What are public, and what are private blockchains?

The name says it all – public blockchains are entirely open to the public and accessible to anyone, which means that anyone with an internet connection is allowed to contribute to and interact with a given blockchain. Thus, any person can download a public blockchain's software and run their own node, allowing them to verify its information and/or add new blocks to the blockchain.

Due to being open for anybody's contribution, popular public blockchains such as Bitcoin, Ethereum, and Tezos are composed of thousands of nodes actively contributing to the maintenance of their blockchains. This forms a global and decentralized network of independent nodes where each node communicates with and verifies the work of other nodes instead of a single entity, or a small group of entities, controlling the system.

On the contrary, running nodes in a private blockchain (e.g. Hyperledger and/or R3 Corda) is only possible for parties which have been granted access beforehand. Restricting access to a private blockchain can be achieved via different methods such as authentication through identity management systems or operating a blockchain in an isolated network.

An analogy for public vs. private blockchains is the internet vs. intranets. When commercial computer-use started to gain traction in the 1980s, many enterprises used intranets. Like the internet, an intranet is a network, however, only authorized users are allowed to access it, whereas anyone may access the internet. Over time, far greater innovation took place on the internet and intranet-use fizzled out.

While the terminology in the blockchain industry is still evolving and not widely agreed upon, a synonym for private blockchains is "permissioned blockchains", whereas public blockchains are often called "permissionless blockchains". Private / permissioned blockchains are operated by pre-selected participants such as members of a consortium. This means, the participants in private / permissioned blockchains are known and on- or off-chain controls (such as a regulatory or audit body) are established to validate whether these participants act in good faith. Because all participants are known, misbehaviour, such as including a counterfeit transaction in a block, can be punished (e.g. punishment may be in the form of a previously defined and agreed upon fine).

Since everybody is able to join a public / permissionless blockchain, its participants may be anonymous