What is a public key?

Public-key cryptography (PKC) is a technique that allows users to send and receive data and/or crypto assets over a blockchain network without the need for a third party or trusted intermediary to verify these transactions. Public and private keys are an essential part of the whole idea of decentralisation and the world of crypto, and it is widely used today by nearly all crypto projects in the market.

A public key is what allows a user to receive crypto transactions from another person on the blockchain. It is a cryptographic code that is paired with a private key. While the public key can be used to send funds to anyone on the blockchain, to access it you require the corresponding private key.

It is essentially like a safety deposit box or a bank locker which requires two sets of keys to be unlocked and its content accessed.