区块链常用术语

- 蚂蚁链《区块链系统开发与应用》A认证系列课程

课程目标

- 了解区块链技术的常用术语

课程目录

01 区块链常用术语

智能合约

协议

双花

共识算法

数字签名

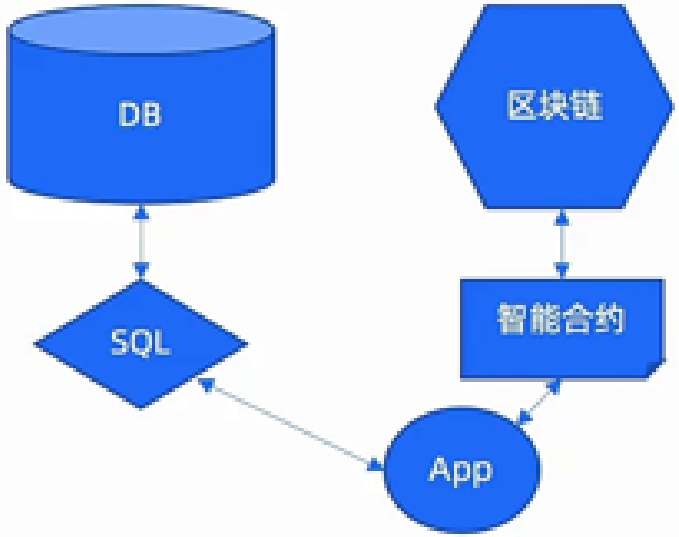
国密算法

区块链常用术语 · 智能合约

工业和信息化部人才交流中心发布的《区块链产业人才岗位能力要求》对智能合约的定义是：

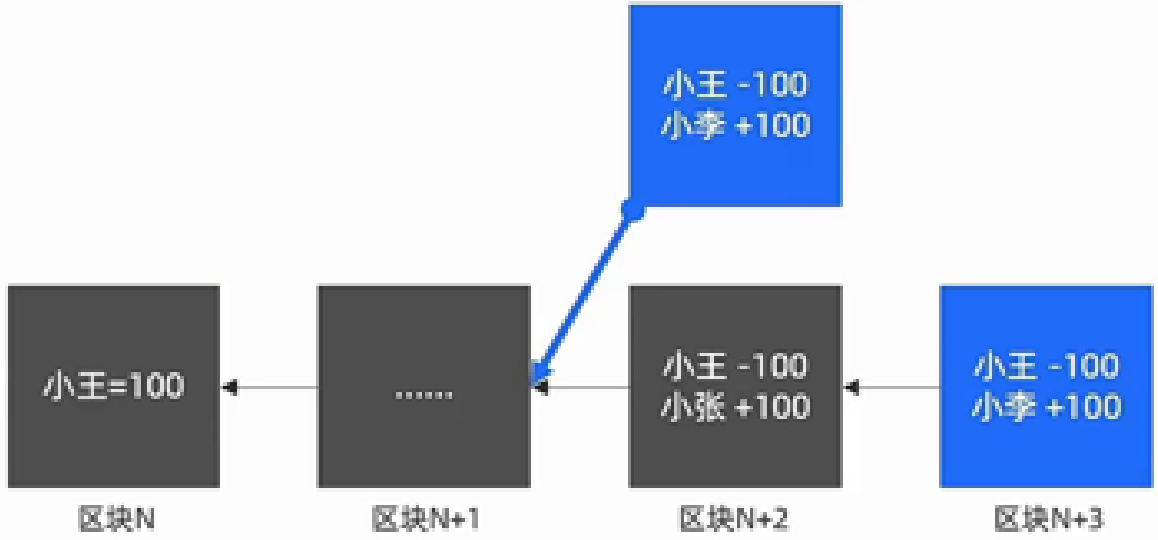
以数字形式定义的能够自动执行条款的合约。

- 智能合约是由尼克萨博（Nick Szabo）于1994年提出的。
- 智能合约之于区块链，相当于SQL之于数据库。



区块链常用术语 · 双花

- 双花即双花攻击，顾名思义也就是把一笔资金花出去2次或多次。
- 双花攻击想要成功，一定要分叉。
- 双花攻击想要成功，一定要算力或资金足够强大。



51%攻击

51%攻击（Majority Attack），就是说在整个网络中有人的算力超过了全网的50%。那么他就可以尝试对区块链的状态进行修改，进行反向交易，实现双花。

“信任危机”

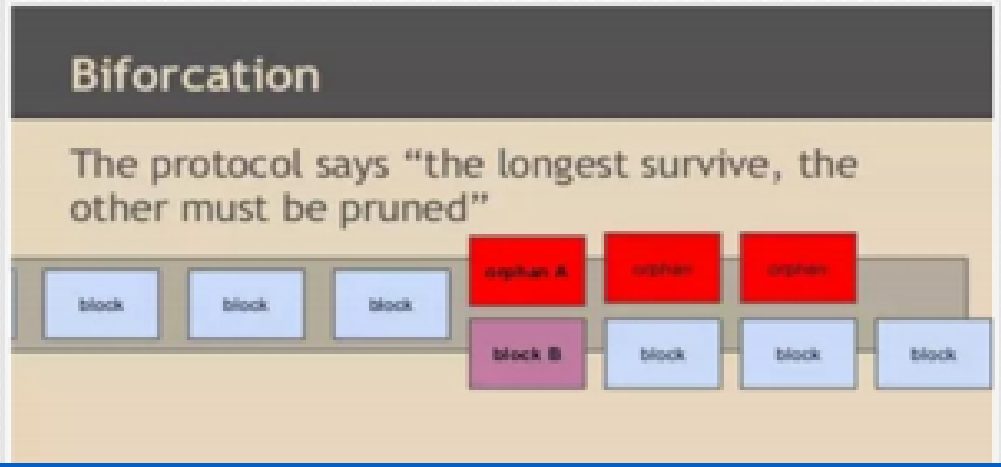
51%攻击

我们设想，Alice现在控制了比特币网络上51%以上的算力，在控制算力的期间，她把一定数量的比特币发给自己在交易所的钱包，这条分支我们命名为分支A。同时，她又把这些比特币发给另一个自己控制的钱包，这条分支我们命名为分支B。分支A上的交易被确认后，她立马卖掉这些比特币，成功套现。

这时候，分支A成为主链。然后，Alice在分支B上进行挖矿，因为她控制了全网50%以上的算力，所以有很大的几率获得记账权，于是很快，分支B的长度就超过了分支A的长度，那么分支B就会成为主链，分支A上的交易就会被回滚。所谓回滚，指的是程序或数据处理错误，将程序或数据恢复到上一次正确状态的行为。

51%攻击

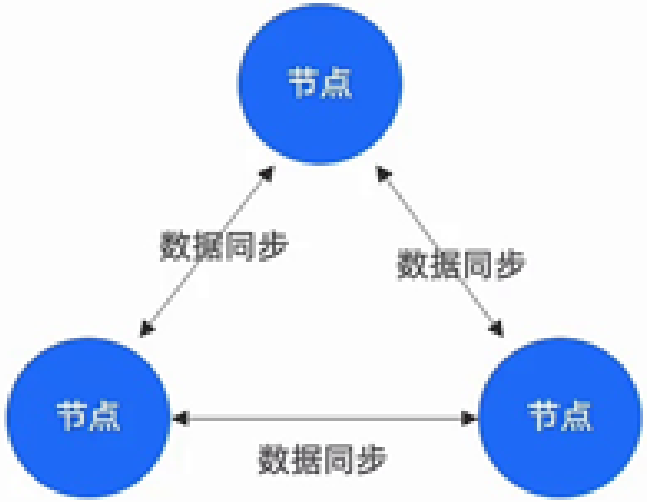
这时候，由于交易回滚，分支A恢复到Alice发起第一笔交易之前的状态，所以她之前换成现金的那些比特币又回到了自己手里。于是这些比特币就成为了交易所的损失。最后，Alice把这些比特币发到自己的另一个钱包。就这样，她凭借51%以上的算力控制，实现了同一笔token的“双花”。



区块链常用术语 · 共识算法

工业和信息化部人才交流中心发布的《区块链产业人才岗位能力要求》对共识算法的定义是：

区块链系统中各分布节点对事务或状态的验证、记录、修改等行为达成一致确认的方法。



区块链常用术语 · 签名

国标《信息技术区块链和分布式记账技术参考架构》（征求意见稿）数字签名的定义是：

附加在数据单元上的数据，或是对数据单元所作的密码变换，这种数据或变换允许数据单元的接收者用以确认数据单元的来源和完整性，并保护数据防止被人(例如接收者)伪造或抵赖。

数字签名是现实社会中的签名（sign）和盖章这样的行为在数字世界中的实现。

区块链中的签名指基于 PKI体系（公钥基础设施）或区块链公私钥的数字签名。

区块链常用术语 · 加密算法

国标《信息技术区块链和分布式记账技术参考架构》（征求意见稿）对加密的定义是：

对数据进行密码变换以产生密文的过程。一般包含一个变换集合，该变换使用一套算法和一套输入参量。输入参量通常被称为密钥。

加密算法可以分为对称加密算法和非对称加密算法。

常见的非对称加密算法	常见的对称加密算法
RSA 、Elgamal 、ECC	AES、DES、3DES

区块链常用术语 · 国密算法

国密即国家密码局认定的国产密码算法。

主要国密算法：

- SM1对称加密
- SM2非对称加密
- SM3消息摘要算法
- SM4 无线局域网标准的分组数据方法

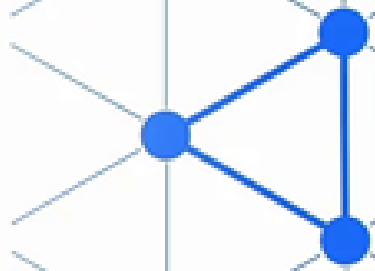
02 总结

总结

■ 常用术语

- 智能合约
- 协议
- 双花
- 共识算法
- 数字签名
- 国密算法

谢 谢



蚂蚁集团 ANT GROUP | 蚂蚁链 ANTCHAIN