

# 第1章: 什么是区块链?

学习 Bluemix 和区块链

**Bob Dill**, IBM 杰出工程师, 全球售前技术支持CTO

**David Smits**, 资深认证架构师, IBM 区块链



# 计划: 30 分钟的章节内容以及1到2小时的实践

第一章	什么是区块链? 概念和架构全览
第二章	我们要构建的故事是什么?
第二章第一节	故事的架构
第三章	建立本地Hyperledger Fabric V1 开发环境
第四章	建立和测试网络
第五章	管理员用户体验
第六章	买家支持和用户体验
第七章	卖家支持和用户体验
第八章	提供商支持和用户体验
第九章	发货人支持和用户体验
第十章	金融公司支持和用户体验
第十一章	综合演示
第十二章	事件和自动化演示

# 从零开始学习区块链

- 在线免费教程开始学习区块链和IBM Bluemix
- 从零开始学习认知视频系列:
  - [https://www.youtube.com/playlist?list=PLnJzIOiv6cVTaS8k90R3T9AIS\\_kf5XWmX](https://www.youtube.com/playlist?list=PLnJzIOiv6cVTaS8k90R3T9AIS_kf5XWmX)
- 本教程将基于IBM Bluemix利用下面的技术建立一个区块链解决方案:
  - Hyperledger Composer V0.10 或更高
  - Hyperledger Fabric V1.0 或更高
  - Go, NodeJS, Angular
  - HTML, CSS, Javascript
- 这个教程的代码都放在GitHub:
  - <https://github.com/rddill-IBM/ZeroToBlockchain>
- 关于IBM Bluemix, 获取 id, 建立你的机器运行环境的基本介绍, 请参照从零开始学习认知视频系列。

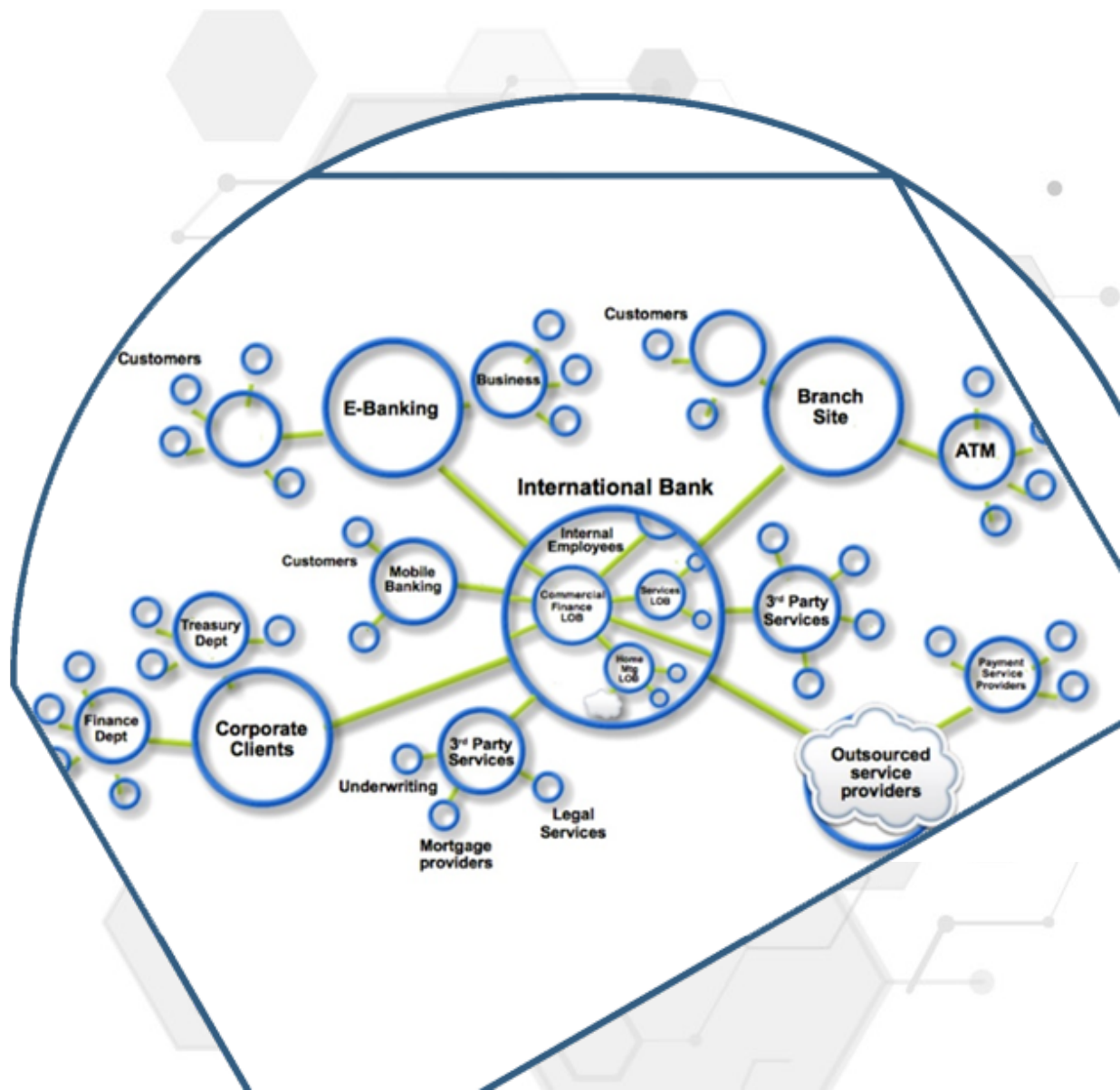
# 区块链介绍



# 什么是区块链

# 商业网络，财富和市场

- 商业网络得益于互联性
  - 参与者包括顾客，供应商，银行，合作伙伴
  - 跨越地理区域和法律监管界限
- 货物和服务以交易和合同的方式在商业网络的流动产生了财富
- 市场是这一过程的核心
  - 公共 (水果市场，汽车拍卖)，或者
  - 私有 (供应链融资，债券)



# 转让资产，构建价值



两种基本的资产类型

- 有形资产, 比如一间房子
- 无形资产, 比如一份按揭贷款



无形资产细分

- 财务型, 比如债券
- 知识型, 比如专利
- 数字型, 比如音乐



现金也是一种资产

- 它具有匿名的属性



# 账簿很关键

**帐簿** 是记录一个业务活 动的系统。商业行为在参与不同的商业网络是有不同的帐本。

**交易** – 一个资产转入或者转出账簿

约翰把车给了安东尼(简单交易)

**合同** – 记载交易发生的条件

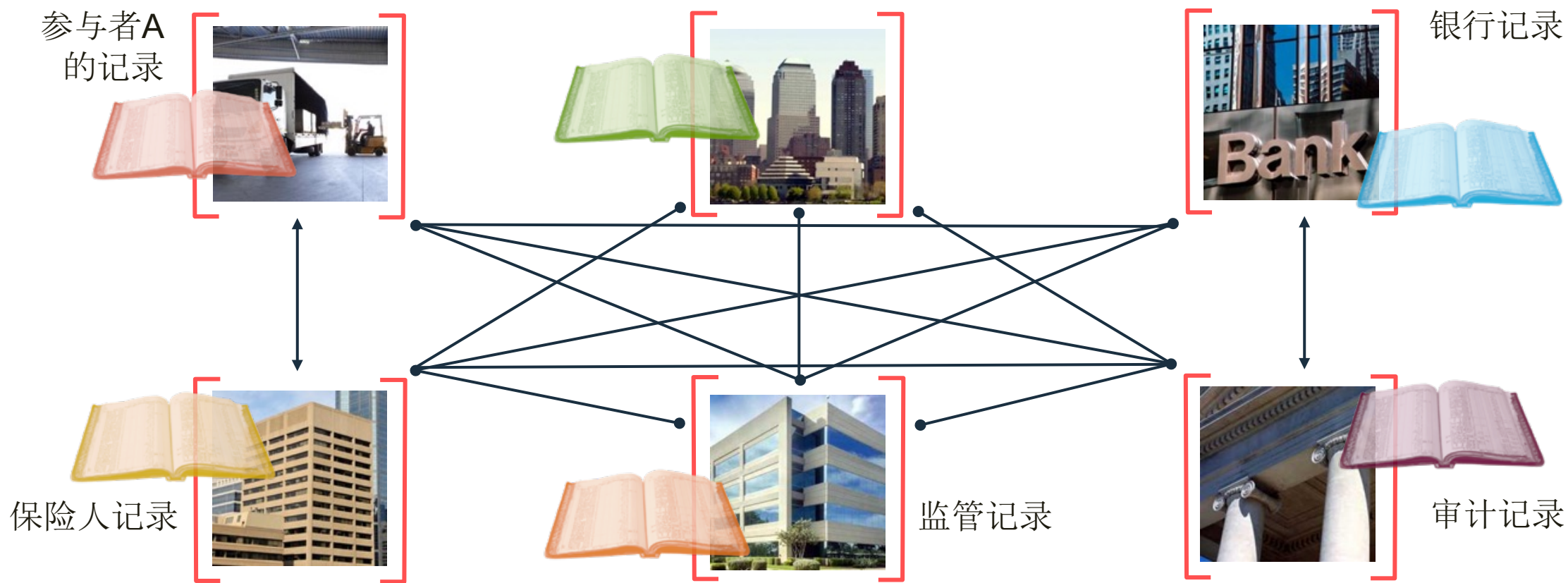
如果安东尼支付约翰金钱, 那么汽车就会从约翰转到安东尼  
(简单交易)

如果汽车不能启动, 钱就不能转给约翰  
(由第三方仲裁决定)  
(复杂一点的交易)





# 问题...

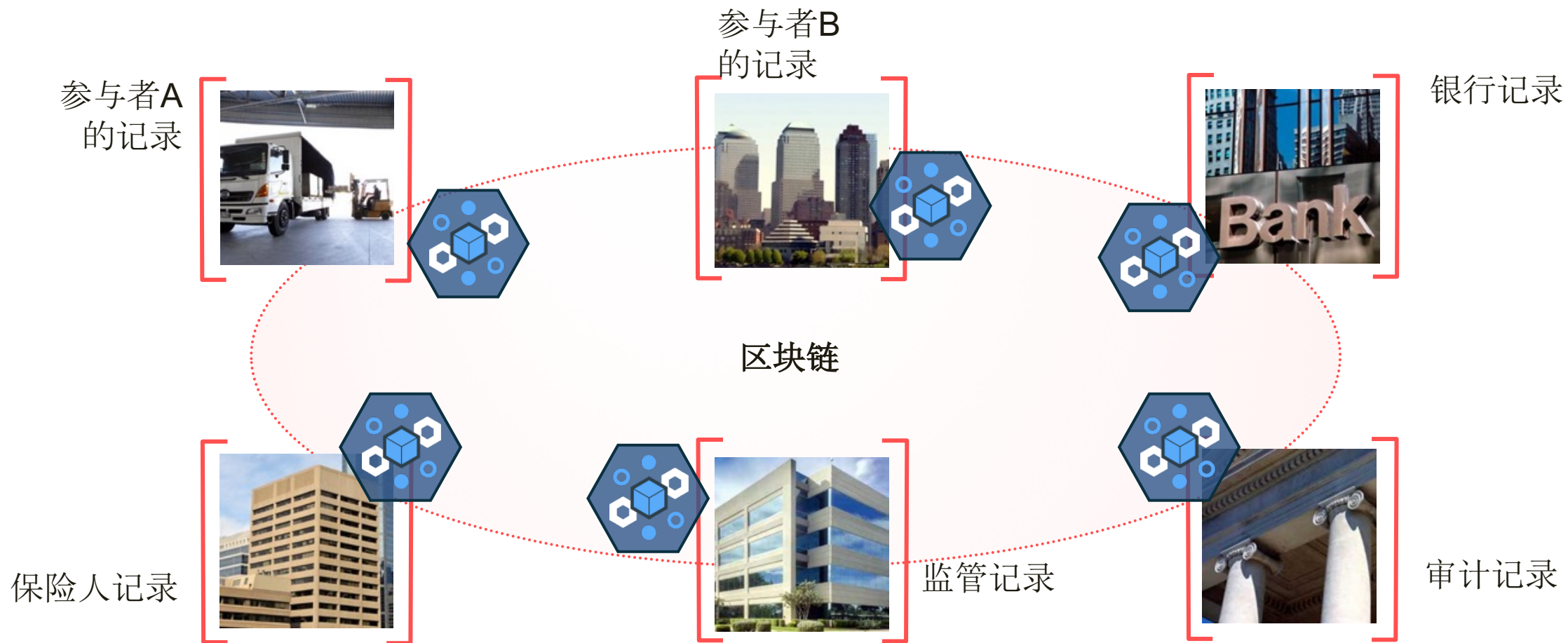


... 低效, 昂贵, 易受攻击

# 引入区块链



# 一个共享复制的、许可的账簿...



... 协商一致, 可回溯, 防篡改, 最终性

# 区块链加固了比特币...



- 一种没有监管的影子货币
  - 首个区块链应用
  - 需要很多资源
- 
- 区块链对于商业而言有以下不同
    - 身份，而非匿名
    - 选择性背书，而非工作量证明
    - 资产，而非加密货币





# 区块链的商业需求

只可追加的分布式记录系统在整个商业网络共享

共享账簿



智慧合同



业务条款嵌入到交易数据库中并和交易一起执行

保证适当的可视性；交易是安全的，认证的和可校验的

私密



信任



交易由相关的参与者背书

# 共享账簿

记录整个商业网络的所有交易

- 在参与者之间共享
- 参与者通过复制拥有自己的拷贝
- 许可的, 参与者只能看到合适的交易
- 共享记录系统



# 智慧合同

业务规则由合同指定 ...业务条款嵌入到区块链中并和交易一起执行

- 可验证的, 已签具
- 用编程语言编码
- 例子
  - 定义合同条件指明债券转让会在哪个公司发生

# 私密

账簿是共享的，但参与者需要私密性

- 参与者需要
  - 在参与者子集之间具备一定的保密性
  - 身份不会链接到一个交易
- 交易需要认证
- 加密是这些流程的核心

# 信任

## 账簿是可信任的信息来源

- 参与者对交易背书
  - 商业网络决定谁会背书交易
  - 已背书的交易会采取合适的保密方式加到账簿中
- 资产有一个可验证的审计跟踪
  - 交易不能被修改、增加和删除
- 信任是通过一致协商, 可回溯, 防篡改, 最终性等方式获得

# 为什么区块链与我们的业务相关？

# 区块链的好处



## 省时

交易时间从天缩减到几乎瞬间



## 降低成本

中介的额外开销和成本



## 减少风险

篡改，欺骗，和网络犯罪



## 增加信任

通过共享流程和保留记录

# 案例: 共享数据

## 问题是什么

- 在一个商业网络中的竞争者/合作者需要共享数据, 比如说银行的汇款路由号码
- 每一个会员保留它自己的代码, 把变动转给一个中央机构来收集和分发
- 一个信息的子集可以由多个机构拥有

## 如何实现

- 在一个区块链网络里, 每一个参与者保留他们自己的代码
- 区块链创建一个全局数据集视图

## 好处

1. 集中、一致的数据集可以减少错误
2. 几乎实时地访问数据
3. 支持代码编辑和参与者之间汇款路由代码的转让



# 案例: 供应链

## 问题是什么

- 在一个复杂的系统中很难追踪每一部件的来源
- 制造商, 生产日期, 批次、甚至生产的机器

## 如何实现

- 区块链可以保存每一个部件的全部来源细节
- 在生产过程的每一个制造商都可以访问这些信息, 比如说飞机的拥有者, 维护者和政府监管人员

## 好处

1. 增强信任, 没有机构“占有”来源
2. 提高系统利用率
3. 召回“具体”的部件而不是整个机队

# 案例：审计和合规

## 问题是什么

- 在一个大型企业中，财务数据分散在许多部门和区域
- 审计和合规需要在审计期间不可篡改的、所有关键交易的记录

## 如何实现

- 区块链从不同的财务系统收集交易记录
- 只追加模式和防篡改的特性可以高质量地追踪财务变动
- 私密性的特点保证授权用户才能访问

## 好处

1. 降低审计和监管合规的成本
2. 给审计员和监管员提供“要找就能找到”式的访问
3. 把合规从被动改成主动

# 案例：信用证

## 问题是什么

- 处理信用证的银行希望把服务提供给更广泛的客户包括初创公司
- 目前受制于成本和执行所要的时间

## 如何实现

- 区块链对信用证提供公共帐簿
- 允许所有合约方拥有相同的、有效的交易和履约记录

## 好处

1. 提升执行速度(小于1天)
2. 大量降低成本
3. 减少风险, 比如汇率波动
4. 增值服务, 比如递增支付

# 未来的行业案例 (选择性)



## 金融

贸易金融  
跨币种支付  
按揭



## 公共事业

资产登记  
国籍管理  
医疗记录  
医药供应链



## 零售

供应链  
顾客忠诚计划  
信息共享 (提供商 - 零售商)



## 保险

保单处理  
风险来源  
资产使用历史  
保单文件管理



## 制造业

供应链  
产品部件  
维护跟踪

# 计划: 30 分钟的章节内容以及1到2小时的实践

第一章	什么是区块链? 概念和架构全览
第二章	介绍我们要构建的故事
第二章第一节	故事的架构
第三章	建立本地Hyperledger Fabric V1 开发环境
第四章	建立和测试网络
第五章	管理员用户体验
第六章	买家支持和用户体验
第七章	卖家支持和用户体验
第八章	提供商支持和用户体验
第九章	发货人支持和用户体验
第十章	金融公司支持和用户体验
第十一章	综合演示
第十二章	事件和自动化演示