

当大数据遇到区块链——可扩展的底层区块链架构

宁志伟

秘猿科技

商业基于大数据

➤ 处理能力要求高

- 2017 年双 11 支付宝峰值每秒 25.6 万笔交易

➤ 数据量大

- 阿里每天产生 TB 级别的日志

区块链的扩展性难题

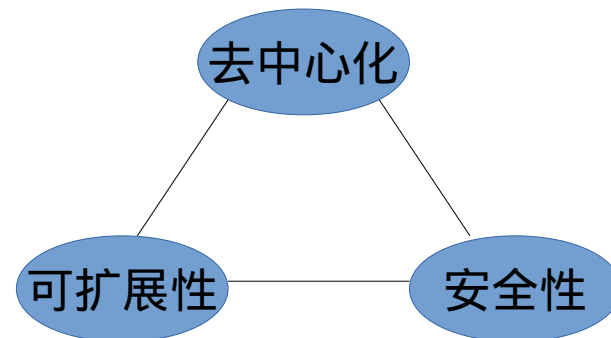
➤ Scalability

- Scale Up(纵向扩展)
- Scale Out(横向扩展)

➤ 消息复杂度 $POW \sim O(n)$ $PBFT \sim O(n^2)$

➤ Scalability Trilemma

- Decentralization
- Scalability
- Security



一些解决方案

➤ 多链 / 分片 / 侧链

- ✓ Decentralization

- ✗ Security

➤ 大区块 / 联合挖矿 / 超级节点

- ✓ Security

- ✗ Decentralization

区块链的数据量问题

➤ 主流区块链项目的数据量

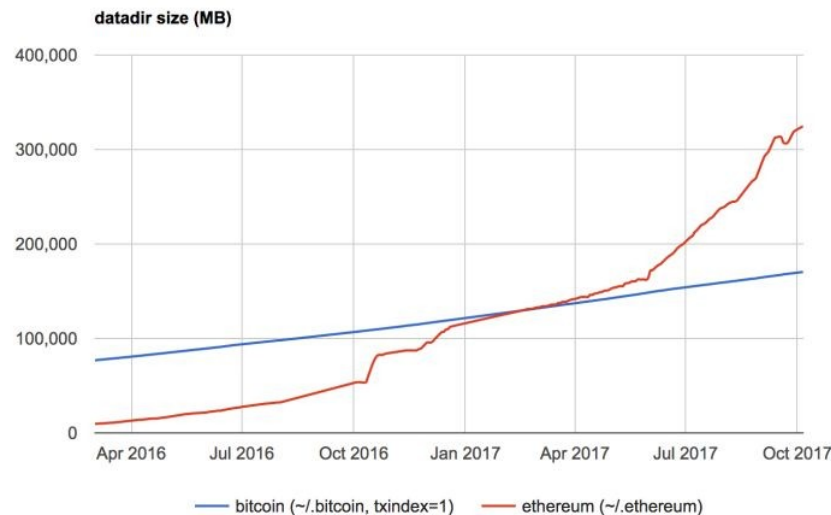
- 比特币 将近 200G
- 以太坊 超过 1T

➤ 特点

- 每个节点都要存储一份
- 一直增长

➤ 问题

- 同步难
- 随机读性能差



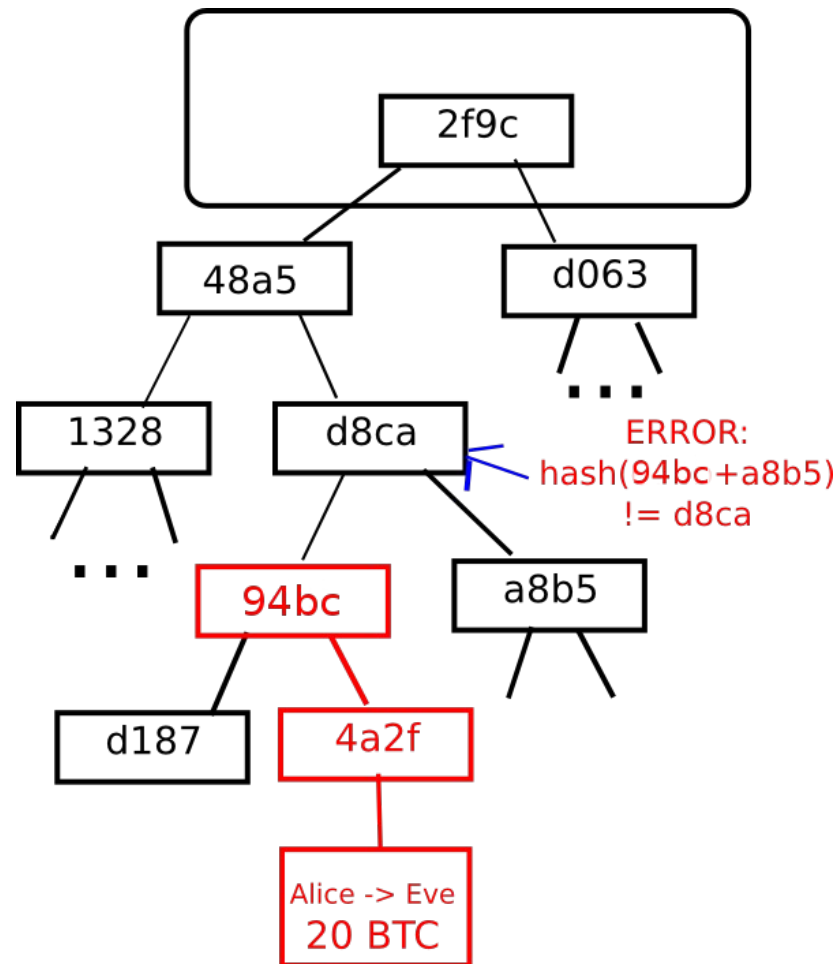
解决方案

➤ 轻节点

- 不存储所有数据
- 依赖全节点给的证明

➤ 数据裁剪

- 保留交易和最近的状态
- 数据量只有 10%



解决方案

➤ 分布式存储

- 分布式文件系统 (IPFS)
- 分布式数据库 (tikv)

➤ 存储成本

- 数据挖掘 / 统计 (研究 / 安全监控 / 投资决策)
- 提供查询业务 (广告)

➤ 存储格式

- Khipu

CITA 介绍

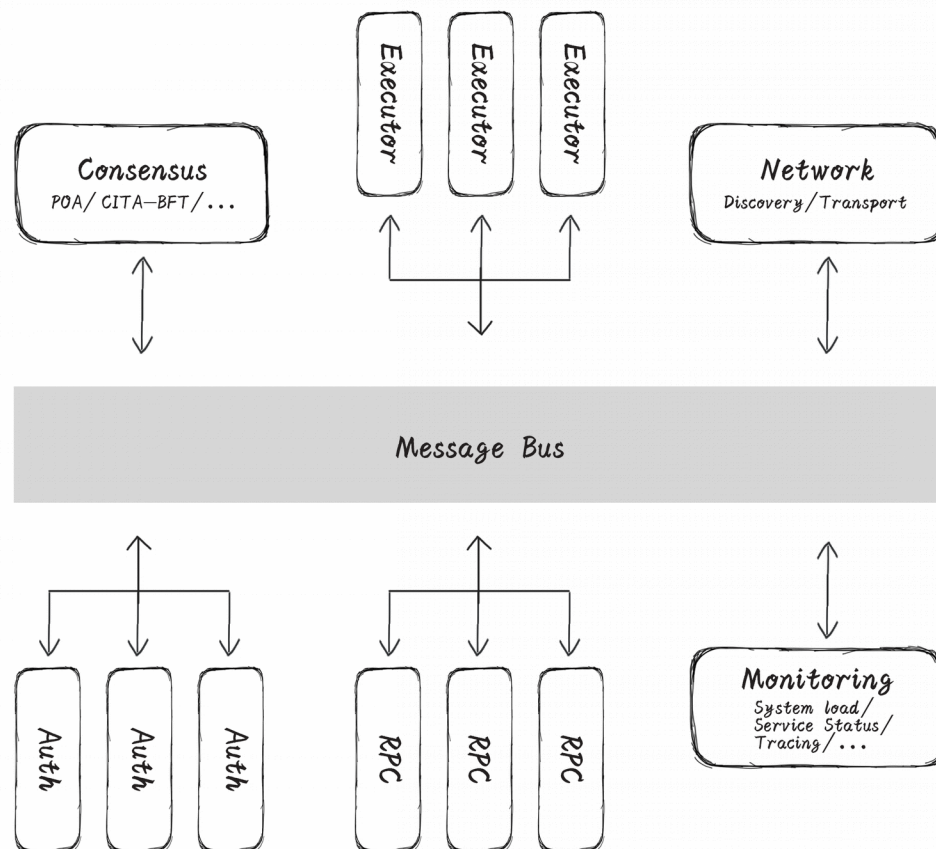
CITA—— 分布式企业间流程自动化系统
Cryptape Inter-enterprise Trust
Automation

➤ 特点

- 开源 <https://github.com/cryptape/cita>
- 微服务架构
- Rust 实现
- 面向企业领域

CITA 扩展性

- 逻辑节点
- 异步交易执行
- 原生合约
- 侧链 / 跨链



CITA 快照

➤ 同步

- 对区块链某个高度的状态做快照，保存状态、区块等数据，然后将快照恢复到另一个节点 / 本节点，就可以在较短时间内同步 / 恢复区块链数据。

➤ 裁剪

- 保留最新的状态
- 最近 100 个完整的块
- 之前的所有块头

未来的计划

➤ 存储

- 分布式数据库
- 存储格式的调研

➤ CITA-HUB

- 以 CITA 为核心的开放平台
- 打造共享的生态
- 欢迎存储和大数据方面的合作

参考资料

- <https://ethfans.org/posts/Sharding-FAQ>
- <https://zhuanlan.zhihu.com/p/29886689>
- <https://ethfans.org/posts/a-primer-on-ethereum-blockchain-light-clients>
- <https://github.com/khipu-io/khipu>
- <https://github.com/cryptape/cita-whitepaper/blob/master/zh/technical-whitepaper.md>
- <https://cryptape.github.io/cita>

Thank You