and incentivized by the chance to earn that blockchain's native currency as a reward when correctly behaving according to the blockchain's protocol and rules. In Proof-of-Stake based blockchains (see box below for a short definition) such as Tezos, participants also can lose part of their stake if they do not follow protocol rules and are accused by another blockchain participant called an "accuser". The accuser then earns this stake for its performed verification work. Each blockchain, whether private or public, needs a control system to ensure participants behave in the correct way according to a blockchain's protocol and rules.

What are open and closed blockchains?

In addition to the definition of public and private, "open" and "closed" are also commonly used terms to describe who can read (i.e. collect and analyze) data on a blockchain. Data stored in an open blockchain can be read by any blockchain participant, whereas in a closed blockchain only a few participants are capable to read data.

Given these two word pairs 'public / private' and 'open / closed', there are four basic characteristics possible to describe a blockchain. Each of these characteristics serves different use cases:

1. Public and Open:

This actually characterizes the type of blockchain people are typically referring to when they speak about public blockchains. Public and open blockchains are available for everybody and written data is accessible and readable by everybody as well. Thus, public and open blockchains support use cases such as public/transparent ledgers where everybody can read and verify data (e.g. account balances of currencies or other assets like in-game assets/trophies or which kind of sport bets have been placed by the blockchain's participants).

Proof-of-Work vs. Proof-of-Stake:

Proof-of-Work (PoW) and Proof-of-Stake (PoS) are two possible methods ("consensus algorithms") to determine which blockchain participant is allowed to add and validate blocks in a blockchain. Participants are financially rewarded for adding and validating blocks to a blockchain. Such rewards typically include a "block reward" plus transaction fees from a block.

For example, PoW is used in Bitcoin and Ethereum and participants have to solve a mathematical "puzzle". Solving this puzzle requires a lot of computational power (hardware and electricity) and the first able to solve the puzzle is allowed to add a new block to the blockchain (a process called "mining"). The difficulty to solve the puzzle is proportional to the total amount of computational power attempting to solve a given puzzle. Since a lot of computational power goes into trying to solve a given puzzle, the Bitcoin blockchain, for instance, was in July 2019 consuming an amount of energy equal to that of Switzerland.[1]

PoS based blockchains do not consume such a massive amount of energy, since the party allowed to add (in Tezos this process is called "baking") or validate a block is determined beforehand. All participants have an opportunity to validate blocks proportional to their tokens ("stake") to bake or validate the next block.

[1] https://www.bbc.com/news/technology-48853230