# 如何挑选最合适的区块链技术与基础架构

IBM 竞争性项目办公室

Angshuman Roy

高级 IT 架构师

2017 年 2 月

# 目录

执行概要 ..... 3
背景 ..... 4
区块链可为企业提供哪些帮助 ..... 5
热门区块链技术 ..... 6
比特币 ..... 6
Ripple ..... 6
Ethereum ..... 7
Hyperledger ..... 7
几个问题，帮贵企业找到最合适的区块链平台 ..... 8
如何挑选最合适的基础架构 ..... 10
安全性 ..... 10
可扩展性与性能 ..... 10
云选项还是企业内部选项 ..... 11
总结 ..... 12

## 执行概要

区块链之所以被认为是一种变革性技术，是因为它具备颠覆各个行业交易流程的潜力。在区块链中，数据存储在分布式账本中，而账本在网络中的所有同行之间共享。这种方式能够消除货物与服务交易过程中的“中间人”，进而节省时间和资金。在传统环境中，需要耗费数小时或数天的时间才能完成业务交易，而借助区块链，仅需数分钟即可完成。根据最新发布的一篇文章 [1] 中的介绍，每年企业通过区块链可节省 5,500 亿美元的资金。正因为此，金融服务行业一直处在区块链技术采用的最前线，也就不足为奇了。据全球经济论坛的一份白皮书 [2] 预测，80% 的银行会在 2017 年启动区块链项目，而全球范围内超过 90% 的中央银行已经开始了这方面的论证。

目前，市场上已经推出了多款区块链实施产品，客户可以选择相应的硬件基础架构，并决定是在云端运行还是在内部运行。在本白皮书中，我们将探讨一些主流的备选方案，并对比它们的优势与劣势，进而总结出在挑选最适于运行区块链的基础架构时应给与考虑的产品特性。

[1] http://www.coindesk.com/blockchain-tech-could-save-global-business-550-billion-per-year/

[2] http://www3.weforum.org/docs/WEF_The_future_of_financial_infrastructure.pdf

## 背景

区块链技术又称作分布式账本技术 (DLT)，它是一种分布式数据库对等网络，在该网络中，所有的实体共享同一"账本"。相同的账本拷贝会分发到所有节点，并通过技术手段保持同步。这种方式可以消除中介角色，进而加快交易速度并降低成本。

区块链的起源可以追溯到非常流行的一种数字货币 - 比特币 (Bitcoin)。比特币的概念最早是在一篇名为"比特币：对等电子现金系统 (Bitcoin: A Peer-to-Peer Electronic Cash System)"[3] 的白皮书中提出，这篇文章发布于 2008 年，由一名笔名为 Satoshi Nakamoto 的社会学家撰写。他在文章中提到，比特币可用于发送互相并不信任的两个实体之间的支付请求，整个过程中不需要第三方金融机构的参与。在比特币网络中，每笔交易都存储在由区块链构成的账本中，最新的区块会通过数字签名与之前的区块相连接。为了确保账本的可信任性，网络参与方会运行复杂的算法对这些签名进行认证，并在区块链中添加交易。通过这种方式，即便是完全互不信任的陌生人也可以在网络空间中相互交换价值。在接下来的几年里，这种分布式账本技术 (DLT) 被广泛拓展到数十个其他领域[4]。大家都认识到，若要将该技术拓展到其他业务领域，就必须具备 4 个关键组件：

1. 共享式账本 - 仅可附加的分布式记录系统，在整个业务网络之中共享
2. 智能合同 - 业务条款嵌入到交易数据库中并随着交易的进行得到执行
3. 隐私 - 确保适当的可视性；确保交易安全性，且能够对交易进行鉴定和验证
4. 共识 - 所有参与方均会同意经网络验证的交易

与传统的系统不同，在区块链中，无需在后续进行对账或结算流程。在双方就交易"达成一致"后，仅会在网络中创建一个包含有交易数据的区块。通过这种方式，就无需单独的结算流程，也不需要中介角色。每个节点都会以记录列表的形式对账本进行维护，此类列表会不断增加而且记录按次序排列，即所谓的"区块"。交易完成后，会在链条上添加一个新的区块，然后分发至网络中的所有同行。这种方式可以确保每个节点账本中的数据完全相同。除了业务内容外，每个区块还包含有一个时间戳、一个由内容衍生的密码散列，以及之前与之后区块的链接。从设计上来说，区块链具有不可变性；换句话说，数据一旦写入到区块之后，就不可更改。若要更改数据，您必须通过更改处理流程创建新的区块。之所以说区块链从设计上来说非常安全，是因为每个细微的更改都会改变区块的哈希值，而该哈希值会将该区块标记为"已损坏"。尽管账本是共享的，但并不表示所有的数据必须对所有节点可见（在比特币实施中，所有数据均可供每个节点使用）。这种可视性通过智能合同中的隐私策略来控制。

为了确保所有节点中的账本都有相同的数据，您必须使用"共识"算法。共识能够确保共享式账本都是一模一样的拷贝。密码散列（比如 SHA256 计算算法）能确保交易输入的任何更改都会改变哈希值，借此显示损坏的交易输入。数据签名则能确保交易来自发送者（用私有密钥签名），不是"恶意"代码。

凭借这种分散式共识，区块链非常适合用于事件、标题、来源、医疗记录和其他记录管理活动的记录，身份管理，以及 CRM 系统中的交易处理。

[3] https://bitcoin.org/bitcoin.pdf

[4] http://www.blockchaintechnologies.com/blockchain-applications

## 区块链可为企业提供哪些帮助

区块链可帮助企业实现以下竞争优势：

### 节省时间

区块链大大缩短了解决争议、寻找信息和验证交易的时间，从而帮助您更快地完成结算和交付。IBM® Global Finance (IGF) 就是一个绝佳的例子。它利用区块链技术快速解决与客户和合作伙伴之间的争议，从争议中腾出了近 1 亿美元的资金[5]。

### 节约成本

区块链不仅能自动执行效率低下的流程，还能减少开销和成本高昂的中介角色。根据埃森哲 (Accenture) 发布的报告[6]，区块链每年最高能帮助投资银行节约 120 亿美元。该报告还预测，通过利用区块链技术运行部分流程，比如财务报表流程，他们分析的八家投资银行还能提高数据质量和透明度，将基础架构成本平均减少 30%。与合规、业务运营（如交易支持）和集成运营（如"了解您的客户"检查）相关的成本最高可降低 50%。

### 降低风险

区块链能将共谋、篡改和无意泄露信息的风险降至最低。很多处理安全问题的金融行业应用可以运用区块链技术。而零售业巨头沃尔玛则利用区块链追踪猪肉的源头，从农场一直到门店货架，全程进行追踪[7]。未来，他们还将利用区块链追踪其销售的其他肉类和产品。

### 支持新的业务模式

与其他颠覆性技术一样，区块链也能带动新型企业的问世。伦敦一家名为 Everledger 的初创企业就为区块链找到了一个独特的用途。2015 年 8 月[8]，该公司宣布他们将利用区块链遏制钻石盗窃问题。他们的首席执行官表示，迄今为止我们都没有一种保险的方法来检测钻石是否曾经被盗。与其他奢侈品一样，钻石的所有权证明依然是纸质文档，因而很容易被篡改和丢失。这种情况下，Everledge 提出了一种方法，他们将以数字方式验证每颗钻石，从矿井到消费者全程追踪每颗钻石。一旦区块链能够追踪所有钻石，那么任何被盗的钻石都能被轻而易举地发现。

[5] http://blogs.wsj.com/cio/2016/07/29/ibm-set-to-launch-one-of-the-largest-blockchain-implementations-to-date/

[6] http://www.reuters.com/article/us-banks-blockchain-accenture-idUSKBN1511OU

[7] http://blogs.wsj.com/cio/2016/12/16/wal-mart-readies-blockchain-pilot-for-tracking-u-s-produce-china-pork/

[8] http://www.coindesk.com/everledger-blockchain-tech-fight-diamond-theft/

## 热门区块链技术

下面，我们将介绍一些热门的区块链实施项目以及它们的属性。贵企业可能会因为它们的一些独特特征和优势而选择这些技术。

### 比特币

这是最早也是最有名的区块链实施项目。它创造了一种可保存在电子钱包中的数字货币。自 2009 年问世以来，比特币的热度不断高涨。比特币目前的市场价值已经超过了所有其他公有加密货币的市场价值总和 [9]。比特币吸引人的特点之一是，它能够在全球匿名交易，不用受任何国家强制法规限制。您可以利用这种数字货币在 100,000 多个商家处购买商品 [10]，其中包括亚马逊 (Amazon)、家得宝 (Home Depot) 和赛百味 (Subway)。


如果贵企业想不受任何政府法规的限制，接收来自全球客户的付款，比特币是一个不错的选择。

### Ripple

Ripple 是一家聚焦转账技术的专用区块链技术供应商。其产品就叫 Ripple，运用分布式账本技术 (DLT) 加快银行之间的跨境转账 [11]。他们宣称最高能将银行的结算成本减少 60%[12]。该平台不用通过中央结算所或监管机构，就能完成银行转账。区块链能帮助他们加快流程，减少成本。

目前的转账系统往往需要超过一天的时间才能完成转账，并且会受银行营业时间的限制。并且，开始转账时，汇率和交易费都是未知数。通常资金会在多个银行之间流动，这会产生延迟和其他费用。银行必须安排专人管理流动资金和交易，响应查询，修改付款明细，跟踪进度，以及纠正错误。

相反，Ripple 能提供全天候、实时、同步、透明且信息丰富的交易。在交易开始前，您能够实时确认汇率和费用，立即完成付款。Ripple 解决方案为 MasterCard 和 Visa 等发卡机构整合了付款消息传递和资金结算功能。

此外，Ripple 还支持自己的加密货币 XRP。2016 年 10 月，他们在 12 家全球银行之间试行了一次转账操作 [13]。他们表示，通过利用 XRP 进行转账，银行甚至能节约更多成本。

---

[9] http://coinmarketcap.com/

[10] http://www.ibtimes.co.uk/bitcoin-now-accepted-by-100000-merchants-worldwide-1486613

[11] https://ripple.com/wp-content/uploads/2016/07/Accenture_Ripple_CrossBorderPayments.pdf

[12] https://ripple.com/insights/ripple-and-xrp-can-cut-banks-global-settlement-costs-up-to-60-percent/

[13] http://www.coindesk.com/global-banks-test-ripples-digital-currency-new-blockchain-trial/

## Ethereum

Ethereum 是应用最广泛的通用区块链平台之一。与其他区块链实施项目一样，这也是一个开源项目。2014 年 1 月，Vitalik Buterin 宣布启动该项目，2014 年 7 月，他们通过众筹筹集了项目资金。Vitalik 是一名编程人员，曾参与比特币项目。2013 年底，他与比特币的核心开发人员的理念发生了冲突，他认为应该扩展比特币平台，让比特币能处理数字货币以外的普通交易。为了做到这一点，他们需要一个强大的脚本语言，来编写"智能合同"中的业务逻辑。由于没有与比特币团队达成共识，Vitalik 另起炉灶，启动了一个新平台的开发，也就是我们所说的 Ethereum。Ethereum 的首个生产版本于 2015 年 7 月发布。Ethereum 支持一种名为 Ether 的加密货币。开发人员可以用多种语言编写智能合同，比如 Solidity、Python、C++ 和 Java。Solidity 可能是最热门的语言，因为微软的 Visual Studio Integrated Development Environment (IDE) 支持该语言。目前，多家供应商在公有云（比如微软的 Azure 和亚马逊的 AWS）上推出了该产品。

自发布以来，Ethereum 经历了多次安全挑战。最大的丑闻可能要算 2016 年 7 月发生的事故，当时一名黑客偷走了价值 5000 万美元的 Ether[14]。这些技术问题导致基础代码出现了"硬分叉"。随之而来的是区块的"不变性"问题和 Ethereum 社区的分裂。最近的一次也是第四次分叉发生在 2016 年 11 月，旨在预防未来网络上出现的拒绝服务攻击 [15]。此次分叉导致其货币 (Ether) 严重贬值 [16]。目前，Ethereum 还面临可扩展性问题，其赞助者希望能尽快找到解决方案 [17]。

## Hyperledger

另一个有名的通用区块链平台是 Hyperledger。这也是一个开源项目，由 Linux 基金会发起。目前，Hyperledger 项目已经有超过 100 个成员，其中包括一些科技巨擘，比如 IBM，因特尔，埃森哲，以及其他行业领导者，如摩根大通 (J P Morgan)，富国银行 (Wells Fargo)，空客 (Airbus) 和三星集团。

目前他们正全力开发 Hyperledger 代码，预计将于 2017 年第一季度推出生产就绪版本 (V1)。此外还有多个正在开展的孵化器项目（如 alpha 代码）。其中最有名的要属 IBM 负责的"Fabric"项目。IBM 通过云端 (Bluemix®) 和企业内部模式以可下载的 Docker 容器形式提供 Hyperledger Fabric 部署。

Hyperledger 的重心是为企业构建区块链平台。考虑到支持数字货币所带来的风险，Hyperledger 决定不涉足该领域。这是它与 Ethereum 的一大区别。它的设计重点放在安全性、可扩展性和隐私上面，其他实施项目（如 Ethereum）同样面临这些挑战。

在 IBM 及其他 Hyperledger 项目成员的帮助下，Hyperledger 已经得到了广泛采用。Crédit Mutuel Arkéa of France 和日本瑞穗银行 (Mizuho Bank of Japan) 等银行已经开始部署该技术。零售业巨头沃尔玛正在其供应链中加入区块链技术，以便从农场到门店货架，跟踪整条供应链。维基上列出了许多这样的用例实例 [18]。

[14] http://www.businessinsider.com/dao-hacked-ethereum-crashing-in-value-tens-of-millions-allegedly-stolen-2016-6

[15] http://www.coindesk.com/ethereum-forks-again-so-far-so-good/

[16] https://cointelegraph.com/news/ethereum-in-free-fall-as-floor-beneath-it-drops

[17] http://www.coindesk.com/ethereum-creator-vitalik-buterin-scaling-devcon2/

[18] https://wiki.hyperledger.org/groups/requirements/use-case-inventory

## 几个问题，帮贵企业找到最合适的区块链平台

区块链是一项快速发展的技术。市场上已经有多个实施项目，比如 Ethereum 和 Hyperledger，每个项目都有其独特功能。比如，您可以选择私有/许可或公有/匿名网络，通用或专用网络等等。为了挑选最合适的区块链技术，首先您应该回答以下问题：

1. **该应用是否已经有了行业标准区块链网络？**

   通常区块链交易发生在实体集团（如银行或供应商）之间。一个关键的要求是所有同行不仅要采用同一种区块链技术，还必须是同一版本的区块链技术。因此，如果已经有了一个区块链网络，您就必须加入这个网络。如果您是在构建一个新的区块链网络，那么您就可以自由选择前一章中的区块链技术。我们目前处于区块链部署的初期阶段，市场上只有少数几个区块链网络。尽管人们已经开始讨论在架构桥梁连接不同的区块链技术，但是这都是未来的事情了。

2. **是否区块链网络必须支持数字货币（或加密货币）？**

   尽管数字货币比特币是最有名的区块链应用之一，但是并非所有区块链实施项目都支持加密货币。有些项目（比如 IBM 支持的 Hyperledger）出于降低安全风险的考虑并不支持数字货币。很多业务应用都不需要数字货币，如汽车租赁应用、安全凭证处理应用和客户身份管理（了解您的客户）应用等。您可以在 Youtube 上找到有关此类示例的更多信息[19]。

3. **您想构建私有网络还是公有网络？**

   在私有网络中，只有预先获得授权的成员能加入该网络，他们必须在交易之前先通过身份验证。这意味着，您知道您是在与"可信"的同行进行交易，这能够降低网络中出现恶意交易的概率。而在比特币这样的公有网络中，任何人都能加入网络然后匿名交易比特币。有些区块链不支持私有网络。

4. **您希望在哪类服务器上运行比特币代码：大型机，Power Systems 还是 x86？**

   大多数区块链软件都是开源软件，可部署在多种服务器上，但有时硬件平台决定了您必须选择某种特定的区块链平台。例如，如果您想在大型机上运行由供应商支持的区块链应用，目前 Hyperledger 是您的唯一选择。后面，我们将详细讨论硬件基础架构的挑选。

5. **您想不想部署特定的公有云？**

   大多数区块链平台都可以在多个公有云上运行，但是区块链处于早期部署阶段。所以，并非所有公有云提供商都能提供所有区块链平台。比如，如果您想在 IBM 的 Bluemix 上部署区块链平台，您只能选择 Hyperledger Fabric。同样的，如果你想在微软的 Azure 或 AWS 上部署区块链，您唯一能选择的通用区块链平台是 Ethereum。未来，大型公有云提供商可能会将多个不同的区块链加入其产品目录中。

[19] https://www.youtube.com/watch?v=F0P7NM7d-ps&list=PLKBlwlwmwx1EFiLLqHxdVd8koIZMQTuzy

6. **您的开发人员在编写区块链代码时倾向于使用哪种编程语言和开发工具？**

应用的业务逻辑被写在了区块链的"智能合同"[20] 中。不同的区块链平台支持不同的编程语言。比如，IBM 支持的 Hyperledger Fabric 就支持 Go language、Java 和 JavaScript。它有一个名为 Fabric Composer[21] 的编程框架。另一个通用区块链实施项目 Ethereum 则支持用 Python、Go 和 C++ 编写的代码以及 Solidity 语言。Solidity 作为微软的 Visual Studio 扩展得到了支持[22]。

[20] http://www.coindesk.com/making-sense-smart-contracts/

[21] https://fabric-composer.github.io/index.html

[22] https://marketplace.visualstudio.com/items?itemName=ConsenSys.Solidity

## 如何挑选最合适的基础架构

您不仅需要为贵企业挑选最合适的区块链技术，还要挑选最合适的基础架构来运行区块链，而且后者与前者一样重要。下面，我们来看一下在挑选最合适的基础架构时您需要考虑的因素。

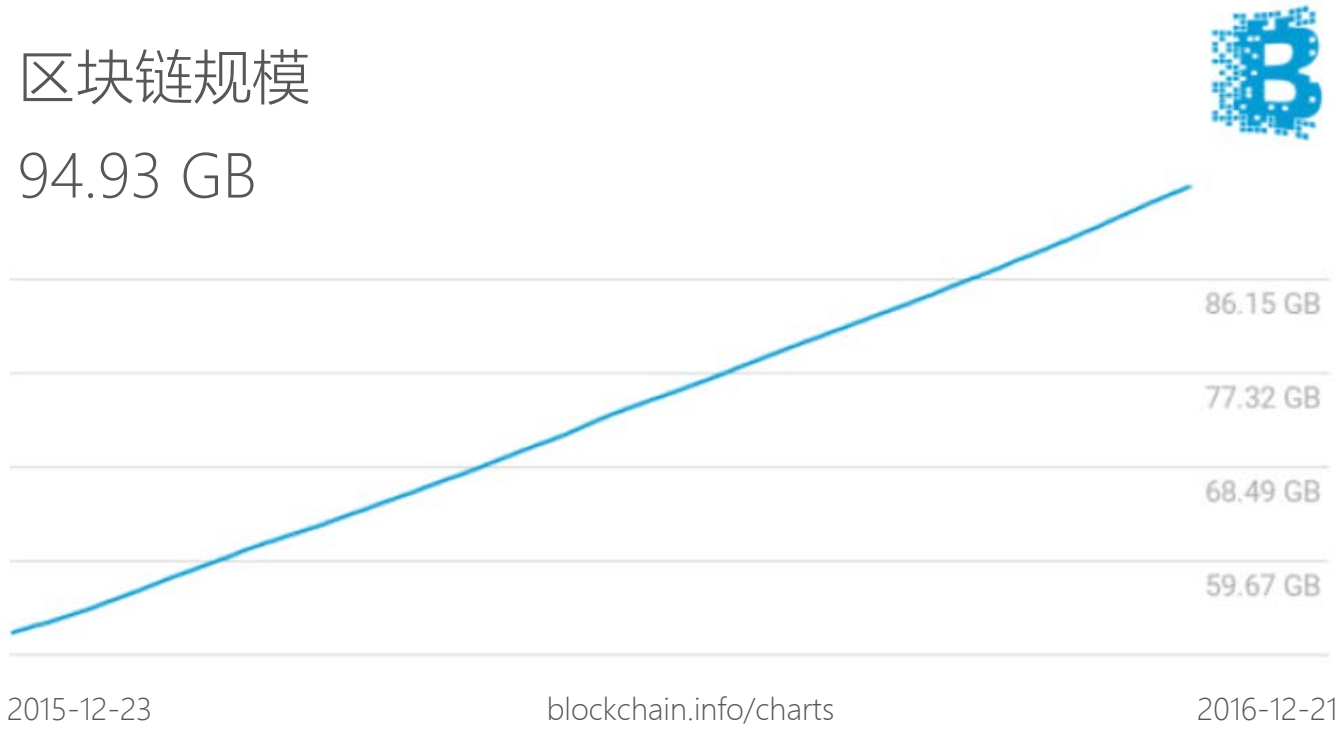
### 安全性

最近 Ethereum 网络中的几次安全漏洞事件被媒体大肆报道，这也就难怪安全性成为了大多数客户最担心的问题。为此，IBM 选择在 IBM LinuxONE™ 上推出首款商用区块链产品 - High Security Business Network，IBM LinuxONE™ 是目前最安全的服务器之一。它只在私有/许可网络中实施 Hyperledger Fabric。这意味着，节点必须通过授权和身份验证才能加入 HSBN 网络。在 Secure Services Container (SSC) 中运行的对等节点是 HSBN 的另一个功能。在 SSC 中访问节点的唯一途径就是通过 API，任何人，包括系统管理员都不能访问节点。利用授权访问的方式，SSC 技术消除了内部人士攻击系统的可能性（俗称斯诺登型攻击）。

### 可扩展性与性能

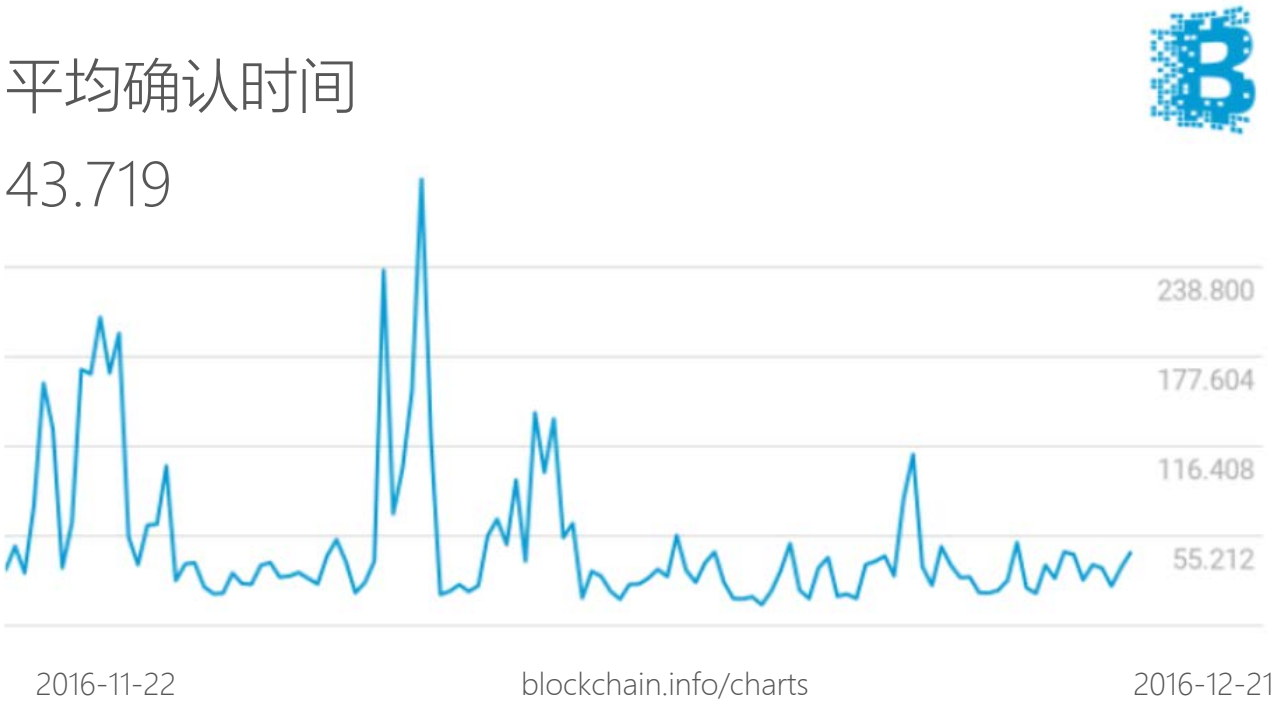
区块链的两个基础功能让可扩展性变得至关重要：

1. 保存在区块链中的账本。随着交易的完成和时间的推移，账本的规模将变得越来越大。因为其不变性，区块绝对不会被丢弃。比如，从 2016 年初到 2016 年 12 月 20 日[23]，共享账本（包括头和交易）的比特币规模已经从 52.9 GB 增加到了超过 94 GB。（注意，在网络上发送的不是整个区块链，只是新的区块。）




[23] https://blockchain.info/charts/blocks-size

2. 账本在所有节点之间共享，必须同步保存。每次交易完成后，它会创建一个新的区块，并通过“共识”机制验证其内容，然后加入每个节点的账本拷贝中。随着对等节点数量的增加，共识流程所花的时间越来越长。截至 2016 年 12 月 20 日，比特币中平均有 5370 个可获得的对等节点[24]，11 月 22 日到 12 月 21 日期间的平均交易确认时间为 43.7 分钟[25]。




随着节点和交易数量的与日俱增，您的计算基础架构也必须能够随之扩展。z Systems® 和 Power Systems™ 都能够线性扩展，因此都是非常适合用于运行区块链的服务器。

## 云选项还是企业内部选项

大多数区块链服务提供商都是通过公有云提供服务。为了获得灵活的基础架构并减少成本，客户一般选择将区块链部署在云端，但是这种模式并不适合所有情况。有些国家的法律规定，企业必须将客户的个人数据保存在本国境内。这种情况下，如果这个国家没有云服务提供商，那么您就只能选择将区块链托管在企业内部。此外，为了在公有云上运行区块链代码，你必须将数据从您的数据中心的“记录系统”迁移至云服务提供商的数据中心中。考虑到传输的数据规模，您可能需要投入大量成本。同时，数据移动还会增加安全漏洞的风险。由于这些原因，有些企业可能会选择在企业内部保存数据的服务器上运行区块链代码。客户的一个常见选择是在云端开发和测试代码，在企业内部运行生产版本。IBM 提供云选项和企业内部选项，并支持所有企业内部平台（z Systems、Power Systems 和 x86）。在公有云中，只有 IBM 提供了大型机选项，名为 High Security Business Network (HSBN)。此外，IBM 还在云端为开发人员免费提供入门包。

[24] https://bitnodes.21.co/dashboard/

[25] https://blockchain.info/charts/avg-confirmation-time?timespan=30days

## 总结

市场上已经有多个区块链技术/平台，每种区块链都有其独特的功能。有些区块链是面向专用任务（如转账）的解决方案，其他则是通用解决方案。本白皮书提供了几个问题，您可以通过回答这几个问题，为贵企业挑选最合适的区块链平台。除了区块链平台外，您还需要重点关注运行区块链的基础架构，因为它会对非功能性要求（如安全性、可用性、可扩展性和性能）产生重大影响。

Hyperledger Fabric 是一个专为企业打造的通用区块链实施项目。Hyperledger Fabric 是由 IBM 和 Linux 基金会下 Hyperledger 项目的 100 多个成员共同开发而成。目前，它已经登陆 IBM 的公有云 (Bluemix)，并且 IBM 以 Docker 容器方式支持您将 Hyperledger Fabric 部署在企业内部的三种服务器平台上 - z Systems、Power Systems 和 x86。

IBM Corporation
New Orchard Road
Armonk , NY 10504
USA

美国印刷
2017 年 2 月