# Definition

Blockchain is founded on Distributed-Ledger-Technology (DLT) that ensures trust through consensus between parties in a decentralized peer-to-peer network, in contrast of centralized systems that rely on central authority or third party in order to process, validate and authenticate transactions.

# Properties and Structure

* Every transaction is stored in the shared ledger.
* Transactions are placed in blocks, which are linked in one way hashes.
* Immutable: transaction data cannot be altered or deleted.
* Secure:
* Traceable:

Hash: A hash function is a type of mathematical function which turns data into a fingerprint of that data called a hash. It’s algorithm or formula which takes the input data and turns it into an output of fixed length. A good hash is irreversible, i.e. hard to back-calculate the original data from the hash, and if the input data changes in the slightest, the hash changes in an unpredictable way.

Blocks: transactions are bundled into blocks. Blocks contain a number of transactions and also some other data including the previous block’s hash. As each block includes the previous block’s hash as a part of its data, a chain of blocks is formed. Key points:

* Each block’s hash is derived from the contents of the block.
* Each block refers to the previous block’s hash, not a sequential number
* Data is internally consistent, that is you can run some checks on it, and if the data and hashes don’t match up, there has definitely been some tinkering.

# Blockchain Types:

* Permissionless or Public Blockchain

Permisionless blockchain networks power up most of the market’s digital currencies. They allow every user to create a personal address and begin interacting with the network, by submitting transactions, and hence adding entries to the ledger.

Additionally, all parties have the choice of running a node on the system, or employing the mining protocols to help verify transactions.

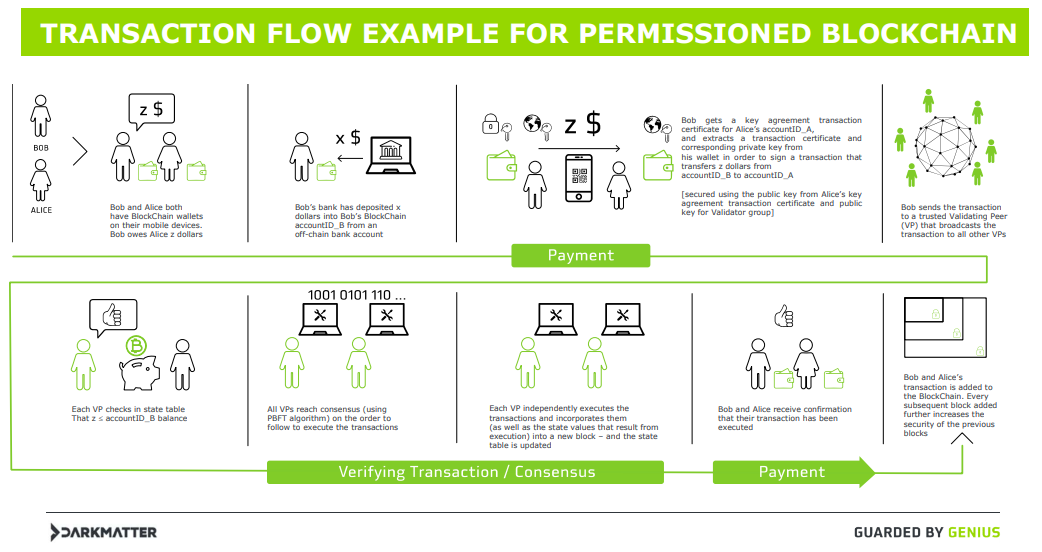
In the case of [Bitcoin](https://blockonomi.com/what-is-bitcoin-ultimate-guide-beginners/), mining is done by solving complex mathematical equations which in return validate the transactions saved on the network – anyone is free to download the bitcoin blockchain and [begin mining operations](https://blockonomi.com/bitcoin-mining-software/), in exchange for mining fees and block rewards.

Additionally, for digital currencies such as [Ethereum](https://blockonomi.com/ethereum-guide/), the blockchain network also supports smart contracts, which are automated transactions that self-execute when certain criteria are met.

As Ethereum also employs a permisionless blockchain, anyone can develop and add smart contracts onto the network, with no limitation imposed by the developers.

Apart from allowing anyone to get involved on the network, there are few more characteristics associated with the permisionless model. These are:

* **Decentralization:** permisionless networks need to be decentralized, which means that no central entity has the authority to edit the ledger, shut down the network, or change its protocols. Many permisionless networks are based on consensus protocols, which means that network changes of any type can be achieved as long as 50% + 1 of the users agree to it.
* **Digital assets**: Another characteristic is the presence of a financial system on the network. Most permisionless networks have some kind of user-incentivising token, which can grow or fall in value depending on the relevancy and state of the blockchain they belong to. Currently, permisionless blockchains employ either monetary or utility tokens, depending on the purpose they serve.
* **Anonymity**: granted the way blockchains operate, anonymity has become quite relevant in the industry. Many permisionless networks do not require users to submit personal information prior to being able to create an address, or submit transactions. However, in certain cases, personal information is required for legal purposes. Bitcoin, for instance, does not offer full anonymity, as user identity is indirectly tied to the addresses they have the private keys of.
* **Transparency:** blockchain networks are bound to be transparent by design. This is a required characteristic, given the fact that users who get involved must be incentivised to trust the network. Therefore, a transparent network needs to freely give users access to all information apart from the private keys – from addresses, to how transactions are processed into blocks, and the freedom to see all transactions processed by the network.
* Permissioned Blockchains: are blockchains where the ledger is maintained in a private and secure walled of participants. Each peer address is discrete and known and access is controlled by a common trust infrastructure of PKI based trust anchors.



Permissioned blockchains act as closed ecosystems, where users are not freely able to join the network, see the recorded history, or issue transactions of their own. Permissioned blockchains are preferred by centralized organizations, which leverage the power of the network for their own, internal business operations.

Company consortiums are also likely to employ private blockchains to securely record transactions, and exchange information between one another.

[XRP](https://blockonomi.com/ripple-price/) is one example of a [semi-permissioned blockchain](https://blocksplain.com/2018/02/07/permissioned-blockchains/), run by Ripple Labs.

With this in mind, private blockchains are run by specific members of consortiums or companies, and members need to opt-in for the creation of such a network.

Additionally, only approved people or computer entities have the possibility of running nodes on the network, validating transaction blocks, issuing transactions, executing smart contracts, or reading the transaction history.

Some of the main characteristics of permissioned blockchains include:

* **Varying decentralization**: members of the blockchain network are free to negotiate and come to a decision concerning the level of decentralization that the network will have. For private blockchain, it is entirely accepted if they are fully centralized or partially decentralized. Some form of central control is required, given the fact that businesses people-managed entities. Additionally, private blockchains are free to choose which consensus algorithms they wish to employ, yet the governance model is more important in this scenario, as power on the network cannot be evenly distributed among all members. This has led to the creation of level tiers of private blockchain users, hence allowing individuals to do only what their job entails them to.
* **Transparency & Anonymity**: private blockchains are not required to be transparent, but they can choose to do so freely, depending on the inner organization of the businesses. In terms of privacy, it isn’t needed on a central level, and can be individually determined on a user-case basis. Many private blockchains store an extensive amount of data relating to the transactions, and operations carried out by users. Lastly, as there is no internal economy for most private blockchains, there is no need to see how monetary tokens are being sent or used.
* **Governance:** for permissioned blockchains, governance is decided by members of the business network – there are numerous dynamics which can determine how decisions are made on a central level, yet there is no need for consensus-based mechanisms, where the entirety of the network must agree to a change.