- Anyone can send transactions through the network; and
- Any individual can read and write relevant data on the blockchain.

Public permissionless blockchains are the closest application of what the blockchain technology was initially designed for by Bitcoin. Cryptocurrencies, and Bitcoin in particular, are the most typical illustration of public permissionless blockchains.

Some public blockchains, however, are permissioned. For example, in the case of the Proof of Stake* protocol – which Ethereum, the second biggest public blockchain, intends to introduce in 2018 – only those meeting certain preconditions can validate transactions based on their "stake" in the blockchain (in particular how many coins he/she has and for how long).

Because of their highly decentralized nature, public blockchains are considered particularly secure and resistant to malicious attacks, with no single point of failure*, but they face issues of scalability (see Section 4.2(a)).

(ii) Private blockchains

In fully private blockchains, the permissions to validate and write data onto the blockchain are controlled by one entity which is highly trusted by the other users, and participants are identified. In some situations, the entity may restrict the read permission to some users. Restricted read permissions provide a greater level of privacy to the users, a feature not available in public blockchains. The entity in control has the power to change the rules of the private blockchain and may decline transactions based on its established rules and regulations.

In a private blockchain, verification of the transactions is carried out by a very restricted number of nodes (according to the rules of the blockchain), which allows for greater efficiency and much faster processing of transactions than public blockchains, while requiring much less computing power. Transaction fees may apply for transaction validation as per the rules of the blockchain.

In addition, given that the validators are known, it is easier for human intervention to fix faulty nodes and risks of a 51 or 99 per cent attack arising from miner collusion do not apply; but the more centralized nature of these networks makes them less resilient to outside attacks, and there is a greater risk of human tampering of data.

The term "Blockchain" in the context of private ledgers is controversial and disputed, as such highly centralized ledgers have little in common with the original idea behind Blockchain.