

区块链

(区块链)
--数字应用的新中断



灵宗, 博士

高级软件工程师/科学家
ibm almaden 研究中心
美国加利福尼亚州圣何塞

关于音箱

灵宗 (棕), 博士。

高级软件工程师/科学家

ibm almaden 研究中心, 加利福尼亚州圣何塞, 美国

日常工作 (工程和服务):

1. (60%)研究与开发
 - 关于云数据存储管理软件
2. (25%)关键客户服务
 - 在特种武器攻击队 (swat)
3. (10%)全球培训和学术讲座
 - 作为技术宣传员和大学大使
4. (5%)技术咨询
 - 硅谷风险投资

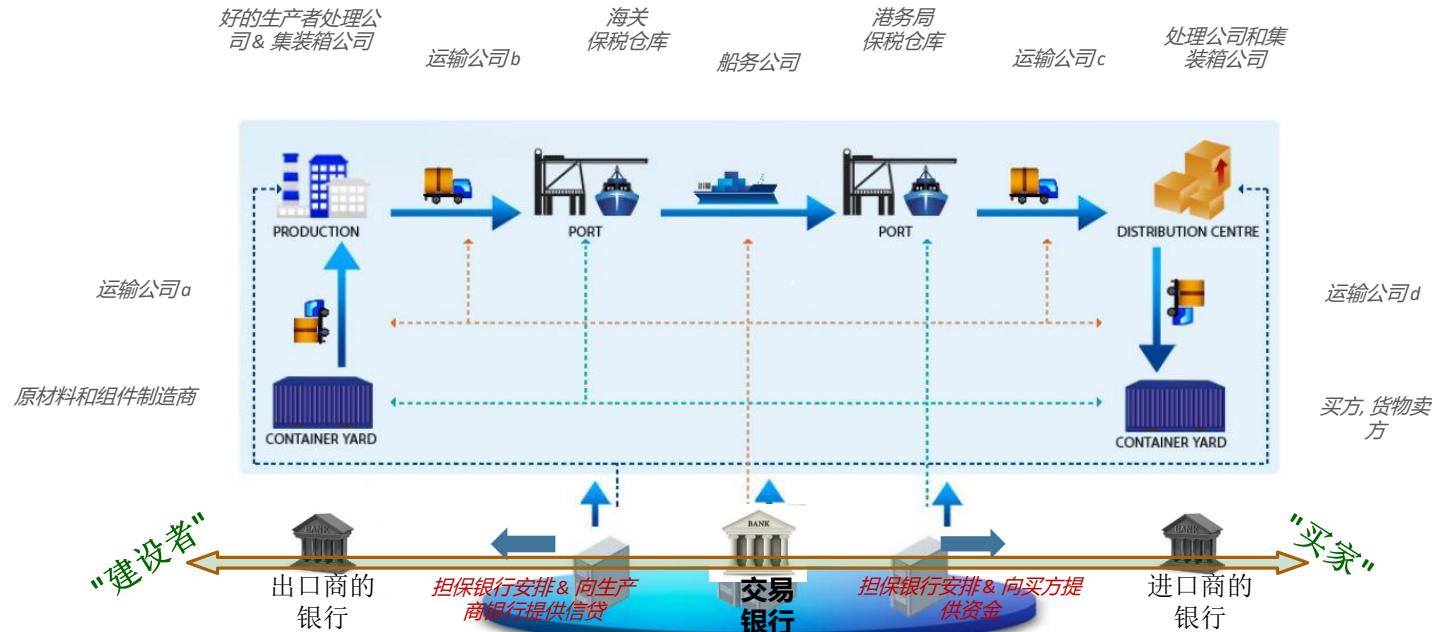


内容

- ❖ 动机
- ❖ 概念
- ❖ 使用案例
- ❖ ibm 优惠
- ❖ 演示

支付交易：今天

几乎完全手动与一个单一的 "交易" 需要长达 50天！

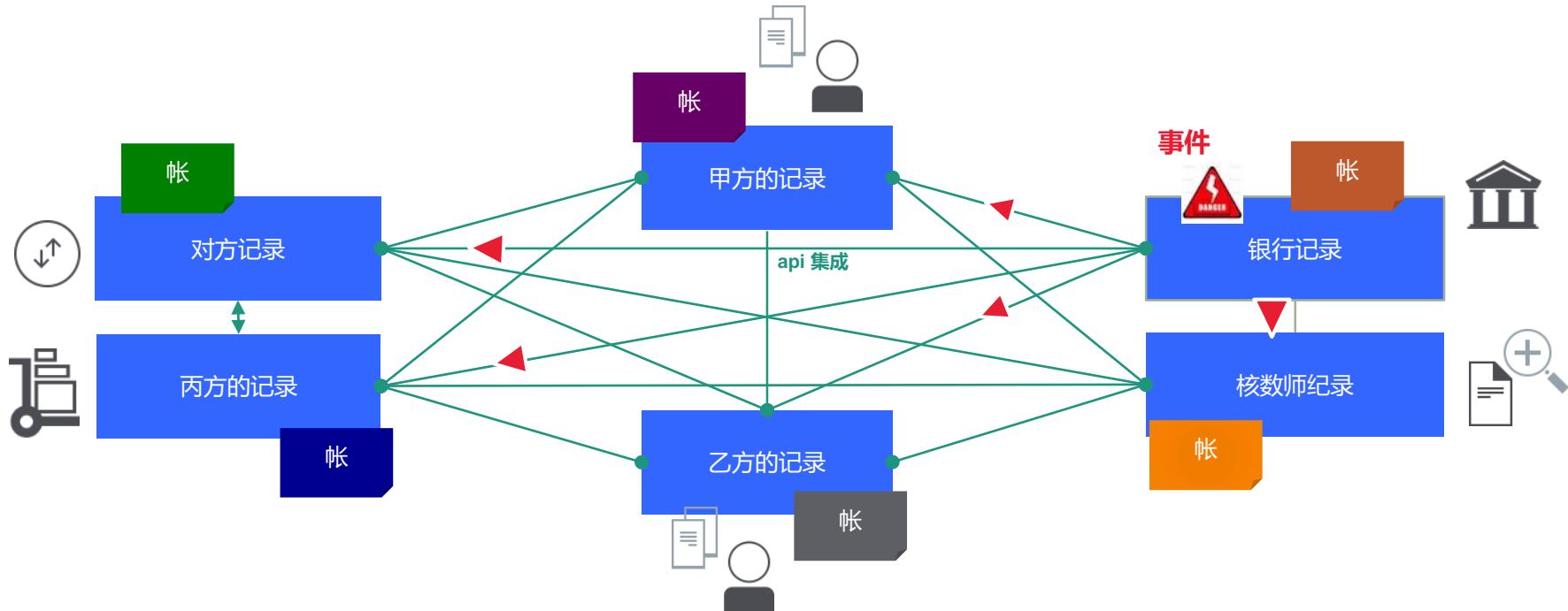


"交易只需几秒钟, 但完成交易需要数天时间。"

--高盛全球技术业务发展主管

问题 分类账

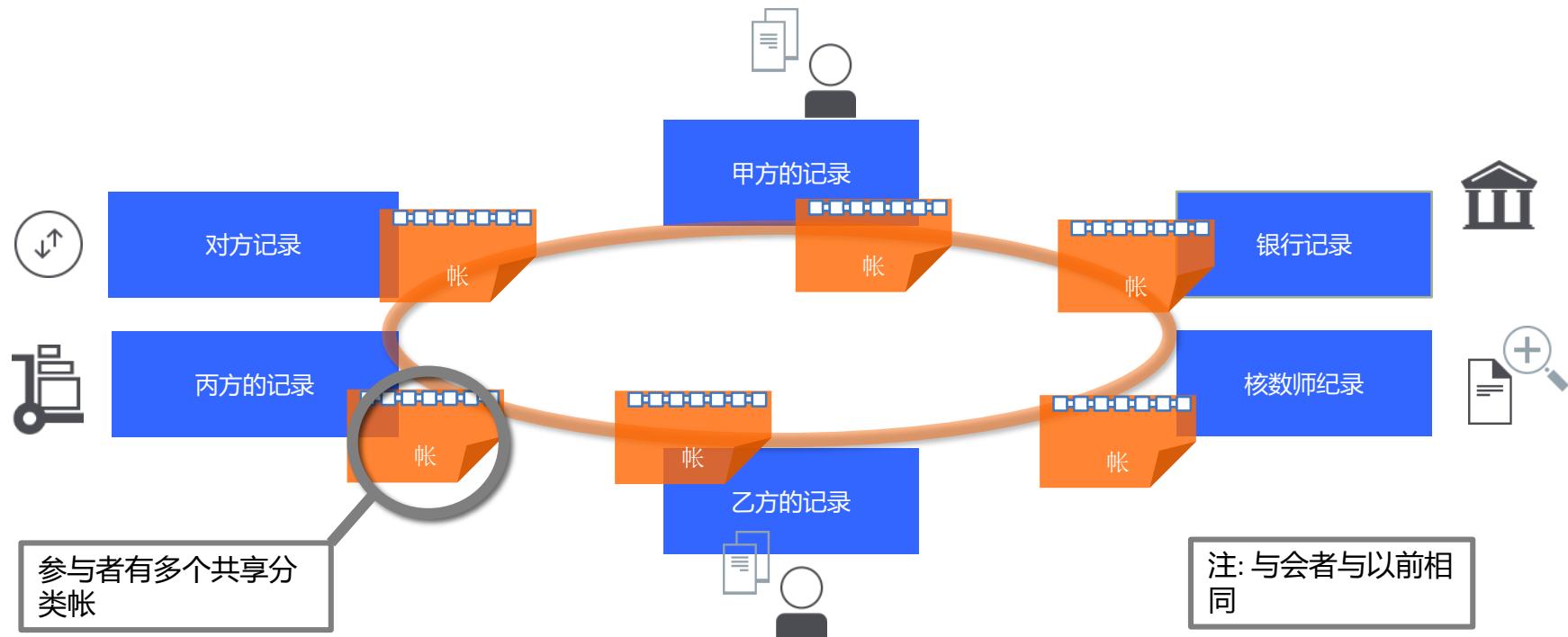
- 在当今的业务网络中, 监控资产所有权和转移既耗时又低效。独立



效率低下、成本高、对错误敏感和易受攻击

解决方案 -a数字许可,复制,共享分类帐 通过打开启用区块链技术

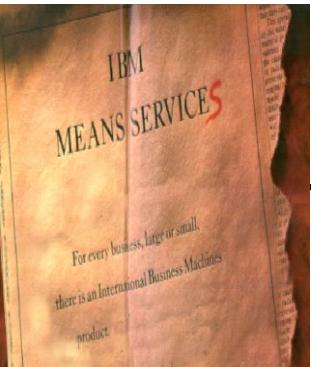
为什么?



一致性、效率、安全性和恢复能力

引领新的计算模型提供服务

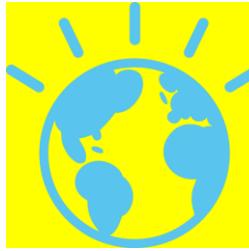
为什么？



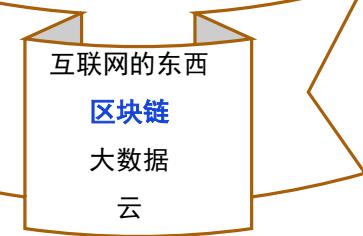
计算



个人电脑



智慧星球



1950年

1965年

1980年

1995年

2010年

2015年



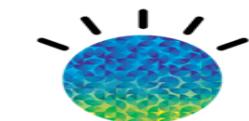
主机



互联网



沃森

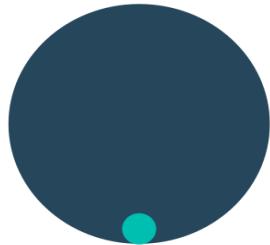
Business
Analytics
&
OptimizationSmarter
CommerceSocial
BusinessSmarter
CitiesWatson
Solutions

一般的区块链



区块链是新一代事务性应用程序的技术，它在简化业务流程的同时建立信任、问责制和透明度。将其视为用于交互的操作系统。它有可能大大降低完成工作的成本和复杂性。

Total Blockchain opportunity

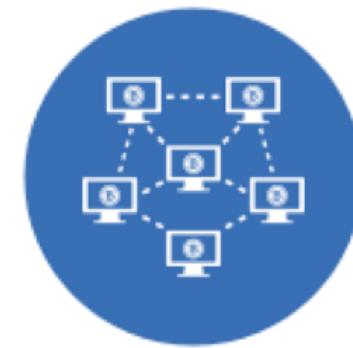


Total Bitcoin opportunity

区块链是一个**设计模式**因其用途而闻名**比特币**.但它的用途去远远超出.



区块链可以**重新想象**世界上最基本的商业互动，并为发明新的数字互动风格打开了大门。



ibm 正在采用**区块链**一个非常**广泛**业务应用程序的支持

区块链技术的价值

降低成本和复杂性



共享的受信任事务



减少错误的



弹性



安全



可审核性



金融服务的区块链--一场数字革命

区块链是一个新兴的**平台**用于交易服务。区块链技术有可能从根本上改变多方业务网络，从而显著降低成本和降低风险，同时推出新的创新业务模式。这是新一代的数字革命，继这一代之后给我们带来了信息互联网。

区块链从根本上说将改变我们做生意的方式。

在金融服务业中，基于**计算技术**，区块链是一种巧妙的简单、革命性的协议，它允许事务同时匿名和安全、对等、即时和无摩擦，通过将信任从强大的中介分发到一个大型的全球网络，通过大规模协作、巧妙的代码和密码学，可以对网络上发生的每一笔交易进行防篡改的公共分类帐。

区块链是新增功能作为一种数字武器

纵观历史，旧范式的领导人很少接受新的范式。

- Skype与AT & T; 贝宝与签证; Twitter与Cnn; 超级与通用或赫兹; airbnb与万豪.....

在金融服务业中，区块链可以从根本上降低对银行来说，提高生产力，更容易向全球客户提供产品和服务，还可以降低风险在行业中，特别是在批发金融领域。许多金融产品的结算时间需要几天，有时甚至几周，占用资本，使行业参与者面临巨大的交易对手风险。区块链承诺从根本上简化许多业务流程，降低风险并提高透明度。

此外，区块链可以使我们能够重新设计公司，支柱之一现代资本主义。随着全球身份、信任、声誉和交易点对点平台的兴起，我们将能够重新设计公司的深层结构，以实现创新和共同创造价值。

与之前的重大范式转变一样，区块链将创造赢家和失败者！

内容

- ❖ 动机
- ❖ 概念
- ❖ 使用案例
- ❖ ibm 优惠
- ❖ 演示

区块链是 (1) 电子, (2) 分发, (3) 复制, (4) 分散帐

什么?
你在说
什么?

帐是一个企业的记录系统

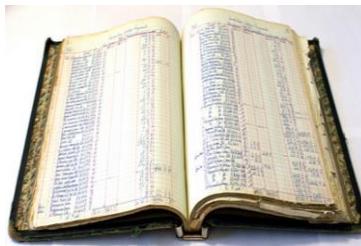
- 记录参与者之间的资产转移。

企业将有多个分类帐多个他们参与的商业网络……因此可能是“同行”在多个铁链…。

“块”是一个已执行和经过验证的交易

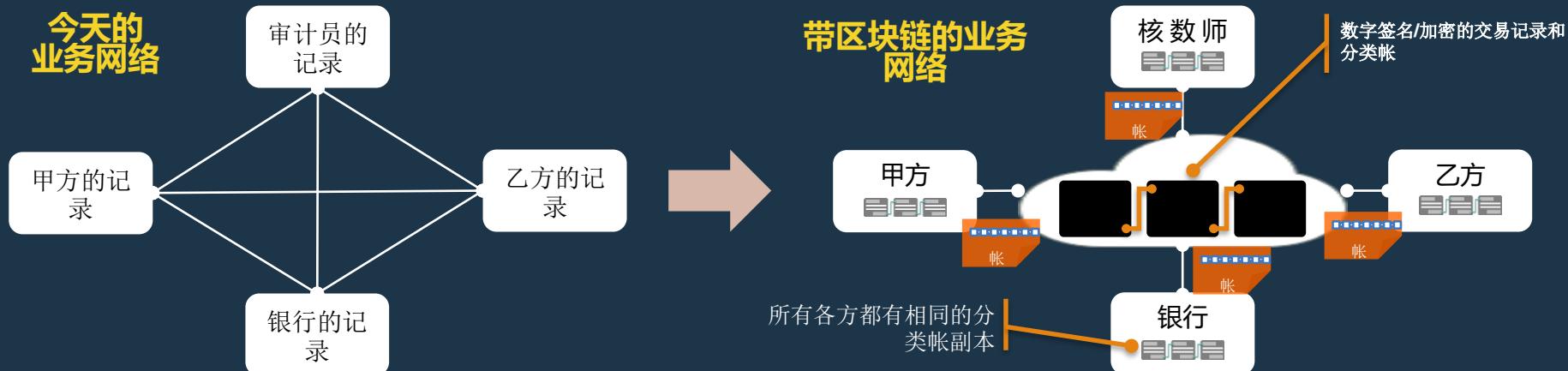


"链"是分类帐
(所有交易的记录簿)



螺母壳中的区块链

- **a 个共享分类帐技术允许业务网络中的任何参与者查看记录系统(分类帐)**
- **智能合同: 合同所暗示的业务规则, 编纂在区块链中, 并与可核查和签署的交易一起执行。**



效率低下、成本、敏感和脆弱性

共识、来源、不可变、终结

区块链的关键概念

好处:



交易时间从几天
到接近瞬间

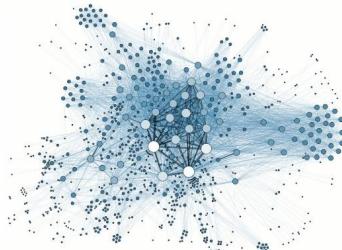


间接费用和费用
中介



篡改、欺诈和网络
犯罪

分布式共享分类帐



共识



密码

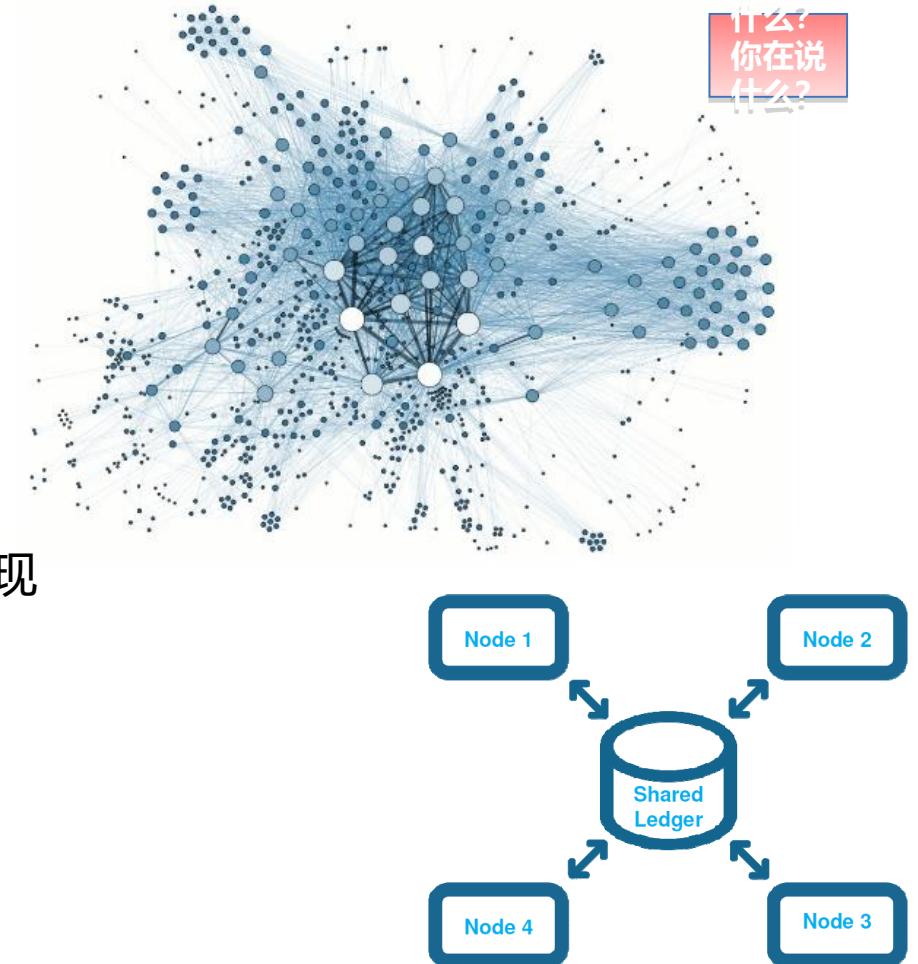
254F1 21B2C809 8833B0CC
3ECAA CB3EE DE038D7F
2AA4D 04143 7571C83
7DED9 B57C 820AE07
696DB 7D7F7 6DD29
0014D 41080C5 9754E072
05552 534146D0 8960929
18BFC 0F130429 90A60B99

智能合同



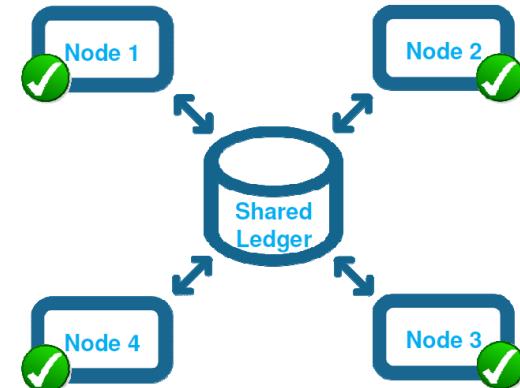
分布式共享分类账

- 组**复制**数据库 (节点)
- 中分发的**事务块**
- 所有节点保持**所有**交易
- 各方**确定**与公钥 (=匿名)
- **可访问性**的交易记录, 具体取决于区块链实现
- **弹性**对于一个或多个节点的故障
- 操作的节点组**防篡改**



共识

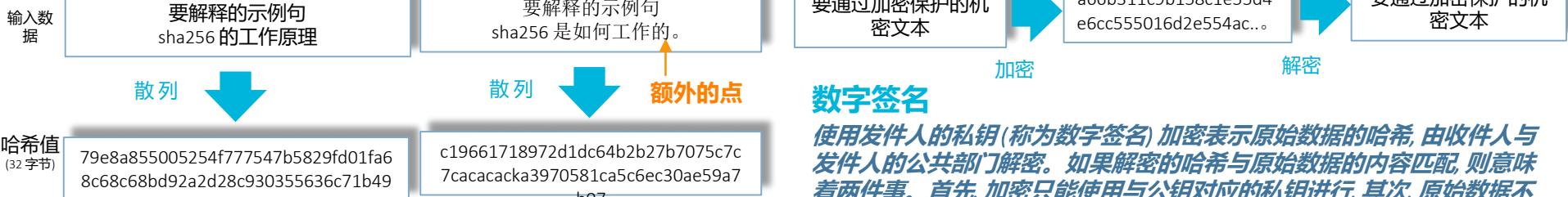
- 共识 = 大多数节点同意交易的有效性
- 包括上的验证 双倍支出
- 无授权(公共) vs。 许可(专用) 区块链设置
- 工作证明/证明节点的有效性
(仅适用于无权限网络)



密码

散列

创建表示内容和其他字符串完整性的位字符串(摘要)。更改原始字符串中的一个字符将导致完全不同的哈希。更改原始字符串中的多个字符(导致相同的哈希)需要很长时间内的大量处理能力。



加密

用收件人的公钥拼凑明文,以便该私钥的持有人是唯一能够对邮件进行解码的人。这用于保证所交换数据的机密性。



数字签名

使用发件人的私钥(称为数字签名)加密表示原始数据的哈希,由收件人与发件人的公共部门解密。如果解密的哈希与原始数据的内容匹配,则意味着两件事。首先,加密只能使用与公钥对应的私钥进行。其次,原始数据不能被篡改。

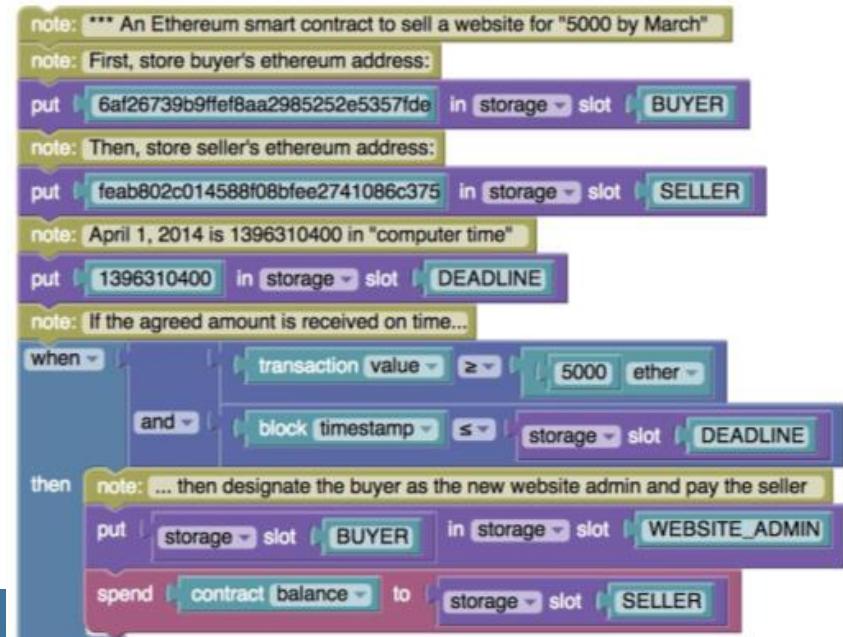


公共和私人钥匙和钱包

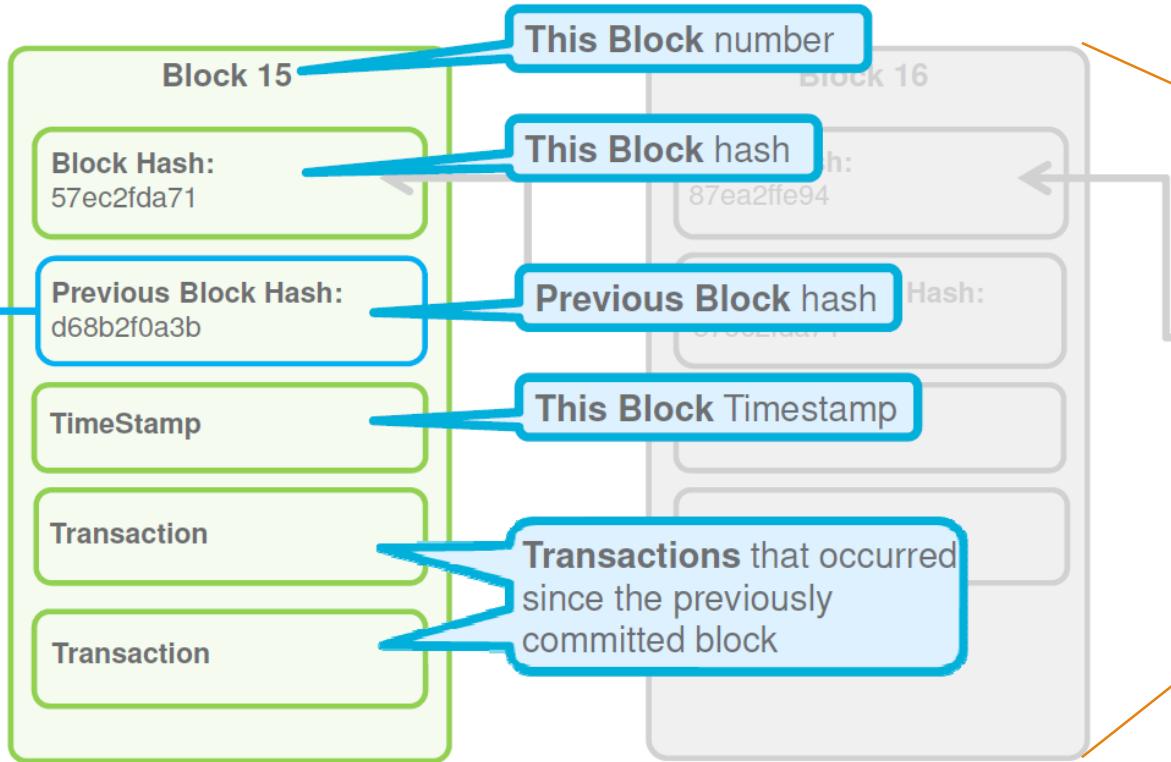
两个大小素数,它们之间有数学关系。使用一个密钥加密的字符串只能用另一个密钥解密。一个密钥需要保密,另一个密钥可以公开,以便其他各方可以使用它以安全的方式与您交换数据。需要存储私钥,以便仅对所有者可以访问私钥。这可以在个人设备(pc、智能卡、usb 记忆棒、手机...)上完成,也可以通过服务提供商(冷和热钱包)远程完成。

智能合同

- 业务逻辑可以分配给区块链上的事务
- 作为一个“公证员”区块链交易
- 持有量条件在其中，必须执行具体的行动
- 促进托管服务
- 不可能是改性没有预定义的权限
- 定义事务有效的条件
- 坚持代码和数据
- 可能从链链链接到关联的侧存储（例如加密的数据库）

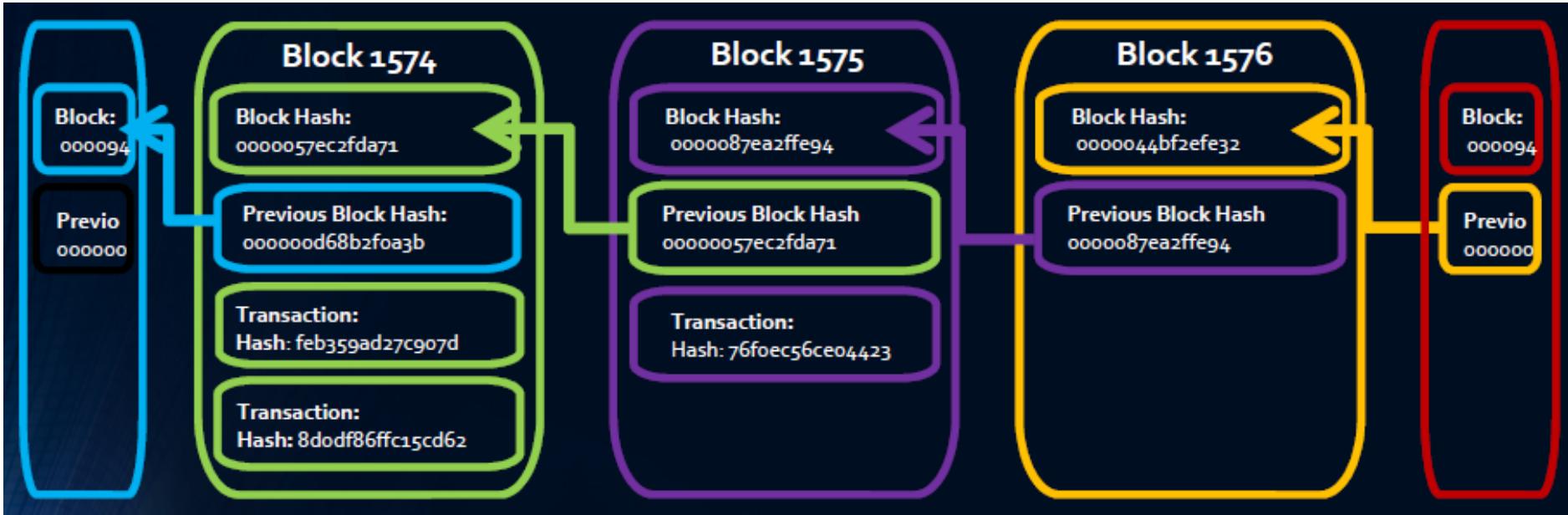


块中的内容是什么?



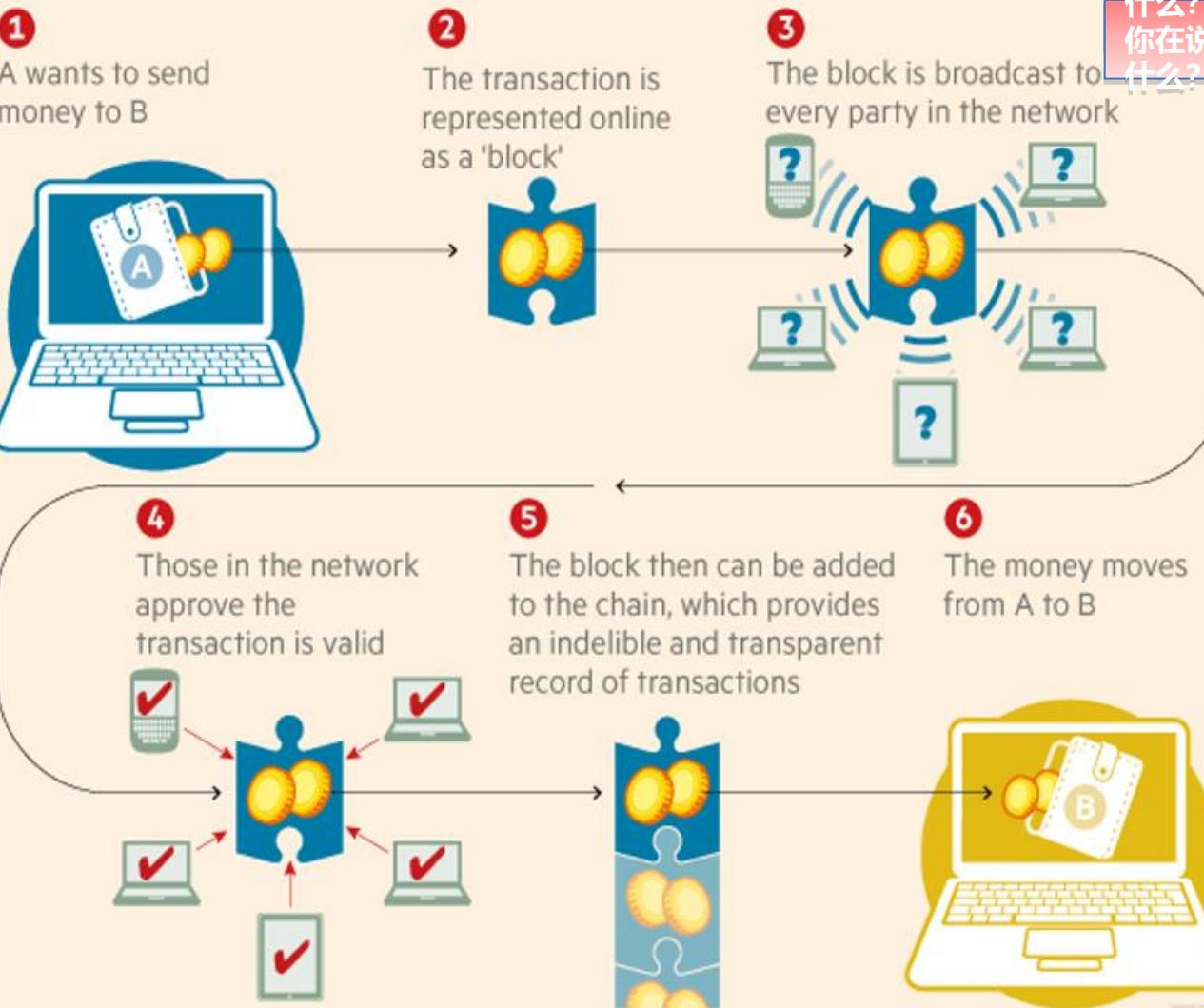
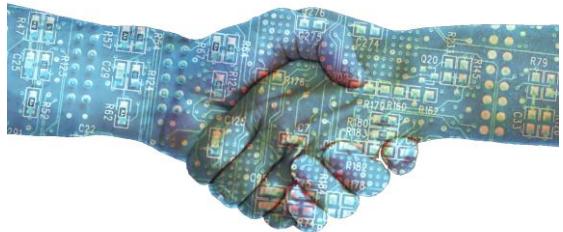
块的链接列表

按时间顺序添加



- 区块链是由一系列区块组成的
- 块具有指向创建链的上一个块的指针

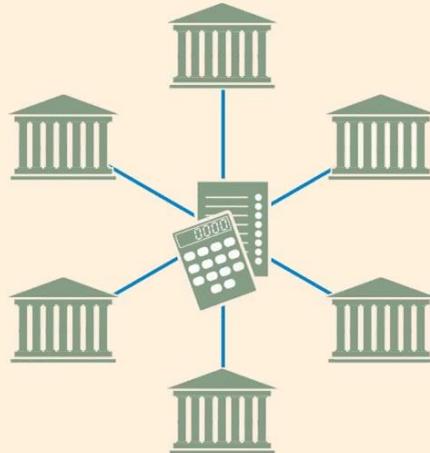
它是如何工作 的



记住-区块链是分散...

Model 1

Current system

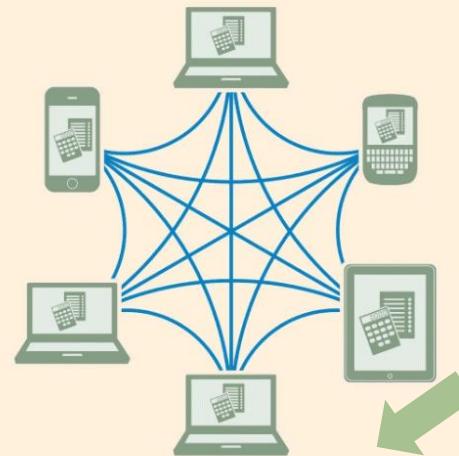


All banks check with central electronic ledger

FT

Model 2

例如比特币
Public blockchain (permissionless)

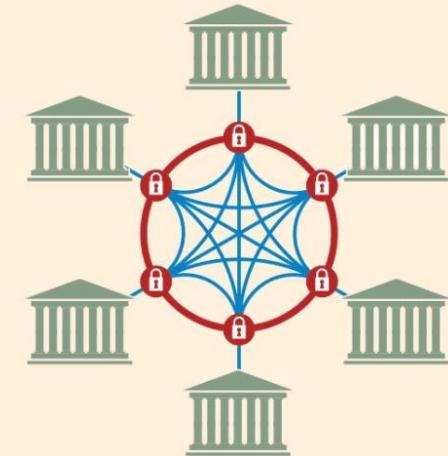


An open network that anybody can access,
like the bitcoin model. The digital ledger of
transactions is shared, transparent and run
by all participants

FT

Model 3

Private blockchain (permissioned)
..适用于企业



The preferred option of most banks. It is a
closed system checking all details and
controlling access via invitation

FT

主要因素影响区块链、加密资产和智能合同的未来

互操作性和标准化

- 消息
- 共识
- Api

可伸缩性

- 卷
- 响应时间

可达性

- ddos 攻击
- 保密

监管

- 加密资产的发行
- 合规性规则
- 监督



ibm 关于区块链的观点 (5/10)



1. 区块链是一种新型的**分布式数据库技术**使企业能够更高效、更安全地在各种业务应用程序中进行交互
2. **区块链不是比特币**;虽然它是流行的比特币,**计算机科学**在过去的二十年里, 封锁链一直在发展
3. 条链必须建立在**打开**. ibm 支持 linux 基金会的超分类帐项目, 因为它专注于平衡的治理方法和开源任人唯贤。这种方法将降低采用风险, 并导致顶级行业公司和监管机构创纪录地采用。
4. 区块链必须做好准备, 以便**企业应用程序**专注于隐私、保密性、可审计性、性能和可扩展性。 ibm obc 结构, 是从头开始构建的, 这些结构被归为捐赠给超账项目的结构
5. 区块链必须是**许可**确保各成员之间更大的信任, 同时实现更优化的共识形式, 避免成员需要挖掘, 这在计算能力和性能方面付出了巨大的代价。因此, ibm 对区块链的看法不包括开采硬币、燃料或任何形式的货币。

ibm 在区块链上的观点 (10 10)



6. 区块链必须是**扩展**使实验能够在共识算法、存储、集成和性能方面实现创新。超级分类帐支持模块化体系结构, 允许第三方创建和插入新价值, 这些价值可以增加或重新放入社区。
7. **基于云的部署**将提供所需的自动化, 使开发人员和运营商采用区块链
8. 区块链的使用案例从大胆的想法想象 (或重新想象) 业务流程到更卑微的使用模式, 更早 (2016年) 采用 (2016年)。ibm 定义**四种使用方式**难度越来越大: 合规分类帐、资产交换、财团分类帐和高价值市场分类帐。
9. ibm 区块链在2016年开展业务。**三个区域**:
 - 社区发展 (大分类账)
 - 云部署, 扩展具有增值功能的超级分类帐
 - 通过区块链车库进行客户参与。
10. ibm 正在吸引**政府和监管机构**教育、展示和鼓励广泛采用用于企业使用的区块链。

区块链是不对于所有用例..。

区块链是

- 不适用于高性能 (毫秒) 事务
- 不适合小型组织或仅适用于一个参与者 (没有业务网络)
- 不适用于低价值、大批量事务
- 不消息传递解决方案
- 不复制的数据库替换
- 不事务处理替换



内容

- ❖ 动机
- ❖ 概念
- ❖ 使用案例
- ❖ ibm 优惠
- ❖ 演示

正在探索的潜在用例正在爆炸



金融服务业

- 付款
- 证券注册和处理
- 贷款



财产

- 房地产
- 知识产权
- 汽车



政府服务

- 投票
- 注册(护照、驾照)
- 许可证



身份识别和安全

- 设备注册
- 认证
- 门禁控制



贸易

- 文件交换
- 资产交换
- 托管服务
- 贸易协定



物联网 (物联网)

- 自治设备, 如
 - 汽车
 - 无人机
 - 机器人

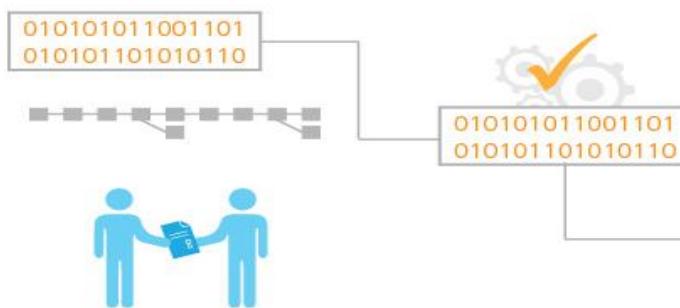
示例但无限制

典型使用案例：智能业务合同

合同隐含的业务规则

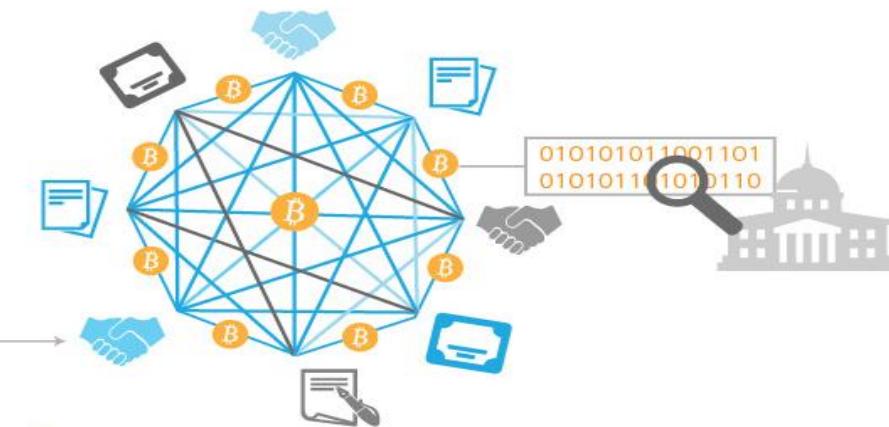
- 嵌入在区块链中，并随交易一起执行
- 可验证，已签名
- 用编程语言编码

- **个人意愿/信任**: 受益人必须履行的条款和条件，才能获得您资产的分配
- **企业债券转让**: 合同定义了发生公司债券转让的条件

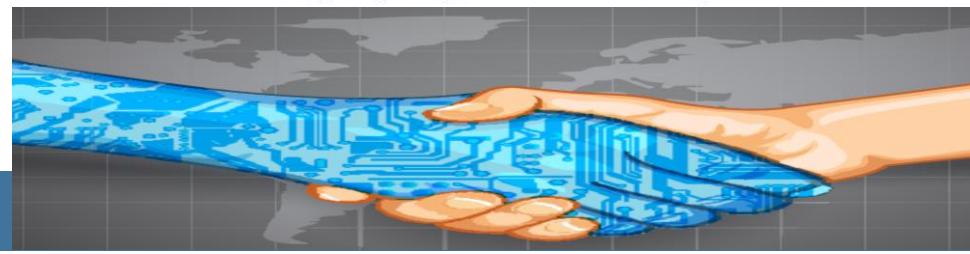


1 An option contract between parties is written as code into the block chain. The individuals involved are anonymous, but the contract is in the public ledger.

2 A triggering event like an expiration date and strike price is hit and the contract executes itself according to the coded terms.



3 Regulators can use the block chain to understand the activity in the market while maintaining the privacy of individual actors' positions.



带有区块链的行业用例

用例-信用证

什么？你在说什么？

银行处理信用证 (l/c) 希望将其提供给包括创业公司在内的更广泛的客户

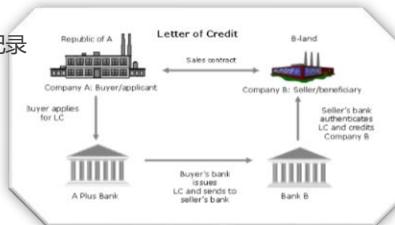
• 目前受到成本和执行时间的限制

如何？

- 区块链提供共同的帐目的分类帐
- 允许银行和交易对手拥有相同的交易和履行记录

好处

- 增加信任
- 提高执行速度 (少于 1 天)
- 极大地降低了成本



用例-公司债务 (或债券)

什么？你在说什么？

持有公司债的银行希望

- 为客户提供验证的交易记录快速向供应商付款
- 允许公司客户看到付款已支付
- 为政府提供对这一过程的监督

如何？

- 区块链提供了记录公司债务/债券的通用分类帐
- 适用于银行、企业客户、供应商和政府

好处

- 加快供应商付款的更大折扣
- 消除风险, 加快决策速度
- 拥有银行可以将成本分散到每个市场



用例-企业对业务合同

什么？你在说什么？

▪ 买方希望以有效的方式将采购订单转换为经过验证的、自动执行的合同，并对其进行更新，以反映供应的状态

▪ 买方、卖方、银行、物流合作伙伴和其他利益攸关方必须能够看到协议

如何？

- 区块链提供合同状态的共享记录，并随着合同的进展而更新
- 提供给协议的所有各方、其银行和合作伙伴

好处

- 提高整个供应链的效率和透明度
- 通过对所有合同进行近乎实时的更新，风险管理得到改善



用例-开放、值得信赖的供应链

什么？你在说什么？

▪ 消费者要求透明地生产他们的产品的地点和方式

▪ 欧盟要求提供更多有关企业供应链的信息，并对不合规行为进行处罚

如何？

- 区块链可实现整个端到端供应链的安全数字资产转移

好处

- 可验证，防止任何一方改变
- 通过提高透明度提高效率
- 消费者可以在知情的情况下购买
- 政府获得可靠的信息



区块链越来越热了..... 与新兴的产业生态系统



"我们内部有已查明20至25个用例这项技术可以应用的地方,"马里亚诺贝林基,桑坦德的头创新事业...区块链技术可以将银行的基础设施成本降低200亿美元每年(128亿英镑)。向波纹提供400万资金



Digital Asset Holdings

数字资产控股,由前摩根大通(j. p. morgan chase & co.)高管布赖特? ,是,就像纳斯达克,开发一个区块链-基于系统的结算证券和资金的转移。



43个潜在的应用区块链从身份到企业在国库的支付,以及供应链融资,正在进行发展。已签署的交易:波正在试验一种电子的、无纸化的提单工艺,使用区块链技术,而基于瑞士链分析,正与巴克莱金融犯罪和安全团队合作,帮助银行与比特币和区块链空间。

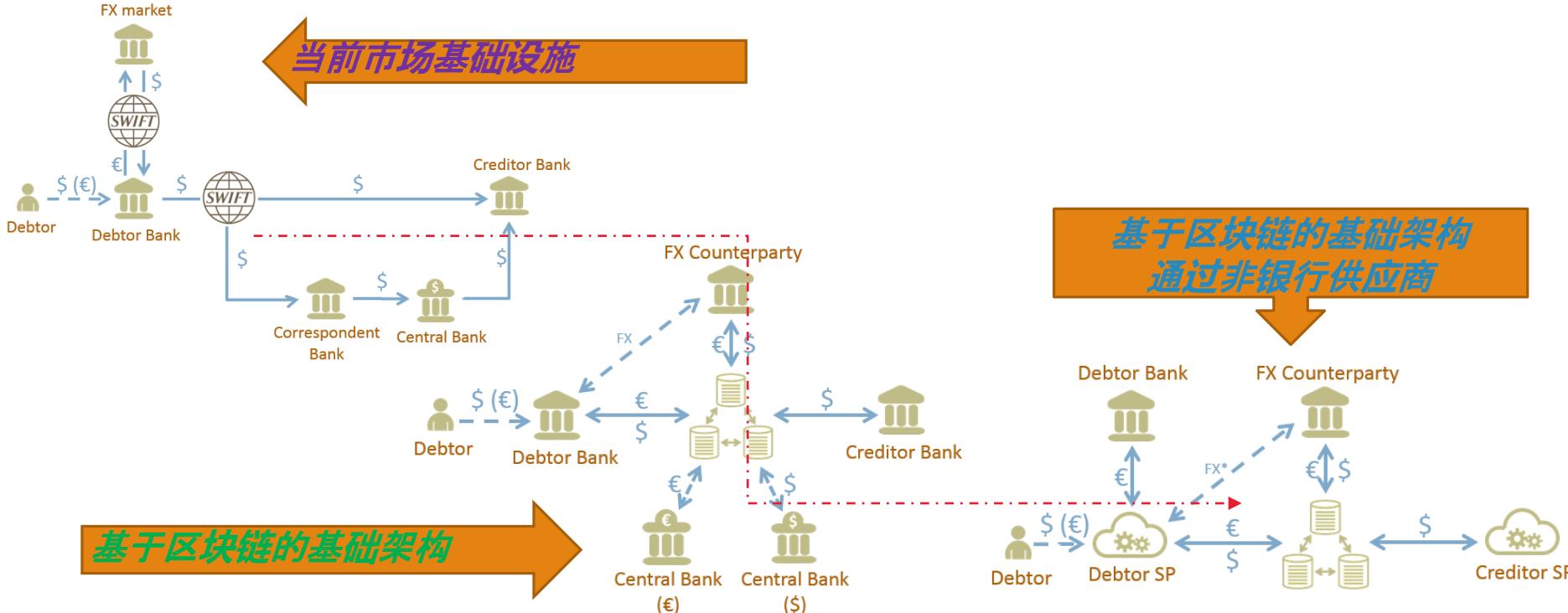


飞利浦医疗公司证实,目前正在探索区块链技术的潜在应用。该公司的兴趣最早是在基于连锁记录的创业公司首席执行官韦恩·沃恩的推特中透露的[铁业](#),他将这项服务吹捧为医疗保健公司的"第一个项目"。

<http://www.coindesk.com/health-care-giant-philips-exploring-blockchain-applications/>



潜在使用案例： 国际付款结算(包括外汇)



金融领域令人激动.....。

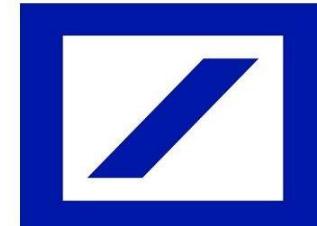
节选自 "区块链上的银行, 重新设计金融架构" 国际金融研究所

usaa(p & c 保险): 拥有和管理约 2,000亿美元资产的 usaa 特别被分布式分类帐技术的可审计性以及如何取代纸张跟踪和耗时的传统审计所吸引。美国国际 aa 公司发展董事总经理亚历克斯·马奎斯



纳斯达克: "区块链技术在让资本市场更高效地运作的同时提供更大的透明度和安全性方面大有希望, 所有这些都是公共利益的根本。 --罗伯特·格雷菲尔德, 首席执行官

德意志银行发现了金融技术的几种可能用途, 包括 "法定货币支付和结算、证券发行、转让、清算和结算、执行衍生合同、资产登记册而不需要中央行政主管部门, 了解您的客户和反洗钱监控, 并提高透明度, 促进差异化的客户和监管报告。



一个全新的生态系统正在出现!

在哪里？在哪里？

BLOCKTECH in FINANCIAL SERVICES VIRTUALscape

by William Mougayar



内容

- ❖ 动机
- ❖ 概念
- ❖ 使用案例
- ❖ ibm 优惠
- ❖ 演示



服务于世界领先的客户

如何?

IBMz 系统和 LinuxOne 为企业推进区块链



中国银行
BANK OF CHINA

Deutsche Bank



WAL-MART®
ALWAYS LOW PRICES. Always.

AstraZeneca



ABB



Improving Home Improvement™



Merrill Lynch



SIEMENS



SUNING 苏宁电器

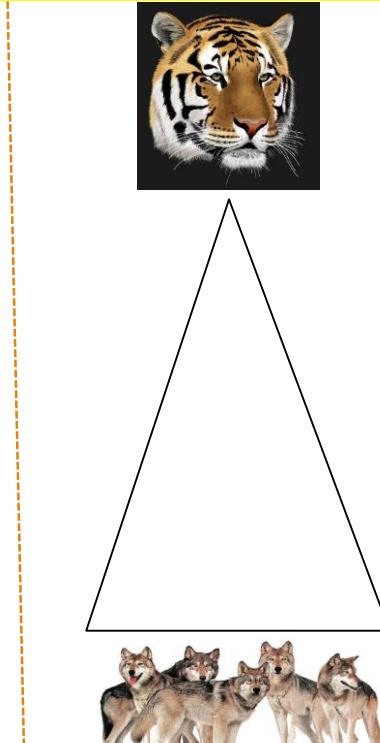
Johnson & Johnson



lenovo



世界触手可及



客户采用模式

如何?

(1) 内部法律

- 内部报告、审计和合规分类账
- 关键业务资产的一致视图
- 来源、不可变和终结比共识更重要
- 与审计员和监管机构的接触

(2) 共享的注册

- 由一小部分参与者创建
- 在他们自己和消费者之间共享参考数据
- 对关键信息进行一致的实时查看

(3) 信息集线器

- 在单个组织中设置的分类帐
- 与会者之间的信息共享 (例如表决、股息通知)
- 资产有信息, 而不是财务价值
- 要求来源、不可变和最终

(4) 高价值市场

- 在市场的许多参与者之间转移高金融价值资产的分类账
- 需要区块链的所有企业功能

ibm 在区块链中的增值

如何
?

帮助指导您的区块链探索



研究



中间件



服务



云



九设计与开发

帮助您设计和构建 poc



部署您的区块链面料的选择



hyperledger



SETL.io



Blockstream



ethereum

ibm 区块链业务堆栈

Runtime Environment

IBM SI and Business Transformation

Developer Environment

Stack Components	Description
Solutions	Solutions to address existing both business issues/needs as well as future opportunities either as SaaS or full managed 'run' service
IBM Blockchain Services	Managed service running and managing IBM platform, VASs, and technical support
IBM or non-IBM Communities	Anchor clients create network to run 1 or more applications for usage by members
IBM Value-Added Assets	Value-Added modules/services on fabric (e.g., Premium Membership, Auditing, Compliance, 'Consensus Plus')
Linux Foundation Fabric: Hyperledger	Pure open source (Linux Foundation) industry standard fabric
IBM Cloud / Power Systems/ System Z / LinuxOne	Physical infrastructure for delivery of platform, ledgers VASs and solutions
	Traditional BP re-engineering and SI to integrate legacy systems with Blockchain capabilities supported by a dedicated core team
IBM Developer Enablement	Environment for development and operations, supporting novice to expert users, to integrate Blockchain to existing systems especially via WebSphere
Linux Foundation Fabric: Hyperledger	Pure open source (Linux Foundation) industry standard fabric
IBM Cloud / Power Systems / System Z / LinuxOne	IBM BlueMix developer platform as point of access

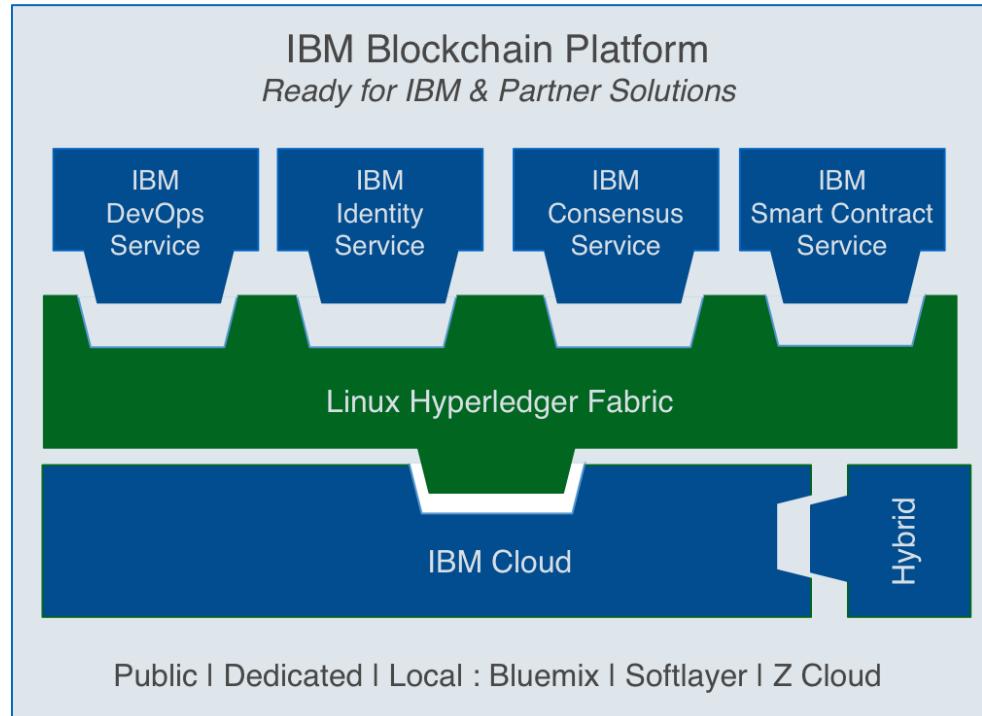
Ibm区块链平台

能力

- 完成devops通过 bluemix 的生命周期
- 智能合同语言和Api标准
- 企业级身份、安全和隐私
- 无缝混合集成与遗留系统
- 市场领先性能和可扩展性

ibm 差异化

- 深度密码学:技能、资产、来自研究的知识产权
- 混合集成:websphere 网关和连接器
- 优化:在 z 上与加密硬件 & 蓝色内核
- 在 ibm 解决方案中体现出行业和领域专业知识
- 未来: 区块链上的分析和认知领导



Ibm 区块链业务战略

社区 + 代码



Linux 基础



HYPERLEDGER PROJECT

开源代码: 从一开始就为企业构建的区块链;
许可 | 隐私
机密 | 审计能

开放协作促进了面向所有人的技术

ibm 捐赠的45k 代码行

云



ibm 区块链云
websphere 区块链连接
ibm 系统上的区块链集线器

bluemix 上的 ibm 区块链

云上的区块链与增值服务;
身份认证共识审计

连接每个 websphere 平台 和 ibm 系统 到一
个区块链

客户



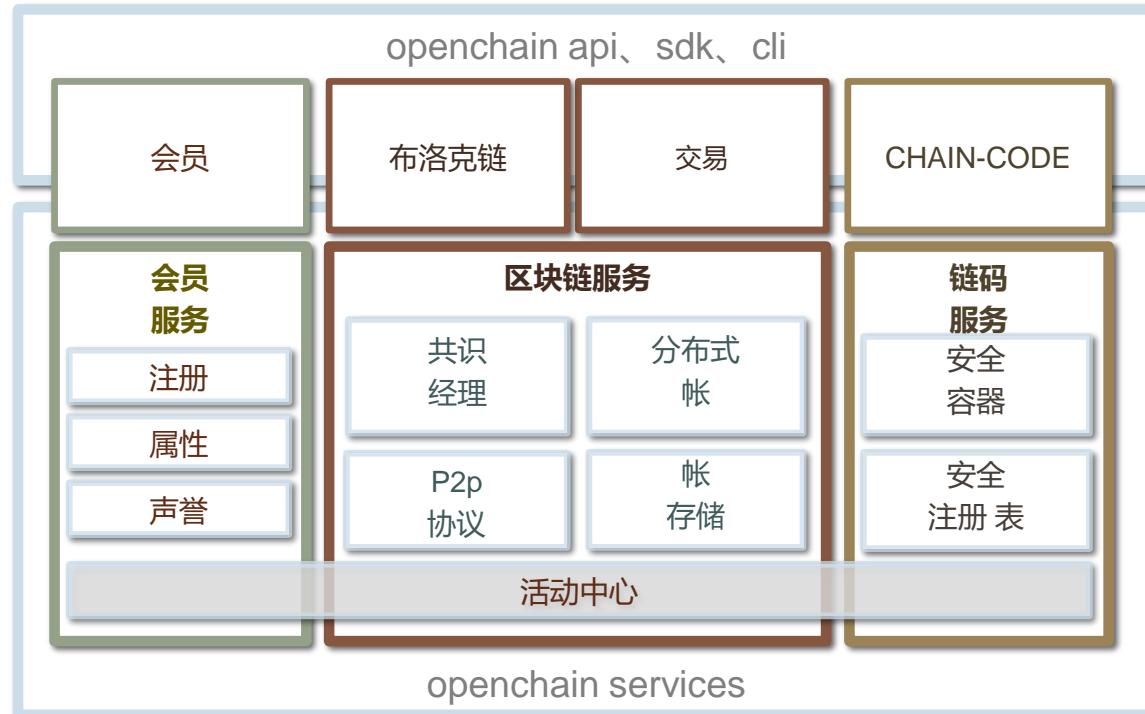
区块链解决方案
区块链车库

区块链解决方案
金融服务;
贸易金融证券结算

区块链车库: 边做边学
伦敦酒店纽约sfo | 新加坡办事处日本

用于区块链的电源
区块链 gbs 实践

ibm 区块链架构和 提供给 linux 基金会的代码



会员

区块链参与者的身份、隐私和可审核性。

布洛克链交易

分布式交易记录分类帐, 通过协商一致方式更新分类帐

CHAIN-CODE

"智能合同", 提供针对区块链运行业务逻辑的能力

api、 sdk、 cli

使开发人员能够以编程方式控制区块链网络

开源代码: 从一开始就为企业构建的区块链;
使用权限隐私保护保密信息可审核

如何
?

ibm 系统上的区块链

集成和连接现有业务流程



z 系统/linuxone

cics/tpfx-db2/vsam

椭圆曲线数字签名

加密加速器

内存中 (10 tb)

散列

应用
程序
1

应用
程序
2

应用
程序
3个

.....

电力系统/电源

db2/oracle/sap企业数据库

加密加速器

内存中 (32 tb)

哈希加速

原料药层

智能合同

加密协议

(身份验证、安全性、不可否认性、受限可见性、隐私/保密性...)

业务规则引擎

(嵌入式业务规则执行引擎)

共享复制的分类帐

共识算法

z 系统区块链资产

区块链代码

- 下载预先构建的 z 系统 docker 映像，并在 z systems 技术上尝试 linux 上的区块链
- 在 linuxone 社区云上快速轻松地设置区块链环境<https://lnkd.in/e4v99vh> 并利用 #docker<https://lnkd.in/eYK4YAH>通过 linux 基金会的超级分类帐项目
- 如果要从源代码中构建 z 系统上的区块链开放分类帐：
<https://github.com/linux-on-ibm-z/docs/wiki/Building-Open-Ledger>

区块链智能合同示例代码 & gui



包括与 cics、db2、ims 和 tpf 的集成



<https://www.youtube.com/watch?v=EqZr4LPQlWk>

客户参与研讨会: z 系统技术上的区块链

- 通过将客户自己的业务知识与 ibm 的区块链知识相结合,使客户能够更好地了解和实现在其业务中应用区块链的好处
- 此次互动将构建一个可交付的解决方案,该解决方案可以部署在客户的业务环境中,证明区块链的好处可以在实践中实现
- 期限和承诺
 - 初步设计思维研讨会 (1天)
 - 敏捷 poc 开发: 通常每次持续3次迭代约2周
 - 客户端和 ibm 都提交了2名全职人员的 poc 持续时间
 - 参与可以计费

z 满足迫切的需求

需要 #1:客户需要能够自我执行的业务逻辑，并保证未经利益攸关方同意，任何一方都不能更改条款 (智能合同 + 共识)

- z systems 具有内置的用于哈希的加速器，可用于对区块链事务进行编码，以便一旦进入分类帐，以前的智能合同就不能被篡改

需要 #2:当事人必须能够将交易的条款和模式保密 (私人交易和集装箱化逻辑)

- z 系统具有用于加密的硬件加速器、数字签名和硬件，允许 z 系统创建无限数量的随机密钥，以唯一地对每个事务进行编码

需要 #3:不同分类帐的客户网络必须能够调用公共逻辑并引用其他分类帐上的交易：例如，只知道一次您的客户 (多分类帐寻址)

- 在 z 系统上，区块链将与作为 z 上当前业务流程存在的公共逻辑并排运行。区块链和当前业务流程将通过微服务和 api 进行最佳集成和引用

区块链和 ibm z 系统的优势

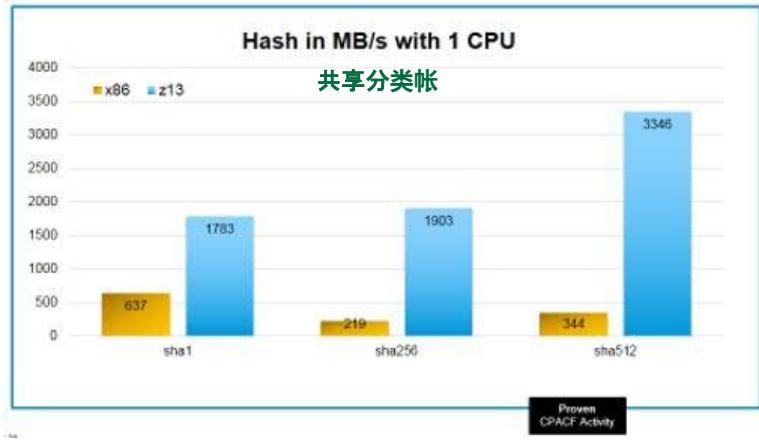
区块链在 z 上

- **佩尔福万克 e**: 高度可扩展的 ito 系统, 非常大的内存空间 10 tb, 工业中最快的商业微处理器, 最大的缓存 (z 运行开源 2x-3x 比基于 intel 的平台快 2x-3x)
- **硬件加速器**: 内置片上加速器, 用于区块链加密 (哈希) 和区块链加密
- **安全**: 用于存储密钥的防篡改安全卡, 用于加密区块链的身份和内容; z 硬件安全模块 (hsm) fips 140-2 兼容, 支持椭圆曲线 suiteb; 企业 PKCS#11 使用 hsm 中唯一的固件负载进行非常安全、完整的实现, 在任何其他平台上都不可用
- **平台**: z 设备基础结构提供虚拟机管理程序安全的容器; 隔离平台 (z 上的 lpar); 内置审计系统, 智能合同可用于控制和记录智能合同交互

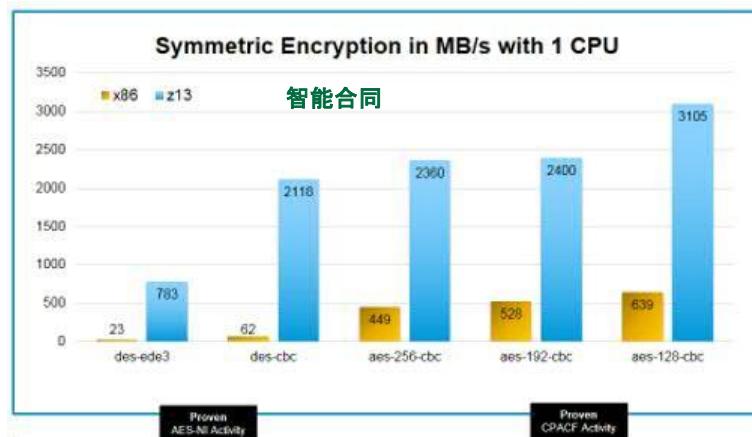
区块链与 z

- **与现有 sor 的更紧密集成**(标准操作记录) 通过 api 与现有的事务子系统 (cics、db2、ims、tpf、批处理 cobol、odm on z) 通过 api 来缓解潜在的瓶颈
- 公司已经具备的现有安全、审计、管理和运营业务实践的最少网络跃点和使用量
- 在 z 上运行的 linux 上运行的区块链允许将其他区块链功能与在 ibm 事务运行时之外实现的智能合同 api 搭配使用

区块链的基础设施比以往任何时候都更加重要:持续的性能



使用linux 在z 系统技术上的改
进高达10倍



使用linux 在z 系统技术上的改
进高达30x



区块链在电源上： 差异化的机会

核心和新数据存储库

- db2、甲骨文、sap
- 企业数据库

云

- 特定行业-由区块链行业用例周围的业务网络定义
- 混合
- 公共(软层和 csp)
- 开发安全的 docker 容器

加速度

- 椭圆加密 (power9)
- 分布式哈希表
- 网络延迟
- 数据层 (rocksdb 加速)

生态

- lsv
- opopower合作伙伴
- 其他合作伙伴



POWER8

区块链和 ibm 电力系统的优勢

区块链在电源上

- **性能和性能:** 高度可扩展的 ito 系统 (4x x86)、高带宽内存子系统 (4x x86)、非常大的内存空间到 32 tb、非常大的高速缓存 (5x x86) 以及高达2.3倍的开源应用程序的价格性能提高到 x86
- **硬件加速器:** capi 附加了用于区块链加密 (哈希)、区块链加密 (开发计划) 和区块链数据存储 (rocksdb–内存中的 nosql 键值存储) 的加速器
- **x86 兼容性:** le linux 和 kvm 简化了 isv 和 ibm sw 应用支持, 并为基于区块链的解决方案和生态系统合作伙伴利用类似的 x86 管理和开发技能
- **灵活消费模式:** 通过 softlayer 和 csp 提供电源 lc 线路和公共云选项, 为 pots/poc 以及业务网络中分布式节点上的 devp 和区块链解决方案提供了灵活性和成本效益高的消费模式
- **安全:** 内置 power8 加密引擎, fips 140-2 兼容, hsm 支持 (硬件安全模块)
- **平台:** 使用 powervm 保护虚拟机; 使用 powerkvm 的隔离容器; 开发安全的 docker 容器, 以创建和部署区块链微服务

区块链与电源

- **与现有 sor 的更紧密集成(标准操作记录)** 通过 api 使用现有的数据和事务子系统 (sap、db2、oracle、企业数据库) 来缓解潜在的瓶颈
- 公司已经具备的现有安全、审计、管理和运营业务实践的最少网络跃点和使用量
- 在 power sor 上运行的 linux 上运行的区块链允许将其他区块链功能与在应用程序运行时之外实现的智能合同 api 进行配置

ibm 区块链参与模型

如何
?



示例议程 为期1天的研讨会

1. 讨论区块链技术 2. 探讨客户业务模式 3. 展示区块链适用性	1. 显示区块链应用程序演示 2. 解释技术使用情况 3. 验证客户利益	1. 了解区块链概念& 元素 2. 手采用区块链技术 3. 使用设计思维进行演示定制	1. 探讨客户特定的业务模式 2. 设计、构建和迭代方法 3. 构建有限范围的可部署解决方案
2小时会议	2小时演示	1天的研讨会	2-6
远程或面对面	远程或面对面	面对面	合用同一地点联合小组
自由的费用	免费的负责	自由的费用	对于充电

- **介绍**(10分钟)
- **技术概述**(50分钟)
- **打破**(15分钟)
- **理解**(90分钟)
- **午餐**(60分钟)
- **探讨**(90分钟)
- **打破**(15分钟)
- **原型**(30分钟)
- **评价**(60分钟)



初始问题

2.1 人的区块链^{世纪商业网络}-这给你带来了哪些机会?

对话开始:

- 前三名是什么? **挑战**在您的组织中, 区块链可以解决?
- 区块链和比特币是独立的技术。ibm 将比特币视为区块链技术的一个潜在用途, 但正在关注其他用例的好处, 如: 供应链管理、物联网、合同、共享分类账等。您的组织对比特币(和其他加密货币)与比特币(和其他加密货币)的看法是什么?**区块链技术?**
- 有您的业务**投资**在区块链行业项目中? (例如 r3, linux 基金会)
- 区块链如何让您的业务网络更大**高效和扩展**它的触角?
- 围绕封锁链及其功能的炒作很多--并不是所有的都很了解情况。您对区块链的进一步信息是什么, 以便能够量化潜在的**为您的业务带来好处?**

咨询/项目工作机会

- 你的计划是什么? **linux 基金会**业务成功的大分类帐项目? 你有**团队**它的任务是探索您的组织的区块链的用例?
- 许多银行和金融科技公司正在尝试区块链--您的组织是否参与其中? 如果没有, 您的**策略**围绕着这一切?
- 2016年将是第一个区块链项目的一年。你的混凝土是什么? **30-60-90天计划?**
- 您的董事会对利用区块链技术有何看法? 什么? 你在干什么**节约成本**你会通过使用这项技术来预测吗?
- 你会成为一个**第一个采用者**谁将从区块链的早期受益, 或**快速的追随者**?

总结

1. 区块链是一种共享的、复制的分类帐技术
2. 区块链可以通过降低成本、提高效率和提高可访问性来打开业务网络
3. 区块链解决了一系列令人兴奋的、主题广泛的业务挑战, 这些挑战贯穿于各个行业
4. linux 基金会开放分类帐项目开发开源、开放标准共享分类帐技术
5. ibm 支持开放标准、开源、开放治理的区块链
6. ibm 拥有一个易于访问、经过验证和增量的参与模式, 为客户提供了立即开始的信心



内容

- ❖ 动机
- ❖ 概念
- ❖ 使用案例
- ❖ ibm 优惠
- ❖ 演示

制作区块链真正 适用于企业

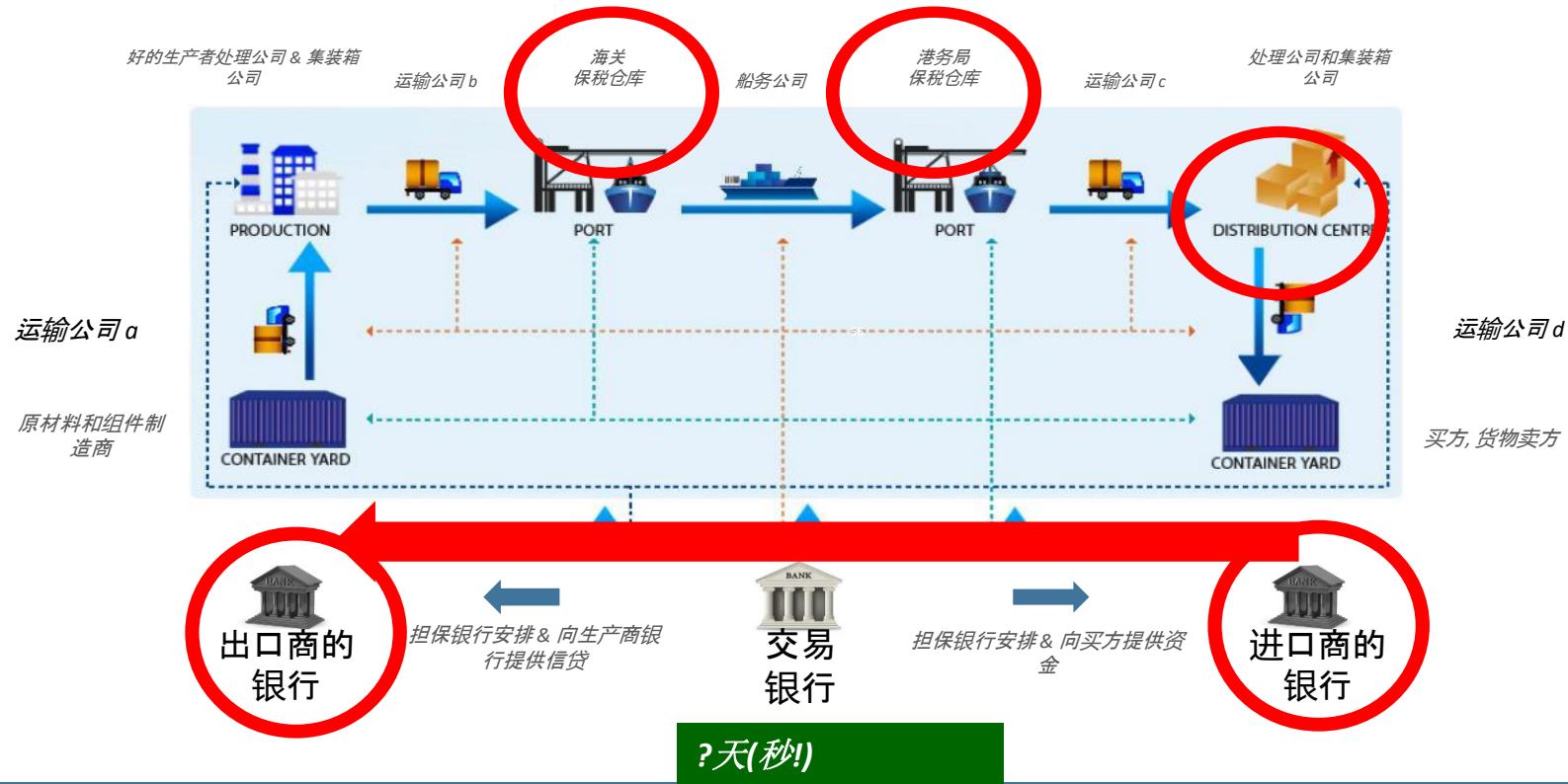
显示演示

<https://www.youtube.com/watch?v=EqZr4LPQIWk>

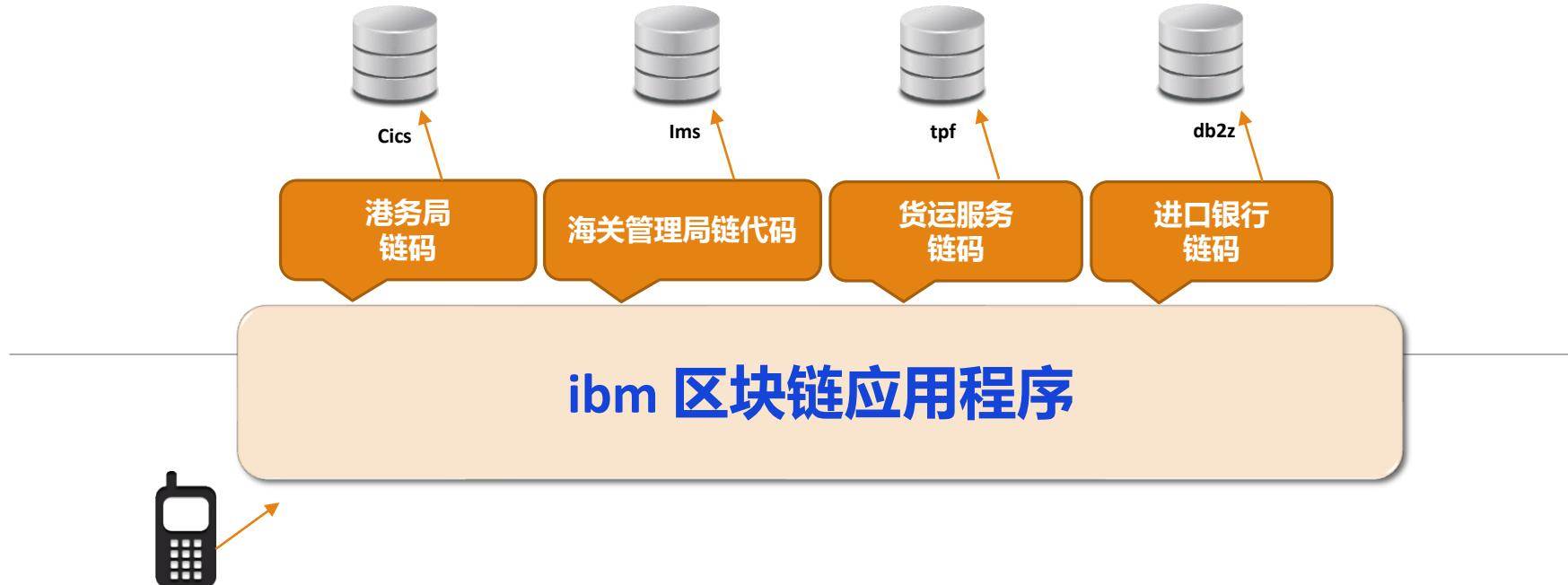
z 系统上的区块链

**贸易金融物流与
与现有业务流程集成**

传统贸易融资:> 10个方, ~ 30份文件, 实际存在, 绝大多数是纸质文件



贸易融资智能合同



Supply Corp's View

Most Visited Bookmarks Toolbar LinuxConDemo Assets | IBM.Next blockchain cognitive

My Contracts: Browse, Edit, and Monitor

Logged in as SupplyCorp ([Sign out](#))

New Contract

[Publish](#)

Product:	<input type="text"/>
Vendor:	<input type="text"/>
Price:	<input type="text"/>
Bank:	<input type="text"/>

Approvals:

Conditions:

Contracts Deployed By Me

[Update All](#)

Contract Name	Contract Type	Signatories	Status	Update
---------------	---------------	-------------	--------	--------

My Bank Accounts

[Update All](#)

Bank Name	Account Balance
ExportBank	2000000

1/4/2019

Number of blocks added to chain: 6

Search [Star](#) [Bookmark](#) [Download](#) [Home](#) [Back](#) [Forward](#) [Redo](#) [Sign out](#)

Logged in as ImportBank ([Sign out](#))

[Update All](#)

Signatories	Status	Update
Trucker	Signed	
PortAuthority	Signed	
CustomsAuthority	Signed	UPDATE

[Update All](#)

Contract Type	Signed By	Register Signature
---------------	-----------	--------------------

[Update All](#)

Contract Type	Signed By	Register Signature
---------------	-----------	--------------------

Number of blocks added to chain: 6

Number of blocks added to chain: 6

基础结构要求和为区块链 poc 提供的可交付结果 /z 支持

- 2个共享 ifl
- 48 gb 内存
- 48 gb 存储空间
- zvm
- debian 7 或8
- 区块链代码
- 示例智能合同/链码
- 要连接到上述6、7的示例 gui

内容

- ✓ 动机
- ✓ 概念
- ✓ 使用案例
- ✓ ibm 优惠
- ✓ 演示



要了解更多信息的资源区块链

有关一般信息:<http://www.ibm.com/blockchain/>

加入社区:

- [ibm 区块链-<http://ibm.biz/InternalBlockchainCommunity>](http://ibm.biz/InternalBlockchainCommunity)

- 区块链上的系统 z gang-<https://ibm.biz/BdHC2P>

访问连接, 用于连接到启用材料。

- <http://ibm.biz/BCEngagement>

演示文稿、视频、实验室

- <https://ibm.box.com/BlockchainBox>

系统 z 上 linux 上的区块链

- <https://ibm.biz/Bd4i4V>

演示中的示例代码, 让您在我们的帮助下创建智能合同

- <https://github.com/linux-on-ibm-z/docs/wiki/Building-Open-Ledger>

是**区块链**将成为下一个大**干扰**因为...。

. 信息技术

我们的经济

我们的社会

我们的生活方式

?

以任尙

多尙謝
繁体中文

努力

谢谢

英語

Спасибо

俄語

ଧନ୍ୟବାଦ

Hindi
印地语

شكراً

阿拉伯语

格拉齐

意大利语

多谢

简体中文

谢谢

西班牙语

ขอบคุณ

泰语

奥布里加
多

西葡萄牙语

丹克

德语

谢谢

法语

ஃண்டி

Tamil

泰米尔语

ありがとうございます

日语

감사합니다

朝鲜语

与区块链相关的术语表



业务网络

业务网络连接

参与者谁是客户、供应商、银行、合作伙伴

跨地理和监管边界

财富是由商品和服务在商业网络中的流动产生的

市场是这一进程的核心

公众: 水果市场, 汽车拍卖
或
私人: 供应链融资、债券



资产

一个资产是任何能够拥有或控制的东西, 以生产价值
资产的两种基本类型

- 有形的, 有形的, 有形的
- 无形的, 如抵押
- 无形资产细分
- 金融, 例如债券
- 知识产权, 例如专利
- 数字, 例如音乐
- 现金 也是一种资产
- 具有匿名性



帐

帐: 企业记录系统

对于他们参与的多个业务网络, 企业将有多个分类帐

交易: 在分类帐上和分类帐上的资产转移

约翰给安东尼一辆车 (简单)

合同: 发生事务的条件

如果安东尼付了约翰的钱, 那么汽车就会从约翰传给安东尼 (简单)

如果汽车无法启动, 资金不会传递给约翰 (由第三方仲裁员决定) (更复杂)

区块链术语表



共享分类帐

包含分类帐的当前世界状态和事务调用的区块链



智能合同

将业务网络事务封装在代码中。事务调用结果的获取和分类帐状态集



共识网络

形成区块链网络的网络数据和处理对等方的集合。负责维护一致复制的分类帐



事件

在区块链上创建重要操作的通知 (例如, 新的块), 以及与智能合同相关的通知。不包括事件分布。



系统管理

提供创建、更改和监控区块链组件的能力



钱包

安全地管理用户的安全凭据



系统集成

负责将区块链与外部系统双向集成。不是区块链的一部分, 但与它一起使用。



会员

管理身份和事务证书, 以及允许访问的其他方面