区块链技术基础

孙毅

中国科学院计算技术研究所

Part · 02

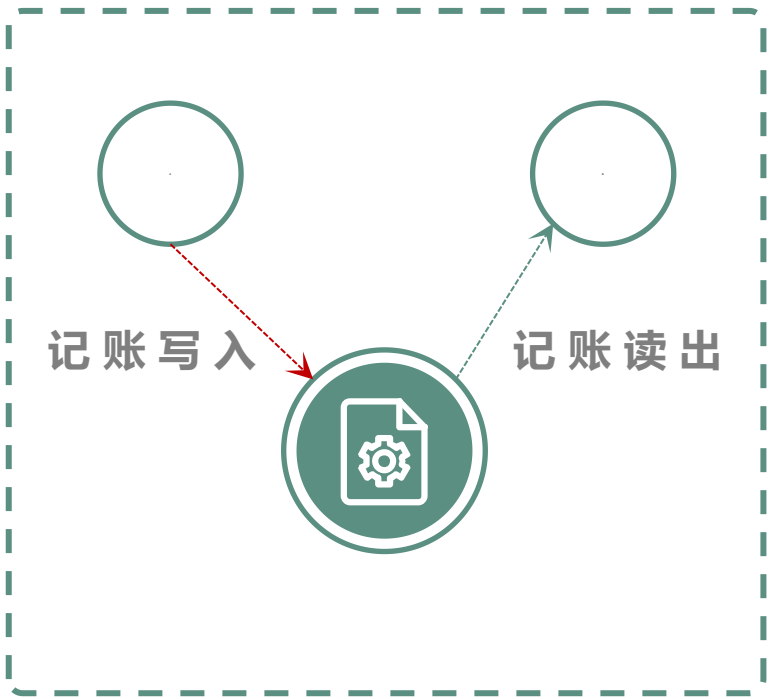
1

区块链基本原理

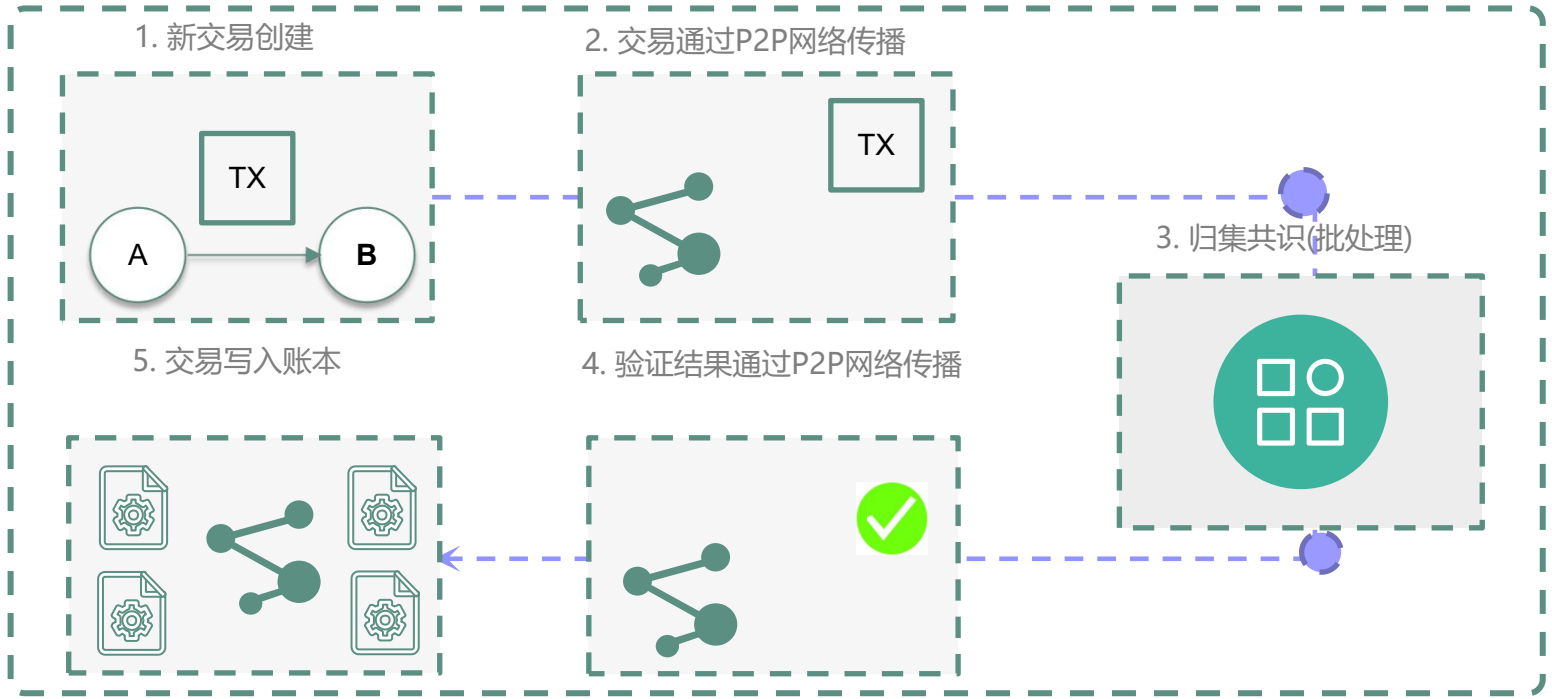
区块链是什么？

- 区块链（Blockchain）是使用密码技术将共识确认的区块按照顺序追加形成的分布式账本（ISO22739）。
  - 宏观：分布式平等部署系统、分布式共享相同数据；无中心化控制，全网参与的节点协作完成交易验证和存储。
  - 微观：数据存储在块（Block）中，这些块在逻辑上串联起来构成链条（Chain）；应用数字签名与完整性校验保证块数据的真实性、时序性、完整性。
  - 在技术层面具有不可伪造、不可抵赖、不可篡改、不可撤销等属性，在应用层面具有分布式的公开透明、交易可跟踪等特征。
- 区块链的核心价值
  - 信任模型：信任人->信任技术
  - 数据保护：产生者->拥有者
  - 治理模式：人治->规则治

传统中心化记账 vs 区块链分布式记账



传统的中心化记账

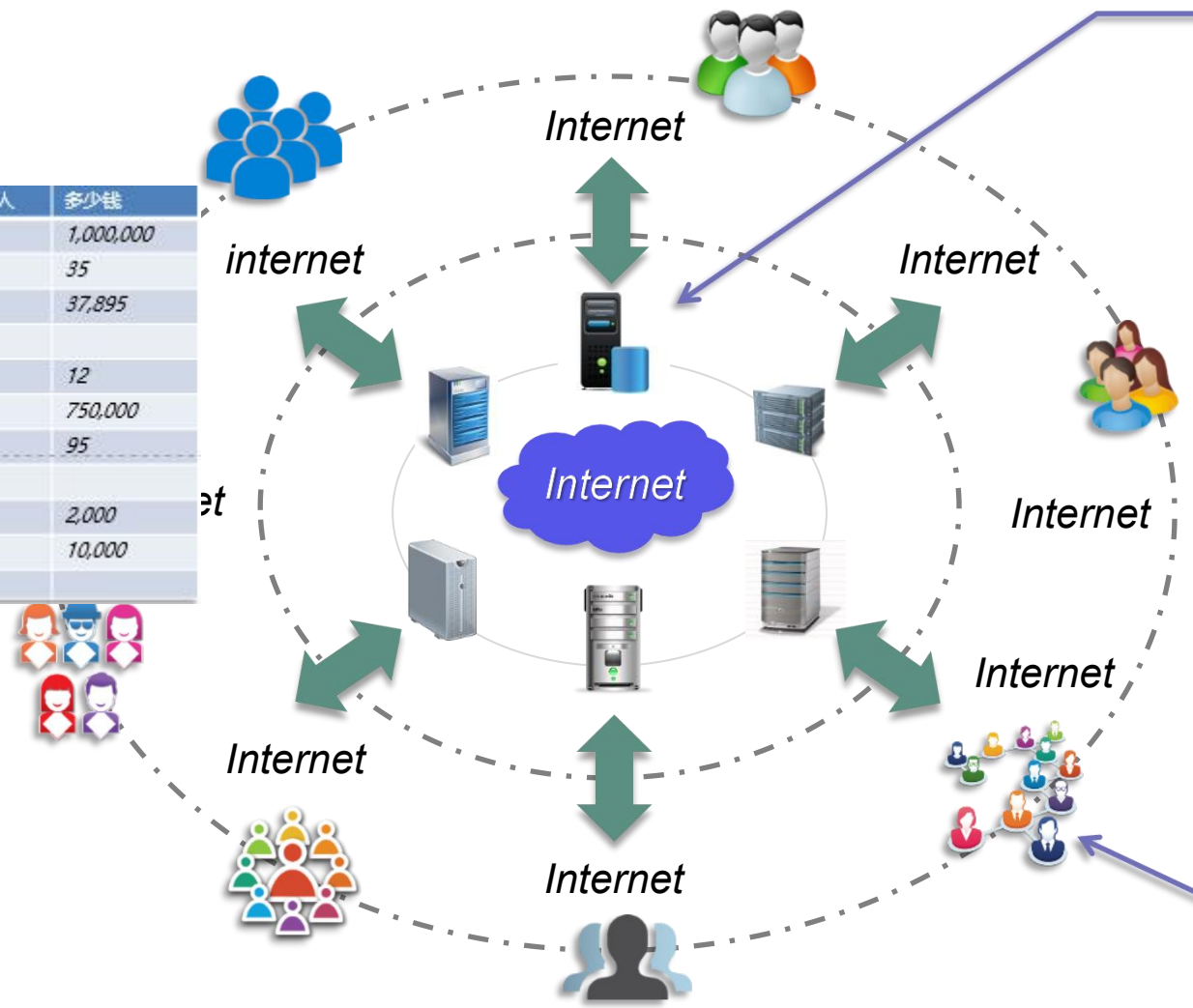


区块链的分布式记账

分布式记账，不依赖单个中心

区块链 – 分布式记账技术（DLT）

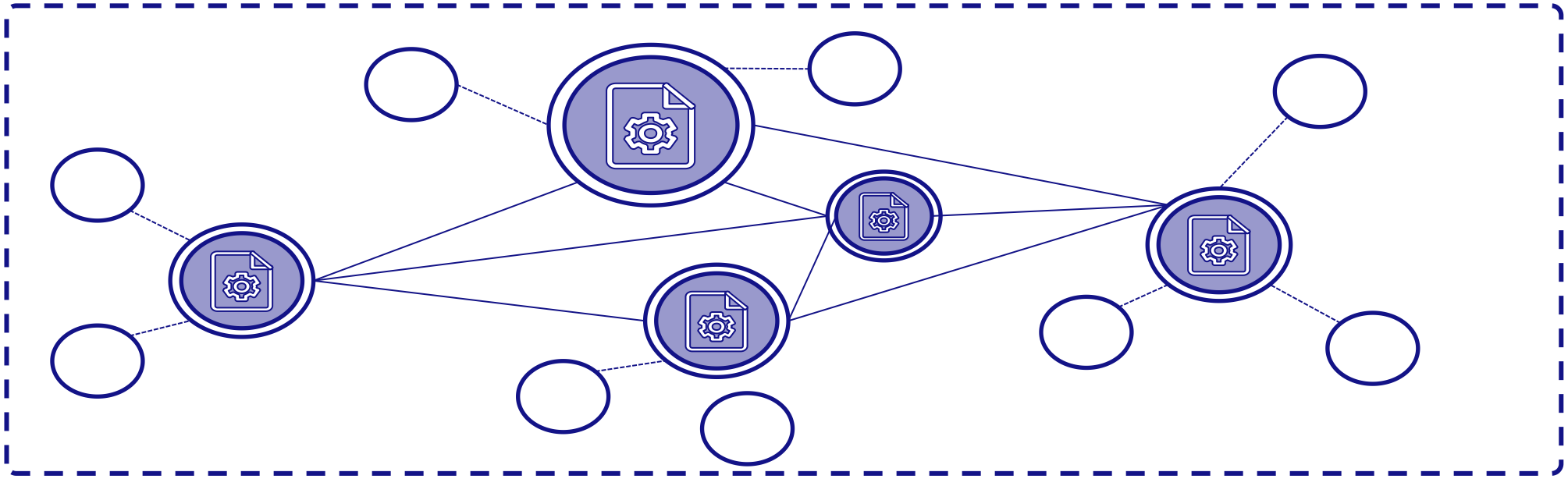
时间	给钱的人	收钱的人	多少钱
2016/11/13	第一次登录	老A	1,000,000
2016/12/31	第一次登录	老B	35
2017/01/12	第一次登录	老C	37,895
.....			
2017/02/02	老B	老A	12
2017/03/19	第一次登录	老D	750,000
2017/07/22	老C	老D	95
.....			
2017/12/21	老A	老C	2,000
2017/03/21	老A	老D	10,000
.....			



所有的节点
组合成
一个服务群组
提供
超级账簿的服务
依既有协议
自动运作

终端使用者
通过 internet
连结任一个服务器
均可上线
取得账簿服务

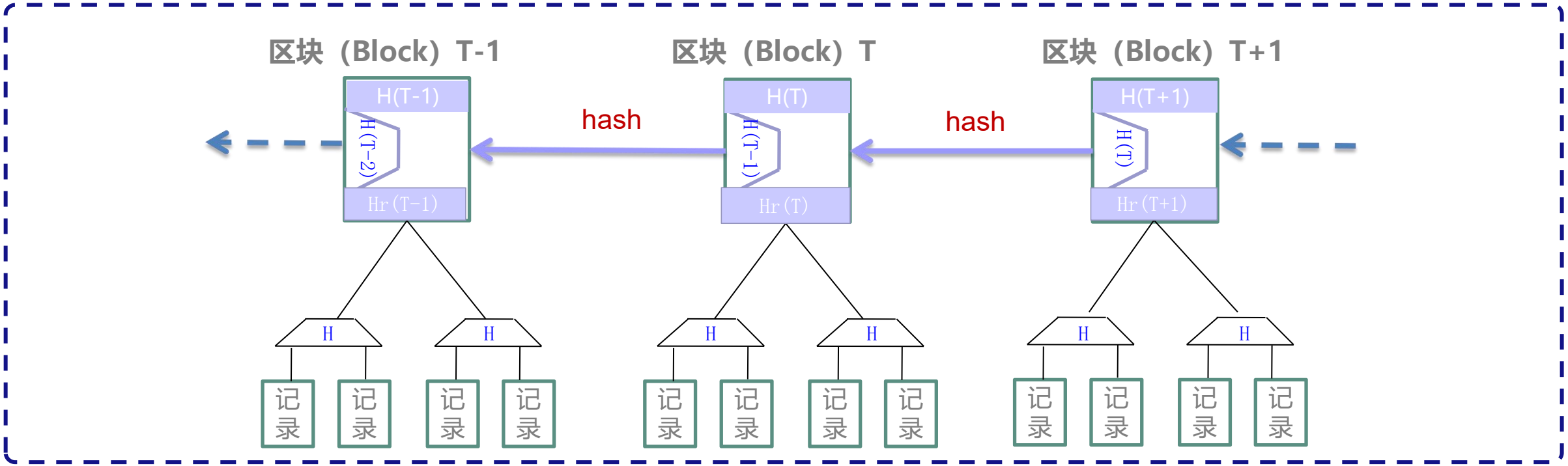
宏观：多中心联合共建共享



所有者多中心化/数据存储多中心化/交易验证多中心化

- **不仅是单纯的多机/多地分布式部署，还要**
  - 分布式平等部署、分布式共享；
  - 全网参与节点协作，完成交易验证和存储；
  - 透明、共享、开放，共建。

微观：块链的逻辑结构



- BlockChain 名称的来源：
  - 区块（block），保存：1 业务记录集合（以hash link的方式） 2 前序块的哈希值（数字摘要） 3 （1+2）的哈希值（数字摘要）。每个记录中有发起者的数字签名，保证操作的不可伪造性和不可抵赖性。
  - 链（chain），就是逻辑上由 “2 前序块的哈希值”串联起来的链条，保证时序性和不可篡改特性。
- 后块为所有的前块背书，起到“联保”作用， 这样的数据结构即使是最初发布数据的人也不能改动他自己的数据了。

区块链解决什么问题

区块链解决的核心和本质问题是：无可信中心机构时，如何在信息不对称、不确定的环境下，建立满足活动赖以发生、发展的“信任”生态体系，即 “拜占庭容错”或者“两军问题”。

拜占庭将军问题

拜占庭帝国派10支军队进攻一敌人，这个敌人可抵御5支军队同时袭击，这10支军队不能集合单点突破，须分开同时攻击。问题是多个将军互相并不信任(存在叛徒)时，这种状态下要保证进攻一致，需要某种分布式协议来进行远程协调。如果每个将军向其他九个将军派出一名信使，总计90 次传输，每个将军会收到9 条信息，可能每一封都附着不同的进攻时间。此外，部分叛徒会故意答应超过一个的攻击时间，所以他们将重新广播超过一条的信息链。这个系统变成不可靠信息和攻击时间矛盾的混合体。

区块链的分类

A 公共区块链

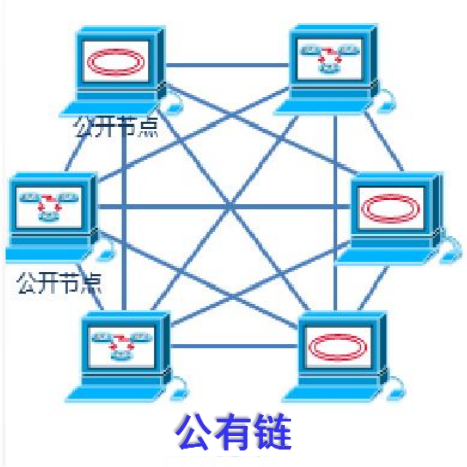
网络中的节点可任意接入，网络中数据读写权限不受限制，任何人都能参与共识过程，比特币属于典型的公有链。

B 私有区块链

网络中的节点被一个组织控制，写入权限仅限在一个组织内部，读取权限有限对外开放，比如企业内部的办公审批、财务审计；政府行业的预算和执行等。

C 联盟区块链

介于公有链和私有链之间，只限联盟成员，权限及记账规则都按联盟规则来定制。多用于行业协会、机构间的交易、清结算等B2B场景

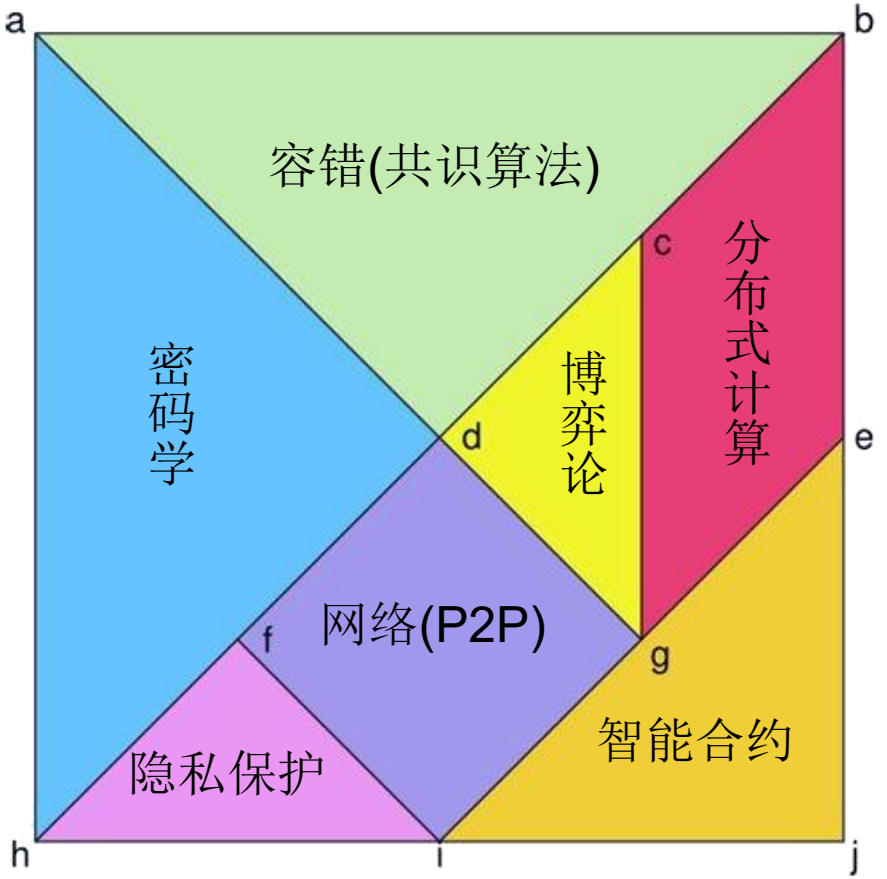


公有链

私有链

联盟链

区块链 – 精巧组合



区块链 – 层次架构


应用层
金融
供应链
…
激励层
发行机制
分配机制
…
共识层
BitcoinNG
Tendermint
…
网络层
P2P网络
传播机制
验证机制
数据层
区块数据
链式结构
数字签名
哈希函数
默克尔树
非对称加密
物理层
专用芯片
网络基础设施
…

区块链特性

多中心化　时序数据　多方维护　智能合约　安全可信

多中心验证

数据的验证、记账、存储、维护和传输等过程均是基于分布式系统结构，采用纯数学方法而不是中心机构来建立分布式节点间的信任关系

块链结构

采用带有时间戳的链式区块结构存储数据，从而为数据增加了时间维度，具有极强的可验证性和可追溯性

多方参与

采用特定的机制来保证分布式系统中所有节点均可参与数据区块的验证过程，并通过共识算法来选择特定的节点将新区块添加到区块链

智能合约

区块链技术可提供灵活的脚本代码系统，支持用户创建高级的智能合约

密码学

采用非对称密码学原理对数据进行加密，同时借助分布式系统各节点的共识算法形成的算力来抵御外部攻击、保证区块链数据不可篡改和不可伪造

常识误区

Blockchain

- 区块链**等于**数字货币？
- 区块链**等于**数据库？
- 区块链**等于**没有隐私?
- 区块链解决**所有**问题？

Part · 05

2

区块链技术挑战

区块链发展面临问题

底层技术尚未成熟

存在性能、安全性、互操作性、强化合约等一系列技术挑战。

监管压力大、挑战多

区块链与金融等业务具有天然的亲近性，承载价值重，迫切需要有效的监管；匿名性、弱中心化等特征给监管带来新挑战。

存在一定研发及改造投入

需要投入一定时间和精力研发新系统或改造现有系统，需要考虑成本投入问题。

人员复合能力要求高

从业人员需要具备复合型能力，需要具备IT技术、密码学原理、业务知识等各方面知识及能力，符合要求的人员较为稀缺，培养难度大。

区块链产业发展如火如荼，但在应用过程中还需要解决各种各样的问题，才能推动区块链技术得到更广泛的认知和发展

区块链技术政策建议

技术层面：
重视区块链底层技术研发

- 加大在体系结构、共识算法、验签机制、（跨链）通信协议、专属硬件等方面的研发投入
- 争取技术自主可控，引领全球区块链技术发展

管理层面：
发展创新监管模式

- 鼓励区块链技术和应用发展
- 引导区块链的应用方向
- 规范区块链应用的审查和部署
- 加大对区块链平台和应用的监管与预警

人才层面：
加强交叉学科人才

- 加强对未来社会所需的精通计算机通信和其它专业领域的跨界人才的培养

区块链技术发展趋势

技术未来发展趋势： 跨链技术、用户认证、安全问题、标准化问题、与云技术结合的BaaS服务等。

提高性能

不断提升区块链计算性能，使其具备大并发适应性及高可扩展性。

保障安全

持续补充面向不同区块链组成模式下的安全防护措施，保障业务及数据安全。

保护隐私

在保证区块链分布式数据同步原则不变的情况下，加强基于权限的隐私保护能力。

促进跨链

推进跨链共识算法的不断发展及成熟，促进不同区块链体系最终实现跨链。

强化合约

持续强化智能合约的事务处理能力，使其适应更多应用场景。

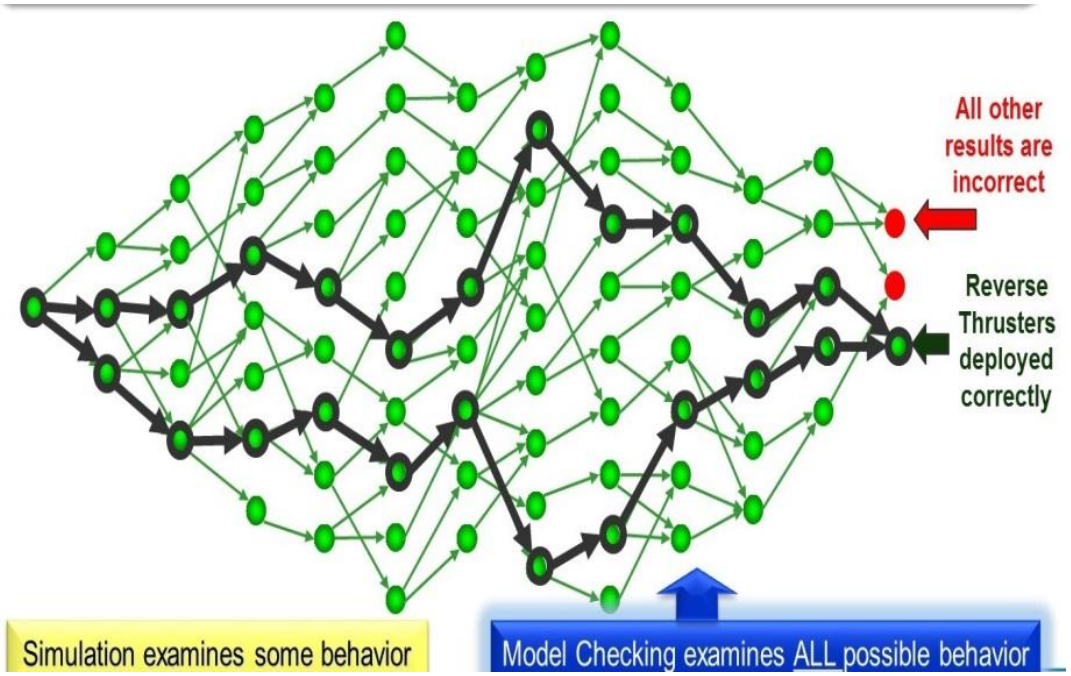
。

区块链技术—性能

- 链上扩容
  - 隔离见证（Segwit）：把签名信息和交易记录分离，降低交易记录大小。
  - 比特币现金（ BCC ）：区块大小可动态调整，最大可达8MB。
  - 效果有限
- 共识算法
  - 经典算法：PoW、PoS、DPoS、PBFT等
  - 新算法：Algorand、Bitcoin-NG、Tendermint等
  - 三难困境问题：去中心化、性能、安全性最多满足两个
- 体系架构
  - 并行化架构：以太坊sharding、Plasma
  - 链外通道网络：闪电网络、雷电网络
  - 早期阶段，尚不成熟

区块链技术—安全性

- 形式化验证
  - 共识机制：Terdermint
  - 智能合约
  - 智能合约执行引擎： KEVM
  - 智能合约编译器
  - 智能合约高级语言
- 钱包、交易所攻击
- 量子计算
  - 公私钥签名算法的冲击
  - 算力集中的冲击



区块链技术—隐私保护

- 混币技术（达世币）：可信第三方把不同的交易混在一起
  - 主节点信任问题
- 环签名（门罗币）：选定签名者集合，把多个签名者按照环状签名
  - 匿名集合比较小
- 零知识证明（零币）：
  - zk-SNARKs（可信初始化过程，证据生成1min，验收40ms，证据290B）
  - zk-STARKs（不需要可信初始化，证据生成快，但是证据大，几百KB）
- 同态加密、多方协同计算等
  - 尚未应用

区块链技术—跨链通信

- Interledger：利用哈希锁定、中间人技术实现跨链转账
  - 保证原子性，本质上不是区块链解决方案
- BTCRelay：采用中继技术，通过使用以太坊的智能合约允许用户在以太坊区块链上验证比特币交易。
  - 一对一连接，可扩展性差，单向通信
- Cosmos：由Hub和Zone组成，Zone之间的跨链通信由Hub去中继，而Zone的正常运行是完全自治的。
  - 必须使用Tendermint共识，同构链
- Polkadot：异构链
  - 非常初期阶段，尚无明确方案

区块链技术—智能合约

- 智能合约虚拟机
  - 自主可控的虚拟机：EVM，效率不高（编译器优化、执行环境研发等）
  - 使用现有成熟的编译运行环境的虚拟机：JVM，改造开销大。

- 智能合约升级：可升级且可解释的智能合约完整方案是智能合约大规模应用的关键所在。

- 链下数据可信喂养：如何与链下真实世界活动相关联
  - Oraclize：将智能合约与Web API链接起来，使得智能合约无需额外的信任，即可获得现实世界的真实活动数据
  - 可信数据喂养系统Town Crier（TC）：通过英特尔最新可信硬件SGX向智能合约提供认证可信以及机密性数据。
  - 现有方案灵活性较差

区块链技术—监管

区块链技术特征

- 公开透明
- 不可抵赖
- 不可篡改
- 地址匿名化
- 去中心化

区块链监管机遇及挑战

- 高质量数据来源使得数据挖掘更加有效，全过程记录易于穿透式监管
- 无法与现实真实身份对应，难以确认责任主体

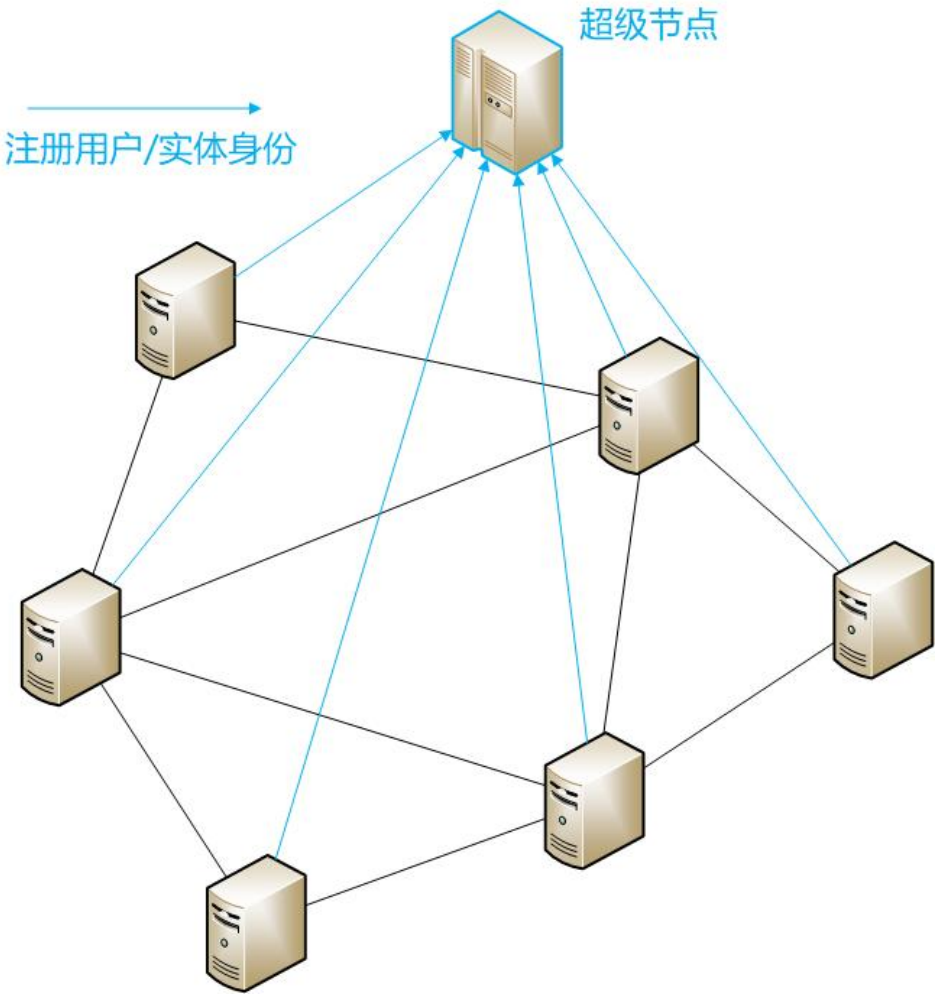
联盟链监管

联盟链特点

- 节点有准入机制
- 用户有身份标识

监管思路

- 设立超级（主权、审计）节点，拥有区块链网络中地址/节点与实体身份的映射关系，具有上帝视角，发出监管指令，对账户、交易、业务进行实时控制。



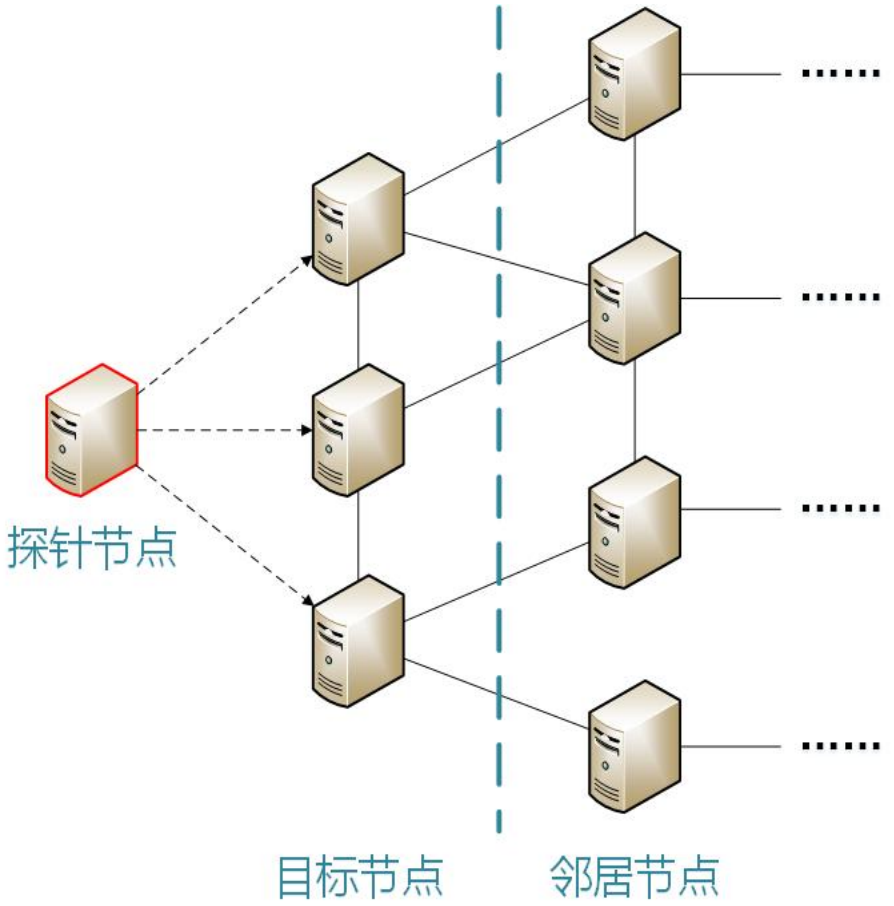
公有链监管

公有链特点

- 任何节点均可自由加入，无审查机制
- 交易在P2P网络中洪泛式广播，难以定位交易的始发节点

监管思路

- 在现有的公有链网络中插入探针节点，探测交易的传播路径，以及网络的拓扑结构。设计特定的模式匹配方案确定异常行为和节点的存在。



感谢聆听！