Published in WeTrust Blog

Get started Sign In

Search

WeTrustLeonD
Jan 29, 2017 ·
3 min read ·
Listen

Why Do I Need a Public and Private Key on the Blockchain?

Leon Di, Product Marketing @ WeTrust

When someone sends you cryptocoins over the Blockchain, they are actually sending them to a hashed version of what's known as the "Public Key". There is another key which is hidden from them, that is known as the "Private Key." This Private Key is used to derive the Public Key. You can know your own Private Key, and everyone else on the Blockchain knows their own Private Key, but the Private Key should not be shared with outsiders

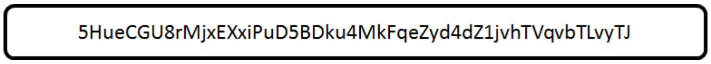
WeTrustLeonD
1.6K Followers
Product Marketing @ WeTrust

Follow

(that is, unless you want your cryptocurrencies to be stolen!).

Both the Private Key and the Public Key are large integer numbers, but since these numbers are so large, they are usually represented using a separate Wallet Import Format (WIF) consisting of letters and numbers.

Sample Private Key in WIF:

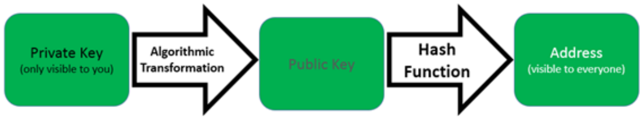


5HueCGU8rMjxEXxiPuD5BDku4MkFqeZyd4dZ1jvhTVqvbTLvyTJ

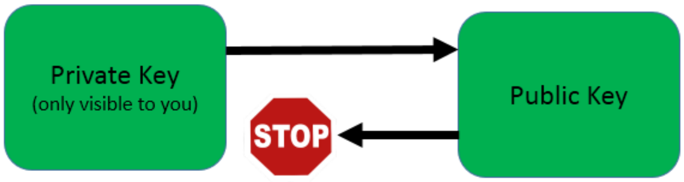
The Private Key is the longer of the two, and is used to generate a signature for each blockchain transaction a user sends out. This signature is used to confirm that the transaction has come from the user, and also prevents the transaction from being altered by anyone once it has been issued. In short, **you sign the cryptocurrencies you send to others using a Private Key**. If someone were to obtain your private key, they would

be able to send your cryptocurrencies to themselves, verifying that transaction with the Private Key — in effect stealing from you!

The Private Key is used to mathematically derive the Public Key, which (along with information about the network and a checksum)is then transformed with a hash function to produce the address that other people can see. **You receive cryptocurrencies that others send to your address (which is a result of the hash of your public key and some additional information).**



At this point, you may be asking yourself, if a Public Key is derived from a Private Key, couldn't someone create a reverse key generator that derives Private Keys from Public Keys, allowing them to steal anyone's coins in the process? Cryptocurrencies solve this issue by using a complicated mathematical algorithm to generate the Public Keys: the algorithm makes it very easy to generate Public Keys from Private Keys, but it is very difficult to "reverse" the algorithm to accomplish the opposite.



At a high level, the algorithm involves converting the Private Key to a binary representation, identifying the bits in this binary representation that have a value of 1, and summing an exponentially multiplied generator variable to arrive at the final public key. As much of a mouthful as that description of public key generation was, the process of reversing the process is even more complex — so much so that the world's most powerful computer would need more than 40000000000000000000000000000000 years (that's 31 zeroes!) to complete this calculation. That's a computer that not even Ali G can think of!

These days, popular cryptocurrency wallets at exchanges such as CoinBase, hardware wallets such as Ledger Nano S, and browser extensions such as MetaMask abstract away the gory details of the public and private key, making it easy to send and receive your favorite cryptocoins!

To learn more about our exciting new project on the blockchain, check out https://www.wetrust.io, and follow the WeTrust blog!

👏 993 | 💬 7