# Hyperledger Fabric关键概念

## 简介Introduction

Hyperldger Fabric是分布式账本解决方案的平台，支持模块化架构，提供高度的机密性（confidentiality）、弹性（resiliency）、灵活性（flexibility）和可扩展性（scalability）。它被设计为支持不同组件的可插拔实现，并适应经济生态系统中存在的复杂性（complexity and intricacies）。

我们建议初次使用者首先阅读下面介绍的其余部分，以便熟悉区块链的工作方式以及hyperledger fabric的特定功能和组件。

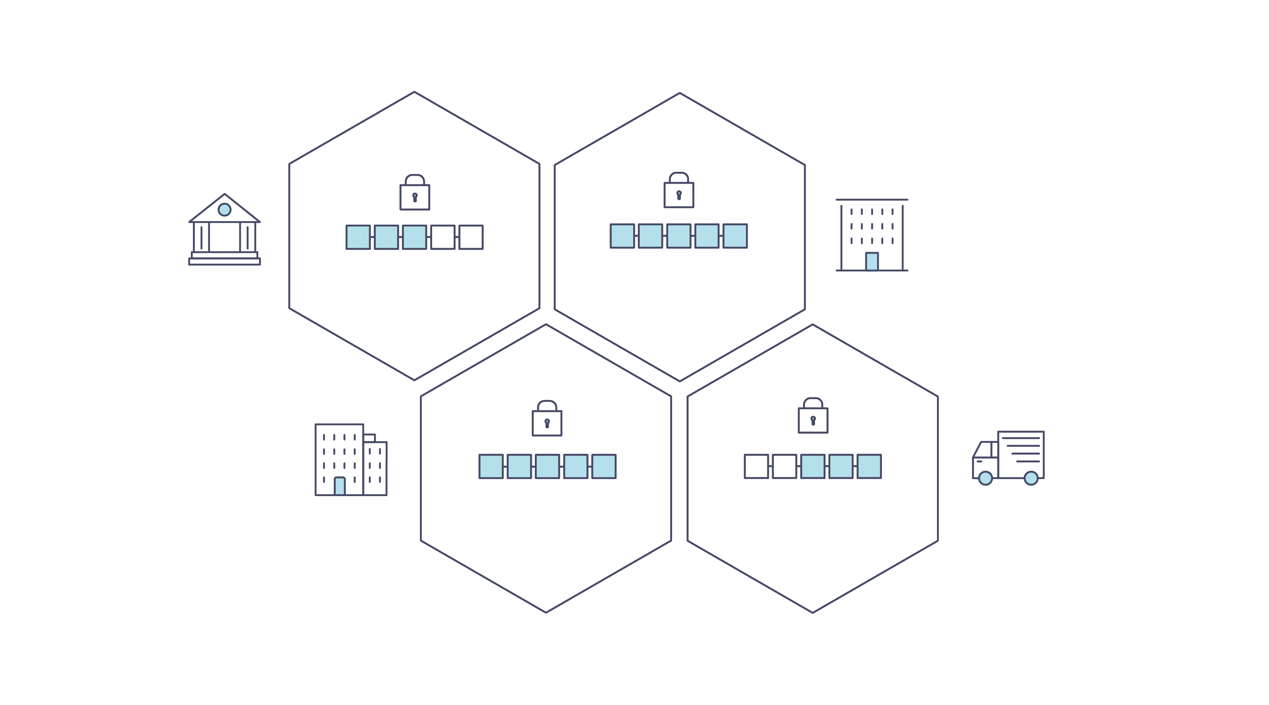
一旦您已经熟悉区块链和hyperledger fabric，可以跳到入门（Getting Started）章节，并从那里探索案例、技术规范和接口等等。

### 什么是区块链？

1. 一个分布式账本

**分布式账本是区块链网络的核心，用于记录网络中发生的所有交易。**

区块链的账本通常被描述为decentralized（去中心化的【去中心化这个翻译现在看来是不太合适的】），因为它被许多网络参与者复制，每个参与者都在协作维护它。我们将会看到，去中心化和合作是反映企业在现实世界中交换产品和服务的强有力的属性。



除了去中心化和合作这些特点之外，记录在区块链中的信息只能追加，使用加密技术可保证一旦交易已添加到账本中，便无法对其进行修改。这种不可篡改的（immutability）特性使得确定信息的来源变得简单，因为参与者可以肯定信息在事后没有改变。这就是区块链被描述为证明体系的原因。

1. 智能合约

为了保证信息的一致性更新和启用一整套账本的功能（转账、查询等），**区块链网络使用智能合约来提供对账本的受控访问。**

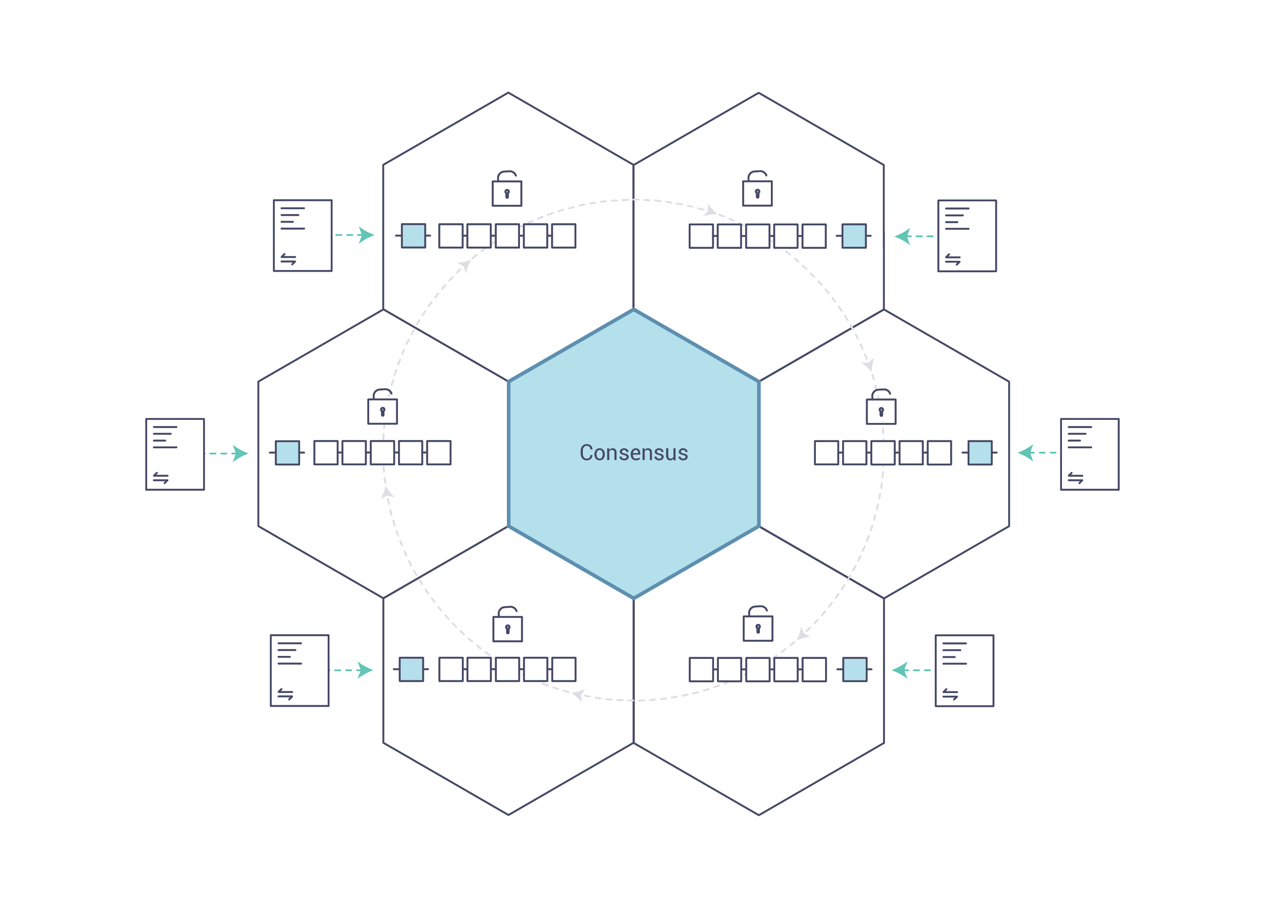


智能合约不仅是封装信息和使信息在整个网络中保持简单的关键机制，还可以通过编写智能合约以允许参与者自动执行交易的某些部分。

例如，可以写一份智能合约，它可以根据物品到达的速度的变化来制定运输费用。根据双方同意并写入账本的条款，当收到物品时，适当的资金会自动划转。

1. 共识

**在整个网络中保持交易同步的过程、确保账本在获得适当参与者批准时才更新、当账本更新时，确保相同的交易以相同的顺序更新，这些机制统称为共识。**



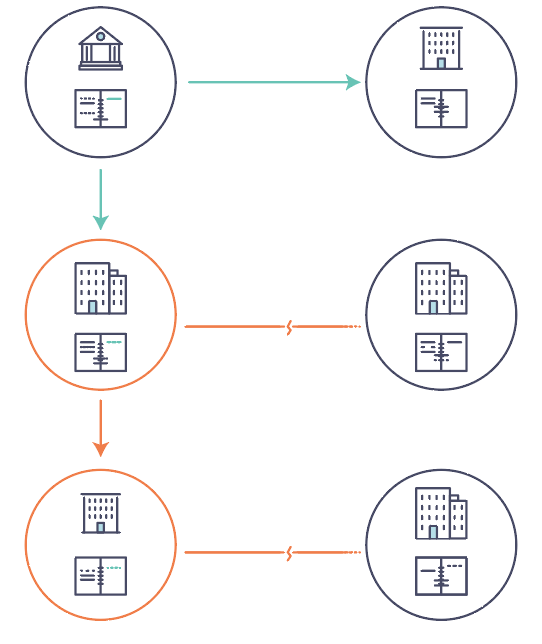
你将在后面学习到更多关于账本、智能合约和共识的知识，当前，**你可以将区块链视为共享的、复制的交易系统就够了，该交易系统通过智能合约进行更新，并通过称为共识的合作过程来保持一致同步。**

## 2、为什么区块链有用？

1. 当今的记录系统（Today’s System of Record）

当今的交易网络只不过是自交易记录被保存以来就存在的网络的稍有更新的版本。一个商业网络的成员彼此进行交易，但他们各自维护着自己独立的记录。而且他们正在交易的物品，无论是16世纪的Flemish毛毯还是如今的证券，每次出售时都必须确立出处，以确保出售商品的商家拥有一系列所有权。

您将接触到一个像下图一样的商业网络：



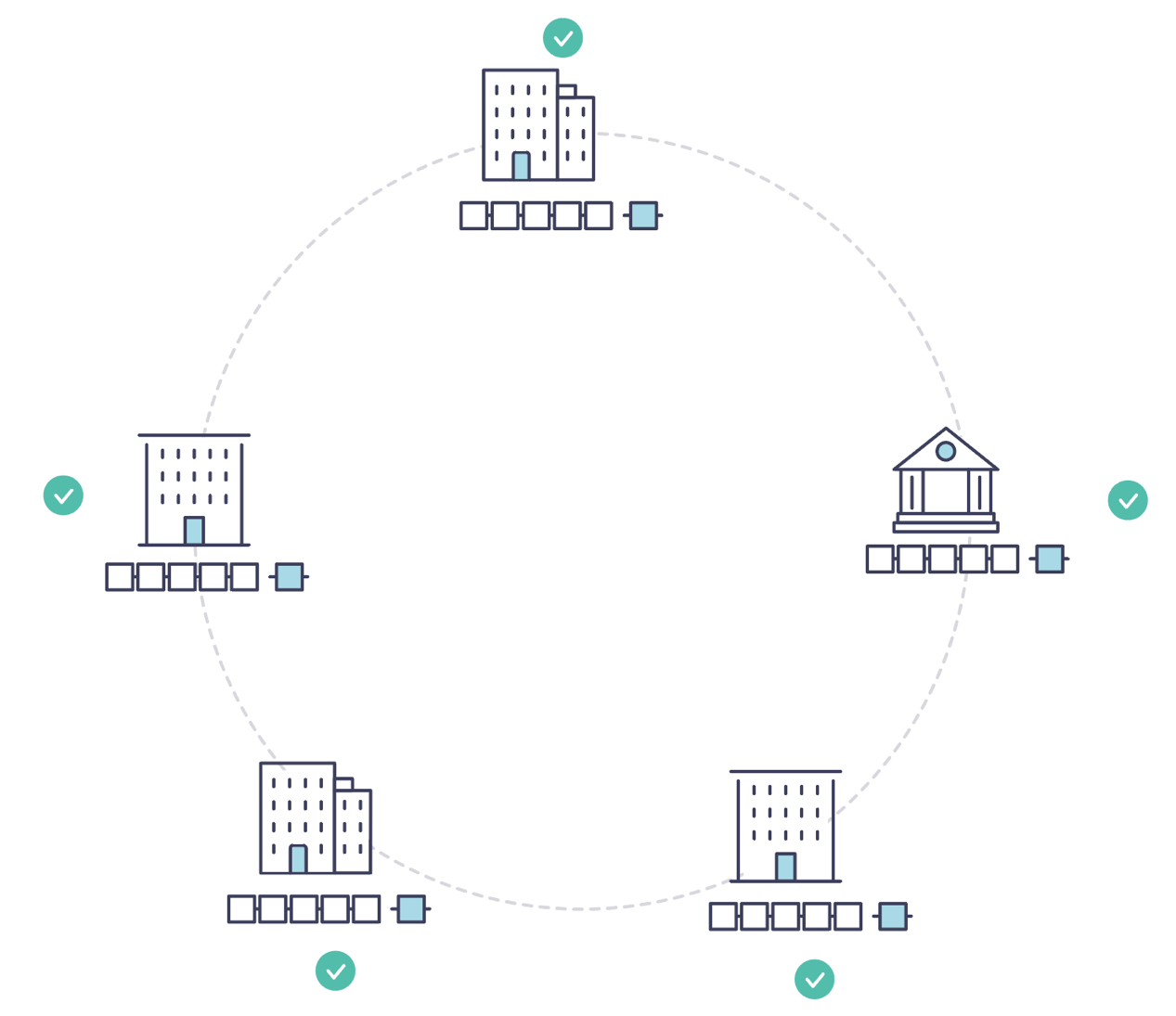
现代技术已经将这些过程从石板和纸质文件夹带到了硬盘和云平台，但是其基本结构是相同的。用于管理网络参与者身份的统一系统不存在，确定起源非常繁琐非常繁琐，需要数天的时间才能理清证券交易（全球的交易额在数万亿美元），合约只能手动签署和执行，并且系统中的每一个数据库都包含唯一的信息，因此存在单点故障。

尽管可见度和信任度的需求是明确的，但使用今天的信息和流程分享方法仍然不可能建立跨越商业网络的记录系统。

1. 区块链系统的不同

如果不是“现代”交易系统代表的低效率，那么商业网络就有了在网络上建立身份、执行交易和存储数据的标准方法吗？如果交易信息交易信息一旦被写入就不可以改变，那么通过查看交易清单来确定资产来源是否可以被信任？

业务系统看起来更像下面这样：



这就是区块链网络，网络中的每个参与者都有自己的账本副本。除了共享账本的信息之外，更新账本的过程也是共享的。与当今的系统不同的是，在参与者的私有程序更新他们的私有账本时，区块链系统是共享程序来更新共享账本。

凭借共享账本协调业务网络的能力，区块链网络可以减少与私人信息和流程相关的时间、成本和风险，同时提高信任度和可视性。

现在你知道了区块链是什么以及它为什么有用。还有很多其他重要的细节，但都涉及到信息和流程共享的基本思想。

## 什么是hyperledger fabric？

Linux基金会在2015年创立了hyperledger项目，以推进跨行业区块链技术。它不是宣布单一的区块链标准，而是鼓励通过社区过程开发区块链技术的协作方法，鼓励开放式开发的知识产权和随着时间的推移采用关键标准。

Hyperledger fabric是hyperledger的区块链项目。和其他区块链技术一样，它含有账本，使用智能合约，并且是参与者管理其交易网络的系统。

Hyperledger fabric从其他区块链网络中解脱出来的地方在于它是私密的（private）和被许可的（permissioned）。Hyperledger fabric网络的成员通过一个可信的成员服务提供商（MSP）来注册身份,而不是允许未知身份参与网络的开放式无权（permissionless）系统（通常这样的系统需要有POW这样的协议来验证交易和保护网络）。

Hyperledger fabric还提供多种可插拔选项。账本数据可以以多种格式存储，共识机制（consensus mechanisms）可以替换，并且支持不同的MSP（Membership Service Provider）。

Hyperledger fabric还提供了创建渠道的能力，允许一组参与者创建单独的交易账本。这对于一些参与者可能是竞争对手并且不希望他们进行的每一笔交易（例如：他们向某些参与者提供的特殊价格）每位参与者都知道的情形尤其关键。如果两个参与者形成一个频道（channel），那么这些参与者（而不是其他人）就拥有该频道的账本副本。

1. 共享账本（shared ledger）

Hyperledger fabric具有由两个组件构成的账本子系统：世界状态（world state）和交易日志（transaction log）。每个参与者都有他们所属的每个hyperledger fabric网络的账本的副本。

世界状态组件描述了在给定时间点账本的状态，它就是账本的数据库。交易日志组件记录导致世界状态当前值变化的所有交易，这是世界状态的更新历史。然后，账本是世界状态数据库和交易日志历史记录的组合。

账本拥有可替换的纾解状态数据库。默认情况下，它是一个levelDB的键值对存储数据库。交易日志不是（does not need to be）可插拔的。它只是简单记录区块链网络使用的账本数据库的前后值。

1. 智能合约（Smart contract）

Hyperldger fabric智能合约以链码（chaincode）的形式编写，并在应用程序需要与账本进行交互时由区块链外部的应用程序调用。在大多数情况下，链码仅与账本的数据库组件（世界状态）交互，而不与交易日志交互。

链码可以使用多种编程语言实现。当前，支持go和Node。

1. 隐私（privacy）

根据网络的需求，B2B网络的参与者可能会对他们共享的信息量非常敏感。对于其他网络而言，隐私不会成为首要问题。

Hyperledger fabric支持把隐私（使用频道）作为关键操作要求的网咯和相对开放的网络。

1. 共识（consensus）

交易必须按照发生的顺序写入账本，尽管他们可能位于网络中的不同参与者之间。要实现这种操作，必须建立交易顺序，并且实施一种方法，用于拒绝错误或恶意插入账本的不良交易。

这是一个经过深入研究的计算机科学领域，有很多方法可以实现它，每个方法都有不同的权衡。例如PBFT（使用拜占庭容错 practical Byzantine Fault Tolerance）可以提供文件副本相互通信的机制，以保持每个副本的一致性，即使发生损坏的情况下也是如此。或者，在比特币中，通过称为挖矿的过程进行排序，计算机竞相解决加密难题来确定所有进程随后建立的顺序。

Hyperledger fabric被设计为允许网络启动者选用最能代表参与者之间存在的关系的共识机制。与隐私一样，还有一系列的需求存在于关系高度结构化的网络到更加对等的网络。

我们将进一步了解hyperledger fabric共识机制，目前包括SOLO和Kafka。