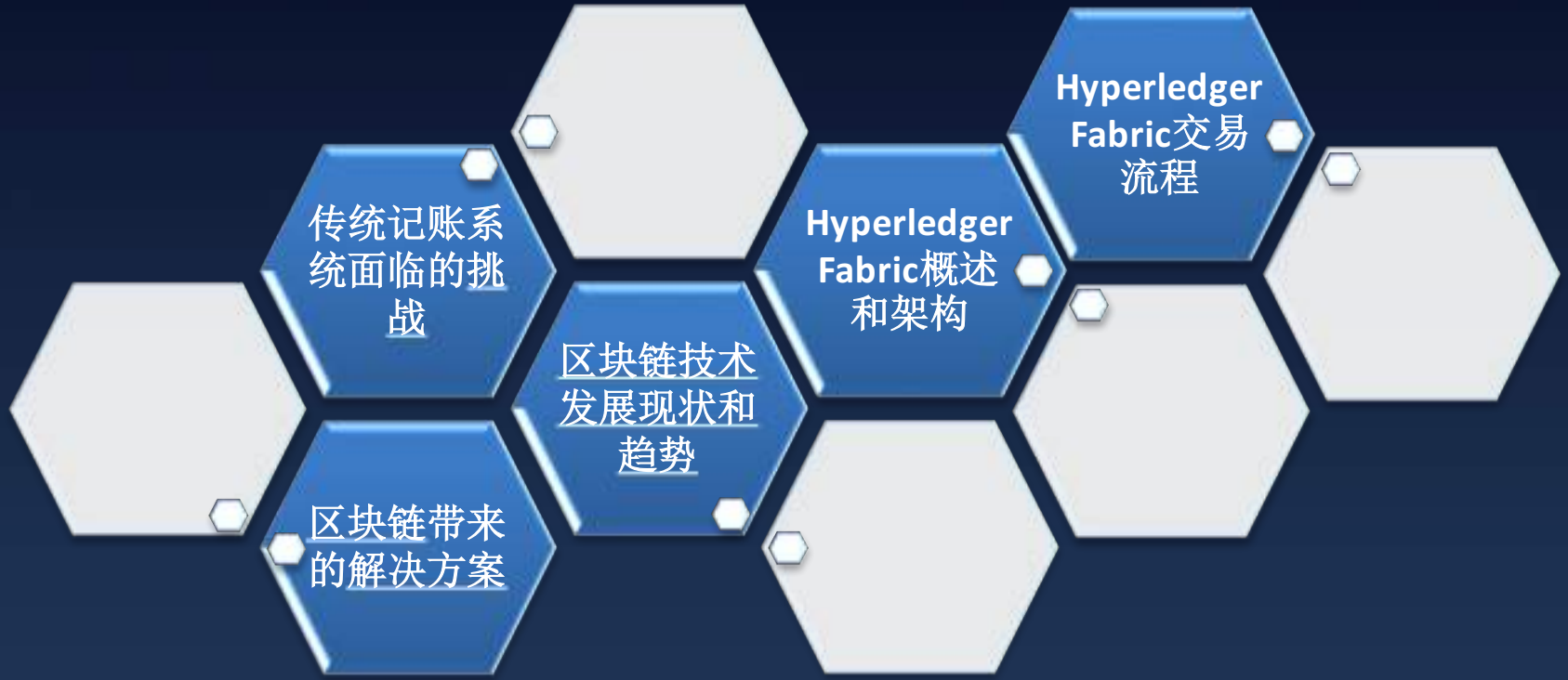
HUAWEI

区块链服务在公有云平台上的重要问题设计实现及解决办法

演讲者 / 张子怡

目 录

区块链介绍及选型说明


传统记账系统面临的挑战
区块链技术发展现状和趋势
区块链带来的解决方案
Hyperledger Fabric概述和架构
Hyperledger Fabric交易流程

在一个不互信的网络中如何高效协调跨机构交易的执行?

传统商业网络面临的挑战

- 每个参与方都有自己的账本，在交易发生时修改各自账本
- 为了协同各参与方需要增加中介等额外的工作及附加成本
- 由于业务条件（合同）-重复分散在各个参与方造成整体业务流程的低效
- 整个业务网络依赖于一个或几个中心系统，一旦中心系统发生问题如欺诈、网络攻击或错误将导致整个商业网络混乱

…效率低下, 成本高, 易遭攻击

复杂账本

HUAWEI

解决方案：所有成员共享账本的区块链系统

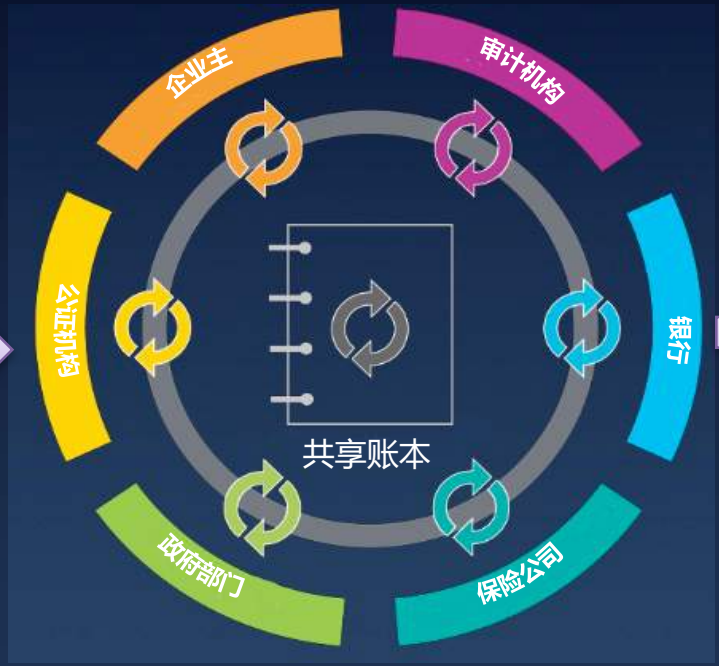
技术组成

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
- 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

多中心化，共识，可信，不可篡改，可追溯

- 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。
- 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

HUAWEI

区块链技术发展现状和趋势

按许可性质分类

账本全公开
任何参与者可见
参与者都是匿名

账本联盟组织内公开
可实名参与过程
可满足监管AML/KYC

账本不公开
组织内可见

区块链技术演进

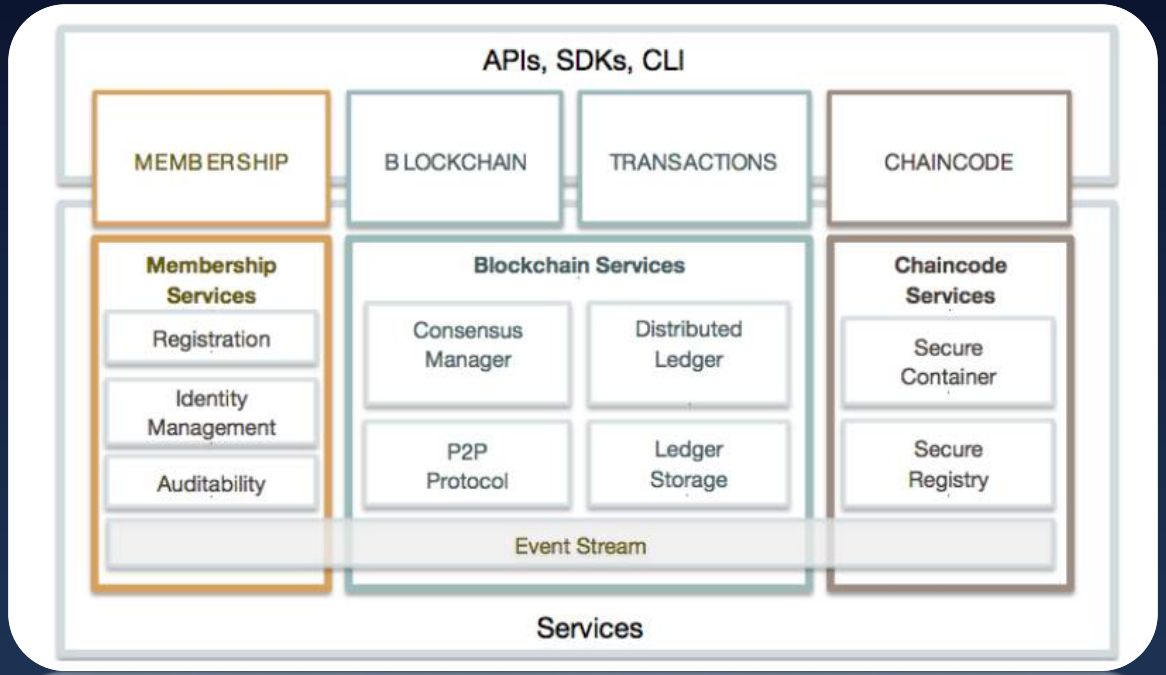
联盟链在合规性、隐私保护，复杂合约和交易效率有非常大的领先优势

HUAWEI

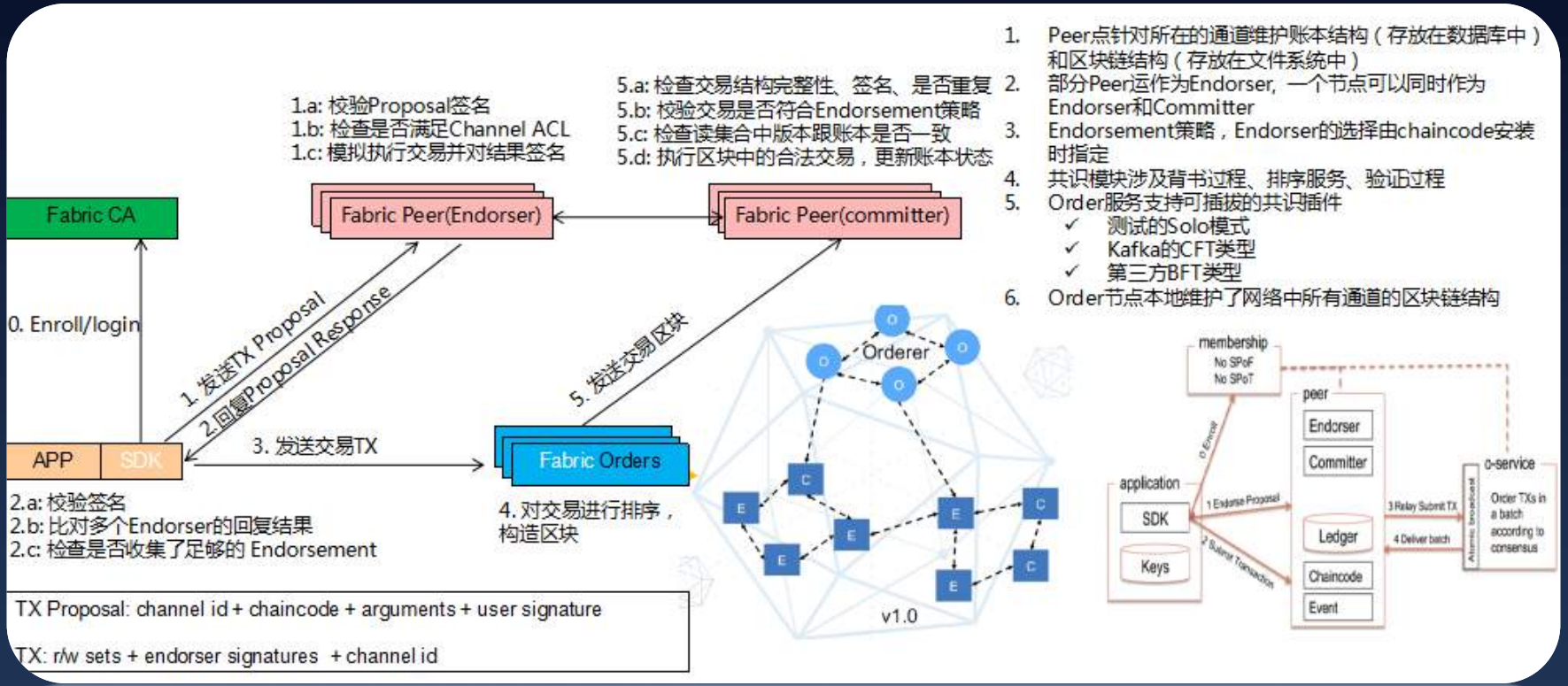
Hyperledger fabric概述和架构

基本概念

- 身份认证： 插件式， 身份管理，隐私和交易审计
- 账本：分布式事物的账本状态在各个参与方达成共识下可以更新
- 智能合约：可编程的账本，提供可以在区块链上运行的业务逻辑
- APIs, SDKs, CLI: 支持多语言的SDK可以使擅长不同语言的研发开发自己的链上应用
- Peer：维护账本状态和管理链码的网络中的节点
- Orderer：共识节点，提供原子广播，使用可插拔的共识引擎
- 通道：数据划分机制来控制交易只对参与方可见，共识只在通道成员中发生

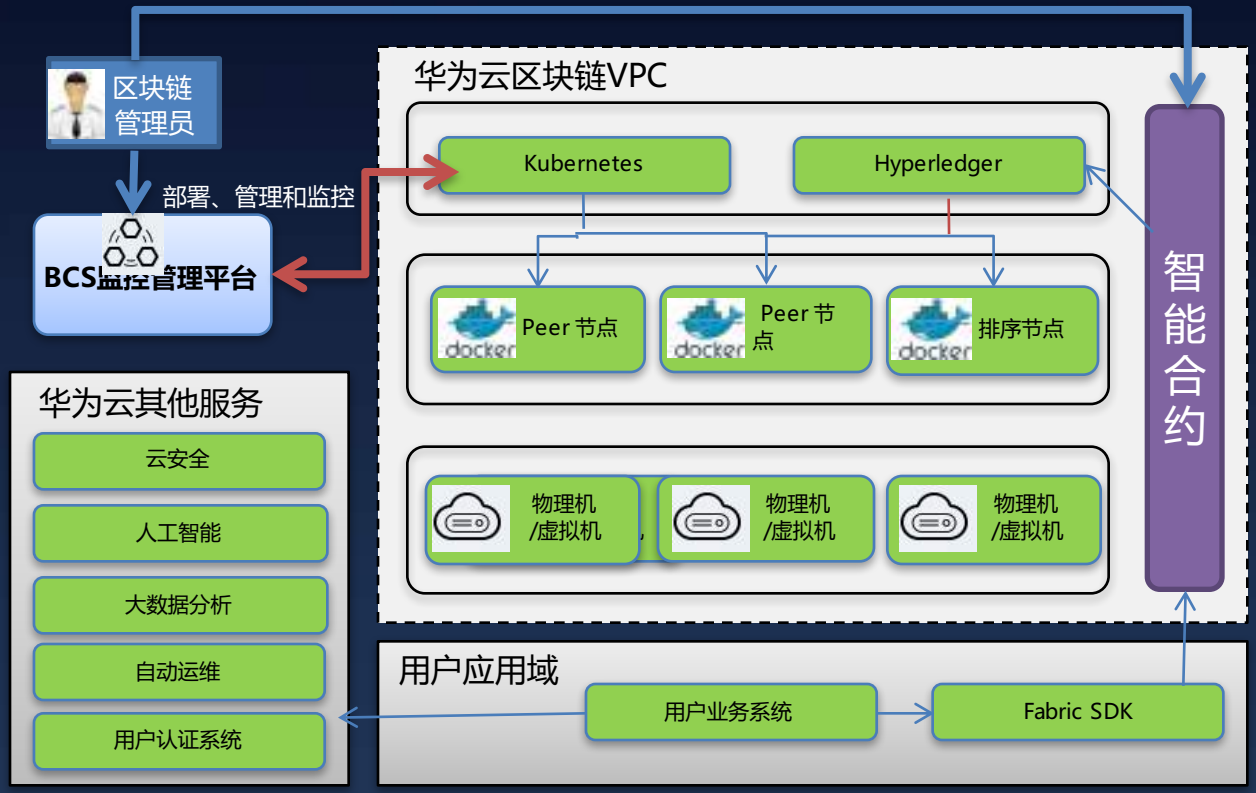


Fabric交易流程


1.a: 校验Proposal签名
1.b: 检查是否满足Channel ACL
1.c: 模拟执行交易并对结果签名
5.a: 检查交易结构完整性、签名、是否重复
5.b: 校验交易是否符合Endorsement策略
5.c: 检查读集合中版本跟账本是否一致
5.d: 执行区块中的合法交易，更新账本状态
Fabric CA
Fabric Peer(Endorser)
Fabric Peer(committer)
0. Enroll/login
1. 发送TX Proposal
2. 回复Proposal Response
5. 发送交易区块
APP
SDK
3. 发送交易TX
Fabric Orders
2.a: 校验签名
2.b: 比对多个Endorser的回复结果
2.c: 检查是否收集了足够的 Endorsement
4. 对交易进行排序，构造区块
TX Proposal: channel id + chaincode + arguments + user signature
TX: r/w sets + endorser signatures + channel id
Orderer
v1.0
1. Peer点针对所在的通道维护账本结构（存放在数据库中）和区块链结构（存放在文件系统中）
2. 部分Peer运作为Endorser，一个节点可以同时作为Endorser和Committer
3. Endorsement策略，Endorser的选择由chaincode安装时指定
4. 共识模块涉及背书过程、排序服务、验证过程
5. Order服务支持可插拔的共识插件
✓ 测试的Solo模式
✓ Kafka的CFT类型
✓ 第三方BFT类型
6. Order节点本地维护了网络中所有通道的区块链结构
membership
No SPoF
No SPoT
peer
Endorser
Committer
application
SDK
Keys
Ledger
Chaincode
Event
0-service
Order TXs in a batch according to consensus
1 Endorse Proposal
2 Submit Transaction
3 Relay Submit TX
4 Deliver batch
Atomic broadcast

目 录

华为平台架构



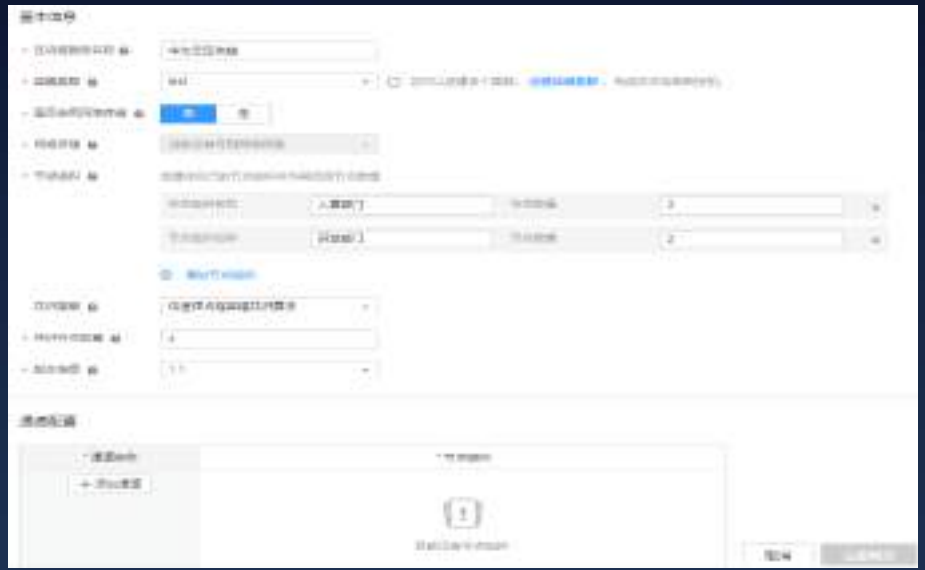
关键技术

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

高性价比：一键上链、区块链系统全生命周期管理

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；



一键快速部署区块链系统：
相对自建区块链：部署时间从天级降至分钟级

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

可编程：可视化智能合约生命周期管理，多语言支持

1、智能合约基础

2、高效、安全的智能合约引擎

- 支持Go、Java和NodeJS编写智能合约
- 使用Docker安全容器运行智能合约引擎
- 对智能合约引擎的威胁和逃逸行为进行全面监控

3、可视化智能合约生命周期管理

链代码查看

链代码安装

链代码实例化

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

安全合规：获得多项权威认证，安全的云平台

区块链安全和隐私

防篡改

用户和交易数据隐私保护

BCS安全隐私支持：国密支持、加法同态和零知识证明等