蚂蚁集团 ANT GROUP | 蚂蚁链 ANTCHAIN

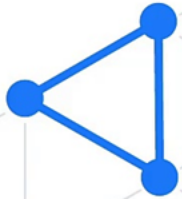
跨链概述

- 蚂蚁链《区块链系统开发与应用》A认证系列课程

课程目标

- 了解跨链定义
- 了解跨链分类
- 了解公证人机制

01 跨链定义



预备知识——互操作性

2020年世界经济论坛与德勤合作发布了一份关于“供应链区块链的包容性部署——区块链互操作性框架”的报告。

- 区块链的互操作性非常重要。
- 区块链的互操作性支持多种功能。
- 区块链的互操作性支持钱包兼容。

互操作性

- 区块链交换和利用数据的能力；
- 在两个或多个区块链之间移动数字资产的能力。

为什么互操作性重要？？？

如何实现互操作性——跨链技术

1、区块链先驱：去中心化的统一支付系统；当前：信息和应用孤岛；
2、多代币数字钱包的发展，区块链互操作性----->多代币交易，依靠单个钱包，轻松实现跨区块链存储和交易（转移）代币

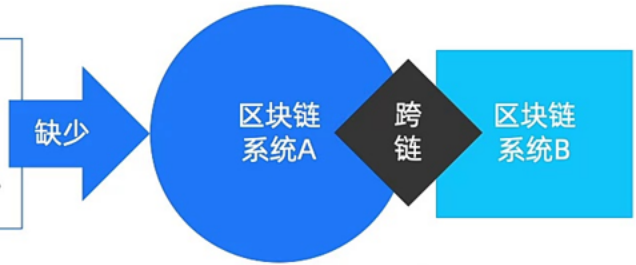
跨链定义

跨链是指在实现不同区块链网络之间的价值和信息传输的协议或者技术。

互操作性

- 区块链交换和利用数据的能力；
- 在两个或多个区块链之间移动数字资产的能力。

缺少



跨链示意图

实践案例

Ripple、Polkadot blockchain、Blocknet、Aion Online、Wanchain等。

Ripple，虽然是初期，但已经支持世界各地的银行，跨链结算

02 跨链分类

跨链分类

从技术角度，我们可以根据“交易如何确认”，“在哪确认”，以及“由谁来确认”等不同的方案，将该过程概括为三种实现方式：

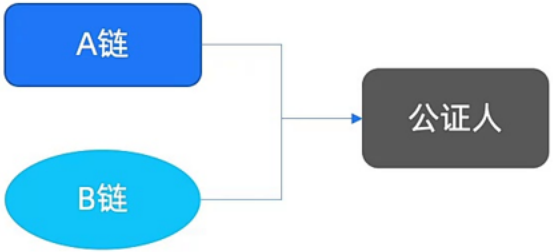
- 公证人机制（Notary Schemes）
- 侧链/中继（Sidechains/Relays）
- 哈希锁定（Hash-locking）

几种可能的跨链应用场景包括资产交换、原子交易、预言机、信息互通等。这里可以参考2016年Buterin的一篇综述性文章《Chain Interoperability》。

Buterin:以太坊创始人

公证人机制

公证人机制是一种简单的跨链机制，在这种公证制度中，一个或者一组受信任的实体充当第三方，主动或者被动进行交易确认和验证。



公证人机制——分类

- **单签名公证人机制**

  一个节点做公证人 速度快、安全性低、非中心化

- **多签名公证人机制**

  多个节点利用签名机制做公证人组 安全性高

- **分布式签名公证人机制**

  多个公证人，通过随机方式产生 安全性高，灵活

公证人机制未能很好解决中心化问题。

实现跨链交易的确认和验证

1、单签名公证人：依赖于中心节点的安全性、稳定性

2、多签名公证人：达到一定的公证人签名数量比例，才能实现跨链交易；依赖于联盟；少数公证人被攻击也不会受影响

3、分布式：基于密码学，生成密钥，拆分成多个碎片，发给随机抽取的公证人，当一定比例的公证人共同签名后即可拼接出完整的密钥；门限性，容错性

04 总结

总结

- **跨链是实现不同区块链系统互操作性的技术**
  - 包括公证人机制、侧链/中继、哈希锁定

- **公证人机制中一个或者一组受信任的实体充当第三方，实现跨链**
  - 包括单签公证人、多重签名公证人、分布式签名公证人机制

谢 谢

蚂蚁集团 ANT GROUP | 蚂蚁链 ANTCHAIN