链滴

超级账本之关键概念 _ 模型

作者：guichun68
原文链接：https://ld246.com/article/1554451950467
来源网站：链滴

<h2 id="资产-Assets-">资产(Assets)</h2>
资产可以是有形资产（不动产和硬件），也可以是无形资产（合同和知识产权）。Hyperledger abric 提供了使用链代码事务修改资产的功能。
资产在 Hyperledger Fabric 中表示为键-值对的集合，状态变化记录为通道帐本上的交易。资产以用二进制和/或 JSON 形式表示。
<h2 id="链代码-Chaincode-">链代码(Chaincode)</h2>
链代码是定义资产的软件，以及修改资产的交易指令；换句话说，这是业务逻辑。链代码读取或改键值对或其他状态数据库信息时强制执行规则。链代码函数根据帐本的当前状态数据库执行，并通交易提议开始。链代码的执行会导致一组键值写操作（写集）提交给网络并应用到所有对等点上的帐。
<h2 id="账本特征-Ledger-Features-">账本特征(Ledger Features)</h2>
帐本是有顺序的，防篡改的在 Fabric 中所有状态转变的记录。状态转变是参与方提交的链代码用(“交易”)的结果。每个交易都会生成一组资产键-值对，它们作为创建、更新或删除提交到帐本。
帐本由一个区块链(“链”)组成，区块链用于在块中存储不可变的、有顺序的记录，以及用于维当前 Fabric 状态的状态数据库。每个通道有一个账本。每个通道的成员对等节点都维护一份帐本副。
Fabric 账本的一些特征：

使用基于键的查找、范围查询和组合键查询来查询和更新分类帐
使用富查询语言的只读查询（如果使用 CouchDB 作为状态数据库）
只读历史查询——查询一个键的账本历史记录，支持数据溯源
交易由在链代码(读集)中读取的键/值和在链代码(写集)中写入的键/值的版本组成
交易包含每个背书节点的签名，并提交排序服务
事务被排序进区块，并从排序服务“交付”到通道上的所有对等节点
对等节点根据背书策略验证交易并执行策略
在添加到区块之前，要执行版本检查，以确保被读取的资产状态自链代码执行以来没有改变
一旦交易被验证并提交，就存在不可变性
通道的帐本包含一个配置区块，定义策略、访问控制列表和其他相关信息
通道包含会员服务提供者（MSP）实例，允许从不同的证书颁发机构派生出加密材料

<h2 id="隐私-Privacy-">隐私（Privacy）</h2>
Hyperledger Fabric 使用了基于每个通道的不可变帐本，以及可以操作和修改资产当前状态(即新键值对)的链代码。一个帐本存在于一个通道的范围内——它可以在整个网络中共享（假设每个参者都在一个公共通道上操作）——它也可以私有化，只包含特定的一组参与者。
在后面的场景中，这些参与者将创建一个单独的通道，从而隔离/分离他们的交易和帐本。为了决桥接全透明和隐私之间分歧这样的场景，链代码可以只安装于需要访问资产状态执行读写的节点（句话说,如果一个链代码没安装在这个节点，则它将无法与帐本正确对接）。
当该通道上的组织子集需要对其交易数据保密时，使用私有数据集合将该数据分离到私有数据库，逻辑上与通道帐本分离，仅授权的组织子集才可访问。
因此，通道使更广泛的网络中的交易保持私有，而集合则使通道上的组织子集之间的数据保持私。
为了进一步混淆数据，可以使用通用的加密算法（如 AES）对链代码中的值进行加密（部分或全），然后将交易发送到排序服务，并向帐本添加区块。一旦加密数据被写入到帐本，它只能由拥有相密钥的用户解密，该密钥用于生成密码文本。
<h2 id="安全和成员服务-Security---Membership-Services-">安全和成员服务(Security & Mmbership Services)</h2>
Hyperledger Fabric 支持一个所有参与者都知道身份的交易网络。公钥基础设施用于生成与组、网络组件和最终用户或客户端应用程序相关联的加密证书。因此，数据访问控制可以在更广泛的网和通道级别上进行操作和管理。Hyperledger Fabric 这种“要许可”的概念，加上通道的存在和能，有助于解决最关心隐私和保密的场景。
<h2 id="共识-Consensus-">共识(Consensus)</h2>
在分布式账本技术中，共识最近已经成为在单一功能中的特定算法的同义词。然而，共识不仅仅括对交易顺序达成一致，在 Hyperledger Fabric 中这种区别通过其在整个交易流程中的根本性角色

突显，从提议和背书、到排序、验证和承诺。简而言之，共识被定义为包含一组交易组成的区块正确验证的完整循环。
当一个区块交易的顺序和结果满足明确的策略标准检查时，最终达成共识。这些检查和平衡发生交易的整个生命周期中，包括使用背书策略来规定哪些特定成员必须对某类交易背书，以及用系统链码来确保这些策略得到执行和支持。在承诺之前，对等节点将使用这些系统链代码来确保有足够的背，并且它们是来自适当的实体。此外，在将包含交易的区块添加到帐本前，在帐本的当前状态达成意一致或同意的整个期间将进行版本检查。这个最终检查为防止重复操作和其他可能危及数据完整性的胁提供了保护，并允许对非静态变量执行功能。
除了进行大量的背书、有效性和版本控制检查之外，在交易流程的各个方向上也进行身份验证。问控制列表是在网络分层结构（从排序服务到通道)上实现的，当交易提议通过不同的体系结构组件时有效负载会反复签名、核实和验证。综上所述，共识不仅限于商定一批交易的排序；相反，它的首要性是交易从提议到承诺的过程中正在进行验证而获得的副产品。