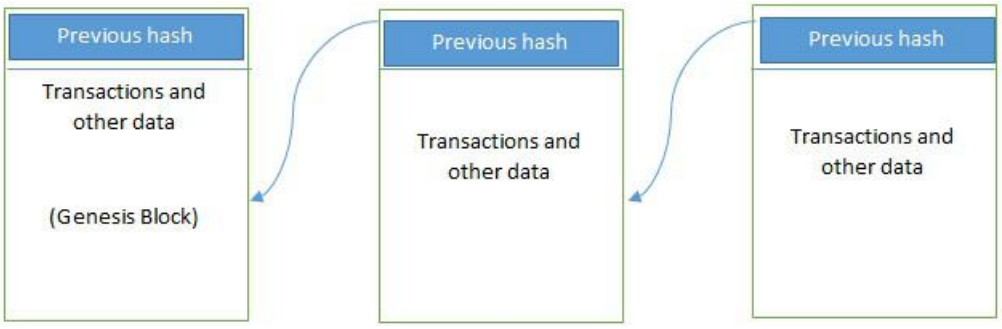
Generic Elements Of A Blockchain

- The structure of a generic blockchain can be visualized by the following diagram:



- Elements of a generic blockchain are:
  - **Address**: Addresses are unique identifiers used in a blockchain transaction to denote senders and recipients. An address is usually a public key or derived from a public key. While addresses can be reused by the same user, addresses themselves are unique.
    - A good practice is for users to generate a new address for each transaction in order to avoid linking transactions to the common owner, thus preventing identification.
  - **Transaction**: A transaction is the fundamental unit of a blockchain. A transaction represents a transfer of value from one address to another.
  - **Block**: A block is composed of multiple transactions and other elements, such as the previous block hash (hash pointer), timestamp, and nonce.
  - **Peer-to-peer network**: A peer-to-peer network is a network topology wherein all peers can communicate with each other and send and receive messages.
  - **Scripting or programming language**: Scripts or programs perform various operations on a transaction in order to facilitate various functions.
    - For example, in Bitcoin, transaction scripts are predefined in a language called **Script**, which consists of sets of commands that allow nodes to transfer tokens from one address to another. Script is a limited language, it only allows essential operations that are necessary for executing transactions, but it does not allow for arbitrary program development.
  - **Virtual machine**: This is an extension of the transaction script. A *virtual machine* allows Turing complete code to be run on a blockchain (as smart contracts); whereas a transaction script is limited in its operation.

Various blockchains use virtual machines to run programs such as **Ethereum Virtual Machine** (**EVM**) and **Chain Virtual Machine** (**CVM**). EVM is used in Ethereum blockchain, while CVM is a virtual machine developed for and used in an enterprise-grade blockchain called **Chain Core**.

- **State machine**: A blockchain can be viewed as a state transition mechanism whereby a state is modified from its initial form to the next one ie. a result of a transaction execution, validation, and finalization process.
- **Node**: A node in a blockchain network performs various functions depending on the role that it takes on. Functions are:
  - Propose and validate transactions and perform mining to secure the blockchain. This is achieved by following a **consensus protocol** - PoW).
  - Perform other functions such as simple payment verification (lightweight nodes), validation, and many other functions
  - Nodes also perform a transaction signing function.
- **Smart contract**: These programs run on top of the blockchain and encapsulate the business logic to be executed when certain conditions are met. These rograms are enforceable and automatically executable. The smart contract feature is not available on all blockchain platforms. Smart contracts have many use cases, including but not limited to identity management, capital markets, trade finance, record management, insurance, and e-governance.

How blockchain works

- Nodes are either

  miners who create new blocks and mint cryptocurrency (coins)

  or *block signers* who validates and digitally sign the transactions.

A critical decision that every blockchain network has to make is to figure out that which node will append the next block to the blockchain. This decision is made using a *consensus mechanism*.

How blockchain accumulates blocks

- Now we will look at a general scheme for creating blocks and what the relationship is between transactions and blocks:

  1. A node starts a transaction by first creating and then digitally signing it with its private key. A transaction can represent various actions in a blockchain. Transaction

data structure usually consists of logic of transfer of value, relevant rules, source and destination addresses, and other validation information.

2. A transaction is propagated (flooded) by using a flooding protocol, called **Gossip protocol**, to peers that validate the transaction based on preset criteria.

3. Once the transaction is validated, it is included in a block, which is then propagated onto the network. At this point, the transaction is considered confirmed.

4. The newly-created block now becomes part of the ledger, and the next block links itself cryptographically back to this block. This link is a hash pointer. At this stage, the transaction gets its second confirmation and the block gets its first confirmation.

5. Transactions are then reconfirmed every time a new block is created. Usually, six confirmations in the Bitcoin network are required to consider the transaction final.

Benefits and limitations of blockchain

- **Decentralization**: This is a core concept and benefit of the blockchain. There is no need for a trusted third party or intermediary to validate transactions; instead, a consensus mechanism is used to agree on the validity of transactions.
- **Transparency and trust**: Because blockchains are shared and everyone can see what is on the blockchain, this allows the system to be transparent. As a result, trust is astablished.
- **Immutability**: Once the data has been written to the blockchain, it is extremely difficult to change it back. It is not genuinely immutable.
- **High availability**: As the system is based on thousands of nodes in a peer-to-peer network, and the data is replicated and updated on every node, the system becomes highly available.
- **Highly secure**: All transactions on a blockchain are cryptographically secured and thus provide network integrity.
- **Simplification of current paradigms**: The current blockchain model in many industries, such as finance or health. A blockchain can serve as a single shared ledger among many interested parties, this can result in simplifying the model by reducing the complexity of managing the separate systems maintained by each entity.
- **Faster dealings**: In the financial industry, especially in post-trade settlement functions, blockchain can play a vital role by enabling the quick settlement of trades because a single version of agreed-upon data is already available on a shared ledger between financial organizations.

- **Cost saving**: As no trusted third party or clearing house is required in the blockchain model, this can massively eliminate overhead costs in the form of the fees which are paid to such parties.
- Some challenges need to be addressed by blockchain technology. The most sensitive blockchain problems are as follows:

Scalability

Adaptability

Regulation

Relatively immature technology

Privacy

Tiers of blockchain technology

In this section, various layers of blockchain technology are presented. The three levels are:

Tier 1, Tier 2 and Tier 3, or Tier X

- **Blockchain 1.0**: This tier was introduced with the invention of Bitcoin, and it is primarily used for cryptocurrencies. This first generation of blockchain technology includes only cryptographic currencies.
    - All cryptocurrencies as well as Bitcoin fall into this category. It includes core applications such as payments and applications.
    - This generation started in 2009 when Bitcoin was released and ended in early 2010.
- **Blockchain 2.0**: This second blockchain generation is used by financial services and smart contracts. This tier includes various financial assets, such as derivatives, options, swaps, and bonds. Applications that go beyond currency, finance, and markets are incorporated at this tier.
    - Ethereum, Hyperledger, and other newer blockchain platforms are considered part of Blockchain 2.0.
    - This generation started when ideas related to using blockchain for other purposes started to emerge in 2010.
- **Blockchain 3.0**: This third blockchain generation is used to implement applications beyond the financial services industry and is used in government, health, media, the arts, and justice.
    - Ethereum, Hyperledger, and newer blockchains are considered part of this blockchain technology tier.

- This generation of blockchain emerged around 2012 when multiple applications of blockchain technology in different industries were researched.

- **Blockchain X.0**: This generation represents a vision of blockchain singularity. It will provide services for all realms of society. It will be a public and open distributed ledger with general-purpose rational agents (*Machina economicus*), making decisions, and interacting with other intelligent autonomous agents on behalf of people, and contracts will be implementable in code.

Features of a blockchain

The features of a blockchain are described here:

- **Distributed consensus**: This mechanism allows a blockchain to present a single version of the truth, which is agreed upon by all parties without the requirement of a central authority.
- **Transaction verification**: Any transactions posted from the nodes on the blockchain are verified based on a predetermined set of rules. Only valid transactions are selected for inclusion in a block.
- **Platform for smart contracts**: A blockchain is a platform on which programs can run to execute business logic on behalf of the users. This is a very desirable feature, and it is available on newer blockchain platforms such as Ethereum and MultiChain.
- **Transferring value between peers**: Blockchain enables the transfer of value between its users via tokens. Tokens can be thought of as a carrier of value.
- **Generation of cryptocurrency**: This feature is optional depending on the type of blockchain in use. A blockchain can create cryptocurrency as an incentive to its miners who validate the transactions and spend resources to secure the blockchain.
- **Smart property**: It is now possible to link a digital or physical asset to the blockchain in such a secure and precise manner that it cannot be claimed by anyone else. You are in full control of your asset, and it cannot be double-spent or double-owned.
- **Provider of security**: The blockchain is based on proven cryptographic technology that ensures the integrity and availability of data.
    - For example, with Bitcoin, confidentiality is not an absolute requirement; however, it is desirable in some scenarios.
    - A more recent example is Zcash, which provides a platform for conducting anonymous transactions.

.

- **Immutability**: This is another critical feature of blockchain: once records are added to the blockchain, they are immutable.
- **Uniqueness**: This blockchain feature ensures that every transaction is unique and has not already been spent (double-spend problem). This feature is especially relevant with cryptocurrencies, where detection and avoidance of double spending are a vital requirement.