关于公钥和私钥的作用是什么和公钥和私钥的作用是什么意义的效果，很多小同伴都是不知道，接下去和软猪手游网汇游网小编往下看公钥和私钥的作用是什么的精细解答吧。

公钥对应的是私钥，这两个是一对。

公钥望文生义，是公开拓布的，主要用于加密音讯。

私钥是自己用的，主要用于解密音讯。

比如路人乙，想给路人甲发一条加密音讯，于是从公开的BBS等下面搜寻到了路人甲公布的公开密钥（公钥），路人乙用这个公钥加密了音讯发给路人甲，路人甲收到这条加密消息后，再用自己的私钥中止解密，就看到了这条消息。他人由于没人路人甲的私钥，收到了信息也看不见外面的方式，所以起到了加密的作用。

梦想生活中，我要给依依转1个比特币，我需求在比特币买卖平台、比特币钱包大约比特币客户端外面，输入我的比特币钱包地址、依依的钱包地址、转出比特币的数量、手续费。然后，我们等十分钟左右，矿工处置完买卖信息之后，这1个比特币就胜利地转给依依了。

这个进程看似很冗杂也很便利，跟我们往常的银行卡转账没什么区别，但是，你知道这个进程是怎样在比特币系统外面完成的吗？它隐藏了哪些原理呢？又大约，它是如何保证买卖可以在一个平安的环境下中止呢？

我们明天就来讲一讲。

关于转出方和接收方来讲，也就是我和依依（我是转出方，依依是接收方）我们都需求出具两个东西：钱包地址、私钥。

我们先说钱包地址。比特币钱包地址其实就相当于银行卡、支付宝账号、微信钱包账号，是比特币支付转账的“凭证”，记载着平台与平台、钱包与钱包、钱包与平台之间的转账信息。

我们在运用银行卡、支付宝、微信转账时都需求密码，才可以支付胜利。那么，在比特币转账中，十分也有这么一个“密码”，这个“密码“被称作“私钥”。掌握了私钥，就掌握了其对应比特币地址上的生杀大权。

“私钥”是属于“非对称加密算法”里面的概念，与之对应的还有另一个概念，名叫：“公钥”。

公钥和私钥，从字面意义我们就可以了解：公钥，是可以地下的；而私钥，是公家的、你自己具有的、需求相对失密的。

公钥是依据私钥计算形成的，比特币系统运用的是椭圆曲线加密算法，来依据私钥计算出公钥。这就使得，公钥和私钥形成了独一对应的联系：当你用了其中一把钥匙加密信息时，只需配对的另一把钥匙才干解密。所以，正是基于这种独一对应的联系，它们可以用来考证信息发送方的身份，还可以做到相对的失密。

我们举个例子讲一下，在非对称加密算法中，公钥和私钥是怎样运作的。

我们知道，公钥是可以对外公开的，那么，一切人都知道我们的公钥。在转账进程中，我不只需确保比特币转给依依，而不会转给他人，还得让依依知道，这些比特币是我转给她的，不是鹿鹿，也不是韭哥。

比特币零碎可以满意我的上述诉求：比特币零碎会把我的买卖信息变短成活动长度的字符串，也就是一段摘要，然后把我的私钥附在这个摘要上，形成一个数字签名。由于数字签名里面隐含了我的私钥信息，所以，数字签名可以证明我的身份。

完成之后，完整的交易信息和数字签名会一同广播给矿工，矿工用我的公钥停止考证、看看我的公钥和我的数字签名能不能婚配上，假定考证胜利，都没效果，那么，就能够说明这个交易确实是我收回的，而且信息没有被更改。

接下去，矿工需求考证，这笔交易破费的比特币能否是“未被破费”的交易。假定考证胜利，则将其放入“未确认交易”，等候被打包；假设考证失利，则该交易会被标志为“有效交易”，不会被打包。

其实，公钥和私钥，冗杂了解就是：既然是加密，那肯定是不希冀别人知道我的消息，所以只能我才干解密，所以可得出：公钥负责加密，私钥负责解密；同理，既然是签名，那肯定是不希冀有人冒充我的身份，只要我才干公布这个数字签名，所以可得出：私钥负责签名，公钥负责验证。

到这里，我们繁杂概括一下下面的方式。下面我们次要讲到这么几个词：私钥、公钥、钱包地址、数字签名，它们之间的联系我们理一下：

（1）私钥是系统随机生成的，公钥是由私钥计算得出的，钱包地址是由公钥计算得出的，也就是：私钥——公钥——钱包地址，这样一个进程；

（2）数字签名，是由交易信息＋私钥信息计算得出的，由于数字签名隐含私钥信息，所以可以证明自己的身份。

私钥、公钥都是密码学范围的，属于“非对称加密”算法中的“椭圆加密算法”，之所以采用这种算法，是为了保证交易的平安，二者的作用在于：

（1）公钥加密，私钥解密：公钥全网公开，我用依依的公钥给信息加密，依依用自己的私钥可以解密；

（2）私钥签名，公钥验证：我给依依发信息，我加上我自己的私钥信息形成数字签名，依依用我的公钥来验证，验证成功就证明确实是我发送的信息。

只不过，在比特币交易中，加密解密啦、验证啦这些都交给矿工了。

至于我们往经常常用的钱包APP，只不过是私钥、钱包地址和其他区块链数据的管理工具而已。钱包又分冷钱包和热钱包，冷钱包是离线的，永世不联网的，一般是以一些实体的方式出现，比如小本子什么的；热钱包是联网的，我们用的钱包APP就属于热钱包。

一、公钥加密

假定一下，我找了两串数字，一串是1*，一串是2*。我喜欢2*这串数字，就保管起来，不通知你们(私钥），然后我通知自己，1*是我的公钥。

我有一个文件，不能让别人看，我就用1*加密了。别人找到了这个文件，但是他不知道2*就是解密的私钥啊，所以他解不开，只要我可以用

串2*，就是我的私钥，来解密。这样我就可以维护数据了。

我的好冤家x用我的公钥1*加密了字符a，加密后成了b，放在网上。别人偷到了这个文件，但是别人解不开，由于别人不知道2*就是我的私钥，

只要我才干解密，解密后就取得a。这样，我们就可以传送加密的数据了。

二、私钥签名

假设我用私钥加密一段数据（当然只要我可以用私钥加密，由于只有我知道2*是我的私钥），结果一切的人都看到我的形式了，由于他们都知

道我的公钥是1*，那么这种加密有什么用途呢？

但是我的好冤家x说有人冒充我给他发信。怎样办呢？我把我要发的信，形式是c，用我的私钥2*，加密，加密后的形式是d，发给x，再通知他

解密看是不是c。他用我的公钥1*解密，发觉果真是c。

这个时分，他会想到，能够用我的公钥解密的数据，肯定是用我的私钥加的密。只有我知道我得私钥，因此他就可以确认确实是我发的东西。

这样我们就能确认发送方身份了。这个进程叫做数字签名。当然精细的进程要稍微冗杂一些。用私钥来加密数据，用途就是数字签名。

总结：公钥和私钥是成对的，它们相互解密。

公钥加密，私钥解密。

私钥数字签名，公钥验证。

公钥和私钥是经过一种算法取得的一个密钥对(即一个公钥和一个私钥)，将其中的一个向外界公开，称为公钥；另一个自己保管，称为私钥。经过这种算法失掉的密钥对能保证逝世界范围内是独一的。运用这个密钥对的时分，假设用其中一个密钥加密一段数据，必需用另一个密钥解密。比如用公钥加密数据就必需用私钥解密，如果用私钥加密也必需用公钥解密，否则解密将不会成功。

上述文章形式就是”公钥和私钥的作用是什么”和”公钥和私钥的作用是什么意义”的精细内容了，希冀有帮到您，更多内容检查软猪手游网百科网。