Public and Private Key

Public Key

- Public key is one of the two keys generated using asymmetric encryption protocols used in blockchain technology.
- Public key which also acts as the address of an account on the blockchain is a fixed length alphanumeric number. Bitcoin's public key is 256 bits long.
- Public key is made using a private key and then broadcasted to the public.
- Public key encryption works such that anyone can encrypt using the public key but only the owner of corresponding private key decrypts the message.
- A shorter representative version of the public key is the address that is used for receiving funds.

Private Key

- A user has a public address and a private key to send and receive transactions. Users can maker transactions to the public address.
- Private key is an alphanumeric string, it is critical to keep the key safe for the safety of crypto tokens.
- Digital wallets are used to store the private keys.
- Transactions use digital signatures to verify the sender. A valid digital signature confirms that the transaction comes from a particular user. Any change in the translation data invalidates the signature.
- Private keys can be stored differently, some method of storage are:
    - Paper wallets,
    - Hardware wallets
    - Cold storage like pen-drives
    - Offline software wallet.
- There are Hot wallets connected to internet which can be used to store the keys online.

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
Role	Used to encrypt data	Used to decrypt data.
Generation	Can be generated from private key	Cannot be generated

Blockchain Council

THANK YOU!

Any Questions?

Visit

community.blockchain-council.org

Mail Us

hello@blockchain-council.org