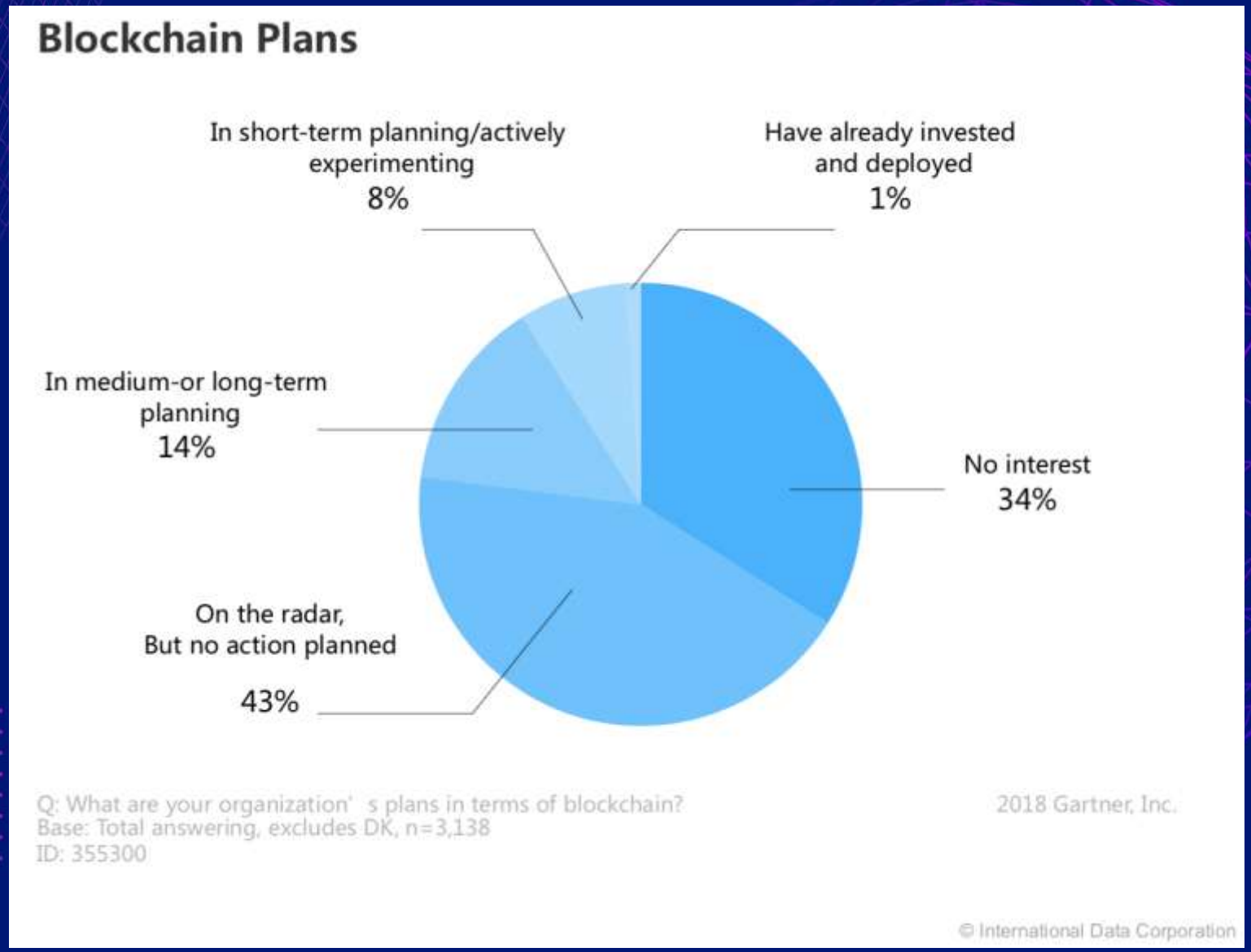
HyperLedger Fabric 在携程区块链平台中的应用实战

演讲人：何鑫铭

何鑫铭

携程技术中心创新研发部区块链技术专家、架构师，携程区块链技术平台技术负责人，精通HyperLedger Fabric、Ethereum、Tendermint等开源区块链技术框架。

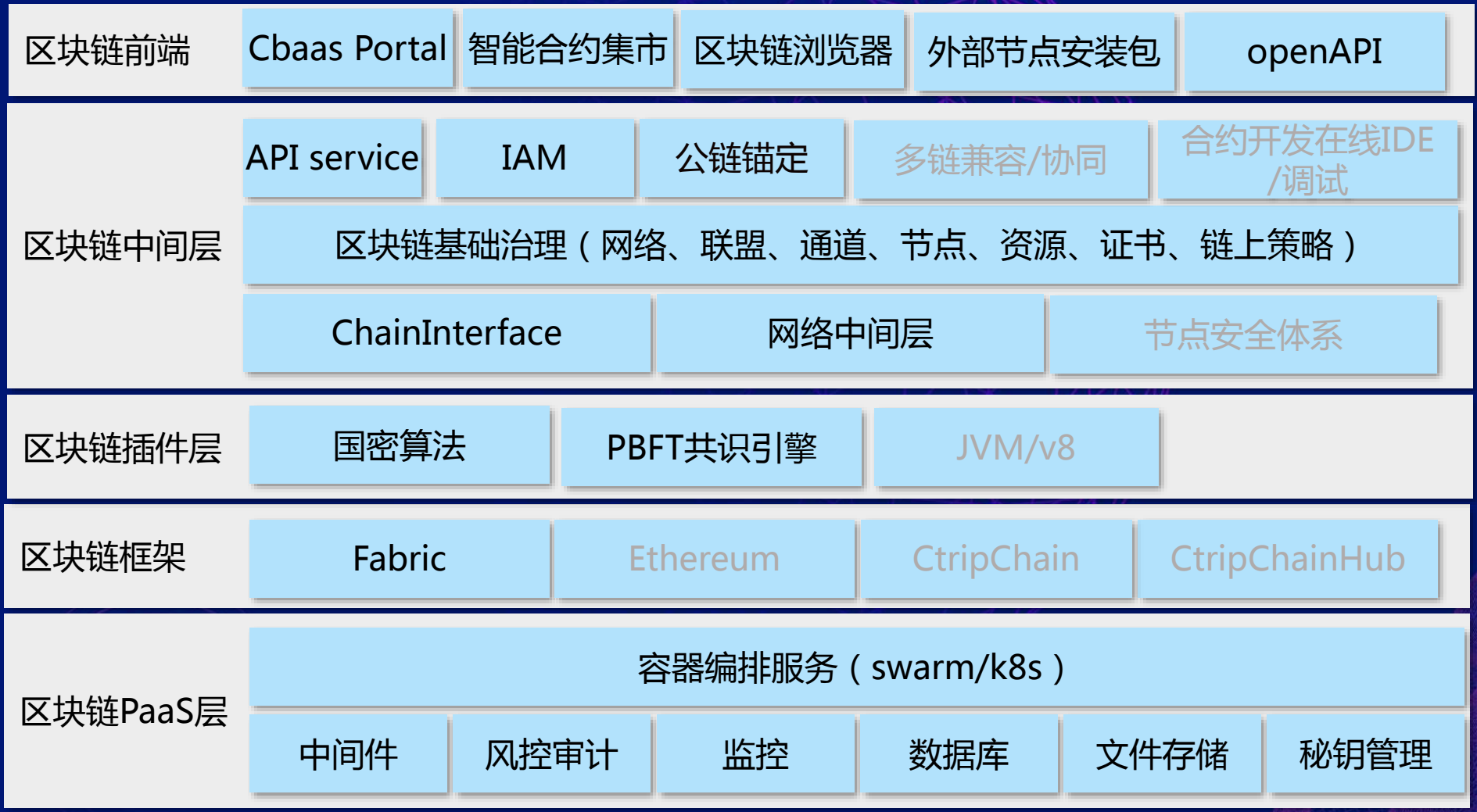
区块链普及普惠的主要障碍



- 开发、部署、运维成本高
- 公有链、私有链、联盟链架构标准多且复杂
- 企业缺乏工程落地经验，各个行业缺乏标准

1 .携程CBaas（Ctrip Blockchain as a service）区块链服务平台的整体介绍

携程CBaas区块链服务平台技术栈



携程CBaas区块链服务平台的整体介绍

2 .HyperLedger Fabric的架构与设计理念

HyperLedger Fabric的架构与设计理念

联盟链：联盟链用于既定商业用途的区块链网络，具备成员需要实名准入的特点。

网络（network）：指一套完整区块链网络。

通道（channel）：fabric对于子链的实现方式，每个通道间数据物理隔离，一个联盟下可以有多个通道.

链码（chaincode）：fabric对于智能合约的实现方式，是由高级语言开发的链上执行程序。

HyperLedger Fabric的架构与设计理念

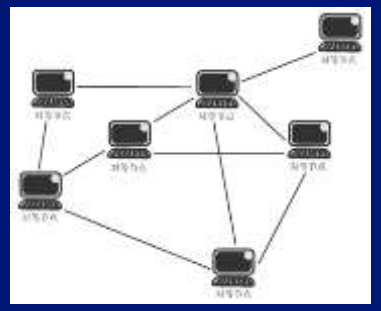
智能合约执行引擎

docker ...

Container as a VM

智能合约开发语言

Gossip P2P网络



Grpc protocol

Kafka共识(CFT)

intermediate CA

Root CA

CA密钥证书
基础设施

底层数据账本

账本索引
LevelDB

历史数据
LevelDB

区块索引
LevelDB

账本数据

Txn
Reads[]
Writes[]

Txn
Reads[]
Writes[]

Txn
Reads[]
Writes[]

状态数据
（可选
LevelDB
CouchDB）

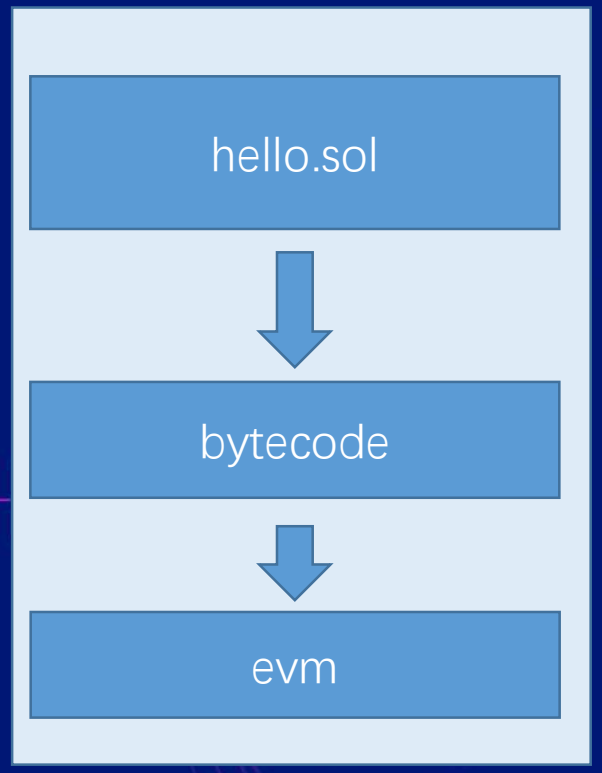
交易提交时更新状态数据

Client(目前社区提供Golang/Java/Node/Py等版本的SDK)

HyperLedger Fabric的架构与设计理念

Fabric模块化设计之——合约执行引擎的解耦

1) 以太坊：以太坊定义了一个全新的智能合约引擎evm



优点：简单、确定、轻量、安全的沙箱环境，使得以太坊在公链运行环境下，几乎没有因为引擎的bug导致重大的事故发生。

缺点：

1.账本数据结构与evm代码绑定较深，修改会互相影响；

2.为了适应更大的内存寻址和复杂的密码学运算以实现安全的gas模型，采用256位整数运算，致使32位/64位x86处理器相对低效。

3.Evm是一个基于栈的虚拟机，大多数操作都使用栈。

4.标准库太少，solidity开发生态、推广还需时日。

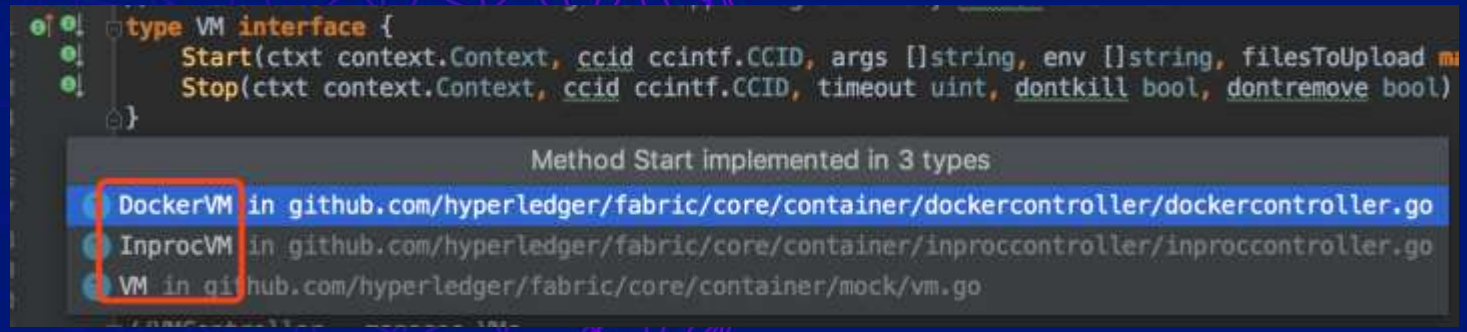
…

HyperLedger Fabric的架构与设计理念

Fabric模块化设计之——合约执行引擎的解耦

2)Fabric

① container接口层代码，该接口有3个实现DockerVM（执行用户合约）、InproVM（执行系统合约）、MockVM（UnitTest的mock环境）。



②VM与节点的通信方式为Grpc。

③后续fabric会将evm集成。

优点：

1.代码层面上实现了对VM和节点进行脱耦，并且易于扩展新的VM方式。

2.理论可支持众多开发语言开发智能合约。。

缺点：依赖docker运行环境，严重限制fabric节点的部署可能性；docker作为沙箱环境相对复杂，安全性、稳定性都面临较大的挑战。

HyperLedger Fabric的架构与设计理念

Fabric模块化设计之——链上代码逻辑的解耦

1) 沿用chaincode的设计，节点代码中的部分标准逻辑，设计成系统链码的形式。

2) 1.2版本后逐渐开放系统链码的自定义修改，如escc/vscc。开发者可修改系统链码，以实现不同需求。
如：定义基于数据状态的背书策略、匿名交易场景（匿名公钥）

HyperLedger Fabric的架构与设计理念

Fabric模块化设计之——共识排序服务的解耦

Fabric的共识过程：

普通节点发起交易请求。 —Tx input→ ① 根据链的背书策略，需要部分组织进行背书，背书组织预执行智能合约并签名。 → ② 将背书组织签名的合约执行结果集给排序节点排序。排序节点根据排序算法进行交易排序，并广播交易 —Tx ouput→ ③普通记账节点接受广播记录到本地账本。

特点：跟公链的共识过程相比，

①公链的共识者，同时承担合约预执行、交易排序的职责；fabric中排序节点只做排序，合约预执行由背书节点做。（fabric中背书节点与排序节点的组合=公链如以太坊中的共识节点）

②目前fabric的共识过程两阶段，背书+共识，都支持扩展。

Fabric这样解耦共识部分：

1)排序节点代码定义了Consenter接口，可以通过实现Consenter接口的拓展共识算法。

2) fabric1.2版本支持插件式开发ESCC/VSCC背书模块和交易验证模块。

HyperLedger Fabric的架构与设计理念

Fabric模块化设计之——权限控制的解耦

1) fabric-ca， 一套PKI公钥基础设施，基于证书/私钥来作为权限最小单元（如节点、用户）的唯一标识和校验依据。区块链系统中每个节点、用户都有唯一证书和私钥。

2)组织、用户、节点，组成权限体系的角色role层级。如：Org1.admin、Org1.member、Org1.peer。

3) 将所有需要进行权限校验的单元作为ACL，代码resources.go中预制了很多ACL。如（调用合约ACL、合约间调用ACL）：

```
# ACL policy for invoking chaincodes on peer
peer/Propose: /Channel/Application/Writers

# ACL policy for chaincode to chaincode invocation
peer/ChaincodeToChaincode: /Channel/Application/Readers
```

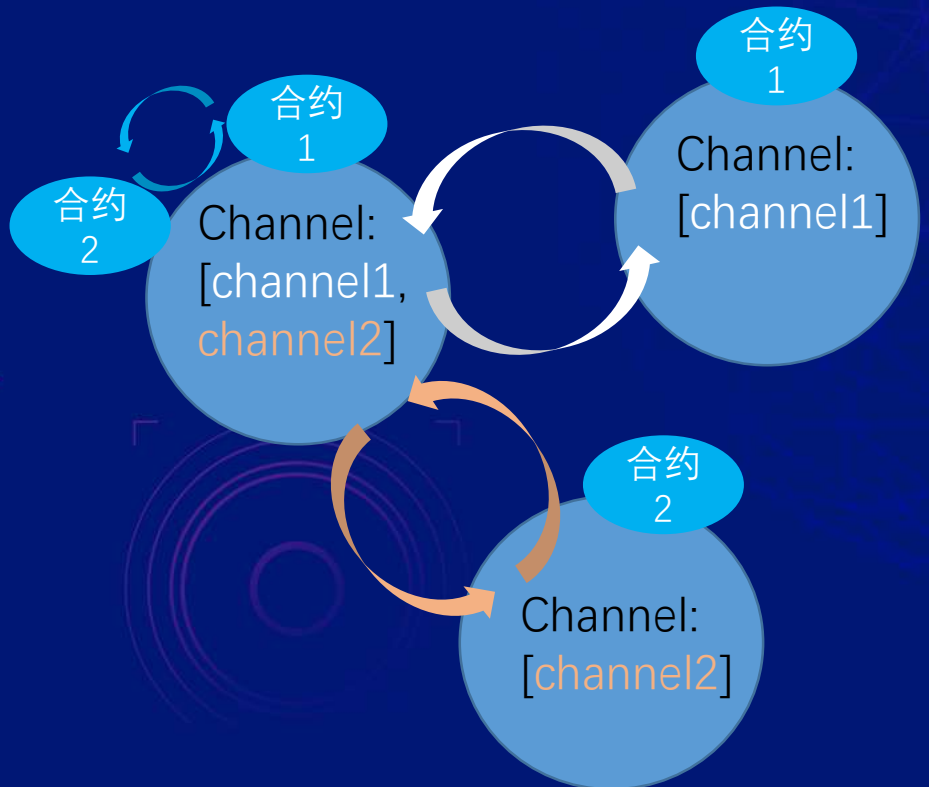
4)1.3版本后，可以为ACL动态（链运行时）配置策略，策略可以由2)中提到的角色组成。

HyperLedger Fabric的架构与设计理念

Fabric对于同构链中多链以及多链通信的设计

1）Fabric多链的设计：通道channel，原理是P2P网络中的数据传输通道。

2）Fabric多链通信的支持：通过智能合约间的调用，如同时在channel1/channel2上的节点安装的合约1/合约2可以互相调用。



① 借助多通道与链码相互调用，可以实现同一业务中，账本数据的隔离与间接共享（如隐私数据保护）。

② 借助多通道，可以缓解现在区块链账本数据逐渐增大，无法分片存储的问题。

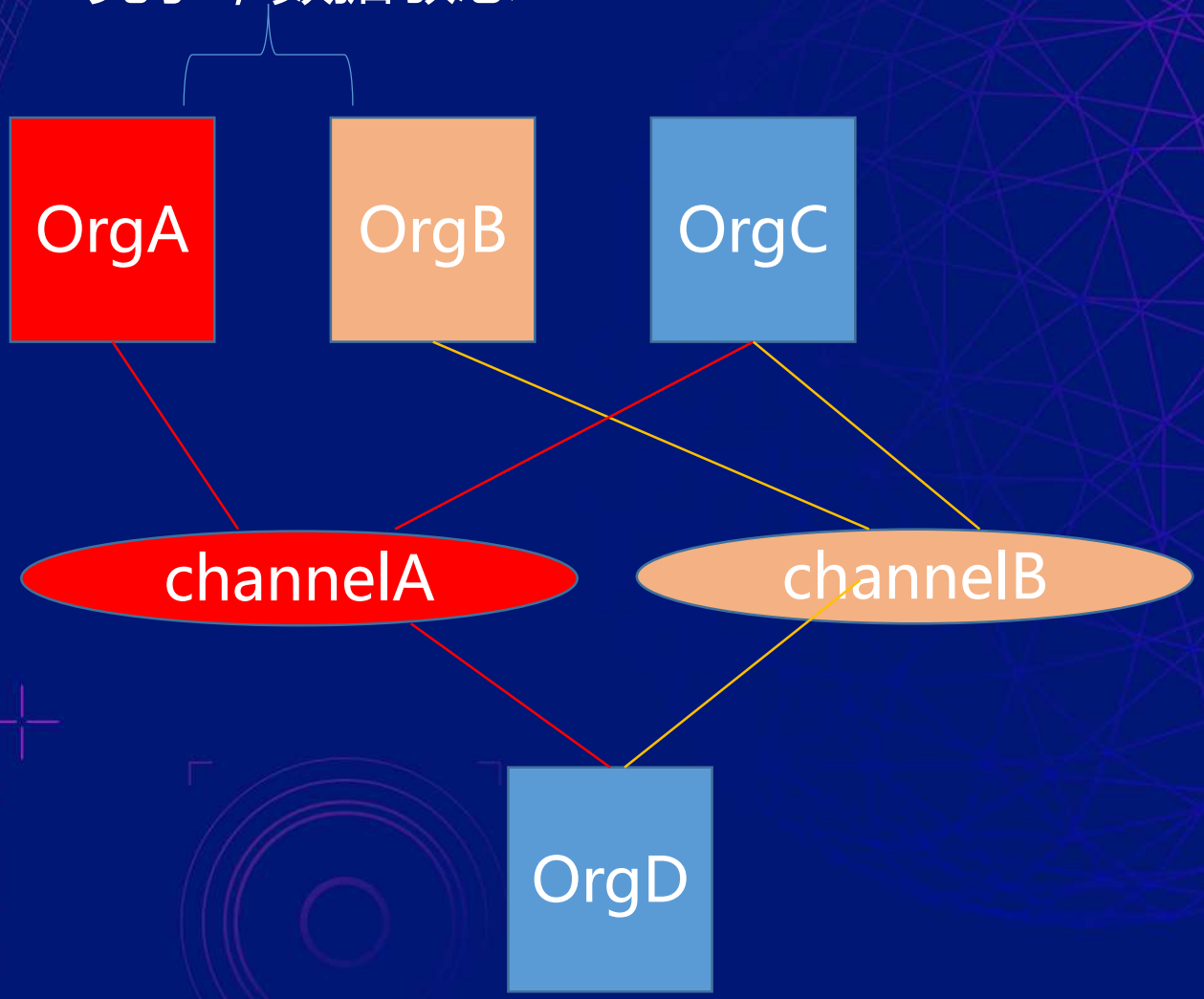
③ 借助多通道与一个组织部署多个节点，可以实现并行计算，提高联盟链对于高并发的支持。

3 .在实践HyperLedger Fabric过程中的经验

在保护数据隐私的前提下，用fabric在链上保存原始数据（非哈希）并可以按需分享的一种解决方案

——多链以及跨链智能合约调用的实际应用场景设计举例

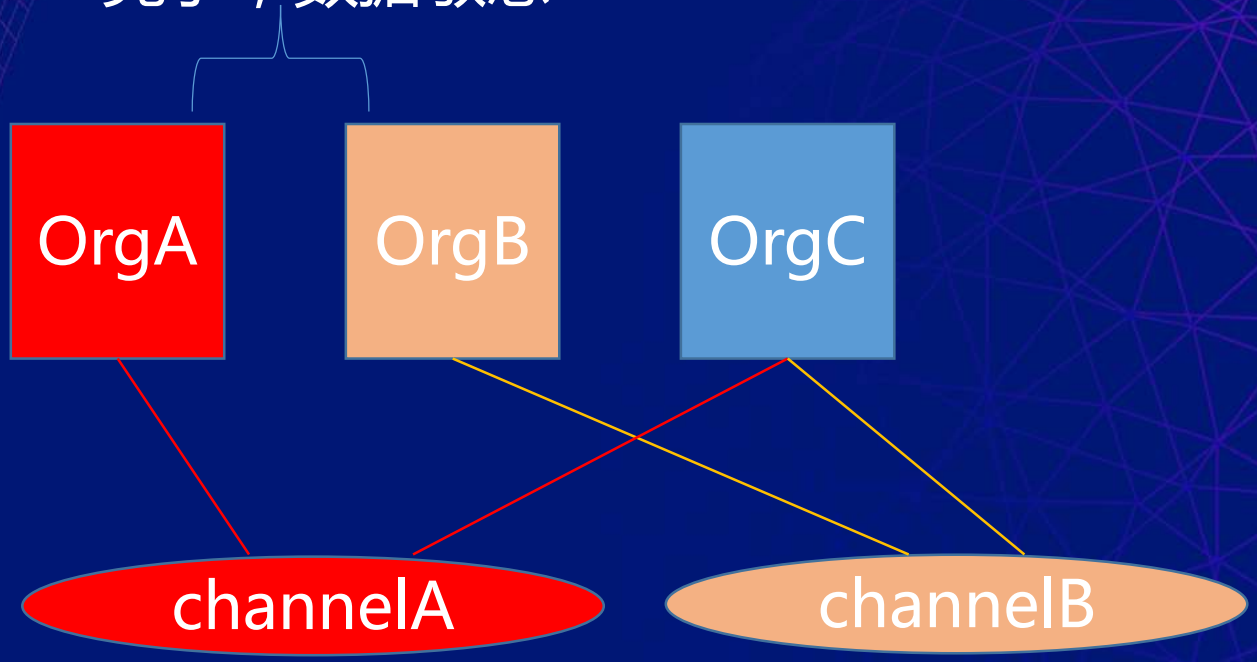
竞争，数据敏感



举例：
OrgA,OrgB与OrgC发生交易，但是OrgA与OrgB是同业，互相不希望与OrgC发生的交易被彼此知道。

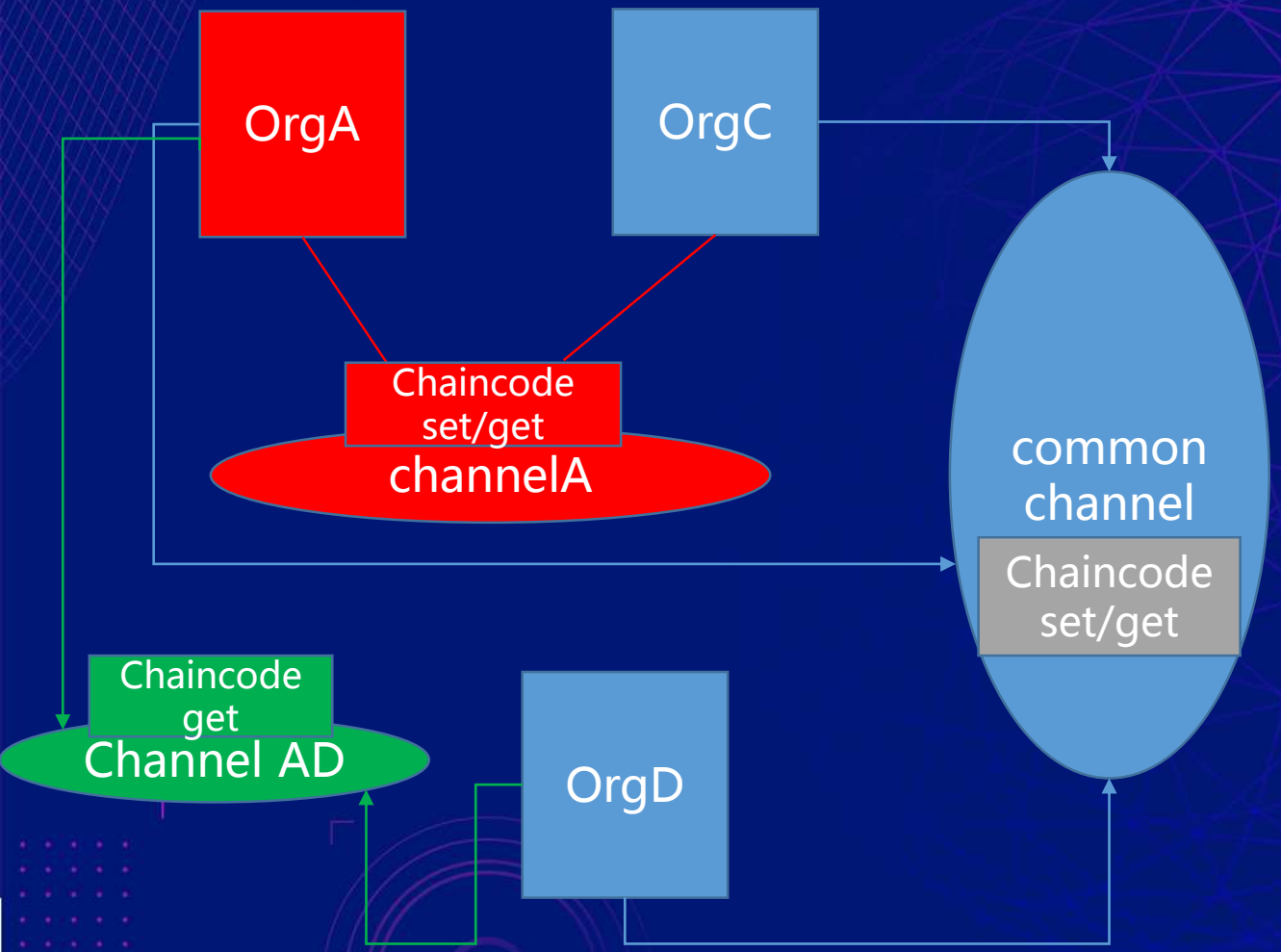
OrgD希望可以看到与OrgB发生的所有交易详情。

竞争，数据敏感



举例：
OrgA,OrgB与OrgC发生交易，但是OrgA与OrgB是同业，互相不希望与OrgC发生的交易被彼此知道。

OrgD希望可以看到某些交易详情，且需要经过A/B的授权查看才可。
怎么办？



1）A与C独立建立专用channelA，同时ACD组成common channel。

2）A/B与C发生交易记账。

① 调用channelA的set合约进行明细数据记账。

② 调用common channel的set，合约会读取channelA的明细数据并Hash计算后记录到common channel。

两步涉及到的明细上链和hash计算上链都由channelA上的所有组织进行背书。保证原始数据真实。

3）当A授权channelA上某条数据查询权限给D后。

① 双方建立私有通道channelAD并安装get合约。

② 执行get acc，该合约分别调用channelA的get acc和common channle的get acc合约将数据取出并进行hash验证有效后返回给OrgD。

整个过程所有操作无链下环节，保证A给到D的数据都是经过A/C背书的真实数据。

4 .关于公有链/联盟链当前问题的一些思考

世界上不需要这么多的公链 -> 除非有一个公认的协议将各个公链打通

世界上很多行业都需要联盟链，大大小小的区块链联盟、技术也已经兴起，但如何将他们互相打通？->需要有一个公认的协议将各个联盟链打通

异构跨链技术

1.通过异构跨链实现主链无法实现的内容：规则/更高的TPS/联盟链锚定公链。

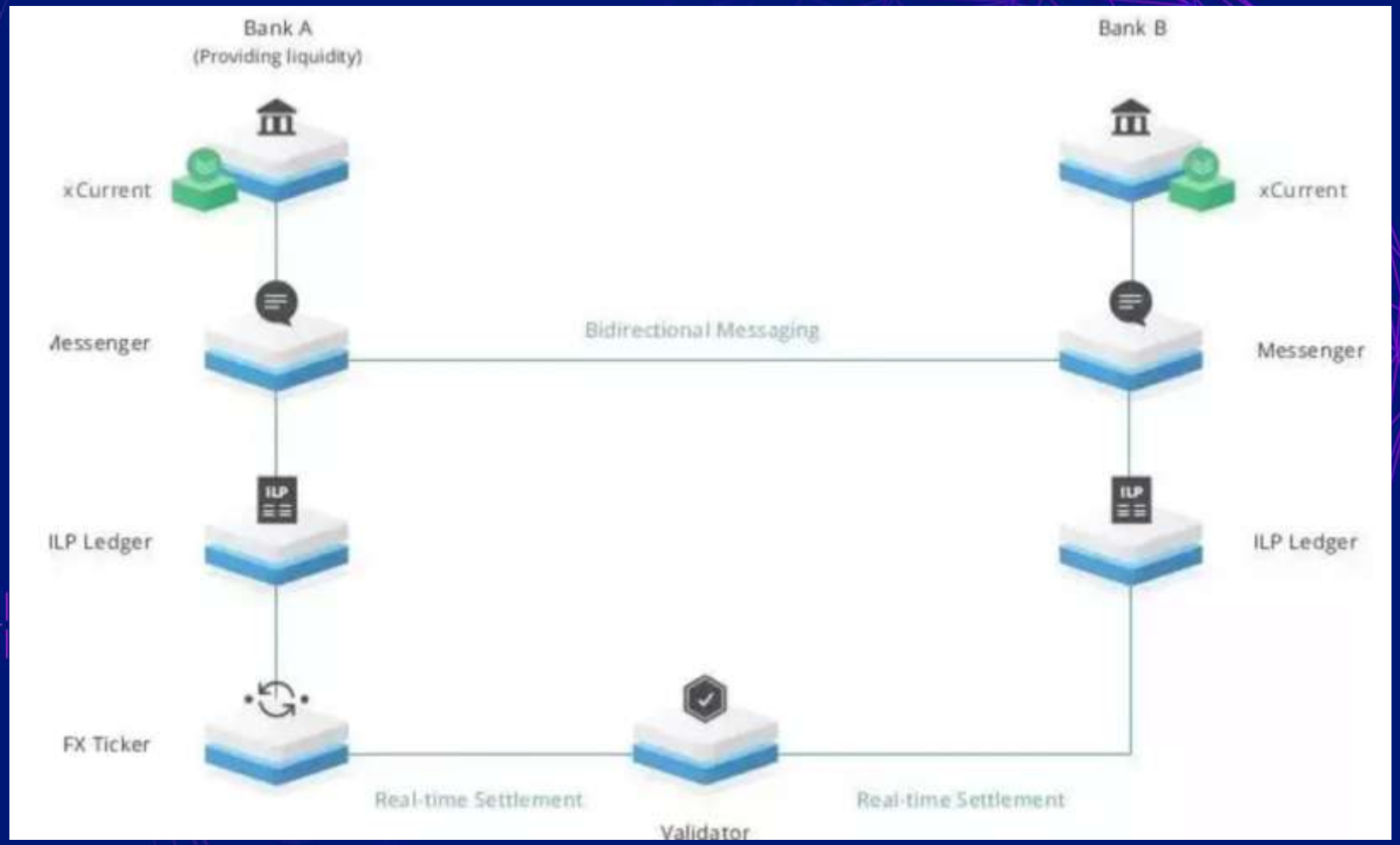
2.通过异构跨链实现主链价值、数据的转移。

(Vitalik Buterin)以太坊创始人给R3写的跨链互操作的报告

跨链技术	Notary公正技术	Relay中继及侧链技术	Hash-locking哈希锁定
互操作性	所有	所有（需要所有链上都有中继，否则只支持单向）	只有交叉依赖
信任模型	多数公证人诚实	链不会失败或者受到“51%攻击”	链不会失败或者受到“51%攻击”
适用跨链交换	支持	支持	支持
适用跨链资产转移	支持（需要共同的长期公证人信任）	支持	不支持
适用跨链Oracles	支持	支持	不直接支持
适用跨链资产抵押	支持（需要长期公证人信任）	支持	大多数支持但是有难度
实现难度	中等	难	容易
多币种智能合约	困难	困难	不支持
实现案例	Ripple	BTC Relay/ Poldadot/COSMOS	Lightning network

跨链技术的目的从起步阶段的传递资产/代币，到现在已经变为了传递数据。

公证技术：瑞波Interledger协议

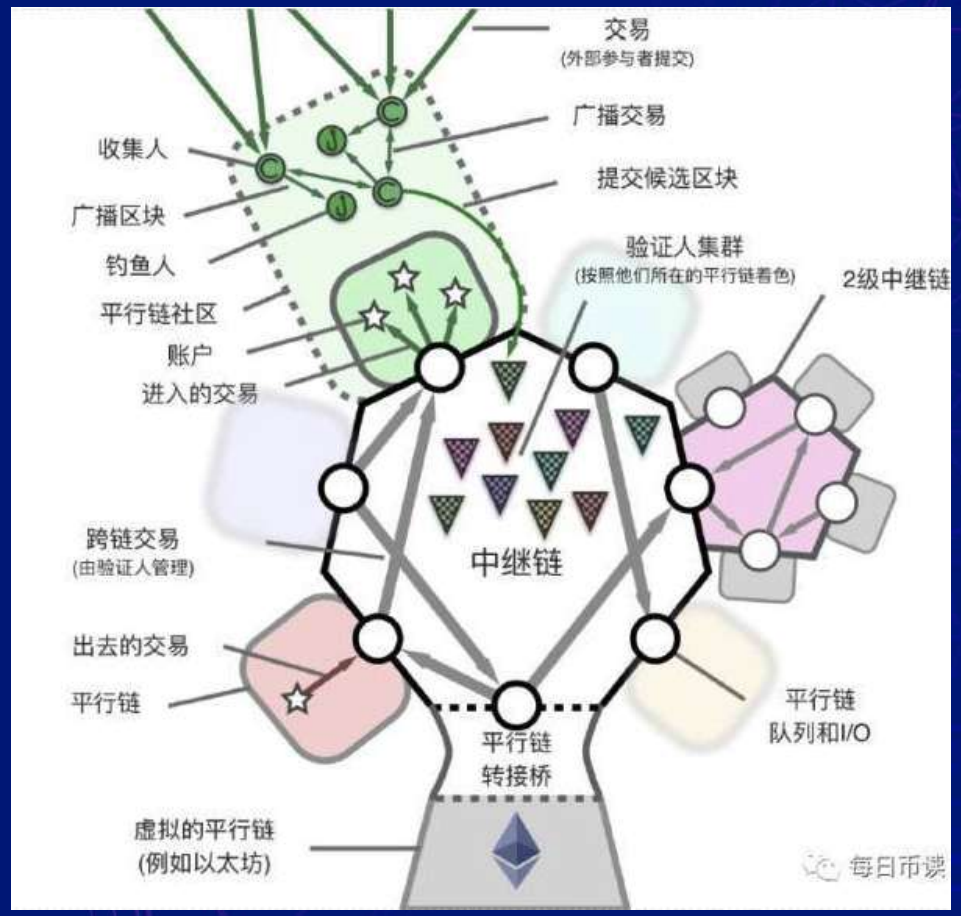


①Interledger协议使两个不同的记账系统可以通过第三方“连接器”或“验证器”互相自由地传输货币、传递状态。

②该协议采用密码算法用连接器为这两个记账系统创建资金托管。

③该协议移除了交易参与者所需的信任，连接器不会丢失或窃取资金，并且连接器上的交易详情是加密的。

中继技术：Polkadot(波卡链)和cosmos



本PPT来自2018携程技术峰会

更多技术干货，请关注“携程技术中心”微信公众号