2020 WEST LAKE CYBERSECURITY CONFERENCE ON LINE

西湖论剑·网络安全线上峰会

之江实验室 ZHEJIANG LAB

数治安全 智理未来

DIGITALLY GOVERNED SECURITY INTELLIGENTLY MANAGED FUTURE

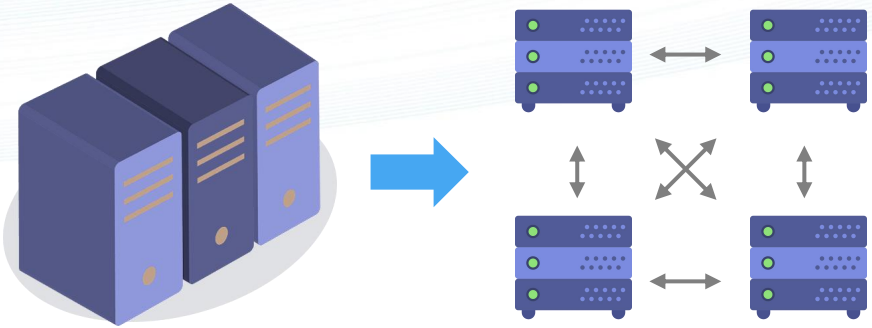
2020 WEST LAKE CYBERSECURITY CONFERENCE ON LINE
西湖论剑·网络安全线上峰会
之江实验室 ZHEJIANG LAB

金融区块链安全规范实践

杭州趣链科技有限公司 李伟

区块链本质

技术本质



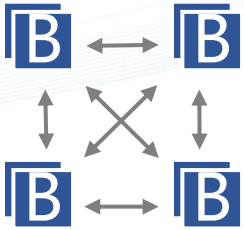
传统系统　　区块链-分布式架构

- **分布式账簿系统**
  - 非对称加密技术对交易进行数字签名
  - 通过共识机制达成多节点一致
  - 数据以链式区块形式组织存储
- **全同步的分布式架构**
  - 存储冗余
  - 计算冗余
- **信用聚合和业务协作平台**

区块链本质

五大特性

- **多中心化**
  - 网络视角：P2P网络
  - 控制视角：不具备中心节点
  - 功能视角：节点功能对等



- **极难篡改**
  - 多方参与、共同维护
  - 哈希函数+数字签名+分布式共识

- **可追溯性**
  - 块链式结构：可追溯
  - 存在性证明：可验证

- **可编程性**
  - 智能合约
  - 多中心化应用

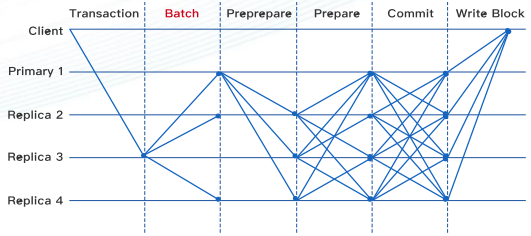
- **安全可信**
  - 非对称密码学技术
  - 零知识证明+同态加密
  - 强大算力

区块链本质

新的安全范式

共识算法

针对区块链上发生的交易，保障区块链所有节点数据一致性。

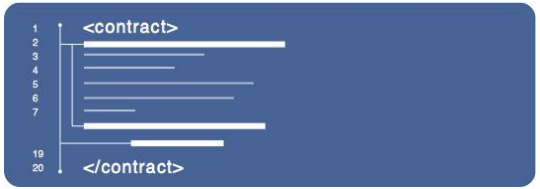


块链式数据结构

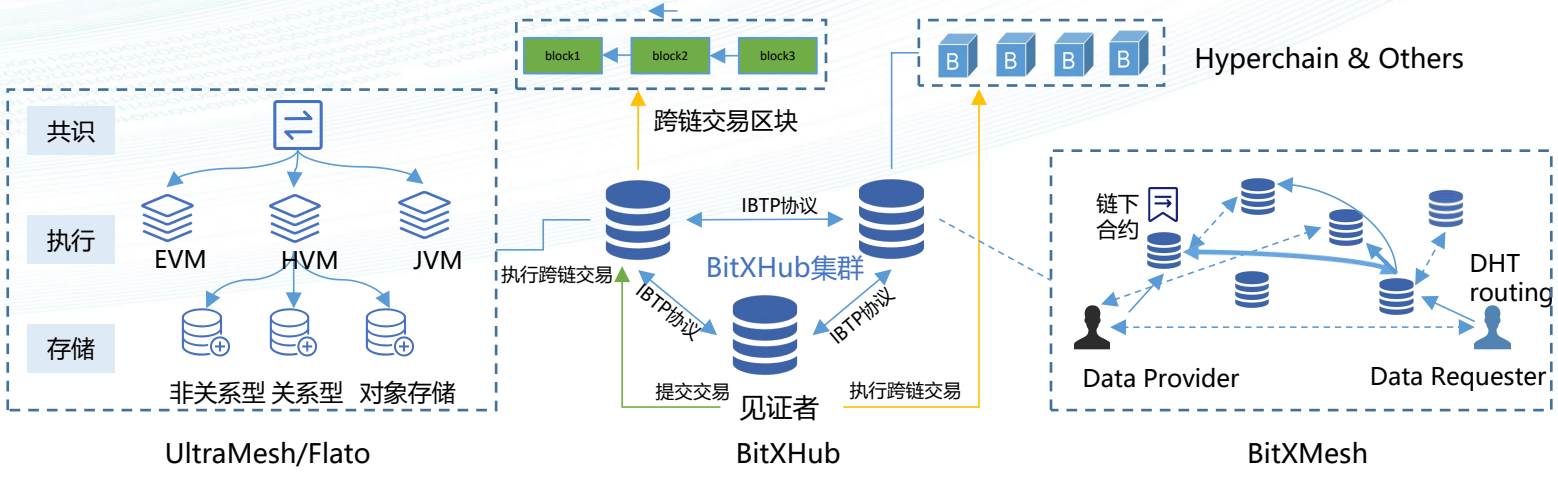
将一段时间内的交易数据打包成区块，再将多个区块按时间顺序有序链接的一种数据结构，用来确保数据的不可篡改性

智能合约

一段部署在区块链上可自动运行的程序，可以自动化地执行预先定义好的规则和条款，通过减少人为干预的风险，提升交易执行的安全与可信程度



区块链平台



UltraMesh/Flato　　BitXHub　　BitXMesh

Hyperchain二代

- 新型共识算法（自适应）
- 可配置执行
- 混合型可信存储
- 链上存储扩容

跨链协议

- 跨链框架
- 哈希锁定
- 可信时钟

可信数据网格

- 链下可信数据存储
- 安全数据交换与共享
- 多方模型计算

区块链平台特性

高性能 HOT

标准投产环境中可支撑3.7W TPS，在硬件加速条件下可支撑5W+ TPS

大规模组网 HOT

首个支持1000+节点的生产级联盟链网络，可以实现数十万个多类型区块链网络节点分层部署

海量存储 HOT

日均存储量可达TB级，支持GB级图片、音视频大文件存储

跨链协同 HOT

- ✓ 首个支持同构/异构区块链跨链能力
- ✓ 全面支持Fabric跨链协同

智能合约 HOT

- ✓ 首个原生支持Java语言，兼容Solidity语言，提供合约全生命周期管理
- ✓ 预言机：提供可信外部数据源服务

安全&隐私

- ✓ 首个支持全国密
- ✓ 分区共识、隐私交易、TEE账本加密
- ✓ 首创链内原生权限控制体系

数据管理 HOT

- ✓ 数据归档、合约数据可视化、数据索引查询

治理审计

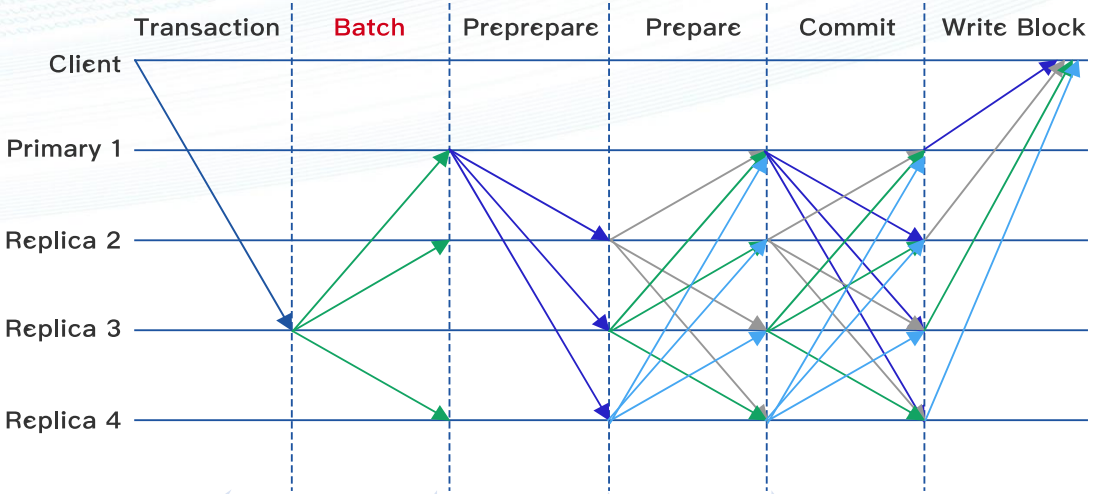
- ✓ 首个支持分布式CA治理
- ✓ 支持系统审计

灵活部署

- ✓ 首个企业级一键部署、支持所有主流公有云/专有云/混合云

共识算法

RBFT共识算法



收到客户端发起的交易的节点，将消息**广播给所有节点**

主节点经计算，将批量交易的**哈希值广播**给所有节点

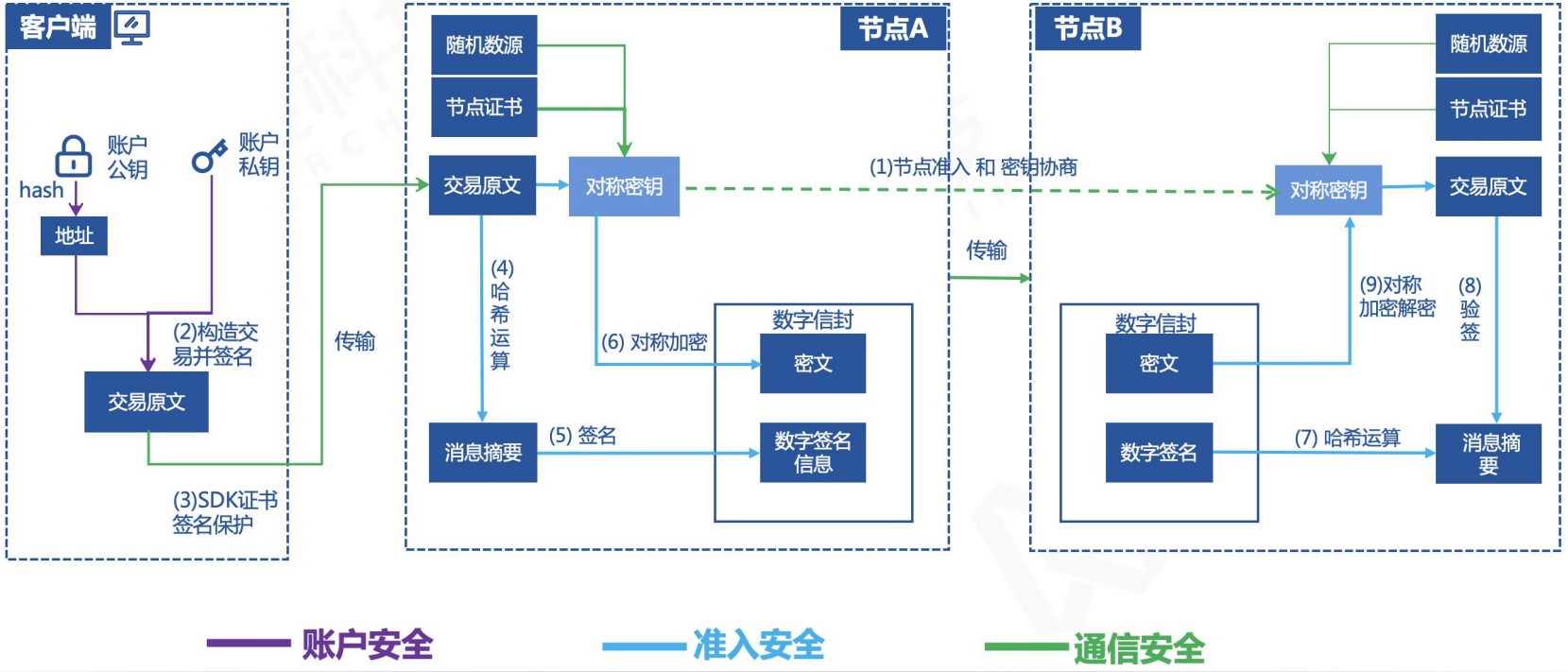
所有节点在接到交易后进行哈希，并与主节点的**哈希序列比对**

所有节点收到2f个对比通过消息后，在**虚拟机运行**这批**交易**

所有节点将这笔**交易写入区块，到检查点**再进行结果校验，检查点规则可配置

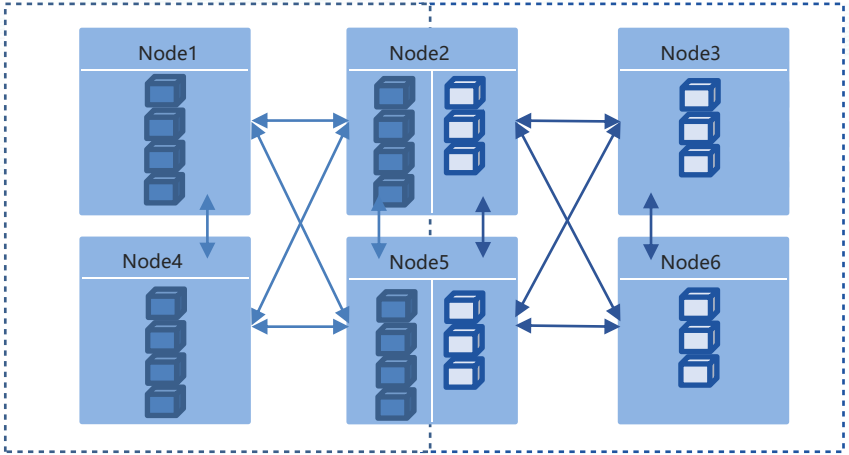
区块链安全体系

全流程安全



隐私保护

分区共识



分区共识

- 交易按名字空间**独立共识**
- 验证节点仅共识其参与的名字空间交易
- 验证节点支持多个名字空间的交易共识

数据隔离

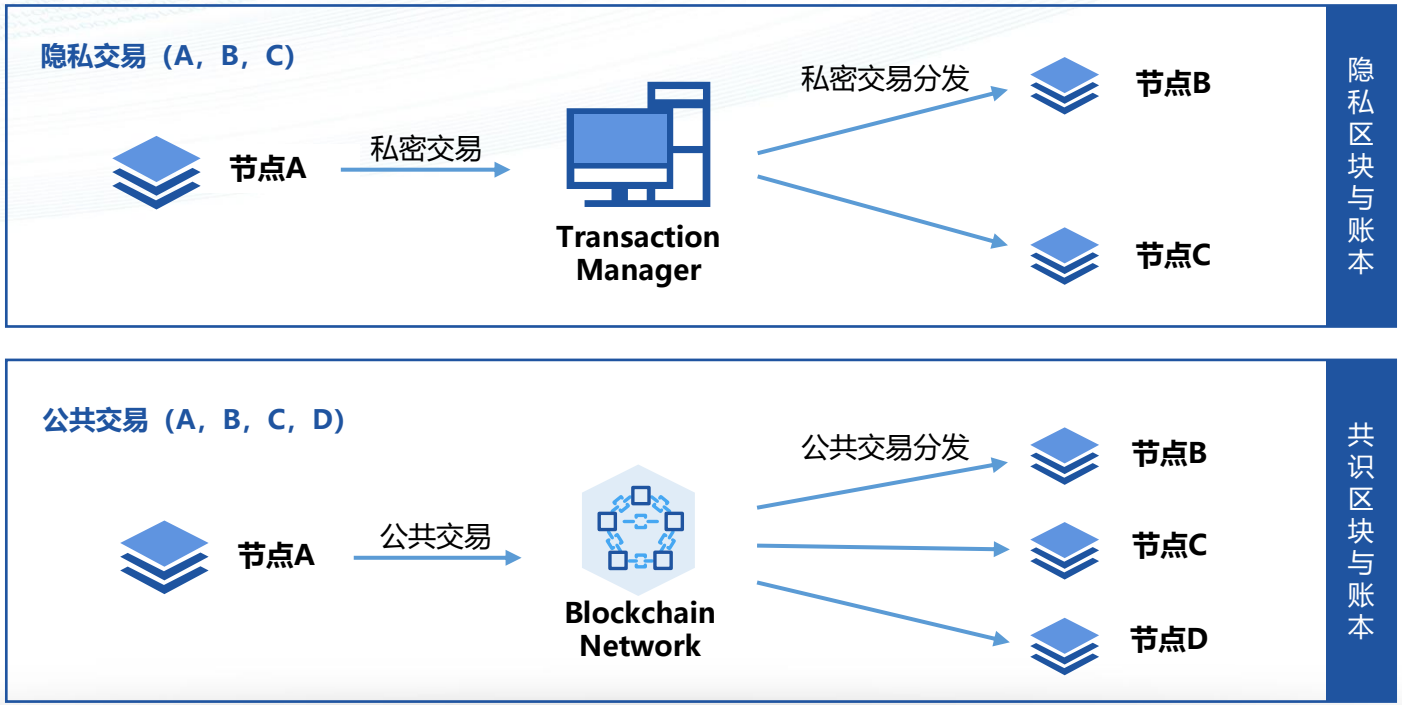
- 数据的传输和存储按照名字空间划分
- 节点内不同名字空间中的账本实现**物理隔离**
- 节点仅存储其参与的名字空间的账本数据

并行执行

- 不同名字空间内部交易并行执行
- 名字空间之间的交易结果互不干扰

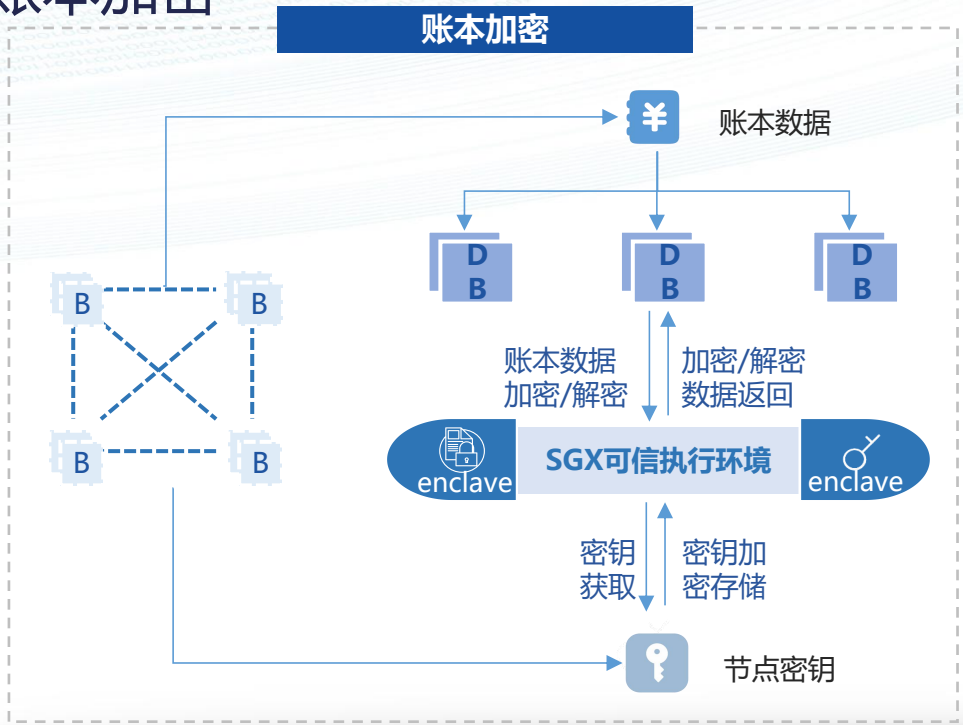
隐私保护

隐私交易


隐私交易（A，B，C）
节点A
私密交易
Transaction Manager
私密交易分发
节点B
节点C
隐私区块与账本
公共交易（A，B，C，D）
节点A
公共交易
Blockchain Network
公共交易分发
节点B
节点C
节点D
共识区块与账本

隐私保护

账本加密



特性说明

1 账本数据加密

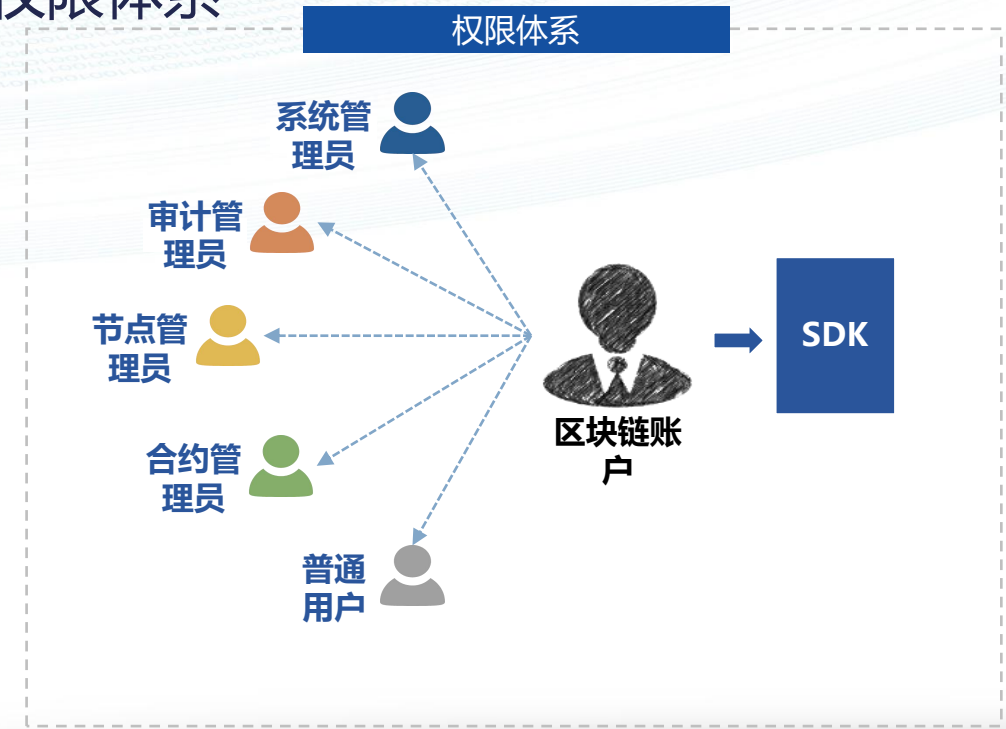
- 通过SGX（一种TEE可信执行环境）将业务数据加密签名，保证业务数据不可篡改，在节点服务器上不能被直接查询

2 节点密钥存储

- 针对节点私钥安全保护问题，通过SGX进行私钥存储，防篡改、防丢失

审计治理

权限体系



权限说明

1 系统管理员

- 负责链的协议、成员、配置管理

2 审计管理员

- 负责合规性监管

3 节点管理员

- 负责节点级别数据与配置管理

4 合约管理员

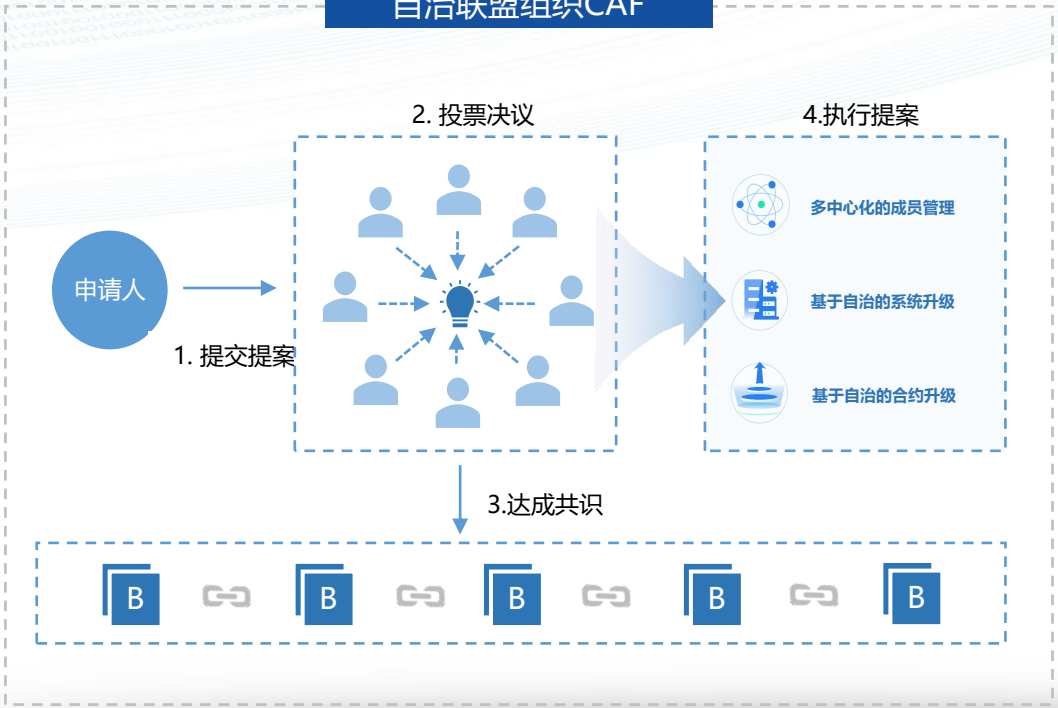
- 负责合约的生命周期管理

5 普通用户

- 负责业务应用相关操作

治理审计

自治联盟组织CAF



特性说明

1 定义

- CAF作为一种有效的联盟治理模式，其组织成员可通过提出提案、审议提案、最终决定某项提案通过与否

2 联盟自治可支持提案

- 成员管理
- 系统升级
- 合约升级

审计治理

区块链安全审计服务

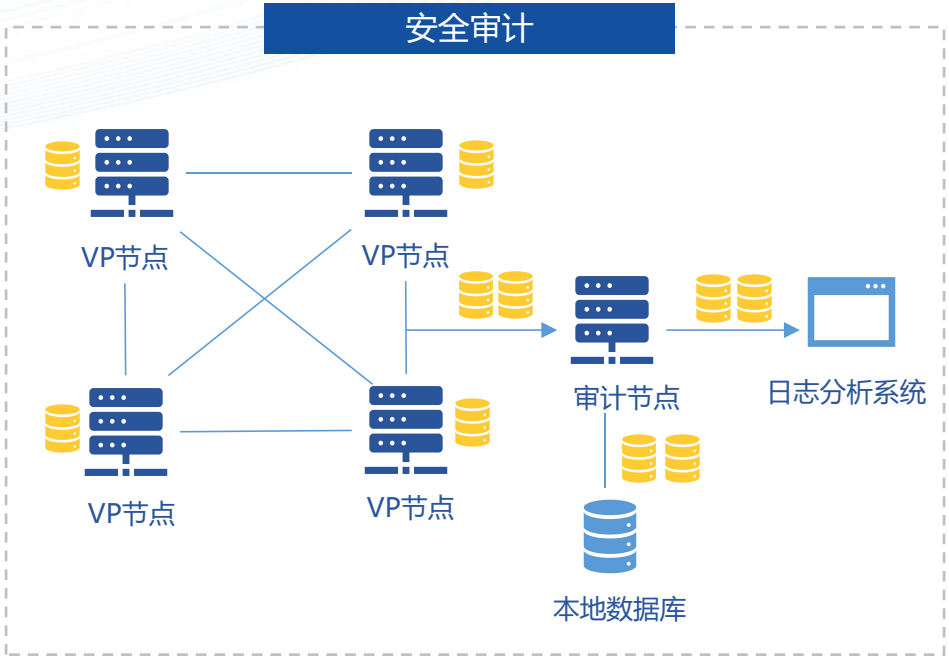
特性说明

1 安全审计

- 通过**审计节点**获取全量审计数据+**审计日志分析系统**，支持审计方进行实时精确的证据采集工作。
- 完全符合**央行《金融分布式账本技术安全规范》**中审计相关要求
- 审计数据再本地加密存储，保障安全性

2 审计内容

- 审计内容包括全量业务数据、数据变更及访问记录、系统事件、审计动作记录等



合约安全审计

MeshSec合约安全

MeshSec合约安全服务

面向区块链开发者智能合约全生命周期管理平台

1 多重合约检测

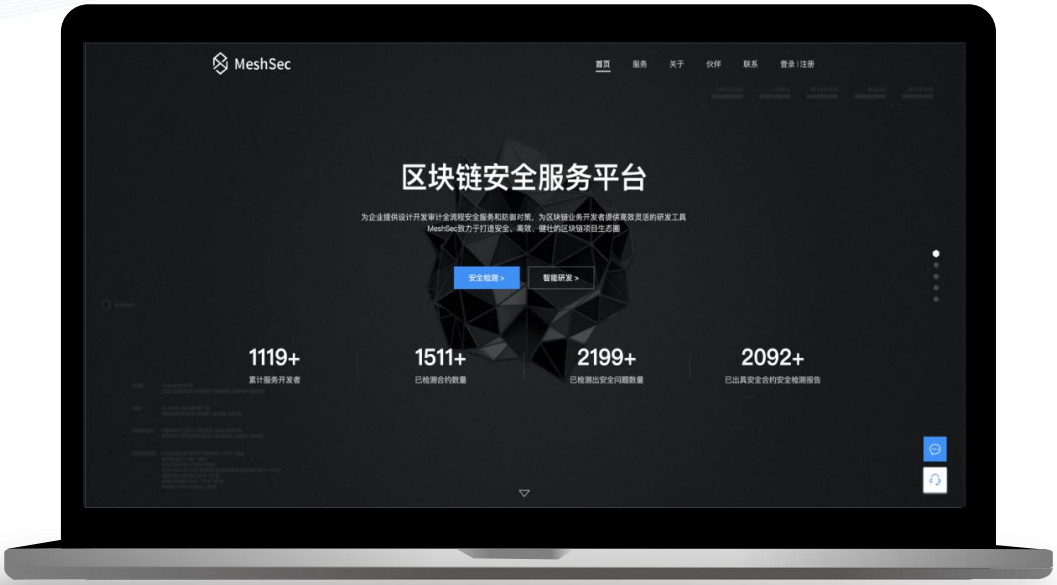
- 支持合约**在线编辑**、**编译运行**
- 静态分析，全面扫描语言漏洞
- 形式验证，业务代码深入分析

2 全方位安全服务

- 提供区块链合约全面安全服务和解决方案
- 合约安全打分，专业权威评级

3 多种服务形态

- 支持私有化部署，安全升级
- **公测版本**面向广大开发者**免费开放**



谢谢！