Hyperledger Fabric 模型

本节讲述了 Hyperledger Fabric 的关键设计特性，实现了全方位、可定制的企业级区块链解决方案：

- 资产 — 资产是可以通过网络交换的几乎所有具有价值的东西，从食品到古董车、货币期货。
- 链码 — 链码执行与交易排序分离，限制了跨节点类型所需的信任和验证级别，并优化了网络可扩展性和性能。
- 账本特性 — 不可变的共享账本为每个通道编码整个交易历史记录，并包括类似 SQL 的查询功能，以便高效审计和解决争议。
- 隐私 — 通道和私有数据集合实现了隐私且机密的多边交易，这些交易通常是在共同网络上交换资产的竞争企业和受监管行业所要求的。
- 安全和成员服务 — 许可成员资格提供可信的区块链网络，参与者知道所有交易都可以由授权的监管机构和审计员检测和跟踪。
- 共识 — 达成共识的独特方法可实现企业所需的灵活性和可扩展性。

资产

资产的范围可以从有形（房地产和硬件）到无形资产（合同和知识产权）。Hyperledger Fabric 提供使用链码交易来修改资产的功能。

资产在 Hyperledger Fabric 中表示为键值对的集合，状态更改记录为 Channel 账本上的交易。资产可以用二进制或 JSON 格式表示。

链码

链码是定义单项或多项资产的软件，和能修改资产的交易指令；换句话说，它是业务逻辑。链码强制执行读取或更改键值对或其他状态数据库信息的规则。链码函数针对账本的当前状态数据库执行，并通过交易提案启动。链码执行会产生一组用于写入的键值对（写集），可以被提交到网络并应用于所有节点的账本。

账本特性

账本是 Fabirc 中所有状态转换的有序的防篡改的记录。状态转换是参与方提交的链码调用（“交易”）的结果。每个交易都会生成一组资产键值对，这些键值对以创建、更新或删除形式提交到账本。

账本由区块链（“链”）组成，用于以区块的形式存储不可变的顺序记录，以及用于维护当前 Fabirc 状态的状态数据库。每个通道有一个账本。每个节点为其所属的每个通道维护一个账本的副本。

Fabric 账本的一些特点：

- 使用基于键的查找、范围查询和组合键查询来查询和更新账本
- 使用富查询语言进行只读查询（如果使用 CouchDB 作为状态数据库）
- 只读历史记录查询（查询一个键的账本历史记录）用于支持数据溯源场景
- 交易包括链码读取键/值（读集）的版本以及链码写入键/值（写集）的版本

- 交易包含每个背书节点的签名，并被提交给排序服务
- 交易按顺序打包到区块，并被排序服务“分发”到通道上的节点
- 节点根据背书策略验证交易并执行策略
- 在附加一个区块之前，会执行一次版本检查，以确保被读取的资产的状态自链码执行以来未发生更改
- 一旦交易被验证并提交，就具有不变性
- 一个通道的账本包含一个配置区块，用于定义策略、访问控制列表和其他相关信息
- 通道包含 Membership Service Provider 的实例，允许从不同的证书颁发机构（CA）生成加密材料

查看 账本 主题来更深地了解数据库、存储结构和 “查询能力”。

隐私

Hyperledger Fabric 在每个通道上使用不可变的账本，以及可操纵和修改资产当前状态（即更新键值对）的链码。账本存在于通道范围内，它可以在整个网络中共享（假设每个参与者都在同一个公共通道上），也可以被私有化，仅包括一组特定的参与者。

在后一种情况下，这些参与者将创建一个单独的通道，从而隔离他们的交易和账本。为了想在完全透明和隐私之间获得平衡的场景，可以仅在需要访问资产状态以执行读取和写入的节点上安装链码（换句话说，如果未在节点上安装链码，它将无法与账本正确连接）。

当该通道上的组织子集需要对其交易数据保密时，私有数据集合用于将此数据隔离在私有数据库中，在逻辑上与通道账本分开，只有经授权的组织子集才能访问。

因此，通道在更广泛的网络上保持交易的私密性，而集合则在通道上的组织子集之间保持数据的私密性。

为了进一步模糊数据，在将交易发送到排序服务并将区块附加到账本之前，可以使用诸如 AES 之类的通用加密算法对链码内的值进行加密（部分或全部）。一旦加密数据被写入账本，它就只能由拥有用于生成密文的相应密钥的用户解密。

有关如何在区块链网络上实现隐私的更多详细信息，请参阅 私有数据 主题。

安全和成员服务

Hyperledger Fabric 支持一个交易网络，在这个网络中，所有参与者都拥有已知的身份。公钥基础设施用于生成与组织、网络组件以及终端用户或客户端应用程序相关联的加密证书。因此，可以在更广泛的网络和通道级别上操纵和管理数据访问控制。Hyperledger Fabric 的这种“许可”概念，加上通道的存在和功能，有助于解决隐私和机密性要求较高的场景。

请参阅 成员服务提供者 (MSP) 主题，以更好地了解加密实现，以及 Hyperledger Fabric 中使用的签名、验证、身份认证方法。

共识

最近，在分布式账本技术中，共识已成为单个函数内特定算法的同义词。然而，共识不仅包括简单地就交易顺序达成一致，Hyperledger Fabric 通过其在整个交易流程中的基本角色，从提案和背书到排序、

验证和提交，突出了这种区别。简而言之，共识被定义为组成区块的一组交易的正确性的闭环验证。

当区块中交易的顺序和结果满足明确的策略标准检查时，最终会达成共识。这些制衡措施是在交易的生命周期内进行的，包括使用背书策略来规定哪些特定成员必须背书某个交易类别，以及使用系统链码来确保这些策略得到执行和维护。在提交之前，节点将使用这些系统链码来确保存在足够的背书，并且它们来自适当的实体。此外，在将包含交易的任何区块附加到账本之前，将进行版本检查，以确保在此期间，账本的当前状态是能与交易中的信息达成共识的。该最终检查可防止双重花费操作和可能危及数据完整性的其他威胁，并允许针对非静态变量执行功能。

除了众多的背书、验证和版本检查外，交易流的各个方向上还会发生持续的身份验证。访问控制列表是在网络的分层上实现的(排序服务到通道)，并且当一个交易提议通过不同的架构组件时，有效负载会被反复签名、验证和认证。总而言之，共识并不仅仅局限于一批交易的商定顺序；相反，它的首要特征是交易从提案到提交的过程中不断进行核查而附带实现的。

查看 交易流程 以获得共识的直观表示。