Public and private keys, how do they work in cryptography and the blockchain:

Public and private keys consist of randomly selected sets of alphanumeric characters, which relate to two cryptographically-generated strings of data safely exchanged between two parties.

The public key is as its name suggests – public - and therefore visible to everyone on the network. It can be shared with others. This key, however, is mathematically related to a private key, which acts as the decoder of the information that the public key secures. One should never share their private key with anyone. Here's how private and public keys work hand-in-hand to keep your data safe.

For example, if John wants to send sensitive information to Christina, to make sure that she alone will be able to read it, he encrypts it with her public key. As only Christina has access to her corresponding private key, she is the only person who will ever be able to decode and read the information coming from John.

Even if someone gets access to the encrypted information by chance or otherwise, it will remain confidential as they don't have Christina's private key. This process is known as public key cryptography and it ensures data confidentiality and security over the Internet.

Another important aspect of public key cryptography is its capability to create digital signature. Digital signatures have the same purpose as handwritten signatures on a paper-based document – to attest to the authenticity and integrity of the data.

Creating digital signatures is a complex mathematical process. However, with the aid of your computer, you won't need to compute anything, your device will do it for you. So, applying a digital signature to a file or email is no more difficult than signing a piece of paper. Here is how it works:

1. Christina signs in to her email application or selects the file that she wishes to digitally sign.
2. Her computer calculates the 'hash' (the hashing function used by Christina's device converts the message into a long string of alphanumeric characters known as 'hash').
3. This hash is encrypted with Christina's private key, which in this case is also the signing key, to create the digital signature.
4. When Christina reverts to John, her original message and her digital signature are sent over to him.
5. John receives the message. It is identified by his computer as being signed, so his email application 'knows' which actions are required to verify it.
6. John's computer device decrypts the digital signature using Christina's public key.
7. John's computer also calculates the hash pertaining to the original message (the mathematical function used by Christina's computer device to create the message and the signature is publicly known).

8. John's device compares the hash it has computed from the received message with the decrypted one it has received from Christina's message.

If the message remains intact during its transit, the two hashes will be identical. However, if the two hashes differ when compared, it means that the integrity of the data transmitted has been compromised. That's when John receives a notification saying that the content of that email or file has been damaged and is therefore unreadable.

That's where digital certificates come into play. These certificates are nothing else than tiny data files ensuring that we're making our public keys available to everyone in a secure and scalable way.

Specifically, digital certificates are used to cryptographically link someone's public key to specific attributes relating to their identity. In the same way that a driver's license or a passport connects a photograph with personal information about its holder, a digital certificate links a public key to information concerning its owner.

Practically, Christina's digital certificate proves that the public key that she uses belongs to her and no one else. Public keys as well as digital certificates contain personal or corporate data used to identify the certificate holder.

But what happens when Christina sends information to John? Upon sending her encrypted information to John along with her digital signature, Christina also sends a digital certificate attached to her message. When John's computer receives the message from Christina, it uses her digital certificate to verify the integrity of the data that Christina has sent. If the verification process is successfully completed, John will have Christina's public key and will be able to verify the validity of the original message signed by Christina.

This is how encryption works and blockchain encryption is no different. Using the SHA256 function (where SHA stands for 'Secure Hash Algorithm') to encrypt, sign, and decrypt the data being transferred with the aid of public and private keys, two computers involved in a wallet-to-wallet exchange will securely transact over the Internet.

All the information relating to crypto transactions is stored in blocks, which are inter-connected to each other, hence the name – blockchain. Every time a new block containing a digital signature is generated, it is broadcast to the network. All the computers (nodes) in the network analyze the validity of the data transmitted by solving complex mathematical problems. This ensures that the information transfer between John and Christina over the blockchain is un-trackable and impossible to decrypt by anyone else apart from them.

However, the verification process differs on a blockchain-by-blockchain basis, depending on the protocol or specific rules for what is a valid transaction or not, or the generation of a valid block. This process can be customized for each blockchain. Rules and incentives may be added as needed when enough nodes reach a consensus on how transactions should be verified.