**Block-Chain**

**Definition:-** A blockchain is a continuously growing list of records called blocks which are linked and secured using cryptography.

**Fields of a Block**:- Field of a block means what are the sections inside a block and what makes it unique from other security domains!!!

1. Data Field :-Contains all the necessary information.
2. Nonce:- Number only once. It plays a significant role in the block chain by allowing to change the **hash** value in the block without changing the data field of the block(Immutable Ledger).
3. **Hash:** In context to Block-Chain, hash is a deterministic Hexadecimal Number. This means that no matter how many characters the input has, the hash will always be the same number of characters. For example,

**SHA-256** hash algorithm developed by NSA. It takes 256 bits in memory(64 Characters Long).

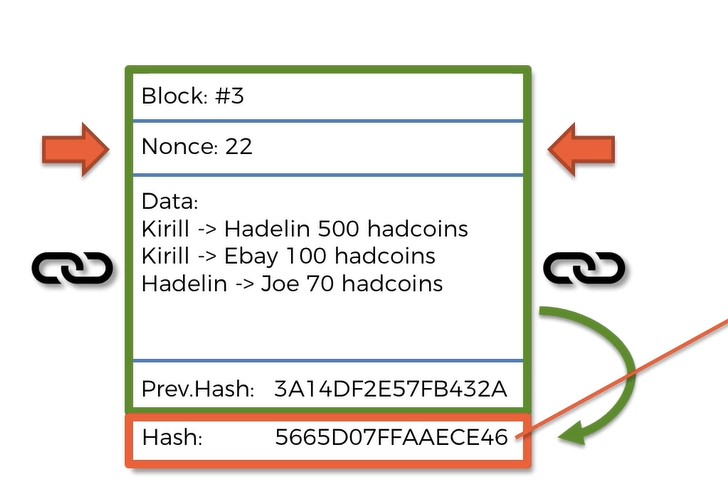
**The five requirements for hash algorithms are:-**

1. One Way:- It states that ,say for example, a word file contains several pieces of information about anything/anybody. When this word file is treated on a hash algorithm, it generates a corresponding hash value for it **but** **the reverse is not true!!!!**
2. Deterministics in nature:- Same file/docs produces the same hash value.
3. Avalanche Effect:- If very little change is made to the document then the entire hash value will change.
4. Fast Computation.
5. Must Withstand collisions.

**A block contains two types of hash value:-**

1. Previous hash:- Contains the hash value of previous block(except First block also called genesis Block).
2. Self hash:- Its own hash value.

**Visual Representation of a block:-**



**Immutable Ledger**

An immutable ledger in blockchain refers to any records that can remain unchanged. It cannot be altered, so the data cannot be easily changed. Immutability means that it's easier to make changes with collusion. The central idea is the security of data and proof that data has not been changed.

Let's take a scenario as such that,

There are 5 blocks(assume) cryptographically connected together, lets suppose a target attacker wants to steal the data from block 3 then what difficulty will arise to the attacker?

Ans:-The attacker has to change the hash value of next block’s previous hash value and continuously next and next block. This is so because the blocks are connected to each other by the value of the hash of the previous block (except the first block).

**Distributed P2P network**

Peer to Peer, commonly known as P2P is a decentralized network communications model that consists of a group of devices (nodes) that collectively store and share files where each node acts as an individual peer. In this network, P2P communication is done without any central administration or server, which means all nodes have equal power and perform the same tasks.

**What is Consensus??**

In BlockChain Technology,consensus mechanism is a system that validates the transactions and marks/identifies as authentic.This mechanism lists all valid transactions of a coin in a blockchain to build trust in the coin among traders.

**Now the Question is:- How does it work in BlockChain ?**

It achieves the agreement of most users on a single network. The consensus mechanism maintains the security of the blockchain by keeping the records of all legitimate transactions.It provides a method of review and confirmation of what data should be added to a blockchain's record. Because blockchain networks typically don't have a centralized authority dictating who is right or wrong, nodes on a blockchain all must agree on the state of the network, following the predefined rules, or protocol.

**The few predefined rules are as:-**

i) check systematic correctness.

ii) check prev hash is present in current block or not

iii) Transaction list must not be empty.

The types of consensus protocol are:-

i)Proof Of Work(PoW): Used by bitcoin

ii)Proof Of Authority(PoA)

**Lets discuss Proof of Work**

Proof of work is a consensus mechanism to choose which of these network participants—called miners—are allowed to handle the lucrative task of verifying new data. It’s lucrative because the miners are rewarded with new crypto when they accurately validate the new data and don’t cheat the system.“Proof of work is a software algorithm used by [Bitcoin](https://www.forbes.com/advisor/investing/what-is-bitcoin/) and other blockchains to ensure blocks are only regarded as valid if they require a certain amount of computational power to produce. It depends on the hashing power

**What is Mining? How Mining works?**

According to the context of Block-Chain Technology,Mining is the process/action of adding new transaction details to the current(existing) digital ledger.

A block in a block-Chain contains the following fields such as the block number, nonce,data,previous\_hash,current hash.

Now ,Miners must solve the hash puzzle by finding the hash below a given target through the difficulty requirement. The target, stored in the header, is expressed as a 67-digit number that will determine the mining difficulty based on the number of miners competing to solve a hash function.

**The above process can be achieved by different ways:-**

i) by manipulating the data in the data section

ii) By manipulating the nonce

**But there is a problem in “ i” step , that is,** we cannot tamper with the data because tampering with it may cause inconsistencies in the blockChain.

**So the only possible solution is to manipulate the nonce and getting a hash below the target level**

**Paper 1 Review:-**

The article assesses blockchain technology's energy consumption, with a focus on Proof of Work (PoW) blockchains like Bitcoin. It notes that PoW blockchains have substantial energy usage, which doesn't significantly correlate with transaction volume. Non-PoW and permissioned blockchains used in enterprises consume less energy but still exceed centralized systems. The article highlights the link between consensus mechanisms and energy use and suggests exploring a balance between performance, security, and energy efficiency. It underscores the importance of considering energy consumption in blockchain-based solutions. While blockchains can enhance sustainability in business applications, minimizing on-chain operations and embracing digitization can mitigate energy concerns and should be weighed against potential benefits such as reduced paperwork and carbon emissions in supply chains.

**Paper 4 Review:-**

This work introduced a framework to assist stakeholders in selecting the most suitable blockchain consensus mechanism for their projects based on energy consumption considerations. It integrated insights from green IT and blockchain to emphasize the importance of green blockchain in reducing carbon footprint. The study reviewed 18 consensus mechanisms, highlighting their advantages and drawbacks alongside real-world examples. It expanded on Wust and Gervais's methodology, creating a decision-support framework for the initial energy assessment of proposed projects. An indicative energy consumption (IECon) chart was developed to predict energy usage for each consensus mechanism. Lastly, the framework was applied to evaluate three live use cases, ranking their consensus mechanisms on the IECon chart.

**Paper 6 Review**

Blockchain transaction energy costs depend on local validation and inter-node communication. In Proof of Work systems like Bitcoin and Ethereum, high validation costs overshadow communication costs. A predictive model, considering factors like hashrate and transaction data, predicts energy usage with 92% accuracy. Ripple's consensus uses minimal energy (0.005 Wh per transaction), rivaling Visa's efficiency.

**Paper 2 Review**

Zero-Knowledge Rollups (zk-rollups) are a cutting-edge development in blockchain technology, leveraging Zero-Knowledge Proofs (ZKPs) to enhance scalability and efficiency. ZKPs enable users to prove the correctness of complex computations without revealing specific details, enhancing privacy and efficiency. zk-rollups bundle multiple off-chain transactions into a single rollup transaction, reducing data storage and computational overhead. They provide robust security, as proofs are verified on-chain, preventing manipulations. This approach significantly reduces gas costs and improves transaction throughput, making blockchain networks more scalable and cost-effective. While zk-rollups offer substantial energy savings, factors like idle power consumption and network size also impact overall efficiency.

**Paper 7**

Proof-of-Stake (PoS) and Delegated Proof-of-Stake (DPoS) are consensus mechanisms that can reduce the energy consumption of blockchain mining by up to 99.5%.

PoS selects validators based on their stake in the network, while DPoS allows users to vote for validators. Both PoS and DPoS are much more efficient than Proof-of-Work (PoW), which is the consensus mechanism used by Bitcoin.

**Paper 8**

To reduce energy consumption in blockchain, consider transitioning to energy-efficient consensus mechanisms like Proof-of-Stake (PoS), employing off-chain scaling solutions, and optimizing algorithms. Additionally, promoting renewable energy usage and regulatory measures can play crucial roles in mitigating the environmental impact of blockchain technology.

Paper 9

The study focuses on energy consumption per transaction in blockchain systems, using PoS protocols like Polkadot. It correlates validator nodes and transaction throughput. Hardware and utilization vary for permissionless and high-tps systems. The research provides insights for comparing blockchain environmental impacts.

Paper 10

This paper investigates the application of blockchain technology in an industrial operating system called Predix. It showcases a practical use case involving green certificates, specifically within an eco-district. In essence, the study examines how blockchain can be employed to track and manage environmental certifications within an industrial context, using Predix as the underlying platform.