CoinMetro

INNOVATION POWERED BY CRYPTO

What are Public and Private Keys?

Hi crypto-adventurer! Welcome back to class, we've been waiting for you!

We've covered a lot so far, is your brain bulging yet? You've basically been on fire up to this point and it looks like you're not showing any signs of slowing down. Good on you!

Let's get cracking with today's topic: Public and Private Keys. We'll find out what they are, how they can be used and why you should know about them.

Here it goes...

A Pair of Keys

Did you ever wonder why the word 'crypto' is incorporated into 'cryptocurrency', or 'crypto-asset'? Well, crypto is short for cryptography and this is the basis of the entire concept of blockchain.

Public-key cryptography, or asymmetric cryptography, is actually any cryptographic system that functions by using pairs of keys. There are two types of key in cryptography (hence the pairing), these are *public keys* – which can, as their name suggests, be disseminated widely to anyone and everyone; and *private keys* – which are known only to the person that owns them.

We like to use the concept of email to describe these two very important things...

Think of a public key as your email address. You're not too fussy about who sees it and you're probably quite okay with adding it to your social media, or on a web-form, to allow people to contact you.

Now, think of a private key as your email password. This is NOT something you want to go flashing about. If someone has your email address and your password, they're IN – and that's something you want to avoid at all costs!

That's a super simple way of looking at it, before we get into the subject. Now, let's get some juicy details...

Public Key

When a crypto-enthusiast states their first-ever transaction with a crypto, be it a Bitcoin, Ether, or any other altcoins, a unique pair of keys are generated, as we've already explained. These keys each consist of a long string of alphanumeric characters which are designed to help keep the user's holdings cryptographically secure.

As we've said in our example above, the private key is known only to the user and serves as their **digital ID**. This private key authorizes the user to spend, withdraw, transfer or carry out any other transaction from their account. The public key is generated by a complicated algorithm, applied to the private key and both keys are then stored in a digital wallet.

Remember we talked about Bitcoin's blockchain and how transactions work? Well, when a Bitcoin transaction is executed by person A sending Bitcoin to person B, this transaction is broadcasted to the entire blockchain network, where distributed nodes (i.e. people on their computers) confirm the validity of the transaction before finalizing it and recording it on the blockchain.

...You know all this stuff already. All good?

Before this transaction can be broadcasted, it is digitally signed using person A's **private key**. This digital signature proves ownership of the private key, but – crucially – does not give any other details, or the private key itself, to anyone – this key remains private to person A at all times.

As a **public key** is created from the private key, Person A’s public key is used to *prove* that the digital signature came from their private key. Once the transaction has been verified, the funds are sent to Person B’s public address.

Because the public key is made up of an extremely long string of numbers, it is compressed and shortened to form the **public address** – this is called *hashing*. The private key creates the public key, which then creates the public address. When a transaction commences, Person A and Person B agree to buy/sell crypto, their public addresses are revealed to one another.

The public address is a bit like a bank account number – signifying where the tokens/coins will come from and where they will go to. This is also where our email analogy comes in. Anyone can send you emails to your inbox (private address), but only you can get access to it by inserting your special, unique password (private key). Simple, right?

Once in the public address, Person B is able to re-invest the received tokens/coins on an exchange, like CoinMetro, or withdraw them – using their private key.

Private Key

As we’ve sort of outlined above, a private key controls access to a user’s crypto. It’s like the ultimate password, consisting of a long string of alphanumeric characters. Its main purpose is to ensure security and prevention of unauthorized access to a crypto portfolio.

Private keys are stored inside digital wallets and if a user loses their private key, they will be unable to access their wallet to spend, withdraw, or transfer crypto. Not good. Actually, there are plenty of examples of people who have lost access to their crypto by losing their private key. So, it’s vital that you keep track of it!

Private keys can be stored in a number of ways:

- On paper wallets – documents that have been printed with the private key and a QR code on them so they can be easily scanned when a transaction needs to be signed;
- Inside a hardware wallet – which uses smart cards or USB devices to generate and secure private keys offline;
- In an offline software wallet.

No panic! We’ll go over digital currency storage a little later.

Conclusion

There’s your crash course in public and private keys. They’re not so scary now, hopefully. Thirsty for more? The next lesson of the CoinMetro Crypto Academy will take a look at the crypto markets themselves and why they’re so volatile! Don’t miss it!