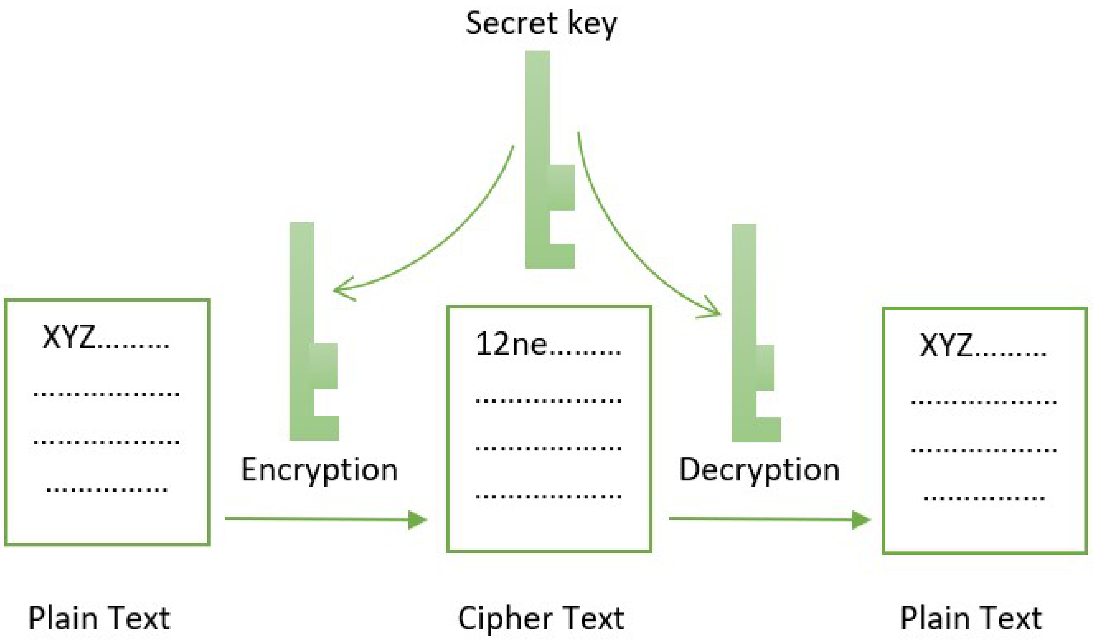
Cryptography in Blockchain

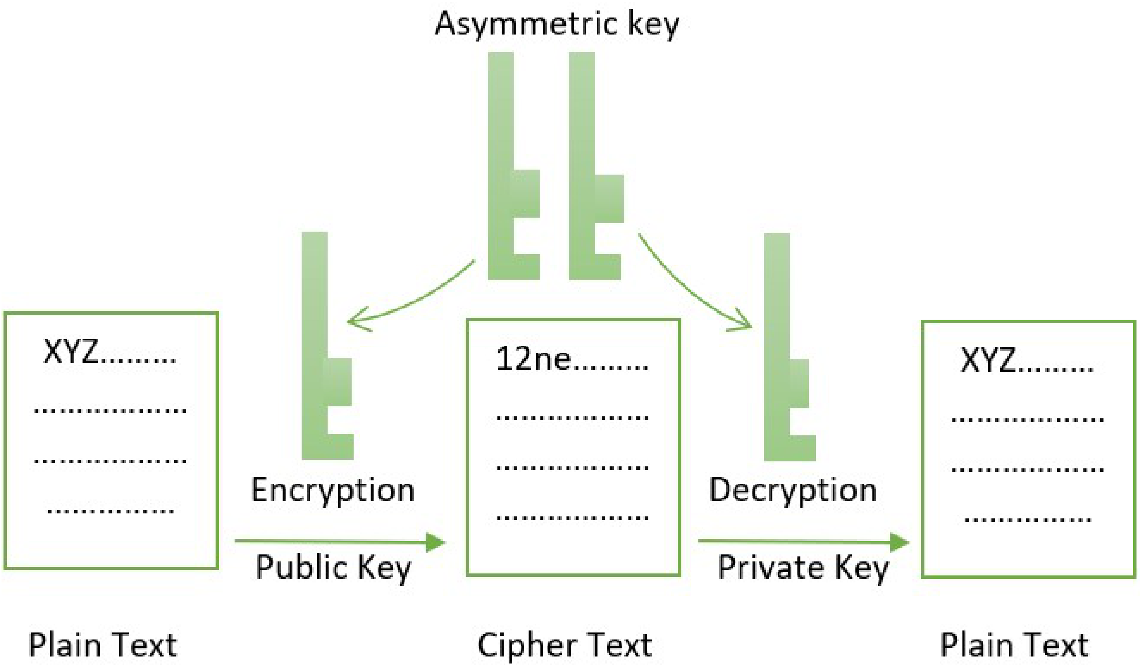
- Cryptography is a technique or a set of protocols that secure information from any third party during a process of communication.
- In a blockchain there are two main concepts cryptography and hashing. Cryptography is used to encrypt messages in a P2P network and hashing is used to secure the block information and the link blocks in a blockchain.
- In the blockchain, cryptography is mainly used to protect user privacy and transaction information and ensure data consistency.

Types of Cryptography

1. Symmetric-key Encryption:
    - It focuses on a similar key for encryption as well as decryption.
    - It is also known as Secret key cryptography.
    - Both parties have the same key to keeping secrets.
    - It is suited for bulk encryptions.
    - It requires less computational power and faster transfer.



2. Asymmetric-key Encryption:
    - This cryptographic method uses different keys for the encryption and decryption process.
    - This encryption method uses public and private key methods.
    - This public key method help completely unknown parties to share information between them like email id.
    - Private key helps to decrypt the messages and it also helps in the verification of the digital signature.
    - It is also known as Public-key cryptography.
    - It requires a long processing time for execution.
    - Plays a significant role in website server authenticity.



Asymmetric key
XYZ.........
Encryption
Public Key
12ne.........
Decryption
Private Key
XYZ.........
Plain Text
Cipher Text
Plain Text