How Blockchain works?

Public and Private Keys

Blockchain implements cryptography using public key infrastructure. A public key is created from a private key. However, it is extremely difficult to create a private key from public key. In this architecture, the sender uses the receiver’s public key to encrypt data and send it to the receiver. The receiver then decrypts the encrypted data using his/her private key. Anyone who intercepts the data will not be able read it because it is encrypted.

Digital signature is used in this Public Key Infrastructure (PKI) to authenticate the sender. The message sent to the receiver is signed by the sender’s private key. When the receiver receives the message, the signature is verified by the receiver using the sender’s public key. If an imposter tries to send data to the receiver, the public key of the authentic sender would detect it.

Nonce

It is a number used only once for specific purpose such as eliminating duplicate transactions. Nonce are used to make every transaction identifier unique.

Hash function

It is a mathematical function used to convert data into encrypted hash vale. Data of any size such as a single string word or hundred string paragraphs will produce the hash value of same size. Hash value is irreversible. It can be used to keep the database size small. Only the value of hash can be stored rather than all the content from which the hash value was created from. Hash value are used as identifier of blocks, addresses and transactions in the Blockchain. SHA-256 is the hash algorithm implemented by Blockchain.

Mining

Miners are computers which expend huge processing power and consumes electricity to generate the desired results. In return, miners are rewarded. The quality of result is directly proportional to the processing power and electricity consumed. This process is called mining. Minors perform significant amount of work to find the nonce which creates the final hash, called the proof of work. This provides integrity by making it hard to add blocks in blockchain.