蚂蚁集团 ANT GROUP | 蚂蚁链 ANTCHAIN

区块链与哈希算法

- 蚂蚁链《区块链系统开发与应用》A认证系列课程

区块链基础/区块链密码技术

课程目录

什么是区块链地址

区块链地址基本概念

- 区块链地址是指区块链网络上的标识，经典的地址生成算法由公私钥产生，具有安全性和隐私性。
- 地址可以绑定数字资产，或者链上有价值的数据。

区块链地址生产原理

- 区块链地址可以由公钥哈希值产生；
- 区块链使用了非对称加密算法中的椭圆曲线算法，通过椭圆曲线算法生成了私钥；
- 然后通过私钥可以生成公钥；
- 为了安全和使用方便，区块链并不是直接使用公钥作为地址使用，而是对公钥再进行一次哈希计算，得出一个新的地址。

02 区块链交易签名

区块链交易原理

区块链交易签名算法

区块链交易过程中的哈希函数使用

区块链交易过程

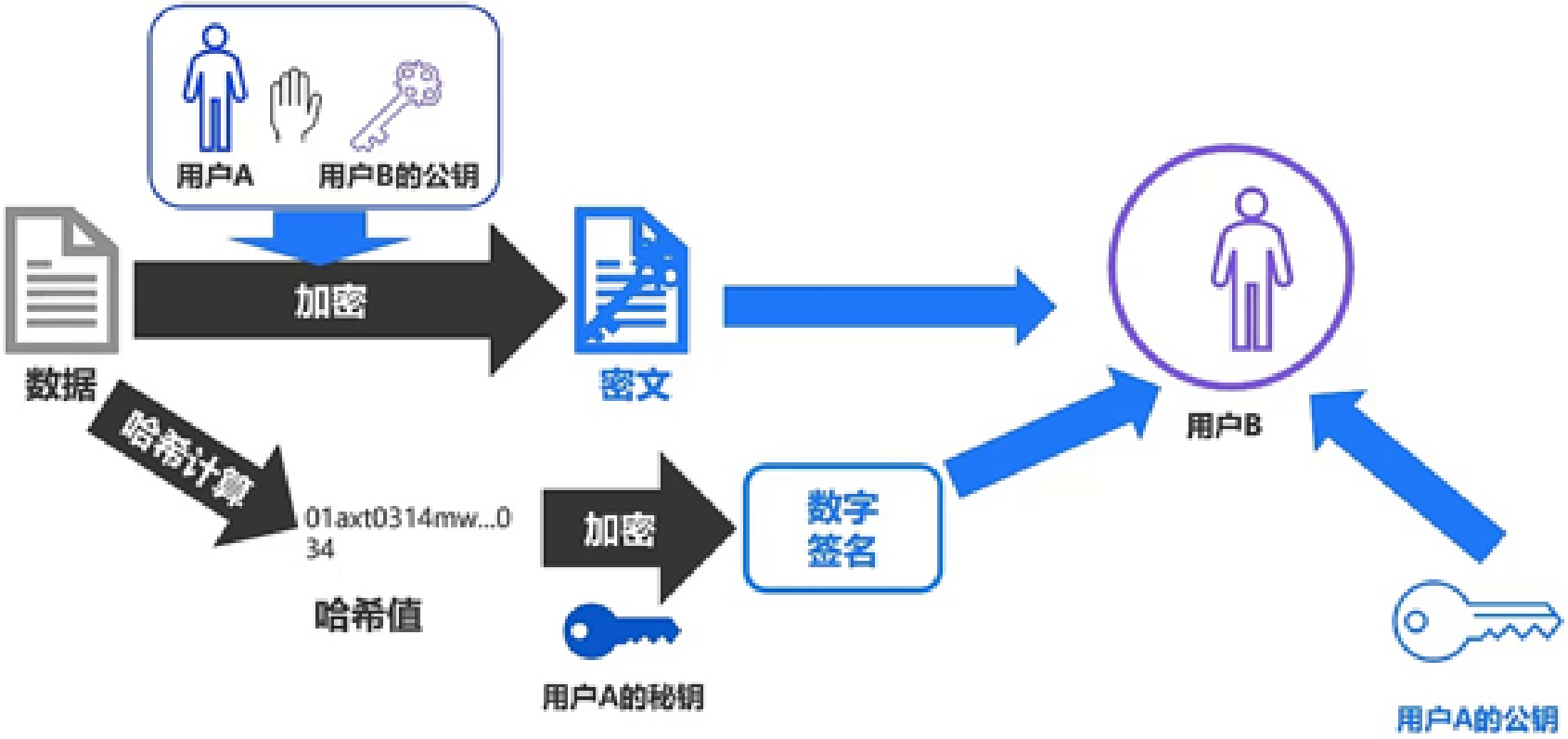
用户A向用户B发送信息

1. 用户A利用私钥对原始数据进行签名
2. 然后利用用户B（全网公开）对1中数据再次进行加工
3. 用户B利用自己私钥解密2中数据
4. 用户B利用用户A的公钥再次验证签名

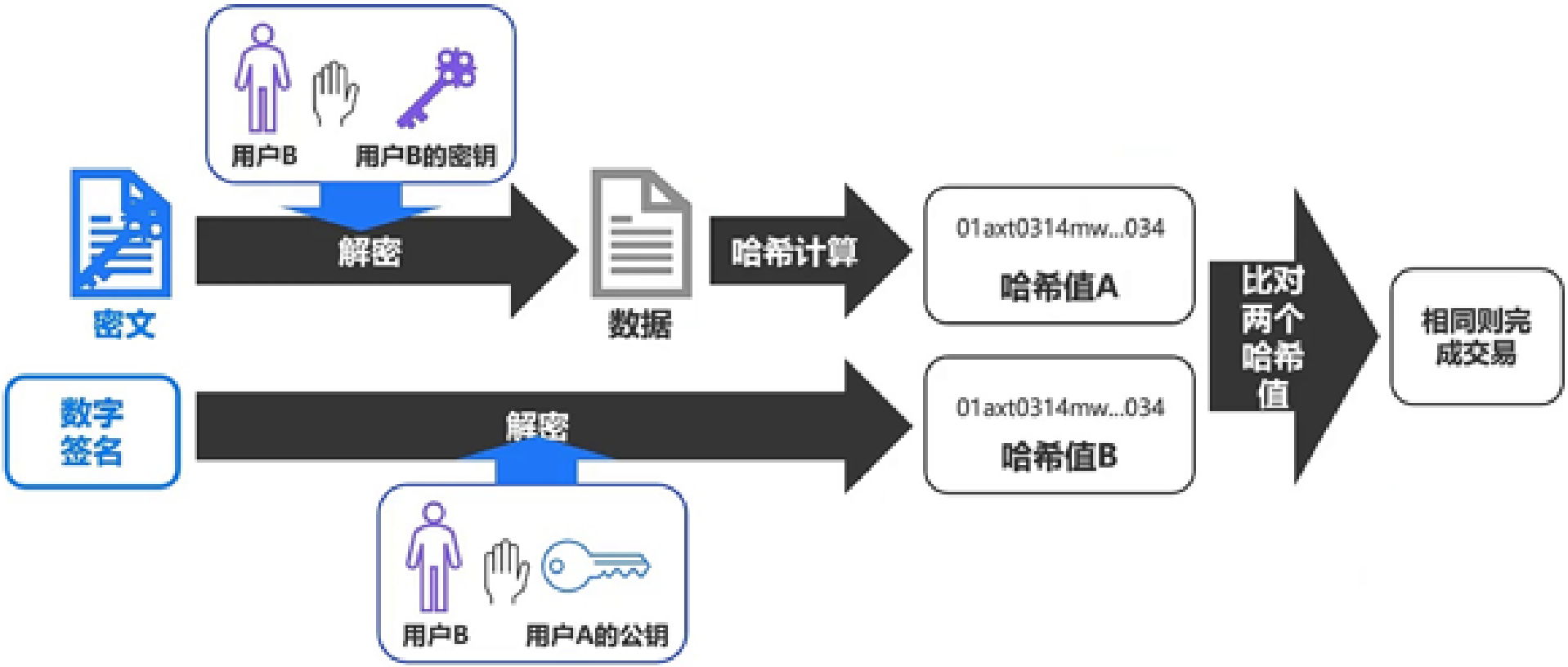
过程分析

1. 用户A利用自己的私钥对原始数据进行数字签名，保证发送者是用户A
2. 用户B利用自己的私钥对接受到数据进行解密，防止数据被篡改

区块链交易过程 · 加密和传输



区块链交易过程·解密和比对确认



区块链交易签名算法

数字签名

- 数字签名是只有信息的发送者才能产生的别人无法伪造的一段数字串，这段数字串同时也是对信息的发送者发送信息真实性的一个有效证明。
- 数字签名主要是用来解决网络环境中的伪造、抵赖、冒充和篡改问题。

ECDSA签名算法

- ECDSA公私钥生成方法是：随机选择一个整数$d < n$,计算$P = dG$，P为公钥，d为私钥
- ECDSA签名算法为$F_Sig = (r, s)$，由一对整数（r,s）组成，其中每个值的长度都与n相同。用m表示需要签名的信息。
- ECDSA签名生成程序如下：
    1. 随机选择一个整数$d' < n$ 作为本次加密的临时私钥，计算 $p' = d'G$。用$x(p')$表示p'的横坐标，计算$r = x(p') \bmod n$。
    2. 对需要的加密信息使用哈希函数SHA-256，得到$z = \text{hash}(m)$
    3. 计算$s = \frac{(z+r\cdot d)}{d'} \bmod n$
    4. （r,s）就是对m的ECDSA签名

签名验证

ECDSA签名的验证

- 用户B为了验证A用户对消息m的签名（r, s），需要A的公钥P
- 第一步：验证r, s在区间$[1, n-1]$中
- 第二步：计算$e = hash(m)$
- 第三步：计算$\omega = s^{-1} \bmod n$
- 第四步：计算$u_1 = e\omega \bmod n$和$u_2 = r\omega \bmod n$
- 第五步：计算$(x, y) = u_1 G + u_2 Q$
- 第六步：判断r是否等于x，如果$r = x$，则接受签名，如果$r \neq x$，则拒绝签名

03 区块链共识机制：POW

区块链共识机制：POW

区块链共识机制 · POW

工作量证明机制——PoW

工作量

- 工作量是对区块头+ 一个随机数数nonce进行两次SHA256的哈希运算
- 当哈希结果的前n位为0的时候（n为难度系数），就认为找到了一个有效的nonce,就可以生成区块并广播给其他的矿工

证明

- 对已知的区块头和随机数nonce进行两次SHA256的哈希运算,验证是否满足前n位为0，满足就是一个有效的区块
- 如果需要伪造交易（修改区块头），需要重新找到一个nonce，需要大量的哈希运算并且需要对后面的所有区块都进行调整，所有计算上是不可能的

04 总结

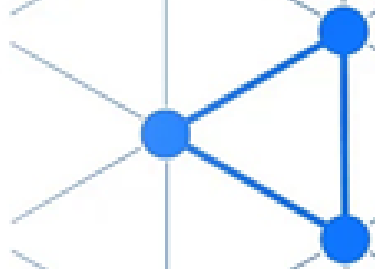
总结

- **区块链地址生成**
  - 通过算法生成私钥，私钥生成公钥，公钥哈希得到区块链地址
- **区块链交易签名**
  - 区块链通过对交易进行数字签名来保证安全性
- **区块链共识机制：POW**
  - POW是工作量证明，需要对区块头+nonce进行两次SHA256的哈希计算，工作量就是寻找一个有效的nonce来满足对应的难度系数，证明就是验证对应的nonce是否有效

总结

- **区块链地址生成**
  - 通过算法生成私钥，私钥生成公钥，公钥哈希得到区块链地址
- **区块链交易签名**
  - 区块链通过对交易进行数字签名来保证安全性
- **区块链共识机制：POW**
  - POW是工作量证明，需要对区块头+nonce进行两次SHA256的哈希计算，工作量就是寻找一个有效的nonce来满足对应的难度系数，证明就是验证对应的nonce是否有效

谢 谢



蚂蚁集团 ANT GROUP | 蚂蚁链 ANTCHAIN