Blockchain Council™

Public and Private Key

Public Key

A public key functions on the basis of asymmetric encryption. In this type of encryption, two keys are used - one key is used for encryption and another key is used for decryption.

Security is ensured because only the person with the relevant private key can decode the message. Public key is made available through the public accessible directory.

Public key is derived from Private key using known algorithm.

A shorter representative version of the public key is the address that is used for receiving funds.

Private Key

A private key allows users to access his or her cryptocurrency. Same secret key is used for encryption and decryption.

Private key can take few different forms, depicted as a series of alphanumeric characters, which makes it hard for a hacker to crack.

If a user loses its private key, they can no longer access the wallet to spend, withdraw, or to transfer coins.

The Blockchain wallet dynamically creates private keys for you and stores them. The app signatures the transaction with your private key as you send from a Blockchain wallet (without explicitly revealing it), which signals to the whole network that you have the ability to transfer the funds to the address from which you are sending.

Public Vs Private Key

	Public Key	Private key
Nature	Asymmetrical Encryption	Symmetrical Encryption
Accessible	Available to everyone	Remains in the confidential use of sender and receiver
Speed	Slower	Faster
Generation	Can be generated from private key	Cannot be generated