**Signing Transactions:**

**Demo Link:** <https://andersbrownworth.com/blockchain/public-private-keys/keys>

**Public and Private Keys:**

Understanding the relationship between private and public keys is essential to grasping the concept of blockchain transactions. In essence, a private key is a randomly generated secret key used to sign all transactions.

The private key Is then passed through an algorithm (the \*\*[Elliptic Curve Digital Signature Algorithm]([https://en.wikipedia.org/wiki/Elliptic\_Curve\_Digital\_Signature\_Algorithm)\*\*](https://en.wikipedia.org/wiki/Elliptic_Curve_Digital_Signature_Algorithm)**) for Ethereum and Bitcoin) to create the corresponding public key. Both the private and public keys are central to the transaction process. However, while the private key must remain secret, the public key needs to be accessible to everyone.

When we send a transaction to the blockchain, we’re passing a private key. This allows others to verify the transaction through the generated public key.

**How does Transaction Signing Happen?**

When we sign a transaction on the blockchain, we’re digitally signing some data with our private key. The hashing algorithm used makes it impossible for something to derive your private key from a message signature.

This signing method allows anyone to verify the validity of a transaction by comparing the message signature to a user’s public key!

**Importance of Hiding Private Keys:**

Anyone with access to your private key can perform and sign transactions, on your behalf consequently making it absolutely vital to safeguard private keys.

**Note:** As an interesting side note, wallet addresses, like the one Metamask provided to you, are actually derived from your public key. A public key is passed through the Ethereum Hashing Algorithm, the last 20 bytes of the resulting hash is the address!

**Wrap Up:**

We discovered that transactions on the blockchain are signed using a user’s `private key`. The generated `message signature` can then be verified by anyone through a comparison to a user’s `public key`.

**KEEP YOUR PRIVATE KEY SECURE!:** Private Keys allow someone to sign a transaction, they should be kept secret and secure.

We learnt that `public keys` are generated by using the \*\*[Elliptic Curve Digital Signature Algorithm]([https://en.wikipedia.org/wiki/Elliptic\_Curve\_Digital\_Signature\_Algorithm)\*\*](https://en.wikipedia.org/wiki/Elliptic_Curve_Digital_Signature_Algorithm)**) on a user’s private keys.

In addition to this, Ethereum addresses are derived from public keys by hashing a user’s public keys with the Keccak256 algorithm.

The deeper we go, the more complicated things get, but you’re doing great and we still have a ways to go. In the next lesson we’ll look again at gas and investigate some of the more low level interactions of gas in a blockchain ecosystem.