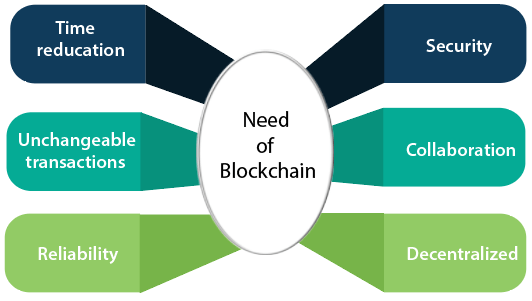
**What is Blockchain?**

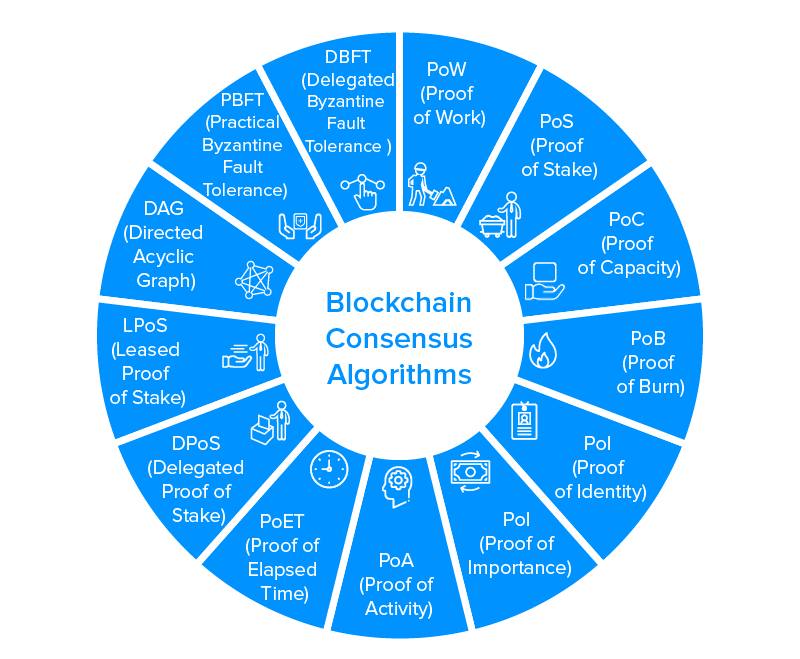
Before moving to the consensus algorithm used in the blockchain , let’s have a look on the blockchain. It was a technology originally created to support the famous cryptocurrency, **Bitcoin**. It was just like internet for emails. Unlike traditional methods, blockchain enables peer to peer transfer of digital assets without any intermediaries. Then the blockchain by itself has taken a life of its own and now have a wide range of applications across many industries, including finance, healthcare, government, manufacturing, and distribution.

Bitcoin enabled an innovative platform for peer to peer transfer of value without any central authority. With no central authority, how did Bitcoin realize trust and security? By implementing software programs for validation, verification, consensus in a novel infrastructure called the blockchain. So here comes the concept of Consensus Algorithm.

****

**Blockchain Consensus Algorithms**

In a blockchain environment, transactions are grouped into blocks and added to the network. However, this only happens once the network participants have reached an agreement, or consensus, on the validity of the transactions. This ensures that all participants are working based on the same ledger containing the same set of historical transactions and the same rules. There are many consensus algorithms used with their pros and cons.



The illustration of some of the mainly used consensus algorithm is given below.

**Proof-of-Work :-** Proof-of-Work is the consensus mechanism used by the bitcoin and many other public blockchains. In Bitcoin’s PoW method, the network operators are called miners and the ‘work’ refers to the computational power.

Miners expend work in competing to become the first to solve a computational puzzle known as a hash, which takes all of the most recent unconfirmed ledger transactions as an input. The hash puzzle is difficult to solve. The miner who solves the hash puzzle mines a block of transactions and presents their solution to the network for verification. If it passes the verification, the block is added to the blockchain, and the miner receives a Bitcoin-based reward for their efforts.

This mechanism is highly secure however, it comes with the significant challenge of being highly inefficient. The process of solving the hash puzzle takes around ten minutes because bitcoin has a fixed block size of 1MB, this limits the network to a processing speed of around 4-5 transactions per second, compared to the Visa network which processes 1,700 per second on average. It is also extremely energy-inefficient.

**Proof-of-Stake :-** Proof-of-Stake(PoS) has some similarities to PoW. In this, those who produce blocks are competing for rewards. However, in a PoS blocks are not mined. The principle of PoS is that those who hold the network tokens will have a stake in maintaining the integrity of the network. The forger will have no incentive to validate or to create fraudulent transactions because when the network detects the fraudulent transactions, the forger node will lose its stakes and also the right to participate as a forger in the future.

Anyone wanting to participate in block production for rewards must stake their tokens to become eligible. PoS offer the advantage of being far more energy-efficient than PoW because it doesn’t require the same computational effort to operate.

**Delegated Proof of Stake :-** Delegated Proof of Stake(DPoS) is similar to a model of representative democracy. Token holders on the network have the right to vote for those who they wish to become block producers. Voting is weighted according to the number of tokens staked, so those who stake more have a bigger share of the vote.

DPoS relies on far fewer block producers than PoW or PoS, meaning it has been criticized for promoting centralization. Furthermore, the voting mechanism can be subject to manipulation, if token holders form groups to try and influence the election.

**Proof of Authority :-** It operates in a similar way to PoS, except that rather than staking tokens, those in the network stake their own reputation, or authority. The underlying principle is that if they prove to be unreliable, they lose their authority and can no longer produce or validate blocks.

PoA consensus generally uses fewer block validators and has proven to be faster than PoW and PoS. PoA is well-suited to permissioned blockchains, as it doesn’t necessarily need to rely on a reward mechanism.