区块链技术基础：分布式账本简介

了解这种改变游戏规则的技术和 IBM 对它的贡献

每个人都认为区块链技术（Blockchain）会彻底改变企业的交易方式。让我们来了解一下区块链网络的工作原理，看看是什么让它如此与众不同，以及 IBM 如何帮助改进该技术。我们首先介绍一下相关背景。

账本的作用

在如今的互联一体化世界中，经济活动都是在跨越国家、地理和司法边界的商业网络中进行的。商业网络通常汇聚在生产者、消费者、供应商、合作伙伴、市场创造者/推动者和其他项目干系人云集的市场中，这些项目干系人能够拥有、控制并行使他们在价值对象（也称为**资产**）上的权力、特权和权利。

资产可以是有形的物理资产，比如汽车和住房，也可以是无形的虚拟资产，比如证券和专利。资产的拥有和转移会在商业网络中创造价值，这个过程被称为**交易**（transaction）。

交易通常涉及不同参与方，比如买家、卖家和中介（比如银行、审计员或司法人员），他们的商业协议和合同记录在**账本**（ledger）中。一个企业通常使用多个账本来跟踪资产的所有权，以及在其各种业务中的参与者之间的资产转移。账本是企业的经济活动和利益的记录系统（System of Record，SOR）。

典型的商业账本类似于：

LEDGER

ACCOUNT TYPE	CASH				
TRANSACTION DATE	TRANSACTION DETAIL	REFERENCE	DEBIT	CREDIT	BALANCE
1/1/16	Expenses for Jan	Ref#1	$100.00		$100.00
2/1/16	Tax withheld	Ref#2		$110.00	($10.00)

当前商业账本存在的问题

当前使用的商业账本存在许多不足之处。它们效率低下、成本高、不透明且容易发生欺诈和滥用。这些问题源于集中化的、基于信任的第三方系统，比如金融机构、票据交换所，以及现有制度安排下的其他中介。

这些集中化的、基于信任的账本系统会给交易结算带来瓶颈和障碍。缺乏透明性，而且很容易发生腐败和欺诈，并导致争议。解决争议、逆转交易或提供交易保险的成本很高。这些风险和不确定性导致了错失商机。

此外，每个网络参与者自己系统上的商业账本副本都是不同步的，这会导致因为临时的、错误的数据而制定错误的商业决策。在最好的情况下，能够解决账本不同副本之间差异，但却延误了制定明智决策的时机。

区块链到底是什么？

区块链是一种防篡改的、共享的数字化账本，用于记录公有或私有对等网络中的交易。账本分发给网络中的所有成员节点，在**区块**中永久记录网络中的对等节点之间发生的资产交易的历史记录。

区块链术语和用例

在我们的“区块链术语表”一文中掌握更多的区块链术语和它所有潜在的用法。

所有经过确认和证明的交易都从链的开头一直链接到最新的区块，因此得名**区块链**。区块链可以充当单一事实来源，而且区块链网络中的成员只能查看与他们相关的交易。

区块链网络的工作原理

区块链网络中的成员节点不依赖于第三方（比如金融机构）来仲裁交易，它们使用一致性协议来来协商账本内容，使用密码哈希算法和数字签名来确保交易的完整性。

一致性能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。**密码哈希算法**（比如 SHA256 计算算法）能确保对交易输入的任何改动 — 甚至是最细微的改动 — 都会计算出一个不同的哈希值，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。

去中心化对等区块链网络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。网络中的参与者是平等的，都遵守相同的协议。它们可以是个人、国家代表、企业或所有这三种参与者的组合。

在其核心，该系统会记录交易的时间顺序，而且所有节点都赞同使用选定的一致性模型的交易的有效性。这会使交易不可逆并被网络中的所有成员接受。

区块链技术的商业优势

在传统商业网络中，所有参与者都在维护自己的账本，账本交易之间的重复和差异会导致争议、更长的结算时间，而且因为需要中介，还会导致相关的间接管理成本。但是，通过使用基于区块链的共享账本，交易在通过一致性验证并写入账本后，就不能再更改，这样企业就能节省时间和成本，同时减少风险。区块链技术可以提高自愿参与者之间的透明性、自动化、账本定制化，以及记录的可信度。

区块链一致性机制提供了经过整合的、一致的数据集的优势，减少了错误，拥有近实时的引用数据，而且参与者能够灵活更改其拥有的资产的描述。

因为没有参与成员拥有共享账本中所含信息的来源，所以区块链技术会提高参与成员之间的交易信息流中的可信度和完整性。

区块链技术的不变性机制降低了审计和合规性成本，增加了透明性。而且因为使用区块链技术在商业网络上执行的合同是智能的、自动化的和最终的合同，所以企业会获得更高的执行速度、更低的成本和更少的风险，并能及时结算合同。

如何才算是好的区块链用例？

要确定您的用例是否适合使用区块链，请询问自己以下问题：

1. 是否涉及商业网络?
2. 是否使用一致性来验证交易?
3. 是否需要审计线索或来源?
4. 交易记录是否必须不可变或防篡改?
5. 争议的解决是否会是最终决定?

如果第一个问题和其他问题中的至少一个问题的答案为“是”，那么您的用例就会从区块链技术受益。要成为合适的解决方案，区块链必须涉及一个网络，但该网络可以具有多种形式。该网络可位于企业之间，比如供应链，或者该网络可以在一个企业内。例如：在企业内，可以使用区块链网络在部门之间共享参考数据，或者创建审计或合规性网络。该网络也可存在于个人之间，比如需要在区块链上存储数据、数字资产或合同的人。

Linux Foundation 的 Hyperledger Project 简介

Hyperledger Project 是一个开源的、协作完成的项目，旨在为 B2B 和 B2C 交易创建区块链。IBM 是 Hyperledger Project 的创始成员之一，向如今成为孵化的第一个项目的 Hyperledger Fabric 贡献了 44,000 行区块链代码。

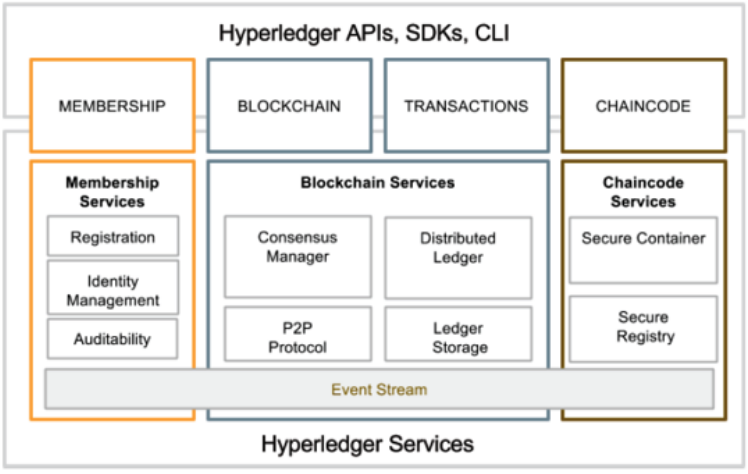
Hyperledger Fabric 旨在创建一种可应用于涉及 B2B 和 B2C 交易的各种不同行业用例的开放标准。这项工作的主要目标是：

- 支持各种各样具有不同要求的行业用例
- 遵守现有的管理制度
- 支持已验证的身份，以及私人的、机密的交易
- 支持许可制、共享的账本
- 支持性能、可伸缩扩展、可审计性、身份识别、安全性和隐私性
- 减少工作证明中涉及的高成本计算

为了提供功能和所需的能力，Hyperledger Fabric 使用了以下概念作为基础：

- 智能合约 (Smart contract)
- 数字资产 (Digital asset)
- 记录系统存储库/存储 (System of record repositories/stores)
- 去中心化一致性网络 (Decentralized consensus-based network)
- 可插拔的一致性算法/模型 (Pluggable consensus algorithms/models)
- 密码安全性 (Cryptographic security)

Hyperledger Fabric 架构支持模块化、即插即用互操作性和容器技术，支持使用任何流行语言编写的智能合约。



可以在 GitHub 上的 Hyperledger Project、Hyperledger 白皮书 和 Hyperledger Fabric 文档 中了解有关的更多信息。

企业区块链需求

我们相信区块链是一种真正颠覆性的技术，能给商业网络带来变革。我们还相信，这一创新需要以开放的方式与其他科技公司及行业协作进行。为实现此目的，IBM 一直在向 Hyperledger Project 贡献代码。

从 IBM 的角度讲，行业级区块链技术具有以下特征：

- **共享的、经过许可的账本** (Shared, Permissioned Ledger) 是仅可附加 (append-only) 的记录系统 (SOR) 和单一事实来源。它对商业网络的所有参与成员均可见。
- **一致性协议** (Consensus Protocol) 是商业网络的所有参与成员都赞同的协议，可确保仅使用经过网络验证的交易来更新账本。
- **加密** (Crytography) 可确保交易的防篡改安全性、身份验证和完整性。
- **智能合约** (Smart Contract) 封装了在网络上发生的交易的参与者协议条款；它们存储在区块链中的有效节点上并通过交易触发。

除了这些属性之外，企业区块链技术还需要支持关键的行业要求，比如性能、经过验证的身份，以及私人的、机密的交易。Hyperledger Fabric 就是为满足这些需求而设计的。它还设计了一种可插拔的一致性协议，允许企业为其网络选择最佳算法。

我该如何开始?

IBM 提供了灵活的平台和安全基础架构来帮助设计、部署和管理区块链网络。了解 IBM Blockchain 解决方案，看看如何 开始在您的交易中使用区块链。

Bluemix 上的 IBM Blockchain

借助 IBM Bluemix 上的免费 Blockchain 服务，您可以创建包含有效节点和安全服务的区块链网络。从这里，您可以部署智能合约 (也称为链码)，查看结果，并构建应用程序。

开始 免费试用 Bluemix 并试用 Bluemix 上的 Blockchain。按照 IBM Blockchain 101：开发人员快速入门指南 中的分步说明，在一个安全的云环境中试验您自己的区块链网络。

来自 Docker Hub 的经过 IBM 签署和测试的镜像

您还可以使用 IBM 签署的 Docker 镜像和 Docker Compose 文件设置和运行区块链网络。这些镜像已经过功能、稳定性和性能测试，可以将它们部署在您选择的任何环境中。IBM 特意为此配置提供了技术支持。

获取 Docker Hub 上的镜像 并 了解更多信息。

其他产品

IBM 为企业部署提供了一个高度安全的环境。网络在安全基础架构上孤立运行，以防止任何后门访问或篡改。

IBM 还提供了 Watson IoT™ Platform，该平台内置了将选中的物联网数据添加到私有区块链的能力。这使得 IoT 设备能将数据发送到私有区块链账本，以便通过防篡改记录的形式包含在共享交易中。

进一步了解 IBM Blockchain 解决方案。

结束语

区块链技术代表着一种全新的交易方式。它们引进了稳健的、智能的下一代应用程序，利用这些应用程序来登记和交换物理、虚拟、有形和无形资产。得益于密码安全性、去中心化一致性和共享公共账本（及其适当控制和许可的可视性）等关键概念，区块链技术能够完全改变我们组织经济、社会、政治和科学活动的方式。

联系IBM

了解更多 IBM Bluemix 云平台信息：https://www.ibm.com/cloud-computing/cn/zh/newplatform/

拨打 IBM Bluemix 云平台免费咨询热线（工作日 9:00-17:00）：400-065-6183

发送电子邮件至：ibmcloud@cn.ibm.com 或填写表单（https://www.ibm.com/marketing/iwm/dre/signup?source=MAIL-cloud&lang=zh_CN&disableCookie=Yes），IBM 业务专家会及时回复。

您还可扫描二维码关注微信公众号“IBM云计算”了解最新资讯