# 介绍

一般来说，区块链是一个由分布式网络中的*节点*维护的不可篡改的账本。这些节点通过执行被*共识协议*验证过的交易来各自维护一个账本的副本，账本以区块的形式存在，每个区块通过哈希和之前的区块相连。

第一个被广为人知的区块链应用是加密货币比特币，而其他应用都是从它衍生出来的。以太坊是另一种加密货币，它采用了不同方法，整合了许多类似比特币的特征，但是新增了*智能合约*为分布式应用创建了一个平台。比特币和以太坊属于同一类区块链，我们将其归类为*公共非许可（Public Permissionless）*区块链技术。这些基本上都是公共网络，允许任何人在上面匿名互动。

随着比特币、以太坊和其他一些衍生技术的普及，越来越多的人想要将区块链基础技术、分布式账本和分布式应用平台用到*企业*业务中去。但是，许多企业业务对性能要求较高，目前非许可区块链技术无法达到。此外，在许多业务中，对参与者身份要求比较严格，如在金融交易业务中，必须遵循“了解客户（Know-Your-Customer，KYC）”和“反洗钱（Anti-Money Laundering，AML）”的相关法规。

对于企业应用，我们需要考虑以下要求：

- 参与者必须是已认证的或者可识别的
- 网络需要获得*许可*
- 高交易吞吐量性能
- 交易确认低延迟
- 与商业交易有关的交易和数据的隐私和机密性

当前许多早期的区块链平台正在为企业应用做*调整*，而 Hyperledger Fabric 从一开始就*设计*为企业用途。下面的部分描述了 Hyperledger Fabric（Fabric）与其他区块链平台的不同，并讲解了其架构设计的一些理念。

## Hyperledger Fabric

Hyperledger Fabric 是一个开源的企业级许可分布式账本技术（Distributed Ledger Technology，DLT）平台，专为在企业环境中使用而设计，与其他流行的分布式账本或区块链平台相比，它有一些主要的区别。

一个主要区别是 Hyperledger 是在 Linux 基金会下建立的，该基金会本身在**开放式治理**的模式下培育开源项目的历史悠久且非常成功，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进行管理，Hyperledger Fabric 项目由多个组织的不同的维护人员管理。从第一次提交以来，它的开发社区已经发展到超过35个组织和近200个开发人员。

Fabric 具有高度**模块化**和**可配置**的架构，可为各行各业的业务提供创新性、多样性和优化，其中包括银行、金融、保险、医疗保健、人力资源、供应链甚至数字音乐分发。

Fabric 是第一个支持**通用编程语言编写智能合约**（如 Java、Go 和 Node.js）的分布式账本平台，不受限于特定领域语言（Domain-Specific Languages，DSL）。这意味着大多数企业已经拥有开发智能合约所

需的技能，并且不需要额外的培训来学习新的语言或特定领域语言。

Fabric 平台也是**许可的**，这意味着它与公共非许可网络不同，参与者彼此了解而不是匿名的或完全不信任的。也就是说，尽管参与者可能不会*完全*信任彼此（例如，同行业中的竞争对手），但网络可以在一个治理模式下运行，这个治理模式是建立在参与者之间**确实**存在的信任之上的，如处理纠纷的法律协议或框架。

该平台最重要的区别之一是它支持**可插拔的共识协议**，使得平台能够更有效地进行定制，以适应特定的业务场景和信任模型。例如，当部署在单个企业内或由可信任的权威机构管理时，完全拜占庭容错的共识可能是不必要的，并且大大降低了性能和吞吐量。在这种的情况下，崩溃容错（Crash Fault-Tolerant，CFT）共识协议可能就够了，而在去中心化的场景中，可能需要更传统的拜占庭容错（Byzantine Fault Tolerant，BFT）共识协议。

Fabric 可以利用**不需要原生加密货币**的共识协议来激励昂贵的挖矿或推动智能合约执行。不使用加密货币会降低系统的风险，并且没有挖矿操作意味着可以使用与任何其他分布式系统大致相同的运营成本来部署平台。

这些差异化设计特性的结合使 Fabric 成为当今交易处理和交易确认延迟方面**性能较好的平台**之一，并且它实现了交易的**隐私和保密**以及智能合约（Fabric 称之为“链码”）。

让我们更详细地探索这些区别。

## 模块化

Hyperledger Fabric 被专门设计为模块化架构。无论是可插拔的共识、可插拔的身份管理协议（如 LDAP 或 OpenID Connect）、密钥管理协议还是加密库，该平台的核心设计旨在满足企业业务需求的多样性。

总体来看，Fabric 由以下模块化的组件组成：

- 可插拔的*排序服务*对交易顺序建立共识，然后向节点广播区块；
- 可插拔的*成员服务提供者*负责将网络中的实体与加密身份相关联；
- 可选的*P2P gossip 服务*通过排序服务将区块发送到其他节点；
- 智能合约（“链码”）隔离运行在容器环境（例如 Docker）中。它们可以用标准编程语言编写，但不能直接访问账本状态；
- 账本可以通过配置支持多种 DBMS；
- 可插拔的背书和验证策略，每个应用程序可以独立配置。

业界一致公认，没有“可以一统天下的链（one blockchain to rule them all）”。Hyperledger Fabric 可以通过多种方式进行配置，以满足不同行业应用的需求。

## 许可和非许可区块链

在一个非许可区块链中，几乎任何人都可以参与，每个参与者都是匿名的。在这样的情况下，区块链状态达到不可变的区块深度前不存在信任。为了弥补这种信任的缺失，非许可区块链通常采用“挖矿”或交易费来提供经济激励，以抵消参与基于“工作量证明（PoW）”的拜占庭容错共识形式的特殊成本。

另一方面，**许可**区块链在一组已知的、已识别的且经常经过审查的参与者中操作区块链，这些参与者在产生一定程度信任的治理模型下运作。许可区块链提供了一种方法来保护具有共同目标，但可能彼此不完全信任的一组实体之间的交互。通过依赖参与者的身份，许可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，而不需要昂贵的挖掘。

另外，在许可的情况下，降低了参与者故意通过智能合约引入恶意代码的风险。首先，参与者彼此了解对方以及所有的操作，无论是提交交易、修改网络配置还是部署智能合约都根据网络中已经确定的背书策略和相关交易类型被记录在区块链上。与完全匿名相比，可以很容易地识别犯罪方，并根据治理模式的条款进行处理。

## 智能合约

智能合约，在 Fabric 中称之为“链码”，作为受信任的分布式应用程序，从区块链中获得信任，在节点中达成基本共识。它是区块链应用的业务逻辑。

有三个关键点适用于智能合约，尤其是应用于平台时：

- 多个智能合约在网络中同时运行，
- 它们可以动态部署（很多情况下任何人都可以部署），
- 应用代码应视为不被信任的，甚至可能是恶意的。

大多数现有的具有智能合约能力的区块链平台遵循**顺序执行**架构，其中共识协议：

- 验证并将交易排序，然后将它们传播到所有的节点，
- 每个节点按顺序执行交易。

几乎所有现有的区块链系统都可以找到顺序执行架构，从非许可平台，如 Ethereum（基于 PoW 共识）到许可平台，如 Tendermint、Chain 和 Quorum 。

采用顺序执行架构的区块链执行智能合约的结果一定是确定的，否则，可能永远不会达成共识。为了解决非确定性问题，许多平台要求智能合约以非标准或特定领域的语言（例如 Solidity）编写，以便消除非确定性操作。这阻碍了平台的广泛采用，因为它要求开发人员学习新语言来编写智能合约，而且可能会编写错误的程序。

此外，由于所有节点都按顺序执行所有交易，性能和规模被限制。事实上系统要求智能合约代码要在每个节点上都执行，这就需要采取复杂措施来保护整个系统免受恶意合约的影响，以确保整个系统的弹性。

## 一种新方法

针对交易 Fabric 引入了一种新的架构，我们称为**执行-排序-验证**。为了解决顺序执行模型面临的弹性、灵活性、可伸缩性、性能和机密性问题，它将交易流分为三个步骤：

- *执行*一个交易并检查其正确性，从而给它背书，
- 通过（可插拔的）共识协议将交易*排序*，
- 提交交易到账本前先根据特定应用程序的背书策略*验证*交易

这种设计与顺序执行模式完全不同，因为 Fabric 在交易顺序达成最终一致前执行交易。

在 Fabric 中，特定应用程序的背书策略可以指定需要哪些节点或多少节点来保证给定的智能合约正确执行。因此，每个交易只需要由满足交易的背书策略所必需的节点的子集来执行（背书）。这样可以并行执行，从而提高系统的整体性能和规模。第一阶段也**消除了任何非确定性**，因为在排序之前可以过滤掉不一致的结果。

因为我们已经消除了非确定性，Fabric 是第一个**能使用标准编程语言**的区块链技术。

## 隐私和保密性

正如我们所讨论的，在一个公共的、非许可的区块链网络中，利用 PoW 作为其共识模型，交易在每个节点上执行。这意味着合约本身和他们处理的交易数据都不保密。每个交易以及实现它的代码，对于网络中的每个节点都是可见的。在这种情况下，我们得到了基于 PoW 的拜占庭容错共识却牺牲了合约和数据的保密性。

对于许多商业业务而言，缺乏保密性就会有问题。例如，在供应链合作伙伴组成的网络中，作为巩固关系或促进额外销售的手段，某些消费者可能会获得优惠利率。如果每个参与者都可以看到每个合约和交易，在一个完全透明的网络中就不可能维持这种商业关系，因为每个消费者都会想要优惠利率。

第二个例子考虑到证券行业，无论一个交易者建仓（或出仓）都会不希望她的竞争对手知道，否则他们将会试图入局，进而影响交易者的策略。

为了解决缺乏隐私和机密性的问题来满足企业业务需求，区块链平台采用了多种方法。所有方法都需要权衡利弊。

加密数据是提供保密性的一种方法；然而，在利用 PoW 达成共识的非许可网络中，加密数据位于每个节点上。如果有足够的时间和计算资源，加密可能会被破解。对于许多企业业务而言，不能接受信息可能受损的风险。

零知识证明（Zero Knowledge Proofs，ZKP）是正在探索解决该问题的另一个研究领域。目前这里的权衡是计算 ZKP 需要相当多的时间和计算资源。因此，在这种情况下需要权衡资源消耗与保密性能。

如果可以使用其他共识，或许可以探索将机密信息限制于授权节点内。

Hyperledger Fabric 是一个许可平台，通过其通道架构和 私有数据特性实现保密。在通道方面，Fabric 网络中的成员组建了一个子网络，在子网络中的成员可以看到其所参与到的交易。因此，参与到通道的节点才有权访问智能合约（链码）和交易数据，以此保证了隐私性和保密性。私有数据通过在通道中的成员间使用集合，实现了和通道相同的隐私能力并且不用创建和维护独立的通道。

## 可插拔共识

交易的排序被委托给模块化组件以达成共识，该组件在逻辑上与执行交易和维护帐本的节点解耦。具体来说，就是排序服务。由于共识是模块化的，可以根据特定部署或解决方案的信任假设来定制其实现。这种模块化架构允许平台依赖完善的工具包进行 CFT（崩溃容错）或 BFT（拜占庭容错）的排序。

Fabric 目前提供了一种基于 `etcd` 库 中 Raft 协议 的 CFT 排序服务的实现。更多当前可用的排序服务请查阅排序服务概念文档。

另外，请注意，这些并不相互排斥。一个 Fabric 网络中可以有多种排序服务以支持不同的应用或应用需求。

## 性能和可扩展性

一个区块链平台的性能可能会受到许多因素的影响，例如交易大小、区块大小、网络大小以及硬件限制等。Hyperledger Fabric 性能和规模工作组 正在开发一个叫 Hyperledger Caliper的基准测试框架。

已经发表了一些研究和测试 Hyperledger Fabric 性能的文章。最新的一篇是 将 Fabric 扩展到 20000 笔交易每秒（Scaled Fabric to 20,000 transactions per second）。

## 结论

任何对区块链平台严谨的评估都应该在其名单中包含 Hyperledger Fabric。

而且，Fabric 的这些特性使其成为一个高度可扩展的系统，该平台是支持灵活的信任假设的许可区块链，因此能够支持从政府、金融、供应链物流到医疗保健等各种的行业应用。

Hyperledger Fabric 是 Hyperledger 中最活跃的项目。围绕平台的社区建设正在稳步增长，每一个连续发布的版本所带来的创新都远远超过其他任何一个企业区块链平台。

## 致谢

前面的内容源自同行审阅的"Hyperledger Fabric: A Distributed Operating System for Permissioned Blockchains"（“Hyperledger Fabric：一个许可区块链的分布式操作系统”） - Elli Androulaki，Artem Barger，Vita Bortnikov，Christian Cachin，Konstantinos Christidis，Angelo De Caro，David Enyeart，Christopher Ferris，Gennady Laventman，Yacov Manevich，Srinivasan Muralidharan，Chet Murthy，Binh Nguyen，Manish Sethi，Gari Singh，Keith Smith，Alessandro Sorniotti，Chrysoula Stathakopoulou，Marko Vukolic，Sharon Weed Cocco，Jason Yellick