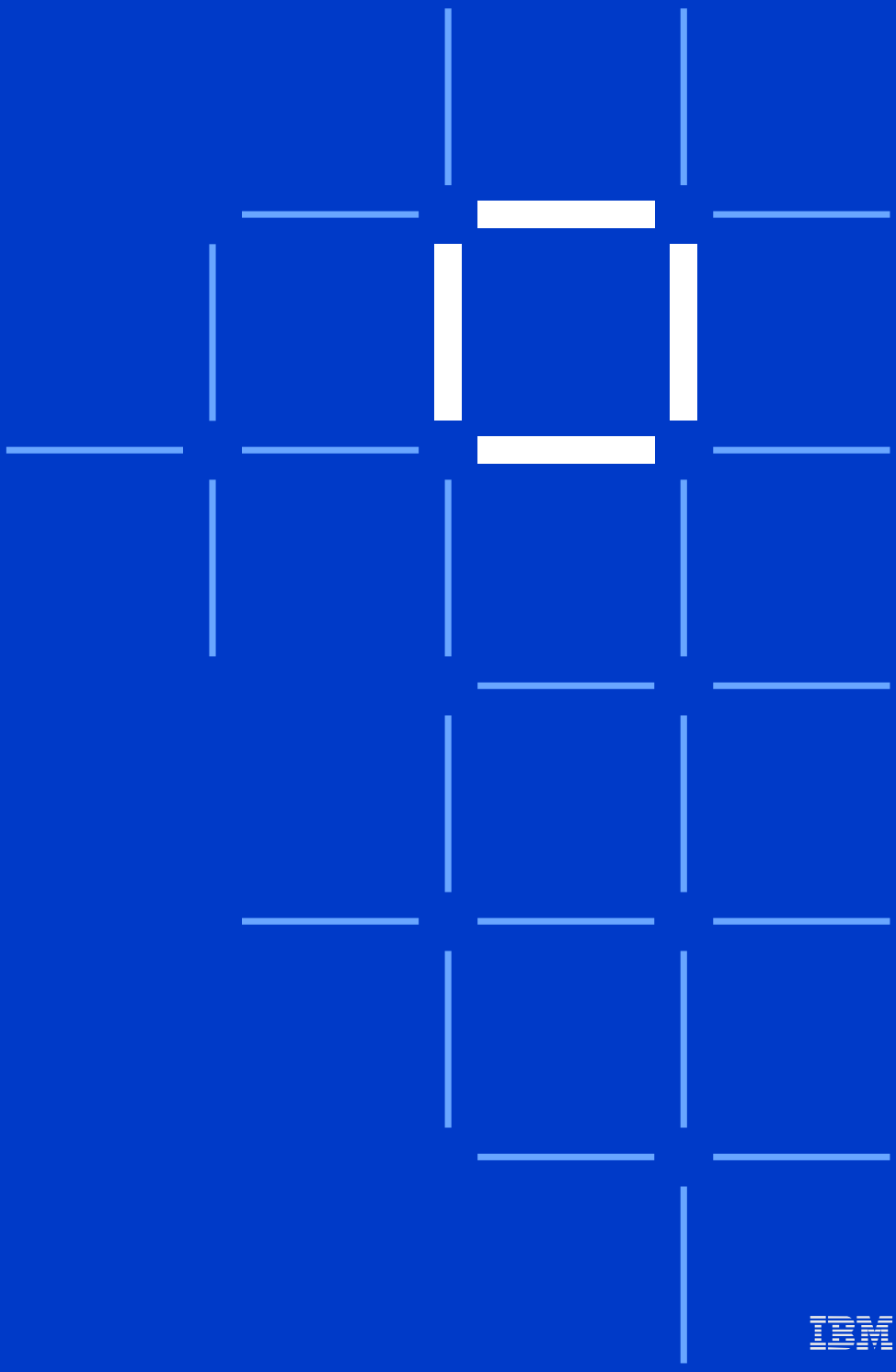
IBM Blockchain Platform 技术概览

发布于 2017 年 11 月



IBM Blockchain

IBM

引言

本报告提供了 IBM Blockchain Platform 功能的概览，IBM Blockchain Platform 基于 Linux Foundation 的 Hyperledger Fabric 和 Hyperledger Composer 构建而成。IBM Blockchain Platform 通过 IBM Cloud，提供托管的全堆栈区块链即服务 (BaaS) 产品，让成员能够开发、治理和运行网络，并且其性能和安全性能够满足监管行业要求。IBM Blockchain Platform 利用 Hyperledger Fabric，支持基于内容不可更改、共识信任和隐私保护原则建立的新型分布式的商业网络。

1. 内容不可更改和数据一致性至关重要

   一旦一笔交易被加入到账本中，该交易就不能被商业网络中的任何一个参与方删除或变更。因为 Hyperledger Fabric 不会形成分支，所以加入区块链中的信息不会发生变化，除非用另一个交易来更新这些信息。只有当各方根据灵活的架构（也称为背书策略）签署了交易，交易才算达成。分布式账本技术必须支持企业联合开发共享的真实信息源，满足特定业务网络的要求。

2. 通过许可型背书而不是匿名方式，建立信任

   与无授权即可访问网络不同，Hyperledger Fabric 和 IBM Blockchain Platform 并非通过匿名方式建立信任。整个业务网络应该知道业务网络的参与者，从而在一个具名的业务网络中建立分布式信任。监管要求（包括 HIPAA 和 GDPR）往往会规定具名网络中的参与者和交易的提供某些信息。

3. 网络的隐私性

   尽管参与者在网络上是具名的，但是他们在网络上交易时的隐私性和安全性是能够得到保证的。企业应对其交易数据和交易本身的安全性充满信心。当企业不想与整个网络共享某些信息时，Hyperledger Fabric 能够帮助企业通过专有渠道进行机密交流。托管 BaaS 平台提供了最快速、最简单、最经济高效的方法，在各团队组织之间运行分布式的网络。随着区块链项目的发展和成熟，从试验性的概念验证发展至分布式多方生产网络，IBM Blockchain Platform 能为区块链项目提供正确的工具和功能。

架构概述

IBM Blockchain Platform 构建于关键开源工具之上，为企业提供开发、运行和治理企业解决方案的必备基础架构。图 1 描述了 IBM Blockchain Platform 的端到端架构。该图结合了 400 多家客户的参与经验，基于企业级区块链网络提供商用环境。这是目前业内唯一的商用端到端平台，能支持企业以最快的时间启用分布式的区块链网络。目前，全世界众多企业都在生产环境中使用该架构。

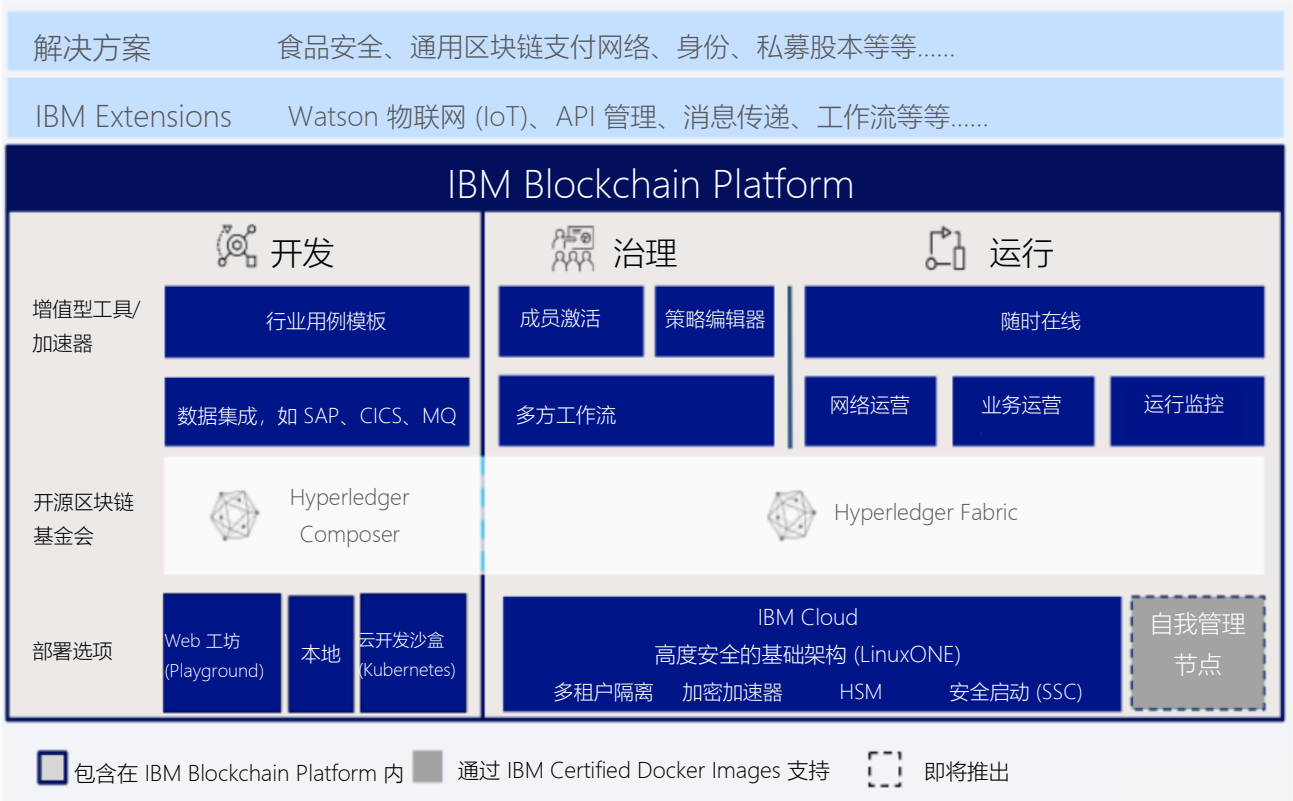


图 1：IBM Blockchain Platform

开发

认识交易业务网络价值的第一步是让开发人员能够将创新的商业理念变成现实。借助 IBM Blockchain Platform，开发人员能够利用通用工具和语言，建立业务应用模型，构建和测试业务应用，并将业务应用部署至分布式的业务网络中。

该平台能帮助开发人员：

- 利用独特的建模语言，确保业务和技术之间保持密切协调，大幅缩短区块链应用的开发周期
- 利用 JavaScript 和 REST 等热门工具和语言，帮助现有程序员快速培养区块链技能
- 利用开放的先进工具集，在首选的环境中灵活学习，并开发应用

IBM Blockchain Platform 构建于 Linux Foundation 的 Hyperledger 管控的两大开源项目之上：Hyperledger Fabric 和 Hyperledger Composer。在 Hyperledger Fabric 之上，由 Hyperledger Composer 提供使用常用编程语言和工具、快速构建区块链业务网络和设计业务应用程序原型的基础平台。

Hyperledger Composer

Hyperledger Composer 为企业构建区块链应用提供了框架，这些应用将能反映业务网络的核心结构。这个框架能帮助开发人员：

- 建立业务网络模型
- 通过自动生成的 REST API，呈现区块链数据和业务逻辑
- 创建使用区块链数据的应用

Hyperledger Composer 中包含强大的面向对象的业务域特定语言，旨在具体说明业务模式，包括资产的结构、参与者和交易。用户可以在 Hyperledger Composer 中使用业务域模型， API 生成、验证类型，用户界面生成等等。

Hyperledger Composer 包含一系列代码库、数据模型和运行时、开发工具，和基于 Web 的开发环境，旨在加速学习和采用。在应用开发流程中，所有这些功能不仅能降低风险，还能提高速度和效率。

Hyperledger Composer 围绕一系列工具包设计而成，这些工具是 Hyperledger Fabric 函数式单元的高层抽象，包括，基于 DSL 的 duchess 主模型，用于定义资产和关系；基于 JavaScript 定义的、面向业务逻辑的功能（即智能合约）；业务域模型中描述访问控制规则的表达式。IBM Blockchain Platform 基于 Hyperledger Composer 构建，让开发人员能够以安全且可重复的方式轻松构建应用，并将应用部署至实时的分布式的业务网络中。

Top coder 挑战

最近的一个 Topcoder 挑战使用了 Hyperledger Composer。在该挑战中，非区块链开发人员利用 Hyperledger Composer，针对分布式的业务网络，建立符合特定规定的模型。这一挑战收到了 100 多个成功提交的注册，包括医疗移动设备溯源和注册、石油出口法规、轮渡和客船登记，以及美国住房和城市发展部核准的贷款和房产销售。在这些代码的开发过程中，开发人员能够轻松地捕获业务建模语言，创建示例应用部署至业务网络中，自动化监管合规性。您可以在 Topcoder 网站上找到更多有关该挑战的信息。[1]

开发人员工具

在将应用部署至生产业务网络之前，开发人员可以拥有多个构建和测试应用的选项。借助 IBM Blockchain Platform，开发人员能够免费利用云沙箱和交互式“工坊（playground）”，帮助任何程序员成为区块链开发人员，快速、轻松地满足业务要求，加速开发区块链应用。这些工具旨在帮助您在首选环境中将业务设计转变成代码：

1. 在线试用：利用开源开发工具 Hyperledger Composer，学习重要的区块链概念，创建网络定义，并利用可重复使用的行业模型和智能合约库。
2. 安装在笔记本电脑上：在线试用后，利用经过认证的 Hyperledger Fabric 和 Hyperledger Composer 的 Docker 镜像。
3. 在云端联合开发：采用云端开发模式，您的生态系统中的所有成员都能通力协作，共享代码，并查看您运行的区块链网络的回放。该功能使用了 IBM 的 Container Service，让您能够利用 Docker 和 Kubernetes 免费、快速地建立区块链测试网络。

行业用例

通过 IBM Blockchain Platform，开发人员无需一切从零开始构建。该平台为开发人员提供了多个简单的行业用例场景，使开发人员可以从探索这些场景用例入手。在完成这份报告时，IBM 提供了以下行业的用例：供应链、金融服务、汽车、房地产、食品安全、身份和国际贸易等等。未来，我们还将增加更多其它行业用例场景。

轻松集成现有业务数据 (SOR – System of Record)

IBM 认为，很多企业都想将区块链运营与他们的大量现有数据资产集成一体。为了在开发应用时更轻松地实现这种集成，IBM 提供了 API，帮助企业利用 Hyperledger Composer REST API 服务器，集成企业现有的 SoR 系统。Hyperledger Composer 还利用 Node-Red，建立业务流模型；利用 LoopBack，辅助数据流路由。

IBM Blockchain Platform 支持多个开发选项，确保业务需求与技术能力保持一致。在了解智能合约领域易受攻击的编程语言后，您无需单独集成多个协议和平台，即可确保业务需求与技术功能保持一致。

治理

构建分布式的业务网络时，最重要的功能可能是清晰、有效的治理定义、模型和工具。IBM Blockchain Platform 提供重要功能，确保构建的网络拥有定义清晰的模型，并且无需重启整个网络即可在需要时完成更新。

构建好区块链网络后，如何在一组成员间启用和治理区块链网络，这需要大量协调工作、时间和精力。人们往往忽视和低估了妥善治理区块链网络的能力。通过妥善治理区块链网络，您最终能确保网络符合规定，消除业务责任的不确定性和风险（体现在智能合约中），确保不同交易类型的隐私性和安全性（体现在渠道），并建立一个引入新成员的审批流程。

IBM Blockchain Platform 提供的重要治理优势：

- 管理工具，让网络成员能够共同管理分布式的业务网络的治理规则和策略
- 动态管理环境，从而随着网络的发展和新智能合约的产生，不断增加网络成员
- 预构建工具，实现更快的入门、定制和激活

IBM Blockchain Platform 提供了第一套集成工具，允许团队能够利用定制化的策略，跨队列执行网络变更管理。

激活工具

随着新参与者和交易的创建，分布式的业务网络在不断变化。借助激活工具，网络成员能够轻松提高网络的规模，设置新的智能合约，并在更广泛的业务网络中构建渠道。

策略编辑器

您必须以灵活的方式支持区块链网络的核心组件，如共识、成员策略、智能合约和交易渠道。借助 IBM Blockchain Platform 中的策略编辑器，分布式的业务网络的（所有或部分）成员能够合作更新网络治理的策略。

多方工作流工具

网络成员需要了解各方如何在网络上互动。IBM Blockchain Platform 提供了一个成员活动面板的工作流工具，展示集成式定制化通知，并在进行规则投票时，保证签名收集的安全。

网络模型

与传统的业务网络一样，不同的参与者有不同的业务目的。IBM Blockchain Platform 能够将参与者设置成特定的角色，并根据业务目的的不同，受不同治理策略管制。IBM Blockchain Platform 上的分布式的业务网络成员能够扮演一个或多个角色，包括参与者、成员、用户，成员提供商或成员消费者。每位成员都能根据其业务需求运行多个对等节点，并参与不同的网络。您可以配置通信"渠道"，确保只有特定的成员能够查看特定的数据。成员能够利用共识和排序的集群，提交并更新他们的账本副本。只有能够通过身份验证的应用，才能成为业务网络中交易的主用户界面。

运行

处理任务关键型应用和交易数据的分布式的业务网络需要构建于满足以下要求的平台之上：支持安全且可扩展的"始终在线"的运行和更新。借助 IBM Blockchain Platform，成员能够利用生产就绪型、安全加固的服务，部署并运行分布式的网络。

操作系统

IBM Blockchain Platform 的核心操作系统是 Hyperledger Fabric。该网络的后端操作环境运行于网络发起者选择的服务计划。对 Enterprise 和 Enterprise + 选项感兴趣的使用者可以选择高度安全的 LinuxONE 基础架构，而入门计划则提供更加灵活的选项。2017 年 7 月，Hyperledger 发布了 Hyperledger Fabric 1.0 生产就绪版。Hyperledger Fabric v1.0 由来自 28 个组织的 159 名开发人员共同开发完成，由企业社区构建，服务于企业社区。Hyperledger 的技术指导委员会根据企业采用需求，推动社区积极参与并作出贡献，支持生产网络的模块化、可扩展性和共识。

Hyperledger Fabric 提供核心功能，满足权限区块链网络的特定需求，网络的组织成员既有大型企业，也有小型企业。Hyperledger Fabric 的整个架构都具有模块化特点，让您能够根据联盟的需求，交换密码、身份、共识算法、智能合约语言和其他方面的各类实施技术。Hyperledger Fabric 为您构建分布式的业务网络提供强大的基础，您无需拼凑不同的解决方案。

模块化

区块链网络必须能够根据企业和行业，融合各种全新和现有的"可插拔式"功能。因此，Hyperledger Fabric 采用模块化设计，从而随着新功能的增加，打造面向未来的网络。Hyperledger Fabric 的重要功能都具有模块化特点：

- 共识：支持任意基于投票的共识算法，满足崩溃容错（crash fault tolerance）和拜占庭容错（byzantine fault tolerance）的要求。目前基于实施配套 Apache Kafka，同时还在开发搭配其他选项的产品，比如基于 Raft 和基于 BFT-SMaRt 的选项
- 数据库：目前提供的数据库选项包括 LevelDB 和 CouchDB，其他选项还在开发中
- 成员服务：目前基于 Public Key Infrastructure 实施，即将推出基于零知识证明(Zero-Knowledge Proof)的实现

借助 Hyperledger Fabric 的模块化设计，IBM Blockchain Platform 能够利用行业领先的安全实践，服务生产就绪型网络。

可扩展性

随着各行各业完成初始的探索和概念验证，企业需要可扩展的解决方案。Hyperledger Fabric 能够支持不断增长的业务网络，动态地增加参与者，并支持与日俱增的交易处理需求。

可扩展性在很多方面取决于共识、成员或安全配置。模块化平台能够配置网络，从而达到所需的吞吐量规模。但是，Hyperledger Fabric 能够进行扩展以支持吞吐量，根据不同的用例，满足企业需求。目前的网络每秒能够处理数千笔交易。

可扩展性的意义不仅仅体现在吞吐量上。网络的增长更要求新参与者能够便捷地加入网络，并在网络上开展交易。Hyperledger Fabric 将参与者分为背书人和提交人两种角色。这意味着，只想要账本副本的参与者可以作为提交人角色加入网络，提交人角色无需承担交易背书的压力，即可更新账本副本。

最后，Hyperledger Fabric 引入了渠道理念，让参与者能够机密地完成交易，并加入多个有特定业务合作伙伴的渠道。

通过利用治理和网络配置工具（后文将详细讨论），IBM Blockchain Platform 进一步增强了这些功能。分布式的业务网络需要一个能够动态增加参与者、资产和交易的平台。

共识

对于每个区块链协议的安全性、可扩展性和成熟度来说，清晰定义并实施的共识算法可能是最重要的功能。选择适当的共识算法，对于在分布式的业务网络中支持互相信任至关重要。

如上所述，Hyperledger Fabric 中的共识具有可插拔的特点，以满足特定的企业用例需求。比如，安全需求相对有限的开发网络可能最好采用 SOLO 共识模型，从而用一个节点验证所有交易。生产网络可能更需要崩溃容错和拜占庭容错共识算法。Hyperledger Fabric 支持上述两种模式。

目前，Hyperledger Fabric 支持许可型网络中基于共识算法的投票。投票和许可的结合让网络运行时的性能远远超过了许多公有拜占庭容错网络。没有未知角色，意味着我们不需要麻烦的共识算法。Hyperledger Fabric 提供开箱即用的 Apache Kafka，并支持崩溃容错。因此，当出现部分网络崩溃时，网络依然能够运转。其他共识算法包括 BFT-SMaRt 和 SBFT （简化的拜占庭容错），以容忍共识中的恶意行动。Hyperledger 详细比较了不同的 Hyperledger Frameworks，包括 Hyperledger Fabric，并发布了相关信息。[3]

Hyperledger Fabric 迄今为止所取得的成绩都离不开 Hyperledger 项目所提供的大量社区支持。代码库目的明确，并采用开放式治理模式，因此，它能够发展成行业领先的协议，满足企业生产网络的需求。

高度安全的基础架构

如上所述，基础架构的选择与服务计划的选择息息相关。IBM Blockchain Platform Enterprise 和 Enterprise + 计划借助 LinuxOne Emperor，利用行业领先的安全性，确保所有代码和数据始终处于加密状态，经过篡改的虚拟机不会启动，不会出现管理员访问或特权访问。代码在 IBM Secured Services Containers（SSC）中执行，以保障账本的安全性。IBM Secured Services Containers 能够确保：

- 租户彼此隔离
- 消除特权访问，避免出现内部攻击或凭证泄密
- 数据密钥是私有的，即使法庭命令要求，IBM 也无法访问数据
- 可信的 Boot Loading，实现防篡改的代码执行

在硬件安全模块方面，IBM Blockchain Platform 满足最高的 FIPS 140-2 Level 4 标准。

此外，IBM Blockchain Platform"始终在线"的设计能够在运行时更新网络，并基于全球最快的 Linux 计算优化了性能。以上每一项功能背后都有 IBM 深厚的 Hyperledger Fabric 专业技能的支持，我们全年全天候 24x7 提供直接融入控制台的区块链技术支持。

我们加入了特定的工具和功能，让网络运行变得更轻松。其中包括：

- 仪表板，监控并管理网络上的资源
- 生命周期管理，无需中断网络，即可无缝升级整个代码堆栈
- 全天候 24/7 技术支持，集成至门户
- 强化的安全堆栈，无特权访问，无恶意软件，防篡改，100% 硬盘加密，以及保护硬件安全模块密钥

网络运行

IBM Blockchain Platform 支持创始人通过一个简单的用户界面，启动、邀请和配置网络。

启动网络时，需创建 3 个订购对等节点，2 个认证中心。这为创始人提供了一个现成的基础，创建自己的业务网络。然后，创始人可以利用任意数量的对等节点，邀请其他参与者加入网络。参与者将收到邮件邀请通知，从而轻松加入网络。

网络运行用户界面还能支持创始人配置核心网络组件，比如身份验证和渠道创建。这有助于确保只有获得许可的用户能够访问网络，机密交易将通过渠道完成。

业务运营

IBM Blockchain Platform 提供用户界面，从而在活跃的区块链网络中支持业务运营。无需放弃网络或中断运营即可完成更新。

智能合约能够自动交换信息和资产，是区块链网络的核心功能。IBM Blockchain Platform 用户能够通过单一用户界面，在网络中轻松部署和升级智能合约。此外，用户还能编辑渠道的策略，该渠道负责管控共识。

运营监控

随着交易和参与者的与日俱增，用户需要监控网络上的活动。IBM Blockchain Platform 提供 Network Traffic Dashboard 和 Network Health Monitor。通过这些仪表板，用户能够主动调整网络运营，清晰定义网络中的资源使用情况。

网络成员

成员共同承担区块链网络的成本。为了加入网络，每位成员必须运营一个或多个对等节点，支持他们开展交易，体现他们的共享账本副本。借助 IBM Blockchain Platform，成员能够根据生态系统在计算性能和隔离方面的需求，从下面四个成员计划中选择一个计划来管理他们的网络对等节点：

1. 入门计划：按小时支付订阅费用，可享受基础级服务（2018 年推出）
2. Enterprise 计划：按月支付订阅费用，可享受更先进的服务，可立即在生产网络中使用（现已推出）
3. Enterprise Plus 计划：采用按月租用计划，获得面向性能和隔离的专用计算资源（2018 年推出）
4. 自托管计划：经过认证和签署的 Hyperledger Fabric 镜像，您可以将这些镜像安装在自己的基础架构上。可连接托管在 IBM Blockchain Platform 上的网络（2018 年推出）

每个成员选项包括所有平台工具，用于开发和治理整个区块链网络与工具，运行 1 个区块链对等节点。

混合部署

值得注意的是，IBM Blockchain Platform 还通过 IBM Certified Docker，支持以自托管模式部署 Hyperledger Fabric。这样，您就能根据业务需求，通过私有数据中心、IBM Softlayer、AWS 或 Azure 设置网络对等节点。

更确切地说，IBM 将支持 Developer Sandbox 和自托管网络，您可以在多个部署环境中部署该网络。IBM Blockchain Platform 将扮演控制中心的角色，让您通过不同的部署选项，控制区块链网络的运行。

结语

2017 年，各类企业取得了诸多区块链创新成果。开源组织将机构和开发人员汇聚一堂，让区块链能够为企业所用，进一步增强了这些创新成果。

IBM Blockchain Platform 代表的是下一阶段的创新方向，因为它能帮助您通过基于企业级协议的便捷界面，构建、治理和运行生产网络。利用免费入门信息，您能够轻而易举地立即着手构建您的用例、应用或网络。

点此了解更多信息：http://www.ibm.com/cloud-computing/cn/zh/newplatform/blockchain/offerings

开发人员入门指南：https://developer.ibm.com/blockchain/sandbox/

IBM Corporation
Route 100
Somers, NY 10589

美国印刷
2017 年 10 月

[1] www.topcoder.com/challengedetails/30057924/?type=develop

[2] www.hyperledger.org/announcements/2017/07/11/hyperledger-announces-production-ready-hyperledger-fabric-1-0

[3] www.hyperledger.org/wp-content/uploads/2017/08/Hyp

[4] erledger_Arch_WG_Paper_1_Consensus.pdf