

本体框架白皮书

Version 2.0.0

2019/07

摘要

1. 本体是一个支持众多信任协作场景的基础性体系，根据场景和应用范围的应用会持续地进行各类模块与协议的扩展。本框架白皮书仅描述本体在当前阶段的规划，后续会根据实际项目进程进行持续更新。

长期以来，人们通过“技术”、“法制”、“社群”等不同维度和方法来建立信任，但这样多来源、多系统和多方法的单点式信任协作也带来了非常高的协作成本，阻碍了信任协作的深度和广度。虽然互联网技术日新月异，但关于信任的很多痛点至今依然存在，如信任源分散化、数据零散化、个体角色缺失、身份认证不准确、虚假信息难判断等。在社会治理、经济协作和金融服务等各种协作过程中，每天为“信任”付出着大量的成本。

去中心化、不可篡改的区块链在一定机制上建立起了特定场景下的技术信任，但要和现实世界的业务场景结合起来需要更多的融合机制。构造起一个结合多样性信任和一体化应用的信任机制，成为对新一代“信任”基础体系的追求。

本体致力于建立一个体系化、流程化和一体化的信任生态，本体将作为信任生态体系的基础设施和连接器，为信任源的有效协同、数据源的互联互通、为各类分布式应用服务提供完整的底层技术基础设施。¹

接下来的章节将重点针对本体项目的整体框架进行阐述。

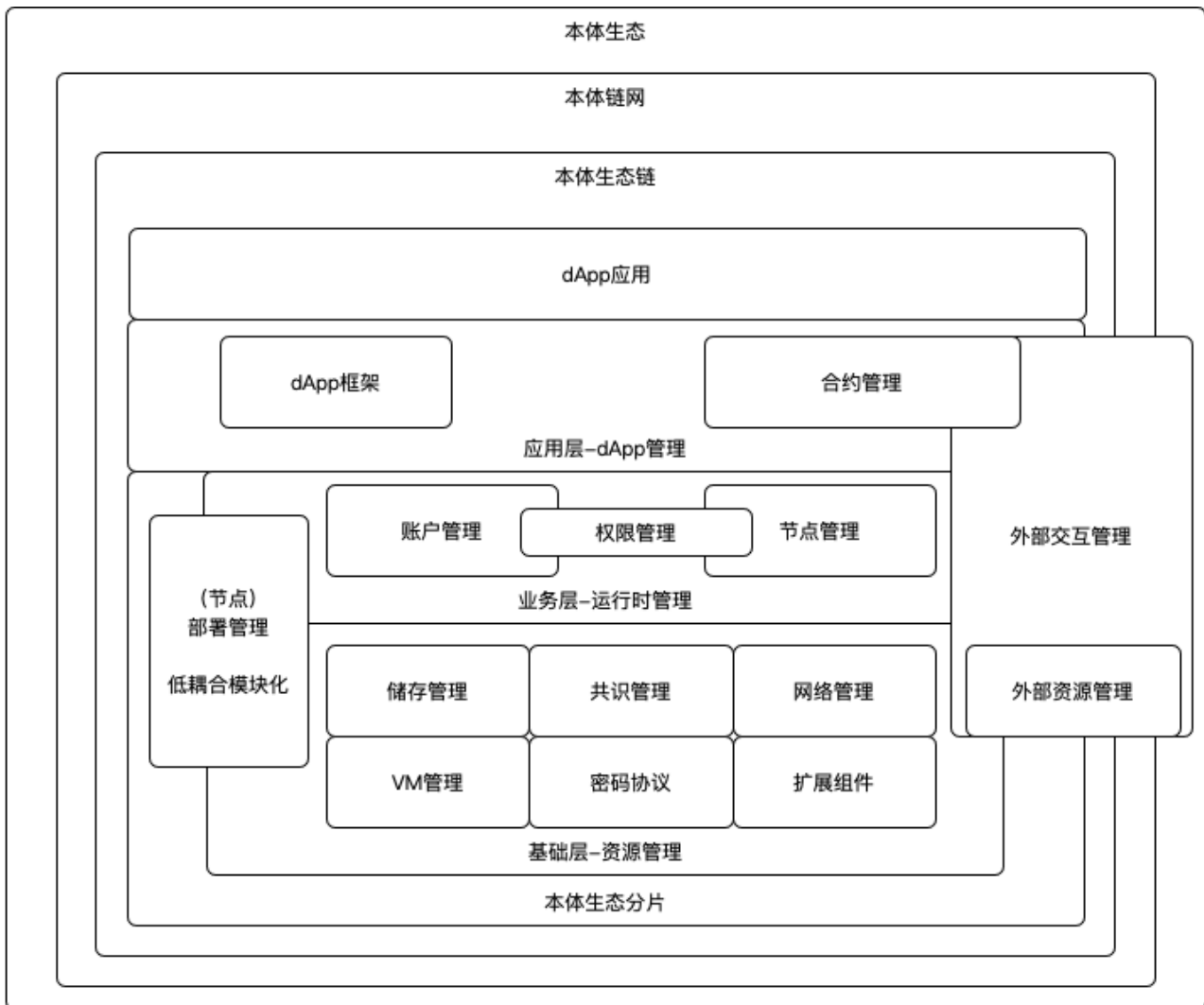
目录

1、概述.....	1
2、术语说明.....	5
3、本体生态概述	9
4、本体治理模型	11
5、本体经济模型	13
6、本体技术架构	14
7、后记.....	15
联系我们	16

1、概述

本体（Ontology）是一个多链、多系统融合的链群结构，除了本体本身的分布式账本框架可以支持实现不同治理模式下的区块链体系，也可与来自不同业务领域、不同地区的不同链，通过本体的各类协议进行协作，形成各类异构区块链和传统信息系统的跨链和跨系统交互映射。因此，本体又被称为“本体链群”或“本体链网”，即区块链之间的互联网。

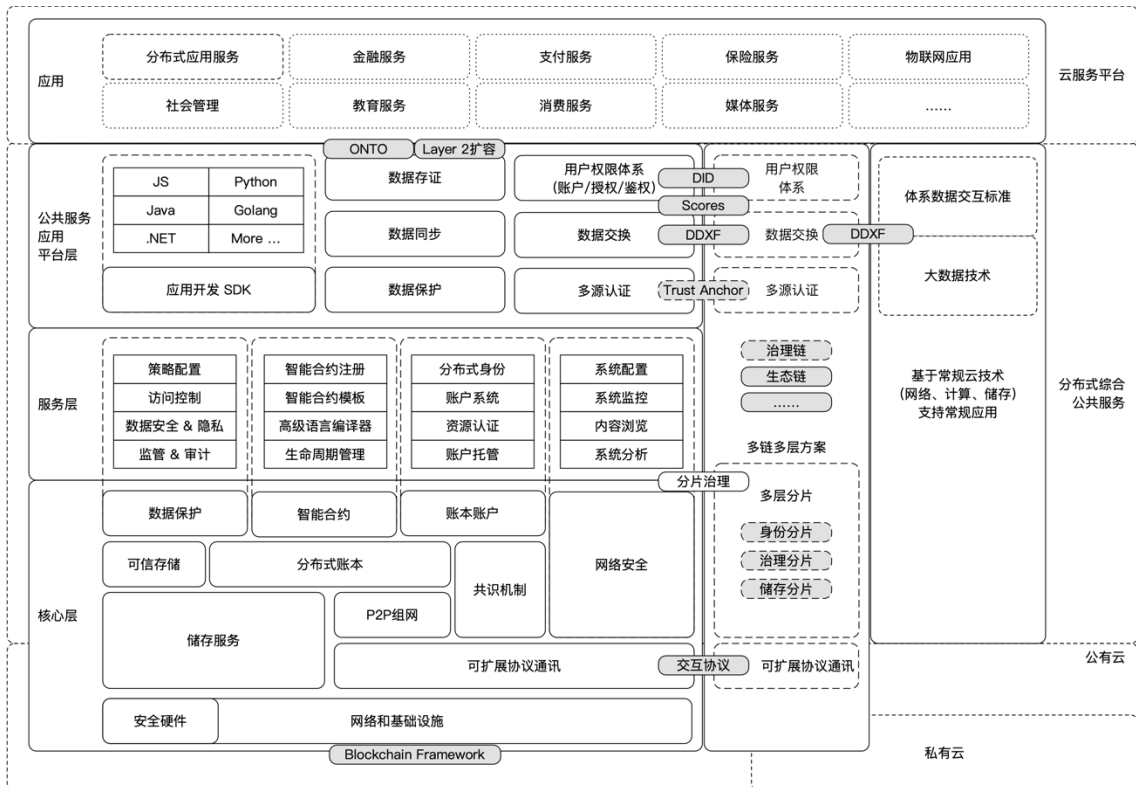
逻辑架构如下图：



图：本体逻辑框架

- 本体生态通过本体多链实现，多链网络结合外部资源；
- 多链网络由本体生态链组成，一条链只适用于一类治理模型，生态链基于不同的治理模型的需求，包含业务链和功能链。本体生态链支持跨链交互；
- 生态链支持多个生态分片，满足技术上的扩容需求。从状态分片、交易分片和网络分片三个维度进行事务扩容的支持。支持跨片事务；
- 本体链和分片之上部署分布式应用；
- 本体基础设施的应用层支持分布式应用的实现，本体应用层框架同时提供分布式应用的管理。其中，本体应用层信任框架提供分布式应用的可信管理；
- 区块链支持业务运行。本体基础设施业务层保证分布式应用执行过程；
- 本体基础层管理本体生态链基础资源。

技术架构如下图：

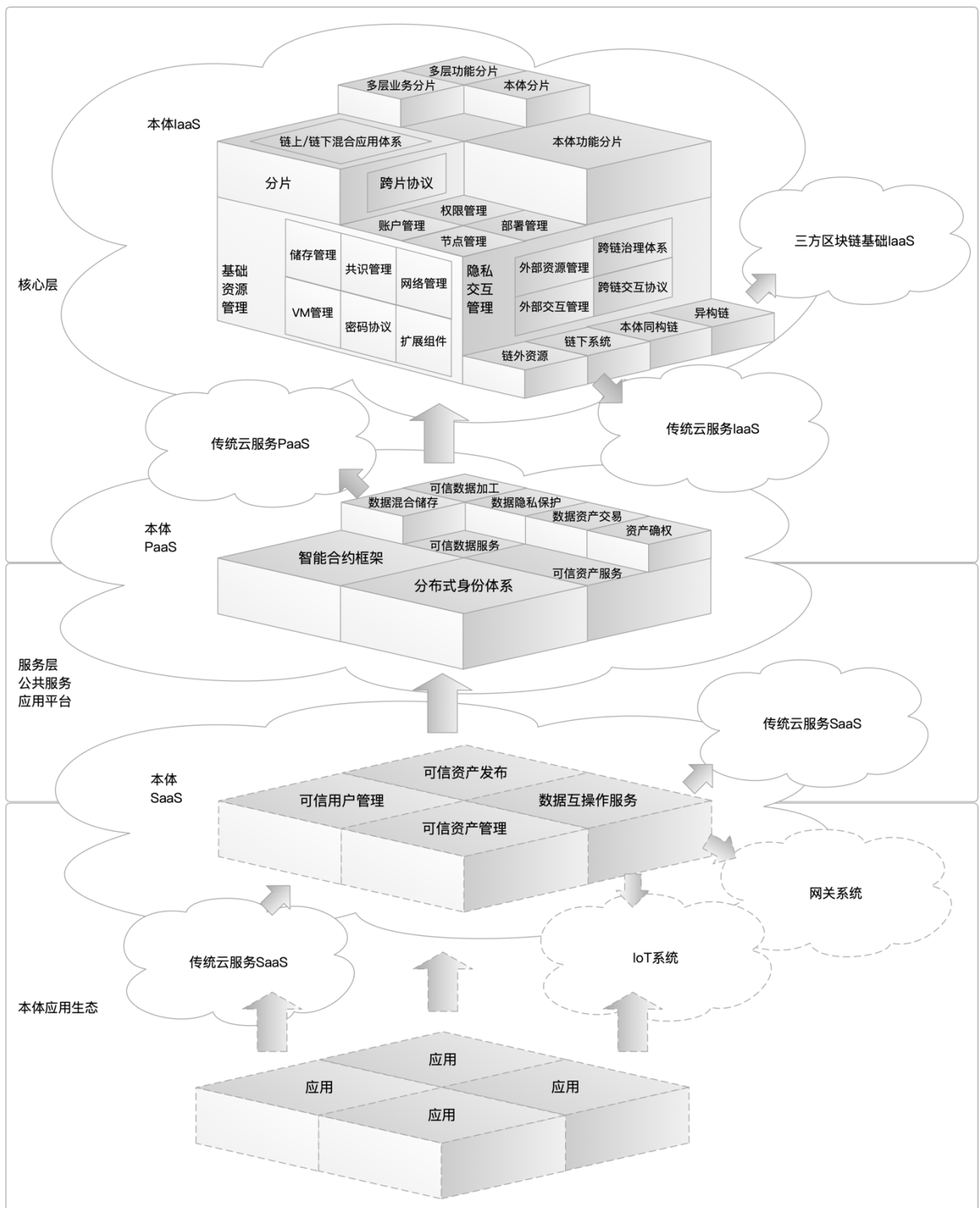


图：本体技术框架

技术角度，本体作为区块链基础设施提供方，提供从区块链构建到用户终端应用整套解决方案，实现本体信任生态。涵盖了区块链核心层、服务层、应用平台层，支持跨链的多链方案。

- 本体核心层。作为本体生态区块链基础设施，本体核心层提供完整的分布式账本体系，包括核心分布式账本、智能合约体系、安全体系。分布式账本技术的去中心化、共同维护、不可篡改等特性是本体实现分布式多方信任的关键。分布式账本包括共识、智能合约体系在内的实现，并为分布式信任框架、上层应用提供共识、存储和智能合约支持。本体核心层支持本体同构链跨链方案；
- 本体服务层。基于本体核心层，本体提供模块化服务层工具，使得整个架构具备更好的伸缩性及灵活性；
- 本体应用层。本体应用层为本体提供上层基于身份和数据资产的应用平台，给出通用信息资产化、资产交易的解决方案，打造本体公共服务平台。本体应用层支持跨链调用和异构链跨链方案；
- 本体多链多层方案。区块链特别是公链的运营需要兼顾经济模型和治理模型的设计，在单一链中，只使用一类治理模型。为了满足不同业务跨地域的治理差异的需求，本体提出多链解决方案；同时，区块链的实现需要在扩展性、性能、安全性之间平衡，以满足不同的性能和安全性业务需求。针对不同业务的基础设施需求，本体采用出多层分片的解决方案。通过多链多层方案，为不同性能和业务需求打造性价比更高的生态区块链基础设施。

本体提供高效可信的弹性基础设施，本质是打造可信生态，本体的多链多层混合应用的设计本质是为本体可信应用生态服务。区块链特别是公链服务，其本质是为链上应用服务，是一种去中心化的“资源租用机制”的体系。因此，本体基础设施作为一种“可信”云，为本体生态持续提供服务。



图：本体服务框架

未来，本体还将联合开发者社区、业务合作伙伴不断丰富功能组件，推动本体生态发展。

2、术语说明

本体链群

也称为“本体链网”，是由多个不同领域、不同地区的链组成链网结构，共同构成整个本体。链群每条链使用独立的分布式账本，通过交互协议进行协作。

本体分布式账本

由本体的分布式账本/区块链框架构建的一个或多个核心公共服务基础链，为本体中的各项服务提供基础性的分布式账本和智能合约体系等服务。

分布式一致性账本

一种增量修改式的数据存储结构，由去中心化的点对点网络中的节点共同维护，具有数据公开且历史数据难以篡改的特点，为本体提供可信存储及智能合约支持。

共识

账本节点按照特定的协议确认写入账本的数据，以保证账本的一致性。

智能合约

记录在账本中的可执行代码，通过账本节点上运行的智能合约引擎执行，每次执行的输入输出可记录在账本中。

实体

参与进行交互行为的个体，在本体区块链中以 ONT ID 作为身份标识。

本体身份标识

ONT ID 是一个去中心化的分布式标识协议，用于本体上对人、财、物、事的身份关联，具有去中心化、自主管理、隐私保护和易用等特点。

分布式信任框架

本体实现分布式信任的核心逻辑层，主要包含分布式身份标识协议、分布式信任模型及分布式信任传递体系等部分。

信任锚

被一定的实体群体所信任的实体，作为一些信任传递链的源头，为本体提供基础身份认证服务。

本体功能链

本体链群中提供特定功能的某些区块链，比如可信执行环境 TEE 等。

本体生态链

使用不同治理模型的区块链项目，参与本体生态，统称为本体生态链。

本体治理链

本体链群中负责整体治理的区块链，即本体主链。

跨链

让信息和数据从一条链到另外一条链的区块链技术，更多的情况是指一条链上的资产交换成另一条链的资产的区块链技术。

同构链

运行相同区块链协议的区块链网络。

异构链

运行不同区块链协议的区块链网络。

网络节点运营者

参与本体网络节点运营的本体生态参与者。

同步节点

在本体网络中对外提供区块同步和交易请求转发服务的本体生态节点。本体同步节点不需要质押。

候选节点

网络节点运营者通过质押的方式加入到本体网络的本体生态节点。

共识节点

在本体网络负责共识区块的本体生态节点。所有共识节点都来自本体候选节点，并随本体共识周期的切换而变化。

PoS

权益证明。基于 PoS 共识的区块链网络中，所有成为“验证者”的节点都能够获得生产（或者发布）区块的权利，其概率取决于其拥有的“权益”多少。

P2P

对等网络，是一种在对等者之间分配任务和工作负载的分布式应用架构，是对等计算模型在应用层形成的一种组网或网络形式。

分片

采用分而治之的方式，对当前区块链的网络，交易和状态进行划分，增强区块链增加交易处理和验证的并发度，是实现区块链扩容的一种方式。

可信执行环境

一种隔离的安全执行环境，可以保证内部代码和数据的隐私性和完整性。

身份认证

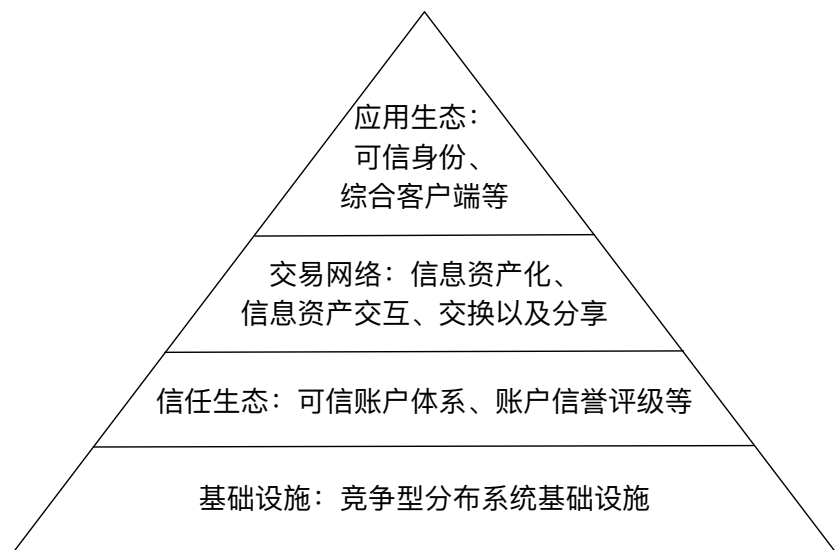
确认操作者身份的过程。常见的身份认证方式有口令、凭证和生物识别等。

3、本体生态概述

本体生态以本体链网为载体。

- 由本体功能链提供基础可信的云服务；
- 由本体生态链提供多样的链上业务服务；
- 由本体身份解决方案实现人、财、物、事的实体识别，从而支持一站式可信应用入口；
- 由本体数据资产化方案和分布式数据交换框架实现业务价值交互、交换和分享。

本体链网由本体链解决方案实现。



图：本体生态结构

- 基础层，即本体基础设施。提供区块链技术框架下的去中心化基础设施；
- 信任层，即本体信任生态中间件。基于身份体系提供可信账户体系，涵盖账户声誉评级等模块，为上层应用提供基础；

- 交易层，即本体价值网络中间件。基于信任层，提供高价值的业务服务功能模块，包含信息资产化，以及信息资产交换、分享和复杂交互业务；
- 应用层，即可信的价值互联网应用生态。基于交易层功能模块实现丰富的链上业务，同时提供可信搜索服务、综合客户端等上层应用工具；
- 生态交互，进一步应用跨链技术实现从基础、信任到交易、应用的 本体生态交互。

本体生态是一个开放性的生态，本体的链网结构支持不同生态链的加入。因此，本体链的解决方案需要兼顾治理模型、经济模型，根据生态链的组网特点进行共识的选择。换句话说，不同生态链的设计需要以满足治理模型为基础，配合经济模型，为每个生态服务提供者提供收益，保证本体生态良性发展。

本体链生态包含以下特点，

- 完备的基础设施支持。包含链网架构、配合治理模型的共识、信息资产化方案，以及跨链信息交换方案；
- 复杂业务生态的支持。包含以下服务：
 - 根据业务特点进行性能优化，可定制的共识；
 - 持续扩展的基础功能链。如，储存服务链；
 - 根据业务确定生态链，使用相关区块链服务，打造业务应用。

4、本体治理模型

本体治理侧重于打造一个开放的治理框架，通过这个框架来承载本体实际投入运营的生态链、功能链的治理，并且支持本体链的治理模型在这个框架之下进行演化。

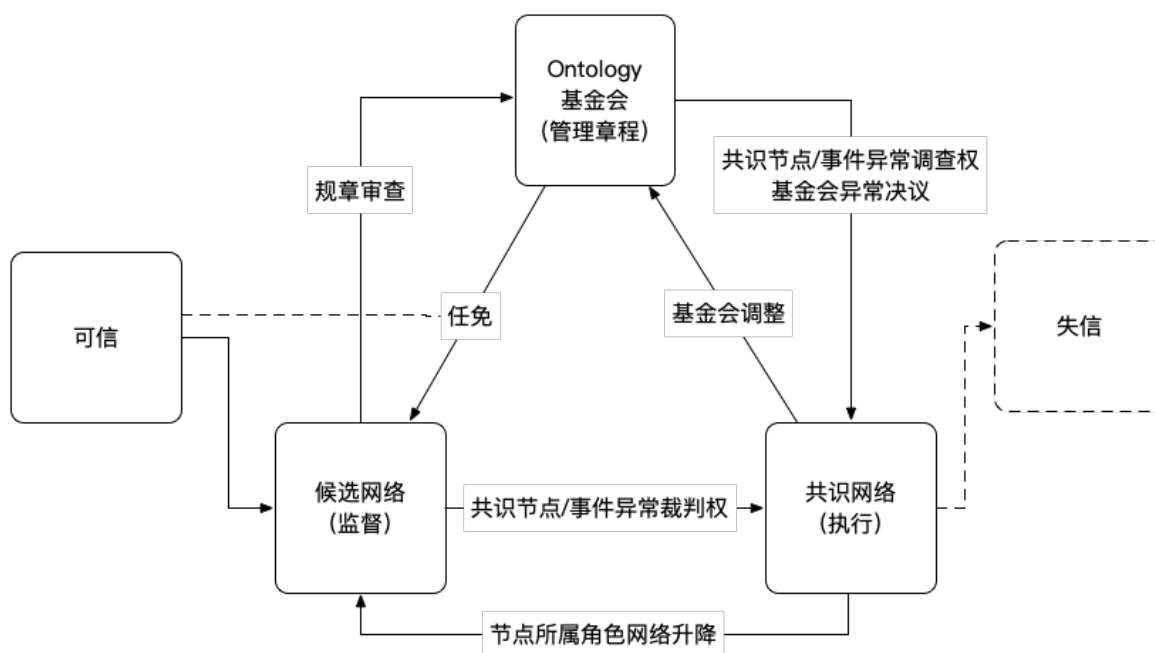
本体生态治理包含链和链之间的治理和本体链内分片的治理，由生态链治理共同完成。

生态的链间治理决策过程也满足一个共识决策的过程，可以复用链内治理的框架，也可以使用传统共识工具达成目标。本书主要介绍本体链内治理框架。

治理的核心在于治理规章的制订和遵照治理规章的执行。本体治理框架包含三个角色、两个流程和一个假设：

- 一个假设。本体链的网络节点大部分（共识算法容错范围内）为理性运营者，这些运营者以经济利润为目标；
- 三个角色。分规章制定、执行和监督三个角色。规章制定者负责规章的制订，执行者负责为规章的执行，监督者负责对规章的制订过程和规章的执行情况进行监督；
- 两个流程。规章制订的流程和工作执行的流程：
 - 治理规章的制订是一个演化完善的过程，由规章制定者起草，监督者审查，后表决通过；
 - 区块链的工作执行过程由执行者完成，执行的过程由监督者监督。执行的过程保持经济激励。执行出错的问题由监督者举证并根据章程实施经济惩罚。执行过程中，
 - 监督者组成监督网络。监督者付出的成本较低，经济激励较少；
 - 执行者组成执行网络。执行者付出的成本较高，经济激励较多；

- 保留监督者到执行者的晋升通道，监督者付出的成本足够高，可以参与到执行网络中。执行网络规模由规章决定，成本竞争落选的执行者，将退回到监督网络中。执行者和监督者是彼此竞争的共生关系。



图：本体治理模型

本体链网体系之内，一个节点运营商可以在一个节点实例中运营不同链的节点，一条生态链中一个节点运营商只能运营一个节点。

5、本体经济模型

本体生态中允许不同生态链拥有不同的经济模型设计，本体生态支持多种经济模型的变化。生态链的服务需要区分链上业务和区块链基础服务。

本体采用双通证设计，配合链网的治理框架。链网基础服务采用统一的通证工具，各生态链可以有自己上层治理类通证，对于选择PoS共识算法的生态链，也可以有权益证明的质押通证设计。本体生态的双通证设计满足多链生态。

6、本体技术架构

本体生态通过本体基础设施支持，基础设施由本体技术架构实现。

本体技术架构满足生态治理和经济的设计，可以根据不同生态链的组网需求进行定制，并且提供链上可信应用的开发框架。

本体技术架构，以本体多链多层的技术架构为基础，满足应用的信任需求。在应用信息加工传输的过程中，选取有价值的信息生成、加工和传递，提供数据资产化方案。本体技术方案支持有价值信息的溯源、确权以及交换。本体技术架构为实现价值互联网提供了一种途径。

7、后记

本书对本体项目提供框架性支持。本体努力打造一个开放、协作和创新的生态，诚挚欢迎您加入我们，共同参与和推进本体项目。

联系我们

电子邮件：
contact@ont.io

Twitter：
[OntologyNetwork](https://twitter.com/OntologyNetwork)

Reddit：
[OntologyNetwork](https://www.reddit.com/r/OntologyNetwork)

Medium：
[OntologyNetwork](https://medium.com/OntologyNetwork)

微信公众号：
本体 Ontology



Telegram：
[OntologyNetworkCN](https://t.me/OntologyNetworkCN)

Facebook：
[ONTnetwork](https://www.facebook.com/ONTnetwork)

Discord：
<https://discord.gg/vKRdcct>

LinkedIn：
[Ontology](https://www.linkedin.com/company/Ontology)

微信客服：
本体研究院小秘书

