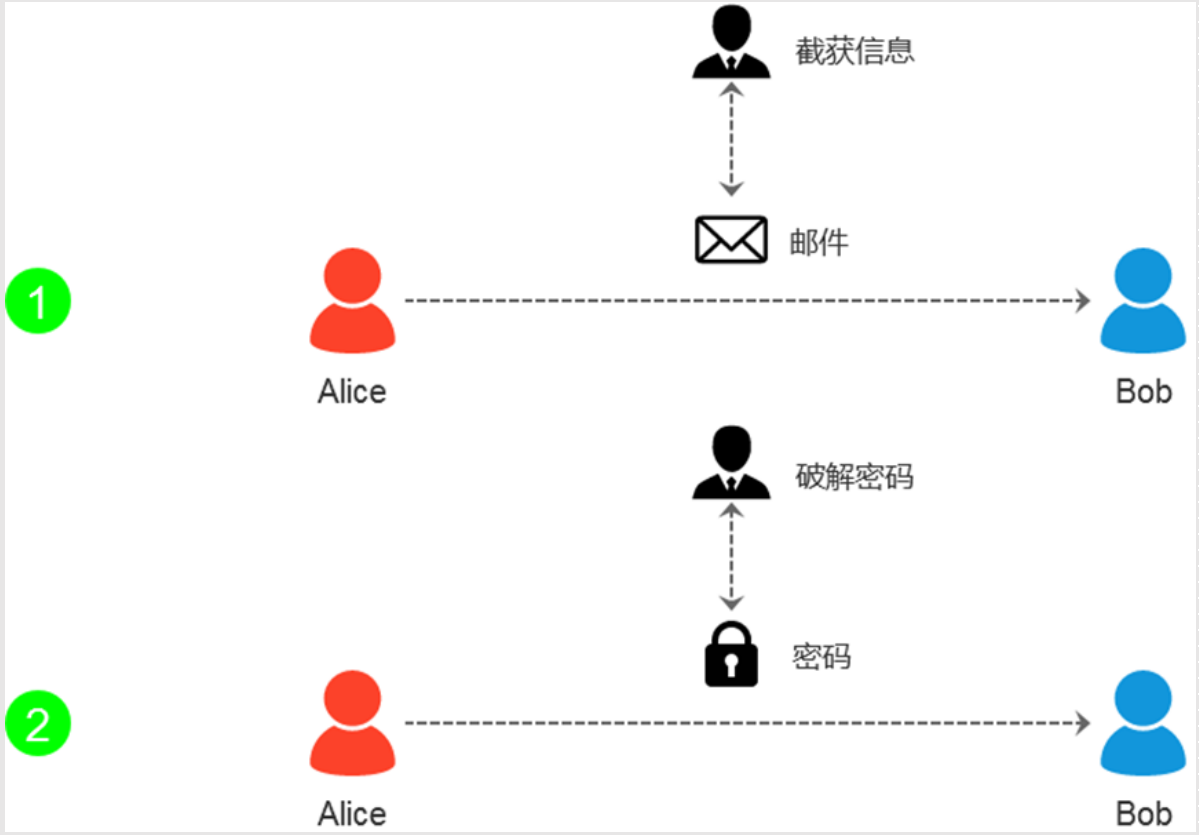
2.3 非对称加密和如何避免记假账

01 为什么要使用非对称加密

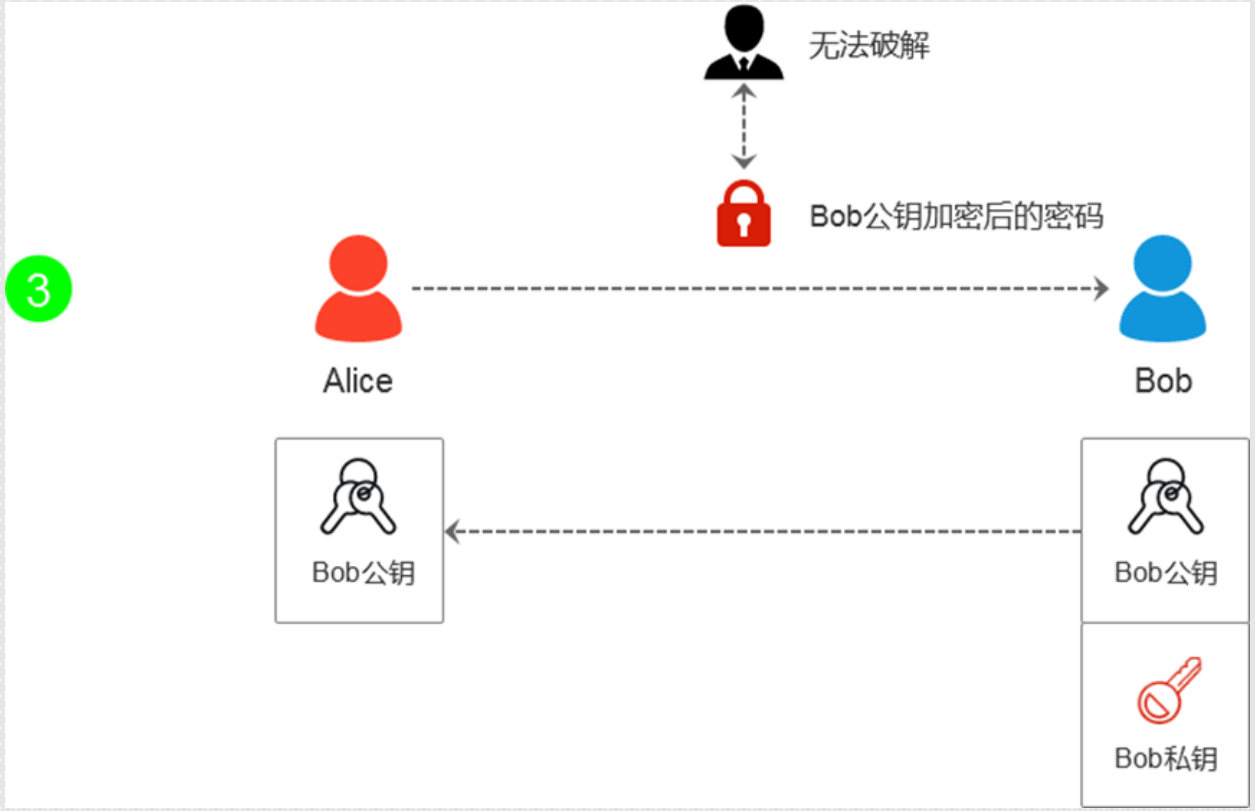


怎么能把加密信息的密码安全传给Bob呢?

02 为什么要使用非对称加密

非对称加密的解决方案

Bob有两把钥匙，一把叫**公钥**，一把叫**私钥**。公钥是公开的让全社会都知道，Bob告诉Alice，你给我发送密码的时候用我的公钥加密以后再传，不用担心这个公钥加密的内容被破解，因为只有我的私钥才能解密（见示意图）。有了非对称加密，分布式电子货币才有了基础，才能解决电子货币所有权的问题。



非对称加密下的信息流通

03 非对称加密的定义

- 什么是非对称加解密算法呢？对称指的是加密和解密使用同一个密钥，称为对称密钥；**那非对称加解密算法在加密和解密时，用的就是不同的密钥，分别称为公钥和私钥。**
- 如果用公开密钥对数据进行加密，只有用对应的私有密钥才能解密；如果用私有密钥对数据进行加密，那么只有用对应的公开密钥才能解密。

04 非对称加密工作原理

1、A要向B发送信息，A和B都要产生一对用于加密和解密的公钥和私钥。

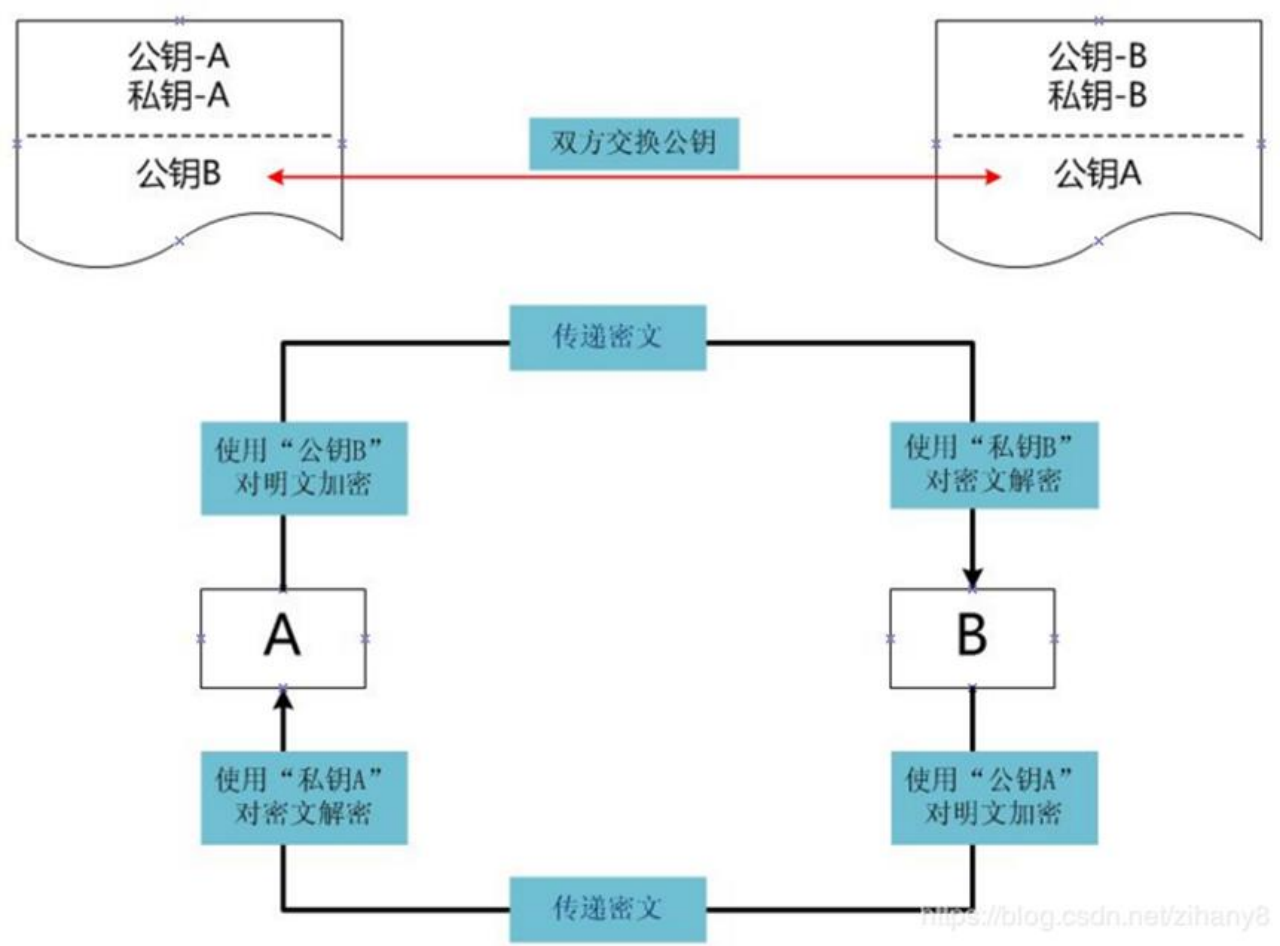
2、A的私钥保密，A的公钥告诉B；B的私钥保密，B的公钥告诉A。

3、A要给B发送信息时，A用B的公钥加密信息，因为A知道B的公钥。

4、A将这个消息发给B（已经用B的公钥加密消息）。

5、B收到这个消息后，B用自己的私钥解密A的消息。其他所有收到这个报文的人都无法解密，因为只有B才有B的私钥。

05 非对称加密工作原理



一句话概括非对称加密算法：公钥加密、私钥解密；私钥签名、公钥验签。

06 非对称加密的应用

- 当使用一个UTXO时，用户要提供这个UTXO中描述的地址对应的公钥、同时用这个公钥对应的私钥对这个交易进行签名，这样比特币的接收者才能去验证这笔交易是否有效。交易验证的环节：把公钥做哈希看哈希值是否与UTXO中描述的地址一致，然后再用提供的公钥对交易中提供的签名信息进行验签，以确定交易是UTXO的所有者发出的交易。在交易的验证环节，我们主要用了“非对称加密”中关于签名、验签的功能。

- **其中比特币中的公私钥生成以及签名算法ECDSA都是基于椭圆曲线算法的。**

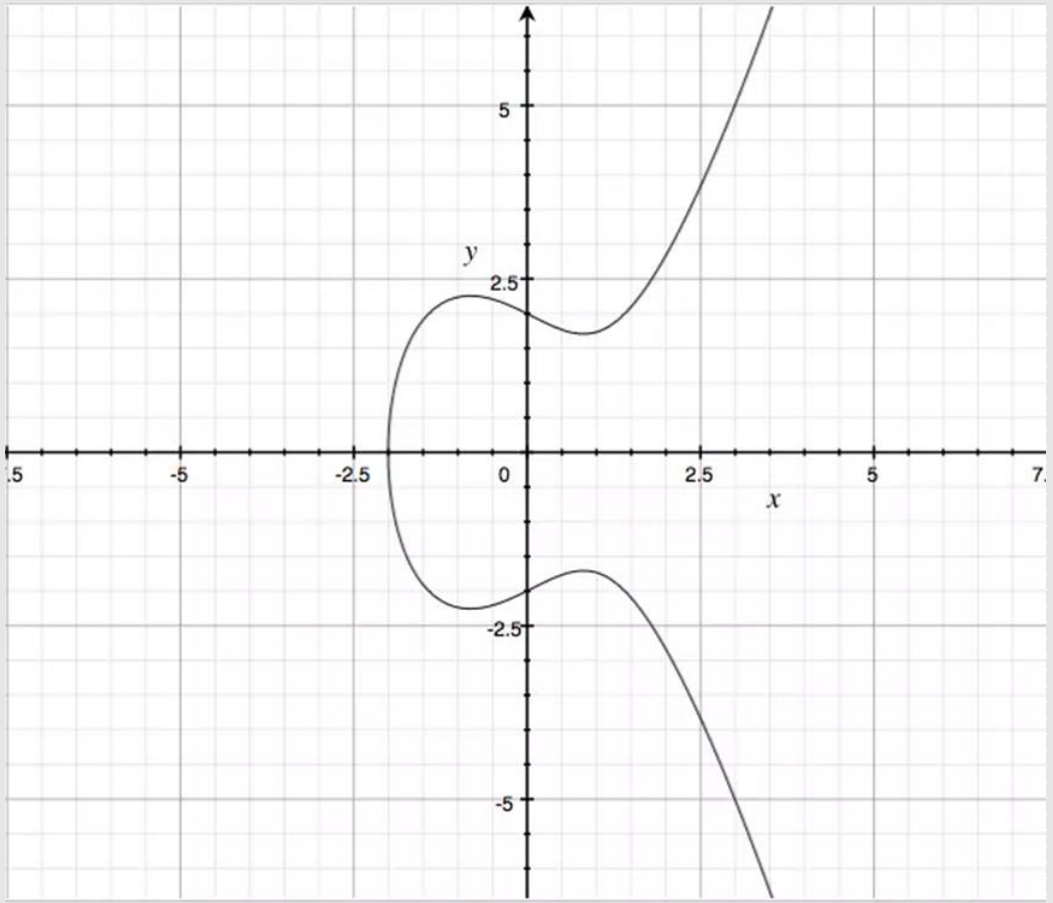
07 非对称加密的应用

椭圆曲线算法

- 椭圆曲线密码学（Elliptic curve cryptography），简称ECC，是一种建立公开密钥加密的算法，也就是非对称加密。类似的还有RSA，ElGamal算法等。ECC被公认为在给定密钥长度下最安全的加密算法。
- 椭圆曲线实际上是一个总称，是一种数学基础算法，不是真正用在密码学上的密码算法。许多非对称加密算法，例如RSA、椭圆曲线，能够被大家认可使用，是因为每种加密算法在数学上都有一个运算，而**这个运算的逆过程被证明是数学难题**。
- 一个椭圆曲线是满足一个特殊方程的点集。一个椭圆曲线方程类似于“y^2=x^3+ax+b”的形式，它的难点在于被广泛承认的解决椭圆曲线离散对数问题的困难性上。

08 非对称加密的应用

椭圆曲线算法



09 如何避免记假账

在比特币交易中有三个保障来避免记假账：

- 首先，用私有密钥对交易信息签名，然后必须用配对的公共密钥验证签名，私用密钥的使用者必须是付款人。
- 其次，被签名的交易信息在网络上进行广播，所有参与到比特币网络的人都可以接收到这笔交易信息，并且可以对交易信息进行验签，确保交易是合法的。
- 最后，接收到交易信息后，大家会按照约定的规则生成区块，就是一个数据块，这个数据块中包括所有的交易明细信息，按照merkle树的方式组装起来。