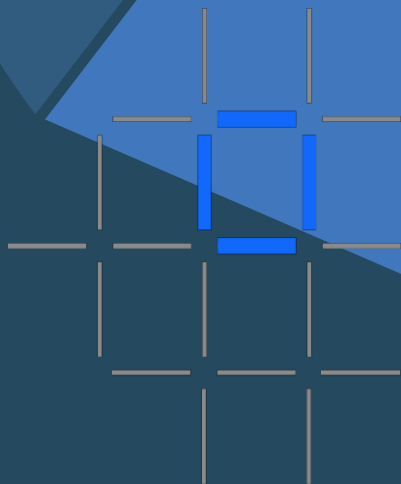




developerWorks
COURSES

Ibm 区块链基础





部分1:超账 作曲家

wHat我sHYPeR我eDgeR C不, 不,不Mp不,不,不seR?

- 区块链提供a低级接口适用于企业 应用
 - 聪明合同代码运行上a分布式处理 系统
 - 输入去成一个变分类帐;输出自a数据 商店
 - 应用都是建立上返回页首的a低水平的 抽象
- 超账 作曲家
 - a 个套房的高水平应用抽象适用于企业 网络
 - 重点上以业务为中心的词汇表快速解决 方案 创造
- FEat美国
Res
 - 模型你业务网络测试和 部署
 - 应用使用Api自互动与a业务 网络
 - 整合现有系统的记录使用 环回/rest
- 打开工具、api和图书馆自支持这些 活动
 - 利用超级分类帐织物区块链 技术
 - 完全打开和部分的Linux基础超账

业务 应用

超账 作曲家

超账 织物

<https://hyperledger.github.io/composer/>

Benefits of Hyperledger Fabric



增加易用性
降低门槛

桥梁简单从业务概念
到区块链



是时候
了

发展区块链应用更
迅速和便宜



减少
风险

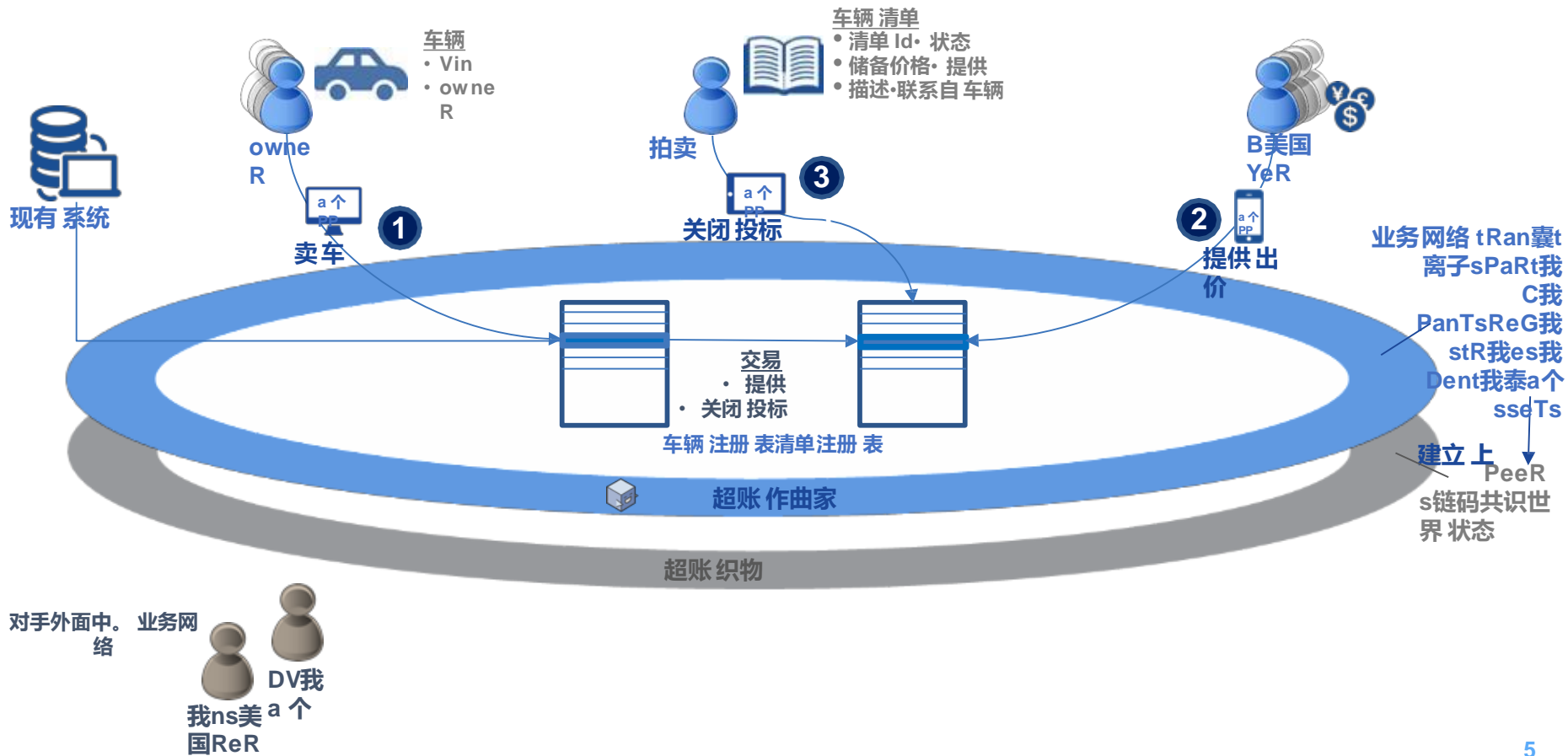
好吧, 好吧经过测试, 高
效设计符合自 最好实践



增加 灵活性

高水平抽象使它容易自
迭代

一个例子业务网络-车拍卖 市场



概念 组件和结构的作曲家

业务网络是定义通过模型脚本文件Acl和元和包装在a业务网络档案



解决 方案开发 人员模型中。业务网络实现了脚本文件那就是定义交易行为和套餐到a业务网络档案



解决 方案管理员提供中。目标环境并可能管理部署

业务网络 档案

mOde
我s

脚本 文件Acl

我taData

广泛熟悉打开发展 工具

```
asset Animal identi  
  o String animal  
  o AnimalType sp  
  o MovementStatu  
  o ProductionTyp
```

数据 建 模



Javascript业
务 逻辑



Web 操场

作曲家-客户端
作曲家管理员



客户 图书馆



编辑 器 支持

\$ 作曲家

Cli公用事业



代码生成

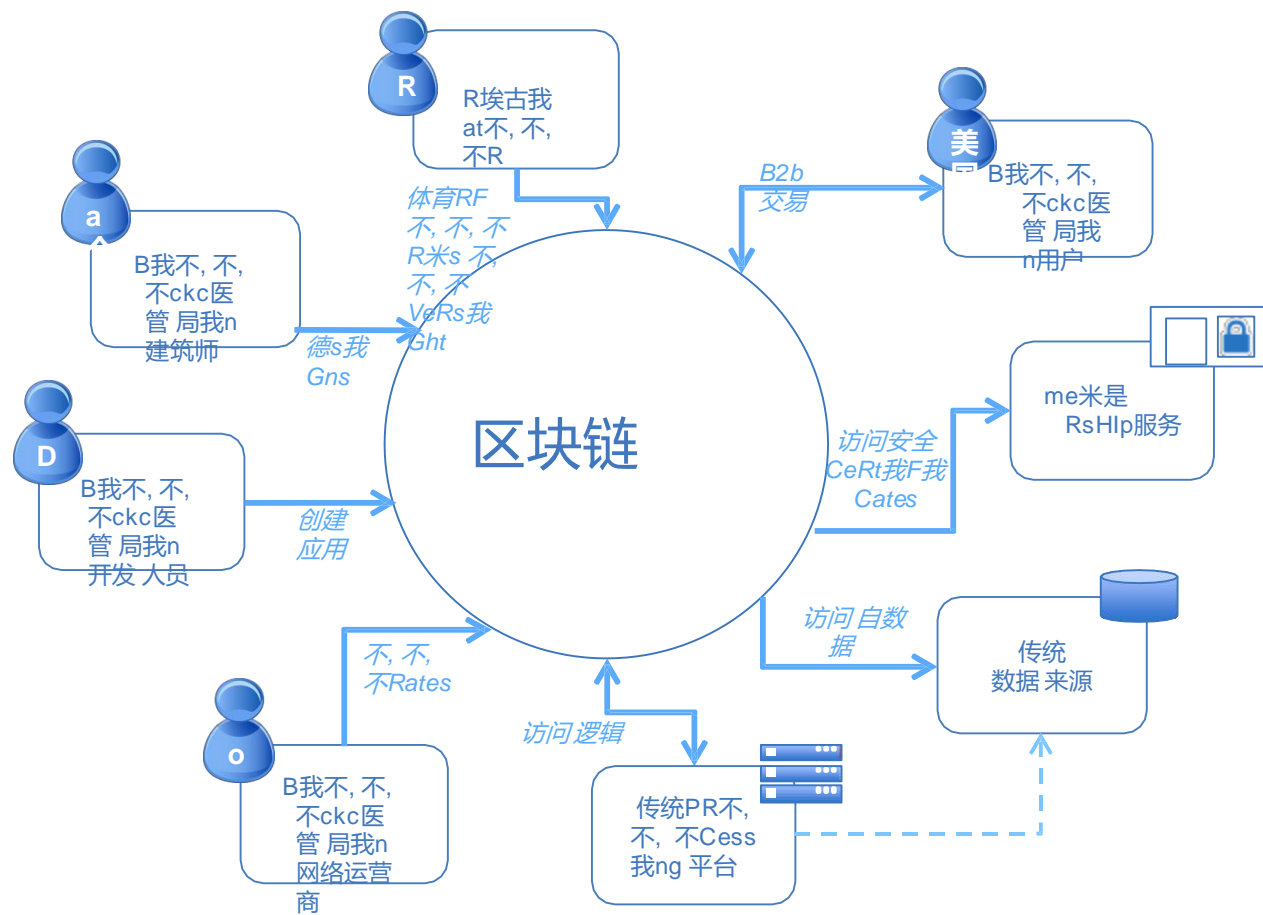


现有系统和
数据



部分2:区块链织物 发展

演员在a区块链 解决方案



演员在a区块链 解决 方案



组件在 a 区块链解决 方案

帐



a 个 帐 是 a 频道的 链 和 当前 状态 数据 其中是保持 通过 每个 同行 上 中。通道。

聪明 合同



软件 运行 上 a 帐, 自 编码 资产 和 中。 交易 指示 (业务 逻辑) 适用于 修改 中。 资产。

同行
netw不,
不, 不



a 个 广泛 术语 总体 中。 整个 事务 流 其中 服务 自 生成 一个 协议 上 中。 以 和 自 确认 中。 正确 性 的 中。 设置 的 交易 构成 一个 街区。

RK
me米是RsH
我P



会员 服务 验证 授权 和 管理 身份 上 a 许可 区块链 网络。

eV恩ts



创建 通知 的 重要 操作 上 中。 区块链 (例如: a 新增 功能 块), 作为 以及 作为 通知 相关 自 聪明 合同。

系统m安拉
奇米恩t



提供 中。 能力 自 创建 改变 和 监控 区块链 组件

wa将
et



安全管理 a 用户 的 安全 凭据

系统我nt
例如Rat我
不, 不, 不n



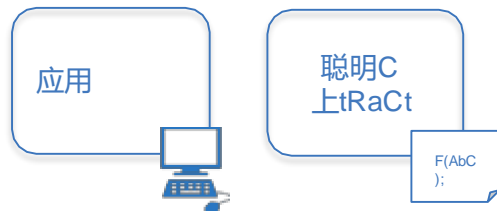
负责 适用于 整合 区块链 双向 与 外部 系统。 不 部分 的 区块链, 但 使用 与 它。

中。区块链 开发 人员



B洛CKC医
管 局我n开
发 人员

区块链开发商的主要利益 是..。



..... 和如何他们与交互中。帐和其他系统的 记录：



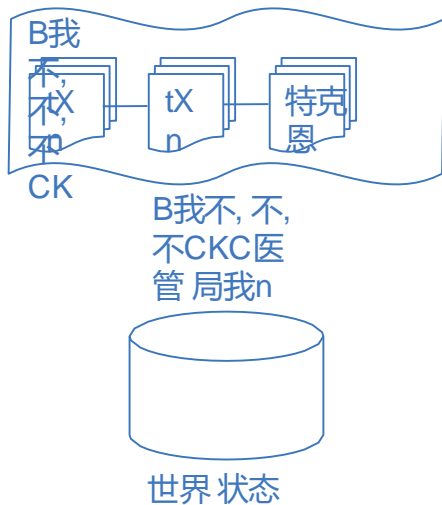
他们应该不有自护理关于操作关注的问题, 例如 为:



同行共识安全

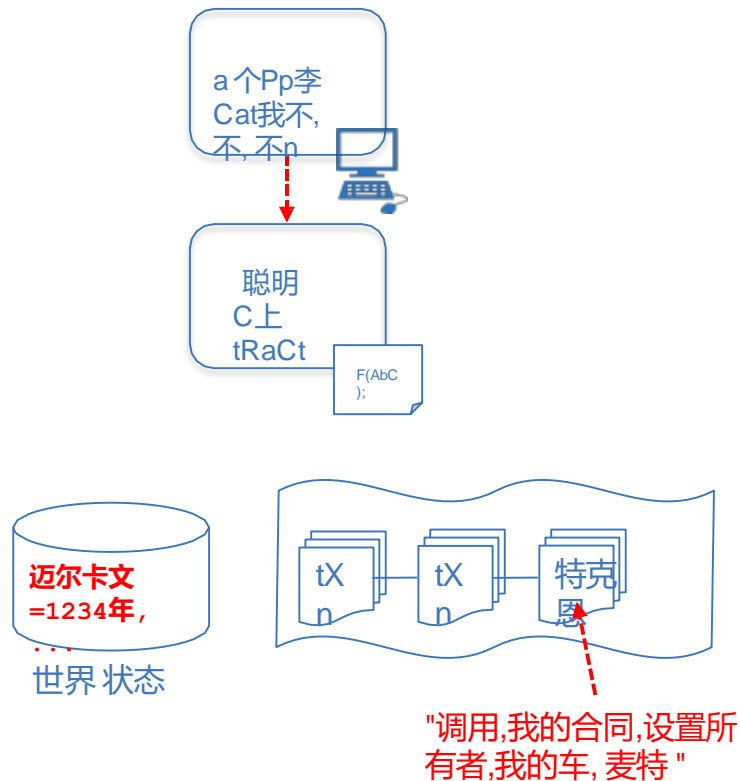
如何 中。 开发 人员与交互中。 帐

a 个帐经常由的两数据 结构



- 区块链
 - a 个联系列表的 块
 - 每个块描述a设置的交易
(例如:输入端自a智能合同 调用)
 - 变-块不能是 篡改
- 世界 状态
 - 一个普通数据库(例如:key/值 专卖店)
 - 商店中。联合输出的所有 交易
 - 不通常 变

工作与中。帐：例子[的a改变的所有权交易\(更换汽车1所有者自 麦特\)](#)



交易输入-送从应用

调用 (我的合同, 设置所有者, 我的车, 马 特)

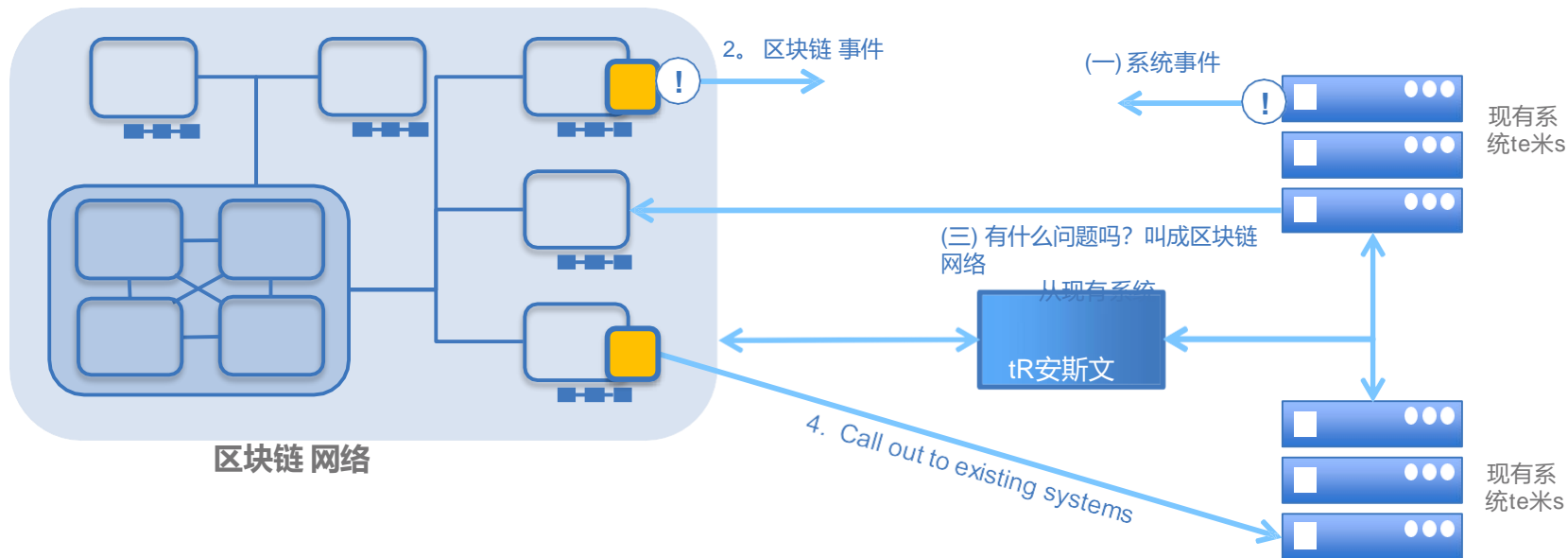
聪明合同 实现

```
(汽车,新业主) {  
    设置车所有者= 纽车主  
}
```

世界状态：新增功能 内容

```
迈尔卡文=1234  
mycars. 所有者=  
matt mycars. 做=  
奥迪  
...
```

整合与现有系统





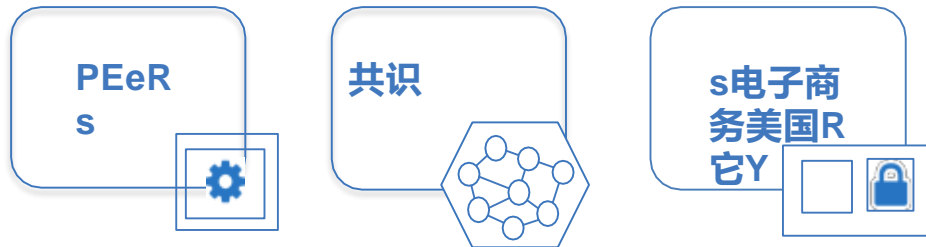
部分3:区块链 建筑

中。 区块链 管理员(接线员)



区块链a个D
米我n我
stRat不, 不,
不R

区块链 管理员 "主要 利益 都是在 中。 部署和操作部分的 区块链:



他们应该不有关心发展关注这样为:

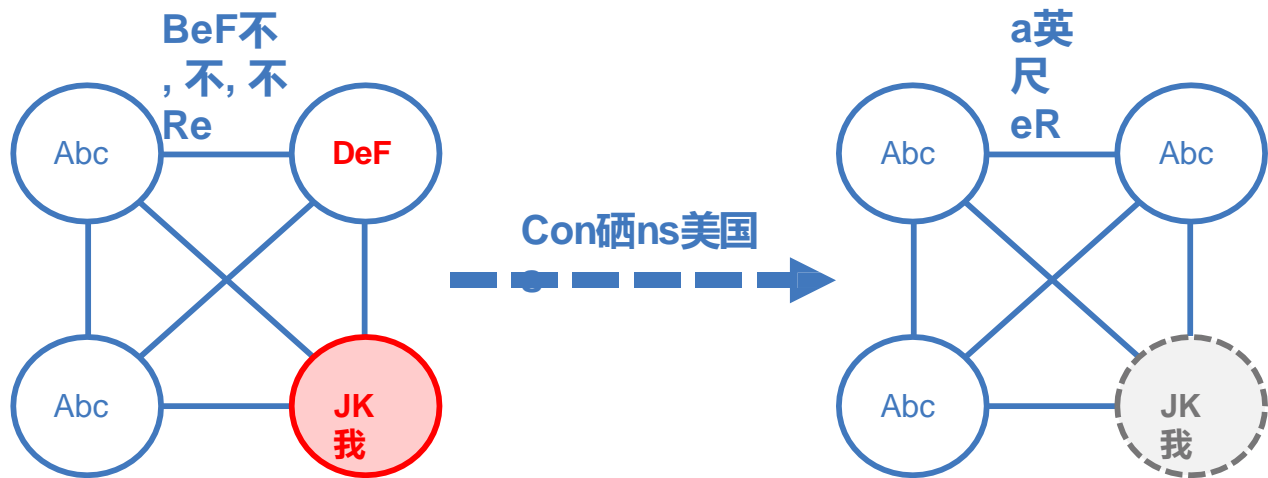
X

应用 代码

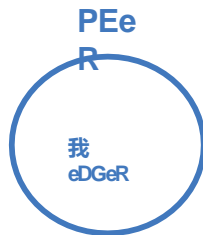
智能合同 代码

事件和集成

共识：中。过程的 维护a一致 帐

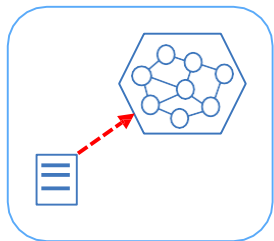


保留所有对等方来自 日期。
修复任何同行在 错误。
忽略所有恶意 节点。

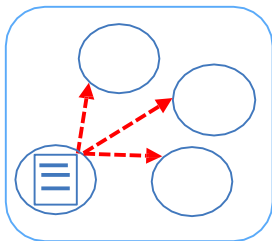


共识：典型流的 执行

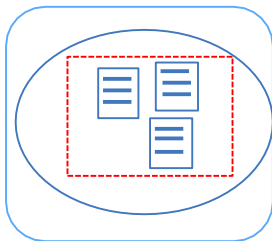
细节不同显著之间区块链实现但a典型流 是：



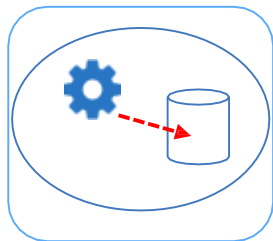
中。应用提交a 请求自
调用a交易



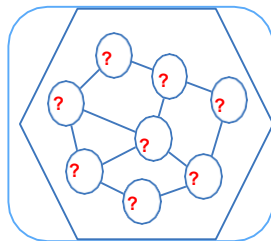
中。交易是共享在
网络上



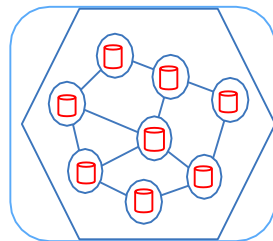
a 个指定同行创建a
块含中。交易



中。方块的交易都是执行
和输出存储在a三角洲



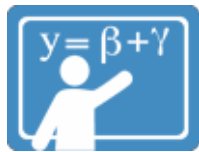
网络试图就正确 结
果



如果是一致的中。正确
输出是应用自中。世界
国家

- 中。过程自同意中。一致状态的中。帐是知道作为**共识**

一些 例子的共识 算法



证明的 工作



证明的 股份



s不,
不,
不洛



卡夫卡
ZOo记PeR



证明的
过去了 时间



PBFt-Bas已
ed

共识算法有不同优势和弱点



证明的工作

需要验证自解决困难加密 拼图

专业报告:工程在可信 网络

cons: 依赖上能源使用;慢自确认 交易

例子使用: 比特币, 以太



证明的股份

需要验证程序自按住货币在 托管

专业报告:工程在可信 网络

康斯: 需要内在(加密) 货币,"没什么在木桩 "问题例子使用: Nxt



证明的
过去了 时间

等时间在a信任执行环境随机化块生成

专业报告:有效

缺点: 目前量身定制一个供应商例子使用:

sawathth-la阶

共识算法有不同优势和弱点



s不,
不,
不我
不,
不



pbft-八seD

验证应用收到交易没有 共识

专业报告:非常速度快;适合自 发展

缺点: 不共识;可以导致发散 链

例子使用: 超账织物 v1

实用拜占庭故障宽容 实现

专业报告:合理有效和宽容针对恶意同行
缺点: 验证 都是 知道 和
完全 连接

例子使用: 超账织物 v0.6



卡夫卡
动物园管
理员

订购服务分布块自 同行

专业报告:有效和故障 宽容

缺点: 是否不警卫对恶意活动
例子使用: 超账织
物 v1

安全：公共与。私人 区块链

公共 区块链



- 适用于例子 比特币
- 交易都是可见 通过任何人
- 参与者身份是 更困难自 控制

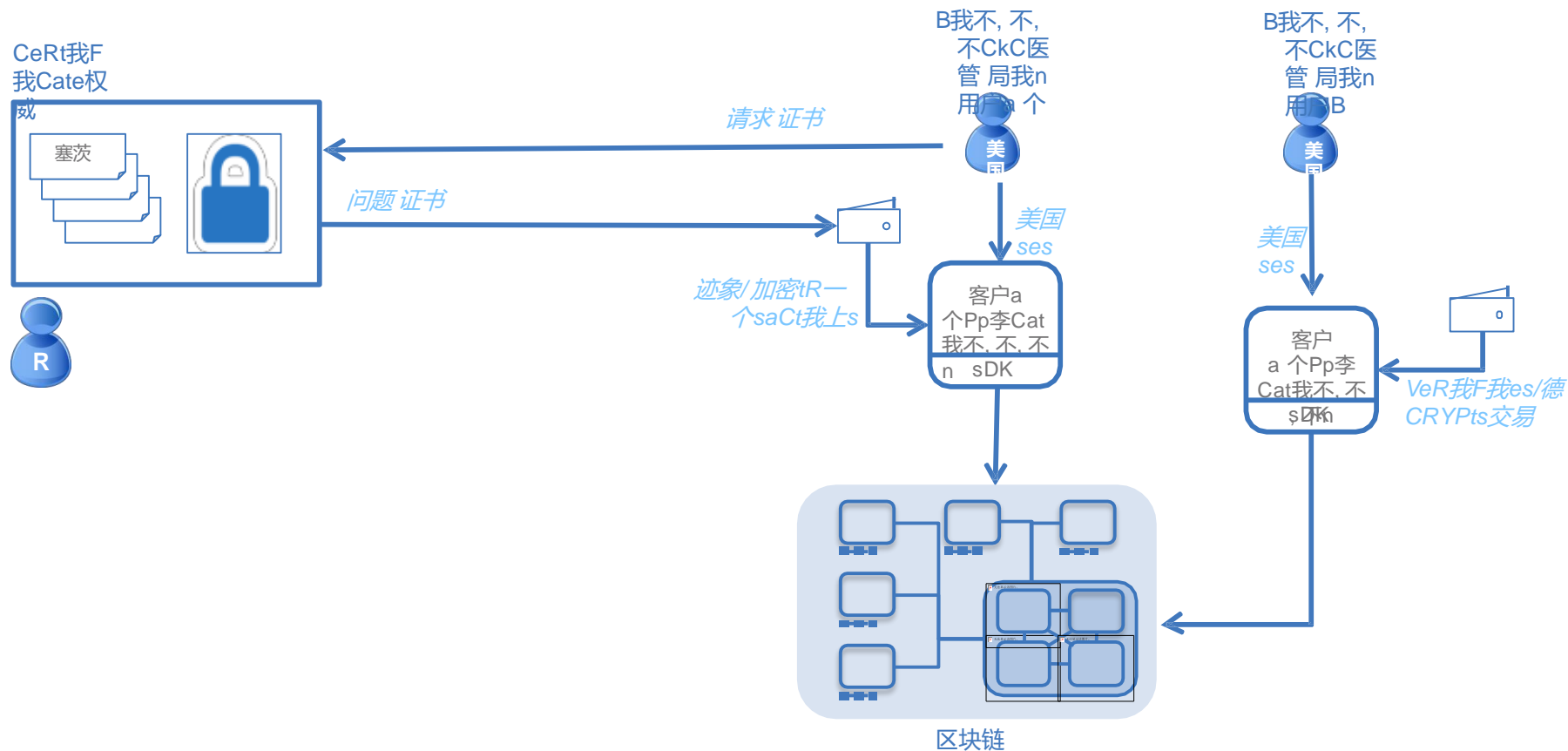
私人 区块链



- 适用于例子超账织物
- 网络成员都是知道但交易都是 秘密

- 一些使用例需要匿名别人需要 隐私
 - 一些可能 需要 a混合物的 中。 两 取决于上 中。 特征的 每个 参与者
- **最 业务 使用 例 需要 私人 许可 区块链**
 - 网络成员知道谁他们是交易与(必填项)适用于kyc、aml 等)
 - 交易是 (通常)机密之间中。 参与者 有关
 - 会员是 控制

证书当局和 区块链



其他不起作用 要求

- 性能

- 中。量的数据正在被 共享
- 数量和位置的 同行
- 延迟和 吞吐量
- 配料 特征

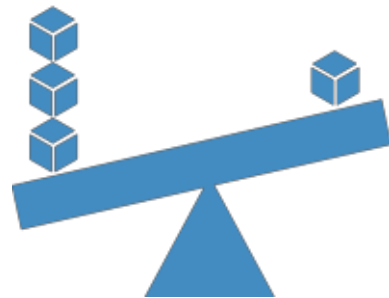
- 安全

- 类型的数据被分享,和与 谁
- 如何是身份 实现
- 保密的交易 查询
- 谁验证(认可) 交易




- 弹性

- 资源 失败
- 恶意 活动
- 非决定论

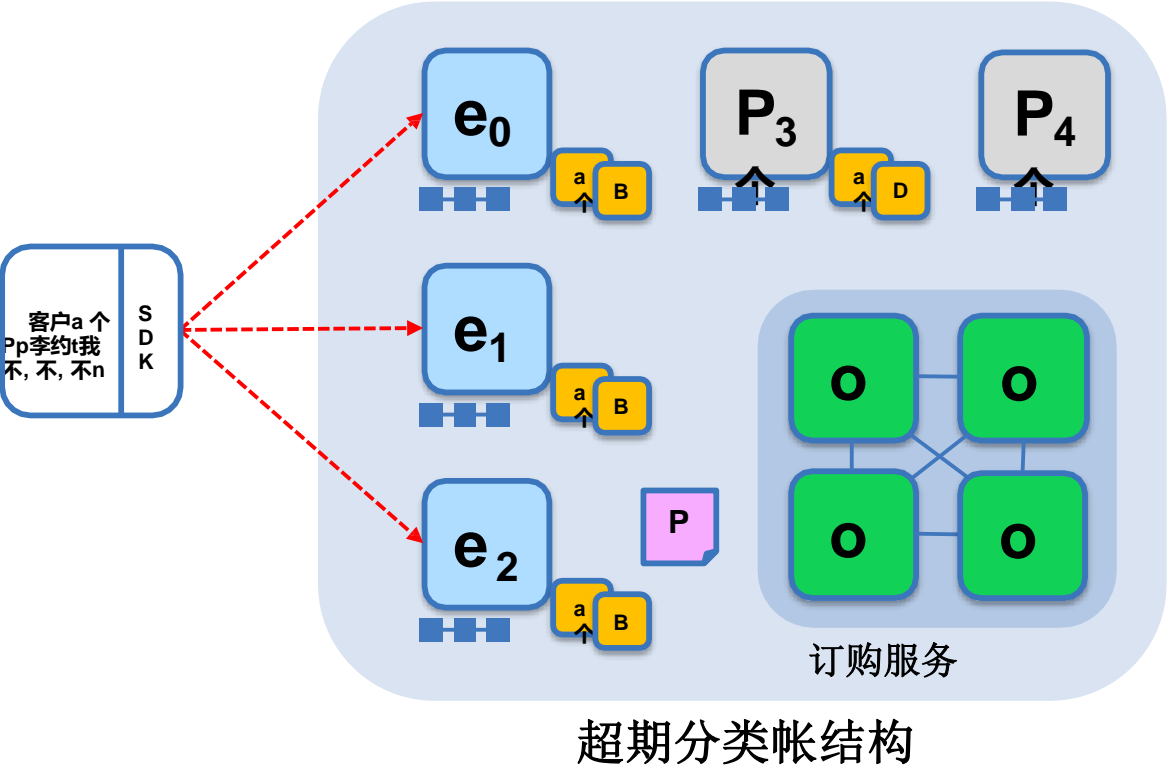
考虑的权衡之间 性能安全 和 弹性!



节点和角色

	犯同行: 保持帐和状态。提交 交易。 可能按住智能合同(链码)。
	赞同同行: 专业犯同行那就是接收一个交易建议适用于背书响应授予或否认背书。 必须按住聪明 合同
	订购节点(服务): 批准中。包含的交易块到帐和沟通与犯和赞同同行节点。 是否不按住聪明合同。是否不按住 帐。

样本交易记录:步--提出 交易



应用提出交易

背书政策:

- "e₀, e₁和 e₂必须签名"
- (p₃个, P₄个都是不部分的中。政策)

客户申请提交a 交易
建议适用于聪明合同a. 我的工作它是 必须
目标中。所需的对等方{e,e,e }_{1 2}

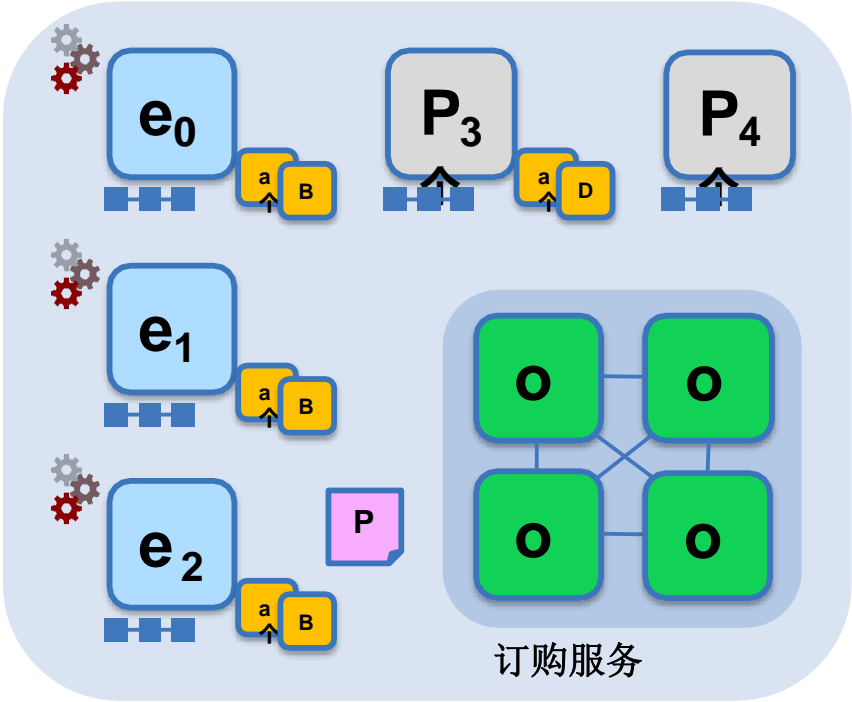
Key:

代言人			帐
犯同行			应用
订购节点			
聪明合同			e恩多Rse米恩t政策
(链码)			

样本交易记录:步2/7-执行 建议

客户a个
Pp李约t我
不, 不, 不n

S
D
K



超期分类帐结构

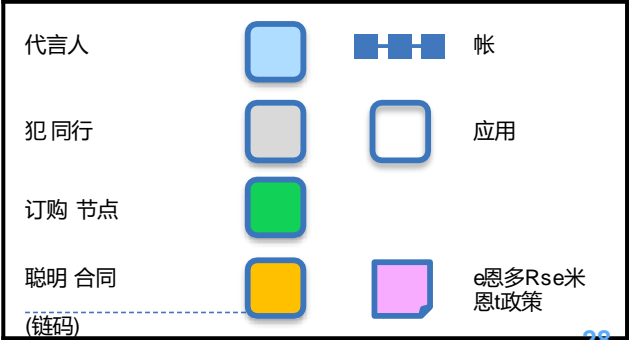
代言人执行建议

$e_0, e_1 \& e_2$ 将每次执行中。提出交易。这些都不是执行将更新中。帐。

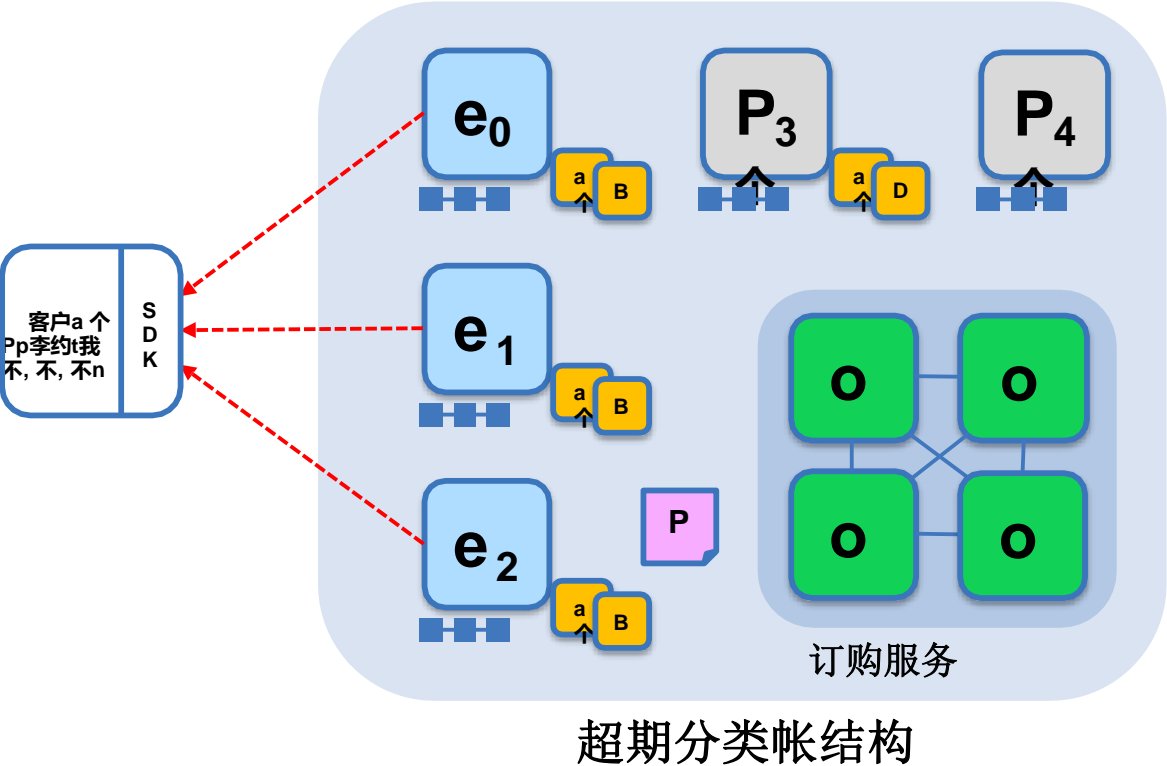
每个执行将捕获中。设置的阅读和写数据叫乌尔曼集其中将现在流在中。织物。

交易可以是签署和加密。

关键:



样本交易记录:步"7"-建议响应



超期分类帐结构

应用接收反应

乌尔曼集都是异步返回 自应用。

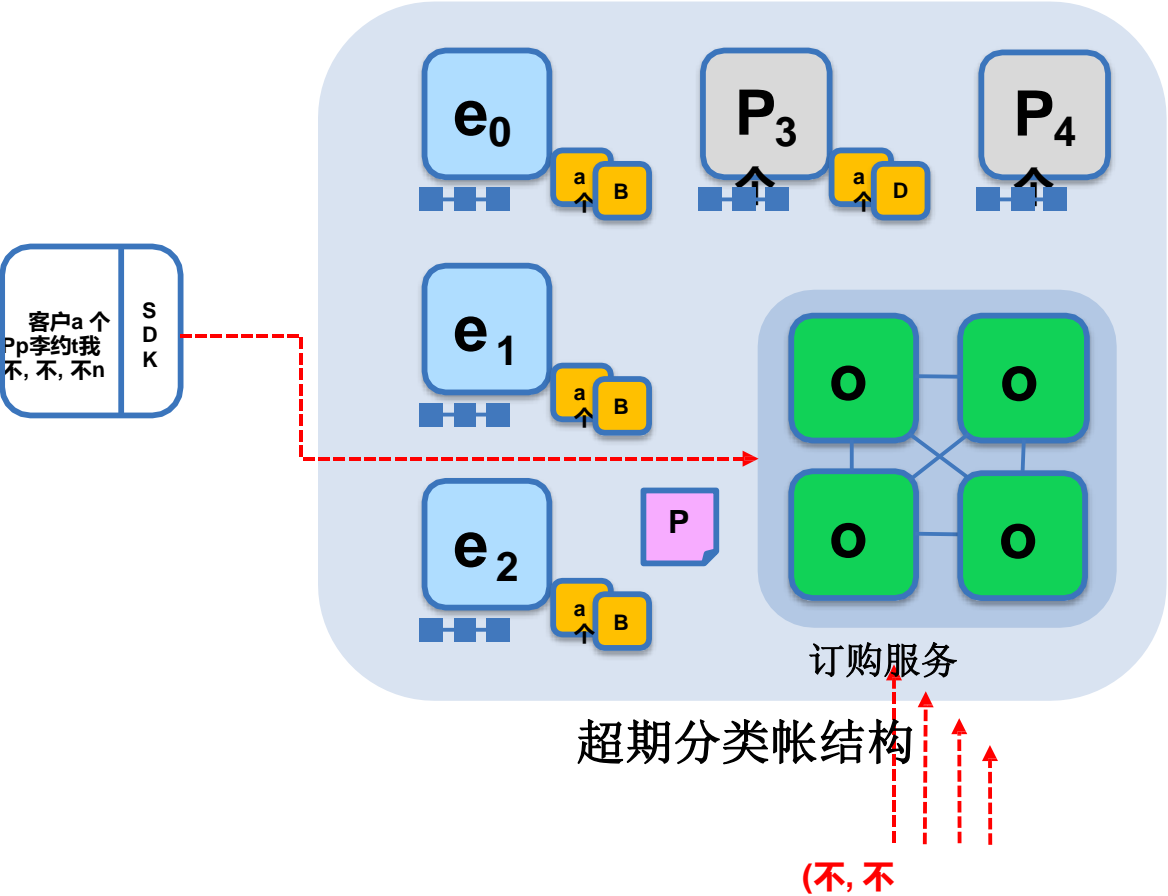
中。乌尔曼集都是签署通过每个代言者,和也包括每个记录版本数量。

这信息将是检查多后在中。共识 过程。

Key:

代言人			帐
犯同行			应用
订购节点			
聪明合同			e恩多Rse米恩t政策
(链码)			

样本交易记录:步7-以 交易



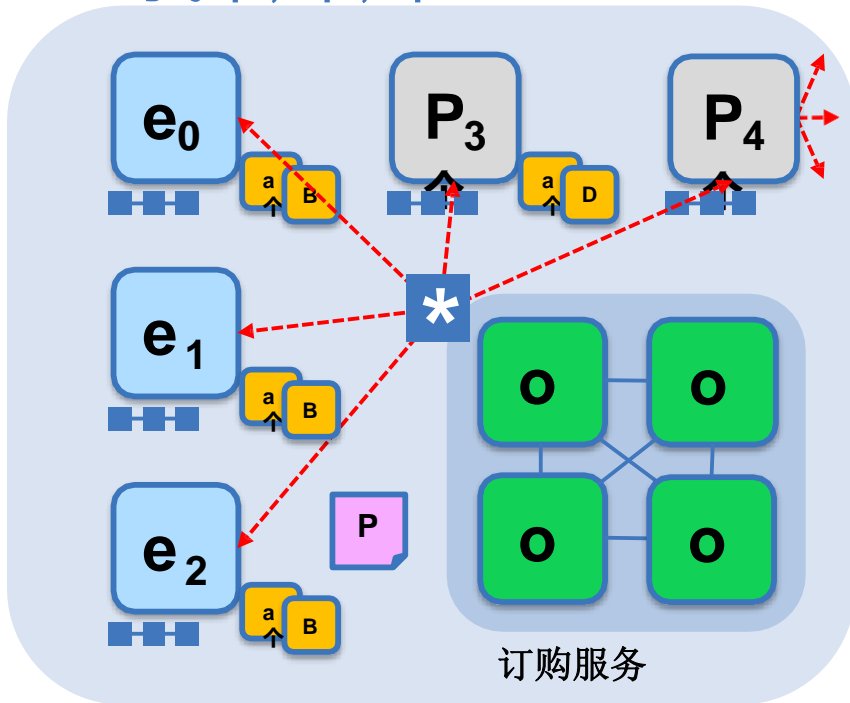
应用 提交 反应适用于 订购

应用提交反应作为a交易自是 命令。

订购发生跨越中。织物在并行的与交易提交通过其他 应用。

Key:

代言人			帐
犯同行			应用
订购 节点			
聪明 合同			e恩多Rse米恩t政策
(链码)			



超期分类帐结构








订单提供自所有犯同行

订购服务收集交易到提出块适用于分布自犯同行。同行可以提供自其他对等方在a层次 结构(不)。

不同订购算法 可用:

- 独奏(单个节点,发展)
- 卡夫卡(撞车故障 公差)

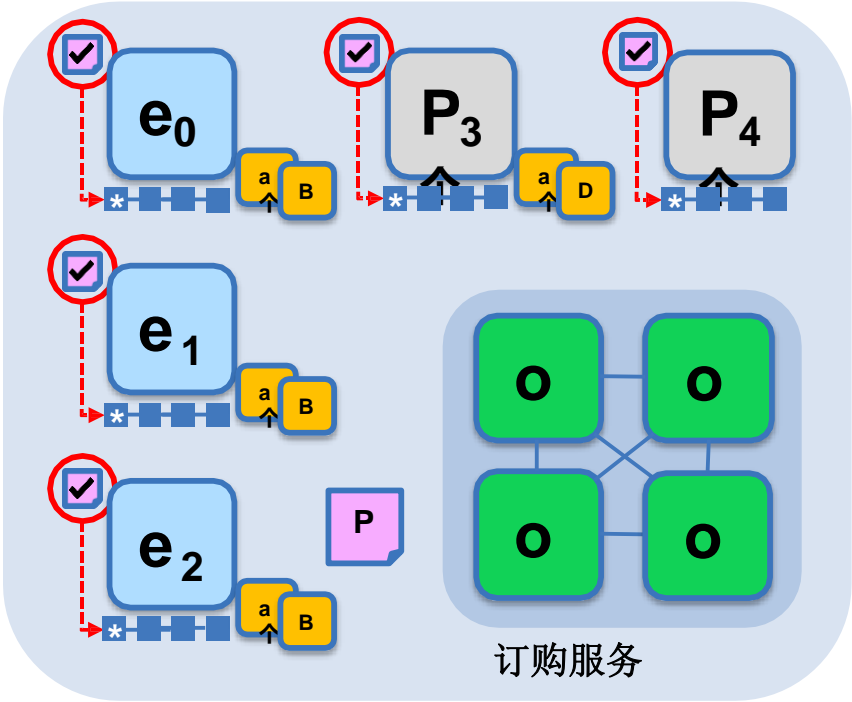
Ke Y:

代言人			帐
犯同行			应用
订购节点			
聪明合同			e恩多Rse米 恩t政策

样本交易记录:步6/7-验证 交易

客户a个
Pp李约t我
不, 不, 不n

S
D
K



超期分类帐结构

犯同行验证交易

每犯同行验证针对中。背书政策。也检查乌尔曼集都是还有效适用于当前世界 状态。

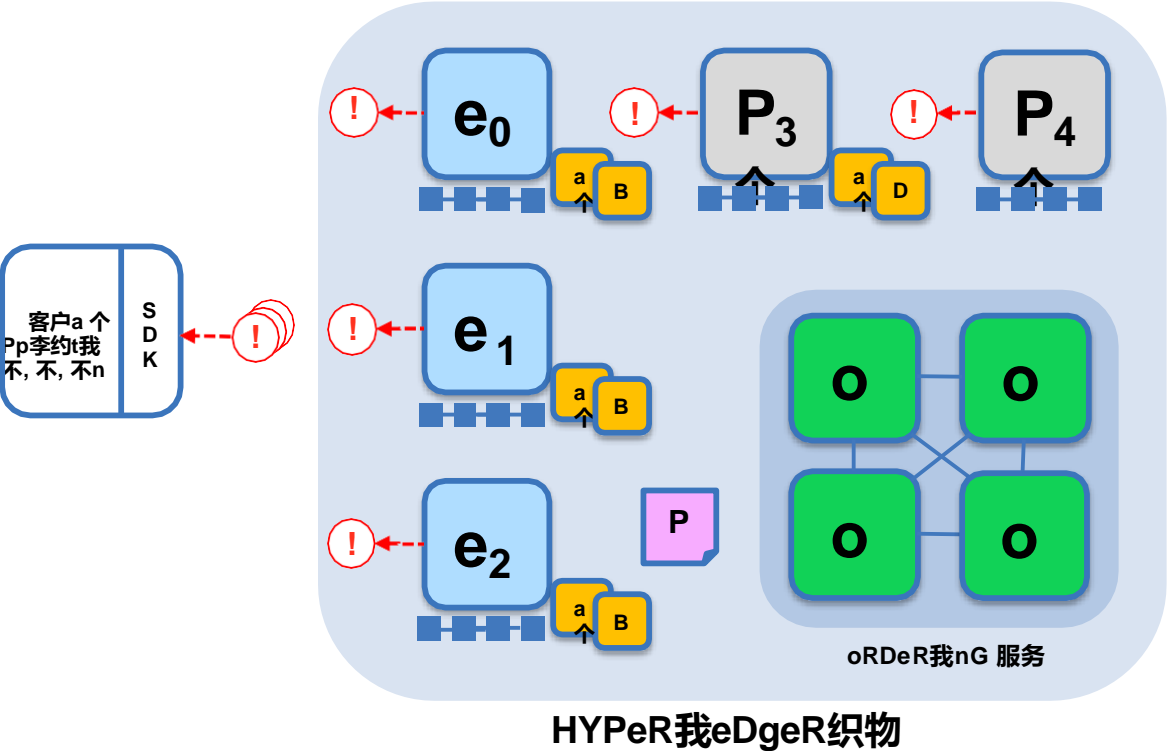
验证交易都是应用自中。世界状态并保留上中。 帐。

无效交易都是也保留上中。 帐但做不更新世界 状态。

Ke Y:

代言人			帐
犯同行			应用
订购节点			
聪明合同			e恩多Rse米恩t政策
(链码)			

样本交易记录:步"7"-通知 交易



犯同行通知应用

应用可以注册自是通知当交易成功或失败和当块都是添加自中。 帐。

应用程序将是通知通过每个对等自其中他们都是 连接。

Ke Y:

代言人			帐
犯同行			应用
订购 节点			
聪明 合同			e恩多Rse米恩t政策
(链条 代码)			

结束！

धन्यवाद

Hindi 印地
语

多謝

繁体中文

ขอบพระคุณ

泰语

Спасибо

俄语

谢谢

西班牙语

شكراً

阿拉伯语

谢谢

英语

奥布里加
多

巴西葡萄牙语

格拉齐

意大利
语

多谢

简体中文

丹克

德语

谢谢

法语

நன்றி

Tamil

泰米尔
语

ありがとうございました

日语

감사합니다

朝鲜语