分布式应用账本

（DAppLedger）

白皮书

中国区块链技术和产业发展论坛

2017年12月22日发布

摘 要

本白皮书基于国内外区块链技术和应用发展现状，提出中国区块链技术和产业发展论坛建立分布式应用账本（DAppLedger）开源社区的愿景。同时根据《区块链 参考架构》标准和国际标准化的相关成果，介绍了DAppLedger采用的架构和关键特征。本白皮书参考国际上开源社区的运营模式和经验，描述了DAppLedger遵循的多维社区治理模式和科学治理理念。此外，基于区块链的应用实践，将区块链应用的实施流程分为应用需求形成、功能组件分析、关键技术分析、应用设计、应用实施和应用运营等阶段。最后，介绍了DAppLedger下的三个项目：BCOS、AnnChain、Ontology Zero。

目 录

目 录

1 背景

1.1 区块链发展现状

区块链是一种在对等网络（也称分布式网络、点对点网络）环境下，通过透明和可信的规则，构建可追溯的块链式数据结构，实现和管理事务处理的模式，具有分布式对等、链式数据块、防伪造和防篡改、透明可信和高可靠性等典型特征。

当前，区块链技术和产业发展的机遇和挑战并存。一方面，全球主要国家的相关政府部门、企业和研究机构等不断加大对区块链技术和产业关注和投入力度。区块链产业参与主体逐渐壮大，从金融服务到智能制造、供应链管理、社会公益、能源管理等各行各业都在探索区块链的应用。全球范围内区块链技术创新不断，应用的广度和深度逐步提升，形成了一批骨干企业，围绕以开源社区为代表的平台，相关技术不断取得进步，产业发展生态初步形成，产业快速生长。另一方面，现阶段区块链产业的发展存在多技术割据、新型安全挑战，以及监管融合、业务创新动力不足、应用发展不均衡等问题，技术发展和应用落地面临一系列障碍。

1.2 开源社区运作

区块链技术的起源和发展都与开源社区相互关联，很多区块链项目发源于开源社区，并在社区中发展壮大。目前，具有代表性的区块链开源项目有两类：一类是源自于技术社区的开源项目，这类项目以公有链为主，具代表性的是比特币开源社区和以太坊开源社区。另一类是由传统组织发起的区块链项目，这类项目以联盟链为主，例如Linux基金会发起的超级

账本项目。

当前区块链技术的发展面临着缺乏统一标准、技术体系复杂、开发模式单一、应用集成能力不足等问题，急需构建面向具体行业、面向应用场景、拥有组件化开发平台的开源社区，以开发针对特定场景和行业的解决方案，建立面向应用集成、交互操作的软件框架。并在此基础上促进全行业范围内的优秀应用解决方案向其他领域的扩散和推广。

为此，中国电子技术标准化研究院联合国内重点企业成立了中国区块链技术和产业发展论坛（China Blockchain Technology and Industrial Development Forum，CBD-Forum），共同开展区块链技术和应用发展研究工作，在此基础上发布了《中国区块链技术和应用发展白皮书（2016）》以及《区块链 参考架构》团体标准等成果。同时CBD-Forum发起建立了一个开放式的社区，社区中文名称为“分布式应用账本”，英文名称为“Distributed Application Ledger”，缩写为“DAppLedger”。未来社区将以成员自主开发的底层平台为基础，逐步建立多平台运营模式，在应用集成过程中探索最优架构。

2 DAppLedger的愿景

在工业和信息化部、国家标准化管理委员会的支持和领导下，DAppLedger的愿景是：

推动全国乃至全球区块链发展。区块链作为“互联网+”时代构建高可信分布式应用的底层平台，对发展数字经济、拉动信息消费升级具有重要的技术支撑作用。在政策环境不断优化、市场需求持续释放的同时，我们也清醒地认识到，当前区块链的应用仍然面临一系列挑战。其中，缺乏统一的底层技术平台是最主要的挑战之一。构建DAppLedger的核心目的就是吸收国内优秀的区块链技术成果，汇聚行业智慧，打造统一的区块链底层平台，逐步完善区块链发展生态，更好地服务于区块链技术研发和应用推广。

制定开放的区块链标准。DAppLedger的建设依据CBD-Forum已发布的《区块链 参考架构》标准，同时积极支持国际标准化组织ISO/TC 307（区块链和分布式记账技术技术委员会）制定参考架构、分类和本体、隐私和安全、智能合约、互操作等方向的国际标准，并率先实践国际标准。除此之外，DAppLedger将通过模块化、统一API（应用编程接口）和数据格式等，逐步形成标准化的区块链底层平台。

实现区块链系统的模块化，支持互操作和可移植。DAppLedger将提供高度模块化、可配置和可扩展的区块链底层平台，以满足各种应用场景的应用需求，并吸纳更多开发者贡献和发展标准化的平台。尤其是应用开发者可以针对不同的应用场景和应用需求选择合适的核心模块，快速构建上层应用，从而降低区块链应用开发难度，提高研发效率，同时实现高度的可维护性和可移植性。

推动区块链核心技术发展。开源社区能提供一个集中的技术生长土壤，通过DAppLedger在多个领域的应用渗透，促进区块链系统所依赖的基础组件、协议和算法相关的技术，例如加密算法、隐私保护、共识机制、智能合约等技术的研发和创新，推动不同技术的选型和应用走向成熟。

支持围绕区块链的创业创新。通过DAppLedger集中创新资源，培育优势项目，通过黑客松、开发大赛、孵化器建设等活动，搭建覆盖技术展示、交流合作和项目孵化等功能的区块链创业创新平台，吸引更多企业和个人加入，开展多种形式的区块链创业创新活动。

服务制造业与互联网融合发展。区块链对于传统制造业向智能制造转型价值巨大，然而，由于应用场景宏大，复杂性高，应用需要更多资源支持，要求多方协作的程度更高，对于底层平台的质量、安全性和互操作性等要求也更高。DAppLedger希望通过更加适合制造业的区块链底层平台的培育，以及相关的应用推进活动，推进区块链在制造业与互联网的融合发展中取得实质性进展。

3 架构

DAppLedger孵化的项目应参考《区块链 参考架构》以及ISO/TC 307最新标准化成果中的体系架构设计，实现核心功能组件，并遵循以下基本原则：

- 组件化设计，面向具体应用场景的功能组件实现封装和集成；
- 可插拔，保障新组件易于添加和扩展；
- 迭代发展路线，随着标准化的推进和应用场景的丰富，不断升级、演化项目以适应商业化的需求。

3.1 参考架构

DAppLedger遵循的分层框架包括5层，此外还有一个跨越各层的跨层功能集合。

其中，分层框架的5层分别是：

- 用户层
- 外部交互层
- API层
- 平台层
- 基础层

跨越各层的功能称为跨层功能。

整体框架如图3-1所示。

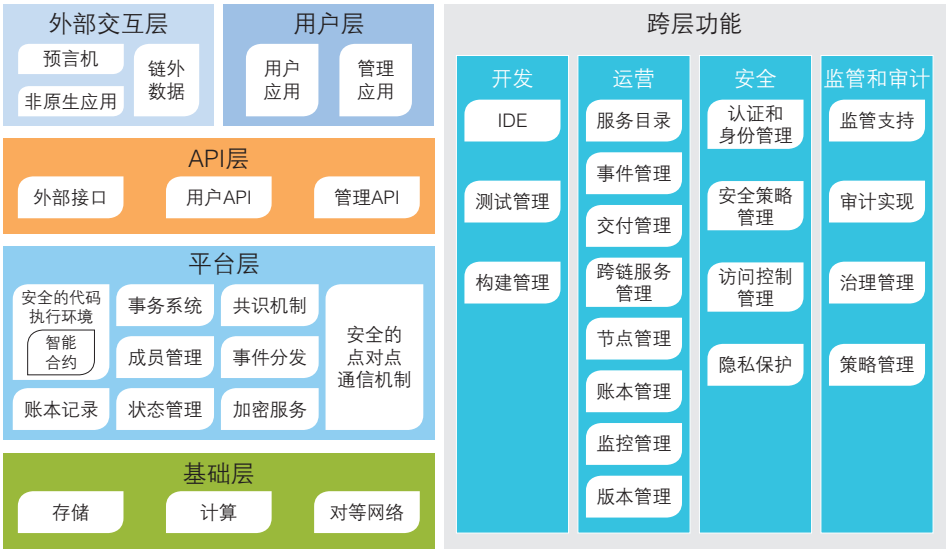

图3–1 DAppLedger分层框架

3.1.1 用户层

用户层是面向用户的入口。通过该入口，使用区块链服务的用户可以和区块链服务进行交互，执行相关的管理功能，维护和使用区块链服务。用户层也可与其他资源层通信，提供对跨层区块链系统的支持。用户层包含用户应用和管理应用。

- **用户应用：**独立于区块链之外运行的应用程序，作为用户使用区块链服务的客户端，支持执行用户相关的特定功能。
- **管理应用：**独立于区块链之外运行的应用程序，作为管理员维护区块链服务的客户端，支持更新和调整系统与应用的功能。

3.1.2 外部交互层

外部交互层包含为了实现业务目标，需要与区块链进行通信的外部系统，它包含三类服务：预言机、非原生应用和链外数据（源）。

- **预言机：**一种向区块链提供可信外部数据的服务。

- **非原生应用**：与区块链进行交互的外部应用程序，主要用于发送或接收数据。
- **链外数据**：在区块链外部保存并与区块链相关的数据存储。

3.1.3 API层

API层通过调用平台层的功能组件为应用程序、用户和外部系统提供可靠、高效访问区块链的能力，同时，提供统一的访问和节点管理功能。

- **外部接口**：链外访问服务提供安全访问区块链外部功能（例如可信数据源）的API接口。
- **用户API**：提供访问用户特定功能的API。
- **管理API**：提供访问管理员和操作者功能的API。

3.1.4 平台层

平台层基于基础设施层提供的硬件或网络基础设施连接到API层实现相应功能，平台层支持的具体功能有：

- **安全的代码执行环境**：在安全的代码执行环境下，事务可能调用需要安全环境的智能合约函数。安全的代码执行环境是服务器端区块链业务逻辑的托管环境，如使用一个安全容器。该环境包含一组签名的代码执行组件，如安全操作系统、用于区块链支持的编程语言的库、各自的运行环境等。
- **智能合约**：智能合约记录在区块链系统中任何节点，是区块链平台中在安全环境下执行的计算机程序。
- **账本记录**：账本记录是一种可保存（业务）事务的最终记录的信息存储功能。账本记录的数据存储功能支持编写和查询各种类型的数据，在区块链系统的运行过程中生成账本、事务信息等，技术实现可以是关系数据库、键值对数据库、文件数据库等。
- **事务系统**：事务系统是管理向账本系统添加事务的组件。

- **成员管理服务：**成员管理服务是在区块链系统中管理成员身份、隐私、保密和可审计性的服务。会员服务只适用于被授权的区块链系统。
- **状态管理：**状态管理是跟踪在账本上持有资产状态的组件，该状态在新的交易记录提交到账本时更新。
- **共识机制：**共识机制是一组规则和程序，允许区块链系统维护和更新分布式帐本，并确保账本中记录的可信度，即其可靠性、真实性和准确性。共识机制在不同的区块链系统中，有许多其他的共识机制在使用。共识机制包括但不限于Paxos算法、拜占庭容错、授权证明、燃烧证明、容量证明、所有权证明、股权证明、零知识证明、工作量证明等。
- **事件分发：**事件分发组件处理在区块链平台中生成的事件的分发，如由执行智能合约生成的事件，用户应用程序可使用该组件来向用户发出事务完成的信号。
- **加密服务：**加密服务组件为区块链系统提供了访问所需加密算法的权限，可以通过提供算法的硬件或软件的接口来实现。哈希函数和数字签名是区块链系统常用的加密算法。哈希函数通常用于保护账本免受修改，对账本中信息的任何更改都将导致计算出的哈希值与之前账本的哈希不同，每次将事务添加到账本时都会计算新的哈希值。数字签名确保接收方接收交易记录不会被第三方更改或伪造，同时确保交易记录来自发件人（用私钥签名）。
- **安全的点对点通信机制：**安全的点对点通信组件可处理网络上节点之间的通信，从而启用分布式账本的操作。

3.1.5 基础层

基础层提供了区块链系统所需要的运行环境，包含计算资源、存储资

源和网络资源。该层为区块链系统提供了基础支撑，它可以以云计算形式提供，也可以以本地服务器设备形式来提供。

- **存储：**存储账本和其他数据的功能应满足以下要求：对等网络中的每个节点都可以部署和使用；可以分布式部署或本地部署；可以支持适当的数据主权；能够高效、安全、稳定地提供数据编写和查询服务。
- **计算：**计算功能为区块链系统的运行提供了执行能力，包括但不限于容器技术、虚拟机技术和云计算技术，该功能应向区块链系统中的每个节点提供运行环境。
- **对等网络：**区块链系统节点的对等网络，可支持区块链系统与用户层和外部交互系统中的实体之间的通信。

3.1.6 跨层功能

跨层功能提供跨越多个功能层次能力的功能组件。跨层功能组件分为开发功能组件、运营功能组件、安全功能组件以及监管和审计功能组件。

3.1.6.1 开发

开发功能组件支撑区块链服务开发方的活动，包括服务实现的开发、构建管理和测试管理。开发功能组件由以下组件构成：

- **IDE（集成开发环境）：**IDE功能组件提供了开发智能合约、区块链和相关应用程序（包括开发支持模块）的工具。IDE功能组件支持使用区块链运算符提供的功能，包括通过API进行访问、节点管理和事件分发功能。IDE允许在区块链平台层的API以及基础结构层中调用函数。IDE组件支持生成配置数据，以便开发智能合约，同时支持由智能合约配置脚本和组件。
- **构建管理：**构建管理功能组件用于构建可发布的软件包，可以提交给区块链节点的所有者或操作者，并部署在生产环境中。它包含用

于智能合约实现的软件、配置元数据和配置脚本。

- **测试管理：**测试管理功能组件支持对区块链系统的功能进行测试，该组件可生成测试报告，并向节点所有者或操作者提供系统软件。一般情况下，测试在一个独立测试环境中进行，该环境是对生产环境的模拟。在不影响生产的情况下，也可以在生产环境中进行测试工作。测试环境应该由区块链的操作者或合作方提供。

3.1.6.2 运营

运营功能组件包括一组与操作有关的管理功能，这些功能用于管理和控制提供给用户使用的区块链服务。运营功能组件包括：

- **服务目录：**服务目录功能提供了一个特定区块链系统、操作者或节点的区块链功能、智能合约和服务，也可包含API的列表。该列表包括部署和操作区块链智能合约的技术信息、服务或API。
- **事件管理：**事件管理功能提供了捕获事件和报告问题的能力，并通过分析来管理问题。事件和问题可以通过区块链节点、区块链操作者或区块链用户来检测和报告。
- **交付管理：**交付管理功能提供了区块链系统交付的管理功能，它以系统实现和访问端点的形式提供。同时，此功能提供了必要的工作流，确保以正确的顺序提供元素。
- **节点管理：**节点管理功能提供区块链平台节点管理的实现，包括逻辑或虚拟系统上的性能和可用性的实现。
- **账本管理：**账本管理功能提供对分布式账本的管理。
- **区块链系统管理：**区块链系统管理功能提供对区块链系统的管理，特别是在性能和可用性上。
- **监控管理：**监控管理功能包括用于响应平台和环境中的更改的监视、分析和自动化工具，包括响应所需的系统容量的改变以及错误分析。

- **版本管理：**版本管理功能提供对节点和区块链系统的管理代码基础和实现工件的管理。

3.1.6.3 安全

安全功能组件主要为区块链各功能组件层以及层间的协议提供保密性、完整性、可用性和隐私保护等安全属性的保障。这些安全功能广泛用在用户和节点身份认证、交易协议设计、链式数据组织、通讯信道加密和应用数据访问控制之中。安全功能组件应至少包括以下功能：

- **认证和身份管理**

身份验证和身份管理功能提供用户的身份验证过程，以确定用户是否对资源具有访问和使用权限，从而使区块链系统访问控制策略能够可靠并有效地执行。

- **安全策略管理**

安全策略管理功能为用户提供访问或使用资源的权限，通过建立一组规则，使用户在安全区域中必须遵循所有与安全相关的活动。

- **访问控制管理**

访问管理组件用于提供对区块链系统的特定功能的访问控制，包括应用于API层中各种接口的访问控制。

- **个人身份信息保护**

个人身份信息保护组件可对区块链系统处理的任何个人身份信息提供适当保护的功能。包括对个人身份信息的标识和分类、加密应用、对个人身份信息的生命周期管理（包括删除早期和不再需要的任何个人身份信息）、提供访问数据对象的个人身份信息。

3.1.6.4 监管和审计

监管和审计功能组件根据相关治理要求使区块链服务符合可监管与可审计的特性，避免区块链网络游离于法律法规以及行业规则之外，成为洗钱、非法融资或犯罪交易的载体。应至少包括以下功能：

- **监管支持**

在区块链系统中，监控支持功能主要用于满足环境、系统、可用性、灾难恢复、系统运行和维护以及支持功能的要求。由于行业监督员与监督方法的不同，所涉及的职能的深度和广度不尽相同。

- **审计实现**

审计支持功能主要用于实现审计内部控制、责任识别、事件可追溯性和区块链系统的其他要求，它需要有效的技术手段和业务部门制定的标准来进行准确的审计管理。

- **治理管理**

控制监管过程中对违反策略的提醒，防止产生异常或错判。

- **策略管理**

策略管理功能为区块链系统及其管理提供定义、更新和访问策略。这些策略包括区块链系统本身及相关的业务、技术、安全、隐私和身份验证。

3.2 关键特征

以下7个区块链系统设计关注点适用于3.1参考架构描述范围内的关键功能组件：

- **模块化**

为了提高区块链应用的研发效率、可维护性和可移植性，区块链系统的核心功能应实现模块化、可配置和可扩展，以便快捷地构建上层应用。

- **高性能**

性能指的是某个区块链系统在一段约定的时间内执行相关功能的能力。从客户角度看，性能通常是区块链系统的一个关键属性，也是当前关注的焦点。构建区块链系统，提供区块链服务，应注重提升区块链系统的吞吐量，以满足主流交易网络高并发的性能要求。

- **可互操作性**

区块链语境下的互操作指：客户与区块链服务之间按照规定的方法交互和交换信息并获得可预测结果的能力，以及服务提供方之间协同工作的能力；要求区块链服务按照商定的规范运营，并采用通用的分布式账本技术，避免使用专有的或高度专业化软件；互操作还包括客户与服务提供方的管理设施的交互。此外，在业务运用中，互操作还会涉及到传统IT应用与区块链服务之间交互的能力，应采用统一的通信协议和API进行交互。实现不同区块链间的互操作，应采用有效的通信协议、统一的API和区块数据格式，以及高效的连接机制。

- **数据一致性**

数据一致性是实现区块链服务互操作和可移植的前提。实现数据一致性，应采用科学合理的数据算法，降低数据同步延迟，保证数据的一致性，避免造成数据混乱和失准，并减少意外分叉带来的风险。

- **安全和隐私**

区块链服务的安全和隐私需求宜包括：认证、授权、可获得、保密、不可抵赖、身份管理、完整性、审计、安全监控、事故反馈和安全策略管理。区块链服务安全和隐私功能应包括：存取控制、保密、完整性和可获得性，保障数据存储、数据传输和数据应用等多个方面的安全和隐私。

- **经济性**

经济合理是指构建区块链系统时，在满足需求的前提下，技术选型应尽可能降低技术复杂度，规避高能耗的技术方案。

- **安全可信**

建设区块链系统，应优先采用安全可信的软硬件产品。

4 治理模式

DAppLedger参考国际上众多成功开源社区的运营模式和经验，综合考虑组织结构、项目管理流程、社区应用推广、知识产权与协议等方面，制订了一个多维的社区治理模式和科学的管理与治理理念，以应对项目和开发者不断增加、技术路线日益复杂等挑战，实现可持续发展，引导社区良性发展，孵化更多区块链应用。DAppLedger社区结构如图4-1所示。

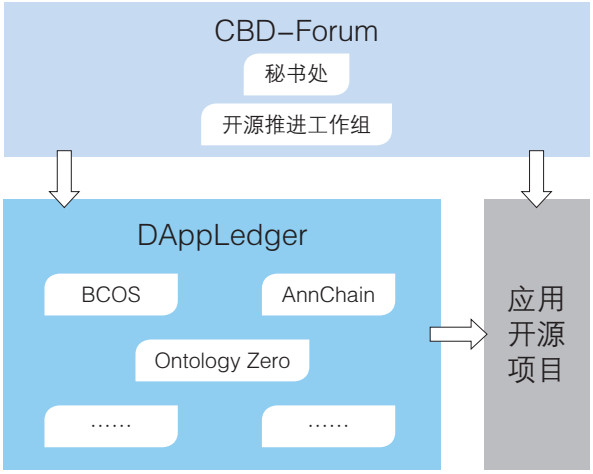

图4–1 DAppLedger组织结构

DAppLedger由CBD-Forum发起并负责战略制定、管理和总体运营工作。DAppLedger由遵循DAppLedger章程的前提下各自独立运行的多个开源项目构成，由项目发起和运营管理方负责相应项目的建立、运营和管理。此外，用户和开发者通过具体项目的使用和更新，参与开源社区的建设。具体参与方和相关活动包括：

- **CBD–Forum秘书处：**负责制定DAppLedger的工作程序和管理制度，协调和组织社区相关活动，API、测试等相关标准。
- **CBD–Forum开源推进工作组：**主要负责制定和提出DAppLedger的技术方案和应用推广方案。并且定期评估各个项目发起和运营管理方对于已有技术方案和应用推广方案的执行情况，保证方案的落实和执行。
- **项目发起和运营管理方：**负责项目的建立、日常运营管理和应用推广，负责保证其发起的一个或者多个开源项目的社区活动良好运转。按照自愿原则，CBD-Forum秘书处可协助项目发起和运营管理方开展日常运营管理和应用推广工作。
- **用户：**指以使用DAppLedger所提供的软件或项目资源为主的个人或团体。用户以错误报告和功能建议等形式向DAppLedger的对应开发者提供反馈，对开发活动做出贡献。
- **开发者：**指通过向DAppLedger提交代码和文档的方式为社区项目做出贡献的个人或团体。开发者被赋予代码仓库的写权限，拥有开源社区提供的统一的邮件地址，并保证邮件能够及时处理。开发者在处理补丁时可独自做出决定，并接受项目发起和运营管理方的监管。

5 应用路径

为了提高开发效率和产品可靠性，有必要采用成熟可靠的开源区块链基础协议来进行区块链应用研发。区别于传统的应用研发，基于区块链的应用开发实践和实施流程可分为应用需求形成、功能组件分析、关键技术分析、应用设计、应用实施和应用运营等阶段（如图5-1所示）。

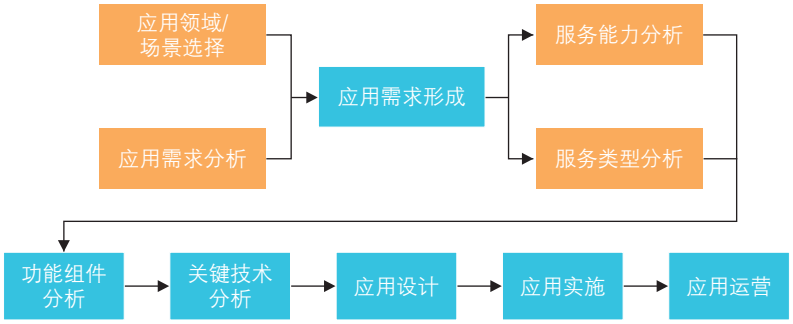

图5–1 应用实施路线

5.1 应用需求形成

在形成区块链应用需求阶段，包括应用需求分析和应用场景选择两个方面。用户分析自身所在行业的应用需求，形成行业可能的应用需求列表，结合自身需求，形成具体的区块链应用需求。

5.2 功能组件分析

对功能组件的分析可参考3.1中对DAppLedger架构的描述。

5.3 技术选型

在技术选型过程中，需要重点关注的实践点有：

- 所选平台适应的链类型（公有链、联盟链、专有链）与应用场景的匹配程度；
- 所选平台使用的开源协议与应用商业化匹配程度。

5.4 应用设计

应用设计主要包括业务架构设计、逻辑架构设计、物理架构设计、数据架构设计、账户架构设计五个方面。

- **业务架构设计：**包含设计应用的角色和场景匹配方案、设计应用的营运模式，以及设计应用的盈利模式等关键点。
- **逻辑架构设计：**包含设计应用与区块链网关对接方案以及设计区块链网络监控方案等关键点。
- **物理架构设计：**包含确定部署节点类型（全节点、验证节点和同步节点等）、设计区块链节点的物理位置分布，以及设计区块链节点的高可用方案等关键点。
- **数据架构设计：**包含明确应用上链数据和非上链数据边界需求、设计区块链账本数据存储方案，以及设计区块链账本归档数据存储方案等关键点。
- **账户架构设计：**包含设计账户标识用户友好性方案、设计账户密钥安全性方案，以及设计账户结构等关键点。

5.5 应用实施

在应用实施的过程中，需要重点关注的实践点有：

- 开发测试环境和生产环境进行隔离；

- 链上数据归档，设定合理的定时任务；
- 需要高性能、大容量磁盘；
- 考虑流量入口的带宽；
- 根据网络的运行稳定情况，动态调配环境资源。

5.6 应用运营

在应用运营过程中，需要重点关注的实践点有：

- 应用营销和运营人员尽早介入熟悉应用；
- 需要关注相关开源社区的最新动态；
- 运营账户分权（多签名）管理；
- 自动监控网络的运行稳定情况。

6 总结

本白皮书描述了区块链行业的现状与技术特点、CBD-Forum的现有基础和建立开源社区的必要性，同时提出DAppLedger的愿景，即：推动全国乃至全球区块链发展、制定开放的区块链标准、实现区块链系统的模块化，支持互操作和可移植、推动区块链核心技术发展以及支持围绕区块链的创业创新和服务制造业与互联网融合发展。另外，本白皮书列出了DAppLedger采用的架构与治理模式，给出了区块链应用实施路径。

未来，CBD-Forum将加快推进社区建设和重点项目的孵化等工作，具体任务包括：开展国内外开源技术、开源社区运营模式和机制研究，以推动社区发展；促进利用区块链技术研发相关创新应用，积极转化创意设计为实际项目方案，孵化区块链开源项目和推广应用；建立相关合作机制，开展区块链开源国内外合作；培养区块链开源人才，扩大区块链产业参与群体，提高产业从业人员技术能力。

附录A

DAppLedger项目简介

A.1 BCOS平台

项目基本情况

BCOS（BlockChain OpenSource）是由深圳前海微众银行、上海万向区块链股份公司、矩阵元技术（深圳）有限公司联合开发的区块链底层平台，于2017年7月31日实现完全开源。BCOS致力于打造一个深度互信的多方合作共同体，进一步推动分布式商业生态系统的形成。

BCOS平台聚焦于“B”（business）端客户，为企业级应用服务的区块链技术平台，帮助各行业的用户构建商用区块链服务，主要覆盖金融、健康医疗、供应链、工业、物联网、能源服务等多领域。

BCOS平台通过集成身份认证、非对称加密算法、引入技术治理功能、支持全面监管审计功能等举措，可支持多个行业的应用需求。

BCOS的特点

- 提供全面的监管和审计支持模块，满足业务合规要求；
- 提供对全网商业机构节点的准入控制、CA身份认证、账户管理体系和安全监控功能，支持分布式商业运作的技术治理需求；
- 实现共识机制的插件化，可支持PBFT、RAFT等多类共识算法，便于匹配不同业务场景需求；
- 采用分布式数据存储架构，支持海量数据容量与弹性扩容能力，并提供高强度加密存储功能和配套密钥管理机制，提升数据存储安全；

- 支持对全网所有节点同时进行灵活的配置修改，配置数据保持高一致性；
- 提供基于密码学的隐私保护功能，支持分布式商业中的保密数据交换；
- 支持全方位的安全防护机制，兼顾物理安全、传输安全、存储安全、网络安全、密钥安全等。

BCOS的价值理念

BCOS遵循以下六大价值理念（DRIVES）：

- 分布式（Distributed）：通过分布式的、多方对等参与的区块链技术，重构安全、可信任的共享账本，帮助各机构在分布式商业场景中实现专业分工与协同合作，完成资源的最优配置与聚变效果。
- 监管科技化（Regtech-ready）：引领监管创新与制度创新，支持监管机构在区块链网络中部署监管节点及在此之上的大数据监控平台，可实时进行数据采集报送、数据溯源及业务风险管控。
- 变革创新（Innovative）：数字化时代即将全面主宰经济与社会的每个侧面，BCOS致力于提供未来前沿的基于区块链技术的分布式商业公共基础设施。
- 价值驱动（Value-driven）：构造可交换、可分享的分布式信息网络与价值网络。
- 广泛适用（Extensive）：支持金融服务、工业互联网、供应链、健康医疗、物联网等多个行业领域。
- 安全可控（Secured）：作为中国企业联合研发的全球化平台，完全实现安全可控，既深度符合国情，又具备全球领先的实力。

BCOS的应用

可应用于溯源、物流、供应链金融等领域。

A.2 AnnChain平台

项目基本情况

AnnChain是由众安信息技术服务有限公司开发的区块链底层平台，适用于公有链和联盟链等多种应用场景，具有模块化设计，可快速构建各种区块链应用；支持JVM、EVM和原生等多种合约执行引擎；支持子账本模式和区块链数据归档，满足区块链扩容需求；支持GPU硬件加速。完善的监控、运维和开发套件等配套基础设施；支持监管节点，可通过权威节点进行紧急事件响应。已应用于多个上线产品和业务系统中，表现稳定可靠。

AnnChain平台特点

- 提供链上交易的授权与监管，提供证书发放，权限管理；
- 拥有专业的密码学相关功能，并提供不同场景的隐私解决方案；
- 提供交易与智能合约的解释与执行，交易管理，比如提供外部数据服务；
- 支持系统和硬件环境的监控，提供多种可视化管理工具，满足管理和维护需求；
- 提供文件存储和结构化数据存储与查询，在节点间同步全局状态；
- 采用一种基于PBFT的共识算法，算法生成区块是经过投票过程产生，生成区块的时间平稳。

AnnChain的优势

- 基于企业级的分布式账本完善体系，全面支持企业级系统业务集成与安全运维。
- 无知识产权风险，企业对平台应用自主可控。
- 开源社区持续增强平台功能，所有社区成员同步得到各类技术增强与新功能实现。
- 广泛应用在各类业务领域，任何潜在的问题、新的技术功能应用都

能得到充分的验证，为提升平台健壮性、技术创新性提供了良好保障。

AnnChain的应用

可应用于防伪溯源、共享经济、供应链金融、保险等各类业务领域。

A.3 Ontology Zero平台

项目基本情况

Ontology Zero（本体）项目于2014年开始设计与研发，经过持续的研发与改进，逐步形成了以基于区块链数字资产应用为基础，可以灵活扩展到各类基于分布式账本平台的业务应用支持的基础平台，并且持续地结合分布式账本领域相关技术的发展、不同业务领域的应用发展创新，开发与增强平台功能与企业级工具，形成了可落地的企业级解决方案。Ontology Zero项目汲取国外主流区块链系统（超级账本、以太坊、Tendermint）的优点，基于国内分布式账本平台体系DNA（Distributed Network Architecture），融入多项创新技术，形成一种全新的区块链网络架构。Ontology Zero项目一方面具备高性能的特征，另一方面实现区块链可配置，打通各种类型的区块链实现信息互联和价值互通。目前，万达网络、分布科技、复星金服等企业与个人已加入Ontology Zero项目开源社区，已有超过80名社区成员可给Ontology Zero项目提供技术支持。Ontology Zero项目发起成员已申请了近20项国内外区块链底层及应用的发明专利。

Ontology Zero作为DNA2.0增强平台，致力于融合最前沿分布式记账技术，密切结合各行业业务发展，形成原创创新开源的技术体系和开放的合作机制，为各行业机构与业务模式提供完整、健壮、灵活的企业级分布式账本框架。Ontology Zero项目汲取了多个区块链优秀的设计思想及成熟的技术，在共识算法、数据传输、分片存储、国密算法、区块管理、消息队列等各方面都做了相应的创新及落地实践。Ontology Zero网络架构的

设计结合国际及国内区块链参考架构标准，进行了矩阵化的架构体系设计，包括5个业务层次体系（用户层、数据交互层、API层、分布式账本平台层、基础设施层）和4个垂直跨层次体系（身份管理与授权体系；安全管理体系；应用开发服务体系；系统管理体系；监管治理体系）。以Ontology Zero项目作为基础模板，可以快速搭建企业级的区块链平台，支持物理机、虚拟机、云、容器等多种部署环境，帮助各行业的用户快速构建商用区块链服务。

Ontology Zero项目特点

- 提供混合认证模式，同时支持传统节点的准入控制、CA身份认证、账户管理体系和安全监控功能和新型的去中心化身份认证模式；
- 共识算法组件化：方便切换不同共识算法实现，目前可支持高性能的Raft算法、dBFT共识算法以及新型的可验证随机函数VRF算法，基于业务对性能和隐私的要求，实现对公有链、联盟链、私有链等不同类型通用支持；
- 融合去中心化存储和分片存储的支持，具备海量数据容量与弹性扩容能力；
- 支持可视化和配置文件结合的策略管理，对区块链体系运行中的各类规则与策略进行通用配置，并可扩展结合特定业务领域的业务规则策略的配置，配置数据保持高一致性；
- 提供基于密码学的隐私保护功能组件包，包括零知识证明、属性加密等技术手段支持安全的数据协作；
- 提供高性能智能合约环境WASM及通用轻量级智能合约虚拟机AVM的支持，具有高确定性、高并发性、高扩展性等优点，并与其他社区分布式应用相兼容；
- 提供实时监管与审计的服务接口。

Ontology Zero项目优势

- 基于企业级的分布式账本完善体系，全面支持企业级系统业务集成与安全运维；
- 无知识产权风险，企业对平台应用自主可控；
- 开源社区持续增强平台功能，所有社区成员同步得到各类技术增强与新功能实现；
- 广泛应用在各类业务领域，任何潜在的问题、新的技术功能应用都能得到充分的验证，为提升平台健壮性、技术创新性提供了良好保障。

Ontology Zero的应用

可广泛应用于供应链、贸易金融、股权登记与转让、交易结算、物联网、医疗制造、工业制造、征信等领域，在数字身份、合同存证、溯源等应用场景已有成熟案例。

附录B

参考文献

[1] 区块链 参考架构，中国区块链技术和产业发展论坛，2017年5月

[2] Blockchain and distributed ledger technologies — Reference architecture，2017年10月

[3] 中国区块链技术和应用发展白皮书，中国区块链技术和产业发展论坛，2016年10月