

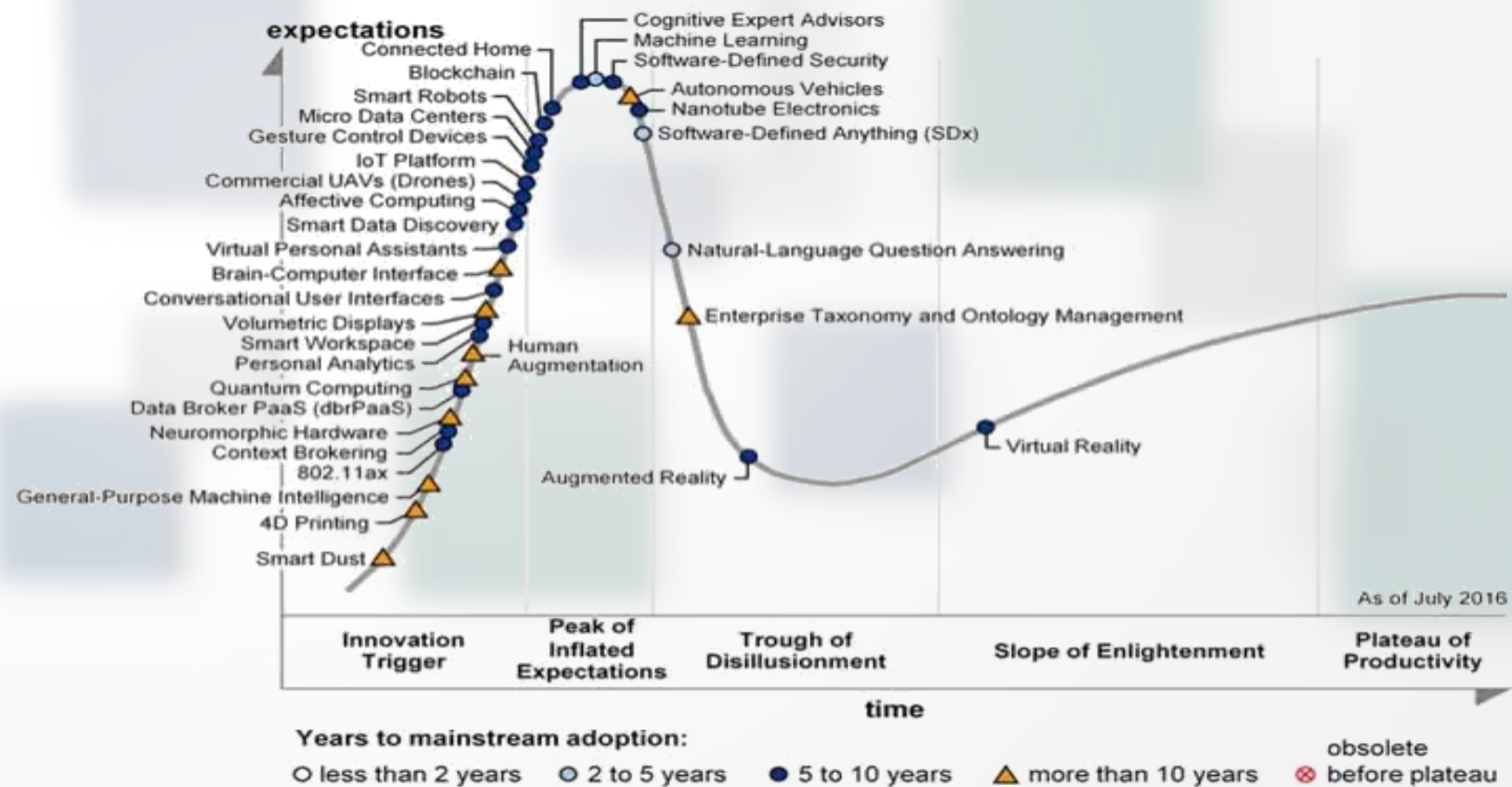
区块链商用之道



董宁

IBM IT经济学顾问，区块链社区推广人
dongn@cn.ibm.com

新兴技术成熟度曲线——区块链



Blockchain Roadmap

Digital Currency (Blockchain v1.0)

- 区块链理论（分布式公开交易账簿）
- 区块链货币（比特币—之前最大的区块链应用）

Smart Contract (Blockchain v2.0)

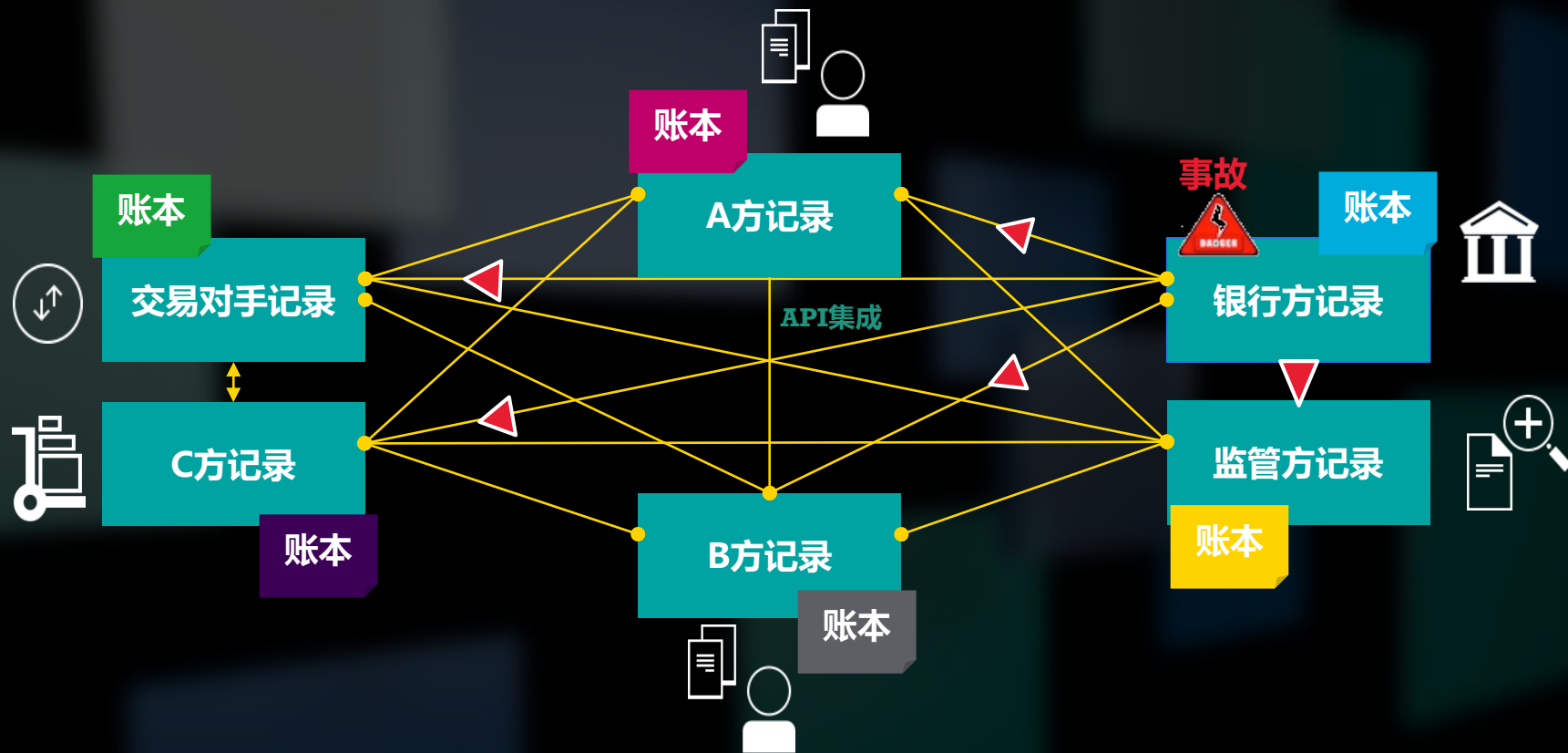
- 资产数字化
- 智能合约（Hyper-ledger, Ethereum等）
-- 基于区块链的图灵完备的编程脚本语言，适合各种区块链数据结构和共识协议

衍生应用，“万物互联” (Blockchain v3.0)

- 广义资产，广义交换
- 设备自主，行业应用



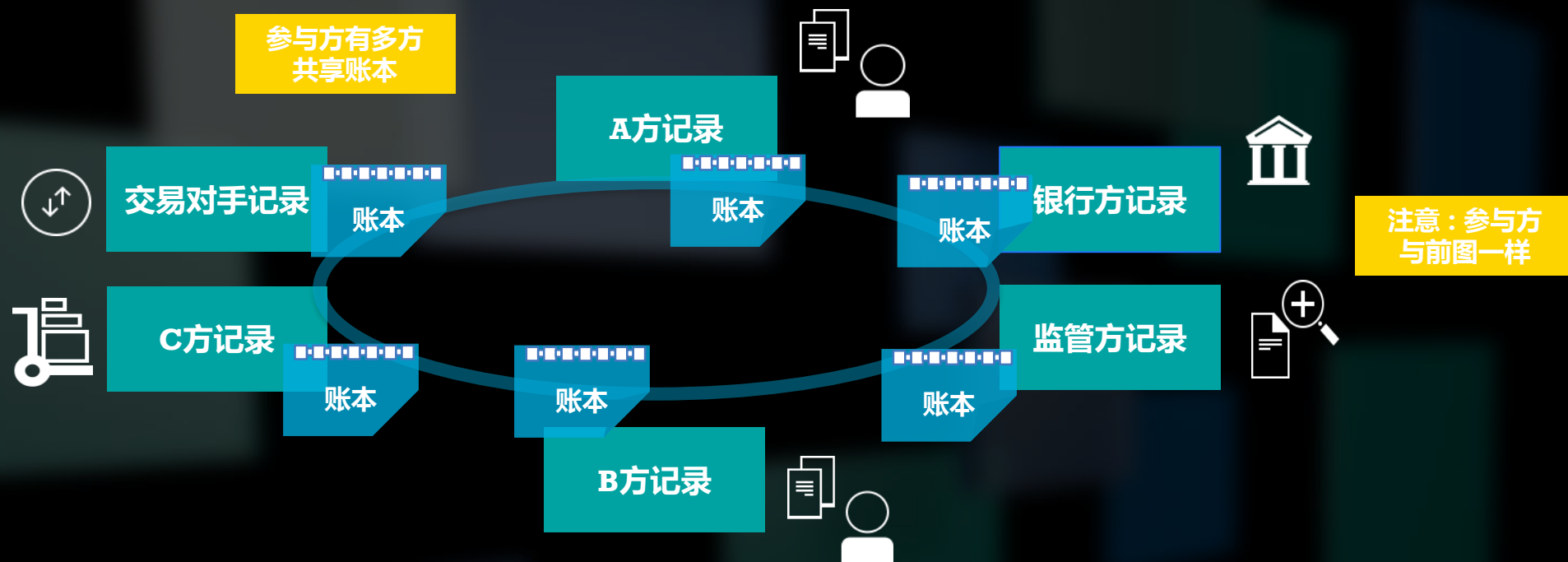
问题——传统的方法很难在一个互信的网络中监视跨机构的交易的执行



传统商业网络面临的挑战

- 每个参与方都有自己的账本，在交易发生时各自更改
- 因此产生为了协同各参与方而带来额外的工作及中介等附加成本
- 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不有效性
- 整个业务网络依赖于一个或几个中心系统，一旦发生问题包括欺诈、网络攻击或错误致使整个商业网络是脆弱的

解决方案——共享的，复制的，授权的账本



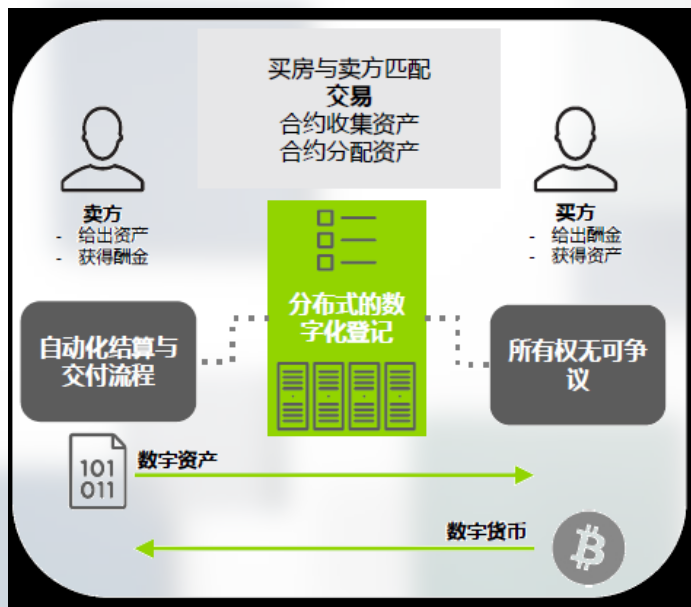
区块链架构带来以下改变

- 区块链架构使每一个商业网络的参与方都具有一个共享的帐本，当交易发生时，通过点对点的复制更改所有账本
- 使用密码算法确保网路上的参与者仅仅可以看到和他们相关的账本内容，交易是安全的、授权的和验证的。
- 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
- 网络参与者基于共识机制或类似的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

区块链架构具有以下特性

- 同样的商业参与方，并不是脱媒的游戏
- 共识（CONSENSUS）– 所有的参与方认同交易的有效性
- 可证明性（PROVENANCE）– 每个参与方了解资产从哪里来，其所有权是如何改变的。
- 永恒性（IMMUTABILITY）– 每个参与方一旦交易被同意发生则无法篡改。如果交易是错误的，必须由新交易冲正并全可跟踪
- 权威性（FINALITY）– 只有一个地方来决定资产的归属权及交易的完整性。这就是共享账本的作用

Blockchain 2.0的思考：区块链对资产流转的价值表述



结算与交付过程缩减至
10分钟
(在区块链上确认一笔交易的时间)



自动化



Non-Stop



实时

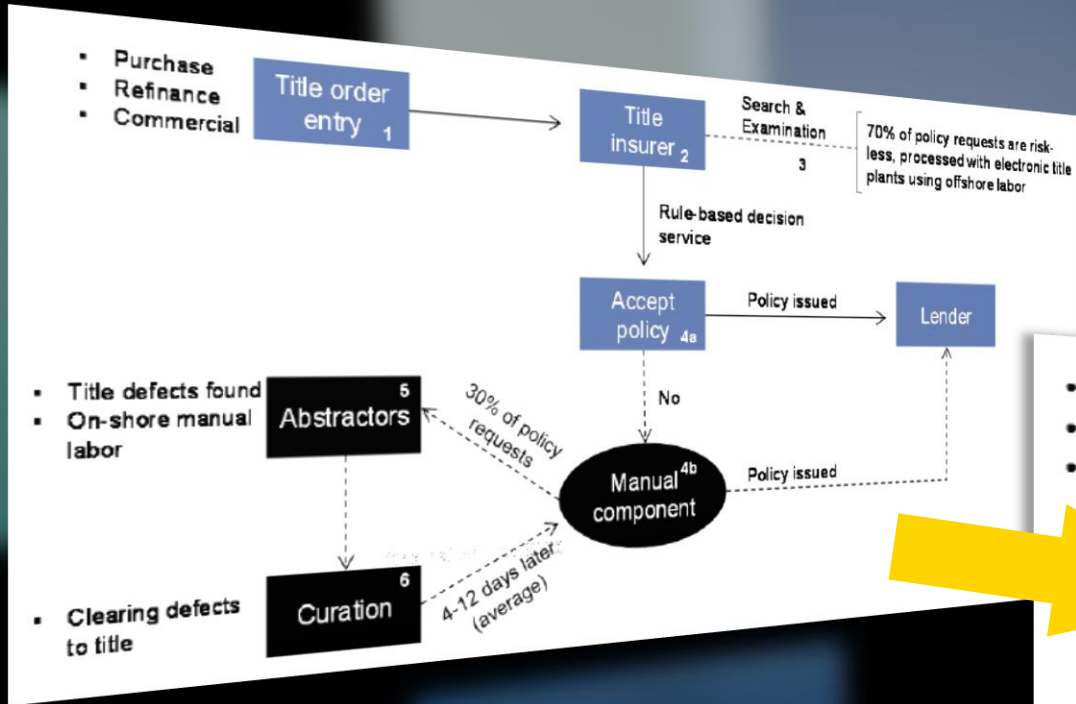


效率提升



成本

IT Economics on Blockchain (I)



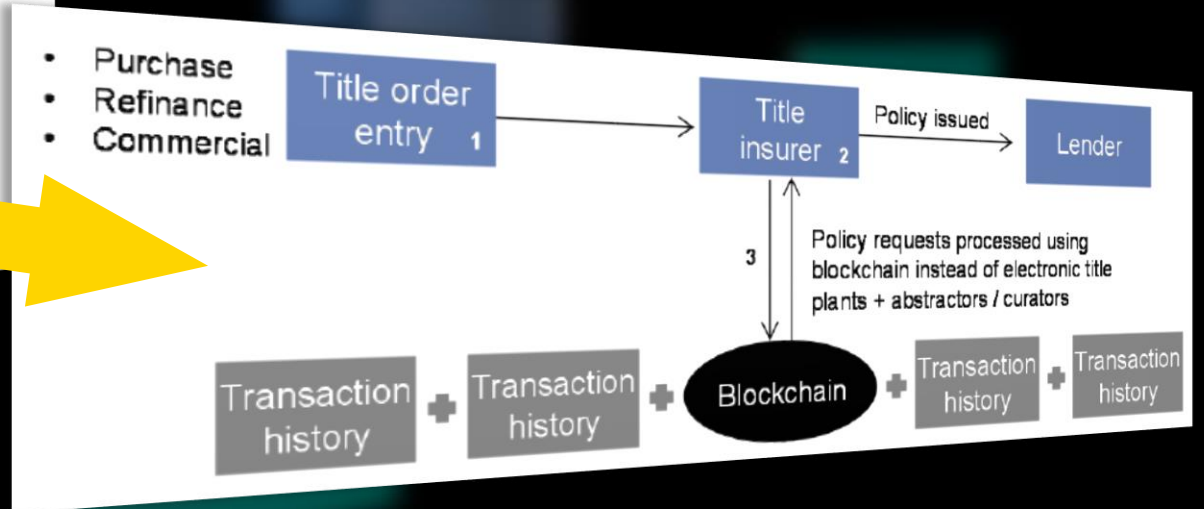
- Blockchain reshapes the insurance industry.
- Eg. It's estimated blockchain could drive \$2 - \$4 bn in US industry cost savings for title insurance due to reductions in headcount and actuarial risk.

业务流程优化

- Property title search is labor-intensive and costly.
- Title insurers rely on a network of parties to underwrite every policy.

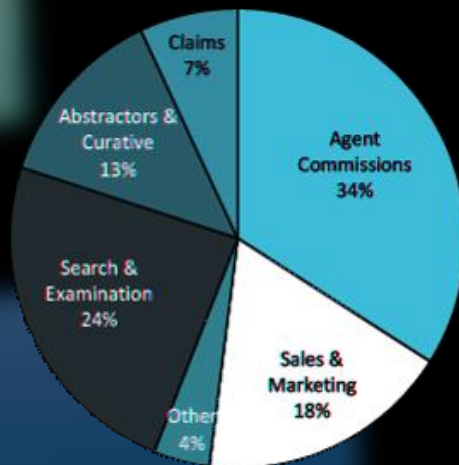
加入智能合约

- Blockchain has the potential to eliminate transactional risk from the existing system.

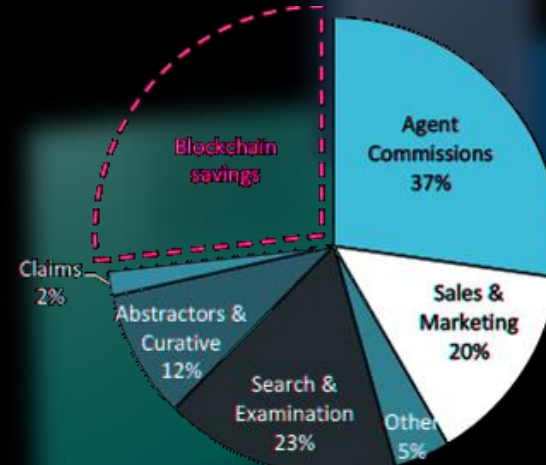


IT Ecomonics on Blockchain (II)

	Current		Blockchain		
Operating Expenses	Absolute cost (bn)	% of Opex	Absolute cost (bn)	% of Opex	Savings (bn)
Agent Commissions	\$3.7	34%	\$2.9	37%	\$0.8
Search & Examination	\$2.6	24%	\$1.8	23%	\$0.8
Sales & Marketing	\$1.9	18%	\$1.6	21%	\$0.3
Abstractors, Curative & Legal	\$1.4	13%	\$0.9	12%	\$0.5
Claim Losses	\$0.8	7%	\$0.2	3%	\$0.6
Corporate & Other	\$0.4	4%	\$0.4	5%	\$0.0
Total	\$10.8		\$7.8		\$3.0

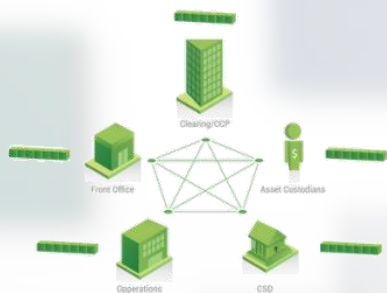


Traditional Cost Structure



Savings from Post Blockchain

企业级区块链的平台要素总结



智能合约

- 数字化合约, 类似业务规则
- 嵌入在 Blockchain 中
- 在交易时执行
- 用编程语言编写, 经过数字签名, 可以被校验



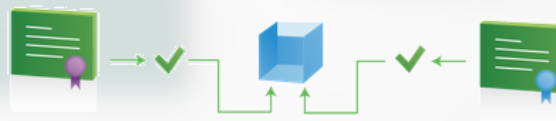
一个商业网络

- 包含市场参与者的对等架构.
- 伙伴间的一个共识协议



共享帐簿

- 记录网络上的所有交易
- 在参与者间共享且每个人都有自己的副本
- 许可制
- 存储



隐私和保密

- 记录通过哈希、加密和个人签名得到保护
- 客户、收据和参考号都有唯一的ID
- 隐私交易
- ID和交易不能直接联系
- 交易认证



共识

- 共识算法确保每份副本的一致性, 降低伪冒交易的风险
- 所有成员都同意这些交易而且做过验证.
- 可以建立交易验证的规则.

Hyperledger参考架构概览（模块与服务）

成员管理 （Membership）

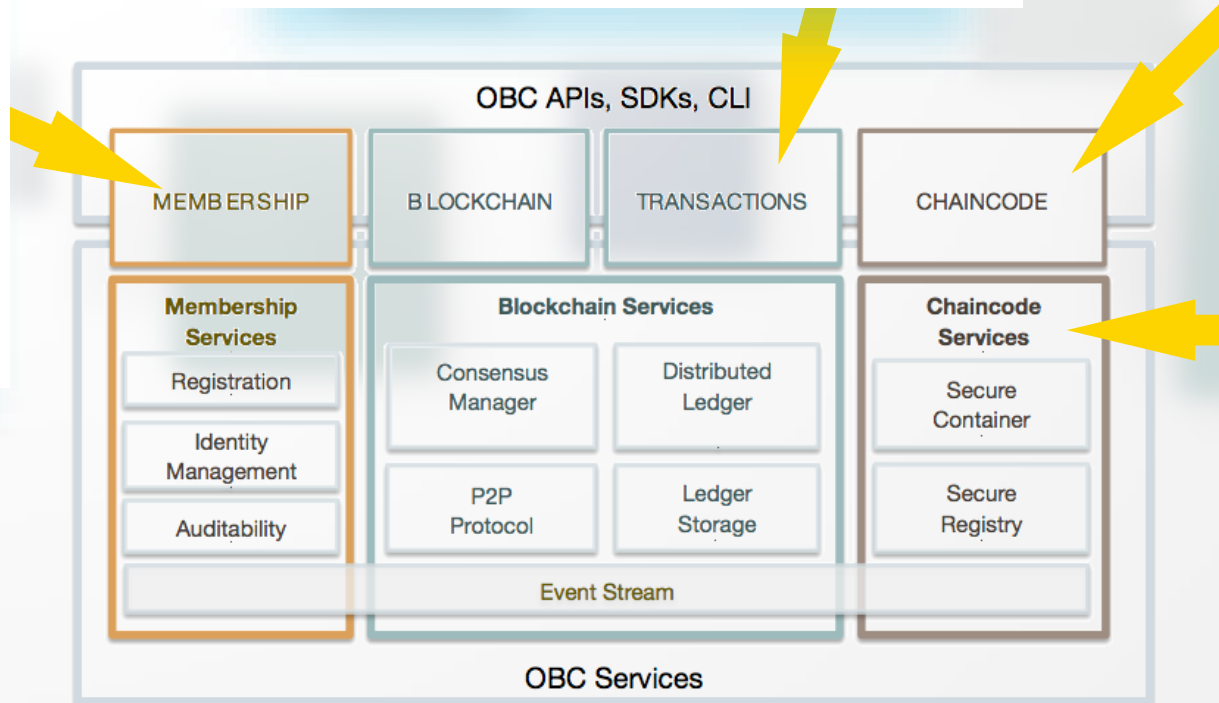
- 成员管理提供会员注册、身份保护、内容保密、交易审计功能
- OBC所有成员必须经过许可才可以发起交易，这一点不同于公有链（所有参与方不需要登录，可直接提交）
- OBC成员发起交易时，若启用Transaction Certificate Authority (TCA)功能，则交易证书会保护成员ID不被无关方看到

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

Blockchain的商用之道 – 3C观点

	Community + Code / 社区 + 代码 Linux 超级账本项目 Hyperledger Project	开源代码：推动区块链技术的快速创新和商用 共识 可溯源 不可更改 定局性 开放性治理模式 (Open Governance) – 40个跨行业成员
	Cloud / 云计算 区块链平台 - 云平台 - 专用服务器 (LinuxONE)	在IBM云平台和Z系列大型机上的区块链托管服务 身份认证 共识算法 系统集成 硬件级性能调优和系统安全 在IBM PaaS平台Bluemix上提供的区块链服务
	Clients / 客户 区块链解决方案 区块链创新车库 (Blockchain Garage)	和客户一起推动区块链技术的成熟落地商用 在全球各地设立区块链创新车库： 纽约 伦敦 新加坡 东京 区块链相关咨询和实施服务  How

区块链领域最大的开源社区：HyperLedger项目

Linux Foundation

致力于打造Linux生态圈，推动Linux技术商用化
2000年成立，600+家大型IT公司组成，提供Linux开源工具、培训、展会

Linux Foundation Collaborative Projects

Linux Foundation的一个工作方向：联合企业共同投资，协作解决尖端技术难题

HyperLedger Project

Linux Foundation Collaborative Projects中的一个课题，开设于2015年12月

由多家公司共同研发，公布Open Ledger标准（规格说明书），创建基于Linux的开源共享账簿（比Bitcoin更适合行业应用）

最终推动区块链技术在行业中的应用（行业区块链）

IBM Cloud开放技术单元首席技术官Chris Ferris当选HyperLedger委员会主席

 **LINUX FOUNDATION**



100

Members

100+

Contributors

6

Projects

2.3K

Membership
Requests

5X

More requests than
next largest in LF
history

6

Hackfests

6

Working Groups

~\$6M

Membership
Investment

Blockchain平台支持多种交付和部署方式



Public (公有)

全球范围的多租户公有云



Dedicated (专有)

隔离的私有云环境



Local (本地)

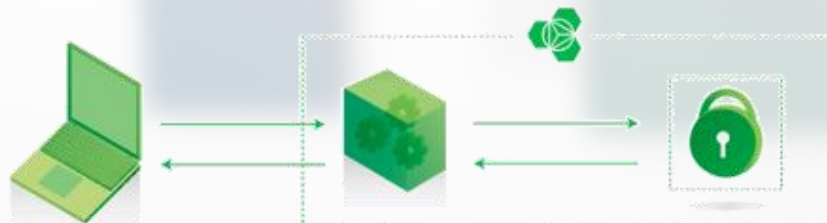
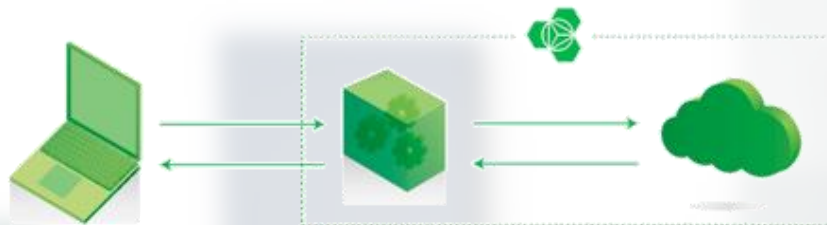
本地数据中心

IBM（中国）系统中心区块链云平台

- IBM中国系统中心是 IBM 全球五大高端(包括 IBM z Systems)测试中心之一，更是亚太地区第一家负责提供系统测试、参观访问、技术交流论坛等多项技术支持活动的中心。
- 目前，IBM中国系统中心已经搭建了基于高性能云平台的IBM LinuxONE区块链环境，实现功能如下：
 - 新技术方案演示
通过多媒体方式演示，使客户全方位了解IBM区块链的产品信息，竞争优势信息和解决方案信息，从而帮助客户进行更加全面和前瞻性的 IT 投资决策，加强客户对IBM区块链技术方案和强大能力的了解和信任。
 - 概念原型验证
针对客户具体需求量身定制，部署相应的软件、硬件环境，快速、有效地检验 IBM 方案总体架构和关键功能的可行性，提前发现和解决潜在的问题，降低风险。
 - 性能指标测试
依据客户的需求提供有关的性能测试，在所要求的配置上运行客户应用，帮助分析影响性能的可能系统架构、软硬件能力等因素,及扩展性相关问题。



区块链即服务 “BaaS” (Blockchain as a Service)



Starter Developer Network

Start a blockchain environment running almost instantly to build an application on industry-standard APIs. Monitor your network and view health status. Leverage the REST API to deploy and invoke chaincode transactions.

[Try the starter developer network](#)

High Security Business Network

This blockchain network plan extends the starter features within an isolated environment that runs in a secure infrastructure and offers higher levels of security.

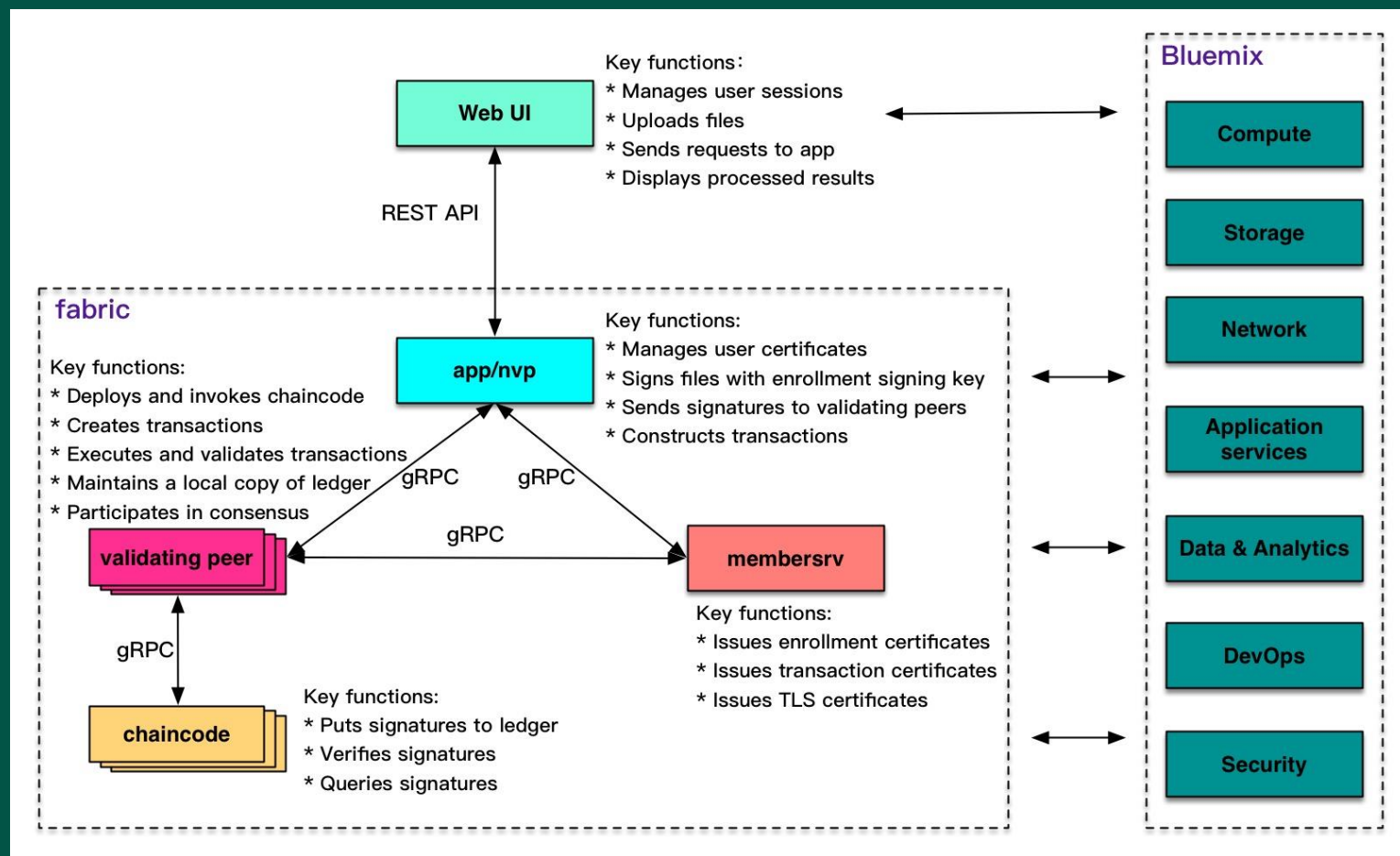
IBM will offer a limited number of high security networks for beta release. Click below to apply for the beta.

[Request the high security business network](#)

Blockchain BP Highlight

➤ **Wutong Tree (云图科瑞)** is a member of Hyperledger and they have been focusing on provide professional services of internet finance, Innovation Financial tools etc.

➤ Wutong Tree has been working on "绿色经济的外部性成本交易所" project that co-works with IBM team, and develops the application platform with blockchain based on Bluemix. During the event, CEO Chen Jianxiong introduced the blockchain scenario and the market value imported by IBM blockchain and Bluemix.



IBM Blockchain Garage

- ❖ IBM Bluemix Garage for Blockchain 汲取了行业专长于区块链的技术，与Design Thinking以及敏捷开发结合，从而推出可行的商业解决方案。
- ❖ 将IBM成功的Bluemix创新车库方法论与区块链社区和实践结合的独特结果，帮助向基于云计算的区块链应用演进。IBM的区块链和Bluemix都有自己独立的产品和解决方案，通过创新车库的形式，能够更好地结合两者的特点和优势
- ❖ IBM区块链创新车库提供了独特的市场视角，能帮助客户快速实现价值
- ❖ 目前已经开放的城市：纽约 | 伦敦 | 新加坡 | 东京



创新车库方法论



IBM Design Thinking



区块链落地实践探索

Blockchain Garage Methodology & Industrial Best Practice

整合多个行业最佳实践

- **Design Thinking,**
- **Lean Startup,**
- **Agile Development,**
- **DevOps,**
- **Cloud**

帮助客户快速构建和交付创新性的解决方案

了解更多详情请访问:

<https://www.ibm.com/devops/method>



IDC report: "Perspective: The Industry Implications of Blockchain Technology"

- Top 10 Industry Implications of Blockchain

1. Next-generation security.
2. Industry clouds.
3. Digital transformation.
4. IoT.
5. Financial services. In payments, In trading, settlement, and clearing, In KYC and AML
6. Government.
7. Health.
8. Manufacturing.
9. Retail.
10. Energy.

IDC's Perspective report begins with this guidance: "The hype volume is about to be turned up on blockchain, and with some considerable merit. IDC Financial Insights recommends that companies consider the opportunity and value of blockchain capabilities as part of digital enterprise strategies, develop a point-of-view document that articulates what blockchain entails (in language that is consumable by nontechnical personnel), and explore what the industry and individual implications might be."

探索应用场景的尝试

- 全局记账：每一步都是账本记录，相关方都可以看到并验证，过程透明。一旦共识，无法修改
- 智能合约：能保证每一步严格按事先设计的流程进行，降低争议风险
- 隐私保护：相关方可以看到或编辑内容，无关方无法看到内容

应用场景：开放可信供应链（Open & Trusted Supply Chain）

业务

- 客户希望知道购买的商品的供应链信息
比如车主希望知道每个零件是否是原厂生产，是否正牌渠道供货
比如消费者希望知道食品的生产、经销、运输过程

挑战

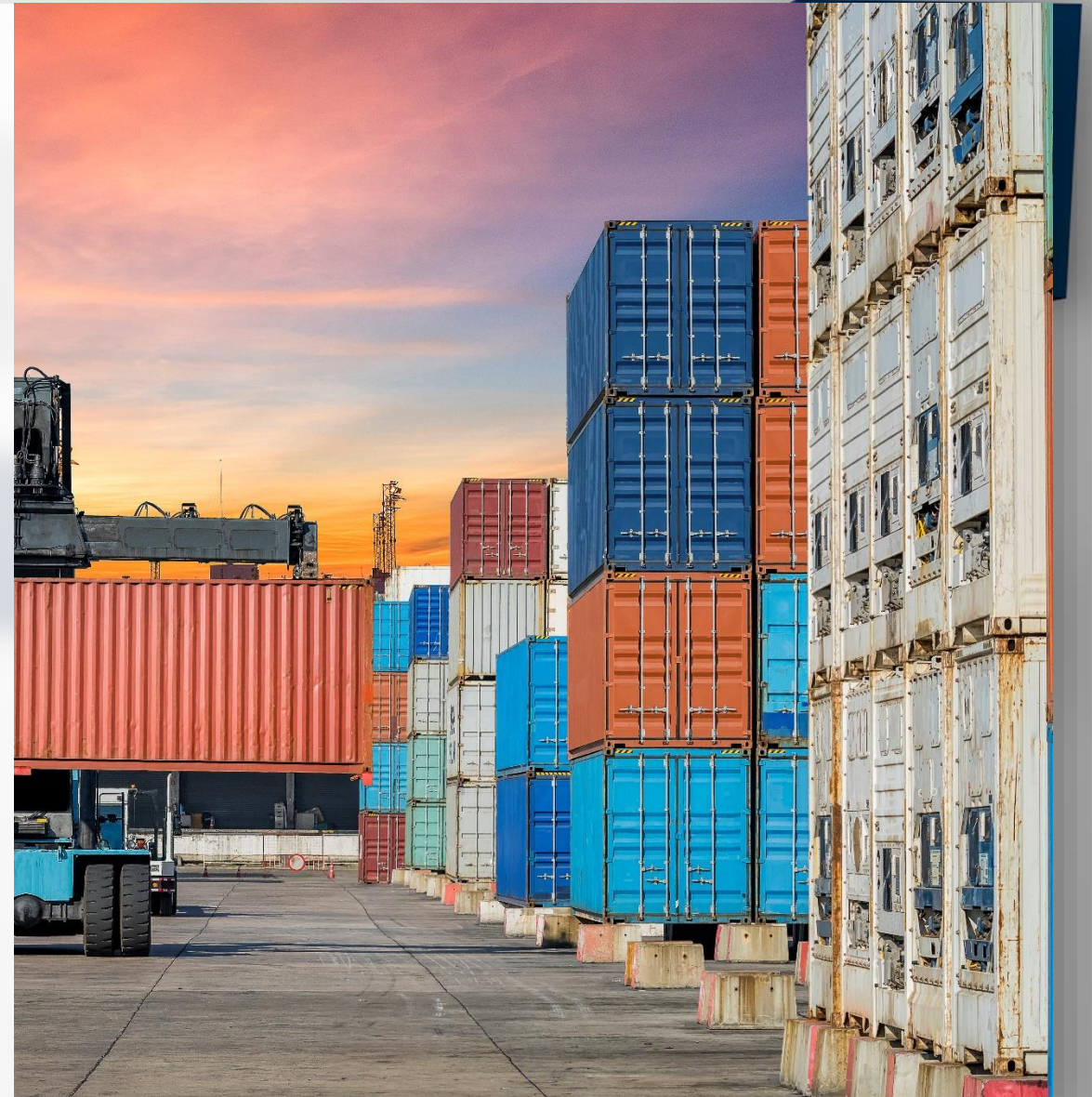
- 商品供应链权属关系（原厂、总代、分销、零售）和上下游关系（生产、总装、维修、保养）都比较长，每个企业各管一段
- 商品形态也会出现很大的变化（小麦、面粉、饼干）

区块链方案

- 区块链可以解决每一件商品的出处（比如：一箱饼干来自一批面粉）

价值

- 把分段的输入输出关系串接起来
- 全局一本账，杜绝凭空生出和凭空消失的零件
- 对原厂渠道管理和政府市场监管有帮助



Use Case: Blockchain Solution for IBM Global Financing (IGF)

概述

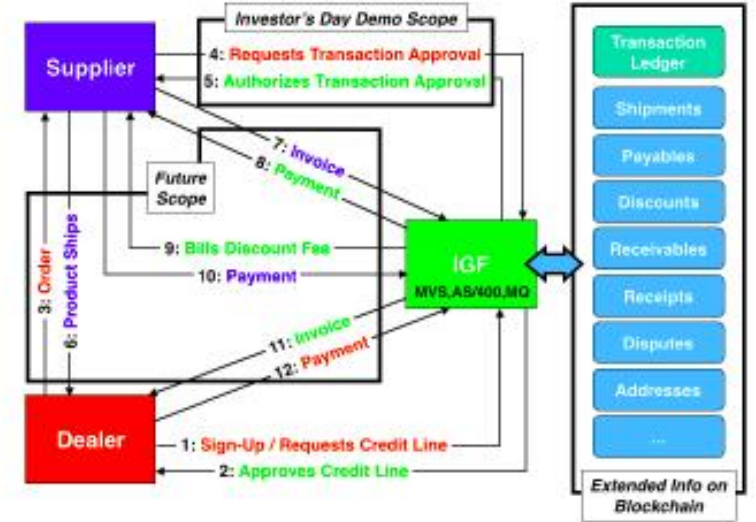
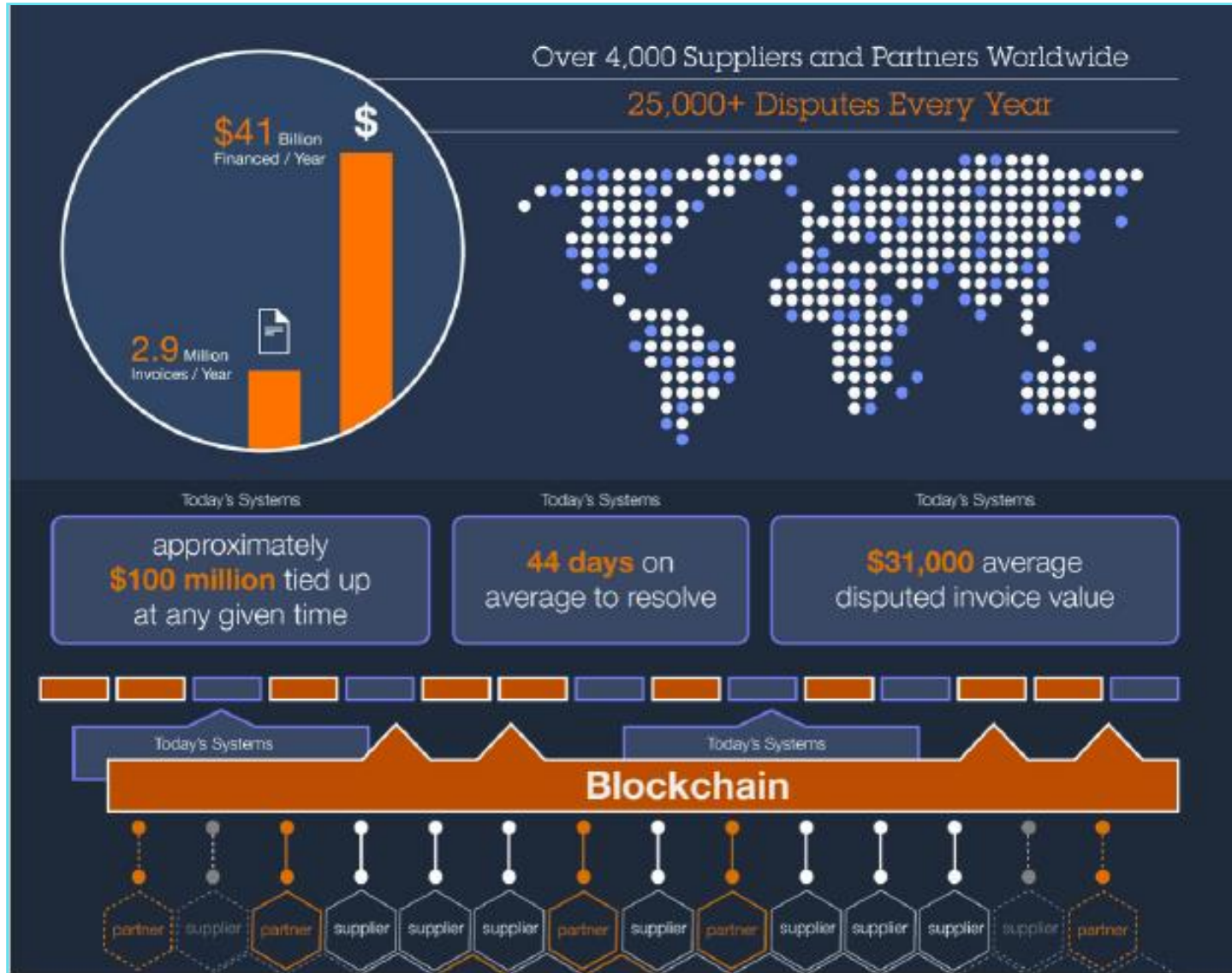
安全

性能

部署

服务

案例



- ❖ Immutability / Non-repudiability of blockchain ledger ➡ Comprehensive view of all operational data
- ❖ Less disputes, faster settlement ➡ Free flow of capital between parties
- ❖ Distributed & Replicated ➡ Less Outages, Highly extensible

China UnionPay & IBM : 以区块链为底层架构的积分交换平台

挑战

- 目前中国各大银行、航空公司、酒店品牌多半都有自家的会员积分回馈制度，但多半相当封闭，无法透过本行的积分兑换其他企业积分活动的产品或服务，银联与IBM打算利用区块链机制来解决跨行积分交换的清算问题

区块链方案

- IBM与中国银联正在联手创建一个基于区块链技术的银行卡积分交换平台。在线上，消费者可以与他人交易自己通过购物和其他奖励措施所获得的积分，而在线下，积分平台用户可以去任何一家配备智能POS机的超市或商场，使用奖励积分兑换商品。在IBM和中国银联的设想中，这一概念还能够被应用于航空里程、话费帐单或者加油卡积分的交易上

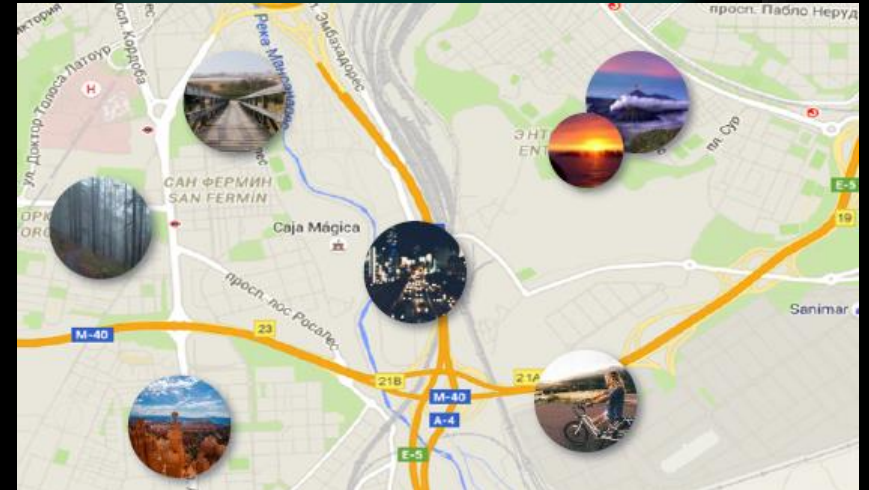


区块链其他应用：商品身份溯源

 everledger [Home](#) [API](#) [Timeline](#) [Smart Contracts](#)

PROTECTION.

We are a fraud detection system, overlaying big data from closed sources like insurers and law enforcement.



Walmart、IBM and Qsinghua: Food Security on Blockchain

挑战

- 中国政府高度重视食品安全问题，作为促进食品安全的举措之一，将食品认证、供应链跟踪作为保障食品安全的重要举措，以此快速发现和消除食品的污染源。

区块链方案

- 区块链技术将实现食品的全程数字化跟踪，从供应商生态系统到商店货架，最终到消费者。对于食品供应商而言，数字产品信息—诸如农场原产地信息、批号、工厂和加工数据、有效期、存储温度和运输等都将与相应的食品建立数字化关联，而整个过程中每一环节的信息将被输入到区块链中。每笔交易的信息都须得到商业网络中所有成员的共同许可；一旦达成共识，就会形成无法更改的永久性记录，以此确保所有的商品相关信息都准确无误。
- 区块链产生的记录可以帮助沃尔玛等各大零售商更好地管理各个卖点的产品保质期问题，进一步增强食品验证的安全措施。



Blockchain for PSB Investment Operation of Custody Business

区块链价值

- 区块链作为共享账本，在资产管理、托管业务、审计之间共享托管业务的核心业务数据

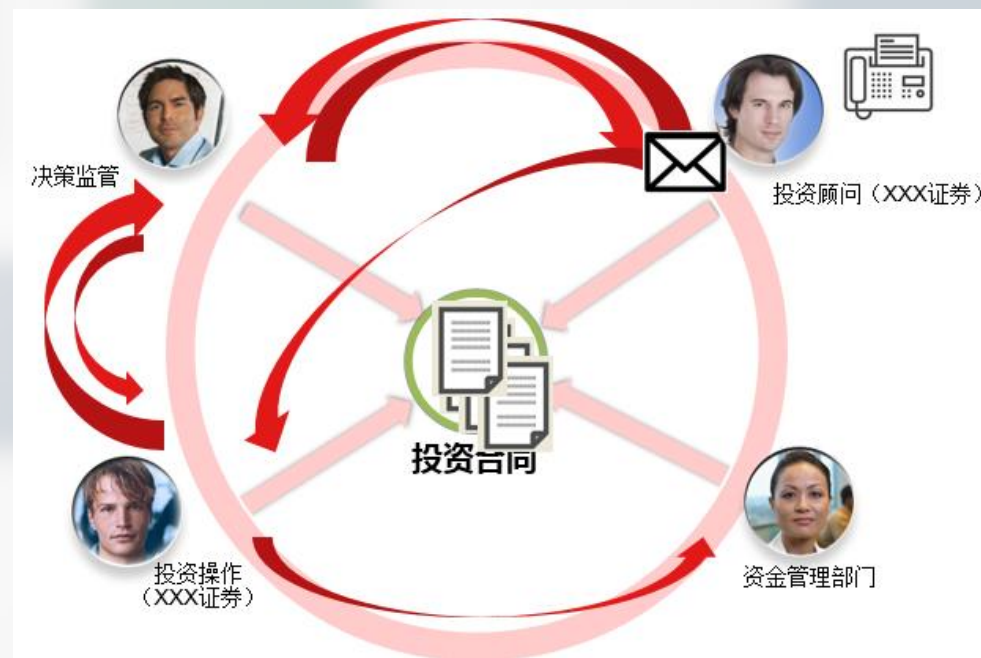
共享账本 - 实现数据共享，更加准确判断报价的合理性。同时，托管人购买资产后的资产保存在区块链中，委托人可以随时查看存量资产情况，审计方也可以实时审计。

- 区块链智能合约自动判断交易的合理性和合规性

智能合约 - 监管前置，可以提前到投资顾问下发指令时判断

- 通过基于区块链的系统来发送投资指令，代替原来的传真电话方式

不可篡改 - 解决传统手段核对预留签印的问题，提高指令发送的执行效率



区块链的其他应用场景

证券，国际贸易 以及零售银行

- 衍生合同
- 证券保险
- 提货单，信用证
- 跨境支付，跨境汇款
- 抵押品管理、合约执行

其他金融

- 电子货币
- 股权（私募、公募）、债券
- 金融衍生品（期货、期权、次贷、票据）
- 选举权、商品所有权、抵押品权属
- 交易记录、服务记录
- 众筹、小额信贷、小额捐赠

公共记录

- 地契、房地产权证、车辆登记证、营业执照
- 公司产权关系变更记录
- 监管记录、犯罪记录、电子护照、出生死亡证
- 选民登记、选举记录、体检记录、安全记录
- 法院记录、法医证据、持枪证、建筑许可证

其他

- 垃圾邮箱防范（每次发送需要一点工作量证明）
- 武器发射密码（多个密码共用）

私人记录

- 合同、签名、遗嘱、信托、契约（附条件）、仲裁
- 证书、学位、成绩、账号
- 医疗记录、染色体、基因序列

有形资产

- 钥匙、酒店门卡、车钥匙、公共储物柜钥匙
- 银行保险柜钥匙
- 特殊包裹递送（发送方接收方钥匙一起打开）
- 彩票、球票、电影票

无形资产

- 打折券、抵用券、付款凭单、发票、预订
- 专利、商标、版权、软件许可、游戏许可、数字媒体（音乐、电影、照片、电子书）许可
- 网络身份

The Global Eco-System on Blockchain and Hyperledger

Banks have also been very active in recent investments and partnerships with Blockchain Fintech

Notable Capital Raises in 2015 and 2016

Company	Date	Raise	Findings
 Digital Asset Holdings	Jan -16	\$60M	□ Raised \$60M from 15 investors, including JPMorgan, Accenture, DTCC, Citigroup, Goldman, ASX and IBM □ Launched in 2015, DAH provides distributed ledger technology solutions to wholesale financial firms
 Chain	Sept -15	\$30M	□ Notable investors: Visa, Nasdaq, Citi Ventures, Capital One and more. Announced plan to pivot away from its free bitcoin API service
 ripple	May -15	\$28M	□ Plan to use funds for international expansion. Relevant use cases for Seagate (investor) include ability to move payments and track positioning of supply chains
 CIRCLE	Apr -15	\$28M	□ Goldman Sachs was lead investor in \$50M round for Circle, payment applications provider
	Mar -15	\$75M	□ Lead investors: Andreessen Horowitz, RRE Ventures, and Chinese PE firm Yuan Capital, as well as Qualcomm □ Launched the 21 bitcoin computer - first computer with native hardware and software support for Bitcoin protocol.
 coinbase	Jan -15	\$75M	□ NYSE invested and plans to use expertise with Coinbase to bring additional transparency to Bitcoin market pricing

DECEMBER 17th 2015

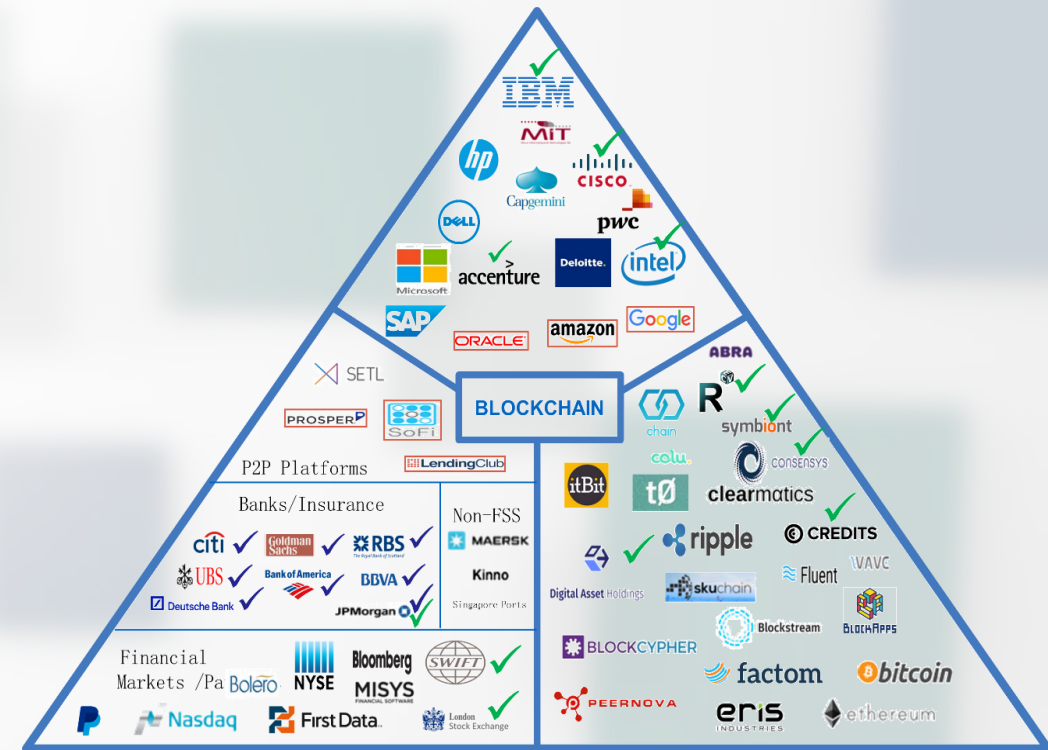
Making Blockchain Ready for Business!



New collaborative effort to advance the blockchain technology standard

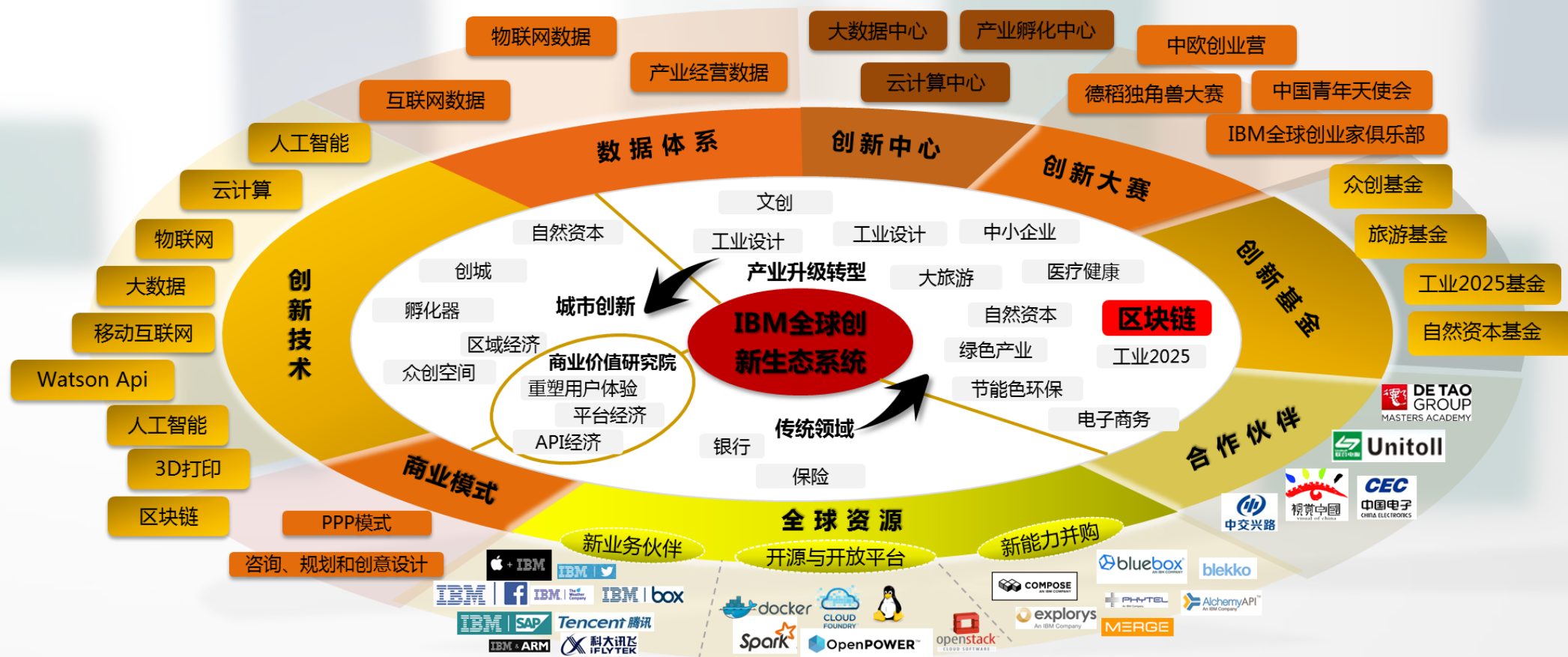
#blockchain #IBM

Announcement from Linux Foundation here: ibm.biz/OpenLedgerProject



Community + Code

Blockchain全球创新生态系统



Cognitive .Smart. Insights. Future

区块链产业的持续发展需要注入全球创新能力



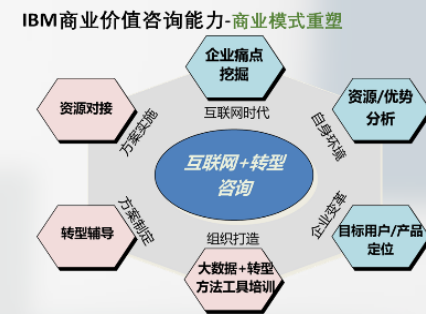
IBM以创新的认知计算能力整合全球网络资源包括技术、资金、人才、专业领域建设资源等联合全球合作伙伴打造细分领域创新与创业中心，助力城市创新发展



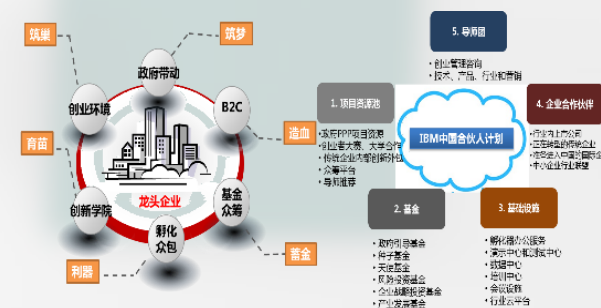
人工智能 IBM认知计算研发落地能力



智能物联网 智能全网采集分析能力



互联网产业咨询能力 商业模式重塑



社区生态网络 全球合作伙伴资源网络能力

感谢各位倾听
区块链助力信任经济未来

