



O n t o l o g y

新一代多链式公有链平台 &
分布式信任生态

■ 目录 ■

第一部分：信任体系和本体

- P1 信任的维度
- P3 痛点
- P4 本体的价值
- P5 愿景与架构体系

第二部分：本体信任网络

- P7 本体的信任生态
- P9 本体技术架构
- P10 分布式身份标识和多维验证
分布式信任传递体系
- P11 分布式账本技术
- P12 分布式数据交换体系
- P13 其他关键功能和组件

第三部分：本体应用领域

- P15 概述
- P16 人的多样性识别与认证体系
- P17 物的多样性识别与认证体系
- P18 分布式数据协同与交换
- P19 分布式流程协作
- P20 分布式权益管理
- P21 分布式社群管理
- P22 分布式内容生产与交易体系
- P23 分布式声誉体系
- P24 分布式普惠金融服务
- P25 更多本体可扩展应用场景

第四部分：生态/治理/激励

- P27 生态建设
- P29 合规

本体基于区块链/分布式账本的链网体系，结合了分布式多维实体认证体系，纳入了分布式多源信息交换协议、分布式数据协同、分布式流程、分布式社群、分布式存证等业务领域基础模块，实现分布式的点对点的信任体系，构建跨链、跨系统、跨行业、跨应用和跨终端的分布式信任基础体系。



信任体系 和本体

■ 信任的维度 ■

“信任”是人类组织和社会协作中的关键因素。自古以来人们一直在采用不同技术、法制和组织方法来建立在各个领域的协作“信任”，“信任”也成为社会和经济领域协作的第一成本来源。在人们为建立“信任”所做的努力中，也形成了“法制”、“技术”、“社群”等不同维度建立信任的手段。

技术信任：

技术信任是进入信息社会后发展最迅速的领域，密码学、生物设备、数据分析等技术为不同的协作场景带来了技术信任支持。

区块链/分布式账本体系的出现带来了更广层面的基础性技术信任框架，去中心化多方共同维护的技术信任，在多方对等的情况下共同进行信息维护、数据协作、达成共识等，对各类协作中的数据、数字资产、协议进行可靠控制和技术手段下的保护，因此，区块链体系带来的新技术竞争不是单业务或单点的信任变化，而是一个体系化的生态型变化，这也是区块链具有变革性的要素所在。

法制信任：

法制信任是历史最悠久的信任机制，也仍是目前最广泛的信任机制。大量的人、财、物、事都通过不同地区、不同行业的各类法律法规进行确权与保护。

区块链等技术体系带来的新的技术信任机制，也创造某些场景下的虚拟信任世界，但在更多情况下要与实体世界的经济活动结合起来，就离不开各类实体法律法规和各类信任源的支持。因此法律信任和技术信任的结合也是信任体系中的重要环节。

部分有法制体系保障的信任源也构成了对区块链生态的一个服务性的体系。

社群信任：

群体化信任虽然自古有之，但是一个局限是它只能在局部范围和局部场景下应用。在乡土社会或者是部落群体中，甚至基本的人和人的交往中，一个人是很难对其他人进行大范围的深入了解的。对一个对象真正深入了解，并且能了解到足够信任的程度的人其实很少。社会学家的研究发现，这一数字也就在几十人到几百人之间。因此，在这一信任社群化的信用体系下，很难进行规模性的协作和规模性的经济活动。

但技术在不断的快速发展当中，在信息化时代和互联网时代来临的情况下，依托于信息化与互联网的发展，以及对等网络和区块链这样的去中心化网络体系的出现，形成了比原来类似乡土、部落、城邦场景下更大范围的网上社群社会。在这一基础上，出现了很多新一代社群和群体互相信任的技术探索，如Google的Page Rank算法，PGP (Pretty Good Privacy) 到 WoT (Web of Trust)，以及分布式声誉体系、分布式社群等。

■ 信任的痛点 ■

虽然现有已经具备了不同维度的多样性的信任机制，但在实际世界中，依然存在不少“信任”痛点，很多场景下的“信任”成本也居高不下。

信任源分散化：在现有需多个信任信息的场景中，证明材料获取、验证等等环节流程长、成本高、数据信息泄露风险大。

个体角色缺失：个人对自身信任数据的使用、授权方面没有足够的话语权和透明度，同时缺乏便捷的低成本的手段。

新型信任源的产生：随着信任源的加入和信任源的分散化，使得获取信任源的综合认证、得到信任源的多元评价的成本大大增加。

数据的寡头化：数据的管理呈寡头化趋势，形成多个“数据孤岛”，并不能完整覆盖用户的信息。

数据的零散化：基于数据量的巨大差异，零散数据源与寡头处在不对等的位置上，使其数据失去了很大的交易价值，无法被使用和证明。

身份认证难准确：基于单一信息管理体系的个人认证难以对个人形成全面的、综合的的评价，难以准确获知“我是怎样的我”、“你是怎样的你”。

物联网管理难识别：物联网管理需要避免非法甚至是恶意的节点接入，但在多方参与的环境中，目前缺乏对物联网设备建立数字身份及进行相应身份认证的可行机制。

数据交换难安全：基于现有中心化的数据交换体系，中心化服务器的数据沉淀往往会对数据源产生利益伤害，对数据客户产生业务威胁等。

流程协作难信任：在没有中心主导的流程协作中，协作者之间的信任往往难以建立，特别是参与者越多，就越难在流程协作中建立信任。

权益管理难透明：对于现在出现的新型权益管理模式（如众筹等），由于透明度低、信息不对称等，项目的运作过程中难以建立可靠的信任。

社群管理难协调：在社群管理中，入口把控是一个重点，但互联网时代缺乏有效机制对新加入者进行有效审核，难以保证该社群的共性不会随着新加入者而降低。

虚假消息难判断：基于浏览数量的鼓励机制造成大量低质量的甚至是虚假、误导信息的广泛传播，如何判断这些虚假消息始终是难点。

声誉评价难综合：对于声誉这类“软信任”，需要大量数据、信息来做支持。但目前缺乏基于声誉管理的有效信息流通和协同机制。

公益捐赠难追溯：提高透明性逐渐成为了公益捐赠管理中的需要。简单的款项追踪能解决部分问题，但还需要对发起人、受捐助人、家庭情况等情况的综合认证。

更多痛点.....

正是因为“信任”的多样性，造成了各种场景下的“信任”成本和痛点，如何构造一个结合多样性的一体化信任机制，成为对新一代“信任”基础体系的追求。

■ 本体的价值 ■

本体信任网络架构了一个分布式融合的信任体系，将信任的多样性在一体化的协议体系下进行协同，整合分布式多维实体认证体系及各类不同区块链体系与信息系统，纳入多源身份认证和多源信息交换协议，并提供不同分布式应用场景的开放基础模块，实现分布式点对点的信任体系，构建跨链、跨系统、跨行业、跨应用和跨终端的分布式信任基础体系。

本体信任网络在分布式实体与数据信任基础上，提出进一步拓展的生态与应用，将信任的应用扩展到很多的维度，从实体认证到数据交换，从分布式流程到分布式社区，从分布式交易到分布式声誉，结合底层的区块链分布式账本体系，联合各类服务伙伴在不同地域、不同领域提供多样化的信任服务，形成新一代的全球信任网络基础设施的一部分。

■ 愿景与架构体系 ■

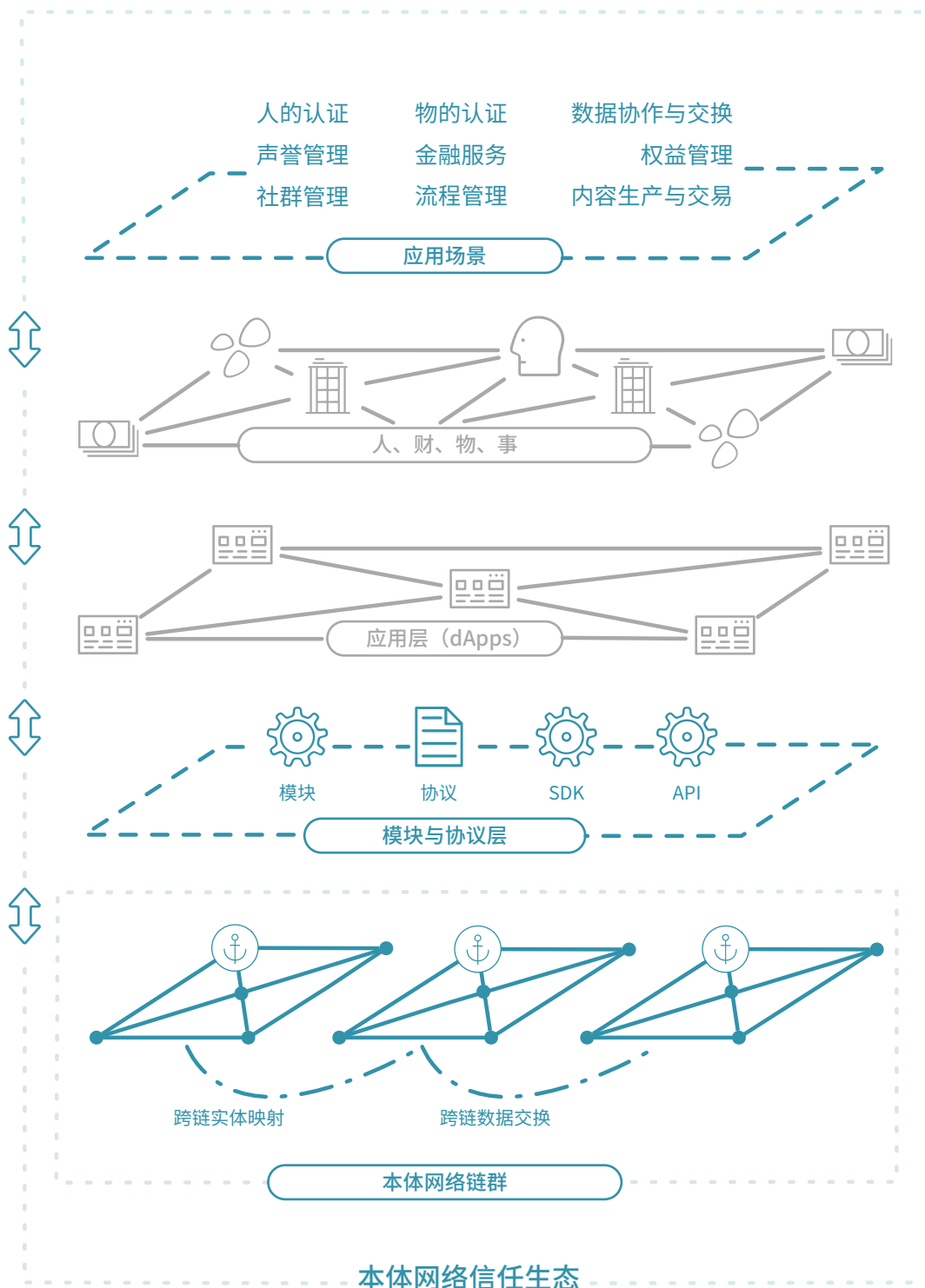
识万物、信万物
人人信我、我信人人

多样性融合的一体化分布式信任协议网络
信任生态的基础设施与连接器

本体信任网络是一个多链、多系统融合的协议网络，来自不同的链和系统可以支持不同业务体系，并通过本体的各类协议进行协作。

架构体系进行模块化、可插拔、灵活扩展的松耦合设计，以支持不同业务领域的需求，可以灵活扩展到各类业务应用支持；

本体合作网络将始终结合区块链/分布式账本领域相关技术的发展、不同业务领域的应用，提供分布式账本、智能合约、分布式实体管理认证协议、分布式数据交换协议等一系列的协议基础层与应用接口，任何应用服务提供方无需分布式底层开发能力，可以直接基于本体提供分布式服务。



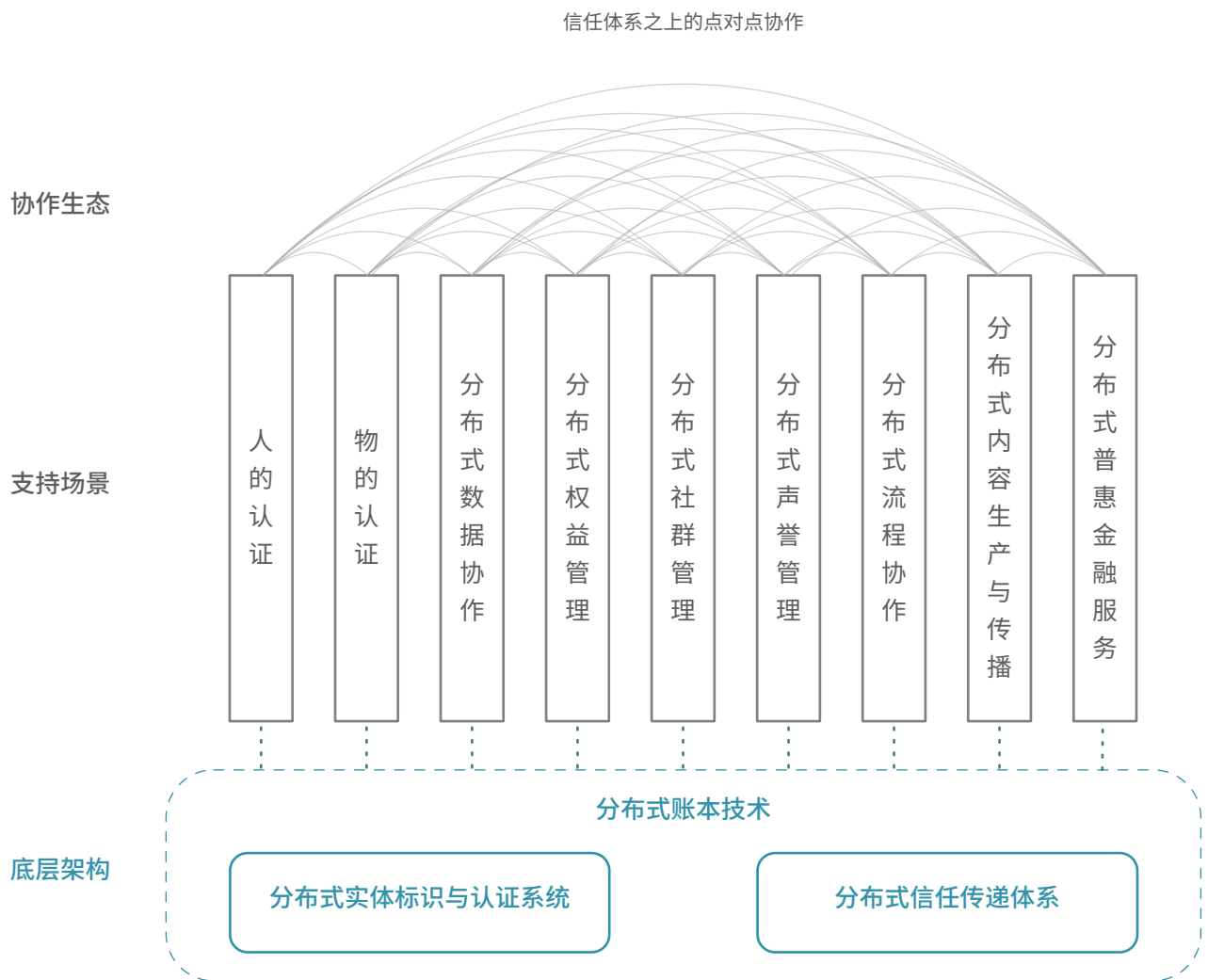


本体 信任网络

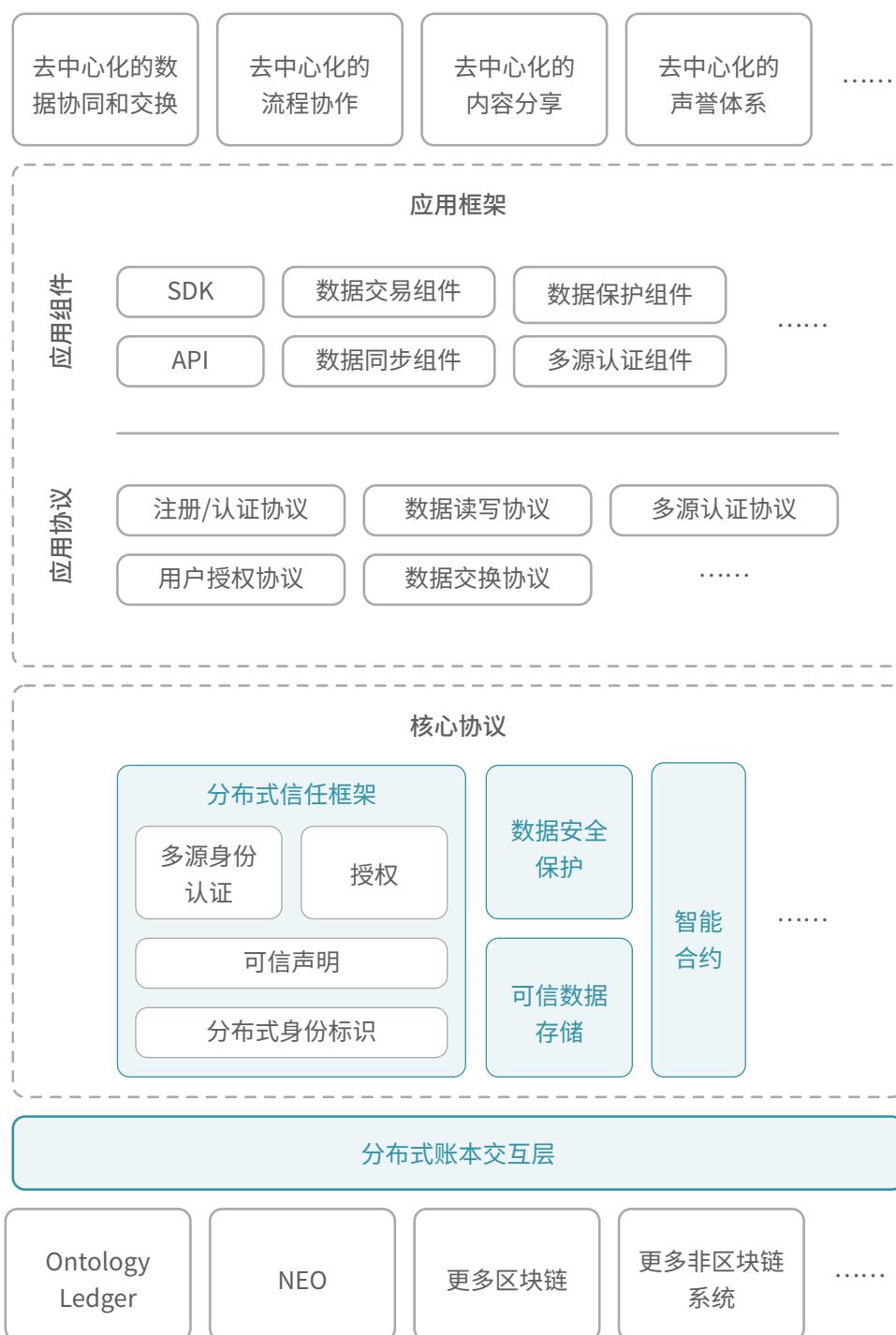
■ 本体的信任生态 ■

本体信任网络致力于建立一个体系化的、流程化的、一体化的信任生态，为信任源的有效协同、为数据源的互联互通、为各类分布式应用服务提供完整的底层技术基础。

本体致力于建立信任的生态体系。本体将作为信任生态体系的基础设施和连接器，基于此，各个行业、各类场景可以进行各类应用的开展与协同。



本体技术架构



本体底层提供了完整的分布式账本体系，包括完整的智能合约体系、安全体系。同时，本体对底层复杂的技术体系及异构的系统进行了抽象，实现支持兼容各类主要协议、密码标准的分布式实体管理和多维认证协议，并支持对各类异构区块链和传统信息系统的跨链、跨系统交互映射。本体还提供了如安全数据存储、异构智能合约、硬件密钥管理、加密数据分析等技术体系。整个网络作为一个应用平台可以支持构建各种应用服务，特别是去中心化应用。

在此基础上，本体提供了一系列应用框架，包括分布式数据交换协议、分布式流程管理协议等等，通过通用API、SDK以及各种应用功能组件，进一步支持各类上层应用的实现。

■ 分布式身份标识和多维验证 ■

一个融合多样性、分布式的，同时保护数据隐私安全和易扩展的实体标识验证体系是本体信任网络的核心协议之一，它能够支持本体信任网络中的各类实体包括人、组织机构以及物品的分布式和多样化的识别与认证。本体同时融合多种通用性和专用性的结合设计：

分布式身份标识与多维认证

本体身份标识使用分布式身份标识方案。分布式身份标识本身并不与特定的业务相关，具体如何使用，由实际的应用定义。

分布式身份标识方案中每一个实体（人、物、机构）身份都可拥有一系列的分布式信任源，并以此在不同场景中选择不同认证方式，所有实体的身份信息只存在于具体的身份信任源

提供方，不会在本体中留存，以确保各类业务中的合规与隐私。

身份实体与分布式身份标识

在本体中一个实体（人、机构、物）也可以对应到多个分布式身份标识。在身份实体授权人授权之前，任何第三方无法根据实体在一个网络系统中使用的身份标识推测出其在另一个系统中使用的身份标识。通过不同的身份标识隔离出各实体在不同系统中的

操作，可以极大地保护隐私安全和身份信息权益。

专用性身份信任源

实体可以根据业务场景或法律法规的需要融合采用不同的身份信任源，如特定领域或地域的eID、CA、政府、机构、学校、公司、社群以及个人等等，以满足不同的信任认证需要。

■ 分布式信任传递体系 ■

在本体中，除了支持传统单信任源机制外，还支持更去中心化的分布式社群信任体系，并支持分布式信任传递体系。其实现方式是：

社群信任

社群信任模式是一种很有效的信任体系。通过在特定社群中的多方背书，个人背书形成特定领域的社群信任认证。

信任锚

信任锚通常是那些经过了实名认证，且在社会中具有一定公信力或声望的政府单位、企事业单位、非营利性组织以及社会名人等。被信任锚背书过的实体就自动的获得了这个信任锚的信任度。信任锚本身的可信任度越高，那么这个网络实体的可信任度也就越高。

声明

声明是社群信任的信任载体。在本体中声明是一个身份主体对自己或对另一个主体做的一个陈述性描述，是本体中传递信任的载体。当一个身份主体需要对外发布一些可信的信息时，只需要签发一张声明即可。

信任传递

信任传递机制是本体中的信任使用的实现方式。特定的身份主体通过各类型、各来源声明的获取，一方面可形成多维度的身份画像，另一方面可形成从自身出发的个人信任生态。在特定需求中，通过声明的出示，和数据记录的提供，可将信任进行传递，一方面向他人出示自己的可信信任认证，另一方面通过信任数据的多次使用，形成多次认可，进一步扩大了信任生态。

■ 分布式账本技术 ■

分布式账本是本体信任网络底层存储的重要基础设施。分布式账本技术的去中心化、不可篡改、共同记账等特点是本体信任网络的分布式多方信任得以实现的关键。在本体中，将在以下方面进一步拓展分布式账本技术的运用：

实体登记与识别

实体身份登记与识别是本体的重要基础性模块，本体设计了多方面、多层次的参与者与相关资源的登记、认证和授权体系。实体身份与授权模块设计提供一个多层次的身份认证和授权体系，通过灵活配置集成自有的授权服务或第三方认证机制（如CA认证），也可以进行社群化的对账户本体进行各类认证背书，并可根据业务场景集成不同的审核机制，对区块链参与节点、参与人进行体系化的身份认证和授权。

数据目录

运用分布式账本技术，可对提供的数据类别进行目录登记，并进行数据的唯一标识（ONT Data ID）和数据资源获取地址（Data URI）的匹配，可以让需求匹配到所需数据，并通过ONT Data ID数据存证的对比确定数据的有效可信。

流程协同

运用分布式账本技术，实体跨链及跨系统隐私，以及特定的跨链协议，实现流程协同（分布式事务）。即流程/事务的多个步骤分散在不同的区块链或系统上执行，保障不同实体在不同系统与区块链中的身份隐私，且保证整个事务的一致性。

数据交换

运用分布式账本技术，可实现以实体（人、物、设备、内容...）为本的数据交换框架，盘活个人数据资产，让数据能够流通使用起来，以规范化的协议设计支持数据的发现、授权与交易，帮助用户对数据进行细粒度的控制，在满足用户自身隐私需求的同时为用户谋取数据再利用的收益。

行为存证

通过分布式账本的运用，将不止提供数据存证，还可对行为存证进行支持。即每一次的数据请求、数据匹配、数据调取与数据使用等均在账本进行记录，形成了一份数据全流程的记录，保障数据的安全、可靠、不被泄露。

智能合约

通过智能合约的支持，可以让不同业务进行更多的业务流程性扩展与创新，在业务流程协同、控制与交换等方面建立特定的技术信任机制。

■ 分布式数据交换体系 ■

本体提供系列用于分布式数据交换的底层功能与协议支持：

分布式数据交换协议

本体将兼容支持多类不同的全球化数据交换协议，以支持不同的业务场景需求，同时将数据交换协议与分布式账本结合，形成分布式的数据交换流程，并提供系列的数据与隐私保护的密码学组件支持。

数据授权机制

在数据交换体系中，数据的隐私保护和数据的泄露防范始终是重点。在本体建立的信任生态中，设计了授权机制，即任何涉及到数据主体相关数据的交易，需要通知数据权益方（单方或多方）进行授权交易。

数据的版权保护

针对数据的数字化特性，本体提供数据存证与生命周期管理功能，设计了相关数据的生命周期溯源机制。首先，实现为每一份数据建立数字身份，以对其登记、请求、授权、交易等全流程进行有主体的追踪；其次，数据的版权保护，数据的交易均在分布式账本进行记录。

数据的分布式存储

提供支持数据交换的分布式数据存储层，对各类数据应用进行支持。

■ 其他关键功能和组件 ■

密码学技术和数据保护组件

Ontology Crypto Package (OCP)

在多维实体身份认证、分布式数据交换、分布式流程协议等等环节中，本体提供一系列的密码学和数据安全组件支持，包括数据加密传输、密钥分享协议、多方密钥管理、环签名组件、盲签名组件、门限分享机制。在身份与数据验证环节，提供零知识证明、同态加密方案。在数据协同应用环节，提供两方计算，并在后续进一步探索多方技术方案。

此外，本体针对特定场景，提供特定安全组件，并支持上层的应用实现方基于安全组件来搭建适用的安全应用协议。这些安全组件根据场景需求会不断开发和拓展。

数据交易市场 Ontology

Marketplace (OM)

数据交易市场是融合了分布式数据集、AI算法和模型的交易所界面。市场中的商品包括数据产品、数据预测、数据计算资源等。借助本体无限的扩展，同时保持与各类主要跨链协议的兼容性，确保面向全球级的交易规模以及跨交易市场的交易需求，支持基于本体的服务全球用户的各类 Dapp 应用。上层数据交易服务商可以在此基础上实现各类别、各领域的

数据交易。

全局事务数据库 GlobalDB

GlobalDB 是一个可插拔 key-value 分布式数据库接口。它提供了多重后端数据库组件选择，其中包括 levelDB、RocksDB、TiDB、cockroachDB 等。

GlobalDB是为区块链/分布式账本以及IPFS高度优化的数据库组件。GlobalDB提供了分布式事务、可扩展、实时链上索引及链外数据交互的能力，可应用在区块链与大数据、区块链与人工智能联合数据训练等计算相关的场景。

混合预言机 HydraDAO

HydraDAO混合预言机融合智能合约、跨链、跨数据源协同的混合数据预测和数据交互组件。它包含本体的分布式自治组织DAO功能和链外的数据交互功能（大数据/人工智能）。本体的治理机制将支持民主提案和人工智能自动化提案/验证，通过算法自动提交的提案形成一个完整的HydraDAO作业，并自动接受有效的验证。此过程将生成一个独特的DAO地址并创建一个代币投票池。它使DAO能够将资金和结果直接收入到本体中。一旦投票期完成，DAO将根据其智能合约中定义的不可篡改的规则自治执行。这种混合机制，为本体的数据交换和治理提供了极高的灵活性，为未来网络大规模自动化运行提供了技术上的支撑。

无限扩展共识引擎 Ontorand Consensus Engine

本体中链网结构的部分分布式账本网络会支持新一代共识引擎- Ontorand Consensus Engine (OCE)，Ontorand是一个高效的，基于DNA的DBFT共识协议的增强版本，实现了近乎无限的可扩展性，它只需要很少的计算量开销，生成几乎不会分叉的区块链网络。Ontorand生成区块速度仅受制于网络速度，常规区块的确认时间小于20秒。Ontorand是真正的去中心化协议，它将共识权力赋予用户，不存在矿工等对交易确认的控制。Ontorand基于可验证随机函数VRF的加密抽签机制来选择验证者集合，每个验证者集合通过隐私排序创造本体的种子seed，指向下一个验证者集合。Ontorand支持可插拔验证者、在线协议修复/升级，是未来本体的核心技术优势。与此同时，本体的分布式账本框架也支持可插拔的共识机制，如DBFT、RBFT或定制的PoW等，以支持本体链网体系中不同链的特定需求。

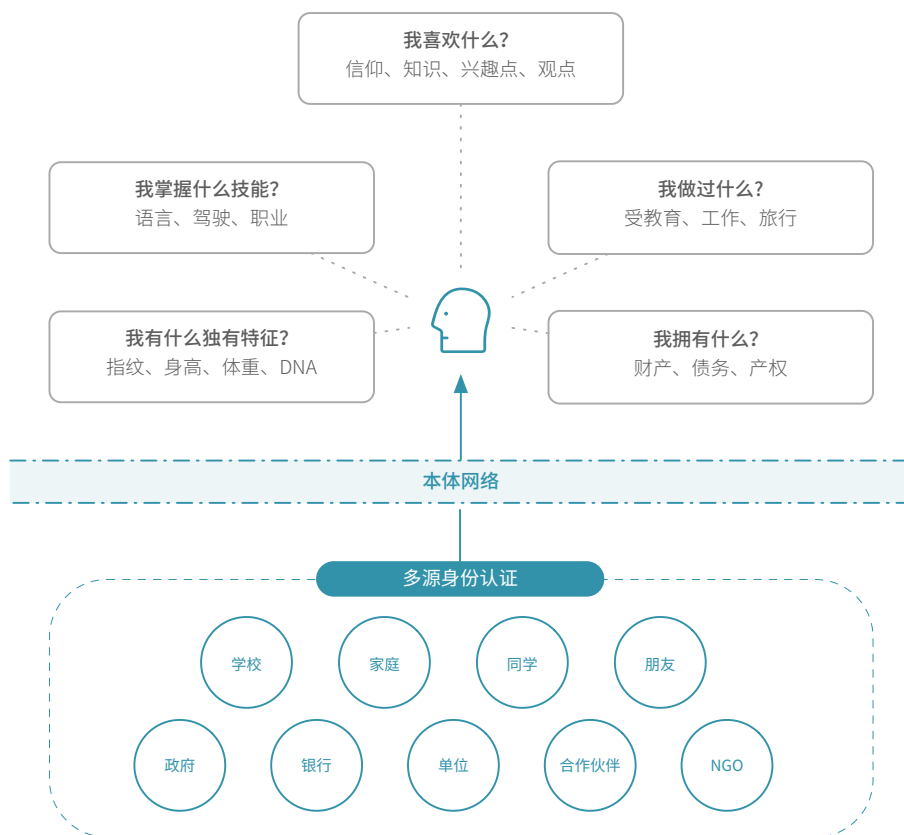
本体还将根据具体场景需求，推出更多的核心支持组件。



本体生态与 应用领域

本体是连接器和业务支持的基础设施。在本体中，来自各行业的伙伴可以实现各类分布式体系的新业务模式，而这些多样化的分布式应用服务，又通过本体连接成一个更大的体系化服务生态，为用户提供更好的服务体验，为社会带来更好的协作信任与效率。

人的多样性识别与认证体系



现实社会中人有多种社会关系，任何与个人有关联的组织机构或个人都掌握有与这个人有关的信息。通过本体，用户可以链接与授权各种与自己有关的数据。从政府机构到学校、银行等各种企事业单位，从家人、朋友到同事、领导、合作伙伴等个人均可成为认证的数据源，并在隐私和授权保护下实现一体化的灵活应用。

多源身份认证

多源认证是指多个不同的认证方从不同的角度、不同的方面对同一个人进行的多源认证是更加全面，更加多样化的身份认证。

完整的个人画像

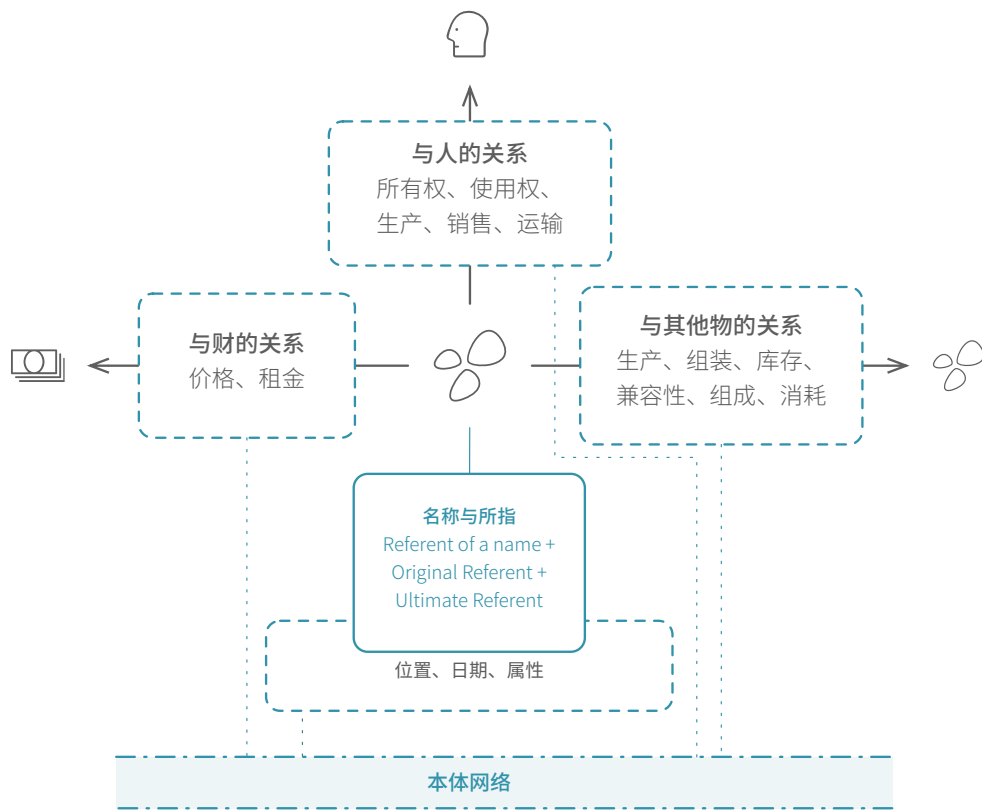
完整的个人画像指可从与个体生活有关联的组织机构及个人收集各种证明数据来描绘个体的各个维度的情况。

可信的数据追踪

本体任何认证方做的认证都经过认证方的签名，具有不可伪造、不可抵赖的特性。同时认证方本身也是可以做认证信任传递的，如果对认证方的权威性，或者是可信性有疑问的话，可以对认证方的资质或者是信誉做认证。这样就会形成一个认证链，最后形成一个认证网络。

■ 物的多样性识别与认证体系 ■

人们在生活中离不开跟各种物（things）打交道，正因为物有不同的功能和用处，因此希望这些物在分布式信任网络中也可以拥有可信的数字身份，由其拥有者或制造者监护，对外提供自身独特的服务接口，并可以与其他拥有数字身份者进行对等的交互。与人类类似，物的识别手段也具有多样性，本体的目标是identify everything。



对物的认证的可信性

通过对“物”的多样性认证，建立对“物”及其生命周期的多方共信。

建立物的数字身份。形成特定“物”在本体中注册的数字身份DID。

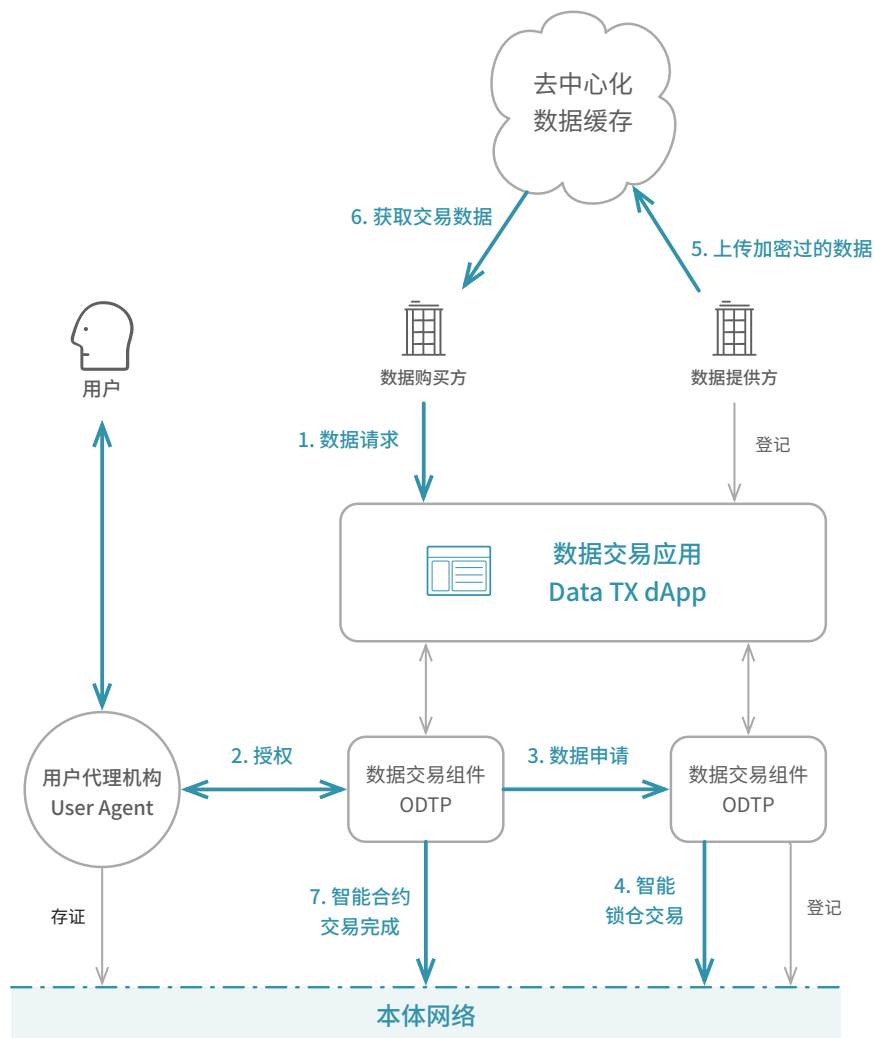
物的验证。通过查询到的DID的签名及背书验证设备的来源与可靠性。

物的流程与数据。与特定“物”相关的流程与数据信息。

对物的数据的记录与识别

基于本体，可实现对物的数据的全流程记录与识别，包括与物相关的所有权、流转记录、参与行为等。

■ 分布式数据协同与交换 ■



数据发现

需要使用数据的应用不再需要逐一对接各数据源，而是从用户出发，根据用户身份ID申请授权访问用户的数据，借此，数据使用者可以发现更多维度的数据、更大规模的数据，实现充分了解用户，为用户提供更有针对性的服务和产品。

数据交易模型

数据使用方通过用户身份ID检索到用户数据的访问地址，发出获取数据的请求。请求将首先发送到用户的客户端，由用户进行确认并授权。只有通过用户授权的请求才能进一步处理。本体的设计让用户（数据生产者）可以充分获得数据服务的知情权和收益权。

用户在使用互联网服务的过程中，会传递用户信息并产生行为数据。这些数据留存在服务提供商，可以被用来做进一步的分析。合理的利用数据能够产生巨大的价值。

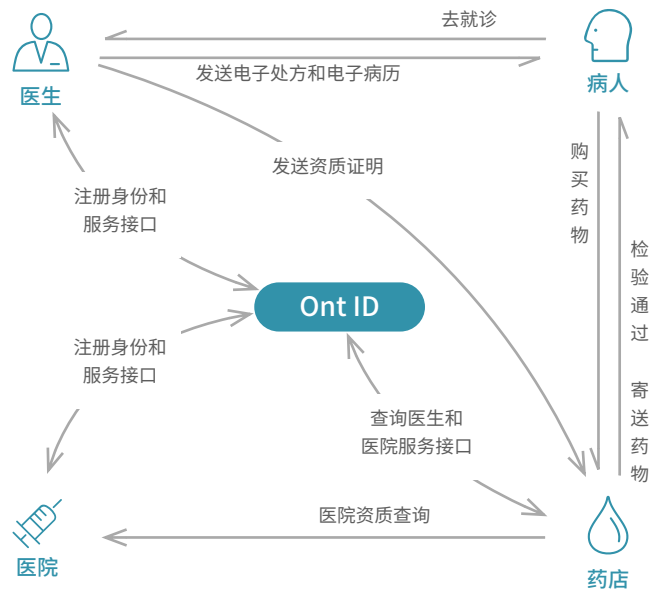
本体提供了一套“以实体（人、物、设备、内容...）为本”的数据交换框架，以多种规范化的协议设计支持数据的发现、授权与交易，帮助用户对数据进行细粒度的控制，

在满足用户自身隐私需求的同时为用户获取数据再利用的收益，也为需要进行数据协同的业务领域提供基础协议与平台。基于区块链和智能合约技术的特性让所记录的数据公开、透明、可追溯、不可篡改，可以充分反映参与数据交易的状况，确保合约的执行，建立信任关系，可以广泛应用在签约授权、联合征信、分布式协同计算、人工智能数据联合训练等不同业务领域。

■ 分布式流程协作 ■

分布式流程协作的医疗场景示例：

当医生、医院和病人均在区块链上注册身份的话，区块链作为一个关键信息基础设施，就能够填充药店与病人之间的信任间隔，因为关于处方的大部分关键信息都可以进行溯源和跟踪查询。药品零售企业通过核验医生资质和医院资质，并经过处方核验医师的确认，就可以将处方药卖给病人。



通过本体的运用，将在多层面为分布式流程协作建立信任：

责任的明晰

通过本体的运用，各参与者的职责和权限可由多方记录及确认。且随着协作的推进，各方可实时进行新的责任划分与确认，加速协作进行。

流程的记录

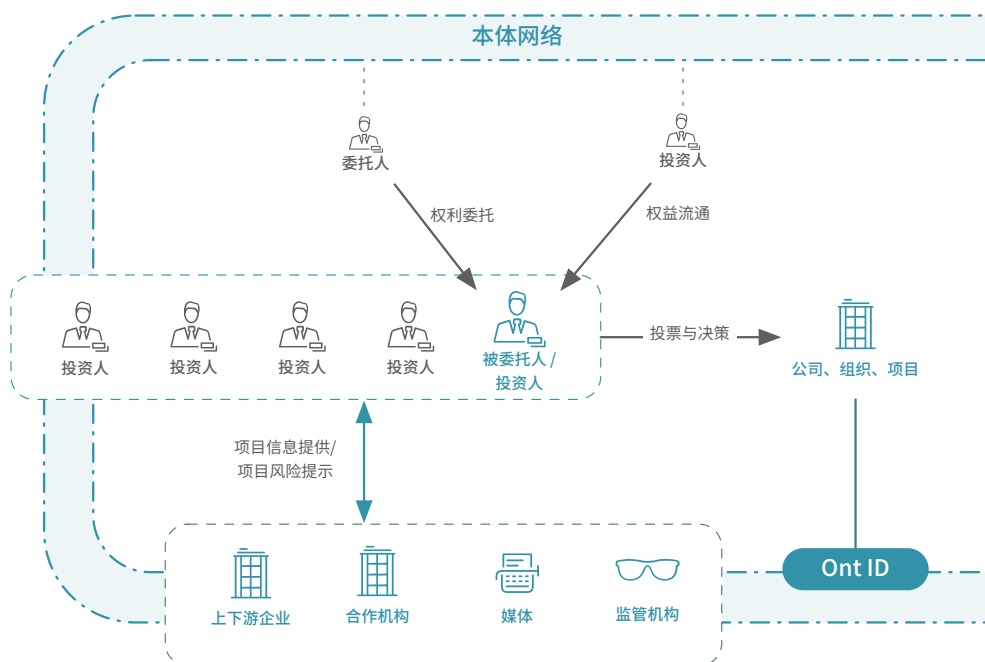
每一个流程的推进均在本体进行记录，保障参与者主体身份的可信，参与行为的可信与协作效果的可信。

结果的可信

通过本体的运用，可为协作结果设计多方确认与背书机制，以保障协助结果与协作主体的可信。

■ 分布式权益管理 ■

新的经济体系有大量的新型权益管理模式。但由于透明度低、信息不对称等，这些项目的运作过程中往往缺乏可靠的信任机制。在权益管理中存在不少难点：项目评估难、风险提示难、信息披露难、权益流转难及权利委托难。鉴于此，本体设计了一套基于信任的分布式权益管理体系。



分布式权益管理的分布式投资管理示例：

基于本体各项功能实现，在分布式投资中，可实现以下功能：

首先，数据的可信流转。基于本体，可设计特定投资项目的项目基本信息、运行情况、风险提示、历史业绩等数据的分布式流转。

其次，多元的评价体系。项目运营方、投资人、合作机构、上下游企业等可将项目相关的客观事实进行提供，并基于自己的身份进行背书。

再次，项目的声誉管理。在数据的归集的基础上，可进

行数据协作，如可根据投资人设定的分析规则，对项目进行声誉评价。

权益的分布式流通

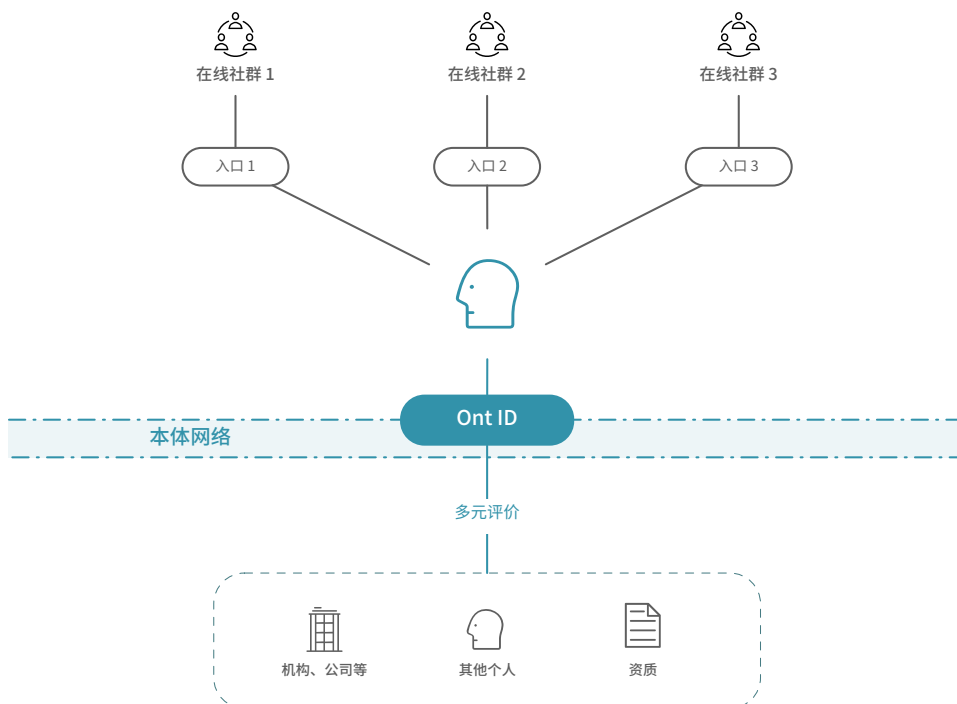
基于本体的信任生态，可设计将权益数字化和可授权化。同时，授权与转让的全过程链上记录，利用区块链的公开与透明，保障了权益流转的可信记录与监督。

分布式权利委托

基于本体，可实现委托的多方认可和行权的有效记录，为可能的委托纠纷提供可信证据。

■ 分布式社群管理 ■

现在的社群主要通过中心化的服务商提供服务，通过本体支持以分布式的体系管理一个社群。主要体现在：



入口把控

社群的健康发展需要合理把控入口，以保证该社群的共性不会随着新加入者而降低。通过本体社群管理者可进行信息的可信确认，以确保社群的新加入者都是高质量的、符合要求的用户。

群体划分

一个健康发展的社群必然有等级制度，不同等级的用户的威信和话语权都不一样。通过本体，在社群中用户可向管理者提供DID证明自己在该方面的阅历或权威信息证明，或在某个具有共性社群中的等级证明(如像技术社群管理者提供自己在某java

交流群中的管理员身份认证信息)可快速合理地划分自己在某社群的等级制度。

分布式交流社群

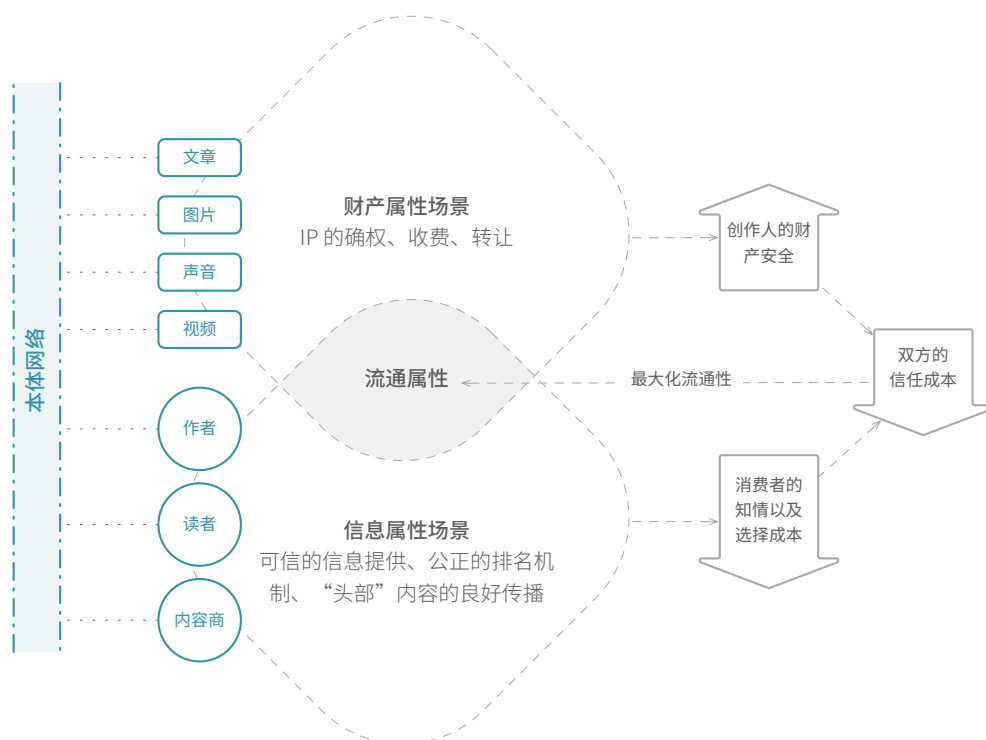
在分布式交流社区中，如何确认一个人的权威与某个消息的可信是始终是难点。通过本体从不同方面进行社群信任增强：

首先，权威主体的认定。根据特定主体个人信息、历史发帖、交流信息的记录，社群各参与者可对其进行多方认定。经多方认定，特定的个人或机构可在相应社群获得一定的公信力，并作为权威主体存在。

其次，内容发布的控制。在分布式社群中，对假消息、低俗消息的把控逐渐成为了需要。通过本体，可设计内容的发布机制，权限较高及获得认可的权威主体的内容可直接发布，其他参与者的内容需要进行相应审核。

再次，激励的设计。在分布式社群，根据群体参与者对某一特定内容的“点赞”等认可，可设计对内容发布者的奖励机制。通过本体的应用，“点赞”等认可进行区块链记录，每一次认可对应一条区块链记录，避免了刷票等行为存在的可能。

■ 分布式内容生产与交易体系 ■



内容作为无形资产，现有的技术和服 务已经可以将其转化为有形资产（付费内容），或其他无形资产（注意力-广告的盈利模式），但是代价较大。

在信息生产者与信息消费者的关系里，从多个角度引入分布式信任体系可以构建两者之间更良好的互动。体现在：

创作者名望与消费者注意力的货币化

基于分布式信任体系的模式可以将声望加入，结合分布式体系下的数字权益机制，使其与注意力自由兑换和交易成为可能。

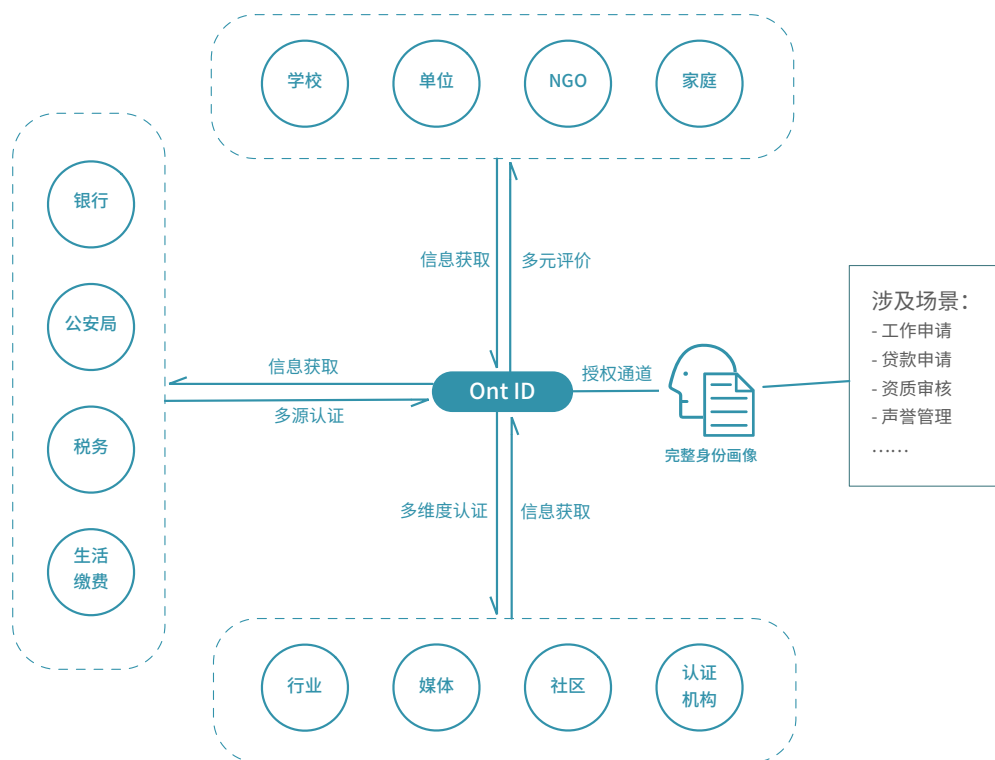
在内容的推荐上用户可以选择只看声望值符合自己期望的作者的内容，或者将数据交于可信任的第三方机构来推荐内容。由于这个系统中用户对自己的偏好数据有了控制权，在与内容提供者的价格博弈中也将获得更加公正的待遇。

保障无形资产的财产安全

本体的身份协同体系由于天然的不可篡改性，可以作为具有法律效力的证据备案。由于区块链技术是开源的第三方技术，这就有可能在全球范围内为IP进行高效无障碍的法律确权、收费、以及转让。当把内容给生产者带来的声望也看做是一种货币的话，对声望意义上的知识产权保护会产生更加深远的意义。

■ 分布式声誉体系 ■

在现实生活中，多类主体希望、甚至需要获得他人的认同与评价，并以此作为一种证明或标榜。例如，医院的锦旗，军人的军功章，学生的奖状。但是声誉从本质上是一种“软信任”，需要通过特定主体的历史行为，来对其将来行为进行预测。这需要大量数据、信息的支撑。



信任分管理

本体的信任分主要包括选定评价标准，并基于此进行本地信任与综合信任（或全局信任）的计算。首先，计算本地信任，本体通过在本地收集评价参数等，形成本地观点；其次，计算综合信任，本体通过融入更多主体的参与，将降低主观不确定性和虚假反馈等对声誉管理的影响。

信任数据管理

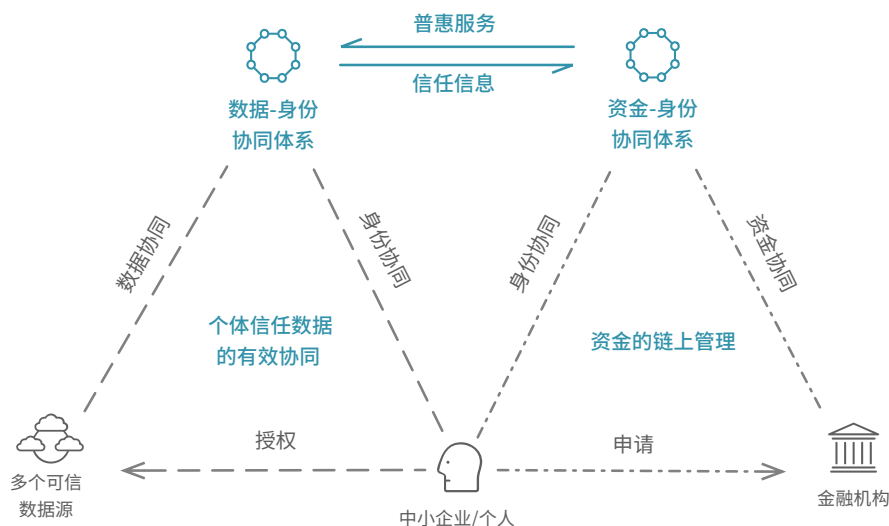
信任数据管理指信任数据的收集和分发方式。在本体中，将结合两种信任数据管理模式：一

是分布式，多个阶段相互合作，共同管理信任数据；二是混合式，结合分布式和部分的集中式方法进行管理。

信任模型扩展

基于分布式内容生产与交易体系，可对信任模型进行进一步的扩展。如可设计一套对内容的分布式上层评价机制。具体体现在：将内容作为一种身份主体，建立多视角的评价机制和多维度的认定方式。

■ 分布式普惠金融服务 ■



普惠金融服务对象以小微企业及个人客户为主，其信用记录一般较少、分散和验证成本高，也普遍缺乏有效的抵质押物。因此在普惠金融中，银行等金融机构的风控风险较大，并采用较高的贷款利率。同时，普惠金融中的单笔交易金额小，规模效应难以发挥，导致运营成本过高。此外，较高的利率水平又带来企业社会责任和道德评价等声誉风险，让普惠金融的发展陷入两难境地。

从金融角度

本体首先将帮助普惠金融服务对象转变角色，个体作为金融服务的需求方，从被动地等待机构审核向主动管理其信用数据转变；同时，通过多源数据协调和数据主体授权机制的设计，帮助个体在申请金融服务时更便捷安全地自证清白，也帮助降低风控风险和成本，以更普惠的利率提供金融服务。

从社会角度

金融机构通过本体进行数据的协同，将有效建立对普惠金融对象信息的多方安全协调、分析机制，进而可为普惠利率的实现提供技术支持，真正满足社会对普惠金融的期望。

更多本体可扩展应用场景

本体作为分布式的基础设施，可以为大量应用场景的分布式服务提供技术基础体系，让各行业服务提供团队在无需掌握区块链、分布式账本、密码机制、分布式网络、各类业务协议等等复杂体系和技术的前提下，便捷地提供各领域的分布式服务。

可基于本体拓展实现的业务场景：

金融行业Finance

交易领域：Trading

财富管理：Wealth management

衍生品交易：Derivatives trading

抵押品管理：Collateral management

供应链金融：Supply chain finance

物联网IoT

支付设备：Device-to-device payments

自动化操作：Automated operations

电网管理：Grid management

智能家居管理：Smart home management

办公室管理：Office management

支付Payments

小额支付：Micropayments

B2B国际汇款：Business-to-business international remittance

税务申报和统计：Tax filing and collection

了解您的客户：Know your customer (KYC)

反洗钱：Anti-money laundering (AML)

消费行业Consumer

共享经济：Sharing economy

供应链管理：Supply chain

药物跟踪：Pharmaceutical tracking

农业食品认证：Agricultural food authentication

物流管理：Shipping and logistics management

保险Insurance

索赔申请：Claim filings

索赔处理和管理：Claims processing and admin

欺诈检测：Fraud detection

远程信息处理和评级：Telematics and ratings

数字认证：Digital authentication

媒体Media

数字版权管理：Digital rights management

艺术认证：Art authentication

广告刊登：Ad placement

广告点击的真实统计：Ad click fraud reduction

正版资产的转售：Resale of authentic assets

软件开发Software Development

微粒化工作：Micritization of work

人工支付：Disbursement of work

面对开发者的直接付款：Ad placement direct to developer payments

API接口平台：Ad placement API platform

公证和认证：Ad placement notarization and certification

医疗卫生Medical

病历共享：Record sharing

处方共享：Prescription sharing

多重认证：Multi-factor authentication

个性化医疗：Personalized medicine

DNA测序：DNA sequencing

资产标的Asset Titles

钻石：Diamonds

设计师品牌：Designer brands

汽车租赁和销售：Car leasing and sales

住房抵押：Home Mortgages

土地所有权：Land title ownership

实体资产数字化：Digitalization of assets

社会管理Government

投票：Voting

车辆登记：Vehicle registration

福利分配：Benefits distribution

版权保护：Copyrights

教育和认证：Education certificates

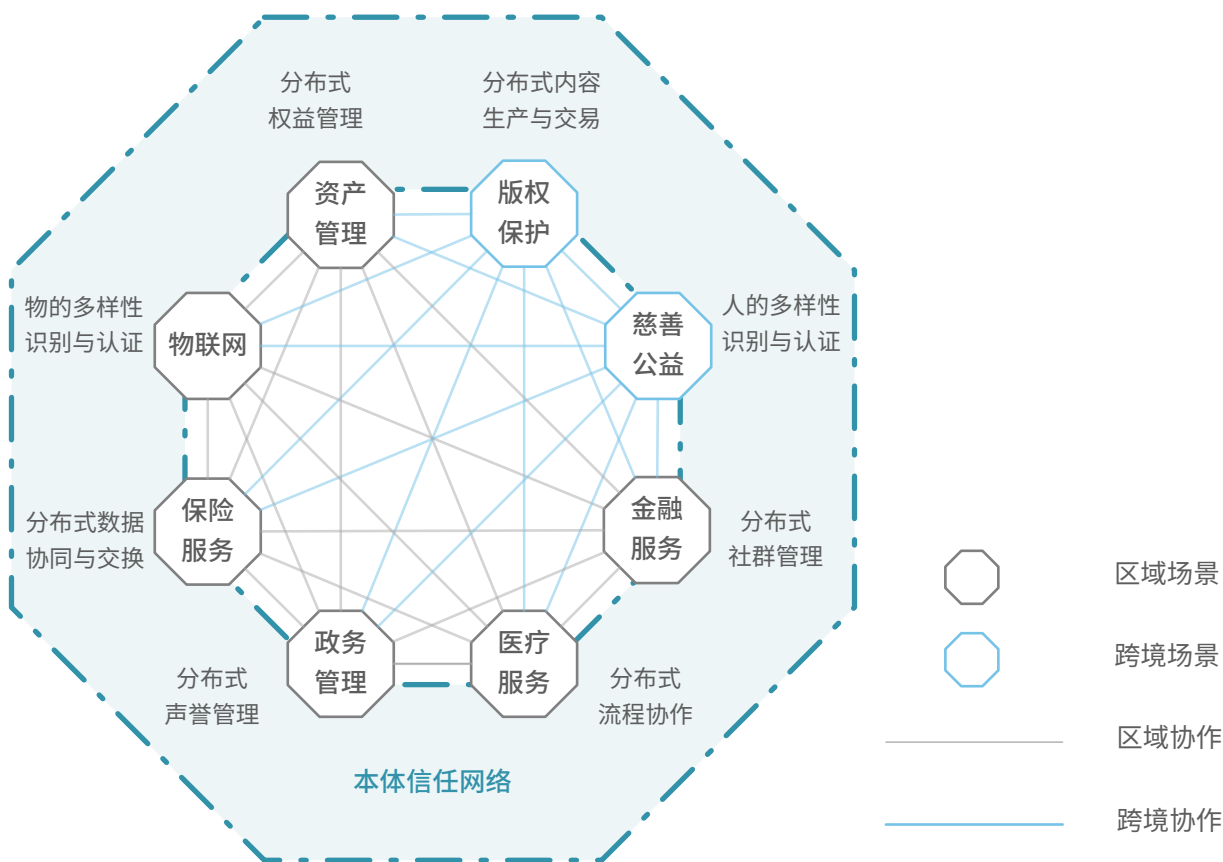


生态与合规

■ 生态建设 ■

本体的定位是信任的**底层基础设施**和信任的**底层价值通道**。一方面，本体作为底层设施支持上层各类应用的开发与应用，应用团队只需要关注自身的业务应用，而不需要将过多精力用于区块链或其他底层技术；另一方面，本体将通过底层的协议支持，串联各数据主体与信息主体，形成多维的场景支持。由此，本体将逐步构建基于可信实体与数据的信任生态。

本体家族是本体生态的主要参与者，本体家族将由多类型的主体构成。以下定义针对的是实体社会中各家族成员的身份和类别：



实体认证服务提供者

CA机构、eID等具有公信力的实体认证服务机构、各类公司、组织、社群和个人生物识别设备都可以成为认证服务提供者，提供各自范围内和信任度级别中的实体认证服务。

行业应用服务提供者

行业应用团队是本体形成生态的关键，也是本体家族的中坚力量。基于本体的基层区块链架构体系，各行各业优秀的团队可以进行自己相关业务的构建。

同时，本体支持各类服务提供者基于本体进行创业或业务拓展。本体将尽最大可能帮助每一个梦想的实现。

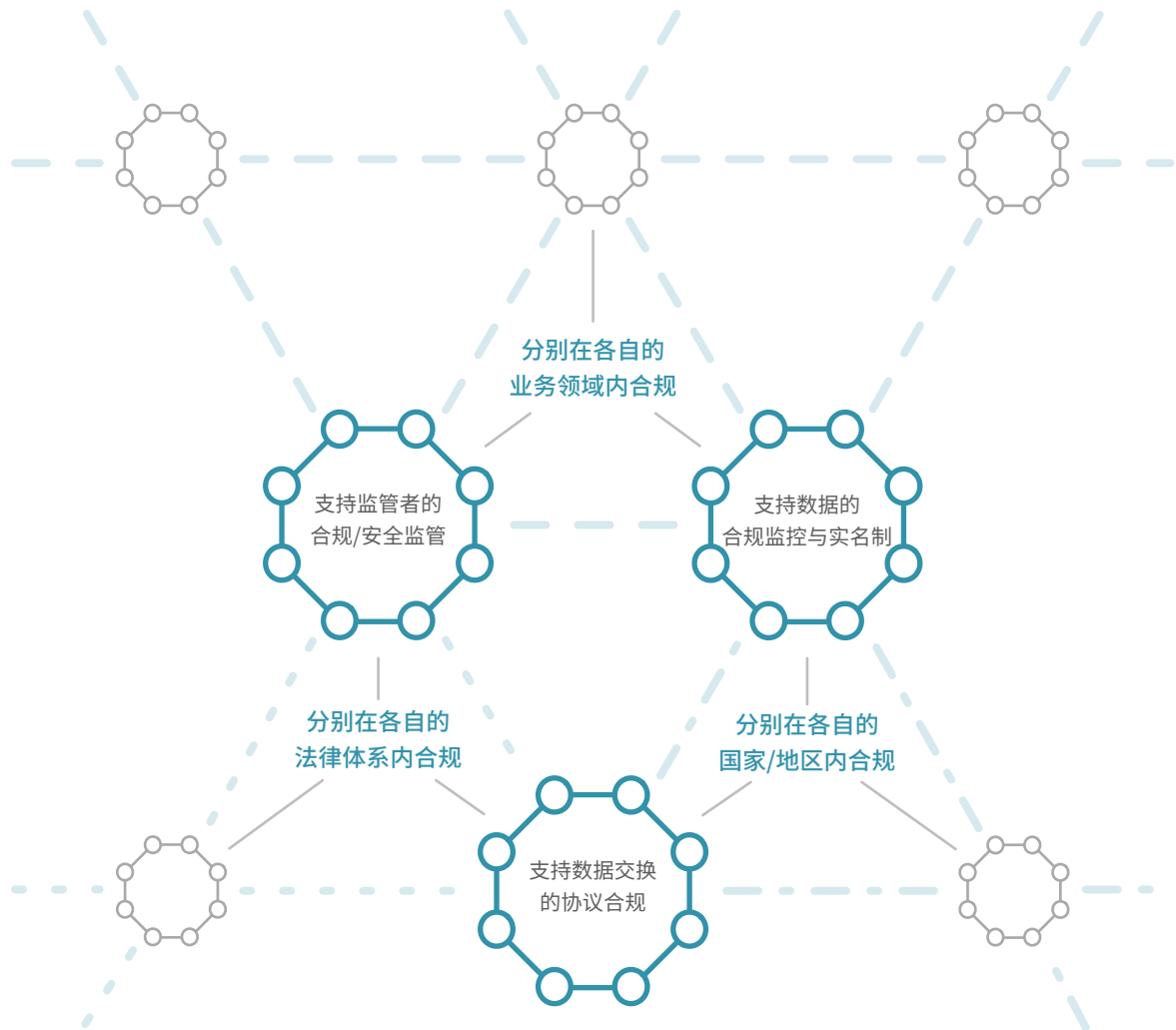
社群

本体重视社群的力量。一方面，本体将通过社区的运用，吸纳来自国内外的机构和个人社区技术人才，为本体的技术实现和技术迭代提供力量；另一方面，本体希望在社群中进行应用的培育，可以通过社群的交流和培训，为社群提供思维碰撞，也可以通过本体团队，为有意向开展应用的个人和团体提供一定程度的技术支持。

个人

在本体家族中，个人是有机力量。本体希望在最大程度上支持更多的个人加入。个人参与本体，为自己建立完整的信任体系，也可为他人进行信任背书，同时也形成自己的可信画像。另外，通过加入本体社群，个人可以为本体生态的发展提供技术、推广、生态发展等贡献，成为本体的一份子。

■ 合规 ■



本体网络的合规支持

- 在不同业务领域的
合规跨链协作
- - - - 在不同法律体系的
合规跨链协作
- . - 在不同国家/地区的
合规跨链协作

信任体系既有其通用型也有其特殊性，特别在不同的地域、应用领域和法规体系下，对身份和信任的要求与各类可信数据源也各有不同，同一个实体（人、机构、物品）在不同的法规体系下和不同的业务场景下，对数据源的等级、认证和规则等都会有不同的法律法规要求。除此之外，在特定的地域和法规体系下，对实体数据的使用范围和数据交换协调的安全规则也各不相同。

因此在不同的法律体制下、业务领域中和地域范围内的合规，以及在合规体制下的数据安全，是本体必须要面对与解决的问题。

本体的链网体系，可以支持不同的法律法规体制，使信任源和数据源在特

定的区域链中符合特定的规则，在跨地域和业务领域的的数据交换中做到相应的协议合规，以及支持对可信数据源和数据交换的观察和审计机制。监管者或观察者可以根据不同的法规或规则，对不同的信任源和数据源进行相应的合规和安全监管。

因此，本体是一个实体世界跟数字世界融合的信任体系，既支持了去中心化的、社群性和分散性的信任源和数据源的协作，也支持不同的业务场景下和法规体系下信任源和数据源的合规，以及各政府的特定要求，这样才能在一个体系下形成全局性和全球性的统一协调，这也是本体在链网和数据安全协议的共享机制下，和在去中心化的体制下，做到对合规与安全的同步支持。

www.

ont.io

■ 联系我们 ■



电子邮件: contact@ont.io



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



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



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



微信公众号: [ONT本体网络](#)



微信客服: [ONT小秘书](#)



