# 区块链简介

## 区块链是什么

一个区块链网络的核心是一个分布式账本，在这个账本中记录了网络中发生的所有交易信息。

## 分布式账本

区块链账本通常被定义为去中心化，这是因为在整个网络中，每个参与者都保存着一个区块链账本的副本，所有参与者通过协作共同维护着账本。信息一旦被写入区块链中就几乎不可被篡改。这也是为什么区块链常常也被称为证明的系统的原因。

## 智能合约

为了持续的进行信息的更新，以及对账本进行管理（写入交易，进行查询等），区块链网络引入了智能合约来实现对账本的访问和控制。

## 共识

保持网络中所有账本交易的同步流程，就是共识。共识保证了账本只会在交易双方都确认后才进行更新。同时在账本更新时，交易双方能够在账本中的相同位置，更新一个相同的交易信息。

# Hyperledger Fabric简介

## Hyperledger Fabric是什么？

Hyperledger Fabric是Hyperledger中的一个区块链项目。与其他区块链技术类似，Hyperledger Fabric包含一个账本，使用智能合约并且是一个通过所有参与者管理交易的系统。

Hyperledger Fabric与其他区块链系统最大的不同体现在私有和许可。与开放无需许可的网络系统允许未知身份的参与者加入网络不同（需要通过工作量证明协议来保证交易有效并维护网络的安全），Hyperledger Fabric通过Membership Service Provider(MSP)来登记所有的成员。

## 共享账本

Hyperledger Fabric包含一个账本子系统，这个子系统包含两个组件：世界状态(world state)和交易记录。在Hyperledger Fabric网络中的每一个参与者都拥有一个账本的副本。

世界状态组件描述了账本在特定时间点的状态，它是账本的数据库。交易记录组件记录了产生世界状态当前值的所有交易，它是世界状态的更新历史。那么，账本则是世界状态数据库和交易历史记录的集合。

## 智能合约

Hyperledger Fabric智能合约被称为chaincode，当一个区块链外部的一个应用程序需要访问账本时，就会调用chaincode。大多数情况下，chaincode只会访问账本的数据库组件和世界状态(world state)（比如查询），但不会查询交易记录。

## 隐私

根据网络的需求，在一个Business-to-Business（B2B）网络中的参与者会对信息共享的程度极为敏感。然而，对于其他的网络，隐私并不是首要考虑的因素。

Hyperledger Fabric支持构建隐私保护严格的网络，也支持构建相对开放的网络。

## 共识

在网络中，不同的参与者写入的交易必须按照产生顺序依次被写入账本中。要实现这一目标，交易顺序必须被正确的建立并且必须包含拒绝错误（或者恶意）插入账本中的无效交易的方法。

Hyperledger Fabric被设计为允许网络构建者依据业务需求来选择采用的共识机制。好比考虑隐私性，就会有一连串的需求，从高度结构化的网络或是更加点对点的网络。

# Hyperledger Fabric 模型

## 身份管理

为了启用许可的网络，Hyperledger Fabric提供了一种成员身份识别服务，用于管理用户ID并对网络上的所有参与者进行身份验证。访问控制列表可用于通过授权特定的网络操作来提供额外的权限层。例如，可以允许特定的用户ID调用链式代码应用程序，但阻止部署新的链式代码。

## 隐私和保密

Hyperledger Fabric使相互竞争的商业利益以及任何需要私密交易的群体能够在同一个许可的网络上共存。专用频道是受限制的消息传递路径，可用于为特定的网络成员子集提供交易隐私和机密性。所有数据，包括交易，会员和频道信息，都是不可见的，任何网络成员都不能访问该频道。

## 高效的处理

Hyperledger Fabric按节点类型分配网络角色。为了向网络提供并发性和并行性，事务执行与事务排序和承诺是分开的。在订购它们之前执行事务可使每个对等节点同时处理多个事务。这种并发执行提高了每个对等体的处理效率并加速了向订购服务交付交易。

除了支持并行处理之外，分工还可以从事务执行和分类帐维护的需求中解除订单节点的负担，同时节点从排序（一致性）工作负载中解放出来。角色分叉也限制了授权和认证所需的处理; 所有对等节点不必信任所有的排序节点，反之亦然，因此一个节点上的进程可以独立于另一节点的验证运行。

## Chaincode功能

Chaincode应用程序对由通道上特定类型的事务调用的逻辑进行编码。例如，为资产所有权变更定义参数的Chaincode可确保所有权所有权交易都遵守相同的规则和要求。系统链码被区分为链码，该链码定义整个通道的操作参数。生命周期和配置系统链接代码定义了通道的规则; 认可和确认系统chaincode定义了批准和验证交易的要求。

## 模块化设计

Hyperledger Fabric实现了模块化架构，为网络设计人员提供了功能选择。例如，用于身份识别，排序（共识）和加密的特定算法可以插入任何Hyperledger Fabric网络。其结果是任何行业或公共领域都可以采用的通用区块链体系结构，并保证其网络能够跨市场，监管和地理边界进行互操作。

# Identity

## 什么是Identity？

区块链网络中的不同参与者包括同行，订购者，客户端应用程序，管理员等等。这些参与者中的每一个都具有封装在X.509数字证书中的身份。这些身份真的很重要，因为它们确定了参与者在区块链网络中拥有的资源的确切权限。Hyperledger Fabric使用参与者身份中的某些属性来确定权限，并为其提供特殊名称 - 主体

最重要的是，身份必须是可验证的（换言之，真实身份），因此它必须来自系统所信任的权威机构。一[成员的服务提供商](https://hyperledger-fabric.readthedocs.io/en/latest/membership/membership.html) （MSP）是Hyperledger面料来实现这一目标的手段。更具体地说，MSP是代表组织成员资格规则的组成部分，因此它定义了管理组织成员有效身份的规则。Fabric中的默认MSP实现使用X.509证书作为身份，采用传统的公钥基础结构（PKI）分层模型。

## 一个解释身份使用的简单场景

想象一下你去超市买些杂货。在结帐时，您会看到一个标志，表示只接受Visa，Mastercard和AMEX卡。如果您尝试使用不同的卡支付 - 我们称之为“ImagineCard” - 卡片是否真实并且您的帐户中有足够的资金并不重要。它不会被接受。

拥有有效的信用卡是不够的 - 它也必须被商店接受！PKI和MSP以相同的方式一起工作 - PKI提供身份列表，MSP说明哪些是参与网络的特定组织的成员。

PKI证书颁发机构和MSP提供了类似的功能组合。PKI就像一个卡片提供者 - 它分配许多不同类型的可验证身份。另一方面，MSP就像商店接受的卡提供商列表 - 确定哪些身份是商店支付网络的可信会员（演员）。MSP将可验证身份转变为区块链网络的成员。

## 什么是PKI？

公钥基础设施（PKI）是一组提供网络安全通信的互联网技术。这是将S置于HTTPS中的PKI - 如果您在Web浏览器上阅读本文档，则可能使用PKI来确保它来自经过验证的源代码。

公钥基础设施（PKI）的要素。PKI由证书颁发机构组成，颁发给各方（例如服务，服务提供商的用户）的数字证书，然后使用这些证书在他们与其环境交换的消息中对自己进行身份验证。CA的证书吊销列表（CRL）构成对不再有效的证书的参考。取消证书可能会有多种原因。例如，证书可能会被撤销，因为与证书关联的密码私人资料已被暴露。

尽管区块链网络不仅仅是一个通信网络，它依赖于PKI标准来确保各个网络参与者之间的安全通信，并确保发布在区块链上的消息得到适当的验证。因此，了解PKI的基本知识以及为什么MSP如此重要是非常重要的。

PKI有四个关键要素：

数字证书

公钥和私钥

证书颁发机构

证书吊销列表

## 数字证书

数字证书是一个文档，其中包含与一方有关的一组属性。最常见的证书类型是符合[X.509标准](https://en.wikipedia.org/wiki/X.509)的证书，它允许在其结构中编码一方的识别细节。

## 身份验证和公钥以及私钥

认证和消息完整性是安全通信的重要概念。身份验证要求交换消息的各方可以确定创建特定消息的身份。完整性要求消息在传输过程中不被修改。例如，你可能想要确保你正在与真正的Mary Morris沟通，而不是模仿者。或者如果玛丽给你发了一条消息，你可能要确保它在传输过程中没有被其他人篡改过。

传统的认证机制依赖数字签名机制，顾名思义，允许一方对其消息进行数字签名。数字签名还保证签名消息的完整性。

从技术上讲，数字签名机制要求每一方都需要拥有两个密码连接的密钥：一个广泛使用的公钥，作为身份验证锚和一个用于生成消息数字签名的私钥 。数字签名消息的收件人可以通过检查附加签名在预期发件人的公共密钥下是否有效来验证收到消息的来源和完整性。

私钥和相应公钥之间的唯一关系是使安全通信成为可能的加密魔术。密钥之间唯一的数学关系是这样的，即私钥可用于在消息上产生只有相应的公钥才能匹配的签名，并且仅在相同的消息上。

在上面的例子中，为了验证她的消息，Mary使用她的私钥在消息上生成一个签名，然后她将该消息附加到消息上。签名可以由任何使用Mary的公钥验证签名消息的人来验证。