

华中科技大学

信息存储技术

课程报告

区块链存储技术--Hyperledger Fabric

院 系 计算机科学与技术 .

专业班级 CS1601 .

姓 名 刘本嵩 .

学 号 U201614531 .

指导教师 胡燏翀 .

2019 年 12 月 13 日

区块链技术介绍

区块链

区块链是借由密码学串接并保护内容的串连文字记录（又称区块）。

每一个区块包含了前一个区块的加密散列、相应时间戳记以及交易数据（通常用默克尔树(Merkle tree)算法计算的散列值表示），这样的设计使得区块内容具有难以篡改的特性。用区块链技术所串接的分布式账本能让两方有效纪录交易，且可永久查验此交易。

当前区块链技术最大的应用是数字货币，例如比特币的发明。因为支付的本质是“将账户 A 中减少的金额增加到账户 B 中”。如果人们有一本公共账簿，记录了所有的账户至今为止的所有交易，那么对于任何一个账户，人们都可以计算出它当前拥有的金额数量。而区块链恰恰是用于实现这个目的公共账簿，其保存了全部交易记录。在比特币体系中，比特币地址相当于账户，比特币数量相当于金额。

区块链技术起源

区块链巧妙利用了现代密码学的数字签名、哈希等已成形的理论，来保证数据的完整性和真实性。

本质上说，区块链是一个分布式数据库，不但数据的存储是分布式的（以共享账本为例，所有的数据可以对等地存储在所有参与数据记录的节点中，而非集中存储于中心化的机构节点中），而且数据的产生也是分布式的（账本所有的节点集体维护，而非一个单独的中心机构来维护）

以比特币的区块链账本为例。每个区块基本由上一个区块的散列值，若干条交易，一个调节数等元素构成，矿工通过工作量证明实现对交易整理为账本区块和区块安全性的维持。一个矿工通过交易广播渠道收集交易项目并打包，协议约定了区块速度生成速度而产生的难度目标值，通过不断将调节数和打包的交易数据进行散列运算而算出对应散列值使其满足当时相应的难度目标值，最先计算出调节数的矿工可以将之前获得上一个区块的散列值、交易数据、当前算出对应区块的调节数集成为一个账本区块并广播到账本发布渠道，其他矿工则可以知道新区块已生成并知道该区块的散列值(作为下一个区块的“上一个区块的散列值”)，从而放弃当前待处理的区块数据生成并投入到新一轮的区块生成。

对于其他基于区块链的应用，主要是针对所负载的数据，区块安全性的维持方式等进行调整。

区块链应用的大致分类

	公有链	联盟链	私有链
参与者	任何人自由进出	联盟成员	链的所有者
共识机制	pow/pos	分布式一致性算法	solo/pbft 等
记账人	所有参与者	联盟成员协商确定	链的所有者
激励机制	需要	可选	无
中心化程度	去中心化	弱中心化	强中心化
如初特点	信用的自创建	效率和成本优化	安全性高、效率高
承载能力	<100 笔/秒	<10 万笔/秒	视配置决定
典型场景	加密货币	供应链金融、银行、物流、电商	大型组织、机构
代表项目	比特币 、 以太坊	R3、Hyperledger	

Hyperledger Fabric

Hyperledger Fabric 是一个开放源代码的企业级许可分布式分类帐技术（DLT）平台，设计用于企业环境，与其他流行的分布式记账或区块链平台相比，它提供的功能有很大不同。

一个关键点是 Hyperledger 是在 Linux 基金会下建立的，它本身有着悠久而非常成功的历史，它在开放式治理下培育开源项目，这些项目发展了强大的可持续社区和繁荣的生态系统。Hyperledger 由多元化的技术指导委员会管理，Hyperledger Fabric 项目由来自多个组织的多元化维护人员管理。自最早成立以来，它的开发社区已发展到超过 35 个组织和近 200 个开发人员。

Fabric 具有高度模块化和可配置的体系结构，可针对银行，金融，保险，医疗保健，人力资源，供应链甚至数字音乐交付等广泛的行业用例进行创新，多功能和优化。

Fabric 是第一个分布式账本平台，支持以通用编程语言（例如 Java，Go 和 Node.js）而非 DSL 编写的智能合约。这意味着大多数企业已经具有开发智能合约所需的技能，并且不需要其他培训来学习新的语言或 DSL。

Fabric 平台也是 permissioned，也就是说，与公共网络不同，参与者是彼此信任的，而不是匿名的。这意味着，尽管参与者之间可能不会完全信任对方（例如，他们可能是同一行业的竞争者），但网络可以在治理模型下运行，该治理模型是基于参与者之间确实存在的信任而建立的，例如法律协议或其他现实中的合约。

Fabric 可以利用不需要本机加密货币的共识协议来激发昂贵的挖掘或推动智能合约的执行。避免使用加密货币会降低一些重大的风险/攻击向量，并且无

需进行加密挖掘操作就意味着可以以与任何其他分布式系统大致相同的运营成本来部署该平台。

模块化

Hyperledger Fabric 专门设计为具有模块化体系结构。无论是 pluggable 的 consensus，认证协议（例如 LDAP 或 OpenID Connect），密钥管理协议还是密码库，都可以被模块化的配置，以便满足企业用例需求的多样性。

总体上看，Fabric 由以下模块化组件组成：

- 订购服务在交易顺序上达成共识，然后将区块广播给同级。
- 会员服务提供商(负责将网络中的实体与身份相关联)。
- 对等 gossip 服务(通过向其他对等点订阅服务)。
- 智能合约(chaincode)可在容器环境（例如 Docker）中运行以进行隔离。它们可以用标准编程语言编写，但不能直接访问分类帐状态。
- 账本的存储支持各种 DBMS。
- 认证策略，可以针对每个应用程序进行独立配置。

业界普遍认为，不存在“one blockchain to rule them all”，模块化的 Hyperledger Fabric 才能满足多种行业用例的不同解决方案要求。

Permissioned 和 Permissionless 的区块链

在 Permissionless 区块链中，几乎任何人都可以参与，每个参与者都是匿名的。在这种情况下，除了一定深度之前的区块链状态是不可变的之外，别无其他信任。为了减轻这种信任的缺乏，Permissionless 区块链通常采用本机开采的加密货币或交易费来提供经济激励，以抵消基于 Proof-Of-Work 形式参与区块链的特殊成本。

另一方面，Permissioned 区块链在一组已知，已识别且经常经过审核的参与者中操作区块链，而参与者在产生一定程度信任的治理模型下运行。Permissioned 区块链提供了一种方法来保护一组具有共同目标但可能不会完全相互信任的实体之间的交互。通过依赖参与者的身份，Permissioned 区块链可以使用更传统的崩溃容错（CFT）或拜占庭容错（BFT）共识协议，这些协议不需要昂贵的挖掘。

另外，在 Permissioned 的环境下，参与者通过智能合约有意引入恶意代码的风险得以降低。参与者是相互了解的，并且遵循针对网络和相关交易类型建立的法律协议，所有活动（无论是提交应用程序交易，修改网络配置还是部署智能合约）都记录在区块链上。除了完全匿名之外，还可以根据治理模型的条款轻松地确定有罪的一方并惩罚破坏者。

Chaincode

智能合约或 Fabric 称之为 Chaincode 的功能，是一种部分受信任的分布式应用程序，可从区块链和对等方之间的潜在共识中获得安全性/信任。这是区块链

应用程序的业务逻辑。

适用于智能合约的三个要点，尤其是应用于平台时：

1. 网络中同时运行许多智能合约，
2. 它们可以动态部署（在许多情况下，任何人都可以），
3. 应用程序代码应被视为不受信任，甚至可能是恶意的。

现有的大多数具有智能合约功能的区块链平台都遵循一种订单执行架构，其中共识协议为：验证并订购交易，然后将其传播到所有对等节点，然后，每个对等方依次执行事务。

订单执行架构实际上可以在所有现有的区块链系统中找到，从以太坊等公共/非许可平台（基于 PoW 的共识）到 Tendermint, Chain 和 Quorum 等许可平台。

在以订单执行架构运行的区块链中执行的智能合约必须具有确定性。否则，可能永远无法达成共识。为了解决非确定性问题，许多平台要求以非标准或特定于域的语言（例如 Solidity）编写智能合约，以便消除非确定性操作。这阻碍了广泛采用，因为它要求开发人员编写智能合约来学习一种新语言，并可能导致编程错误。

此外，由于所有事务由所有节点顺序执行，因此性能和规模受到限制。智能合约代码在系统中的每个节点上执行的事实要求采取复杂的措施来保护整个系统免受潜在的恶意合约的侵害，以确保整个系统的弹性。

总结与展望

区块链是一门新技术，Hyperledger Fabric 更是作为一种优秀的区块链平台实现，在区块链的舞台上占有重要的地位。Fabric 的高度可扩展性以及 Permissioned 的特点，使该平台能够支持从政府，金融，供应链物流，医疗保健等广泛的行业中进行应用。

更重要的是，Hyperledger Fabric 是当前十个 Hyperledger 项目中最活跃的，该平台的社区正在稳步增长，并且每个后续版本提供的创新远远超过了其他任何企业区块链平台。

可以预见的是，区块链存储技术的高可靠性在未来必然拥有适当的用武之地，这包括加密货币这个自由世界的开源货币的唯一解决方案，和传统行业中 Permissioned 区块链的广泛应用。