

说到公钥和私钥，相信很多投资者都听说过，尤其是私钥。毕竟私钥决定了存储在数字货币中是否安全，相当于银行卡密码的存在，但是我听说过。真正知道什么是公钥私钥的投资者只有少数，那么什么是公钥私钥呢？下面小编就来详细告诉你什么是公钥和私钥？同时，公钥和私钥有什么区别？



什么是公钥和私钥？

## 1. 私钥

私钥用于加密和解密数据。该密钥在加密敏感信息的发送方和接收方之间共享。私钥，也称为对称，是双方共有的。私钥加密比公钥加密快。

私钥本质上是一个包含64位的随机数：

例如：6kyzdsdo39z3GDRtux2qcowgnnp5ztd7yfr2sc1j239scbnwjee。

私钥是随机生成的，这个随机数可能是2的256次方。你能感受到这个数字。可以说，几乎不可能通过“暴力破解”即使有最先进的量子计算机。

私钥只能由钱包自己生成。创建钱包时，输入密码，即可导出私钥。

注意：钱包地址只有一个私钥。谁拥有私钥，谁就能控制这些数字货币。私钥不能忘记，必须备份。记住！

## 2. 公钥

公钥由私钥通过椭圆曲线加密算法生成。转换后是一个65字节的数组，通常经过十六进制处理后显示。早期的比特币开发者并不知道公钥可以被压缩。压缩的公钥有33个字节数组。有了私钥，你就可以解出公钥。公钥可以；不需要计算私钥，所以数字加密货币具有很高的安全性。

## 公钥和私钥区别的详细说明

### 1. 算法

私钥用于加密和解密数据，在加密数据的发送方和接收方之间共享。公钥只用于加密和解密数据，私钥用于共享。

### 2. 性能

私钥机制更快，公钥机制更慢。

### 3. 秘密

私钥是秘密的，除了发送方和接收方，不向任何人公开。公钥可以免费使用，私钥只能保密。

### 4. Type

私钥机制称为对称，即两方之间的单个密钥，公钥机制称为不对称。，是两把不同用途的钥匙。

### 5. 在共享

中，私钥将在两方之间共享，任何人都可以使用公钥，但私钥只能在两方之间共享。

### 6. 目标

性能测试，检查系统的可靠性。、可扩展性和速度，负载测试来检查系统的可持续性。

那个；什么是公钥和私钥。众所周知，对于私钥和公钥来说，公钥是私钥和地址之间的中间桥梁，其在交易中的验证最为关键。毕竟对于交易的验证，公钥的作用包括生成地址，验证发送交易的地址是否与公钥生成的地址一致，验证私钥的

签名。公钥用于验证交易是否由正确的私钥签名。此外，私钥成对生成公钥。公钥可以生成对应的唯一地址，从而可以确认该地址发送的交易是否使用了对应的私钥

。