现实生活中，我要给依依转1个比特币，我需要在比特币交易平台、比特币钱包或者比特币客户端里面，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，矿工处理完交易信息之后，这1个比特币就成功地转给依依了。

这个过程看似很简单也很便捷，跟我们现在的银行卡转账没什么区别，但是，你知道这个过程是怎样在比特币系统里面实现的吗？它隐藏了哪些原理呢？又或者，它是如何保证交易能够在一个安全的环境下进行呢？

我们今天就来讲一讲。

对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）我们都需要出具两个东西：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”，记录着平台与平台、钱包与钱包、钱包与平台之间的转账信息。

我们在使用银行卡、支付宝、微信转账时都需要密码，才能够支付成功。那么，在比特币转账中，同样也有这么一个“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，从字面意思我们就可以理解：公钥，是可以公开的；而私钥，是私人的、你自己拥有的、需要绝对保密的。

公钥是根据私钥计算形成的，比特币系统使用的是椭圆曲线加密算法，来根据私钥计算出公钥。这就使得，公钥和私钥形成了唯一对应的关系：当你用了其中一把钥匙加密信息时，只有配对的另一把钥匙才能解密。所以，正是基于这种唯一对应的关系，它们可以用来验证信息发送方的身份，还可以做到绝对的保密。

我们举个例子讲一下，在非对称加密算法中，公钥和私钥是怎么运作的。

我们知道，公钥是可以对外公开的，那么，所有人都知道我们的公钥。在转账过程中，我不仅要确保比特币转给依依，而不会转给别人，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。

比特币系统可以满足我的上述诉求：比特币系统会把我的交易信息缩短成固定长度的字符串，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。因为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起广播给矿工，矿工用我的公钥进行验证、看看我的公钥和我的数字签名能不能匹配上，如果验证成功，都没问题，那么，就能够说明这个交易确实是我发出的，而且信息没有被更改。

接下来，矿工需要验证，这笔交易花费的比特币是否是“未被花费”的交易。如果验证成功，则将其放入“未确认交易”，等待被打包；如果验证失败，则该交易会被标记为“无效交易”，不会被打包。

其实，公钥和私钥，简单理解就是：既然是加密，那肯定是不希望别人知道我的消息，所以只能我才能解密，所以可得出：公钥负责加密，私钥负责解密；同理，既然是签名，那肯定是不希望有人冒充我的身份，只有我才能发布这个数字签名，所以可得出：私钥负责签名，公钥负责验证。

到这里，我们简单概括一下上面的内容。上面我们主要讲到这么几个词：私钥、公钥、钱包地址、数字签名，它们之间的关系我们理一下：

（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，这样一个过程；

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

私钥、公钥都是密码学范畴的，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，是为了保障交易的安全，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，验证成功就证明的确是我发送的信息。

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。

至于我们现在经常用的钱包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，永远不联网的，一般是以一些实体的形式出现，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。