区块链

笔记本: 区块链
创建时间: 2019/9/24 14:38 **更新时间:** 2019/10/15 22:31
作者: jyyhermance@163.com
URL: https://ethfans.org/wikis/%E4%BB%A5%E5%A4%AA%E5%9D%8A%E7%99%BD...

区块链系统基本结构

- 区块链账本
- 共识机制：通过公式算法让各节点账本数据达成一致
- 密码算法：区块哈希，事务哈希（梅克尔树结构）
- 脚本系统： 一组程序规则，驱动区块链系统进行数据的收发
- 网络路由： 各个节点连接，进行通信

典型演化场景

场景	功能	智能合约	一致性	权限	类型	性能	编程语言	代表
数字货币	记账功能	不带有或较弱	PoW	无	公有链	较低	简单脚本	比特币网络
分布式应用引擎	智能合约	图灵完备	PoW、PoS	无	公有链	受限	特定语言	以太坊网络
带权限的分布式账本	商业处理	多种语言，图灵完备	包括 CFT、BFT 在内的多种机制，可插拔	支持	联盟链	可扩展	高级编程语言	超级账本

分类

按参与者分类

- 公有链（面临挑战和风险过大
- 联盟链（多组织合作，引入权限管理机制，主要落地应用
- 私有链（和传统的中心式记账差异不明显

按应用场景分类

货币链，产权链，众筹链，通用链

问题与挑战

隐私保护

医疗健康领域需求最为强烈，零知识证明，同态加密等密码学手段在实际应用中还存在问题

分布式共识

基于概率的算法：pow, pos, dpos等，用于公有链，考虑最坏情况，安全性高但效率低，浪费能源

确定性算法：PBFT等，适于带权限管理的场景

共识问题核心指标包括：容错的节点比例、决策收敛速度、出错后的恢复、动态特性等

交易性能

区块链不适于高频交易

提升交易性能：吞吐量，确认延迟

方法：提升单个节点性能（硬件和算法优化）；交易处理卸载到链下，区块链只记录最终交易信息（比特币闪电网络）

扩展性

单个节点要求处理能力很高

联盟链：核心节点+访问节点？多层处理结构分散交易

跨链需求

安全防护

网络安全（认证、过滤、攻防）、信息安全（密码配置、密钥管理）、管理安全（审计、风险分析控制）

代码漏洞管理

交易匿名化 --> 仍然存在被破解的风险

公有链缺乏治理和调整机制

数据库和存储系统

LevelDB、RocksDB 等键值数据库，具备很高的随机写和顺序读、写性能，以及相对较差的随机读的性能

缺乏针对区块链这种新型数据业务的数据库

互操作和运营治理

企业已有系统和区块链系统如何共存

运营管理往往摆脱不了中心化