蚂蚁集团 ANT GROUP | 蚂蚁链 ANTCHAIN

跨链机制

- 蚂蚁链《区块链系统开发与应用》A认证系列课程

课程目标

- 了解中继
- 了解哈希时间锁定机制

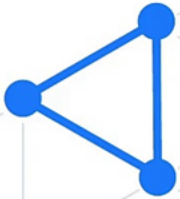
课程目录

01 中继

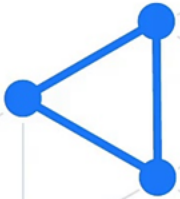
02 哈希时间锁定协议

03 总结

01 中继



01 中继



中继模式本质上是公证人和侧链机制的融合和扩展。

侧链是指与主区块链平行的“区块链”。具有以下三个特征：

侧链是相对的

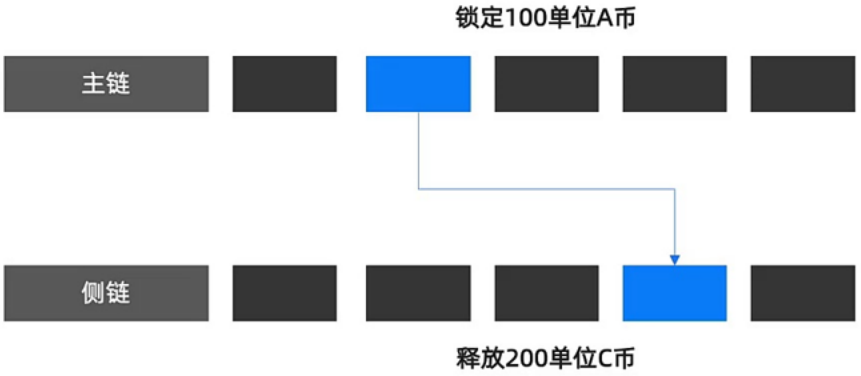
侧链与主链是独立的

侧链与主链可以连接互通，即跨链

1、相对概念：要说谁是谁的侧链；
2、侧链需要知道主链的存在，主链不需要知道侧链的存在；
3、在侧链完成隐私保护、智能合约等新功能；侧链：更安全的协议升级方式，提升协议的安全机制；
4、跨链时，才执行

侧链跨链的基本机制——双向锚定(Two-Way Pegging)

在锁定主链数字货币的同时，将等价的侧链数字货币进行释放。根据锁定和释放的模式，即交易验证，又可以划分为以下几类：单一托管模式、联盟模式、SPV模式、驱动链模式。



双向锚定示意图

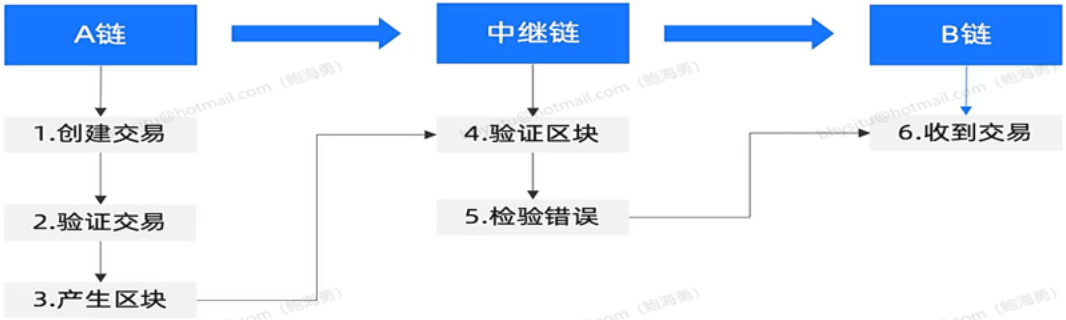
侧链跨链交易验证模式

交易验证模式简介。

交易验证模式	简介
单一托管模式	在主链上指定一个托管方（比如交易所）来锁定和释放数字货币
联盟模式	多个托管中心共同确认锁定和释放数字货币
SPV模式	通过SPV算法进行管理数字货币释放与锁定活动
驱动链模式	节点通过投票方式何时解锁数字资产以及将解锁的数字资产发送到何处

通过对侧链知识的介绍，这里可以将中继链看作是为跨链交易验证而设计的区块链。

Polkadot是由原以太坊主要核心开发者推出的公有链。



1、2个平台：Polkadot和CosMos

2、Polkadot：原以太坊核心开发者，解决当前的2大问题：扩展性和延伸性；计划将私有链和联盟链融入到有公有链的共识网络中，同时又能保证私有链和联盟链的原有数据隐私，跨区块使用的特性

Cosmos是Tendermint团队推出的一个支持跨链交互的异构网络。其机制如下

Zone110个单位数字货币转账

1、类似于拜占庭容错、共识引擎；高性能、高一致性；严格的分叉责任制保证，能防止恶意的参与者进行不当操作

2、A向B转账10个跨链代币为例

02 哈希时间锁定协议

哈希时间锁定协议

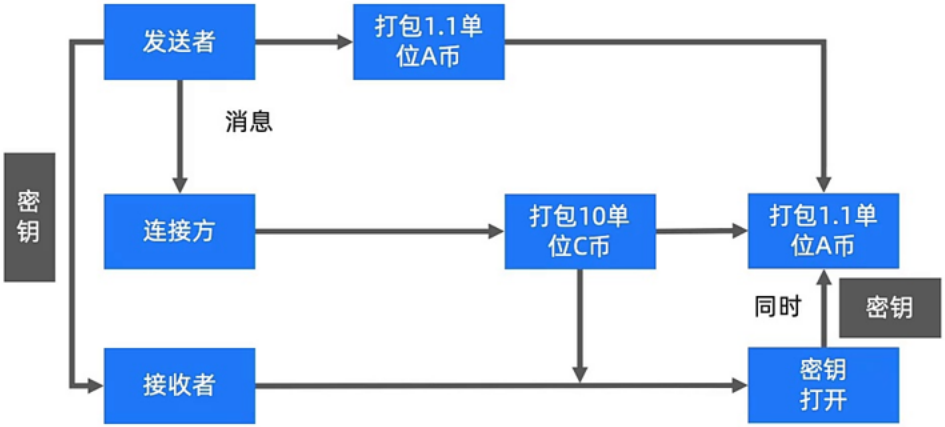
哈希时间锁定协议（Hashed-Timelock Agreements, HTLAs），是哈希锁定合约的泛化，主要目的在于适应跨链交易。

在哈希时间锁定协议中，

- 只需发送者、连接方、接受者三方，即可实现代币的交易，期间不需要任何交易所平台；
- 且在交易失败时，代币并未发生实际转移，不需支付额外的交易费用。

哈希时间锁定协议——基本原理

以小王以1单位A币交换小李价值10个单位C币服务为例。



03 总结

总结

- **中继模式本质上是公证人和侧链机制的融合和扩展**
  - 侧链通过双向锚定实现跨链
  - 单一托管模式，联盟模式，SPV模式三种具体的模式
  - 中继目前落地的项目有Polkadot、Cosmos平台

- **哈希时间锁定协议是哈希锁定合约泛化**
  - 无需交易平台，发送者、连接方、接受者三方，即可实现代币的交易

谢 谢

蚂蚁集团 ANT GROUP | 蚂蚁链 ANTCHAIN