

# IBM区块链技术 ( Blockchain ) 简介

“区块链(Blockchain)无疑是最近在金融服务领域谈到的最多的技术” IBM

“Blockchain 会从根本上改变我们做生意的方式”

“每一个客户的每一个 CEO, 都想了解 Blockchain”

“The good news is more financial institutions are interested in blockchain and are working to understand and think through where it could be used. Whether blockchain completely changes – or is just an addition to – the way we solve problems remains to be seen.”

SURESH KUMAR, SENIOR EXECUTIVE VICE PRESIDENT  
AND CHIEF INFORMATION OFFICER, BNY MELLON

Blockchain是否能够改变我们解决问题的方法，我们拭目以待。



什么是区块链  
(Blockchain)



区块链应用场景



IBM区块链技术 &  
z Systems

- **Blockchain** 技术有极大可能性使得有多方参与的商业网络转型，从而明显地降低成本和风险，并进行业务模式创新。

“过去的20多年，互联网使得个人和组织能够更有效地进行商业和社会活动。然而个人和组织相互之间进行交易基本模式并没有改变。Blockchain 可以带给那些流程更多的开放性和效率，正如我们在互联网时代所期待的那样。” —Arvind Krishna, Senior VP, IBM Research

Blockchain技术是一种因为Bitcoin而出名的设计模式，但它的用途更加广泛。

比特币（Bitcoin）是目前最大的区块链应用。它是一种点对点的电子现金系统，基于密码学原理而不基于信用，使得任何达成一致的双方能够直接进行支付，不需要第三方中介的参与。



比特币的概念最初由中本聪（Satoshi Nakamoto's）在2009年提出，基于开源及P2P网络建立全球一本公开账。

JPMorgan CEO如是说：

In 2014 at an annual meeting of the banking elite, CEO Dimon famously stated:



*(Bitcoin developers) Are going to try to eat our lunch, and that's fine.....That's called competition, and we'll be competing.*

In late 2015, Dimon dismissed Bitcoin as “a waste of time” while being more encouraging toward blockchain technology.

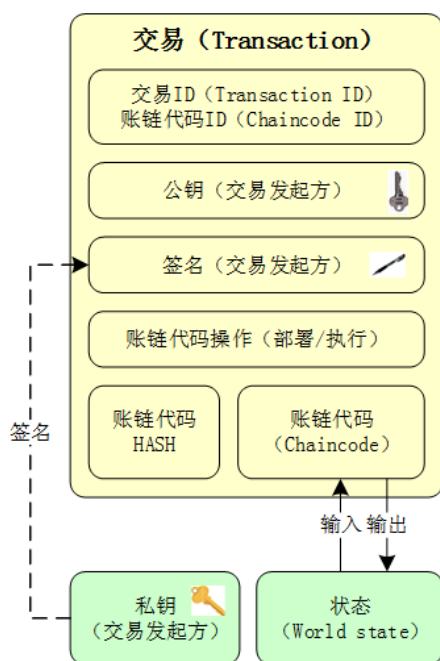
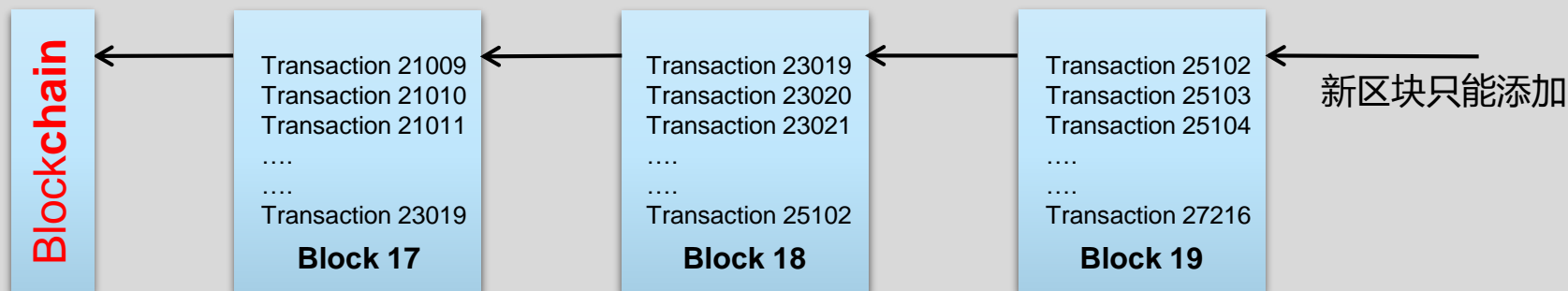
More recently, at the World Economic Forum in Davos, Dimon reiterated his stance on Bitcoin “going nowhere”. About blockchain, he added:



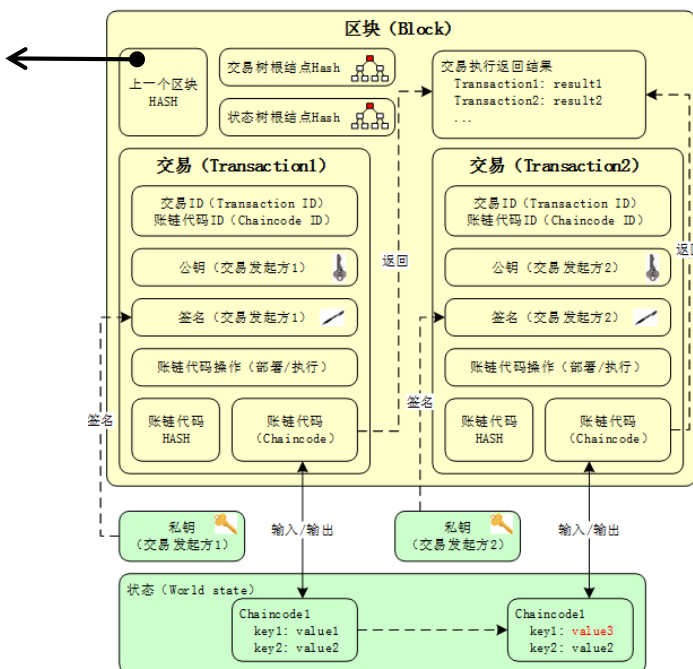
*The blockchain is a technology which we have been studying...and yes, it's real.*

# 区块链 (Blockchain) 账簿：大量使用密码学算法防篡改 如Hash, 数字签名, 加解密等

## 共享帐簿



一个交易:记录一笔资产转移的过程



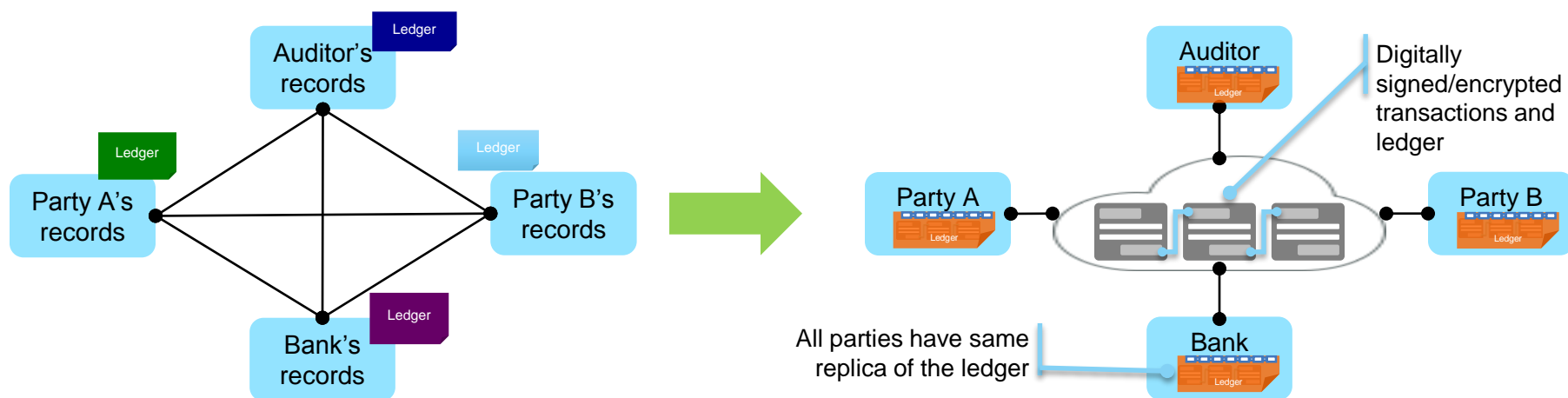
一个区块:记录一段时间内全局最新交易的数据块

- 区块链 (Blockchain)
  - 通过协商机制, 确定全局认可的区块, 把区块按时序串接在一起, 形成全局账簿.
- 帐簿 是记录一个业务活动的系统
  - 记录了参与者之间的资产转移.
  - 商业行为在参与不同的商业网络是有不同的帐本.



# 共享帐簿 ( Shared Ledger ) : 解决分布式环境中多方参与的互信问题 ( 业务处理中由于信用不连续导致的冲突和摩擦 )

- **Blockchain 共享帐簿技术**实现了在分布式环境里多方参与的双边交易中的去中介化。共享帐簿全网记录，可追溯，防篡改具有最终性。从而在保证安全的情况下，提高效率，降低成本。

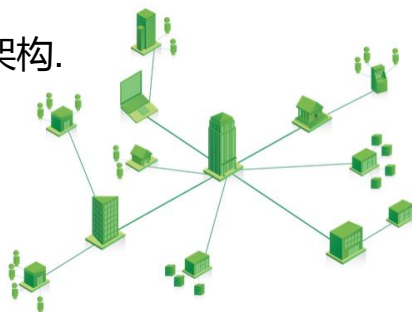


低效, 贵, 易受攻击

协商一致, 可回溯,  
防篡改, 最终性

## 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



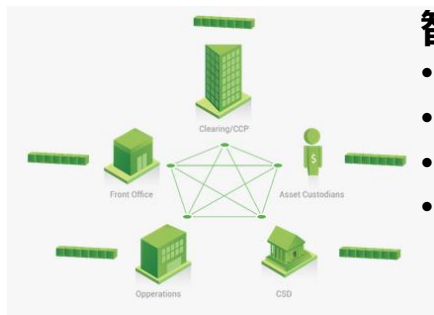
## 共享帐簿

- 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
- 批准制



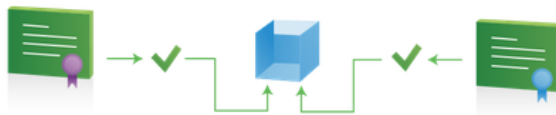
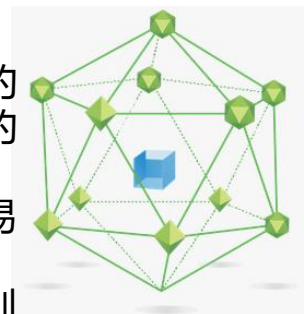
## 智能合约

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



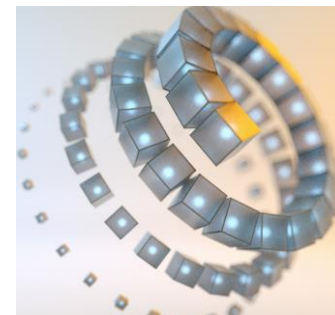
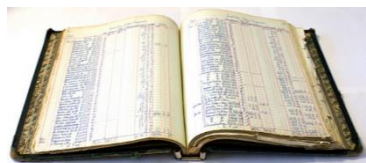
## 共识

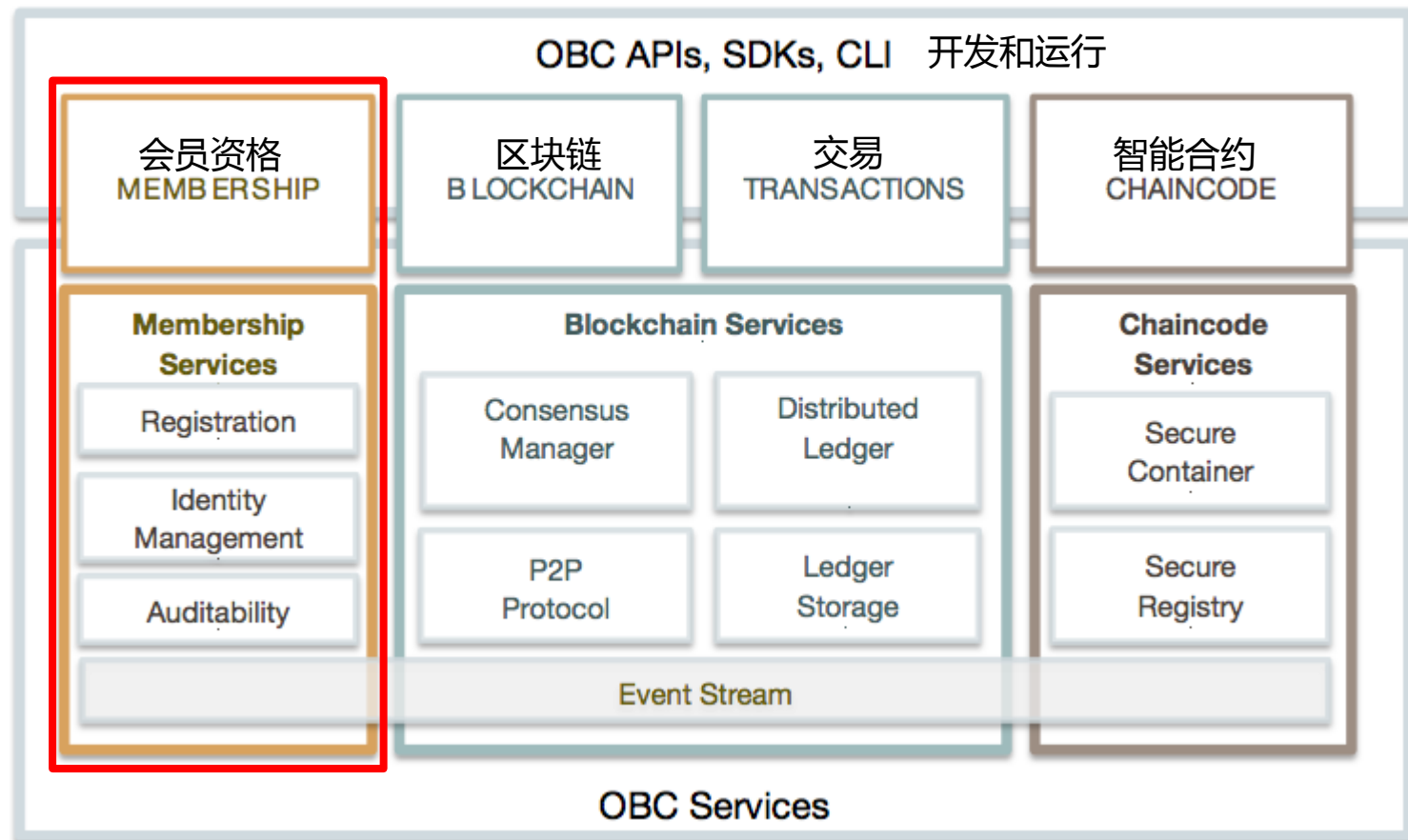
- 共识算法确保每份副本的一致性, 降低伪造交易的风险
- 所有成员都同意这些交易而且做过验证.
- 可以建立交易验证的规则.



## 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





- 除了Blockchain和智能合约的支持外，**商用的架构中的重点在隐私和保密及监管**。Membership会员资格服务模块提供所需的安全ID管理，实现批准制的帐簿访问和审计能力。安全隐私等的管理也要渗透到其他的模块。
- Blockchain有**公有链**和**联邦链**的区分。企业级商用应用中，**联邦链**是更贴合的选择。



- **第一步 ( 数字货币 , 也称为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——目前最大的区块链应用 )
    - 包含具体算法、数据结构、竞争协商机制
  
- **第二步 ( 智能合约 Smart Contract , 也称为Blockchain v2.0 )**
  - 资产数字化
  - 智能合约
    - 基于区块链的编程脚本语言, 图灵完备, 适合任意区块链数据结构和共识协议
    - 在各方监督下, 在符合条件时会自动执行, 无法反悔、篡改、干预、操纵
  
- **第三步 ( 衍生应用 , 也称为Blockchain v3.0 )**
  - 广义资产, 广义交换
  - 设备自主, 行业应用



DECEMBER 17<sup>th</sup> 2015

## Making Blockchain Ready for Business!

THE LINUX FOUNDATION  
IBM

New collaborative effort to advance the blockchain technology standard

**IBM Blockchain / Hyperledger**

#blockchain #IBM

Announcement from Linux Foundation here: [ibm.biz/OpenLedgerProject](http://ibm.biz/OpenLedgerProject)

## 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	<ul style="list-style-type: none"> <li>Raised \$60M from 15 investors, including JPMorgan, Accenture, DTCC, Citigroup, Goldman, ASX and IBM</li> <li>Launched in 2015, DAH provides distributed ledger technology solutions to wholesale financial firms</li> </ul>
Chain	Sept -15	\$30M	<ul style="list-style-type: none"> <li>Notable investors: Visa, Nasdaq, Citi Ventures, Capital One and more. Announced plan to pivot away from its free bitcoin API service</li> </ul>
ripple	May -15	\$28M	<ul style="list-style-type: none"> <li>Plan to use funds for international expansion. Relevant use cases for Seagate (investor) include ability to move payments and track positioning of supply chains</li> </ul>
CIRCLE	Apr -15	\$28M	<ul style="list-style-type: none"> <li>Goldman Sachs was lead investor in \$50M round for Circle, payment applications provider</li> </ul>
coinbase	Mar -15	\$75M	<ul style="list-style-type: none"> <li>Lead investors: Andreessen Horowitz, RRE Ventures, and Chinese PE firm Yuan Capital, as well as Qualcomm</li> <li>Launched the 21 bitcoin computer - first computer with native hardware and software support for Bitcoin protocol.</li> </ul>
	Jan -15	\$75M	<ul style="list-style-type: none"> <li>NYSE invested and plans to use expertise with Coinbase to bring additional transparency to Bitcoin market pricing</li> </ul>
Notable Ventures in 2015	Date	Commentary	

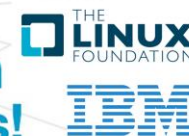


- ✓ R3 Consortium
- ✓ Linux Foundation
- Potential entrants



DECEMBER 17<sup>th</sup> 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](http://ibm.biz/OpenLedgerProject)



Community + Code

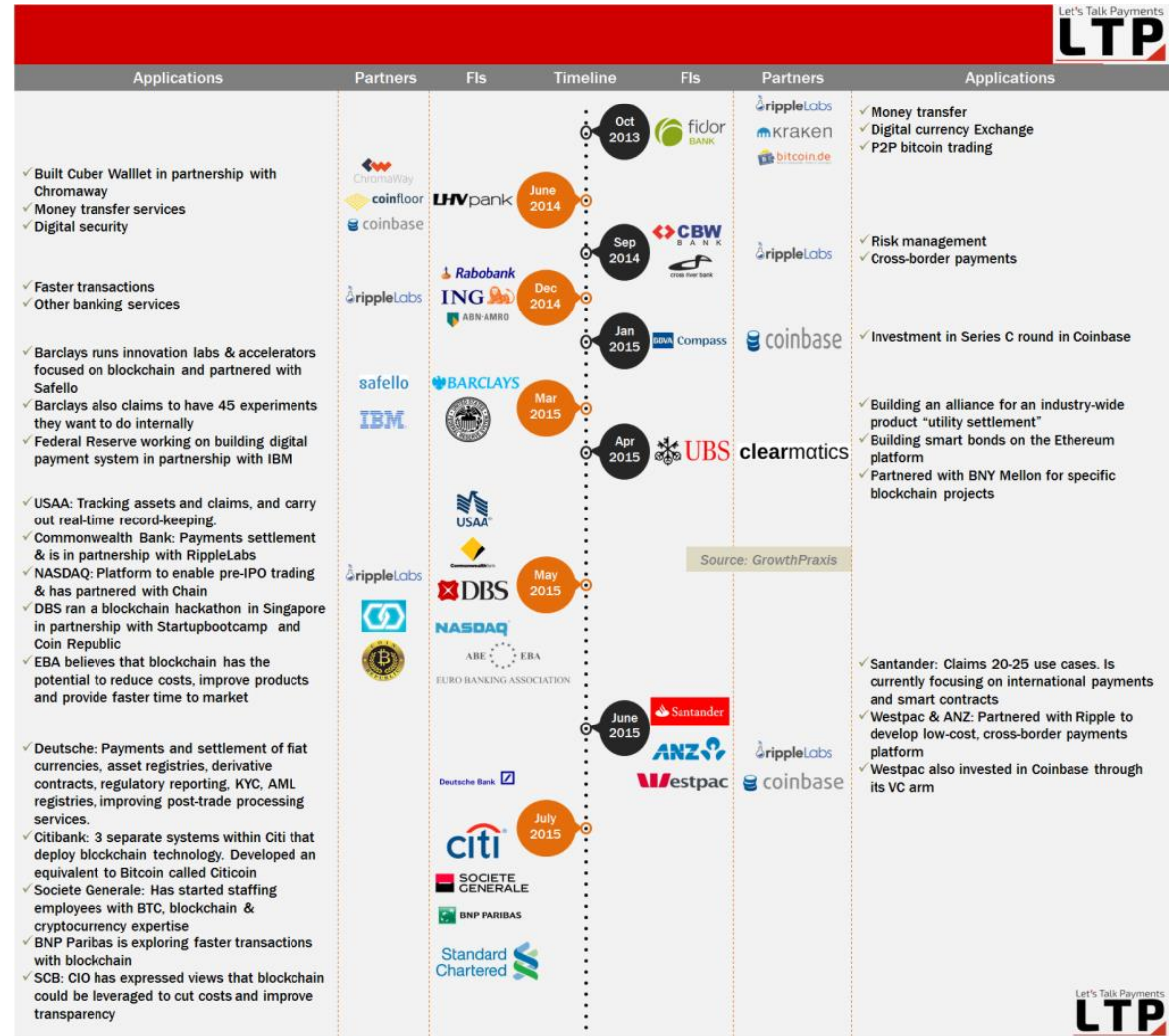


## ■ JPMorgan Already Testing Dollar Remittance via Blockchain Technology Between 2,200 Clients 23/02/2016 CCN.LA

- JPMorgan Chase & Co has been testing a blockchain program over the past few months wherein US dollars are being moved between London and Tokyo using distributed ledger or blockchain technology, the same innovation used to power Bitcoin.

## • Mizuho turns to blockchain for financial record keeping 17 February 2016 by Finextra

- Mizuho is to use distributed ledger technology to secure record-keeping of documents passed across the group globally.







什么是区块链  
(Blockchain)



区块链应用场景



IBM区块链技术 &  
z Systems

降低成本、风险、  
复杂度



提高记录可信度



增加监管透明度

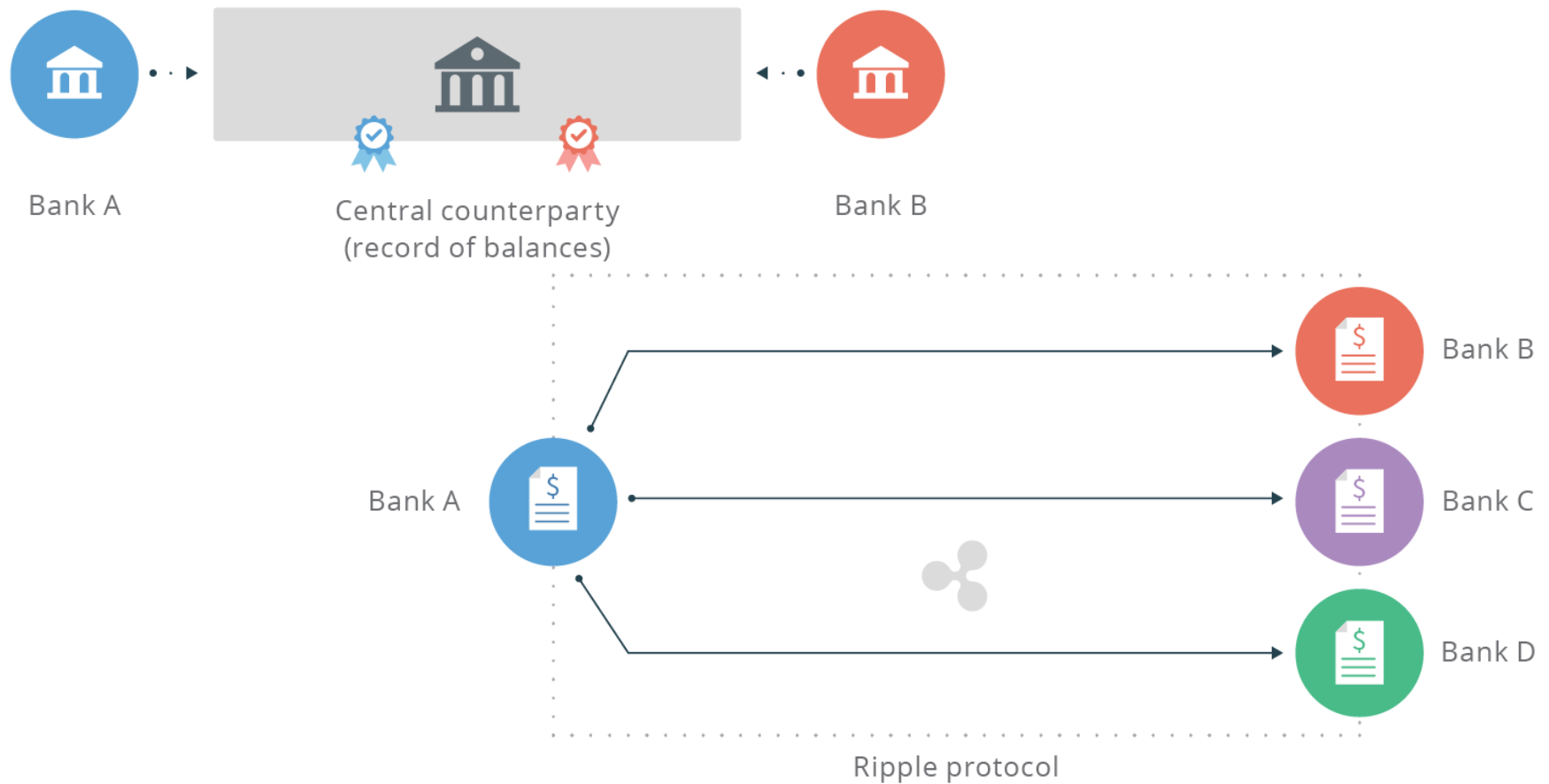


共同执行可信流程

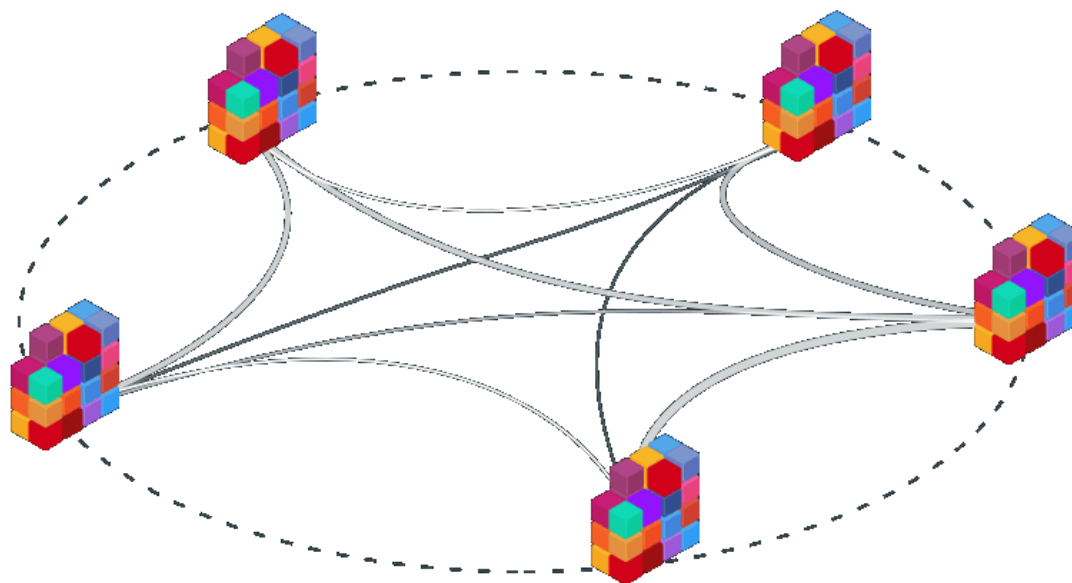




- 基于blockchain的payment解决方案
- 主要的用户是银行和金融机构



- Ethereum is a **decentralized platform that runs smart contracts**: applications that run exactly as programmed without any possibility of downtime, censorship, fraud or third party interference.
- The project was crowdfunded during August 2014 by fans all around the world. It is developed by the [Ethereum Foundation](#), a Swiss nonprofit, with contributions from great minds across the globe.



- 什么是the DAO
  - <https://daohub.org/about.html>
  - 基于smart contract的p2p
  - 1亿5千万美元
- 被攻击
- 软分叉
- 硬分叉
- 反思
  - 合法，不合法？
  - 谁的责任？

## ■ 国内区块链公司

### 应用领域

已应用于积分、股权、供应链等领域，正在与交易所、银行开展实验及应用测试。



#### 股权

**以信任为基础，私有股权流通。**

不可篡改的数字股权凭证，为股权登记与转让提供信任基础。布比区块链拥有的高扩展性，可灵活应用于：众筹平台、P2P平台、初创企业、Pre-IPO企业、区域交易所。提供可视化的股/债权管理，实现高效的场外股/债权交易、流转。



#### 积分

**多方联合开放，积分发行及兑换，促进积分流通。**

平台合作方可共同参与交易验证、账本存储、实时结算；商户、积分发行方、第三方支付平台进出更灵活。激活存量积分，满足商圈内不同商户的积分兑换。



#### 供应链

**利用不可篡改，溯源供应链管理。**

布比区块链，利用密码学可证明的算法构建多中心网络信任，公开、透明、不可篡改、不可撤销；多方参与信息透明共享，建立真品溯源的全程链式路径，直达消费者；全面的数据链提供决策依据，为大数据共享提供支撑；多中心，实现互动、协同、监督的利益共同体。

## 在区块链上建立审计公证业务流程 – Factom

- Factom是基于比特币区块链协议而构建的另一层分布式的、匿名的、数据协议，赋予把比特币区块链技术拓展到其他应用场景中的能力。另外，用户无需持有加密货币也可以使用Factom的系统功能。Factom旨在解决速度、交易成本和区块链膨胀这三大核心约束的协议，构建了一个标准的，有效的，安全的基础，这将使应用程序的运行速度更快，更便宜，并且不会造成区块链膨胀。
- Factom利用区块链技术来革新商业社会和政府部门的数据管理和数据记录方式：
  - 通过Factom, 用户可以对文件进行哈希, 并把这个哈希公开发布。这就像为文件制作了一枚电子指纹一样。通过这个电子指纹就可以对文件进行验证, 同时不泄露任何个人信息。
  - 每个数据会被拷贝成百上千份并分布在世界范围内。Factom系统会为所有数据发布一个分布式的哈希表。所有数据会由Factom发布, 任何人都可以维护一个节点来记录Factom系统里的数据。
  - Factom通过把哈希值上传到比特币的区块链中, 以此来证明数据的存在(Existence proof)。每个哈希值代表了那个时间点数据所处的状态。把这些多个时间点的状态联系起来就能反映数据如何随着时间变化的。由于时间,成本,容量的限制, Factom不会把所有数据都上传到比特币区块链上。



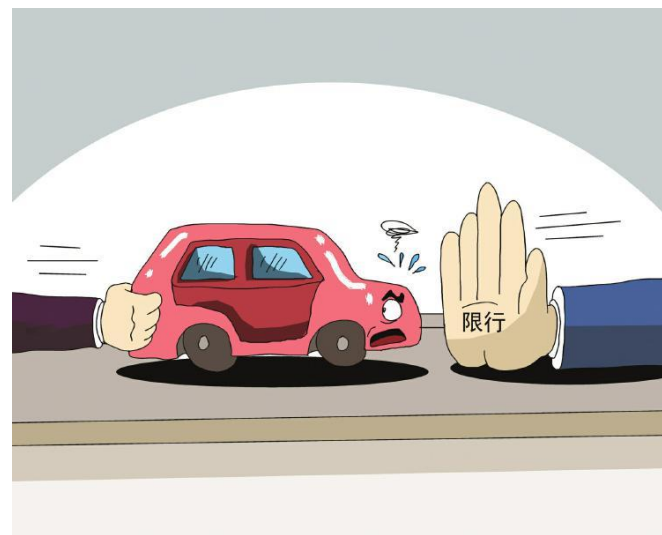


- **证券**
  - 股权交割
  - 衍生合约
  - 证券保险
- **国际贸易**
  - 提货单
  - 跨境支付
- **企业银行**
  - 财团贷款
  - 银行间结算
- **零售银行**
  - 跨境汇款
  - 抵押品管理
  - 抵押合约执行 (smart contract)
- **公共档案**
  - 房产登记
  - 车辆登记
  - 产权登记
  - 营业执照登记



- 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、营业许可证
    - 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
  - 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
  - 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）
5. Financial services.
- a. In payments, blockchain technology could address serious issues with delayed settlement of funds inherent in most payment networks, issues that impose costs on users looking to either speed up settlement or mitigate risks as those funds are in transit.
- b. In trading, settlement, and clearing, blockchain could help automate, reduce costs, and alter how financial firms compete over a range of asset classes.
- c. In know your customer (KYC) and anti-money laundering (AML) programs, blockchain could share data and improve transaction monitoring and reporting for compliance.

- 不适合高频高性能交易环境（如毫秒级交易响应时间）
- 没有业务网络的小组织
- 不是一个数据库替代方案
- 不是一个消息传递替代方案
- 不是一个交易处理系统替代方案





什么是区块链  
(Blockchain)



区块链应用场景



IBM区块链技术 &  
z Systems



# IBM Blockchain is open for business, Mar, 2016.



www.ibm.com/blockchain/ Search

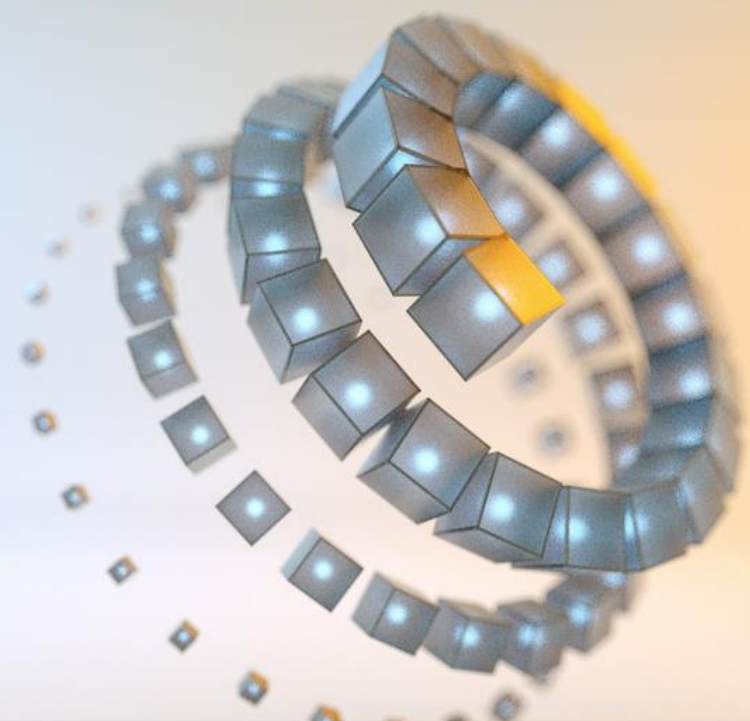
IBM Analytics Cloud Commerce IT Infrastructure MobileFirst Security Watson Search

IBM Blockchain What is Blockchain? What Can Blockchain Do? How Can IBM Help? For Developers

# IBM Blockchain is open for business

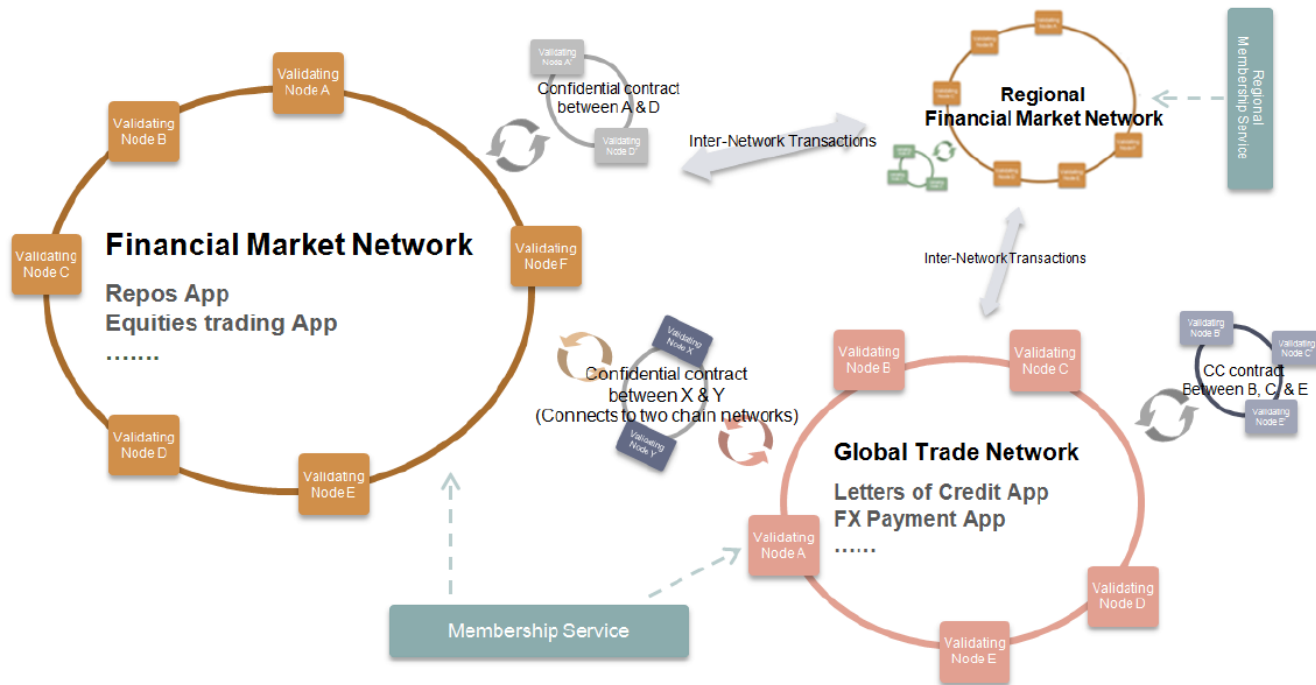
Learn how blockchain will fundamentally change the way we do business. Then let us help you give it a try.

Get started



Connecting to www.google-analytics.com...





- **世界上应该有很多个Blockchain网络**：每个网络有自己的帐簿，服务于不同的目的，在核心功能上，不会依赖于某个网络。网络和网络之间应该可以互相访问帐簿(在控制之下)。
- **许可网络的需求日增**：网络的节点由已知白名单的组织运行。网络的参与者都有授权的ID。访问权限有不同的级别和范围。
- **隐私和秘密都很重要**：任何人的ID和行为模式，在blockchain的网络上都不应该被没有授权的人通过研究帐簿搞清楚。任何在网络上的业务逻辑和交易参数也应该不能被除了保管方以外的其他人所访问。

# Blockchain for Business – Our Point of View

## Community + Code



Linux  
Hyperledger Project

Open Source Code: Blockchain built from the ground up for business;

**Permission | Privacy**  
**Confidential | Auditable**

## Cloud



IBM Blockchain Cloud  
WebSphere Blockchain Connect

Blockchain on Cloud with value add Services;  
**Identity | Consensus | Audit**

Connect every WebSphere system to a Blockchain

## Clients



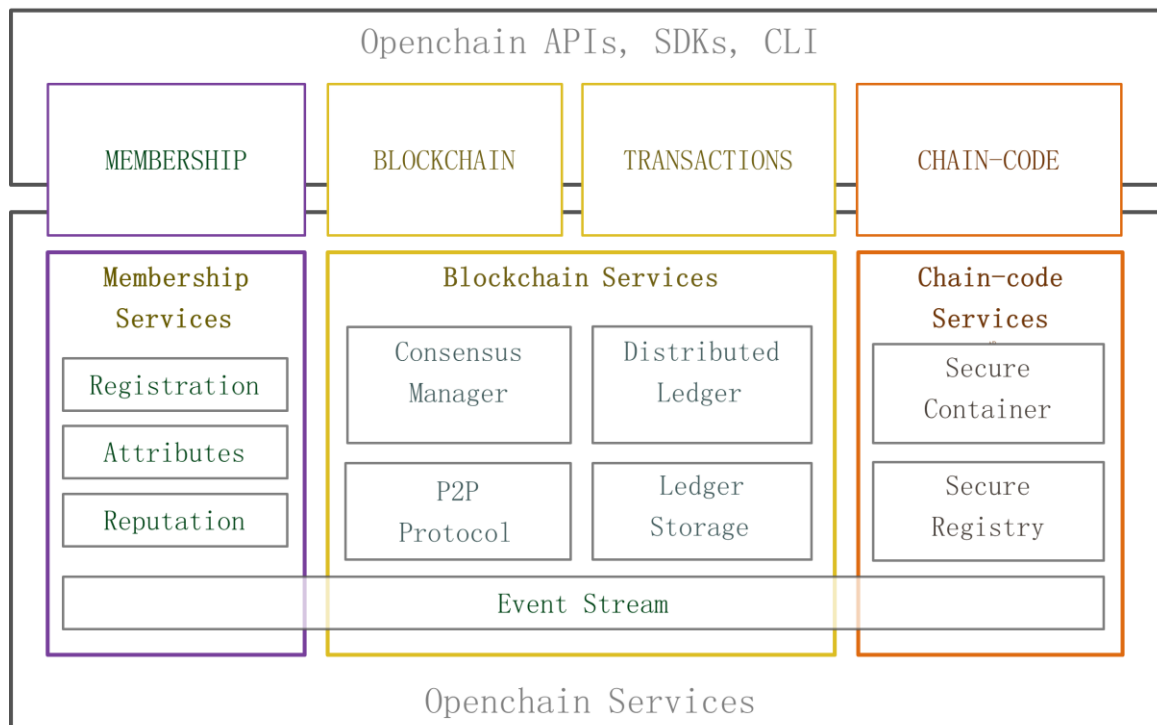
Blockchain Solutions  
IBM Bluemix Garage for Blockchain

Blockchain Solutions for Financial Services;  
**TradeFinance | Securities Settlement**

Blockchain Garage  
**NY | London | Singapore | Japan**

Blockchain GBS Practice

**\*\* Openchain = Open Blockchain = OBC = IBM Blockchain \*\***



Open Source Code: Blockchain built from the ground up for business;

**Permission | Privacy**  
**Confidential | Auditable**

- 可插入式共识算法, 现在提供noops, PBFT, SIEVE算法
- P2P协议使用Google RPC (gRPC)
- 帐簿存储使用RockDB
- Chain-code目前支持GO语言编程, 未来支持Node.js ...

## MEMBERSHIP

Identity, Privacy and Auditability of blockchain participants.

## BLOCKCHAIN | TRANSACTIONS

Distributed transaction ledger whereby the ledger is updated by consensus

## CHAIN-CODE

“Smart Contracts”, provide ability to run business logic against the blockchain.

## APIs, SDKs, CLI

Gives developers the ability to programmatically control the blockchain network

- 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17th December 2015
  - 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）



## Blockchain on z Systems

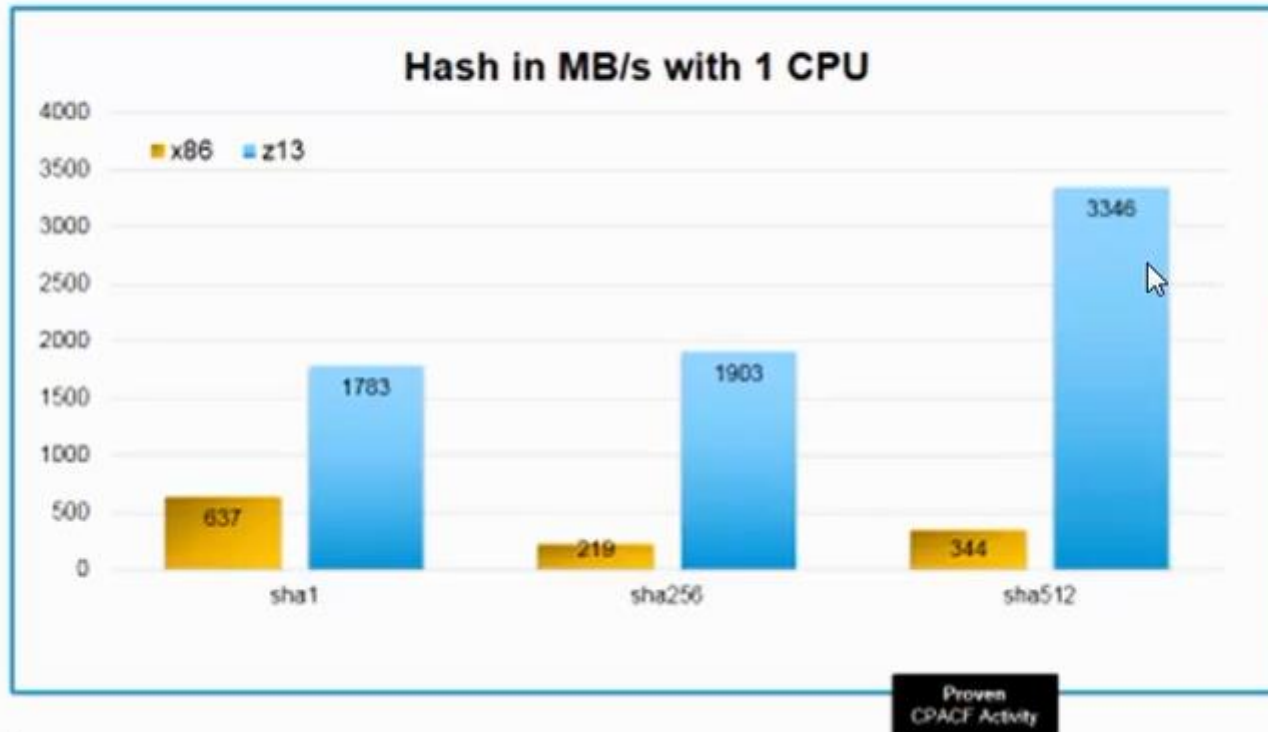
**"-Z" Z hardware acceleration**



**Enterprise Public Key Crypto Standard 11 (PKCS 11) Compliant**  
**Federal Information Processing Standard (FIPS) 140-2 Compliant**  
**Optimized Network – 41% to 82% faster response time, 1.4x – 7x more throughput**



## HASH ENCRYPTION COMPARISON



- z Systems上优化的通讯使得通讯效率提升最大致7倍
- z Systems可用性和扩展性提供一个可靠的开发/测试及生产环境
- 硬件加密来加速Blockchain的哈希，签名和安全控制
- Z的安全性和规世界标准
- 防干扰密钥保存在firmware/加密卡中
- 减少数据中心的占地面积，简化管理，节省能源



1. 区块链是一种共享账簿技术，具有分布式、全网记录、低成本、高效率、安全性等特点
2. IBM在区块链技术的研究是领先的，支持开放标准、开放源码、开放治理结构的区块链技术
3. 区块链技术的业务价值在于提高流程透明度、数据可信度、降本增效
4. 区块链技术的难点和突破在于行业应用



- WW blockchain community
- <https://w3-connections.ibm.com/communities/service/html/communityoverview?communityUuid=a0bde329-ce7b-4b02-a134-88b7628a8e70>
- Z blockchain community
- <https://w3-connections.ibm.com/communities/service/html/communitystart?communityUuid=d39c77b1-d858-4bf9-9e89-3a182dbc3822>
- GCG blockchain community
- <https://w3-connections.ibm.com/communities/service/html/communitystart?communityUuid=b9cd2613-9143-48d0-b53f-2ce187c9843a>
- Z Blockchain interest group in China lab --- in plan

**THANK YOU!**

- 工作量证明 ( 挖矿 )
  1. 计算世界上最后一个账簿的Hash值 (H)
  2. 不断接收世界中广播出来的新交易单 ( T, 未归入账簿链 ) , 剔除无效交易
  3. 猜一个随机数(N), 使 $\text{sha256}(1,2,3) < \text{难度值}^1$
- 创建临时账簿
  1. 一旦猜中, 立即生成临时账簿 ( Block ) , 包含以下内容
    - sha256()的计算结果作为账簿ID
    - 创建账簿**奖励交易单**
      - 创建第1~210,000个账簿, 每账簿初始50元
      - 创建第210,001~420,000账簿, 每账簿初始25元
      - 创建第420,001~630,000账簿, 每账簿初始12.5元
      - 以此类推...
    - 工作量证明过程中接收的全部新交易单 ( T )
    - 随机数 ( N )
    - 最后一个账簿的Hash值 (H)
    - 最后一个账簿的ID等
  2. 通过P2P网络全局广播
- 每10分钟计算出一个账簿

## 比特币总量是有限的

$$100\text{元} * 21\text{万} * \sum_{n=1}^{\infty} \frac{1}{2^n} = 2100\text{万元}$$

## 账簿结构

账簿ID ( 0x00000000000001e34f2a234ea33f..... )  
初始比特币奖励交易单  
创建这个账簿过程中收到的交易单数据 ( T )  
上一个账簿的散列数据 ( H )  
幸运随机数 ( N )  
上一个账簿ID

1. 难度值自动调整, 确保平易CPU计算速度, 保证全局账簿创建速度为10分钟



## ■ 检验账簿

- 收到临时账簿全网广播后，每个节点都要判断其中的交易单是否合法，逐一比对交易单从来没有出现过，不是重复支付
- 如果通过，把该临时账簿链接到本地账簿

## ■ 协商选择

- 由于网络传输延时，有时一个节点会先后收到收到多个临时账簿，似乎都有是正确有效的，这时会产生一个分支 ( fork )，各节点可在“最大工作量” ( 分支的难度和最大 ) 分支上继续追加新账簿，并全网广播。最终“最长工作链”胜出，其它分支被丢弃

