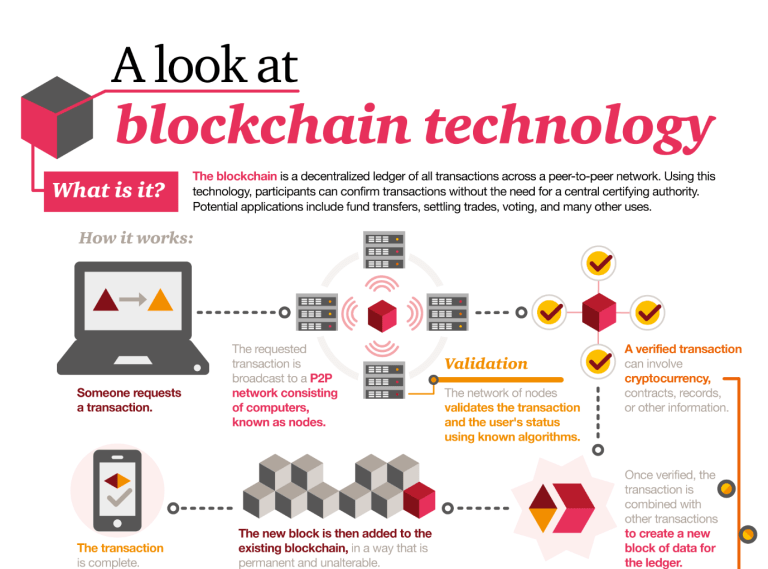
BLOCKCHAIN

Blockchain technology is a structure that stores transactional records, also known as the block, of the public in several databases, known as the “chain,” in a network connected through peer-to-peer nodes. Typically, this storage is referred to as a ‘digital ledger.’

Some of the features are :

* Decentralised
* Secure
* Peer-to-Peer



TYPES OF BLOCKCHAIN CONSENSUS MECHANISMS

1.Proof of Work

Proof of Work (POW) process is also called mining and the miners are known as nodes. Miners solve complicated mathematical puzzles that require extensive computational power. For this purpose, miners utilize multiple mining methods like CPU mining, GPU mining, FPGA mining, mining pools, ASIC mining, and many more. After solving mathematical puzzles, a miner receives a block as reward if they are the first one to find the solution. Additionally, the puzzles can only be solved with trial and error. Hence, miners require an increasing amount of computational power for finding solutions quickly.

The level of difficulty for the puzzles changes according to the speed at which the blocks are being mined. In case the blocks are created quickly, then the puzzles would get more difficult and vice versa. Therefore, new blocks have to be created within a particular time frame to carefully adjust the difficulty level of puzzles. Several popular cryptocurrencies like Bitcoin utilize Proof of Work process. However, Proof of Work consensus mechanism consumes resources at a staggering rate. [According to the sources,](https://digiconomist.net/bitcoin-energy-consumption) Bitcoin’s current estimated annual power consumption is 51.13 TWh. Hence, this approach can be expensive.

2. Proof of Stake

Proof of Stake (POS) uses a randomized process to figure out who gets a chance to produce the next block. Blockchain users can lock up their tokens for a certain time for becoming a validator. After becoming a validator, users can be able to produce blocks. Validators can also be selected based on the design of blockchain. Generally, the user who owns the biggest stake or owns coins for the longest period of time has better odds of creating a new block.

Validators usually get rewarded for their work with all or part of transaction fees of all the transactions carried out in the block they created. Alternatively, validators may receive a specific amount of coins due to inflation. With this approach, Proof of Stake method offers incentives to validators for maintaining the blockchain network. Proof of Stake is more energy efficient compared to other blockchain consensus mechanisms like Proof of Work.

3.Delegated Proof of Stake

In Delegated Proof of Stake process, users can stake their coins and vote for a particular number of delegates. The weight of a user’s vote is based on their stake. For instance, if a user ‘X’ stakes 20 coins for a delegate and another user ‘Y’ stakes 2, then X’s vote will have more weight compared to that of Y. The delegate that receives the highest number of votes gets a chance to produce new blocks. Delegates get rewarded with transaction fees or a specific amount of coins just like other blockchain consensus mechanisms such as Proof of Stake.

Delegated Proof of Stake (DPOS) mechanism is one of the fastest blockchain consensus mechanisms. This mechanism can handle a higher number of transactions compared to Proof of Work mechanism. Due to its stake-weighted voting system, DPOS is often considered as a digital democracy.

4.Proof of capacity

In Proof of Capacity method, solutions to complex mathematical puzzles are stored in digital storages such as hard disks. This entire process is called plotting. After a storage device is filled with solutions for mathematical puzzles, users can utilize it for producing blocks. Users who are fastest in finding the solutions get a chance to create a new block. Hence, users with the highest storage capacity will have to higher chances of producing a new block.

5.Proof of Elapsed Time

Proof of Elapsed Time process randomly and fairly decides the producer of a new block based on the time they have spent waiting. For this purpose, the mechanism provides a random wait time for each user and the user whose wait time finishes the earliest will produce a new block. This consensus mechanism only works if the system can verify that no users can run multiple nodes and the wait time is truly random.

6.Proof of Identity

Proof of Identity compares the private key of a user with an authorized identity. Basically, Proof of Identity is a piece of cryptographic evidence for a user’s private key that is cryptographically attached to a specific transaction. Any identified user from a blockchain network can create a block of data that can be presented to anyone in the network. Proof of Identity ensures integrity and authenticity of created data. Additionally, smart cities can use blockchain consensus mechanisms like Proof of Identity to verify the identity of their citizens.

7. Proof of Authority

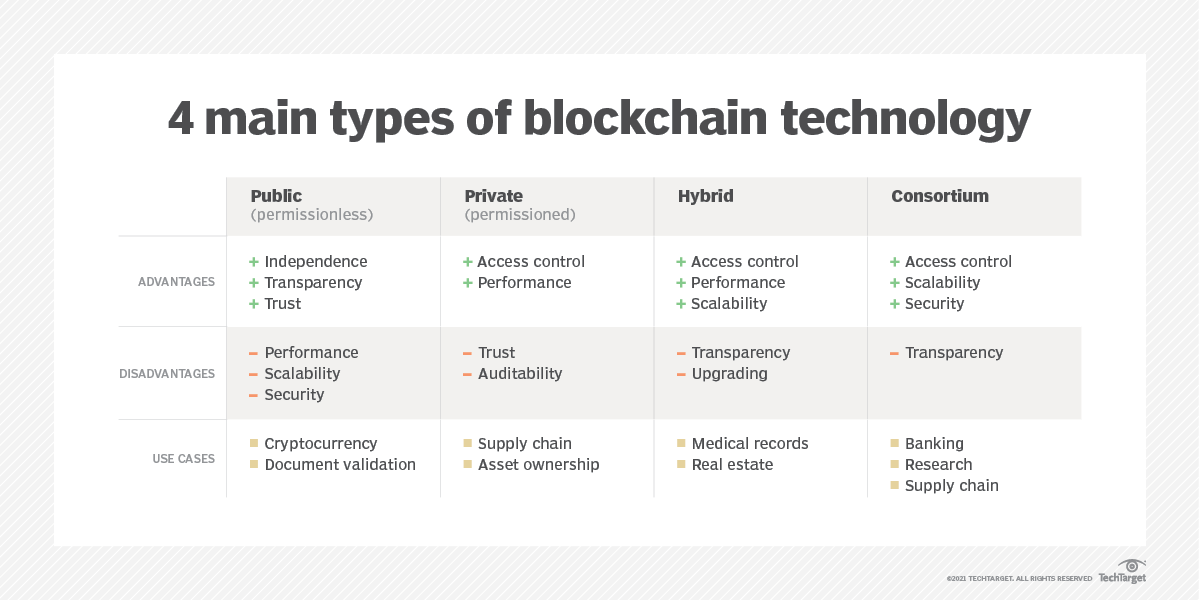
Proof of Authority mechanism is a modified version of Proof of Stake where the identities of validators in the network are at stake. In this scenario, the identity is the correspondence between validators’ personal identification and their official documentation to help verify their identity. These validators stake their reputation on the network. In Proof of Authority, the nodes that become validators are the only ones allowed to produce new blocks. Validators whose identity is at stake are incentivized to secure and preserve the blockchain network. Also, the number of validators is fairly small (i.e. 25 or less).

8. Proof of Activity

Proof of Activity mechanism is the combination of Proof of Work and Proof of Stake. In Proof of Activity, miners try to find the solution to a puzzle and claim their reward. However, the blocks created in Proof of Activity mechanism are simple templates with mining reward address and header information. The header information is then used to choose a random group of validators for signing a block. The validators with larger stakes will have greater odds of being selected to sign a new block. Once the selected validators sign a new block, it becomes a part of the network. In case the block stays unsigned by some validators, it gets discarded and a new block is utilized. The network fees generated in the process are distributed between the winning miner and the validators.

Despite having similar goals, various blockchain consensus mechanisms ensure consensus with a varying approach. A single reliable consensus mechanism does not exist yet but the existing ones have evolved over time to meet the needs of blockchain technology. Additionally, predicting the type of blockchain consensus mechanism that will be popular and useful in the long run can be increasingly complex as the underlying technology is fairly new. Hence, business leaders who wish to introduce blockchain technology in their organization must be well informed about the various blockchain consensus mechanisms.

TYPES OF BLOCKCHAINS



1.Public or Decentralised Blockchain

Public blockchains are **permission-less in nature**, allow anyone to join, and are **completely decentralised**.  Public blockchains allow all nodes of the blockchain to have equal rights to access the blockchain, create new blocks of data, and validate blocks of data.

To date, public blockchains are primarily used for exchanging and mining cryptocurrency.  You may have heard of popular public blockchains such as **Bitcoin, Ethereum, and Litecoin**.

On these public blockchains, the nodes “mine” for cryptocurrency by creating blocks for the transactions requested on the network by solving cryptographic equations.

In return for this hard work, the miner nodes earn a small amount of cryptocurrency. The miners essentially act as new era bank tellers that formulate a transaction and receive (or “mine”) a fee for their efforts.

**Use cases:**

The most common use case for public blockchains is **mining and exchanging cryptocurrencies** like Bitcoin. However, it can also be used for creating a fixed record with an auditable chain of custody, such as electronic notarization of affidavits and public records of property ownership.

This type of blockchain is ideal for organizations that are built on transparency and trust, such as social support groups or non-governmental organizations. Because of the public nature of the network, private businesses will likely want to steer clear.

2.Private or Centralised (Managed )Blockchains

Private blockchains, which may also be referred to as managed blockchains, are permissioned blockchains controlled by a single organization. In a private blockchain, the central authority determines who can be a node.

The central authority also does not necessarily grant each node with equal rights to perform functions.  Private blockchains are only partially decentralized because public access to these blockchains is restricted.  Some examples of private blockchains are the **business-to-business** virtual currency exchange network **Ripple** and **Hyperledger,** an umbrella project of open-source blockchain applications.

Both private and public blockchains have drawbacks - public blockchains tend to have longer validation times for new data than private blockchains, and private blockchains are more vulnerable to fraud and bad actors. To address these drawbacks, consortium and hybrid blockchains were developed.

**Use cases:**

The speed of private blockchains makes them ideal for cases where the blockchain needs to be cryptographically secure but the controlling entity doesn't want the information to be accessed by the public.

Other use cases for private blockchain include supply chain management, asset ownership and internal voting.

"For example, companies may choose to take advantage of blockchain technology while not giving up their competitive advantage to third parties. They can use private blockchains for trade secret management, for auditing," Godefroy said.

3.Consortium Blockchains

Consortium blockchains are permissioned blockchains governed by a **group of organizations**, rather than one entity, as in the case of the private blockchain.

Consortium blockchains, therefore, enjoy more decentralization than private blockchains, resulting in higher levels of security.  However, setting up consortiums can be a fraught process as it requires cooperation between a number of organizations, which presents logistical challenges as well as potential antitrust risk (which we will examine in an upcoming article).

Further, some members of supply chains may not have the needed technology nor the infrastructure to implement blockchain tools, and those that do may decide the upfront costs are too steep a price to pay to digitize their data and connect to other members of the supply chain.

A popular set of consortium blockchain solutions for the financial services industry and beyond has been developed by the enterprise software firm R3.  In the supply chain sector, **CargoSmart** has developed the Global Shipping Business Network Consortium, a not-for-profit blockchain consortium which aims to digitalize the shipping industry and allow maritime industry operators to work more collaboratively.

**Use cases:**

Banking and payments are two uses for this type of blockchain. Different banks can band together and form a consortium, deciding which nodes will validate the transactions. Research organizations can create a similar model, as can organizations that want to track food. It's ideal for supply chains, particularly food and medicine applications

4. Hybrid Blockchains

Hybrid blockchains are blockchains that are controlled by a single organization, but with a level of oversight performed by the public blockchain, which is required to perform certain transaction validations.  An example of a hybrid blockchain is IBM Food Trust, which was developed to improve efficiency throughout the whole food supply chain.

**Use cases:**

Hybrid blockchain has several strong use cases, including real estate. Companies can use a hybrid blockchain to run systems privately but show certain information, such as listings, to the public. Retail can also streamline its processes with hybrid blockchain, and highly regulated markets like financial services can also see benefits from using it

Medical records can be stored in a hybrid blockchain. The record can't be viewed by random third parties, but users can access their information through a smart contract. Governments could also use it to store citizen data privately but share the information securely between institutions.

STABLECOIN AND PRIVACY COIN

STABLECOIN

With the fluctuation in the price of crypto, the returns one might get back is questionable.

The short -term volatility aspect of bitcoin and other cryptocurrencies makes it even more tough to expect good money and affects its valuation.

Stablecoin provides a solution to this problem. They offer speed and privacy of cryptocurrencies, along with the stability of government issued fiat currency(mostly paper currencies).

TYPES:

1.Fiat-collaterised stablecoins:

Fiat-collateralised stablecoins maintain a fiat currency reserve, like the U.S. dollar, as collateral to issue a suitable number of crypto coins. Other forms of collateral can include precious metals like gold or silver, as well as commodities like oil, but most of the present-day fiat-collateralized stablecoins use dollar reserves.

Such reserves are maintained by independent custodians and are regularly audited for adherence to the necessary compliance. Tether (USDTUSD)and TrueUSD (TUSDUSD) are popular crypto coins that have a value equivalent to that of a single U.S. dollar and are backed by dollar deposits.

2.Crypto-collaterised stablecoins

Crypto-collateralized stablecoins are backed by other cryptocurrencies. Because the reserve cryptocurrency may also be prone to high volatility, such stablecoins are over-collateralized—that is, a larger number of cryptocurrency tokens is maintained as a reserve for issuing a lower number of stablecoins.

For example, $2,000 worth of ether may be held as reserves for issuing $1,000 worth of crypto-backed stablecoins, which accommodates up to 50% of swings in reserve currency (ether). More frequent audits and monitoring add to price stability. Backed by Ethereum (ETHUSD), MakerDAO's DAI (DAIUSD) is pegged against the U.S. dollar and allows for using a basket of crypto assets as a reserve.

3.Non-collaterised stablecoins

Non-collateralized stablecoins don't use any reserve but include a working mechanism, like that of a central bank, to retain a stable price. For instance, the dollar-pegged basecoin uses a consensus mechanism to increase or decrease the supply of tokens on a need basis.

Such actions are similar to a central bank printing banknotes to maintain valuations of the fiat currency. It can be achieved by implementing a smart contract on a decentralized platform that can run in an autonomous manner.

PRIVACY COINS

Privacy coins are cryptocurrencies that obscure transactions on their blockchain to maintain the anonymity of its users and their activity. Participants within a transaction will know the amount transacted and parties involved. However, the same information will be unobtainable to any outside observer.

The anonymity that privacy coins provide offer a potentially appealing outlet for money laundering or other criminal transactions. As such, privacy coins are a point of contention in the ongoing debate around cryptocurrency privacy and regulation.

Privacy coins are altcoins that focus heavily on the security and anonymity of the transactions made through the currency.

HOW Do Privacy coins work???

For cryptocurrencies operating on public blockchains, any recorded transactions will show the sender, the receiver, and the amount exchanged. The two main privacy coins on the market, Zcash and Monero, obscure this information through different methods.

Zcash offers private and transparent transactions. Users can choose between a t-address, which operates like a non-private cryptocurrency address, or a z-address, which will conceal the identity of the seller. These z-addresses operate on zero-knowledge proofs, which validate that the transaction occurred for both sellers and buyers without revealing any information about the transactions.

So in a transaction between two z-addresses, you can identify that a transaction occurred at a certain time on the blockchain, but you don't have any information on who participated in the transaction and how much money was involved.

Monero has several features that, combined, make it very difficult to identify any transaction information on the blockchain. To start, Monero uses stealth addresses, also known as one-time public keys, which dissociates the two accounts participating in a Monero transaction to outside viewers of the blockchain. At the same time, Monero uses ring signatures, which further hides the identity of the sender by mixing their identity with decoy identities. In 2017, Monero implemented RingCT, which obscures transaction amounts.

Legality of privacy coins

The legality of privacy coins vary depending on the country. In the US, privacy coins remain legal. However, the Secret Service recommended that Congress regulate privacy-enhanced cryptocurrencies.

Countries like [South Korea](https://www.bbc.com/news/business-42784384) and Japan have banned trading or holding privacy coins altogether, citing them as a potential outlet for financial crimes such as money laundering or terrorist financing. The Financial Action Task Force (FATF) has similarly [listed the use of privacy coins](https://www.fatf-gafi.org/media/fatf/documents/recommendations/Virtual-Assets-Red-Flag-Indicators.pdf) as a potential red flag for money laundering through virtual assets.

-Sujay L Gowda