



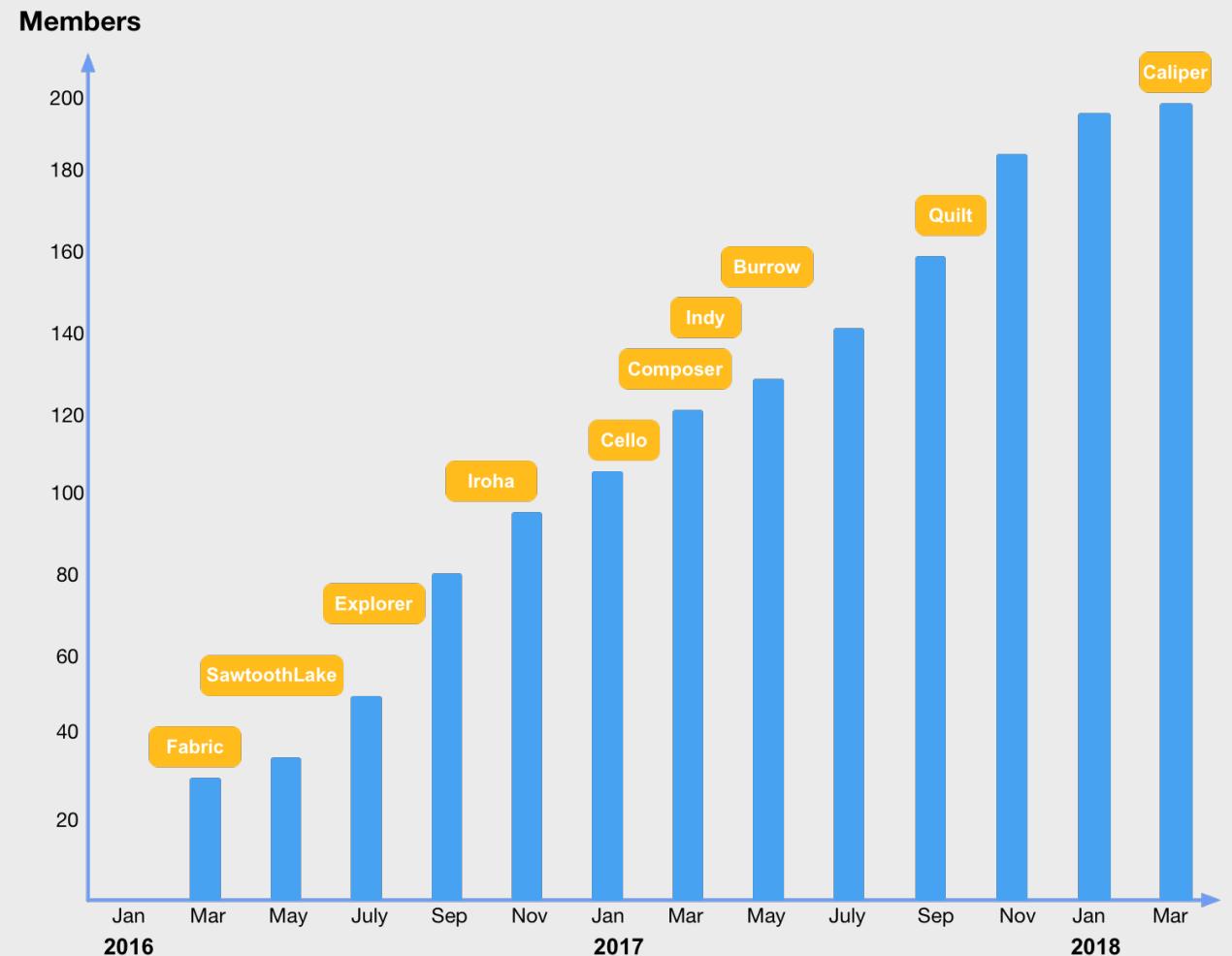
分布式账本关键科技探索

杨保华

2018年5月27日

超级账本-全球最大企业级开源分布式账本

- Linux 基金会支持的开源项目
- Apache v2 许可
- 30 家全球金融和科技领军企业发起
- 21/40+/200+ 高级/中国/全球会员
- 10 大顶级项目
- 500+ 活跃开发者
- 30000+ 代码提交
- 注重性能、权限、可插拔、可扩展



欢迎加入我们！

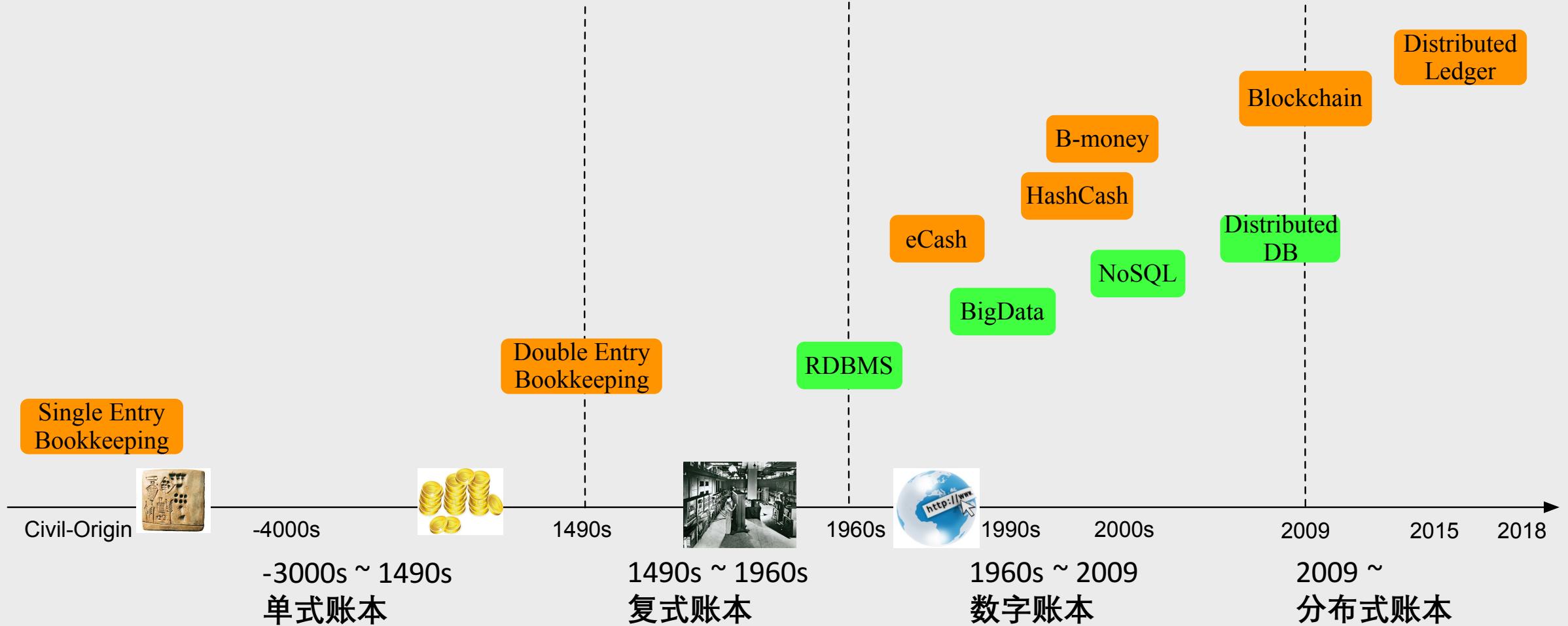
- 超级账本中国社区！

- <https://wiki.hyperledger.org/groups/twg-china>
- twg-china@lists.hyperledger.org
- <https://chat.hyperledger.org/channel/twg-china>
- 双周周三上午10点电话例会：
<https://zoom.us/my/hyperledger.community>
- 超级账本官方微信公众号：lf_hyperledger

内容

- 分布式记账问题
- 发展现状与关键技术
- 未来展望

记账科技简史



分布式记账科技

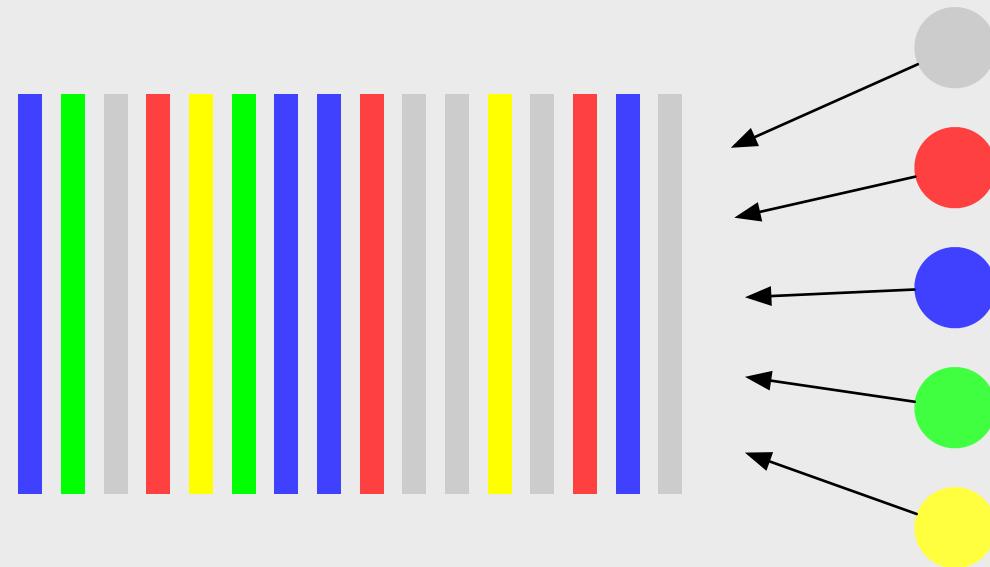
- Distributed Ledger Technology

多方参与，协同合作 记录交易历史

- 三个基本问题
 - 谁来记账：公开、联盟、私有
 - 如何确保记账正确：防篡改、共识
 - 谁可以访问什么：权限管理、隐私保护

分布式记账问题——极简思路

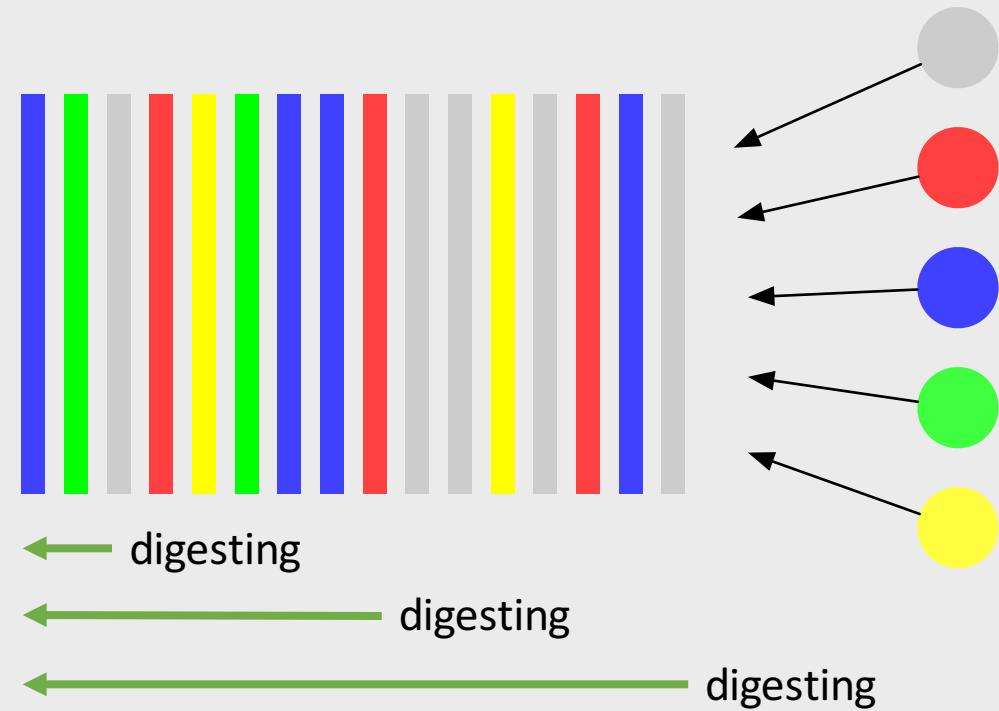
方案(1)：简单记录



思考
如果是非线性
结构呢？Trie、
DAG.....

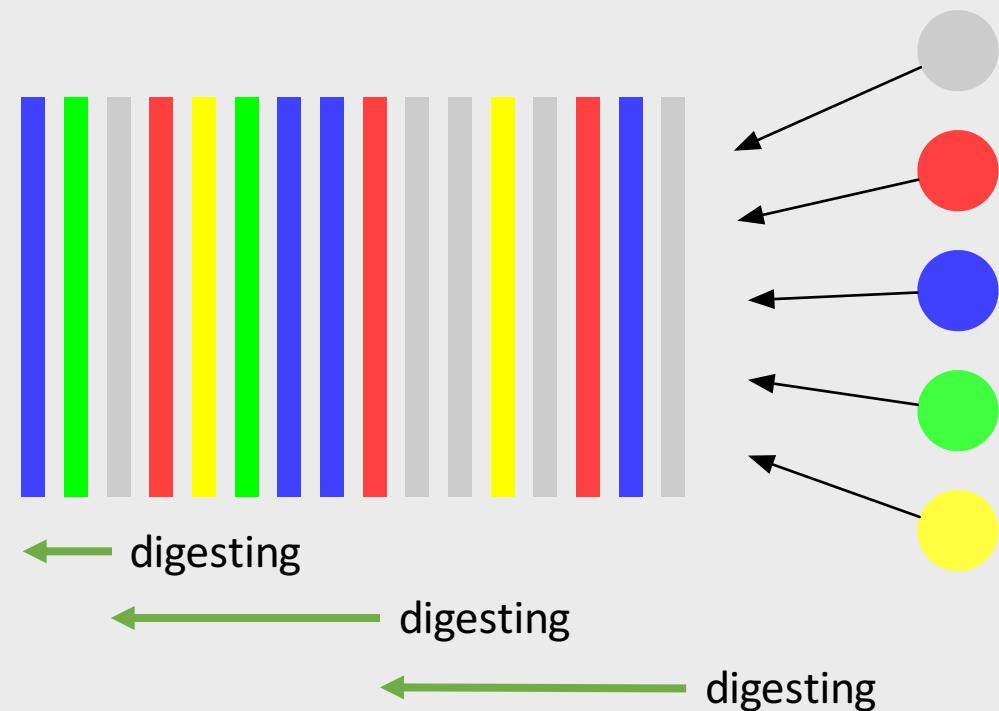
分布式记账问题——极简思路

方案(2)：摘要校验，可防篡改



分布式记账问题——天然思路

方案(3)：增量校验，可扩展



区块链第一性原理（First Principle）

区块链是记账科技演化到分布式场景下的天然结果

- 区块链结构可以满足分布式记账的两个基本需求
 - 防篡改
 - 可扩展
- 但并没有考虑
 - 安全、隐私？
 - 性能？

分布式记账科技到底为何重要

互联网已经解决了分布式场景下传递 **信息** 的问题；
分布式账本技术可能会解决传递 **可信信息** 的问题。

分布式记账科技的演进，将促使商业协作形态发生变革；
核心价值在于（通过合约）为多方协同网络提供 **可信基础**。

内容

- 分布式记账问题
- **发展现状与关键技术**
- 未来展望

技术现状：类比互联网

互联网 (10年尺度)	区块链为代表的DLT (5年尺度)
1974 ~ 1983 • ARPANet 试验网络	2009 ~ 2014 • 比特币试验网络
1984 ~ 1993 • TCP/IP 基础协议确立 • 可扩展基础架构完成	2014 ~ 2019? • 超级账本、以太坊等 • 基础协议和框架探索
1990s ~ 2000s • HTTP 开始被应用 • 正式向商用领域开放	2018 ~ 2023? • 核心协议探索中 • 商业应用的加速落地
2000 ~ • 互联网普及	? • 商业协同网络普及

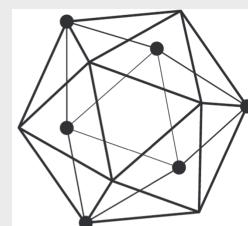
发展早期，加速落地。欧美领跑，中国紧跟。

项目分类

- 公有链账本
 - 面向公众，人人皆可参与，类比公共互联网
 - 匿名化，多面向完全不可信场景，支持加密货币
 - 比特币（Bitcoin）、以太坊（Ethereum）
- 联盟链账本
 - 面向企业，联盟成员可参与，类比企业网
 - 实名，访问权限控制，存在一定信任前提
 - 超级账本（Hyperledger）

三大代表性项目

指标	比特币	以太坊	超级账本
上线日期	2009.1	2015.7	2016.2
目标	加密货币公有链	公有链	联盟链
吞吐量	< 10	10~100	1K~10K
延迟	分钟级	10秒级	< 1秒
智能合约	不支持	支持，Solidity	支持，Go、Node、Java
共识机制	PoW	PoW，PoS	CFT，BFT
升级支持	分叉风险	分叉风险	平滑升级
评价	首个大规模加密货币项目	首个大规模公有智能合约*引擎	首个面向企业的分布式账本

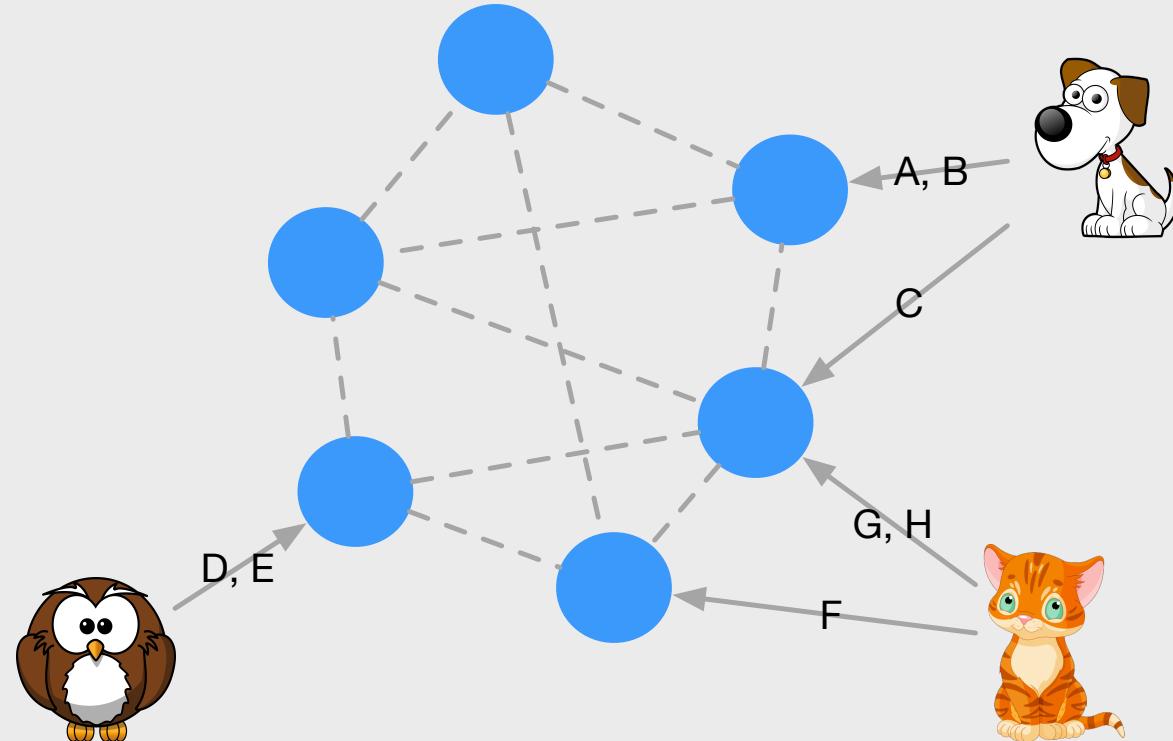


核心问题

- 共识：提高可信度
- 性能：如何快速记账
- 安全：隐私保护、权限管理、防攻击
- 扩展性：大规模、演化
- 互操作性：集成、管理、互通

共识 (Consensus)

- 定义：分布式系统（大部分节点）对收到的提案（Proposal），达成一致意见的过程。关键在于顺序。
 - 分布式系统基础性问题：扩展性、容错性



共识问题的难点

- 网络不稳定
- 延迟、带宽有限
- 任何环节都可能发生故障或被攻击
- 参与共识的节点动态加入或退出
-

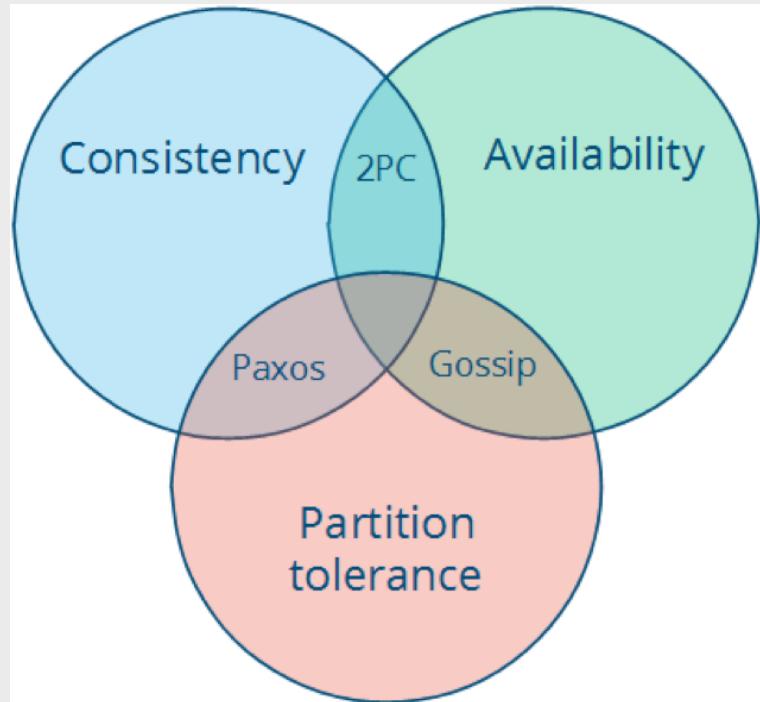
共识-FLP

- *No completely asynchronous consensus protocol can tolerate even a single unannounced process death.*

Fischer , Lynch, Patterson. 1985

- 在异步模型中，允许处理者失效的情况下，不存在分布式算法（在理论上能确保）解决共识问题。
- 网络延迟很重要 → 互联网尺度的共识很难！

共识-CAP



	M/S	Gossip	2PC	Quorum
Consistency		Eventual		Strong
Transactions	Full	Local		Full
Latency		Low		High
Throughput		High	Low	Medium
Data loss		Some		None
Failover	Read only			Read/write

Transactions across datacenters, Google IO, 2009

共识算法

- CFT
 - Paxos, Raft
- BFT
 - 概率型 (PoW, PoS, DPoS... Algorand)
 - 确定型 (PBFT, SBFT)
- CFT类算法短期内应用，BFT类算法是未来重点
- 算法和实现的合理性证明

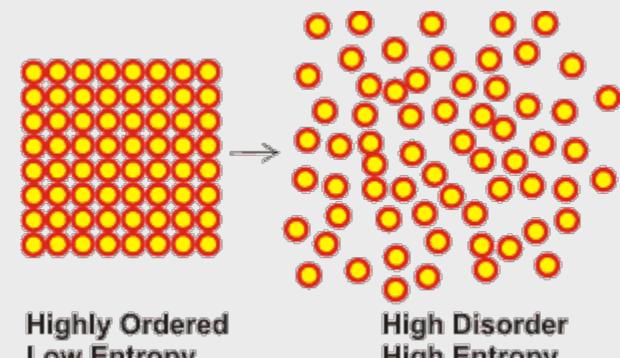
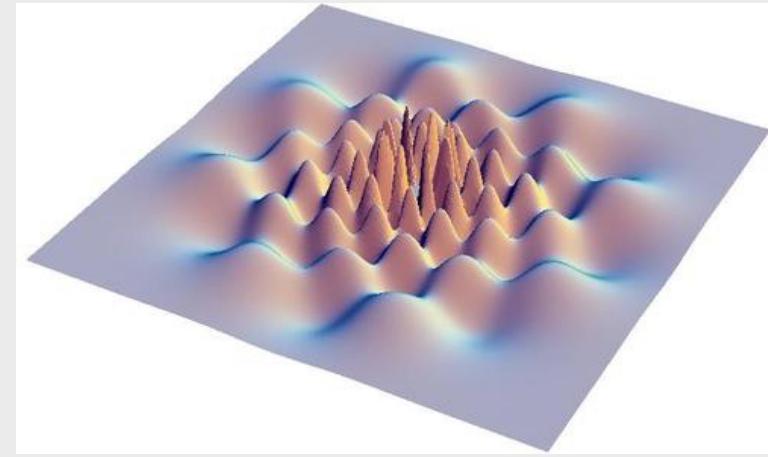
共识优化的关键思路

- 核心突破点在于提案环节
 - 提高门槛 (Proof)
 - 随机算法 (VRF)
 - 硬件加速 (TEE、Google Atomic Clock)
- 工程实践中的优化
 - 解耦 (分片、代理人)
 - 利用先验知识 (联盟链)

共识的另一种理解

- 牛顿时空观 vs 爱因斯坦时空观
 - 可信第三方 vs 不存在可信第三方
 - 局部低速 vs 广域高速
- 概率波的塌缩
- 熵减需要代价
 - 熵减越多自然代价越大 → 公有链更难
 - 但如何量化？

$$T = \frac{t}{\sqrt{1 - (\frac{v}{c})^2}}$$



”[On Time Versus Space](#)”, John Hopcroft , etc. 1977

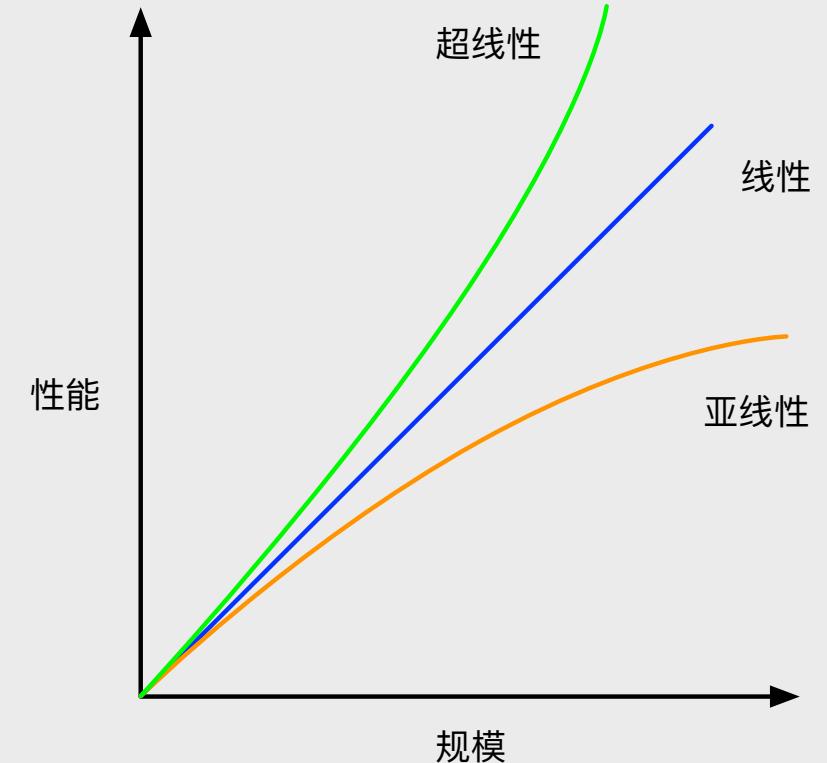
”[Time, Clocks, and the Ordering of Events in a Distributed System](#)”, Leslie Lamport, etc. 1978

性能

- 场景和如何测试，比数字本身更重要
 - 1 M+ tps is not difficult under ideal condition
- 生产环境下的表现和理论值并无必然联系
- Premature optimization is the root of all evil --
Donald Knuth

性能 (Performance)

- 系统性问题 (经典信息技术为例)
 - 网络 (0.1ms vs 100ms)
 - 存储 (SSD : 10 K iops)
 - 账本处理 (SHA2 : < 10 K tps)
 - 智能合约 (CPU、 network latency)
- (大部分)系统的性能扩展都是亚线性



性能 (Performance)

- 评测指标
 - 规模
 - Throughput : transaction/second
 - Latency
- 参考性能
 - 公有链 (Ethereum) : 大规模 , 10 tps, 10s
 - 联盟链 (Hyperledger Fabric) : 中小规模 , 3.4 Ktps, 1s

Hyperledger Fabric: A Distributed Operating System for Permissioned Blockchains, 2018

安全 (Security)

- 数据隐私性
 - 敏感数据离线、加密、混淆
 - 多账本隔离
 - 隔离域
 - 零知识证明
 - 同态算法
 - GDPR 带来的挑战和机遇



安全 (Security)

- 合约安全性
 - 形式化验证（难）
 - 约束合约能力
 - 安全环境技术，如 TEE
- 密码学技术的突破和挑战
 - 量子计算

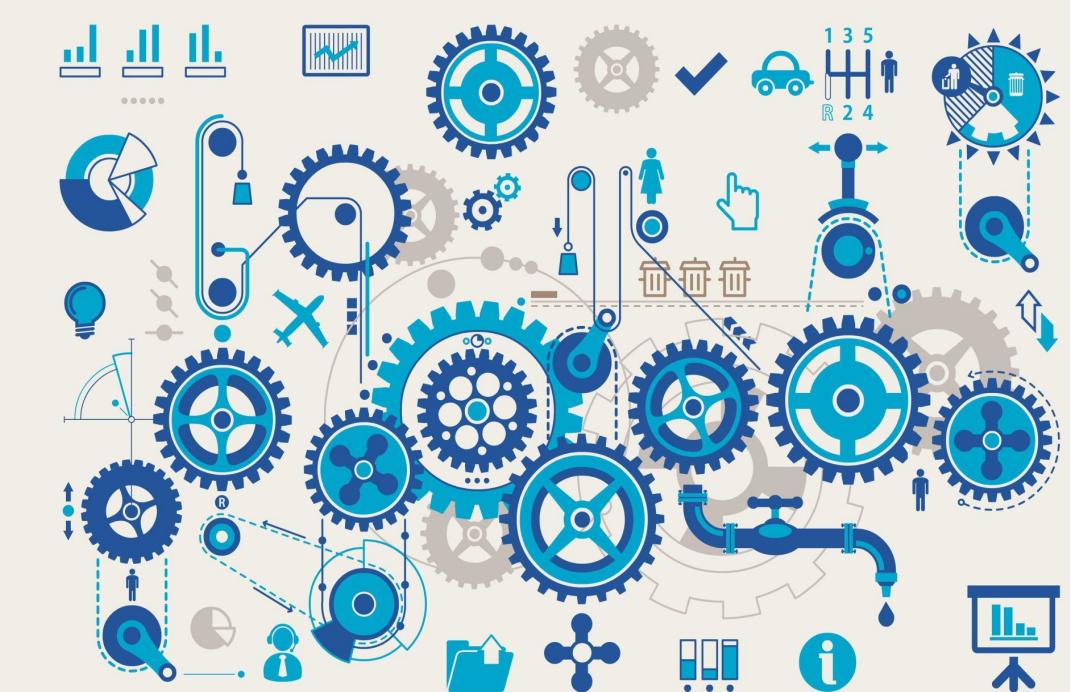


可扩展性 (Scalability)

- 数据存储的可扩展性
 - Storj
 - IPFS
- 网络规模的可扩展性
 - 辅助加速 (off-load)
 - 分片 (sharding)
 - 多账本 (multi-ledgers)
 - 新型 P2P 技术 (beyond DHT)

互操作性 (Inter-operability)

- 与已有系统的集成
 - 数据库
 - 分析系统
 - 智能决策系统
- 区块链系统的管理
 - Hyperledger Cello
- 跨账本互联
 - Hyperledger Quilt



内容

- 分布式记账问题
- 发展现状与关键技术
- 未来展望

未来展望-以史为鉴

- ❖ 实践决定标准
- ❖ 开源技术是唯一出路
- ❖ 自底向上的渐进式创新

互联网发展史对区块链极具借鉴意义

未来展望-跨领域合作是必然



分布式账本的学科金字塔

道生一，一生二，二生三，三生万物。

-- 《道德经》

单账本，复账本，分账本，可信协同。

-- 《账本科技演化录》

Reference

- [Hyperledger Project](#)
- 《[区块链原理设计与应用](#)》
- 《[超级账本 Fabric 源码剖析](#)》
- 《[Docker 技术入门与实战](#)》
- [github.com/yeasy/blockchain_guide](#)

