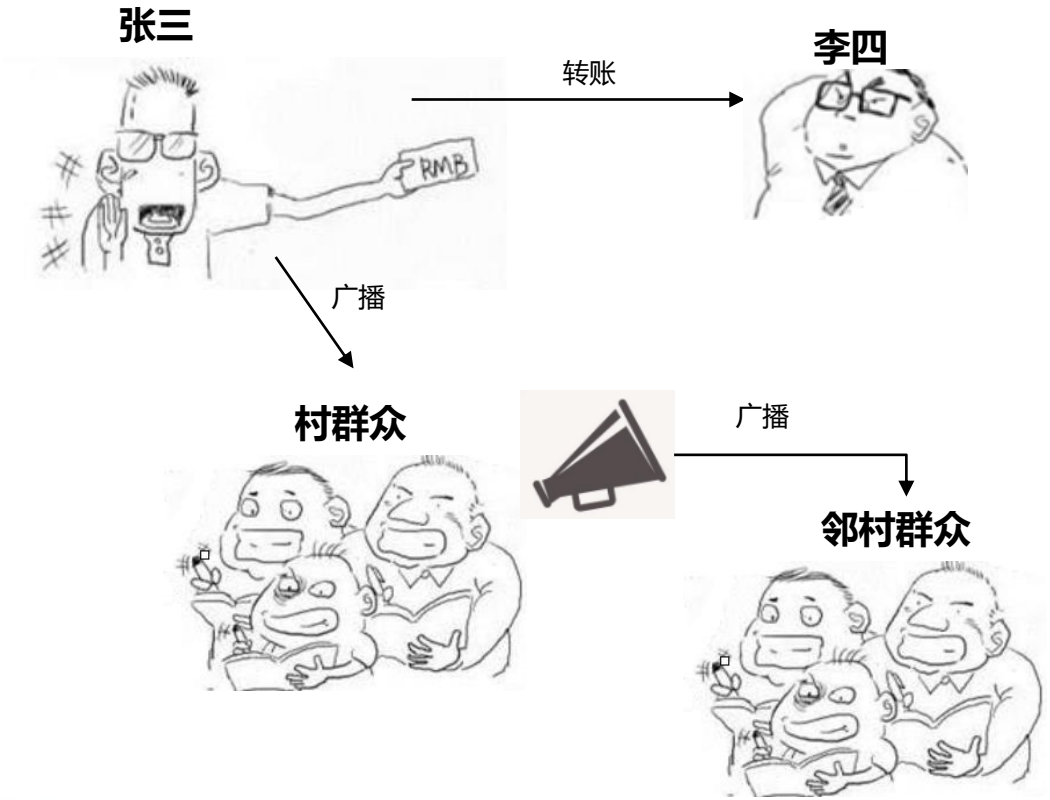
HUAWEI

区块链技术初探

比特币的通俗故事

故事：村里张三要给李四转1000元



1. 张三大吼一声：大家注意了，我用A账号给李四B账号转1000元；

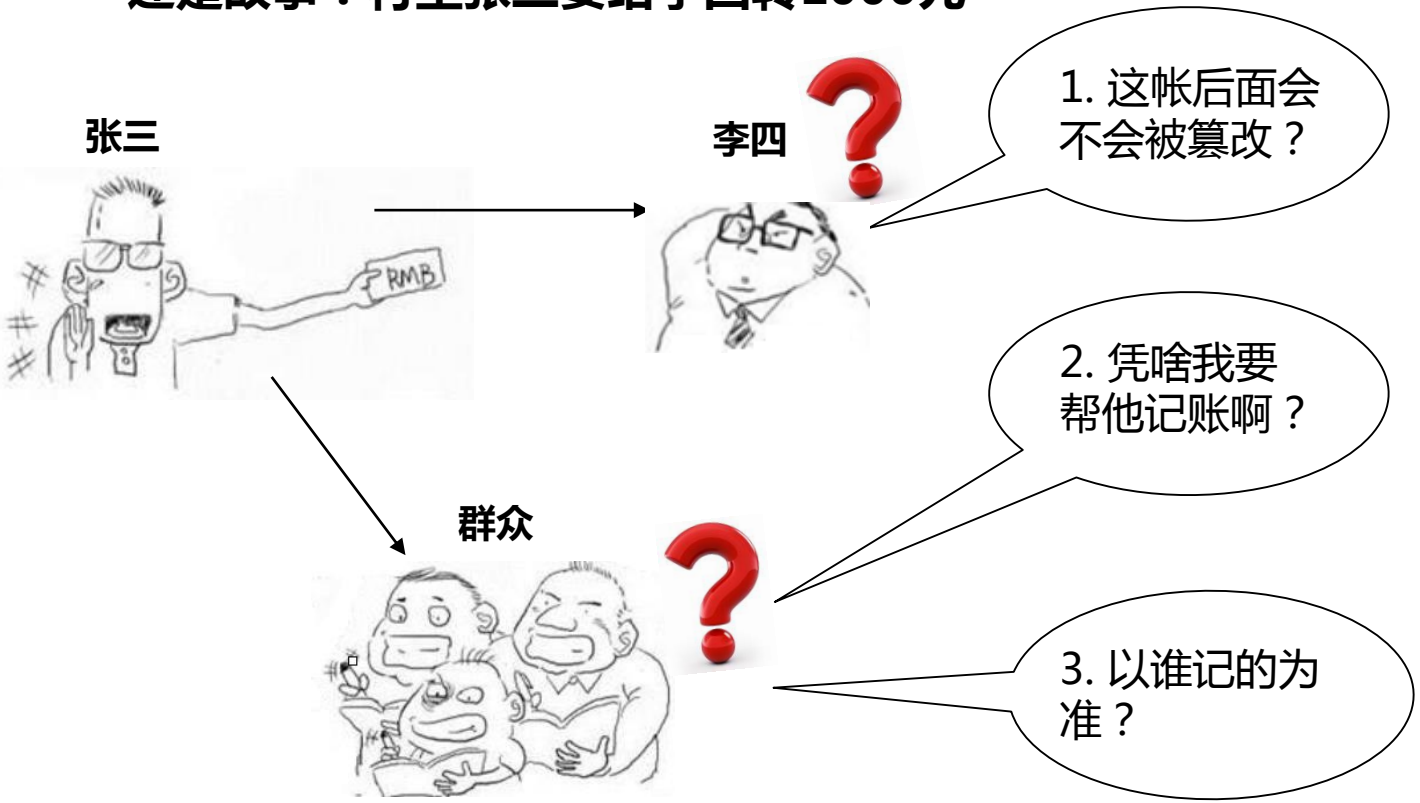
2. 张三附近村民听了确认是张三的声音，并且检查了张三的账号是否有足够余额；

3. 检查通过后，村民往自己的账本上写：A账号向B账号转账1000元比特币，A账号余额=3000-1000=2000元，B账号余额=2000+1000=3000元；

4. 张三附近的村民把转账告诉较远村民，一传十十传百，直到所有人都知道这笔转账，以此保证所有人账本的一致性；

故事并未结束…

还是故事：村里张三要给李四转1000元



采用特殊账本

区块+链
帐不可篡改

被认可第一个记账的奖励50元

矿工激励
维护系统安全

张三喊的时候，村民从村里题库找一个难题，谁破解了难题就以谁记的为准，并奖励50元，其余的人以他记的帐为准

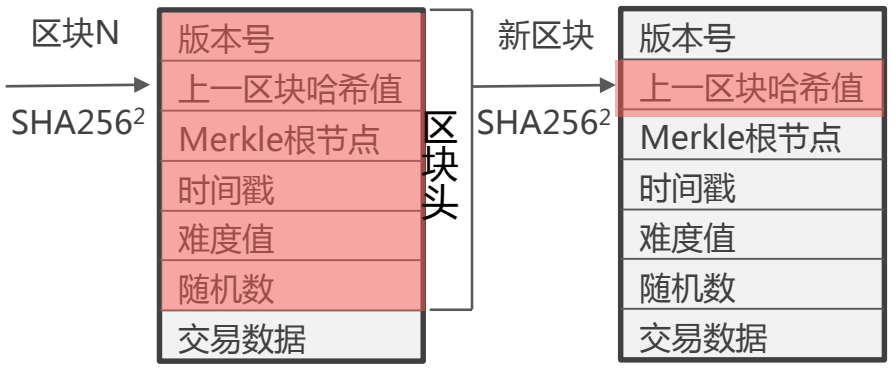
矿工挖矿
保持数据一致

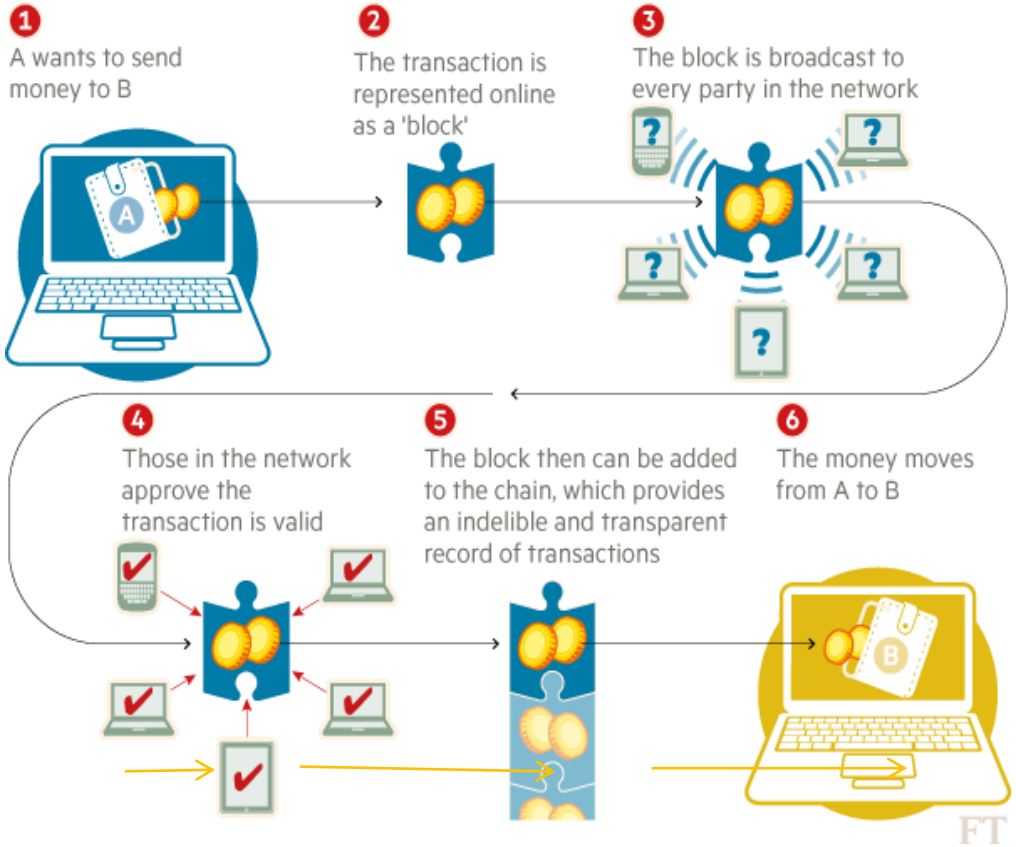
比特币通过分布式账本保障不可篡改，通过激励保证链自动安全运行，通过矿工挖矿解决记账一致性

区块链的基本概念

区块链主要运用了四个基础技术，即哈希运算（SHA256）、数字签名、P2P网络和共识算法，达成信用系统自动化、价值转移自动化、合约自动化，解决多方信任与高效协同问题。

区块(Block) + 链(Chain) = 区块链(Blockchain)

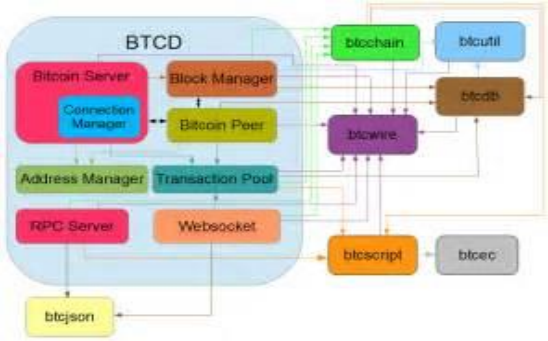




- 数据以区块（block）为单位产生和存储，并按照**时间顺序连成链式（chain）数据结构**
- **所有节点共同参与区块链系统的数据验证、存储和维护**。新区块的创建需得到共识确认，并向各节点广播实现全网同步，之后就不能更改或删除。

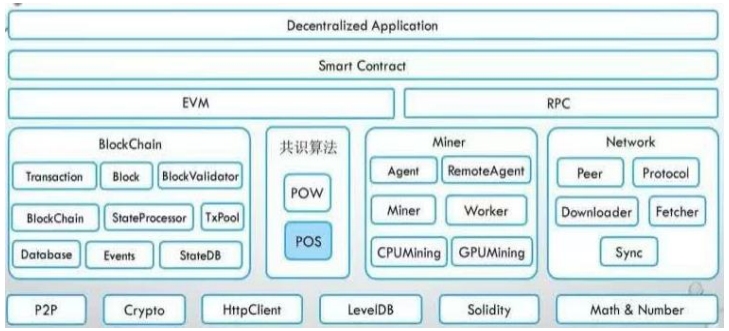
从三种主流方案技术框架变迁看区块链技术演进

1.0: 比特币专用系统-2009



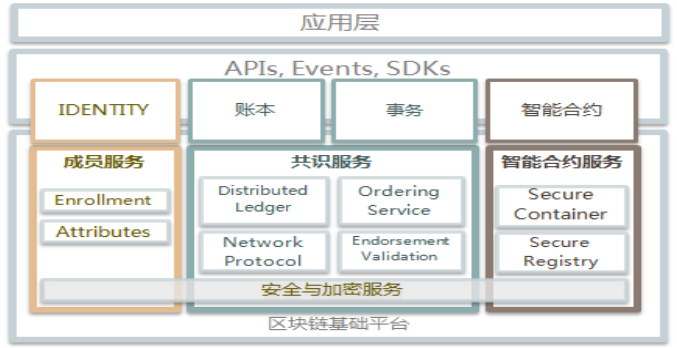
- 分布式账本
- 密码学：加密/签名
- 挖矿/PoW共识
- 简单脚本(非完备)

2.0:以太坊延伸至数字资产-2013



- + 智能合约 /语言/ EVM/ Gas
- + 账号支持
- * 改进的PoW

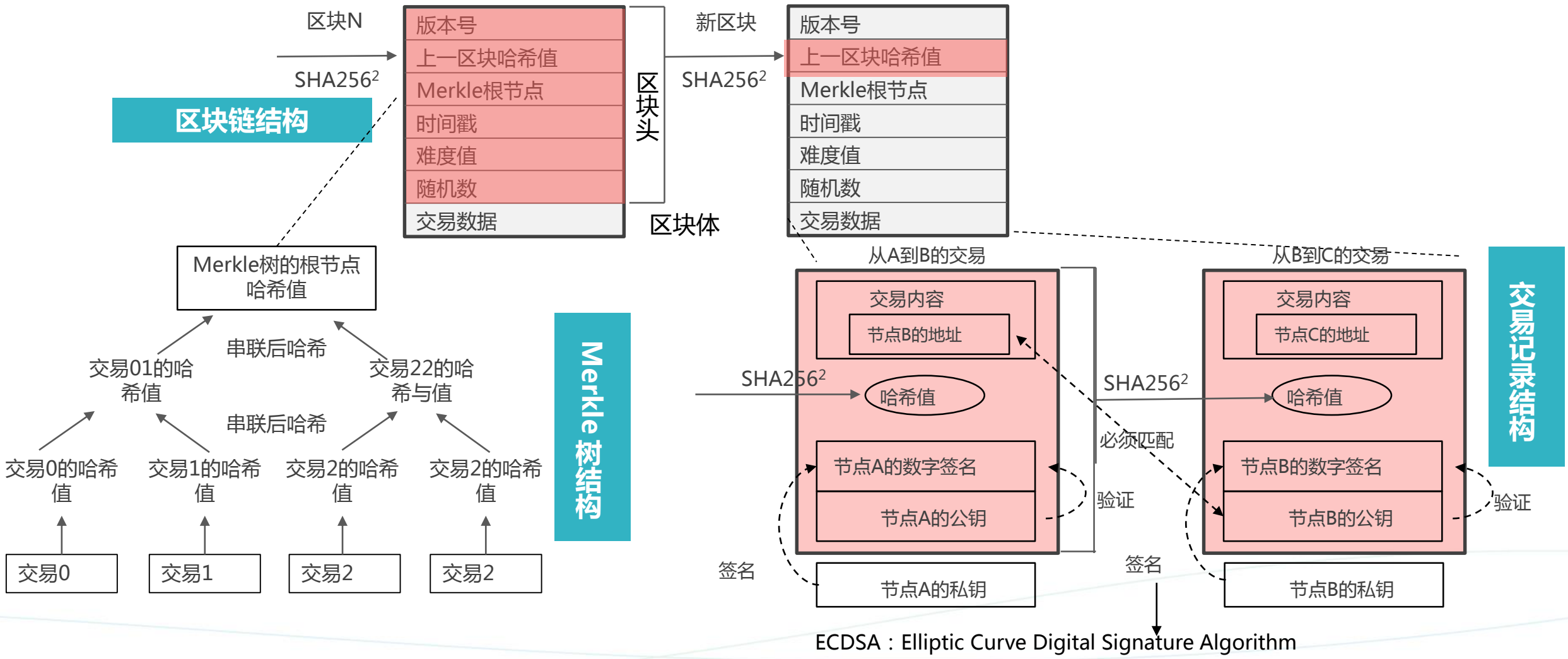
3.0: Hyperledger除货币外其他企业领域-2015



- + 成员管理、接入认证
- + 插件式共识：PBFT/Paxos/Raft,
- + 分区/channel
- * 性能及扩展性更好

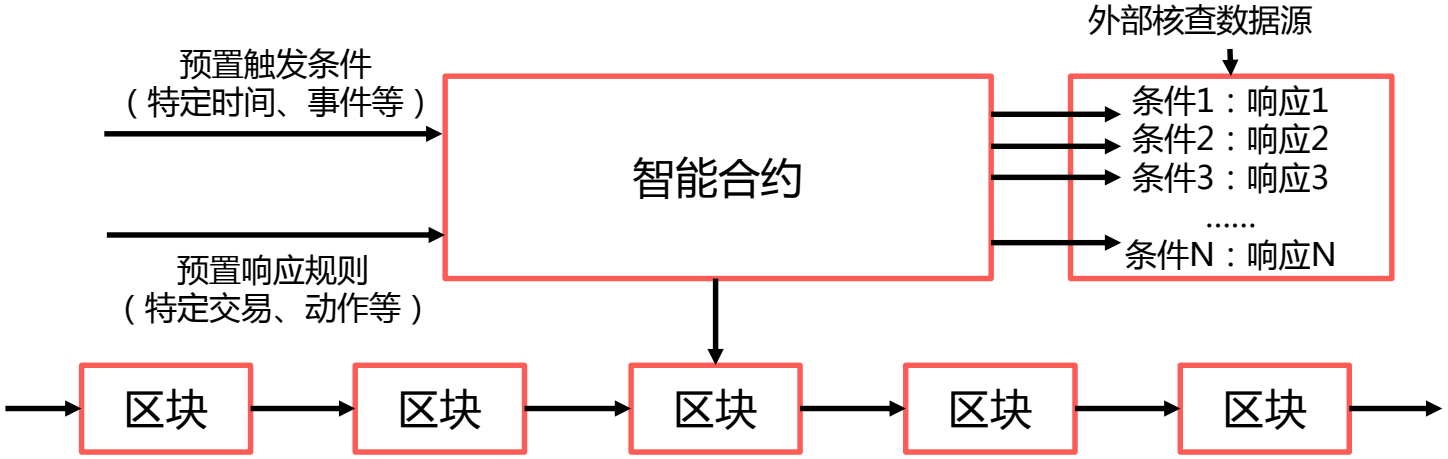
关键技术	技术点	比特币	以太坊	Hyperledger Fabric
	有无内置代币	有	有	无
分布式共识	共识算法	Proof of Work	改进的Proof of Work， PoS	PBFT/pluggable架构
	出块速度	约10分钟	平均十几秒	可配置
分布式账本	数据存储	File+LevelDB	File+LevelDB	File+LevelDB/CouchDB
分布式P2P网络	分区、channel	无	无	可配置的分区、channel
智能合约	合约运行环境	简单脚本引擎	Ethereum Virtual Machine（EVM）	Docker
	合约语言	脚本（非完备）	Solidity	Go/Java
	组织形态	公有链	公有链	联盟链

区块链的哈希/签名机制


区块链结构
区块N
SHA256²
版本号
上一区块哈希值
Merkle根节点
时间戳
难度值
随机数
交易数据
区块头
区块体
新区块
SHA256²
版本号
上一区块哈希值
Merkle根节点
时间戳
难度值
随机数
交易数据
Merkle树的根节点
哈希值
串联后哈希
串联后哈希
交易01的哈希值
交易22的哈希与值
交易0的哈希值
交易1的哈希值
交易2的哈希值
交易2的哈希值
交易0
交易1
交易2
交易2
Merkle 树结构
从A到B的交易
从B到C的交易
交易内容
节点B的地址
交易内容
节点C的地址
SHA256²
哈希值
SHA256²
哈希值
必须匹配
节点A的数字签名
节点A的公钥
节点B的数字签名
节点B的公钥
验证
验证
签名
签名
节点A的私钥
节点B的私钥
交易记录结构
ECDSA：Elliptic Curve Digital Signature Algorithm

链码（智能合约）的基本概念

智能合约是由事件驱动的、具有状态的、存储和运行在区块链上的程序



今天凌晨2:45，欧冠皇马VS拜仁慕尼黑

↓

发布一个智能合约，皇马赢，小明给我1000元；拜仁赢，我给小明1000元

↓

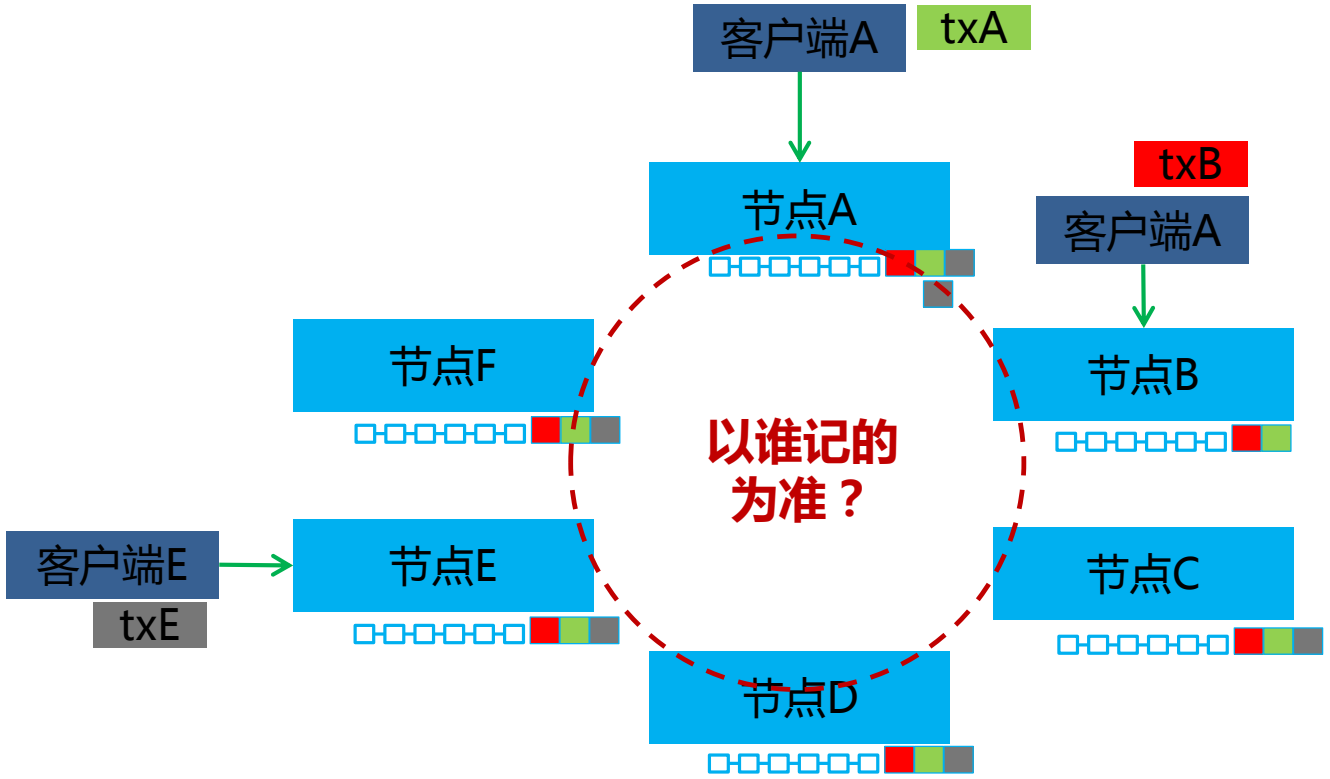
比赛结果发布，皇马4:2拜仁。触发智能合约响应条件

↓

履行智能合约，将小明的1000元打入我的账户

共识算法

解决的问题：多人共同记账，**以谁记的为准？**



- **出个猜谜题谁先猜出来给谁？**
  - ✓比特币工作量证明
- 每隔一段时间**选个组长，大家举手表决是否同意组长的记账**？
  - ✓实用拜占庭容错协议
- 利用**可信硬件掷骰子**，选数字最小的？
  - ✓最小幸运数算法

华为云区块链服务

聚焦区块链生态建设，与合作伙伴深度合作

一键上链

通过管理界面设置区块链的初始参数，数分钟内部署完整区块链系统

成本低廉

- 按需付费，无一次性大投入
- 业务扩展容易，降低边际成本和时间周期

安全隐私

- 云安全全栈防护，私密网络
- 零知识证明和隐私保护
- 同态加密加密数据

高性能

- 秒级共识，受理和共识分离
- 可水平扩展，共识可达每秒2000+TPS

HUAWEI

所有成员共享账本的区块链系统

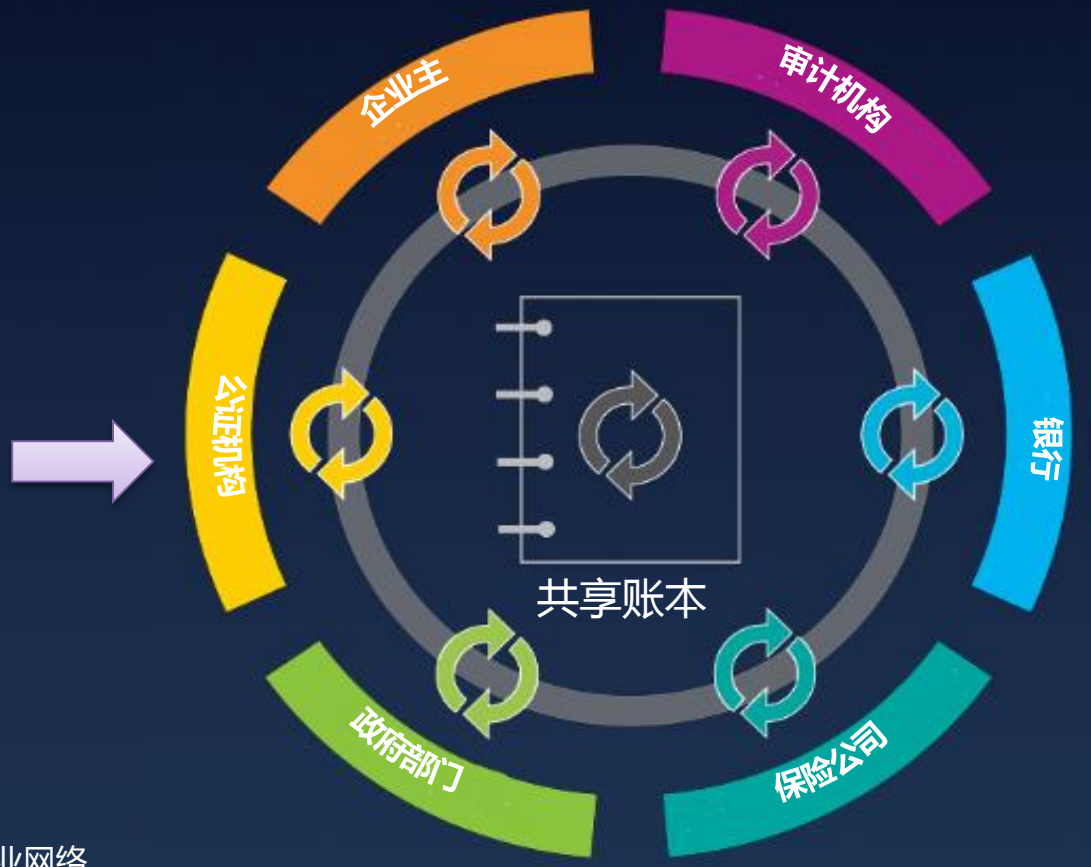
技术组成

只可添加
共享账本

账本修改需共识
共识算法

哈希、公私钥对
安全隐私

可编程，图灵完备
智能合约



区块链系统价值

提高效率

降低成本

降低风险

促进互信

- 共享账本：区块链架构使每一个商业网络的参与方共享同一帐本，当交易发生时，通过点对点的同步更改所有账本
- 安全隐私：使用密码算法确保网络上的参与者仅仅可以看到和他们相关的账本内容，确保交易的安全、授权和验证性。

去中心化，共识，可信，不可篡改，可追溯

- 智能合约：区块链也将资产转移交易相关的合同条款嵌入交易数据库以做到满足商务条件下交易才发生
- 共识算法：网络参与者基于共识机制来保证交易是共同验证的。商业网络满足政府监管、合规及审计

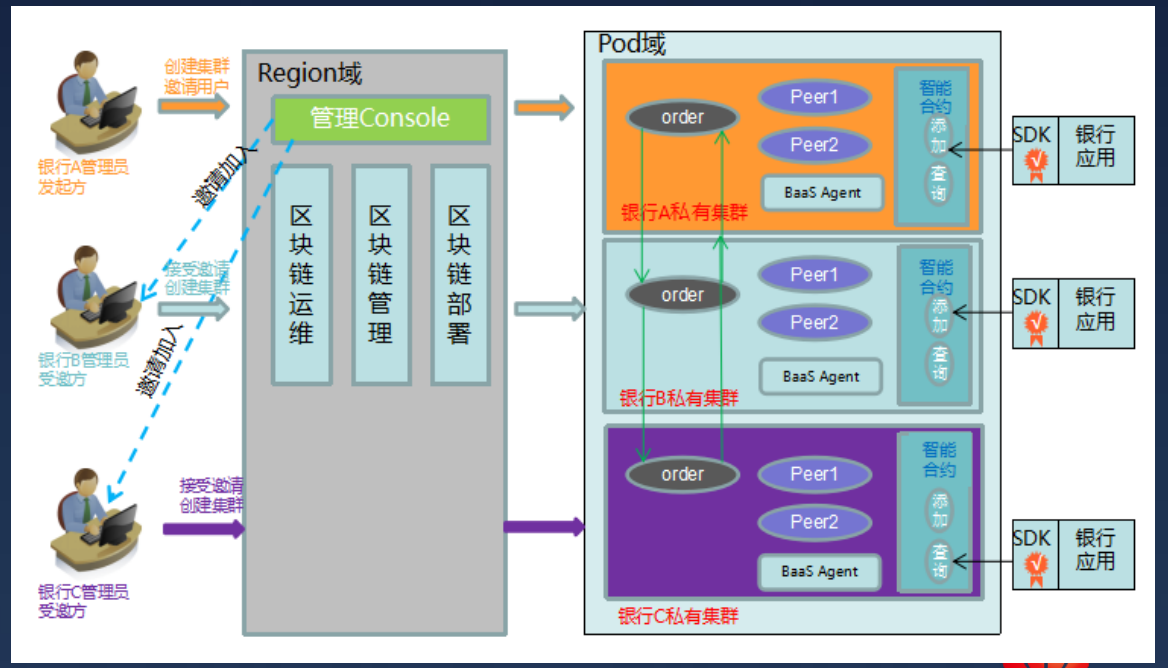
HUAWEI

华为云区块链服务 - 帮助客户在华为云上快速、低成本的创建、部署和管理区块链应用

- **基于hyperledger1.0搭建的联盟链：多中心、权限控制、隐私保护、复杂智能合约和高效共识**
- **高性能：使用快速拜占庭容错共识算法（FBFT），具备高吞吐量和低系统延时**
  交易吞吐量大于2000 TPS，系统延时小于200毫秒 - 节点机器16核32G内存
- **高可用：通过邮件邀请机制实现成员动态扩容，节点使用容器部署，可实现节点弹性伸缩和快速恢复机制**
- **高安全、隐私：多级加密、国密支持、同态加密、VPC物理隔离、通道账本共识隔离等**
- **多语言可编程：支持Go、Java和NodeJS语言编写智能合约**

逻辑架构图

集群部署模式



HUAWEI

可持续商用区块链网络设计原则

1 高性价比	• 快速搭建，屏蔽技术细节 • 高效运营，区块链系统全生命周期管理
2 高性能	• 高性能共识算法和海量存储，支持秒级确认和千级以上TPS • 电信级网络，高速网络传输能力，低延时
3 高可用	• 成员动态准入 • 节点弹性伸缩和快速故障恢复
4 安全隐私	• 节点成员准入控制，国家安全标准支持，记录可靠一致 • 拥护和业务数据隐私保护，安全的秘钥体系管理
5 可编程	• 图灵完备且安全的智能合约引擎 • 复杂、多语言智能合约支持 • 支持SQL访问和存储共享账本
6 快速接入	• 多种接入方式，满足各种用户需求 • 开放访问和全球协作网络支持

HUAWEI

高性价比：一键上链、区块链系统全生命周期管理

全方位、全生命周期区块链企业应用解决方案一站式规划、采购、配置、开发、上线和运维

1 创建区块链服务 —— 2 管理链代码 —— 3 业务应用访问区块链系统 —— 4 区块链服务运维

配置基本参数和各节点参数

编写链代码、链代码上传、链代码实例化

下载SDK到业务应用、通过SDK调用链代码

区块链服务运维。查看区块链服务节点运行状态、监控告警、升级、弹性伸缩等

一键上链，节约80%的开发、部署成本；按需付费，统一运维和管理，减少60%的初始和运行成本

服务名称	服务状态	容器集群	共识策略	创建时间	操作
bcsdemo	运行	bcs-demo	快速拜占庭容错共识算法	2018-02-22T14:53:49+08...	更新版本 链代码管理 下载SDK配置 删除

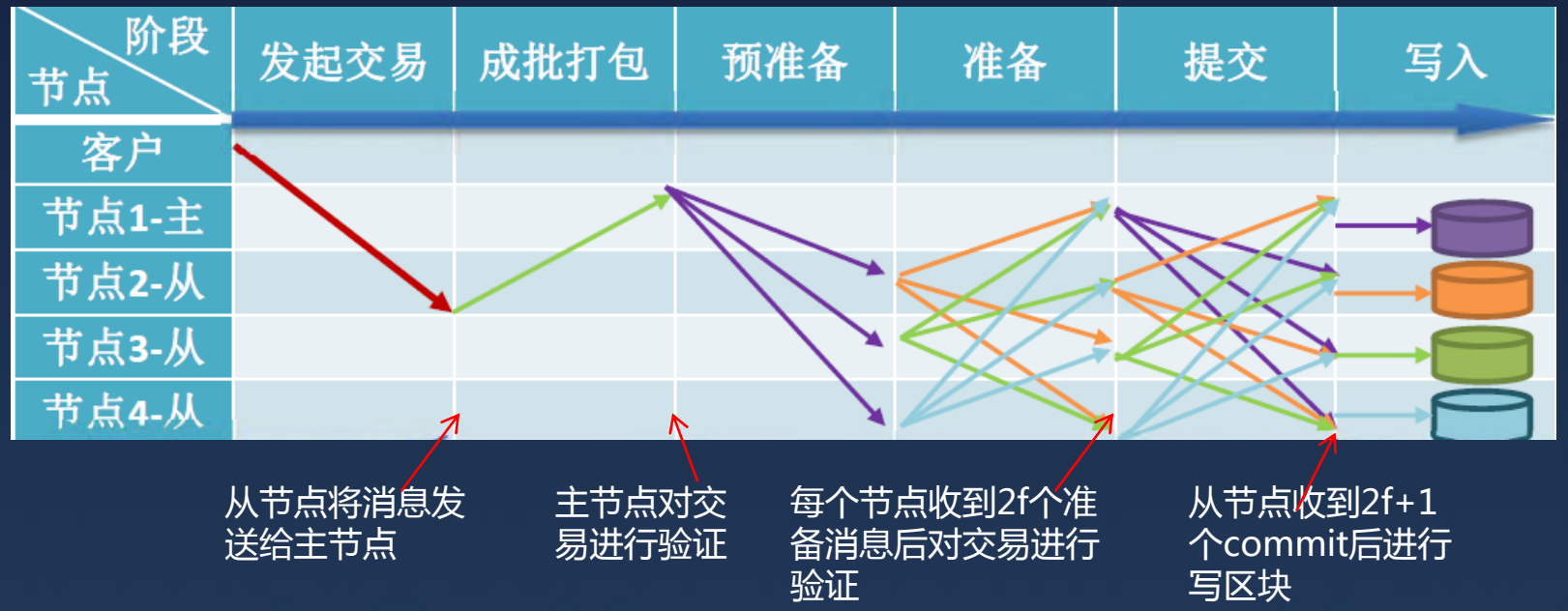
组织名称	组织状态	组织类型	实例数量	操作
bcsdemo-orderer	运行	共识	4	下载管理员证书
bohaibank	运行	节点	2	下载管理员证书 下载用户证书
tianjinbank	运行	节点	2	下载管理员证书 下载用户证书
baotoubank	运行	节点	2	下载管理员证书 下载用户证书

HUAWEI

高性能：提供多种安全、高效共识算法，按需选择

共识算法	SOLO	kafka（CFT）	FBFT
节点数	1	2f+1	3f+1
错误节点容忍	不容忍	最多1/2个crash节点	最多1/3个拜占庭错误节点
交易性能	一般	10000+TPS	2000+TPS

– 快速拜占庭容错算法（Fast Byzantine Fault Tolerance ）



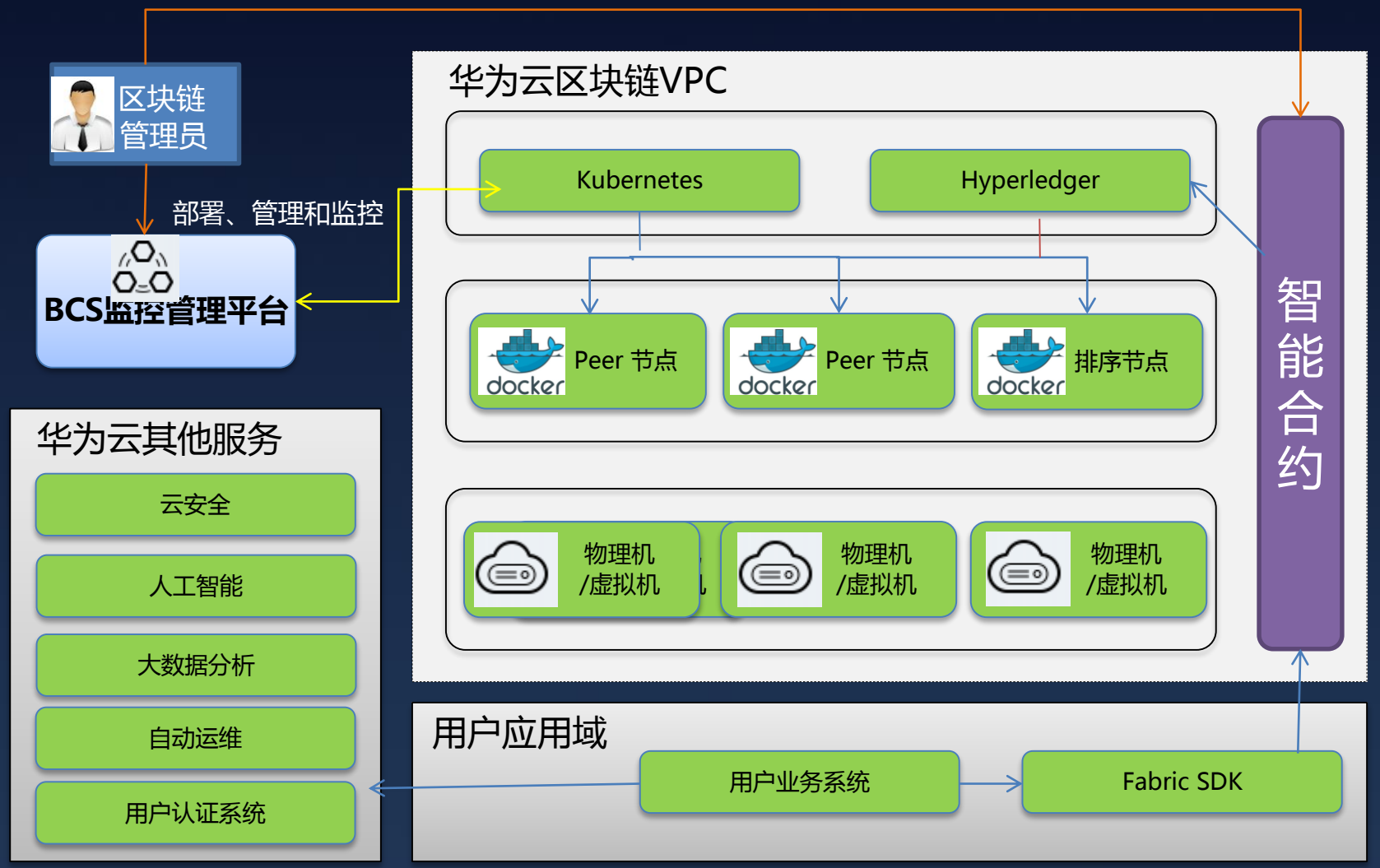
关键技术

用户可以根据不同的使用场景以及安全和性能等不同需求选择共识算法

- **SOLO模式**：只需要一个共识节点，简单、快速，建议在开发测试环节使用
- **kafka/Zookeeper**：高速共识算法，1:n个节点，能容忍crash节点；
- **FBFT**：快速拜占庭容错算法，使用3f+1个节点，能容忍最多1/3拜占庭错误节点。

HUAWEI

高可用：成员动态准入，节点弹性伸缩和快速故障恢复



关键技术

构建于 Docker 和 Kubernates 之上，具备极高的可靠性和扩展性，与其他云服务完全打通，无数据膨胀和性能等问题

- **成员动态加入**：通过邀请机制可快速、动态添加联盟链成员。
- **节点弹性伸缩**：通过K8S实现节点弹性伸缩和快速故障恢复
- **灵活部署**：同时支持私有链和联盟链部署方式，规划支持混合部署模式
- **互联互通能力**：充分使用现有IT 基础设施，并连接周边生态和业务合作伙伴

HUAWEI

安全隐私：云平台+区块链全面安全隐私保护

云平台安全

华为云完整安全体系

基础设施安全

物理和环境安全　网络安全
云平台安全　数据安全

了解详情

服务安全

权限管理机制　网络隔离
外部防御攻击　数据安全

了解详情

运维运营安全

安全事件管理　漏洞管理
运维账号认证　集中日志管理
运维权限管理　运维接入安全

了解详情

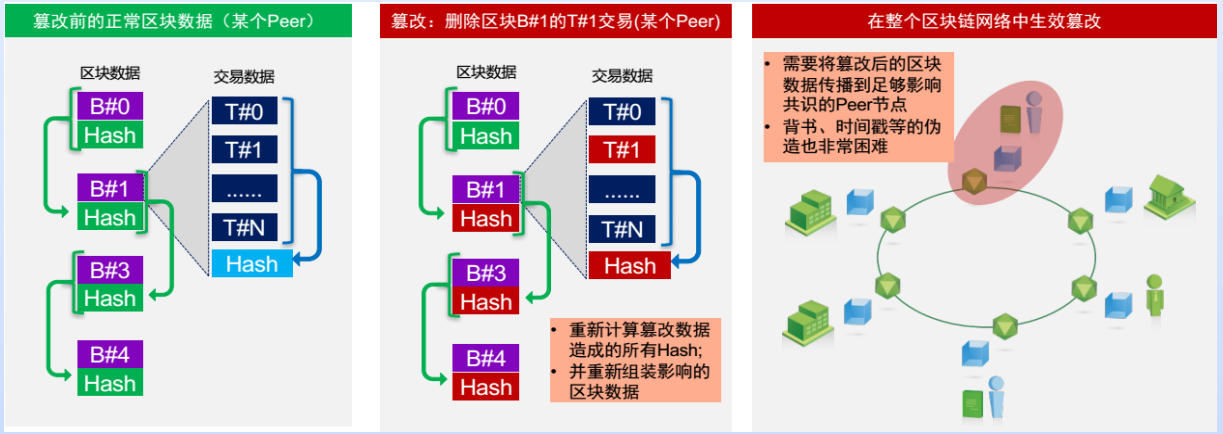
安全合规：获得多项权威认证，安全的云平台

CSA STAR 金牌认证　ISO 27001:2013　C-STAR　公安部信息安全等级保护三级

网信办网络安全审查试点　可信云认证　金牌运维　国际通用准则CC+EAL3+

区块链安全和隐私

防篡改



用户和交易数据隐私保护

快速接入：开放访问和全球协作网络支持，构建去中心化区块链网络

第一阶段：支持在华为云不同区域构建跨域区块链网络
第二阶段：和合作云（天翼云，德电云，法电云等）合作构建全球区块链网络

Thank You.

华为云区块链服务BCS

扫码关注