



基于Hyperledger的区块链应用研究

5130369007 罗祖添 指导教师：黃征

2017年6月



上海交通大学
SHANGHAI JIAO TONG UNIVERSITY

1

应用研究背景

2

我们的贡献

3

区块链技术与Hyperledger

4

数字证书颁发与验证系统

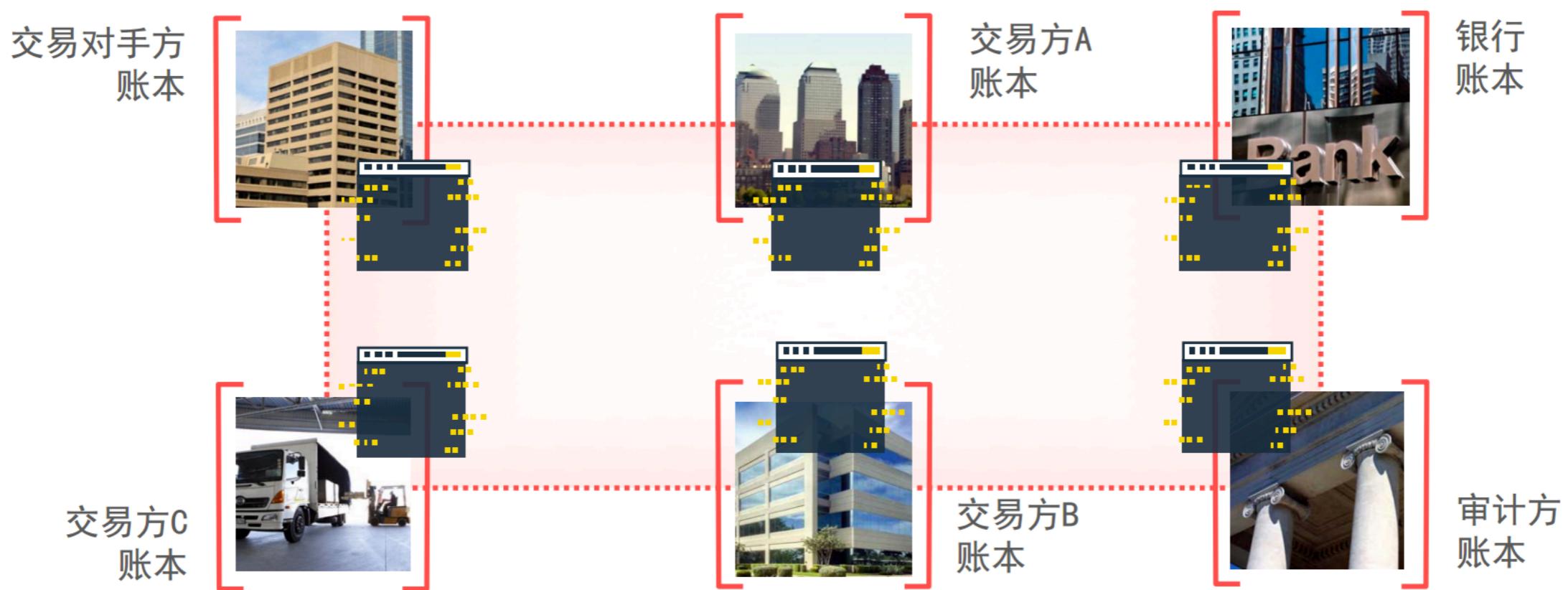
5

基于供应链的产品溯源系统



术语解释：商业网络、区块链技术

- 商业网络的构成：账本、交易、资产、合约。
- 区块链网络中的交易各方不依赖于第三方来仲裁交易（去中心化），它们使用一致性协议（即共识机制）来共同维护账本内容，使用哈希算法和数字签名来确保交易的完整性和不可逆性。



区块链技术：商业网络下一个解决方案的灵感？

- 现有的商业网络方案有不足之处

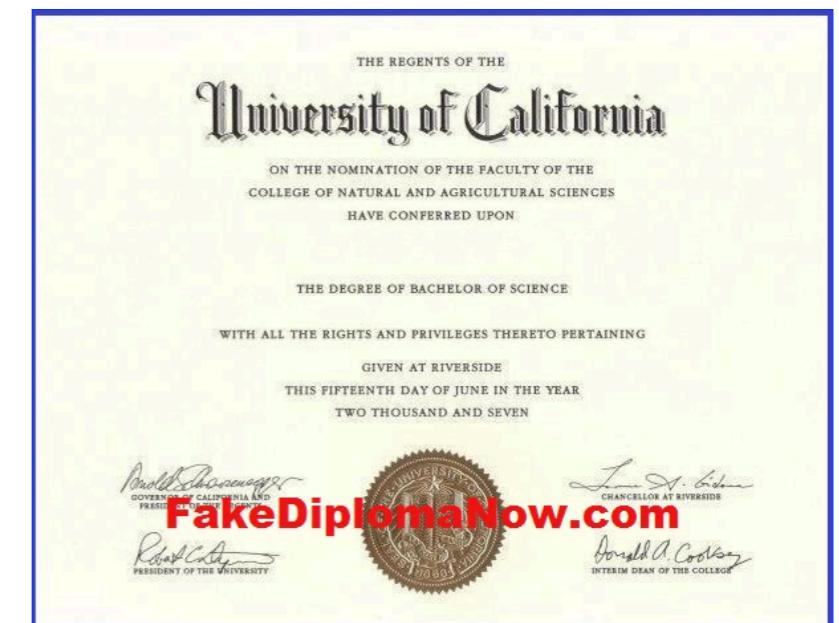
- 中心化体系的机制的内部弊病
- “假”现象层出不穷
- 相应防范措施与验证手段不力



伪造物流信息的快递点

- 区块链技术或能提供新的解决方案

- 比特币体系成功运转的启示
- 基于共识机制、不可篡改、交易不可逆
- 应用场景广泛



专门提供假学历证书的网站

领域现状 (@CoinDesk2017共识大会, 2017/05)

- IBM研究总监提出区块链技术可以为**资本市场和海运业节省几十亿美元的成本**, 并以马士基的合作为例, 解释区块链如何通过简化整个流程, 来增加流程的可控性, 进而降低成本, 保证运输产品利润率。
- 普华永道、阿里巴巴、澳洲多家食品公司、澳大利亚及新西兰邮政就全新**食品供应区块链项目**进行测试, 以减少食品供应链中的欺诈问题。该项目将在未来13周内构建成型。



1

应用研究背景

2

我们的贡献

3

区块链技术与Hyperledger

4

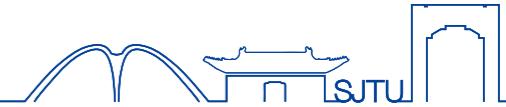
数字证书颁发与验证系统

5

基于供应链的产品溯源系统



我们的贡献



- 基于Hyperledger，提出若干商业网络的解决方案，并搭建相应的区块链应用
 1. 数字证书颁发与验证系统 - 基于Hyperledger Fabric（简称HLF）0.6版本
 2. 供应链上的产品追踪与溯源系统 - 基于HLF 1.0版本与Hyperledger Composer
- 对搭建的区块链应用进行评估、改进与探索
 - 项目中期，发现HLF 0.6版本存在不足之处（安全性、机密性、可扩展性），采用最新版本的HLF 1.0 Alpha开发第二个应用
 - 项目后期，关注更加复杂、前人试水更少的供应链，并尝试使用最新的Composer套件搭建AngularJS应用，总结出新的区块链应用搭建流程
 - 研究不止，展望商业网络与区块链技术融合的新方向——与数据分析相结合，为风险管理与评估服务

1

应用研究背景

2

我们的贡献

3

区块链技术与Hyperledger

4

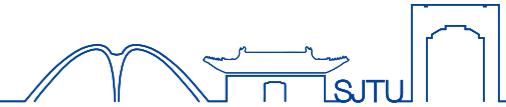
数字证书颁发与验证系统

5

基于供应链的产品溯源系统



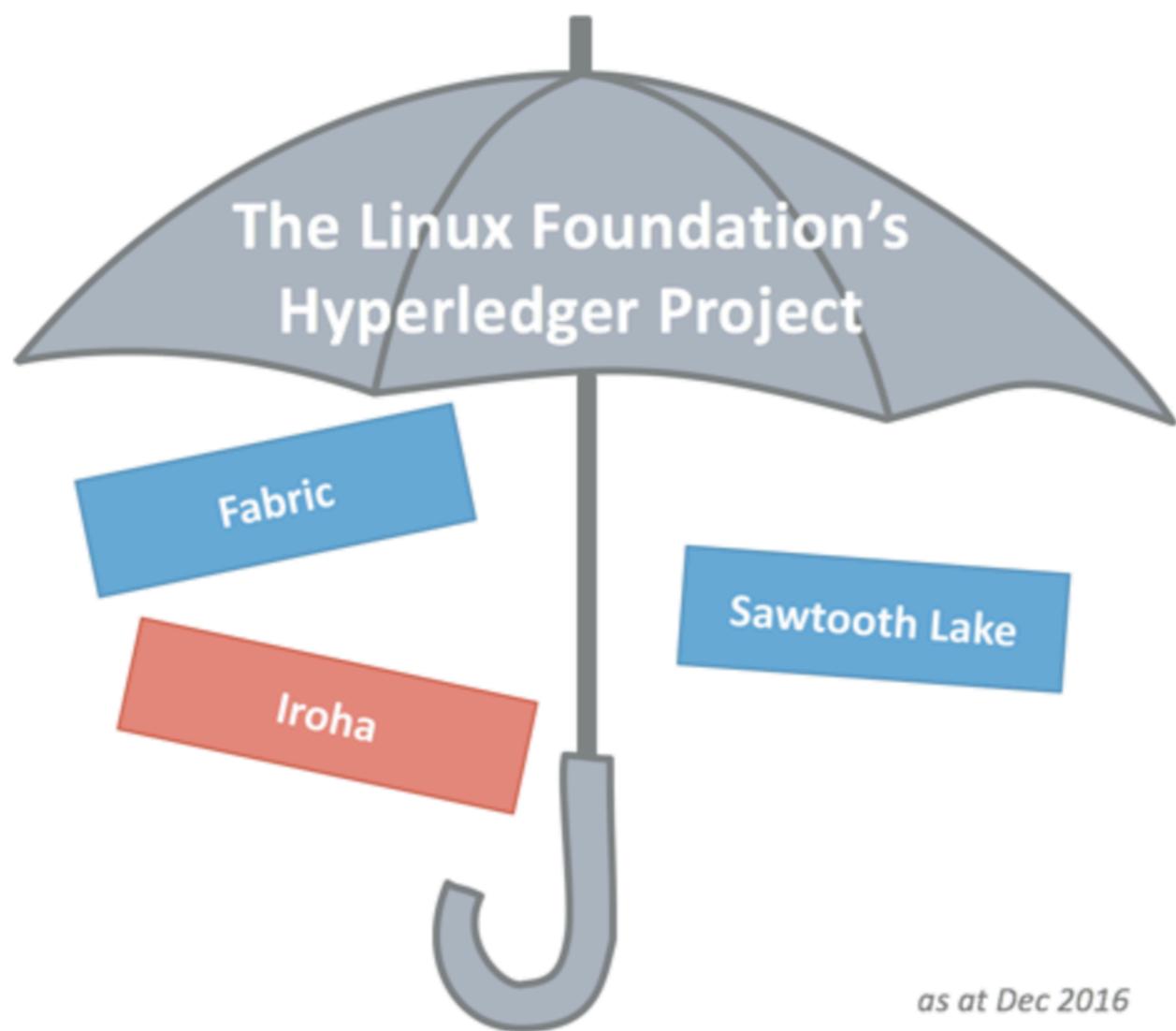
时下流行的区块链平台



	比特币 (Bitcoin)	以太坊 (Ethereum)	超级账本
性质	货币交易平台	货币交易开发平台	面向企业的区开发平台
货币	比特币	以太币	无
共识机制	工作证明	工作证明	PBFT, 可插拔
权限	公开	公开/带权限访问	带权限访问
智能合约	Script (功能局限)	Solidity (图灵完备)	Go或JAVA

- 选择Hyperledger的理由：
 - 工作证明机制适用于无监督的开放平台，与商业网络不符。
 - 带权限访问的共享账本（亦称“联盟链”）相较于公开账本（“公有链”），更符合实际商业网络的情景。
 - “货币”的概念在商业网络中应被弱化，否则区块链技术的应用范围将受限。
 - 我们搭建的区块链应用是基于商业网络的，与其面向企业的初衷相符合。

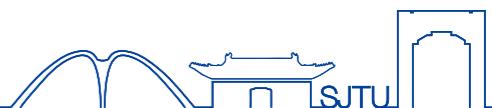
Hyperledger子项目



- Fabric
 - 区块链技术的实现, “骨架”
 - 可插拔共识机制, 目前支持 PBFT, 较成熟
- Sawtooth Lake
 - 高度模块化的分布式账本平台
 - 目前处于试验阶段
- Iroha
 - 轻量级的分布式账本, 移动应用



Hyperledger Fabric逻辑架构

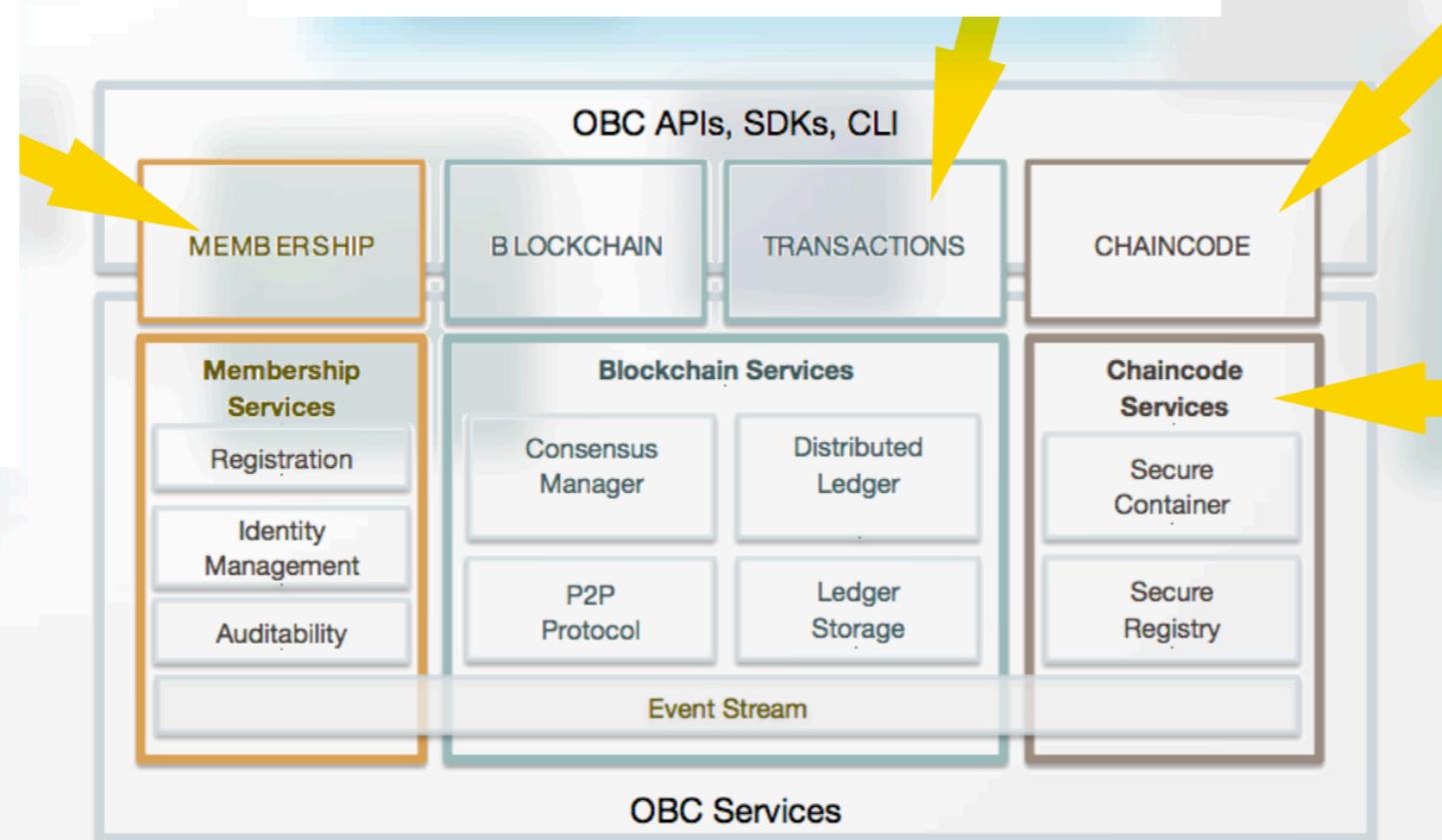


成员管理 (Membership)

- 成员管理提供会员注册、身份保护、内容保密、交易审计功能
- OBC所有成员必须经过许可才可以发起交易，这一点不同于公有链（所有参与方不需要登录，可直接提交）
- OBC成员发起交易时，若启用Transaction Certificate Authority (TCA)功能，则交易证书会保护成员ID不被无关方看到

区块服务（Blockchain & Transactions）

- 区块服务用于维护全网一致的分布式账簿
- 基于P2P的通信网络（gRPC），通过HTTP的报文实现节点之间的消息传输
- 高度优化设计，使状态同步高效可靠
- 共识算法（PBFT, Raft, PoW, PoS）模块化，可插式



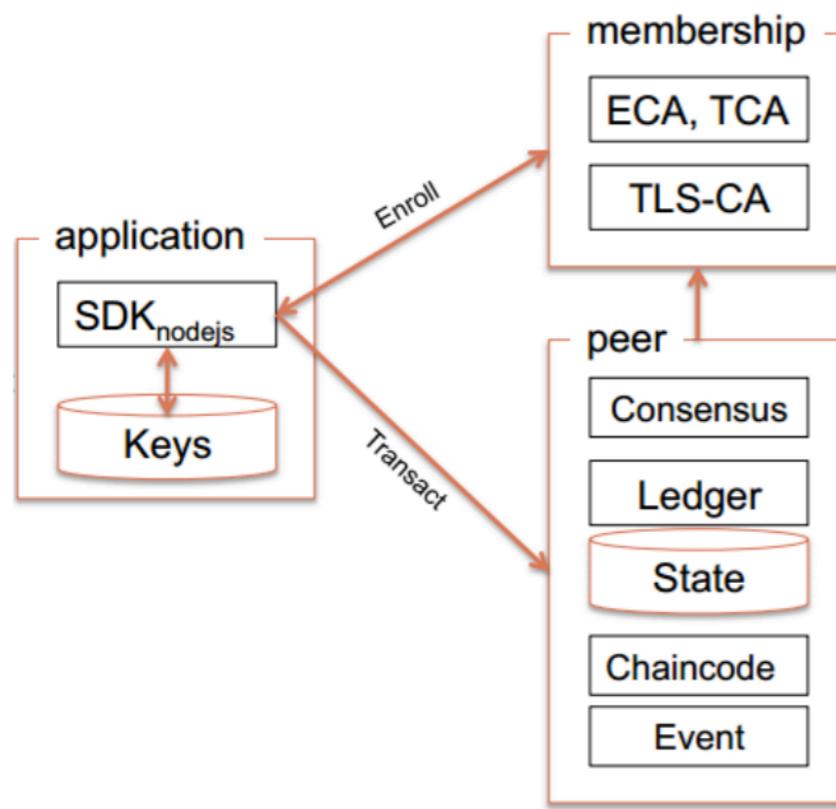
页面封装

- OBC提供REST API来访问各种服务
- OBC也提供CLI客户端工具，使开发人员能够快速测试账链代码（Chaincode），或者查询交易情况。CLI工具由Go语言编写，目前只支持部分REST API

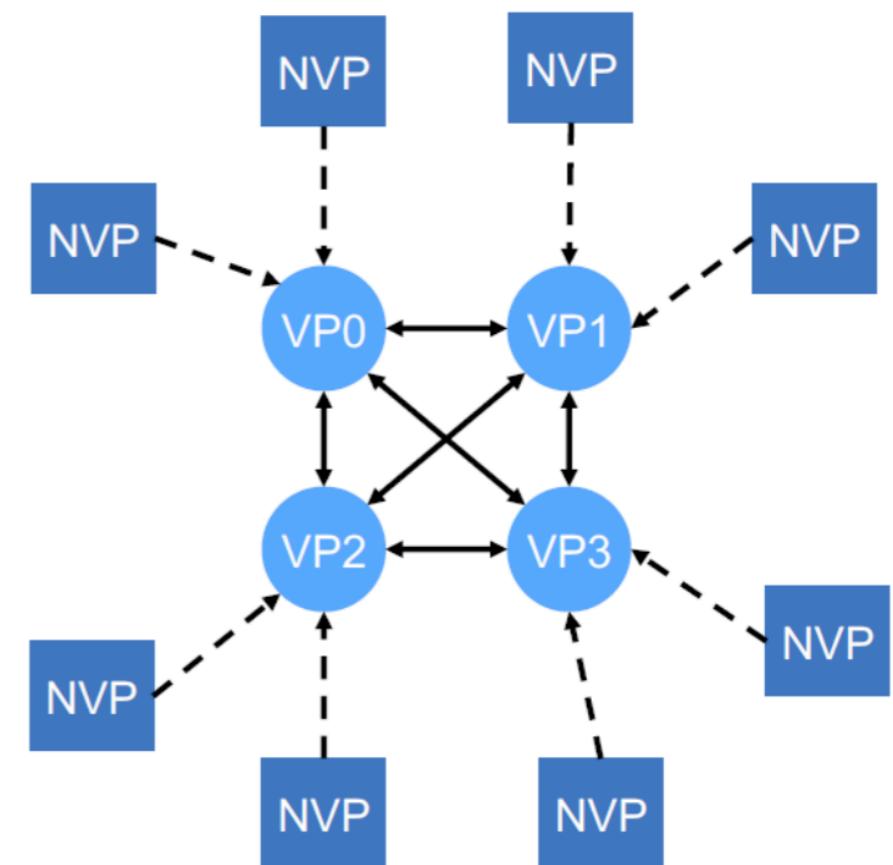
账链代码（ChainCode）

- 账链代码用于构成智能合约（Smart Contract）
- 它嵌在交易中，所有确认节点在确认交易时都必须执行它
- 执行环境是一个“沙箱”（Docker）
- 目前支持Go，将来支持Java, Node.js

Hyperledger Fabric 0.6



运行架构



网络拓扑

1

应用研究背景

2

我们的贡献

3

区块链技术与Hyperledger

4

数字证书颁发与验证系统

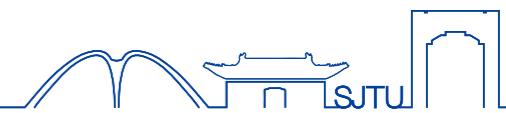
5

基于供应链的产品溯源系统

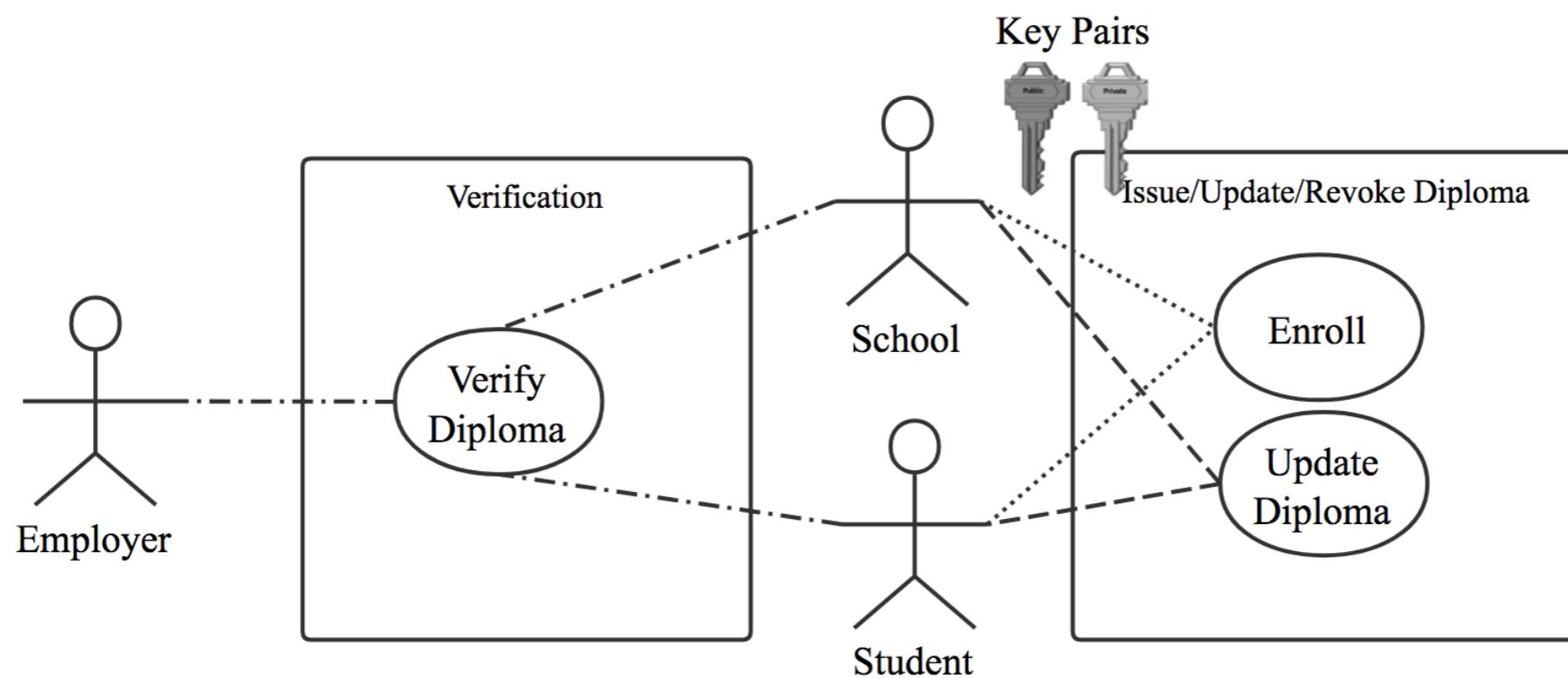




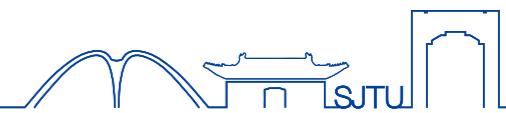
数字证书颁发与验证系统



- 提供数字学历证书的颁发、验证服务
 - 基于HLF v0.6 (Go Chaincode + Fabric CLI)
 - 参与者：学校、学生、任意需要验证数字学历证书的用户
 - 用例图如下所示



数字证书颁发与验证系统



- 提供数字学历证书的颁发、验证服务

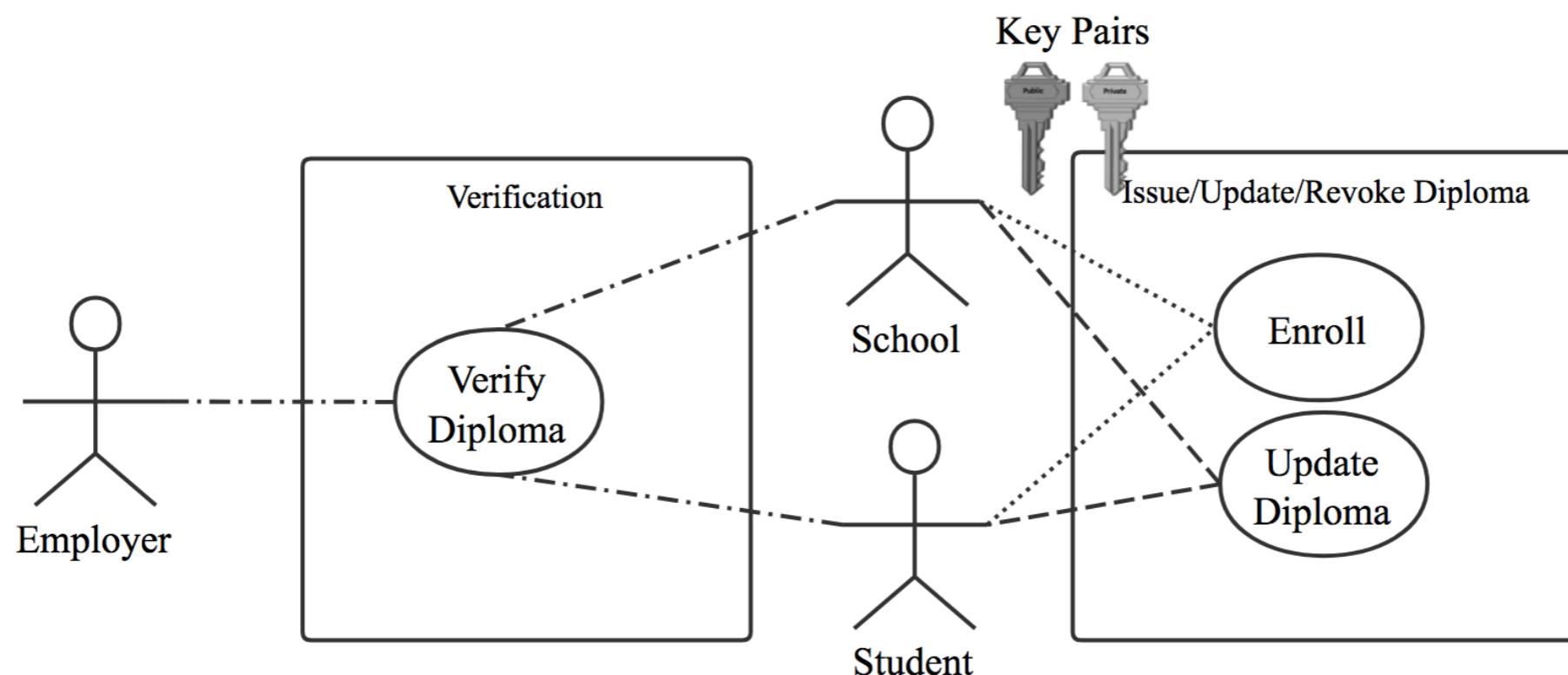
School Name: SJTU

Address: bb2785f578f16601b2274586dd41de6d

PubKey - N (modulus): 99479564460341971246989239187620075502725982343459679777799681460985437954919

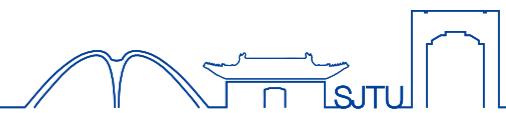
PubKey - E (exponent): 65537

- 学校在注册（实例化）阶段时，客户端会在本地生成一对RSA 2048位的公私钥对，用以签名与验证。私钥由学校保存，公钥公开。

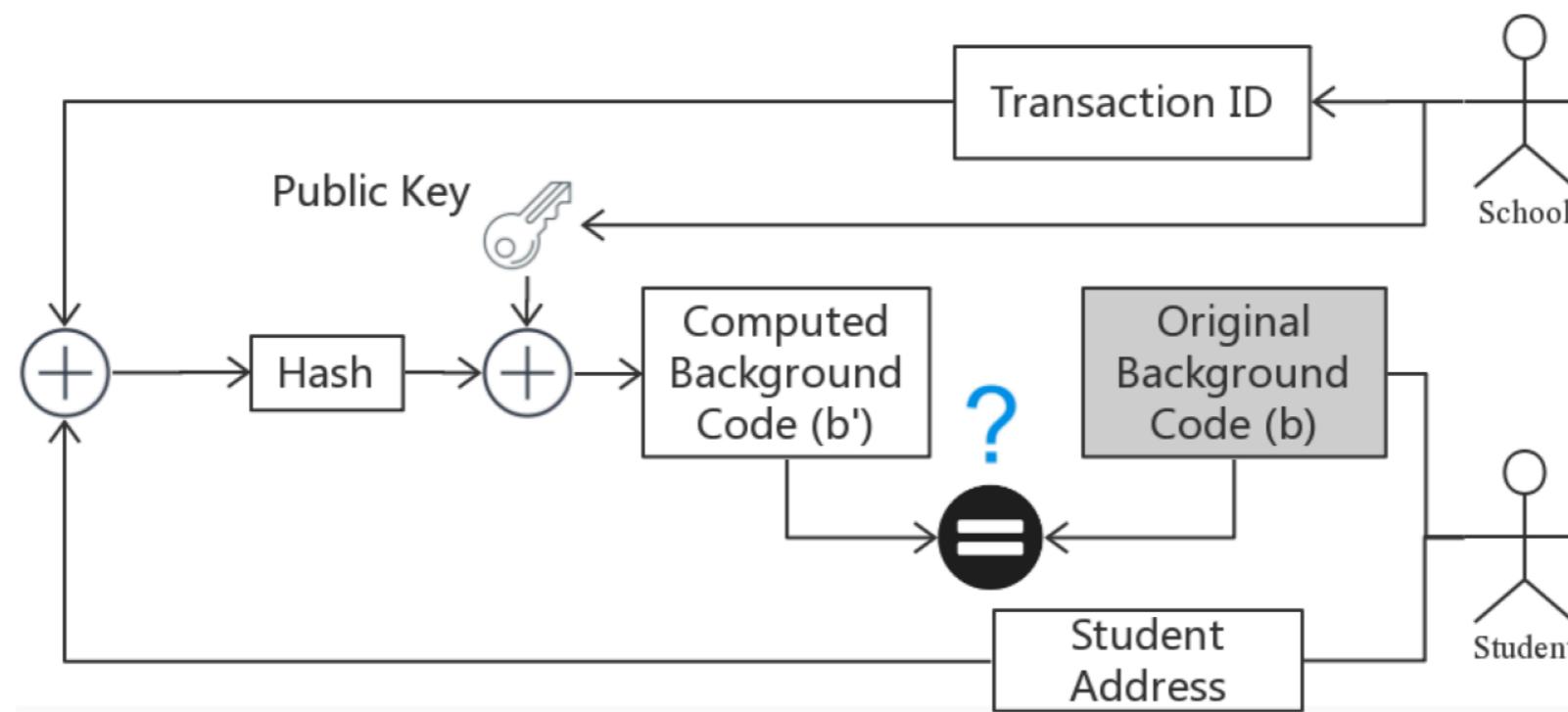




数字证书颁发与验证系统



- 系统以48位随机数唯一标识学校和学生，被称为**地址**（Address）
- 验证码 $b = E(Hash(TXid, a_{st}))_{K_{scPri}}$
- 核心思想：**值匹配**。（验证时长：2-3s，4节点）





Hyperledger Fabric v0.6 不足之处

- 传统意义上联盟链的性能瓶颈
- 不够成熟的商业网络架构
- 某些攻击方法仍然有效

1

应用研究背景

2

我们的贡献

3

区块链技术与Hyperledger

4

数字证书颁发与验证系统

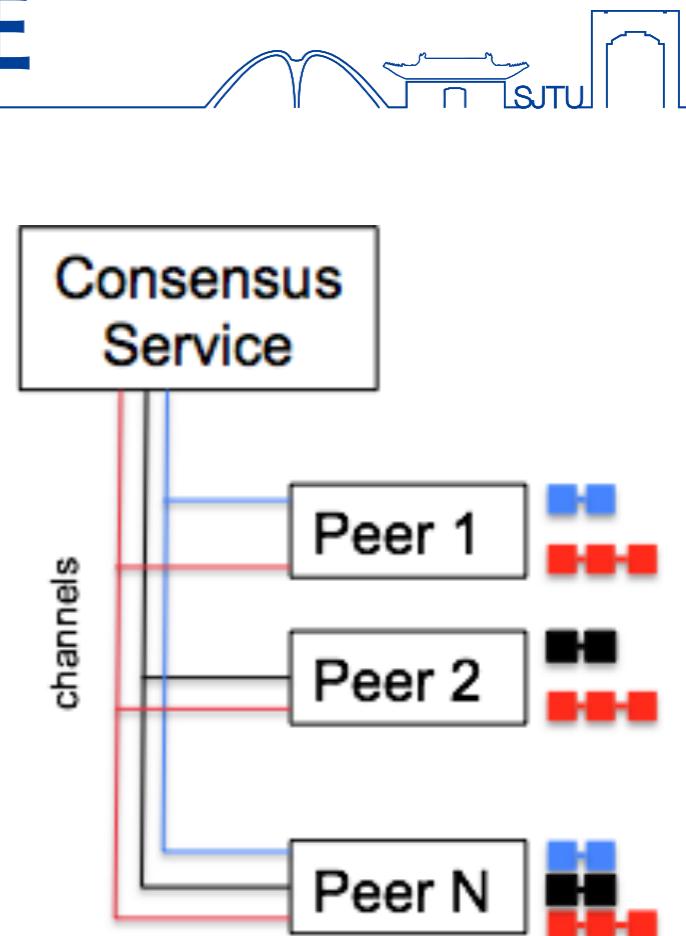
5

基于供应链的产品溯源系统



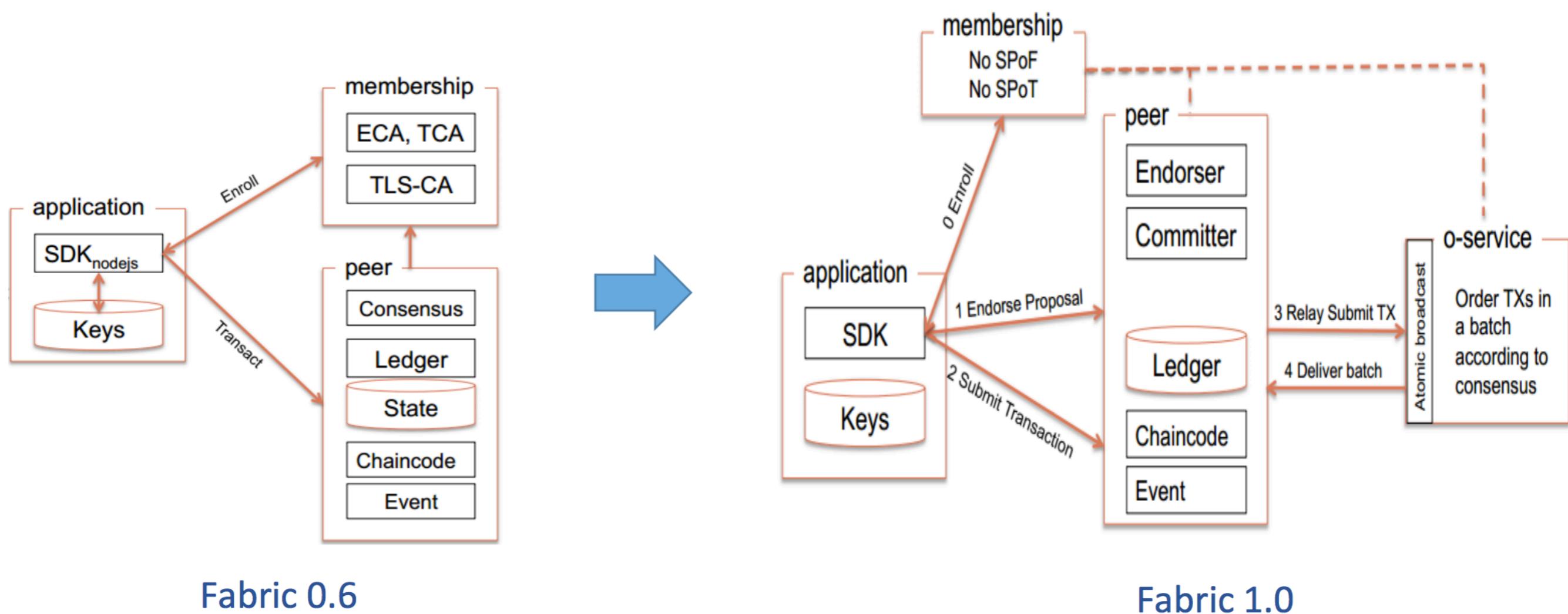
Hyperledger Fabric v1.0 新特性

- 引入背书策略
- 多链、多通道体系 - “分而治之”
- 交易流程得到改进，性能得到提升
- 提供可插拔式数据库，增大吞吐量
- 优化了成员服务，改为Client+Server模式的CA
(*Certificate Authority*) 服务





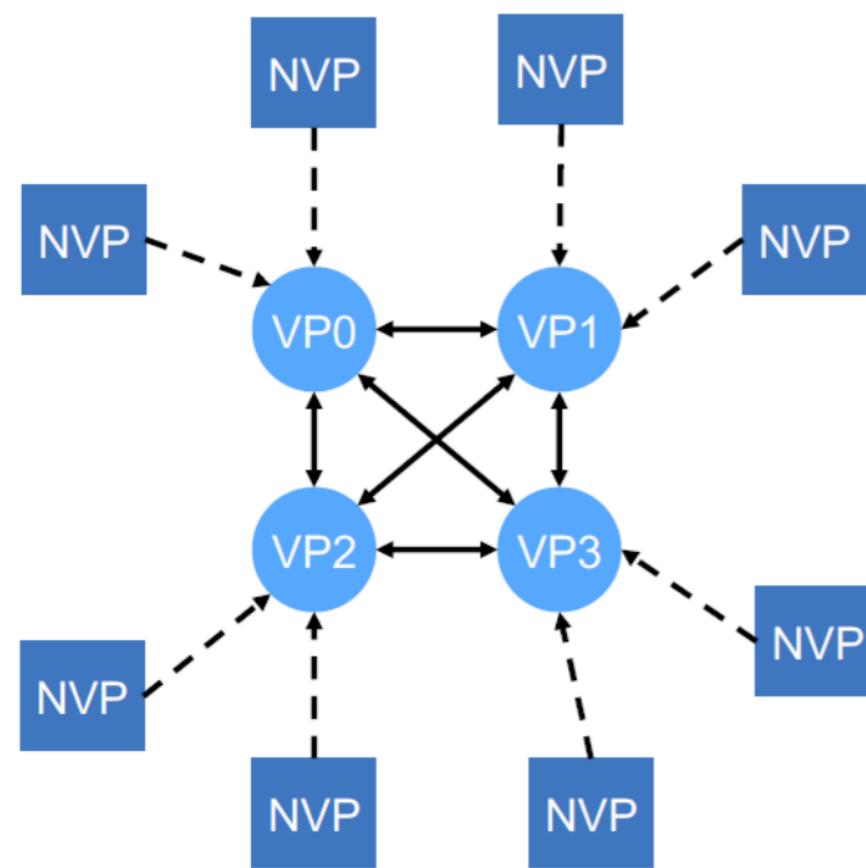
Hyperledger Fabric运行时架构 (基于Docker)



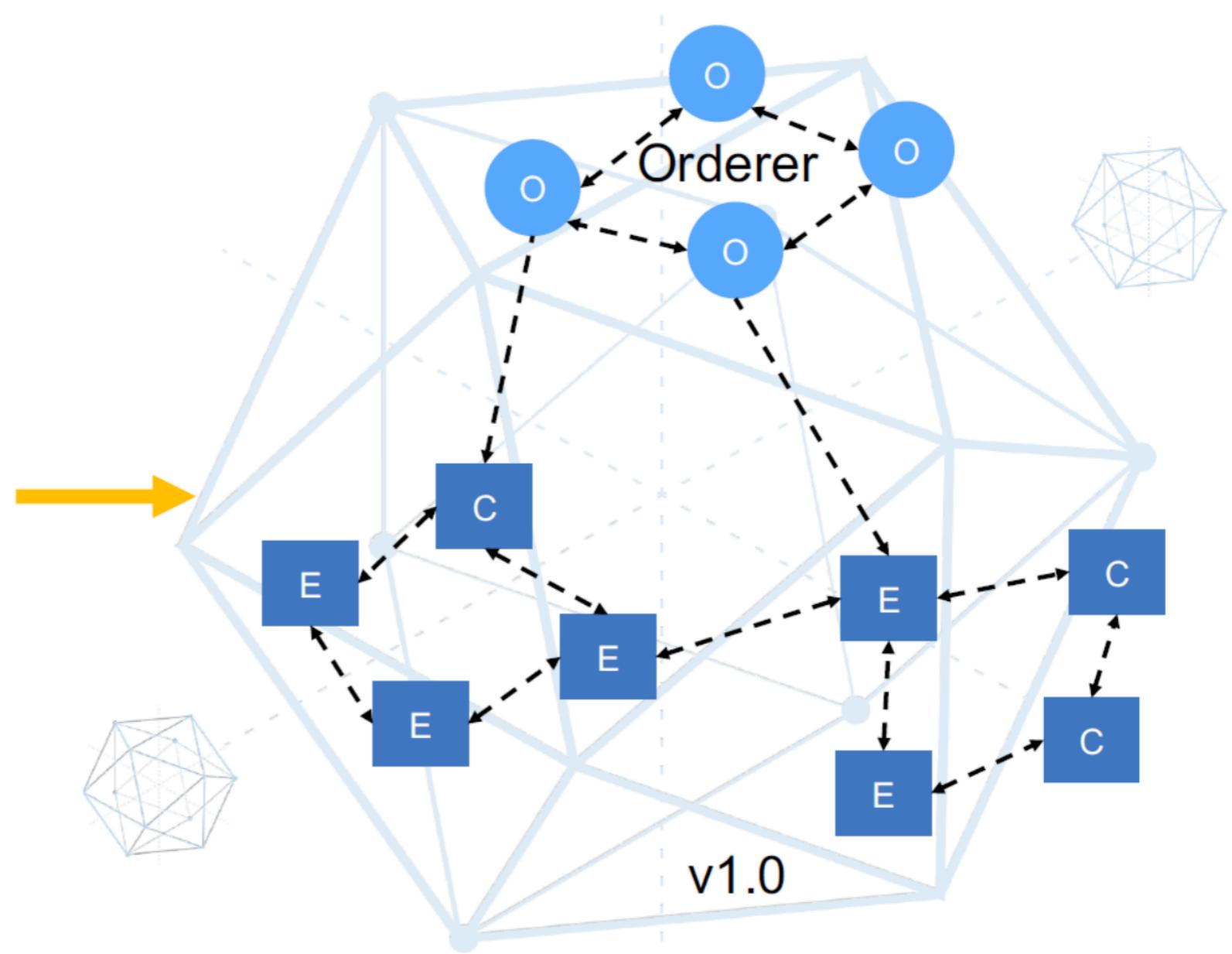
Fabric 0.6

Fabric 1.0

Hyperledger Fabric网络拓扑

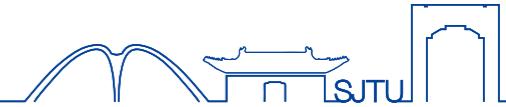


v0.6

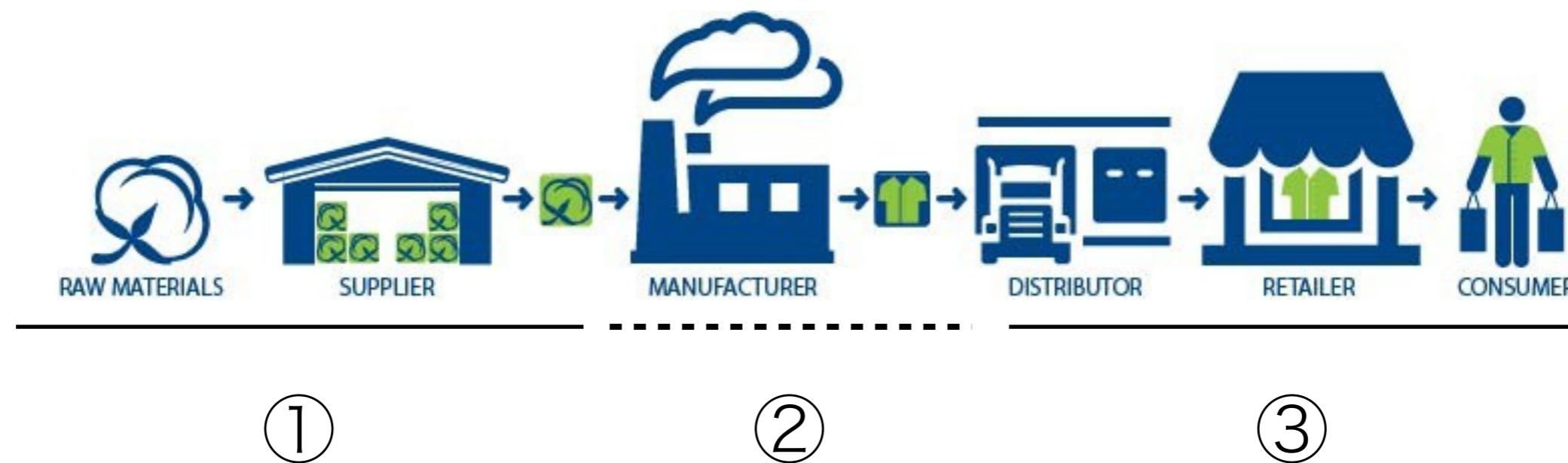


(Image Credit: <http://ibm.biz/hyperledger0301>)

基于供应链的产品溯源系统

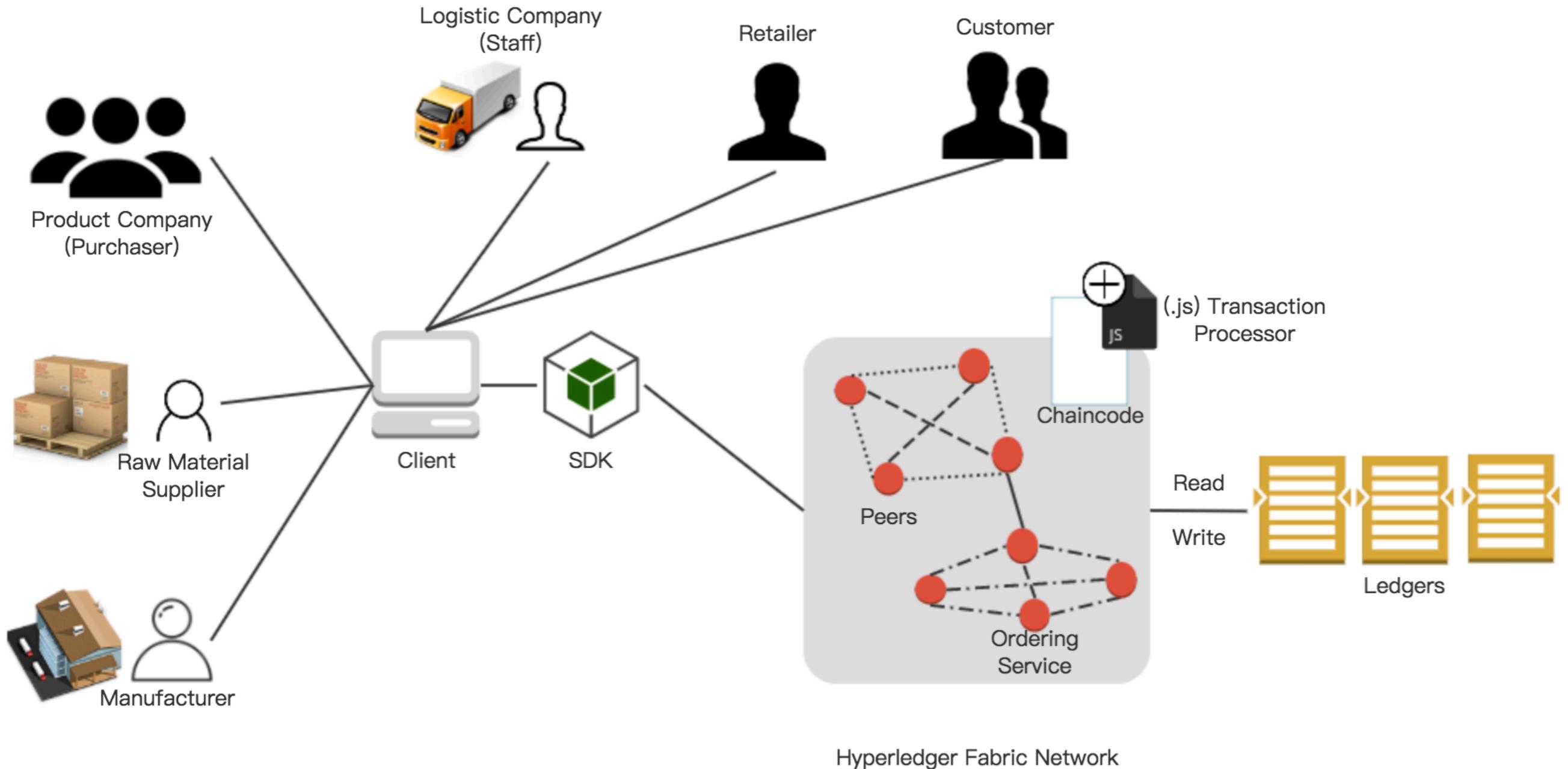


- **供应链**：由原料获取、加工、并将成品送到用户手中这一过程所涉及的企业和企业部门组成的网络。
- **产品溯源系统**：仅关注产品生产与运输。三个子环节：①原料采购与运输 ②产品生产与加工 ③产品送至终端用户

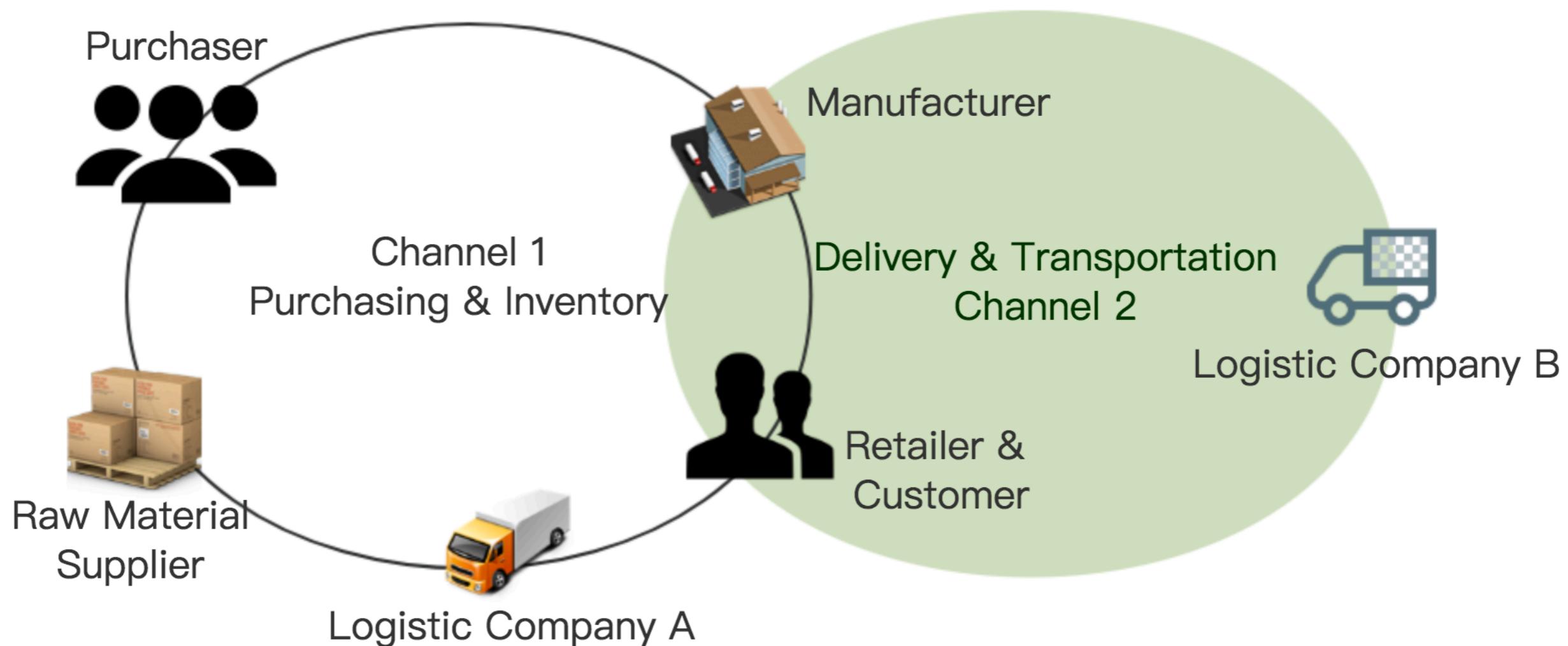


(Image Credit: <https://www.swtc.edu/academics/programs/business/supply-chain-management>)

产品溯源系统 - 架构



产品溯源系统 - 角色与通道

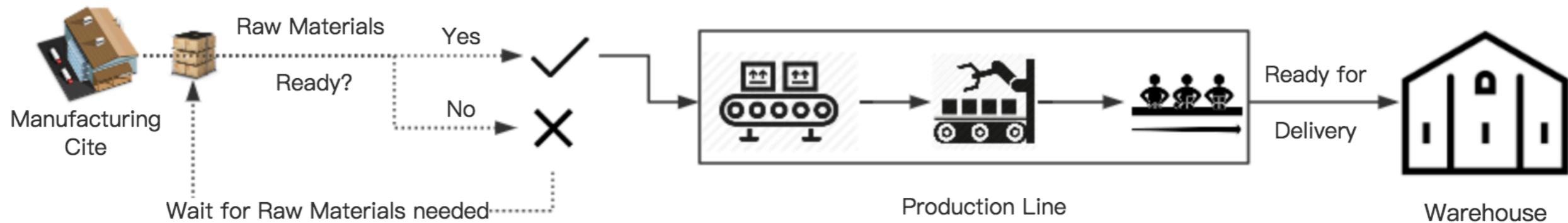


产品溯源系统 - 子环节

- 原料采购与运输



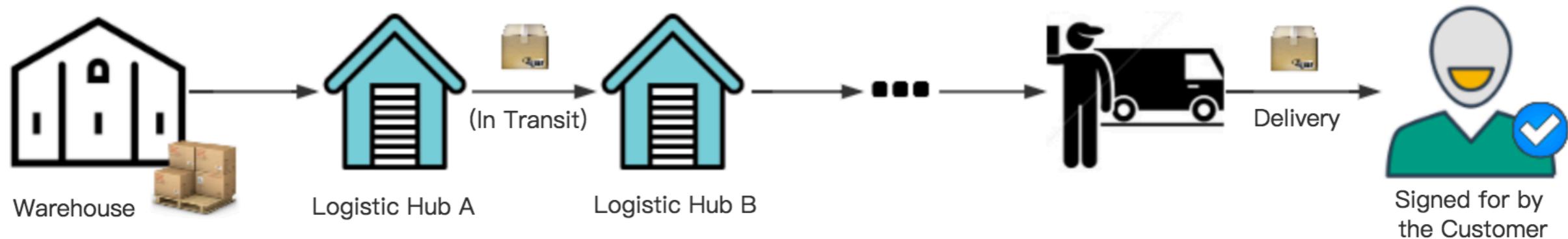
- 产品生产与加工





产品溯源系统 - 子环节

- 产品送至终端用户

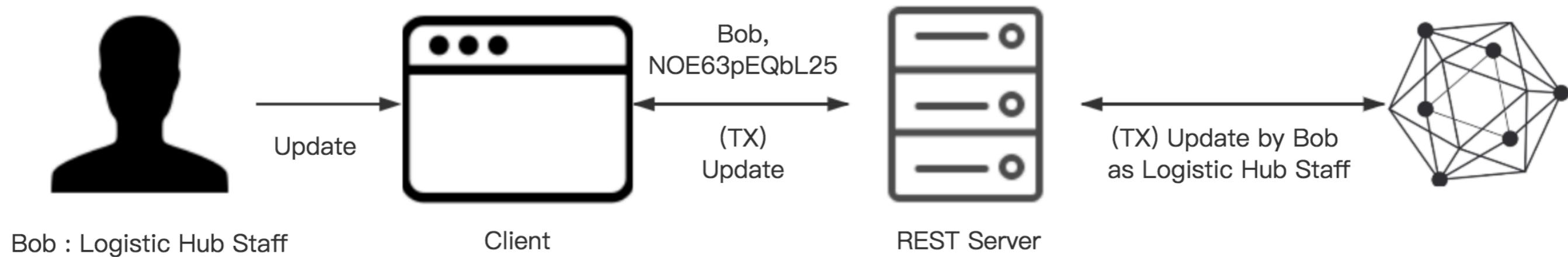
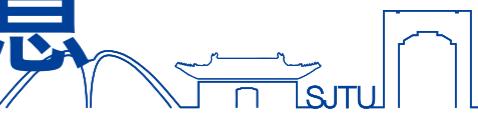


- 使用Hyperledger Composer搭建的子应用：物流信息跟踪系统

localhost:4200/Shipment						Search	Star	Bookmark	Download	Home	Logout	Menu
												Delete Asset
1017	ELECTRONIC_COMPONENTS	IN_TRANSIT	resource:com.biz.Facility#2601	resource:com.biz.Facility#1017	resource:com.biz.PIC#halina.dellen@dellen.com.au							Update Asset Delete Asset
1018	METALS	IN_TRANSIT	resource:com.biz.Facility#2601	resource:com.biz.Facility#1018	resource:com.biz.PIC#ryann@hotmail.com							Update Asset Delete Asset
1019	BULK_PRODUCT	IN_STATION	resource:com.biz.Facility#2601	resource:com.biz.Facility#1019	resource:com.biz.PIC#svugteveen@vugteveen.net.au							Update Asset Delete Asset

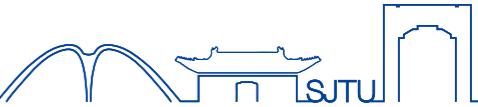


物流信息跟踪系统 - 如何更新物流信息



- Bob在客户端以物流中转站员工身份登录Fabric P2P网络中一个节点
- Bob发送物流信息更新交易，客户端通过服务器与Fabric交互
- 交易执行完毕后，结果返回；Bob可以通过客户端查看执行情况

物流信息跟踪系统 - RESTful服务器



Hyperledger Composer REST server

com_biz_Facility : An asset named Facility

[Show/Hide](#) | [List Operations](#) | [Expand Operations](#)

GET	/com.biz.Facility	Find all instances of the model matched by filter from the data source.
POST	/com.biz.Facility	Create a new instance of the model and persist it into the data source.
GET	/com.biz.Facility/{id}	Find a model instance by {{id}} from the data source.
HEAD	/com.biz.Facility/{id}	Check whether a model instance exists in the data source.
PUT	/com.biz.Facility/{id}	Replace attributes for a model instance and persist it into the data source.
DELETE	/com.biz.Facility/{id}	Delete a model instance by {{id}} from the data source.

com_biz_PIC : A participant named PIC

[Show/Hide](#) | [List Operations](#) | [Expand Operations](#)

com_biz_Shipment : An asset named Shipment

[Show/Hide](#) | [List Operations](#) | [Expand Operations](#)

com_biz_ShipmentArrive : A transaction named ShipmentArrive

[Show/Hide](#) | [List Operations](#) | [Expand Operations](#)

com_biz_ShipmentDepart : A transaction named ShipmentDepart

[Show/Hide](#) | [List Operations](#) | [Expand Operations](#)

System : General business network methods

[Show/Hide](#) | [List Operations](#) | [Expand Operations](#)

[BASE URL: /api , API VERSION: 0.0.1]

物流信息跟踪系统 - 操作界面

101	CHEMICALS	Update Asset	
1010	CHEMICALS	trackingId	1010
1011	BULK_PRODUCT	shipmentContentsType	CHEMICALS
1012	CHEMICALS	shipmentStatus	IN_TRANSIT
1013	CHEMICALS	destination	resource:com.biz.Facility#2601
1014	AMBIENT	currentLocation	resource:com.biz.Facility#1010
1015	ELECTRONIC_COMPONENT	person_in_charge	resource:com.biz.PIC#lynelle.koury@koury.net.au
1016	ELECTRONIC_COMPONENT		resource:com.biz.PIC#della.selestewa@gmail.com
1017	ELECTRONIC_COMPONENT		resource:com.biz.PIC#homasena@gmail.com
1018	METALS		resource:com.biz.PIC#fschimke@schimke.com.au
1019	BULK_PRODUCT	IN_STATION	resource:com.biz.Facility#2601
			resource:com.biz.Facility#1019

Update Asset

trackingId

shipmentContentsType

shipmentStatus

destination

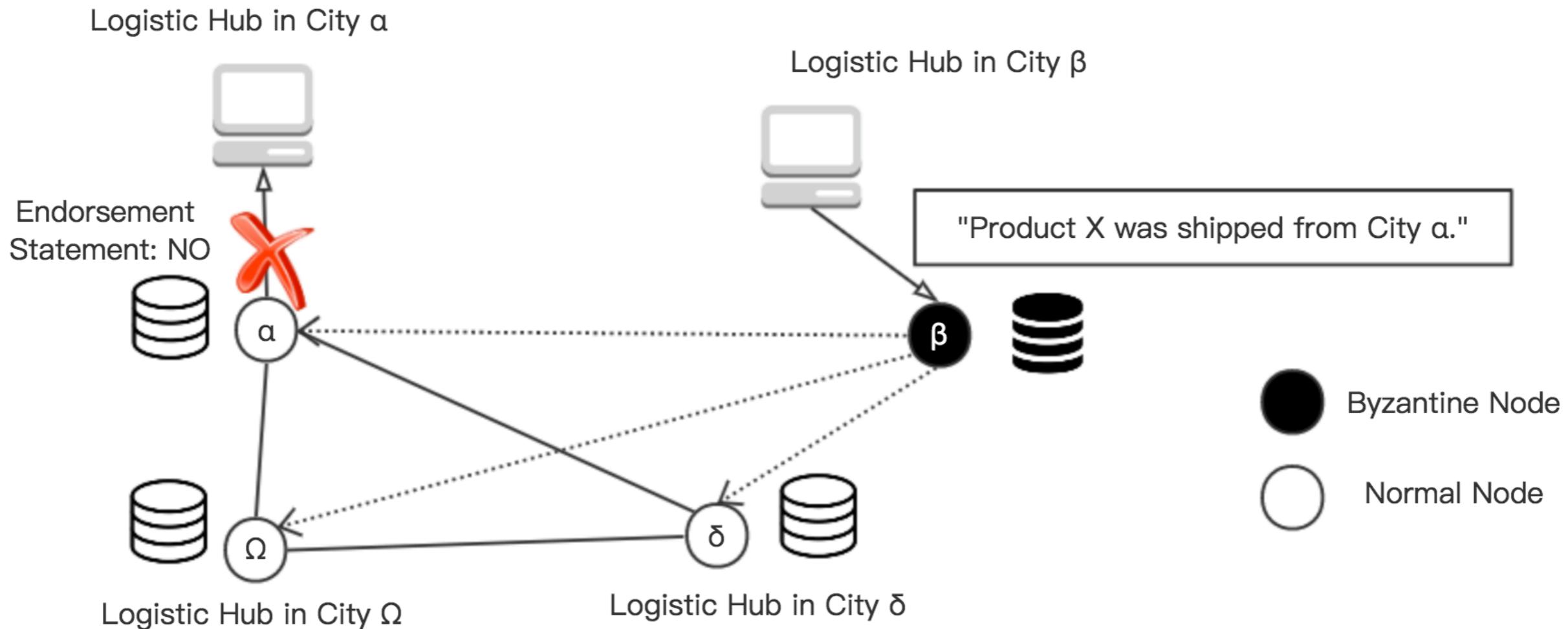
currentLocation

person_in_charge

Submit Close



产品溯源系统的可靠性



以物流点 β 身份发送的虚假物流信息“货物已从物流点 α 发出”无法通过背书环节
原因：物流点 α 维护的账本中无此记录，物流点 β 无发送该消息的权限



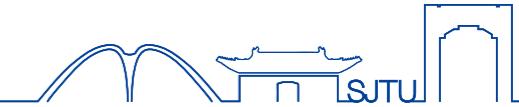
产品溯源系统的性能

■ 交易处理速度/响应时间

- P2P网络构成：1 排序服务节点 + 2 背书节点 + 1 CA
- 配置：2GB RAM + 1核CPU（阿里云香港服务器/本地虚拟机服务器）
- 剔除因网络中断而产生的异常值
- 发送交易：2000条/服务器，串行
- 平均响应时间：1.21秒/条
- 最大有效响应时长：8.30秒/条
- 最小有效响应时长：0.47秒/条



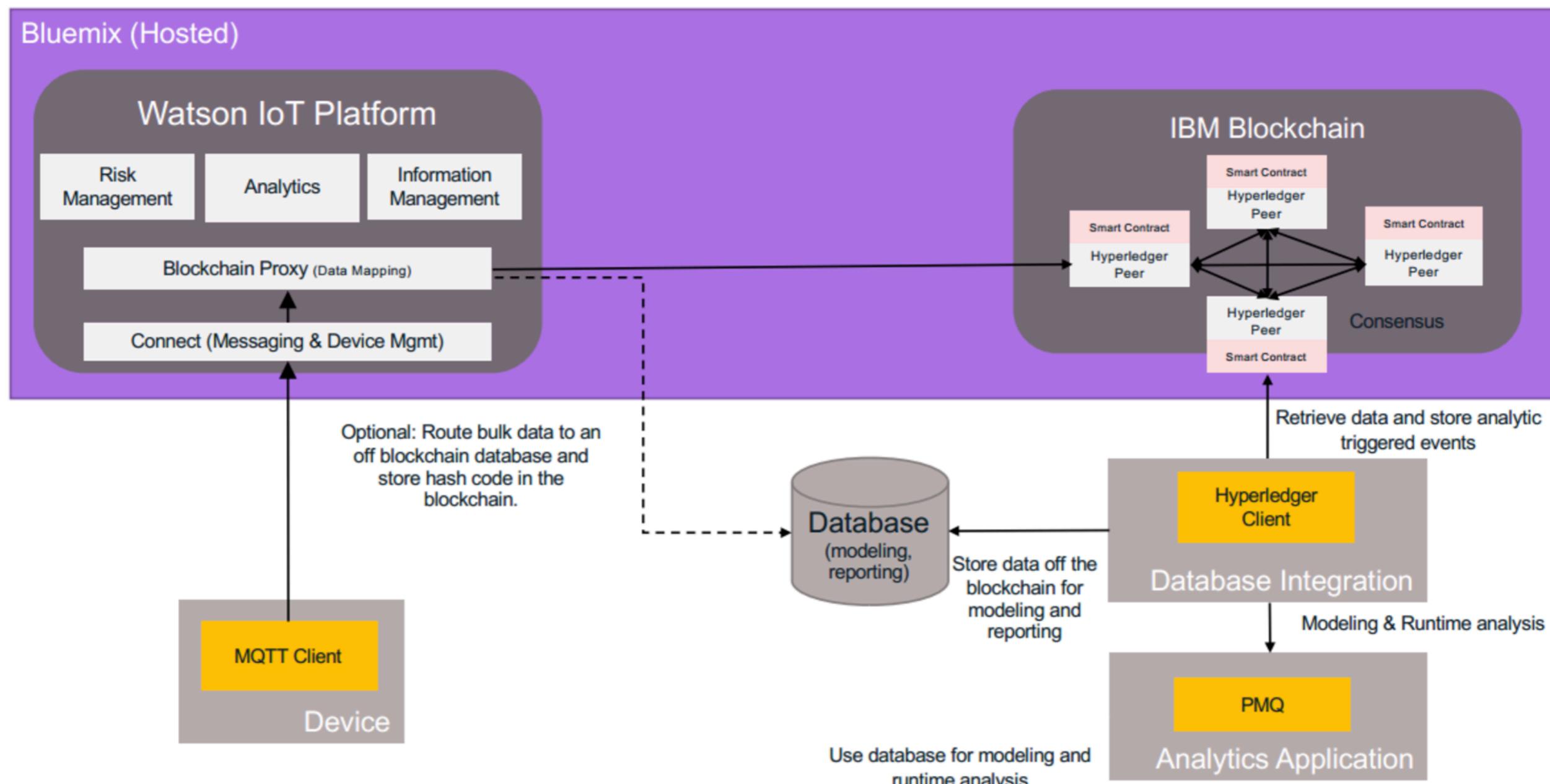
产品溯源系统的性能



▪ 吞吐量

- P2P网络构成：4 排序服务节点 + 4 背书节点 + 2 Kafka + 1 zookeeper
- 内置**GoLevelDB**
 - 测试模式：以280-350条/秒的速度发送交易，120个线程
 - 共36000条交易，104.455秒完成响应，吞吐量为344条/每秒
- **CouchDB**
 - 在相同的测试速度+仅50个线程时挂起，无法完成压力测试

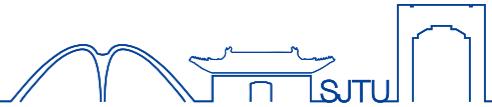
展望：与数据分析相结合，为风险管理与评估服务



Q&A

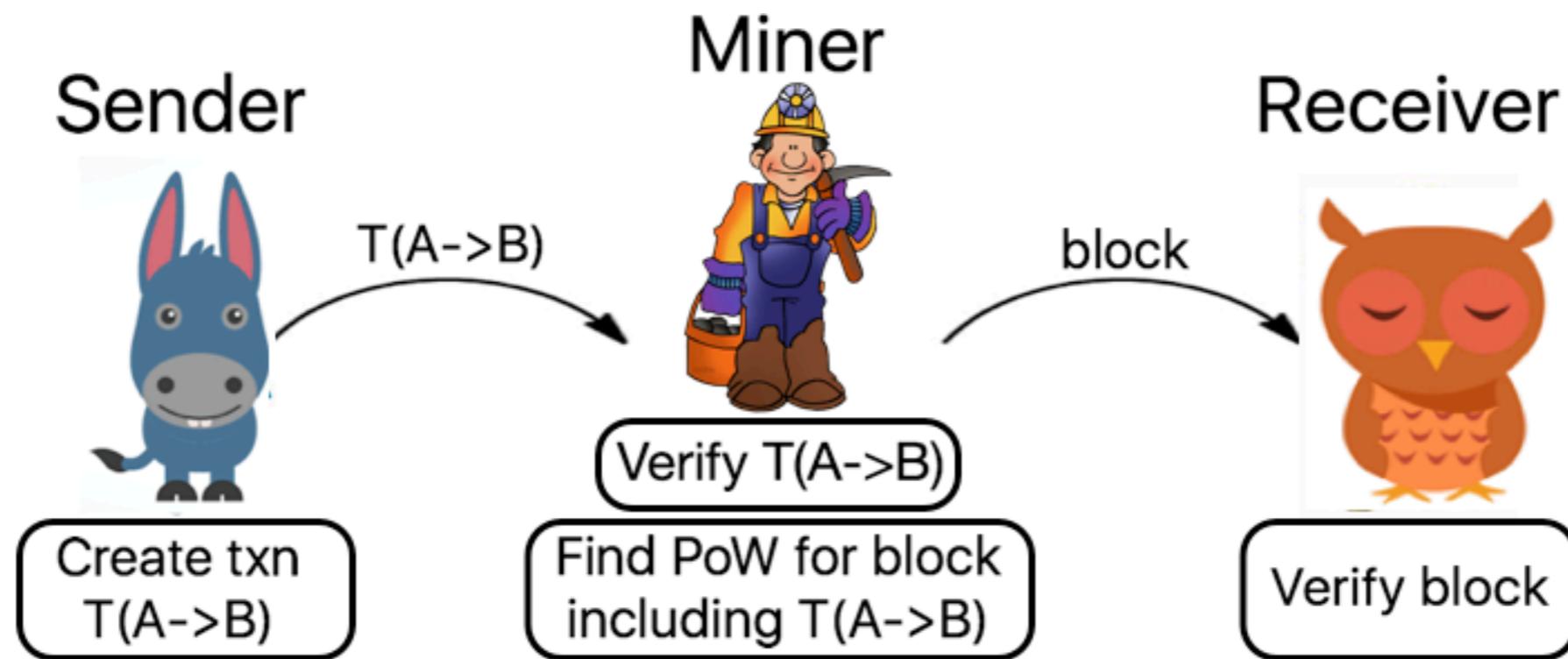


区块链技术的特点



- **共识机制**：能够确保共享账本是精确副本，并降低了发生交易欺诈的风险，因为篡改需要同时在许多地方同时执行。
- **哈希算法(e.g. SHA-256)**：能确保任何交易输入的改动 – 甚至是细微的改动 – 都会对应一个不同的哈希值，表明交易输入可能被损坏。
- **数字签名**：确保交易源自发送方（已使用私钥签名）而不是冒名顶替者。
- **去中心化**：可阻止任何单个或一组参与者控制底层基础架构或破坏整个系统（女巫攻击）。网络中的参与者是平等的，都遵守相同的协议。
- **交易不可逆性**：交易号具有唯一性（相当于一个“时戳”），而且所有节点都认可交易的有效性。这会使交易不可逆，并被网络中的所有成员接受。

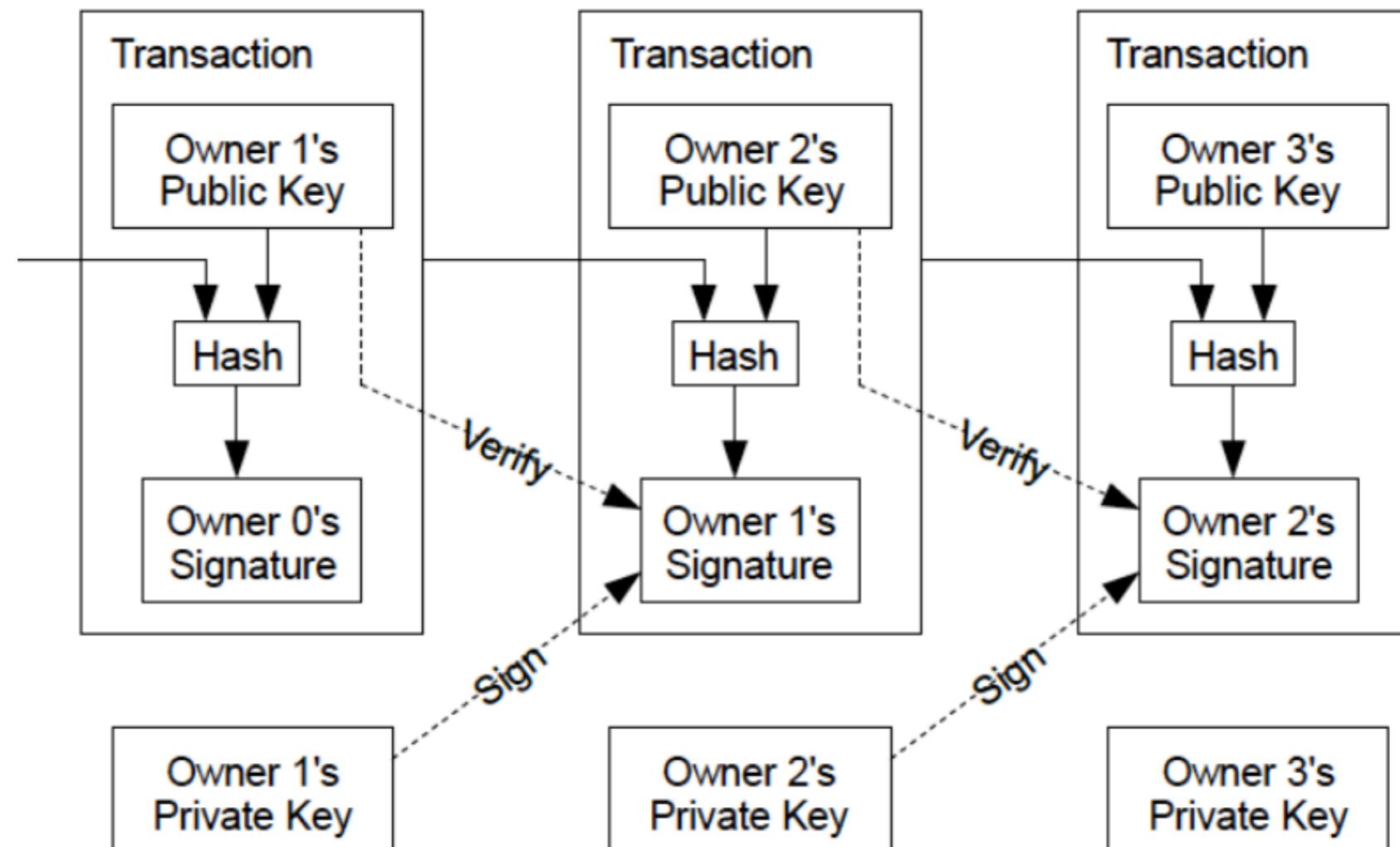
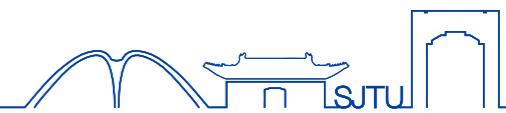
一次比特币交易1（简化版）



财产持有方发送交易，矿工挖矿并发现区块，
新区块（包含最新交易）将被所有参与者同步

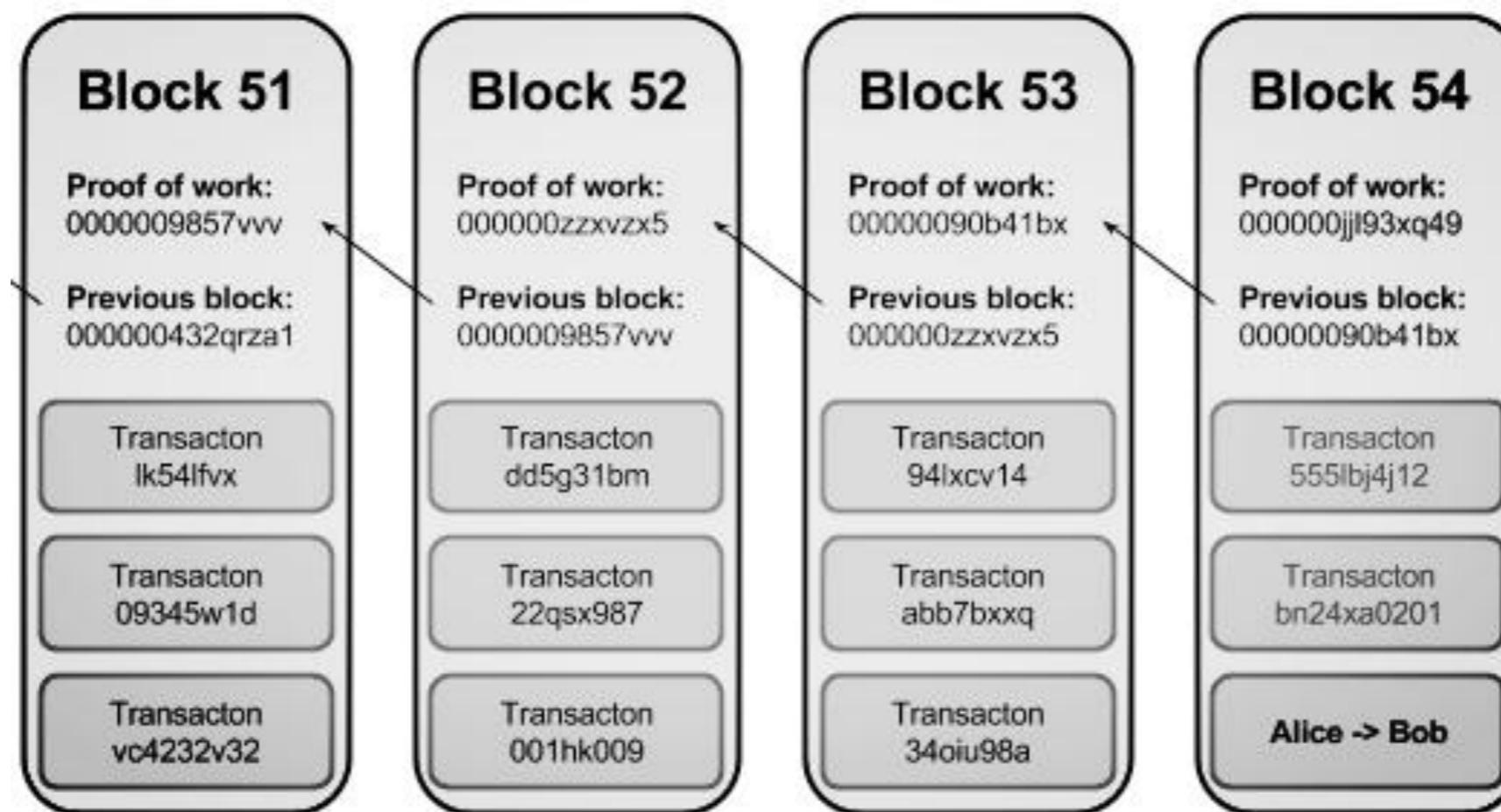
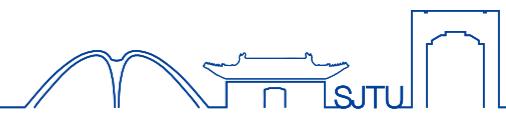


一次比特币交易2（简化版）



交易签名和验证过程

一次比特币交易3（简化版）

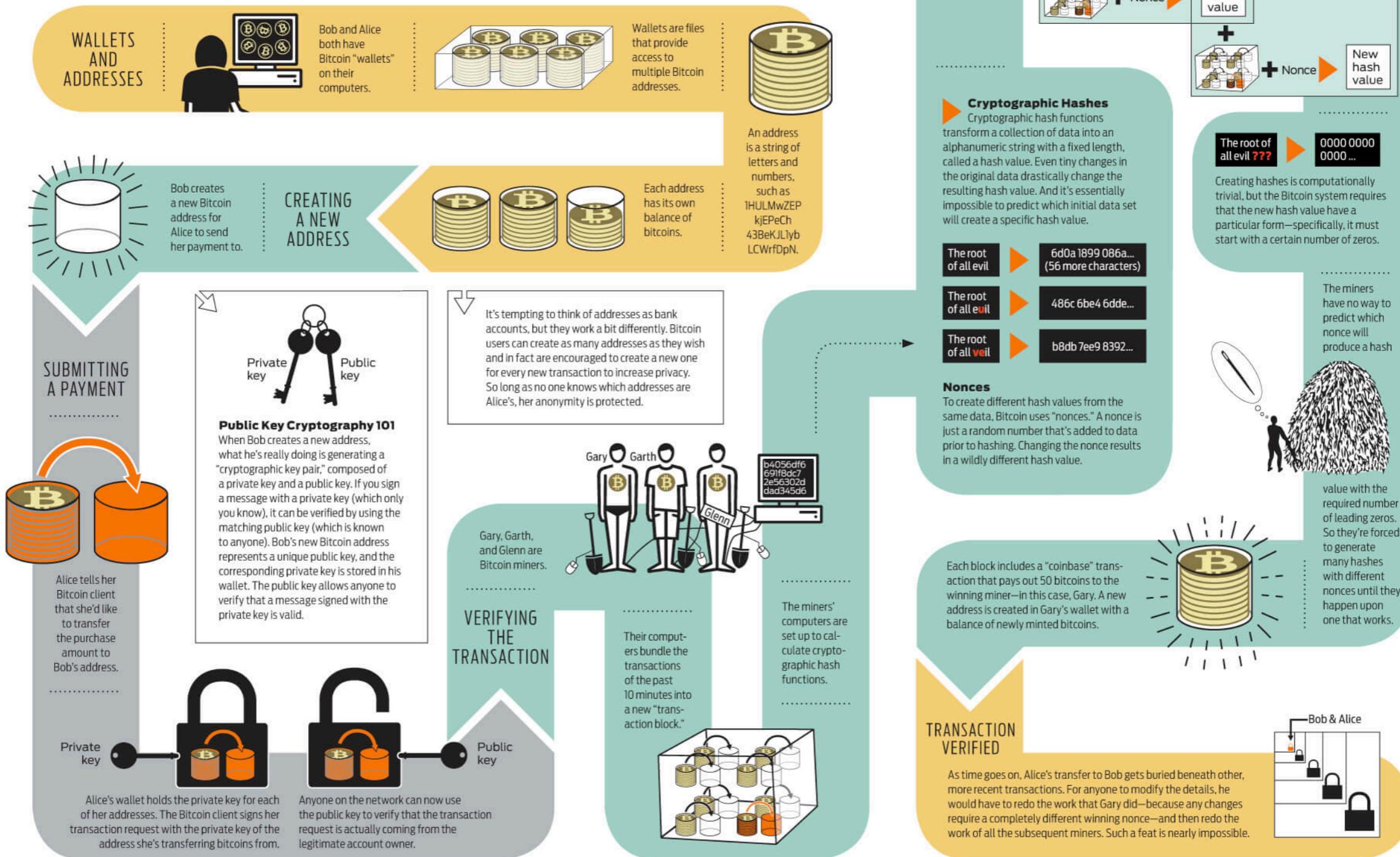


多条交易被打包在一个区块中，
新区块加入唯一最长链，指向前一区块

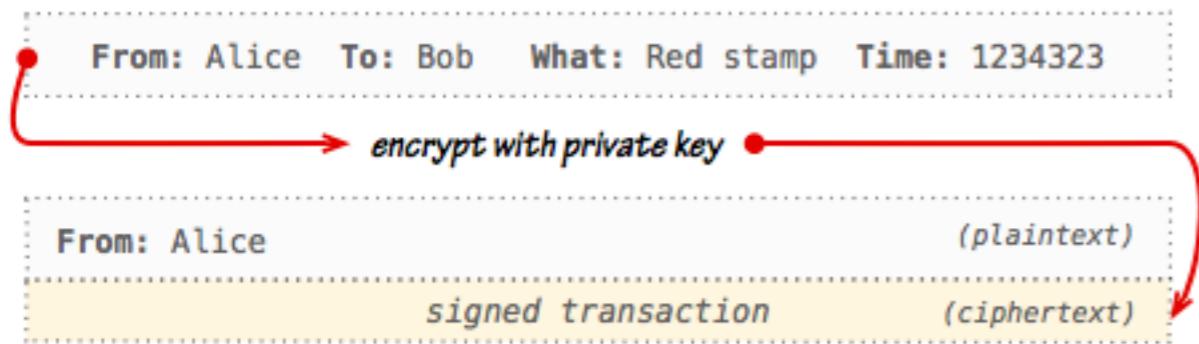


How a Bitcoin transaction works

Bob, an online merchant, decides to begin accepting bitcoins as payment. Alice, a buyer, has bitcoins and wants to purchase merchandise from Bob.

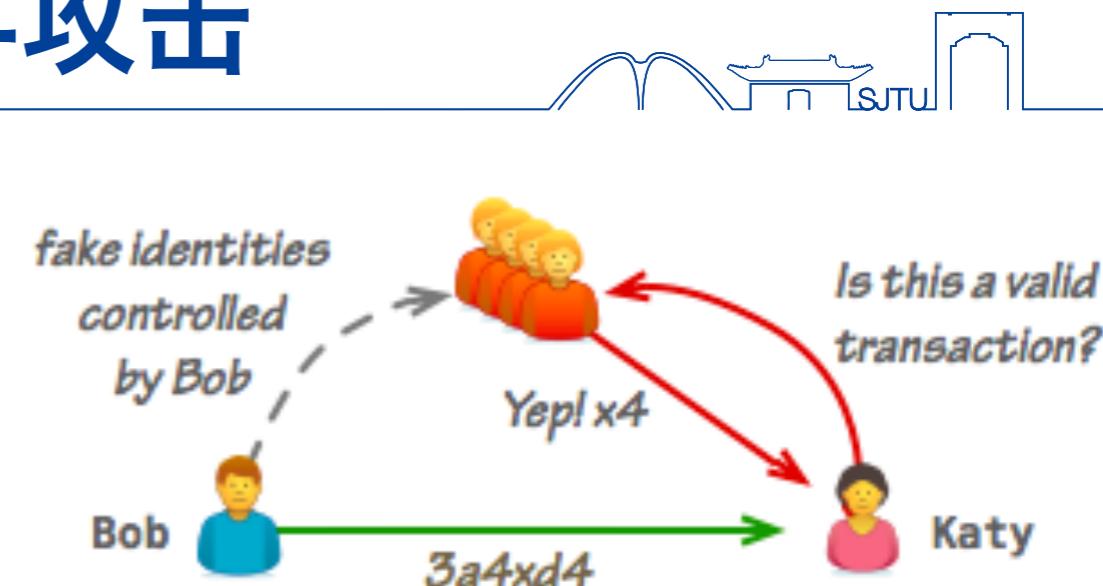
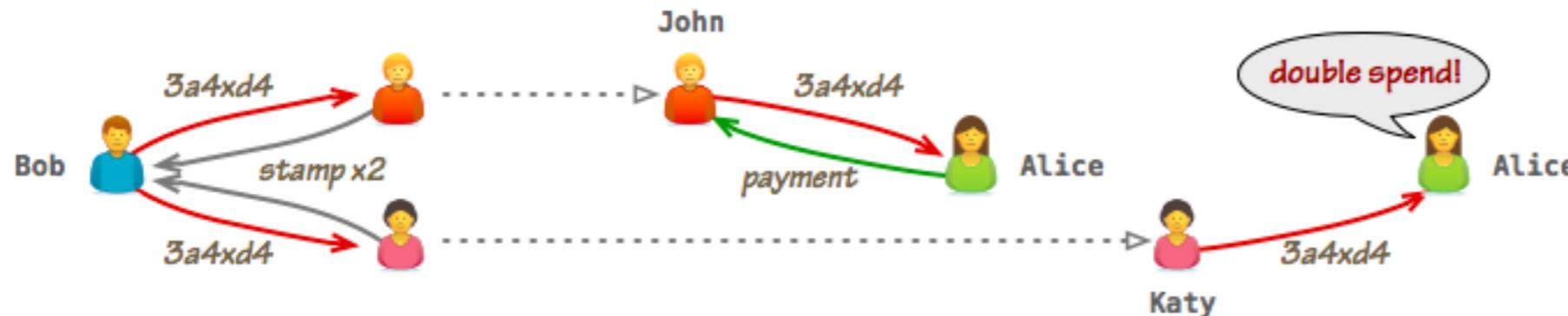
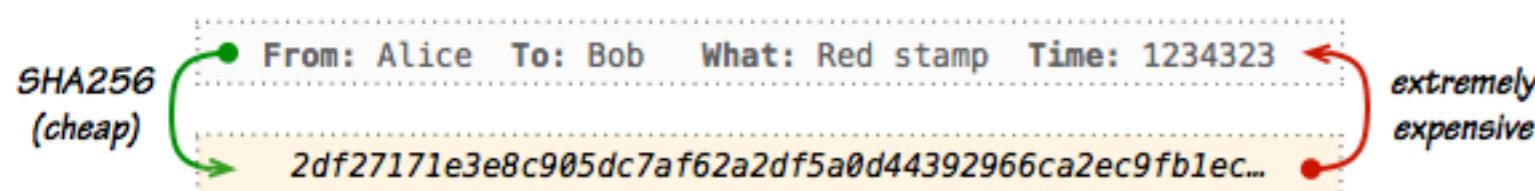


图解1：交易，数字签名与攻击



数字签名

Proof-of-Work

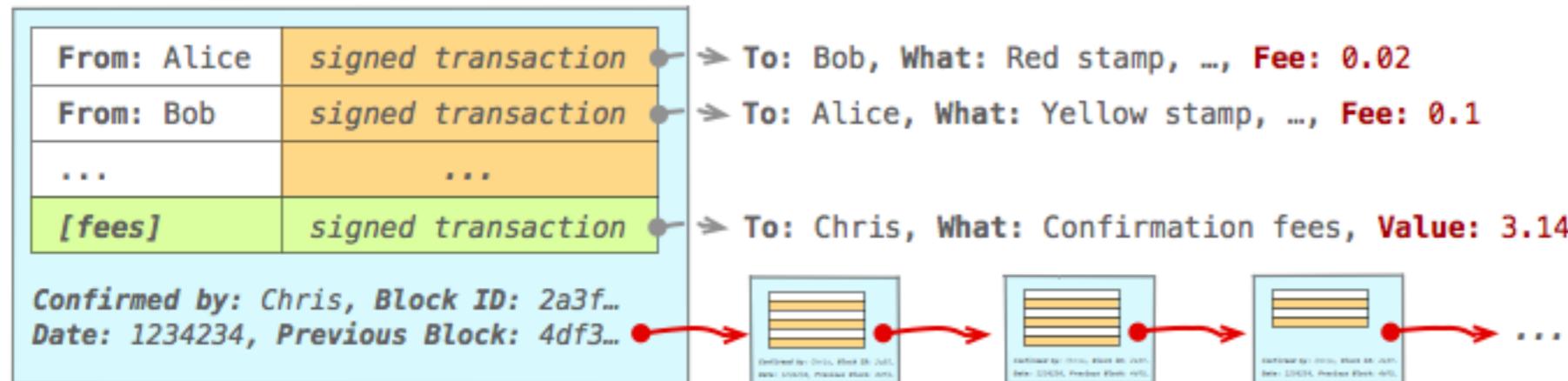


一种可能的Eclipse Attack

双花问题

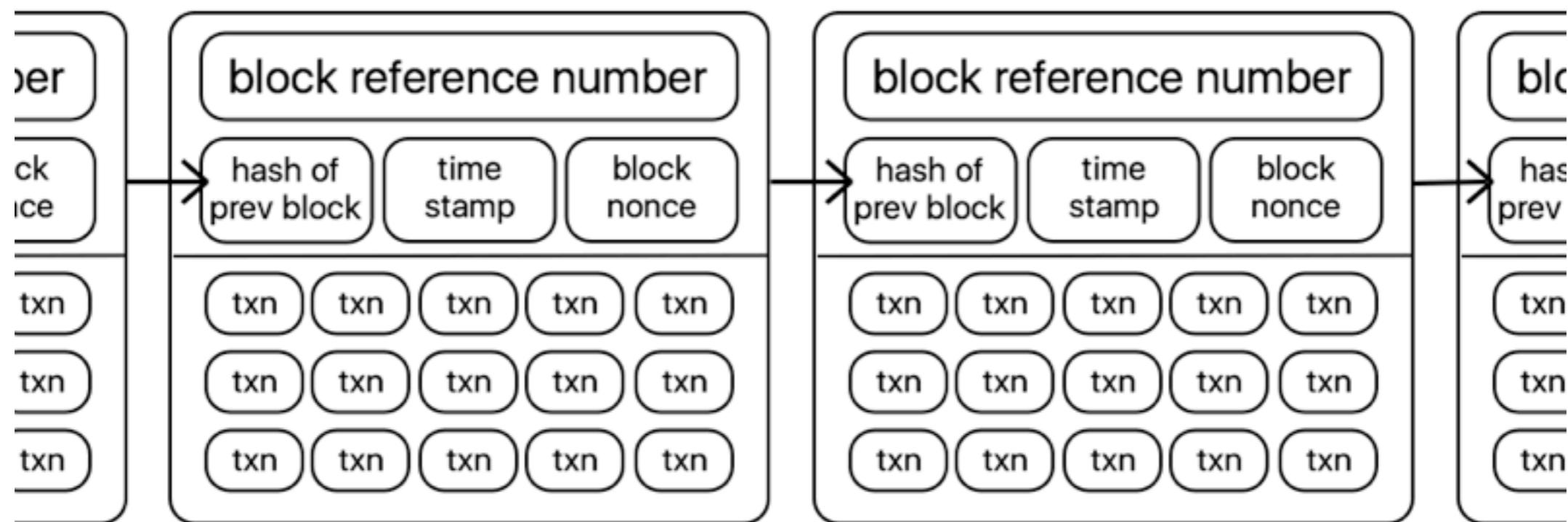


图解2：

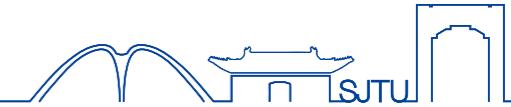


比特币交易

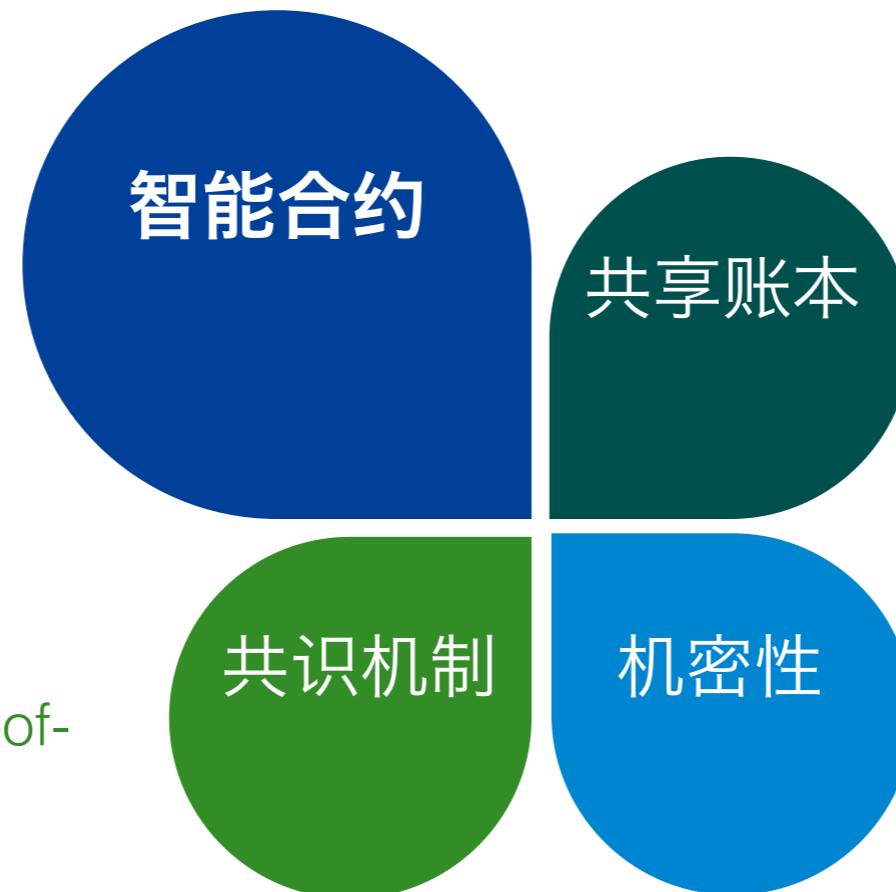
每十分钟以区块的形式打一个包



商用区块链技术：4个关键概念



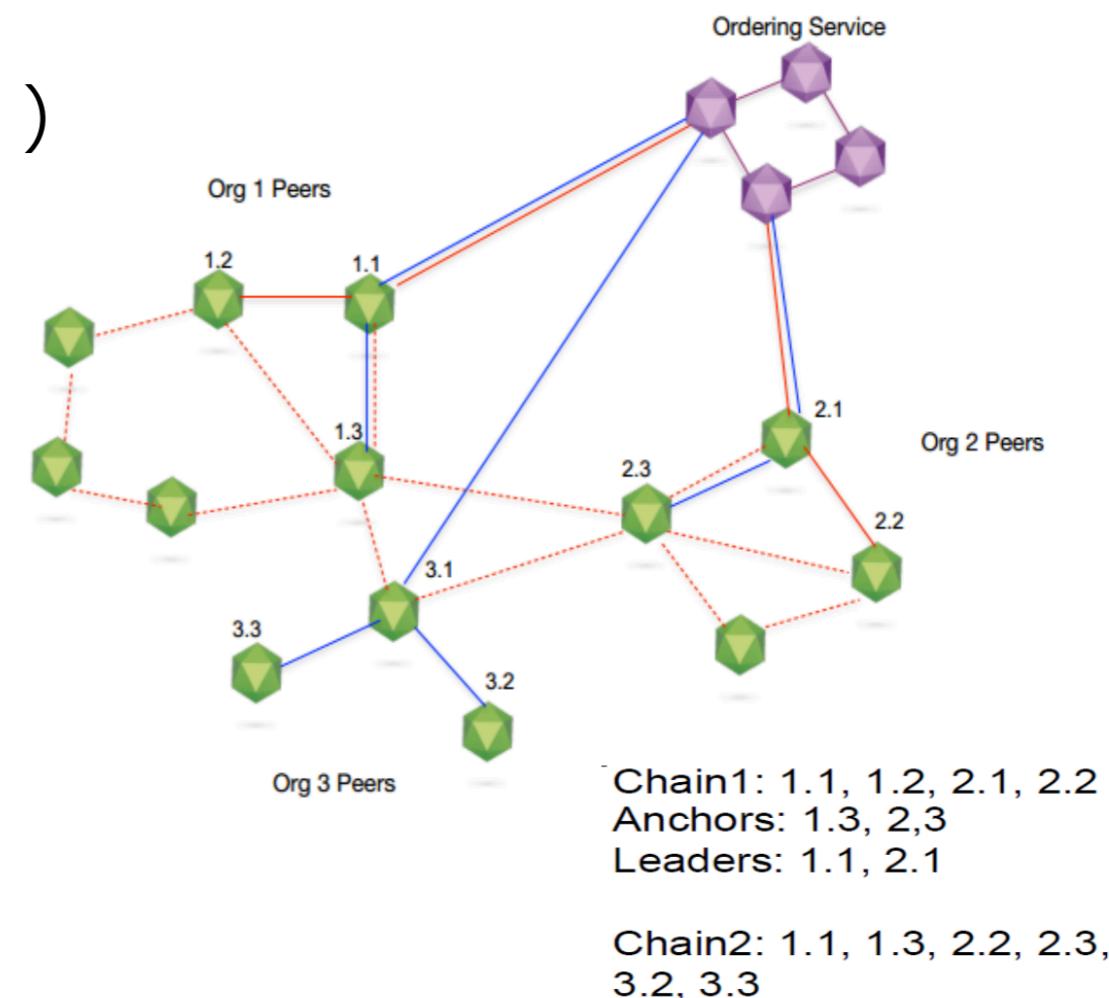
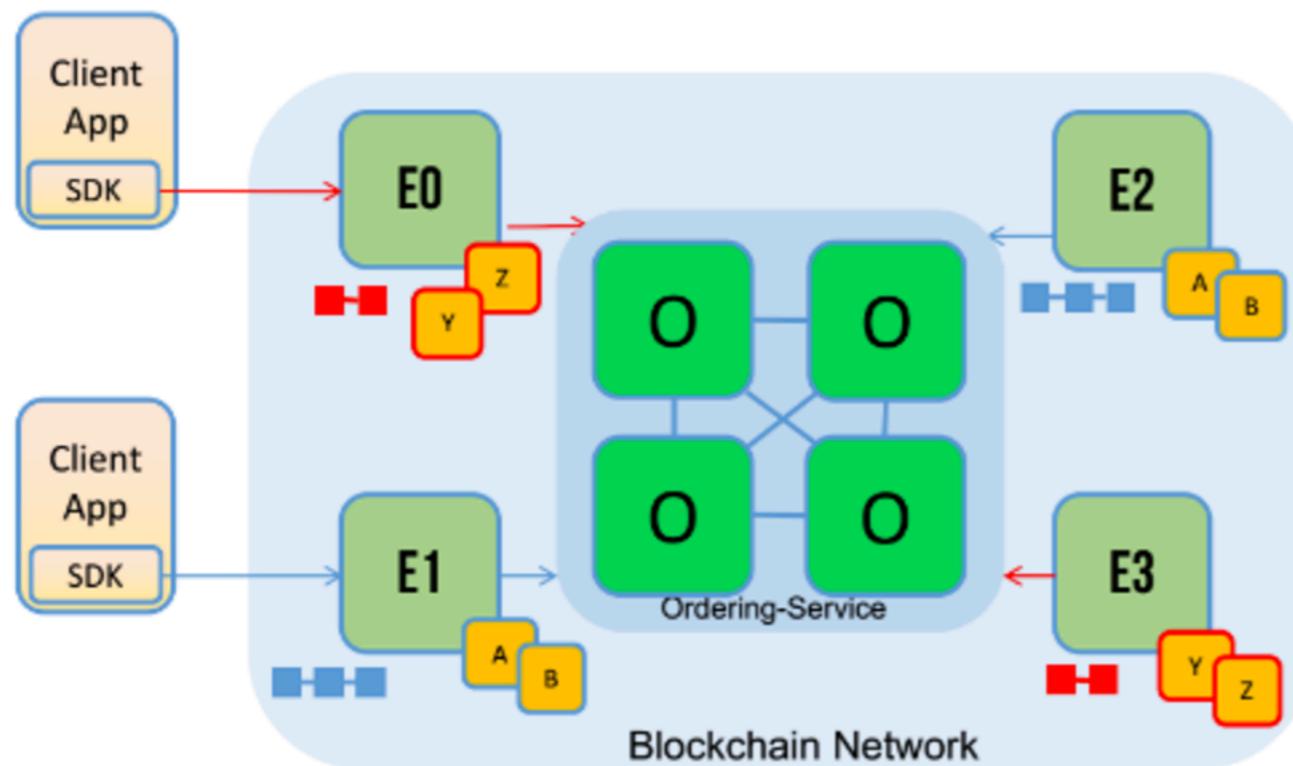
- 合约中设定的**商业规则**
- 被嵌入到区块链系统中
(可编程的)，在交易时被执行
- 多种共识机制：工作量证明(proof-of-work),权益证明(proof-of-stake),拜占庭容错(PBFT)
- 商业网络中的区块链应用需要**可插拔的共识算法**



- 商业网络中，所有的交易记录均记录在共享帐本上
- 参与方只能在被授权后，看到被允许查看的交易记录
- 虽然账本是共享的，但参与方的私密性可以得到保证
(密码学是关键)
- 参与方要求①保障交易隐私
②不为某笔交易所关联

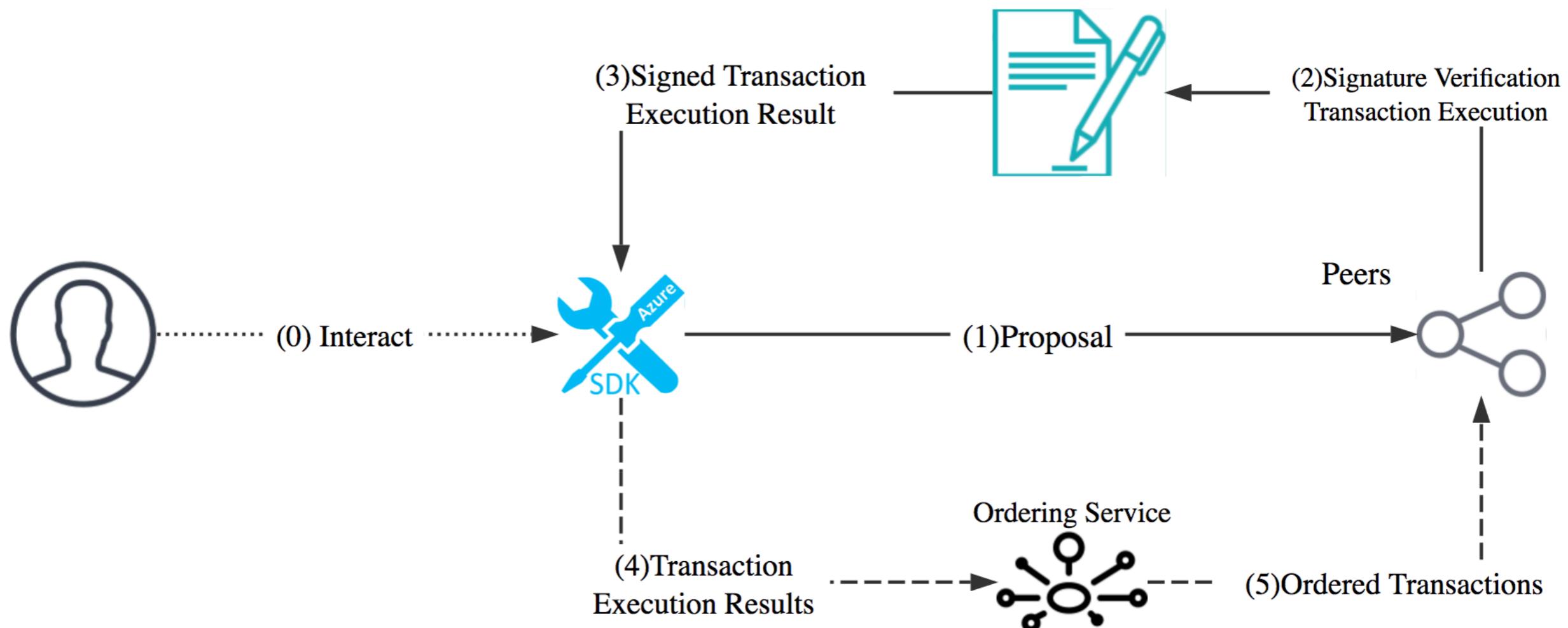
Hyperledger Fabric 1.0新特性 多通道 多链

- 多通道、多链
 - 链将参与者和数据（包含chaincode）进行隔离
 - 一个节点可参与多个链





Hyperledger Fabric 1.0新特性 交易流程



Hyperledger Composer 架构

