超级账本白皮书

翻译：周平、单旭（中国电子技术标准化研究院软件工程与评估中心）

摘要

本白皮书描述了区块链的行业应用案例，以推动形成新的区块链结构原理。另外，本白皮书根据这些应用案例，列出了针对区块链的基本需求和高级体系结构。本白皮书中所呈现的超级账本（Hyperledger）描述了区块链结构的演进，并作为商对商（B2B）、商对客（B2C）交易的一种协议。当在相同的网络中发生业务竞争时，Hyperledger 允许在符合规则的前提下支持各种需求。本白皮书后面所描述的内容包括智能合约、数字资产、记录存储库、去中心化的一致网络和密码安全。最后，本白皮书还描述了区块链的主要产品、各行业对性能的要求、身份验证、隐私和机密交易和可插拔的共识模型。

一、背景

区块链是一种新兴技术模式。这种技术模式能够快速改进银行、供应链以及其他的交易网络，在降低与业务运营相关的成本和风险的同时，能创造新的创新和增长机会。自 2009 年比特币在交易领域迅速崛起以来，许多商业组织和行业机构投入了大量资源来研究比特币的底层技术，从而传播这种广受欢迎但又颇具争议的加密币。

区块链是一种点对点（P2P）分布式账本技术。由于能够有效、安全地支持资产的发行、交易、管理和服务，区块链首先在金融行业得到了支持。在不要求中心控制点的情况下，区块链技术能够容易地建立成本合适的商业网络，这与记录系统（SoR）的生态中需要每一个成员维护自己的账本系统、审核与其他成员的交易进展形成了鲜明的对比，因为后者即低效、又昂贵，而且经常是非标准化的内部操作流程。

由于共享账本概念得到了商业世界的支持，区块链智能合约也引起了更多行业的关注。智能合约是商业规则的集合，是部署在区块链上，并由一组利益相关方共享和共同验证。在自动化商业流程中，智能合约是非常有用的，而且诚信可靠，允许所有利益相关方共同处理和验证合约规则。

比特币及其他加密货币的设计是完全开放、去中心化和非授权的：任何人在没有确定身份的情况下都能参与，而且只需要贡献一点时间完成计算周期就行。在区块链的比特币模型中，没有中心机构来发放许可，因为网络是非授权的。由于需要无数的工作量计算来证明，比特币的运行是昂贵的。

Hyperledger 是对传统区块链模型的革新。即使希望授权的区块链作为起点，但 Hyperledger 通过提供一个模型，在某种程度上是允许创建授权的和非授权的区块链。另外，Hyperledger 通过一个提供针对身份识别、可审计和隐私的安全和健壮模型，使得缩短计算周期、提高规模效率和响应各个行业的应用需求成为可能。

二、为什么是一个新的架构

作为一种新兴技术，现有的区块链实现不能满足商业交易中各种复杂的应用需求。可扩展性挑战、机密和隐私交易支持的缺失以及其他限制，使得很多关键业务应用不能投入使用。为了及时部署弹性平台、支持跨行业的应用需求，需要轻量级、模块化和通过配置插入各种组件（交易验证器、阻止协商一致等）支持可扩展的平台。为了满足今天市场的各种需求，Hyperledger 的设计以行业应用为重点，解决了现有技术的缺点，并拓展了业内先行者原来的工作。

三、我们的愿景

通过 Hyperledger，我们规划了针对区块链技术的未来愿景。我们相信区块链技术将会对现实生活的很多方面产生根本性影响，包括从商业到数据存储和其他事情。基于这一点，我们认为针对区块链/分布式账本技术制定健壮的和开放的标准是必要的，因为，这能推动这样的技术在主流商业化领域得到应用。我们相信未来世界将建立许多内部互联的分布式数据库和区块链，每一个分布式数据库和区块链都将满足特定用户的需求，但也要求与其他的账本进行通信。

因此，我们认为任何针对区块链技术的开放标准都必须尽量模块化。未来让开发人员能够按照自己的意愿来回替换不同版本的各种区块链组件，必须建立这样的标准。例如，一些区块链应用案例在要求快速一致算法的同时要求更多的可信，而某些应用案例可能不要求速度但要求更加可信。密码算法、智能合约和数据库存储是需要实现“即插即用”的其他特征。

模块化的另一个重要方面是使外部开发更容易。如果某个公司能够改进 Hyperledger 的某些模块，这个公司就可能做到并按自己的意愿发布这些改进的模块。实际上，公司或个人都应该能构建全部的模块（能够按要求一起使用，或

者与其他 Hyperledger 组件实现“即插即用”），以容纳或与 Hyperledger 实现互动。本质上，不使用 Hyperledger 框架中的任何核心组件也能够构建区块链。

我们对 Hyperledger 的长期愿景就是它包含丰富的、易用的 API 和数量庞大的核心模块，这样就能容易实现开发和互操作。虽然我们希望核心的 Hyperledger 模块能够满足尽量多的应用案例，但我们也知道 Hyperledger 的核心内容是不可能覆盖每个行业的应用案例。然而，我们的 API 应该足够灵活，使得不使用 Hyperledger 核心组件构建的应用案例能很容易地与核心的 Hyperledger 组件和区块链实现互动。

我们不可能考虑到 Hyperledger 和通用区块链技术将来所有的使用方式，因此，为了能够容纳将来未知的开发，Hyperledger 的设计是尽量模块化和可扩展。除此之外，Hyperledger 的模块化应该能让更多的人围绕 Hyperledger 工作。我们希望这种模块化的方式允许发明或开发新的区块链技术的人们发现：使用或与 Hyperledger 合作是很容易的。

than the stakeholders for the contract or the asset being transferred.

我们相信，针对任何区块链结构根本需求的一个方面就是网络中任何一方行为的识别和模式必须不能被未授权方通过检查账本就能查明。我们也期望某个需求允许区块链用户确认业务逻辑和/或交易机密的其他参数、使他们对任何人都是不可访问的，而不是合同的利益相关方或资产被转移。

Hyperledger 应该为核心协议之上轻松实现的各类丰富应用提供支持。这必将要求支持各种交易语义、密码算法、协商机制和数据库存储协议。例如，加密的 Hyperledger 应该包括所有的加密、签名和更高级的功能密码，从简单的、快速的对称加密到复杂的功能加密和基于属性的签名。这些基本的技术原理应通过配置来支持重要的商业交易，例如不同程度的授权交易的不可改变性和可审计性。

总的来说，我们希望 Hyperledger 是一个易用、十分有用和健壮的平台，任何对构建区块链软件的机构和个人都可以把它作为核心代码。尽管由于实际考虑不足，Hyperledger 针对每个潜在用户和应用案例可能缺乏这种理想的功能，但我们的目标就是使 Hyperledger 尽可能接近这种理想的状态。

四、行业应用案例

我们已经编制了一套本质上支持下述抽象应用案例的区块链初始需求。这些应用案例并不代表 Hyperledger 的所有应用案例，而是一组展示 Hyperledger 某些能力和特征的典型样本。

（注：这些应用案例为体系结构设计和测试驱动的开发提供指南。虽然还是一项推进中的工作，这些应用案例应该是所有贡献者一致认同的，无论是内容还是堆

栈中排名的优先次序。如果您觉得这些内容有欠缺，可以提出改变建议。理想的情况是不超过四个抽象应用案例中有三个是首选。）

4.1 金融资产处置

诸如证券这样的金融资产必须能在区块链网络上实现去中心化，这样所有同种资产的利益相关方就能直接访问这一资产，进而发起交易，获取相关信息而不需要通过层层中间环节来进行了。交易可以在利益相关者之间商定的时间期限内解决，交易可以实现实时结算，利益相关者都可以实时掌握资产情况。对于任何种类的资产，利益相关方应该有权增加商务规则，这样也能通过自动化逻辑的应用来降低成本。创建资产的人必须像用例保证的那样，实现资产和相关交易规则保密或者公开。例如，资产创建者应该能够创建资产，而这一资产的交易记录以及交易模式对于利益相关者之外的群体是不可见的，甚至创建人本身也不能访问。

4.2 协作

公司 A 发起一个协作的事件请求，无论这个过程中涉及多少中间环节（如代理接收/支付，CSD，ICSD，本地/全球保管银行，资产管理公司等）公司 A 需要将邀请的完整细节信息实时发送给利益相关方。一旦利益相关者作出交易决策，这个决策也需要被实时处理完成(包括作为协作事件一部分的新增份额)。如果需要，投资者的响应会被保密，这样他们就可以基于价值作出决策，而不用担心自己的操作行为带来的负面影响。

4.3 供应链

区块链的框架必须满足供应链中每一位参与者的如下需求：录入并追踪原材料的来源；记录部件生产的遥测数据；追踪航运商品的出处；保证包括成品生产、储存、销售及后续事宜在内的所有数据都不被篡改。除了之前描述的商务合约和资产存管模式的特征，供应链这一用例更多强调的是其深度可搜索性，保证能够在过去的层层交易中追溯所需记录。其核心是为每一个基于其它部件构成的商品创建出处（可追溯的源）。

4.4 主数据管理

主数据通常并不是交易信息数据，而是行业信息的关键和基础组成部分，如：customer（客户）、employee（员工）、supplier（供应商）、product（产品）、location（地址）和 contract（合同）等。授权认证机构发起变更并对变更进行校验，维护核心数据的唯一性和真实性可以解决许多数据质量和一致性问题。

4.5 共享经济和物联网

共享经济将在许多传统行业领域产生可带来营收的新型产业，如：智慧城市、互联家园、自动化、运输、医疗、分销、建筑、教育、健身等领域。
交易中的个体、组织以及监管机构并不总是相互信任。善加利用基于分布式账本的区块链技术有助于解决交易各方相互间的信任问题。区块链技术同时也有助于

交易的实时处理和资产状态的实时访问。灵活的部署模型，可插拔的共识机制，私下交易以及保密合约对于超级账本的部署都很重要。
了解更多关于用例和需求的细节，以及如何将这些用例嵌入到基于区块链技术的系统中，请访问：
https://www.google.com/url?q=https://github.com/hyperledger/hyperledger/wiki&sa=D&ust=1466139262975000&usg=AFQjCNEbquySu8Mky1D8rZnWvxF3rswKlQ

五、典型需求

我们接下来描述超级账本的典型需求。这里描述的典型需求满足了多种用例和商务情境，我们希望产记账本将来能够发展出更多的特性。

首先，超级账本最关键的需求是架构。正像我们反复强调的，不同的应用会对机密算法、一致性算法和数据库存储方式有着不同的需求。然而，我们基于架构细化一些更具体的需求，可以广泛应用于更多领域。

私下交易和保密合约

超级账本最终应该支持多种加密工具和方法，确保满足相应的加密和隐私管理需求。这些工具用于确保诸如身份识别、交易属性、智能合约状态等信息的真实性，同时不会侵犯信息的私密性。

与那些金融领域的用例不同，某些用例（如物联网）需要性能优化的基本保密功能，其加密和共识算法需要兼顾基本的加密功能和复杂的定制需求。

身份识别和审计

不考虑私下交易和保密交易，超级账本使用基于 PKI（公钥基础设施）的加密算法实现了交易中的身份识别和审计功能。

超级账本对用户和交易相关者除了单纯提供基于 PKI 的身份识别功能还应该支持对这些访问和识别操作的归档功能，包括交易相关者之间的加密请求，以便实现对涉及所有权变更的相关用例进行基于文档的审计追踪。

除了主动进行身份识别，超级账本也允许用户在特定情况下隐藏身份识别操作，仅当需要的时候才提供证明。当然，这已经超出了传统的身份识别概念。此外，PKI 非常灵活，允许用户根据特定的需求选择不同强度的加密措施。

互操作能力

在松耦合的网络中，独立的网络相互间不需要了解彼此的运行细节。然而，这样的独立网络也需要具备一定的共性，以实现彼此间正确的信息交换。尤其是对着

区块链技术的普及，应该考虑各种不同的区块链系统相互间的信息交换操作。各类区块链网络实现上的差异以及其演进和不断变化的特性会导致实现的高度专业化。制定专业的通信分类标准，创建在多种网络间通信的通用语言将是一项漫长而艰巨的工作。

区块链技术在设计和实现上存在差异，当不同服务彼此间交互操作，互操作就产生了。

超级账本定义可在两个或多个系统(组件)间进行信息交换，并使用交换的信息。为实现跨行业和跨用例的广泛应用，超级账本支持两个或多个区块链间进行信息交换的协议功能。

可移植性

超级账本项目通过从其核心组件接口中提取的增值系统实现移植操作。例如，智能合约就可以不做任何变更地移植部署。可移植性的增值系统，诸如：API（应用程序编程接口）库，GUIs（图形用户接口）开发应用，扩展库等，保证了超级账本的增值系统可以跨版本使用、实现和部署，同时也保证了超级账本项目的功能在异构环境下的大型区块链网络中得以实现。

六、体系结构

图 2 展示了 Hyperledger 所参考的架构，包括四个大类：身份识别服务，策略服务，区块链和智能合约。这些分类都是逻辑结构，而不是将组件划分成独立的进程、地址空间或（虚拟）机的物理描述。

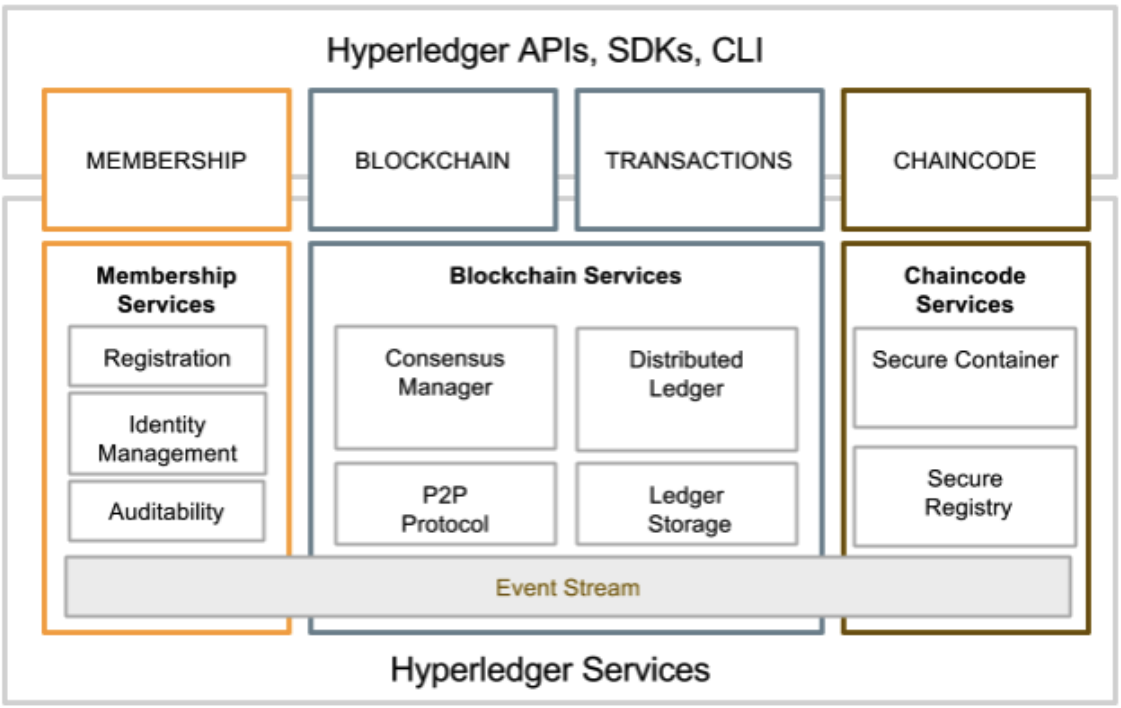


图 2：Hyperledger 参考架构

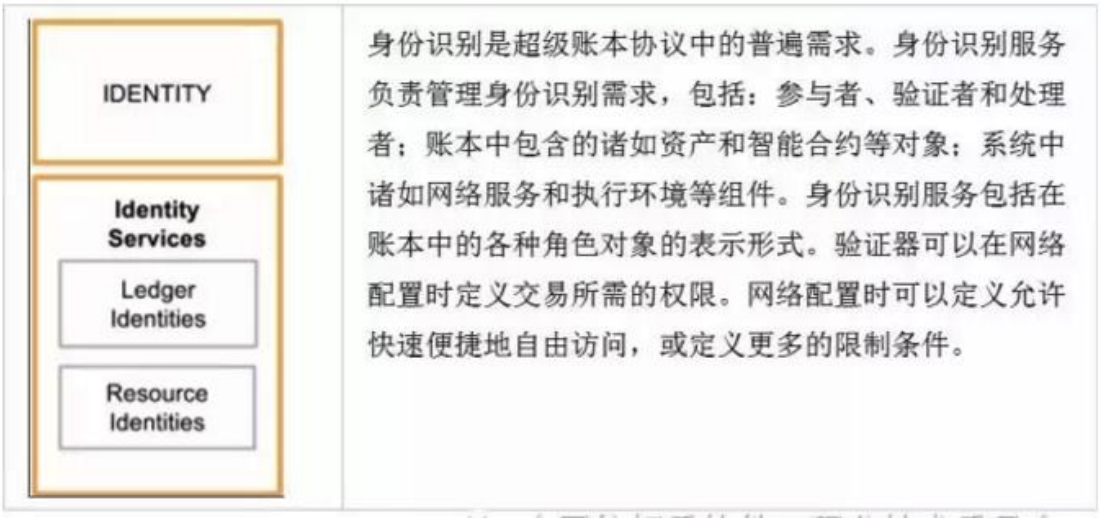
身份识别服务负责管理诸如资产、智能合约这样的实体、参与者和分类帐对象的身份识别。(参与者通过注册获取身份,之后通过授权机构发放的密钥进行交易。)

策略服务负责管理访问控制、隐私、联盟规则、共识规则等。

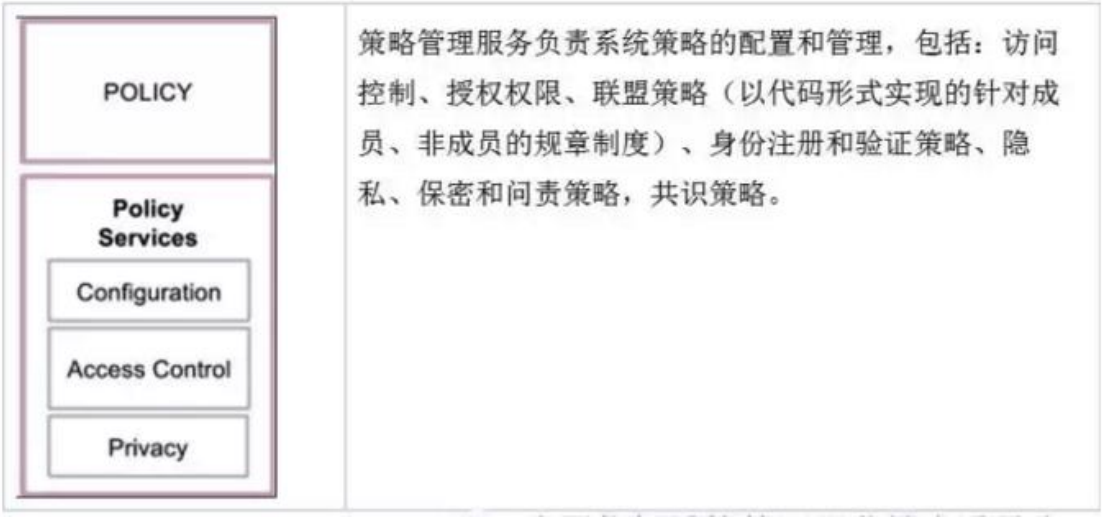
区块链服务负责通过点对点通信协议管理分布式账本。经过优化的数据结构可以有效维护在众参与者间复制的整体状态信息。不同的共识算法或将嵌入到每一个配置中，以保证高度一致性（通过 BTF 算法处理错误，通过崩溃容忍机制处理延迟和中断，或借助工作量证明方案应对审查。）

智能合约服务负责提供安全又轻便的方式供智能合约在验证节点上运行。

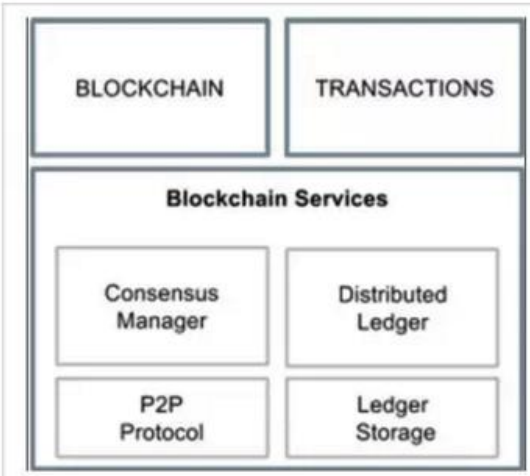
6.1 身份识别服务



6.2 策略管理服务



6.3 区块链服务



区块链服务包括三个关键组件：点对点(P2P)协议、分布式账本和共识管理器。

点对点(P2P)协议支持的功能：双向数据流、流量控制和连接的请求复用。最重要的是，它可以在现有的互联网基础设施中使用，包括：防火墙、代理服务器及安全设备。这个组件定义了对等节点所使用的信息，可以是点对点，也可以是组播。

分布式账本通过对交易的处理和校验、更新和维护账本中对象的状态来管理区块链以及整体状态信息。

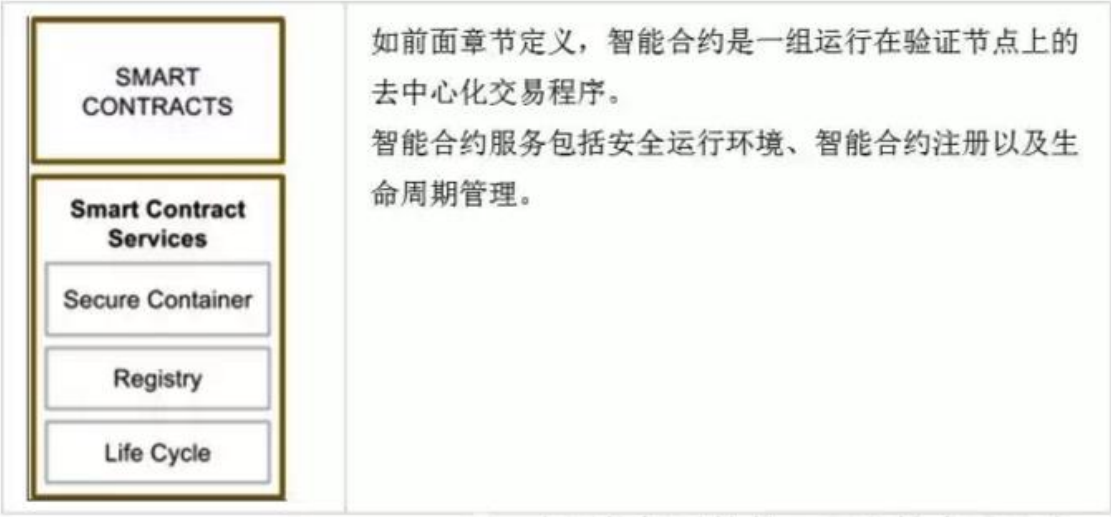
- 有效计算每个区块后部的整体数据集的哈希加密值。
- 当某个节点状态不同步时，向数据集有效传递数据变化量。
- 尽量减少对每个节点操作所需的存储数据的数量。

分布式账本使用数据存储维护数据集，同时建立内部的数据结构区别不同的状态，以此满足上述三个属性。大文件使用链外存储，不记录在账本中。它们的哈希函数值作为交易的一部分被存储在数据链中，以此维护文件的完整性。共识管理器是共识算法和其它超级账本组件间接口的抽象定义。共识管理器接收交易请求，借助相关算法判断如何组织以及何时执行交易。交易的成功执行将导致超级账本状态发生改变。

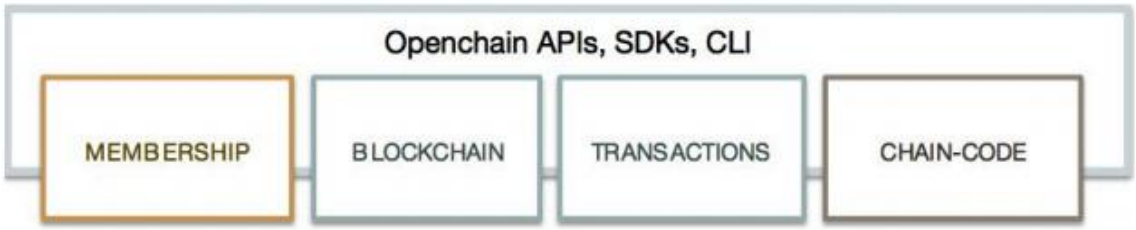
通过模块化的可插拔共识功能，超级账本支持为评估和记录特定系统风险而设计的各种共识模块。

超级账本提供 pub/sub（消息的发布/订阅）模式的事件管理框架，这样外部应用就可以监控和收到超级账本的事件告警。

6.4 智能合约服务



七、应用编程接口



超级账本的特色之一是提供了一套易用、可灵活扩展的 API 接口。 超级账本的每个模块都清晰完整地定义了相应的 API 接口，因此这些模块可以实现“即插即用”。例如共识算法的 API 支持用户无需修改算法代码就可以在各类用例中使用这一算法。完善的 API 接口为超级账本支持各类用例提供了有力保障。

此外，非模块对模块通信的外部 API 接口设计更便于普通开发人员在超级账本顶层编写代码。

一整套完全独立的 API 接口、智能合约模块以及共识协议模块是保障参与者能够在整个生态系统中提供贡献的基础。这一特性保障了整个生态系统的快速成长。

八、网络拓补

理论上讲 Hyperledger 的的网络拓扑应该是完全不同的：特别是参与者可以通过云服务操控各种类型的对等节点，包括验证节点，或者参与者本身就是验证节点。Hyperledger 运行在不可知的底层网络结构中，我们无法得知究竟谁在使用这些节点设备。

假如云节点是主服务节点，那么就必须考虑使用更加有效的加密解决方案避免云服务器中的信息被恶意泄露。

有些部署的 Hyperledger 可能会面临较大的系统变化，导致节点间通信延迟。网络失效，节点失效，因此网络的冗余性和可恢复性在部署之初就应加以考虑。

九、结论

Hyperledger 的任务是将区块链技术引入主流产业市场。回顾了可行的区块链解决方案，也了解了业界领先者及技术推广者给出的相关用例后，我们相信区块链将会成为至关重要的技术模型，推动众多工业和企业进行革新。

我们注意到，业内急需一套为企业打造的区块链架构，做到既高效又可扩展，并且能够支持企业级的加密和隐私保护。此外，我们还发现针对众多的区块链用例目录需求需要不同的底层实现。为挖掘区块链技术的潜力和创建适应不同用例的标准，我们设计 Hyperledger 框架时兼顾了灵活性和可扩展性。

参考资料

[CL02] Miguel Castro and Barbara Liskov, Practical Byzantine Fault Tolerance
[N09] Satoshi Nakamoto, Bitcoin: A Peer-to- Peer Electronic Cash System
[Eth] Ethereum Whitepaper