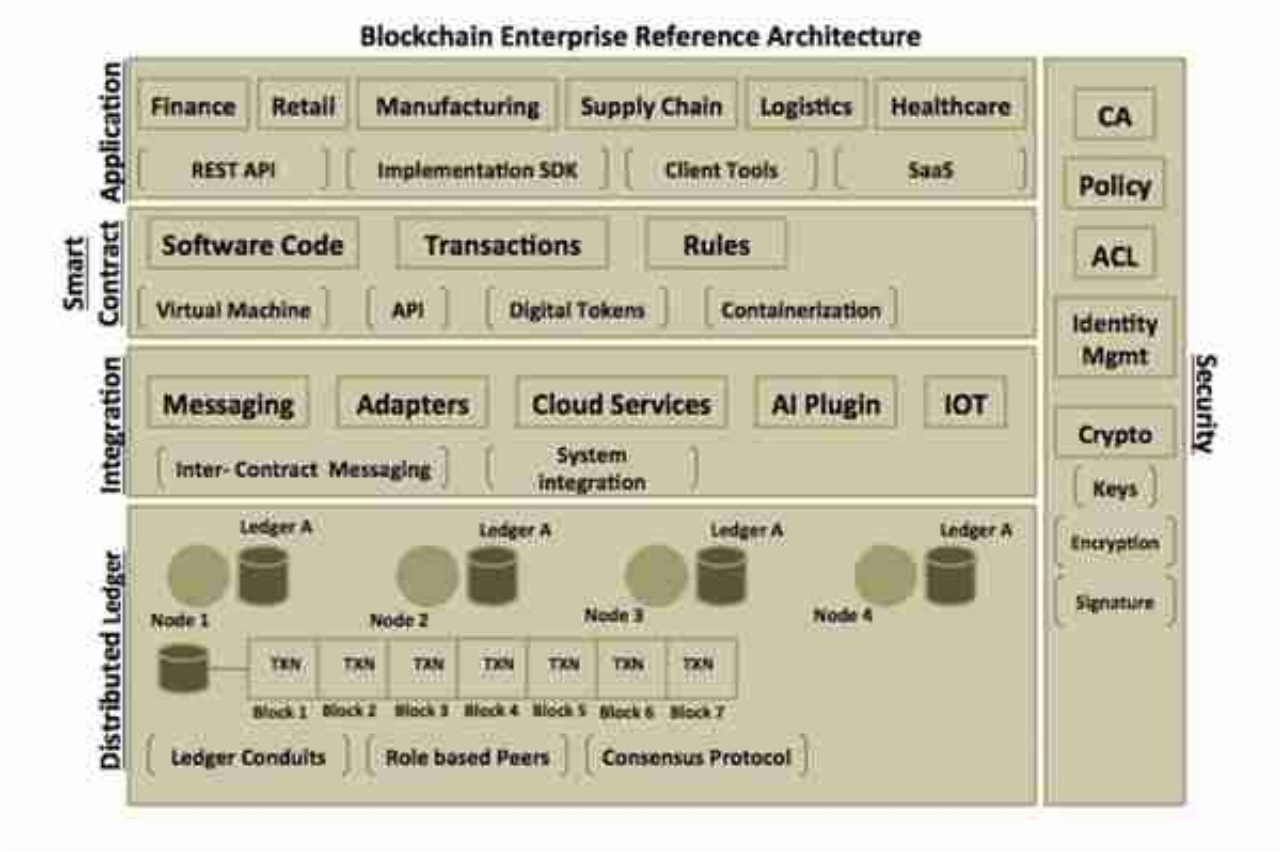
本文提出了一种分层的区块链参考架构，该架构包括应用层、智能合约层、集成层、分布式账本层以及安全层。该架构提供了区块链应用程序所必需的组件和服务，并适用于公链或私链各种应用程序的设计。

直至今日，区块链的设计已经远远超越了它最初作为加密货币技术的存在。区块链已经发展成为一个支持适合公众和企业需求的全行业用例技术平台。下面所示的区块链参考架构将作为构建或实现全行业用例区块链应用程序的基础。该参考架构描述了一个分层的体系结构，它提供了满足企业需求的区块链应用程序所必需的组件和服务。基于不同的商业目的和业务对象，该架构可以用于开发包含单个或多个网络（涉及多个业务单元或组织）的区块链。在该参考架构指导下，开发者既可以实现许可链（即私链）应用程序的设计，也可以实现非许可链（即公链）的设计。



上图所示参考架构可用于构建任何区块链应用程序。该架构被划分为多个重要的逻辑层。这些层分别是应用层、智能合约层、集成层、分布式账本层以及覆盖全架构的安全层。接下来，让我们来了解每一层及其所包含的组件：

应用层

应用层是你的终端用户或客户端应用程序所在的层次。客户端应用程序通常通过触发交易来启动整个业务工作流。之后，该交易由节点调用智能合约层功能继续向下

执行。客户端应用程序可以使用任何软件编程语言实现，并且可以运行在各种操作系统上。应用程序既可以使用任何区块链框架实现所提供的命令行接口（CLI）工具，也可以使用特定于编程语言的软件开发工具包（SDK）与网络上的节点通信。随着区块链技术的演进早已超越其传统的基于数字加密货币的网络形象，我们看到越多越多不同类型的客户端和工具现已支持区块链框架。如今客户端应用程序还可以侦听发生在区块链网络上的各种类型的事件（event），并对这些事件执行必要的操作。这些网络事件可能是很简单的事件，比如仅仅是从网络向应用程序提供状态更新。在开发时，还可以使用一个单独的专用应用程序来监测区块链网络。

智能合约层

智能合约层的软件代码实现了区块链网络中的交易。这些代码是由区块链网络节点调用的关于业务规则或条件的一组逻辑集合。智能合约可以有自己的运行环境或虚拟机环境。这可以让它在安全的上下文中运行，就像在虚拟容器里一样。而且智能合约可以用任何一种流行的软件编程语言来实现，例如（但不仅限于）热门的语言 Java、Python、Go、JavaScript 和 Scala 等等。也可以将智能合约编写为一种服务（service），并将其放在注册表中，以便客户端以独立于位置的方式来查找相同的服务。注册表可以安全地被保护起来，并且可以控制访问，这样只有经过授权的客户端才能根据该合约来执行操作。还可以使用加密哈希散列算法来保护智能合约本身，使其内容（其形式是软件代码和相关元数据）成为机密。智能合约还可以被编写为事件（event）的形式来进行交易状态转换的通信或广播。该事件可以实现为合同本身的生命周期事件。客户端应用程序可以侦听这些事件并相应地对它们进行处理。

集成层

当今世界，在所有的颠覆性技术中，应用程序的集成和互联通信已经变得十分重要，因为现在没有一个技术平台可以孤立存在。区块链也同样如此。应该保证区块链网络能够访问自己网络之外的任何数据。这些数据可以为区块链工作流提供重要价值，可能是外部应用程序或外部系统的一部分。类似地，也需要保证外部系统能够与区块链网络进行通信。一种实现方法是设立一个外部事件 hub，该 hub 作为媒介，通过事件处理器与外部系统交换数据。而外部应用程序可以侦听来自该 hub 上的特定事件，并相应地执行某些任务。另一方面，智能合约软件也可以侦听来自外部系统的事件，并相应地执行业务功能。下面几小节解释了集成场景中一些有趣的其他用例：

人工智能（AI）集成

正如我们所了解的，区块链本质上是一个分布式账本，它采用去中心化和自动化的

方法来处理基于共识的交易结算过程。那么，又如何将人工智能应用在区块链中呢？人工智能的应用必须基于大量数据。而区块链本身就是一个包含大量交易的数据库，于是可以将其中的数据提供给诸如机器学习（machine learning）的人工智能分支应用来完成某些功能，例如，可以对数据应用复杂的算法来优化特定的业务功能。人工智能分支应用还可以用来改进整个业务流程或工作流。人工智能算法可以检测出明显的异常，并进行预测性建模或分析，从而找到能够降低交易成本和增加区块链网络中各方业务收入的那些指标。在需要自治工作的系统之间，也可以应用人工智能的解决方案来达成交易共识。总之，人工智能和区块链的强强联合可能会在未来真正地改变游戏规则。

云集成

还可以扩展区块链架构来实现在云上的组件托管，云可以提供诸如路由、数据转换、协议转换、扩展的证书授权中心（CA）等应用程序的集成服务。该组件还可以充当中间件，在云中提供“区块链即服务（blockchain as a service）”功能。在区块链实现中可以提供一个适配器，以便从区块链网络内部和外部连接到该中间件组件。区块链中间件组件可以托管在安全的“沙箱”环境中，也可以托管在一个安全的虚拟容器中。而外部应用程序可以通过该适配器，在获取访问区块链网络的有效证书后，与区块链中间件进行交互通信。

物联网（IoT）集成

新的一波关于技术集成的浪潮是区块链网络与任意可连接的设备进行通信。不同类型的物联网（IoT）设备或传感器可以将数据注入区块链网络，然后由区块链节点进行验证。可以实现一个标准化的中间件，它可以从设备获取数据，并根据区块链网络的需求执行必要的数据换算和格式转换。之后，区块链网络中的节点可以使用智能合约的特定共识算法来对这些数据进行验证。

注：有关区块链和物联网集成的更多细节，请参阅这篇概述文章。

分布式帐本层

这个分布式账本层是区块链架构的核心持久层。它提供了一个去中心化的分布式数据库，该数据库包含所有的交易条目。这些交易条目按其出现的顺序进行记录，并组成哈希散列块。因此，该数据库，或分类账，实际上就是交易的一个哈希块链，其中每个块都指向链中的前一个块。分类帐在区块链全网络中进行共享，这就意味着每个节点都有分类帐的副本，所以每个节点都能独立地对交易进行验证。当每个节点都同意并确认交易的真实性时，此时就宣告分类帐达成共识。区块链网络使用不同的共识算法来达成共识。共识算法是监管交易的一组规则和条件。为公众实现

的区块链网络，即公链，有一个无需许可的分类账，而在私链或联盟链（半公开，介于公链和私链之间）中，分类账可以实现为需要许可。在访问和管理交易的方式上，需要许可的分类账引入了某种形式的访问控制。

分类帐管道（Conduits）

对于许可链（私链）的区块链网络，开发者可以实现一个名为分类帐管道的模式。在区块链网络中，可以将这样的管道视为私有通道，这样甚至能在该网络中让两个或多个节点更私密地执行交易。这种节点必须是成员节点，并被专门授权对这些私有管道拥有使用权。可以将这些管道视为大型网络中的小型网络。在企业中实现区块链时，这种模式能进一步加强安全性。

共识算法

区块链网络通常由不受信任的匿名实体或节点进行监管。而区块链中的共识是在网络中提供信任机制的最关键因素。每个节点都可以用交易形式的数据来对区块链网络进行更新，而这些交易最终需要经过验证，然后才能作为区块链的一部分被正式记录在分类帐中。关于如何创建和验证交易块并实现区块链的信任机制，有多种不同的共识算法。

实用拜占庭容错算法（PBFT）这是基于多数表决的共识。网络中每个节点根据给定的规则或条件集更新和验证区块链网络。如果网络中的大多数节点在更新时反映了相同的结果，则宣告网络达成共识。可能会有少数流氓节点（Rogue Nodes）违反网络规则，但它们的表决结果不被接受，因为它违反了该算法给出的结果。该共识算法应该满足所有必要条件，并且所有的节点必须同意并执行相同的条件才能得到所期望的输出。

工作量证明算法（Proof-of-work，PoW）工作量证明是最早设计出来的传统算法之一。比特币的区块链网络和以太坊网络都使用了这种算法。与上面的实用拜占庭容错算法不同，工作量证明算法并不依赖于多数表决来达成共识，它是一个需要消耗大量计算资源的算法。只有计算能力更强的节点才能争得工作量证明算法的记账权。第一个完成指定任务并有正确输出的节点会赢得创建块的记账权利，并得到相应的报酬。工作量证明算法通常涉及到某种加密哈希散列算法，以实现所需的目标或结果。在我的免费教程中，第 2 章对工作量证明算法有详细讨论。

股权证明算法（Proof-of-Stake，PoS）前面提到，使用工作量证明算法需要巨大的计算能力，从而导致较高的能量消耗。这种情况可能并不适用。而股权证明算法通过提供一种称为用户权益的替代方法来克服这个问题。那些占据或拥有最高数字货币量（或某些资产）的用户会赢得在区块链网络中创建块的记账权利。因此，在

这种算法机制下，并不用需要花钱在升级节点的算力上，而是直接买下加密货币（或其他资产）来增持用户权益并争得记账权，从而取得对一个交易块的验证和创建的权利。

安全层

我们在前面的区块链其他组件部分也涉及了一些安全性的讨论。安全层是区块链架构中的重要组件之一。无论是公链还是私链，基于区块链的实施都需要保证安全性和共识策略。在公链中，每个节点都可以参与交易，而在私链中，由于有某种形式的访问控制，只允许被许可的节点参与交易。

区块链网络中的每个实体都必须进行身份绑定。在公链网络中，通常会限制只有参与交易的用户才能成为这样的实体，而在私链网络中，实体可能由组织、节点、用户以及在区块链网络中可以发挥作用的任何东西所构成。

对于私链网络而言，可以使用公钥基础设施（PKI）平台，在这个平台里，受信任的证书授权中心（CA）可以颁发加密证书。而这些加密证书可以采用证书和密钥的形式。私钥可用于数字签名，而公钥可用于验证。这种机制实现了一个可信网络，在该网络中所有参与者都知道他们是谁，也知道他们可信度的来源。既然现在区块链网络种的各方参与者都可以使用自己的加密证书，还有可能建立自己的证书授权中心（CA），所以至关重要的是，区块链的实现需要提供一种即插即用式的服务，或者是一个抽象的逻辑层，来有效地管理、测试和验证在网络中采用不同安全机制的各种实体。

简而言之，区块链安全层需要具备鉴权、访问控制、完整性、保密性、不可篡改性五大有效措施。

结语

区块链被认为是继互联网之后的下一波网络技术革命，在商业领域的潜力尤其巨大。区块链这种自我监管的环境，在身份管理方面提供共识和来源的支持，在安全性方面提供密码学和策略支持，这将为产生众多新一代应用程序铺平道路，而这些应用程序又会在未来为区块链网络提供更健壮的基础设施支持。如今已经有许多不同风格的区块链问世，从诸如以太坊这样的非许可分类账到诸如 IBM 超级分类账（HyperLedger）这样的许可分类账。而区块链的行业用例已经从以加密货币为中心的金融领域延伸到各行各业，如保险、供应链、医疗、物联网等。根据用例的类型，你可以选用非许可的区块链（公链）或许可的区块链（私链），甚至是二者的组合技术，即使用公共的共识机制来驱动私有的业务交易。

区块链式思维已经拉开帷幕，云、大数据、人工智能、物联网和分布式账本的组合力量将在未来带来更多创新的业务解决方案。