. Computer scientists say hackers can rig the electronic system to manipulate votes. The ledger would prevent this since votes become encrypted. Private individuals can confirm that their votes were counted and confirm who they voted for. The system saves money, by the way, for the government, too.

The blockchain ledger, also, provides a platform for what we call “responsive, open data.” According to a [2013 report from McKinsey and Company,](http://www.wired.co.uk/article/blockchain-is-the-new-signature) open data – freely accessible government-sourced data that is available over the internet to all citizens – can make the world richer by $2.6 trillion. Start-ups can use this data to uncover fraudulent schemes, farmers can use it to perform precision farm-cropping, and parents can investigate the side effects of medicine for their sick children. Right now, this data is released only once a year and is, largely, non-responsive to citizens input. The blockchain, as a public ledger, can open this data to citizens whenever and wherever they want.

Examples of Blockchain Government Applications,

1. Public value/ community:

The blockchain can facilitate self-organization by providing a self-management platform for companies, NGOs, foundations, government agencies, academics, and individual citizens. Parties can interact and exchange information on a global and transparent scale – think of Google Cloud, but larger and less risky.

1. Vested responsibility:

Smart contracts can ensure that electorates can be elected by the people for the people so that government is what it’s meant to be. The contracts specify the electorate’s expectations and electors will get paid only once they do what the electorate demanded rather than what funders desired.

1. Blockchain Identity:

Whether we like it or not, online companies know all about us. Some companies whom we purchase from sell our identity details to advertisers who send you their ads. The blockchain blocks this by creating a protected data point where you encrypt only the information that you want relevant people to know at certain times. For example, if you’re going to a bar, the bartender simply needs the information that tells him you’re over 21.

10.6 Blockchain Identity-

The blockchain protects your identity by encrypting it and securing it from spammers and marketing schemes.

Examples of Blockchain Identity Applications,

1. Passports:

The first digital passport launched on [GitHub](https://github.com/) in 2014 and could help owners identify themselves online and off. How does it work? You take a picture of yourself, stamp it with a public and private key, both of which are encoded to prove it is legitimate. The passport is stored on the ledger, given a Bitcoin address with a public IP, and confirmed by Blockchain users.

1. Birth, wedding, and death certificates:

Few things are more important than documents showing you’re born, married, died which open your rights to all sorts of privileges (such as voting, working, citizenship), yet mismanagement is rife. [Up to a third of children under the age of five have not been issued a birth certificate,](https://www.unicef.org/media/media_71508.html) the UNICEF reported in 2013. The blockchain could make recordkeeping more reliable by encrypting birth and death certification and empowering citizens to access this crucial information.

1. Personal Identification:

We carry a range of identifications: Our driver’s license, computer password, identity cards, keys, social security ID, and so forth. Blockchain ID is a digital form of ID that’s engineered to replace all these forms of physical identification. In the future, fintech scientists say you’ll be able to use the one digital ID for signing up at any registrar. It is open source, secured by the blockchain, and protected by a ledger of transparent account.

# CHAPTER 11

# CONCLUSION

In this short we have seen several concepts of Blockchain by taking Bitcoin as a main application. 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.

**CHAPTER 12**

**REFERENCES**

* [www.telusko.com](http://www.telusko.com/)
* [www.eduka.co](http://www.eduka.co/)
* [www.binance.vision](http://www.binance.vision/)
* hackernoon.com
* [www.guru99.com](http://www.guru99.com/)
* [www.javatpoint.com](http://www.javatpoint.com/)
* www.coindesk.com
* [blockgeeks.com](https://blockgeeks.com/)
* bitcoin.org
* [www.researchgate.net](http://www.researchgate.net/)
* lisk.io
* medium.com
* [https://blog.goodaudience.com](https://blog.goodaudience.com/)
* [www.blockchain.com](http://www.blockchain.com/)
* [www.powerpointschool.com](http://www.powerpointschool.com)