物数链

IOT DATA BLOCK CHAIN

构建 物联网数据生态体系

V1.3

目录

物数链·万物数据互联

物数链，是融合物联网万物互联理论与区块链技术，致力于打造一个万物互联的大数据区块链。传统物联网运行平台采用中心化技术，不管在数据采集或运行上都基于物联网参与的任何一方都是尽职尽责的前提，由于信任机制发展缓慢，严重阻碍了物联网市场的发展.。针对物联网过程中出现的问题，物数链重点围绕区块链技术应用于物联网行业所面临的数据获取、数据并发、数据并存问题，结合区块链—物联网—大数据，构建新一代物联网体系架构

物数链将物联网参与方在每一个环节的数据加以储存，实现资产化转化。同时，物数链借助区块链的特点，为基础数据建立了一个基于技术的信任体系。在物数链中，由于具有不可篡改性和可追溯性，参与者对于交易公平机制有绝对的信任，保障了交易的正常运行。

LDBC（Logistics data block chain）是物数链基础 token，LDBC 通过物数链，促成物联网中商品流通数据的资产化，颠覆了传统数据的获取办法。物数链透过物品基础流通数据，衍生其他智能合约，最终促成真实可信、可溯源、高可用物联网大数据区块链。

第一章 项目背景

1.1 物联网

物联网是新一代信息技术的重要组成部分，也是“信息化”时代的重要发展阶段。其英文名称是：“Internet of things（IoT）”。顾名思义，物联网就是物物相连的互联网。这有两层意思：其一，物联网的核心和基础仍然是互联网，是在互联网基础上的延伸和扩展的网络；其二，其用户端延伸和扩展到了任何物品与物品之间，进行信息交换和通信，也就是物物相息。物联网通过智能感知、识别技术与普适计算等通信感知技术，广泛应用于网络的融合中，也因此被称为继计算机、互联网之后世界信息产业发展的第三次浪潮。

物联网架构分为三层，分别是感知层、网络层和应用层，具体如图 1 所示

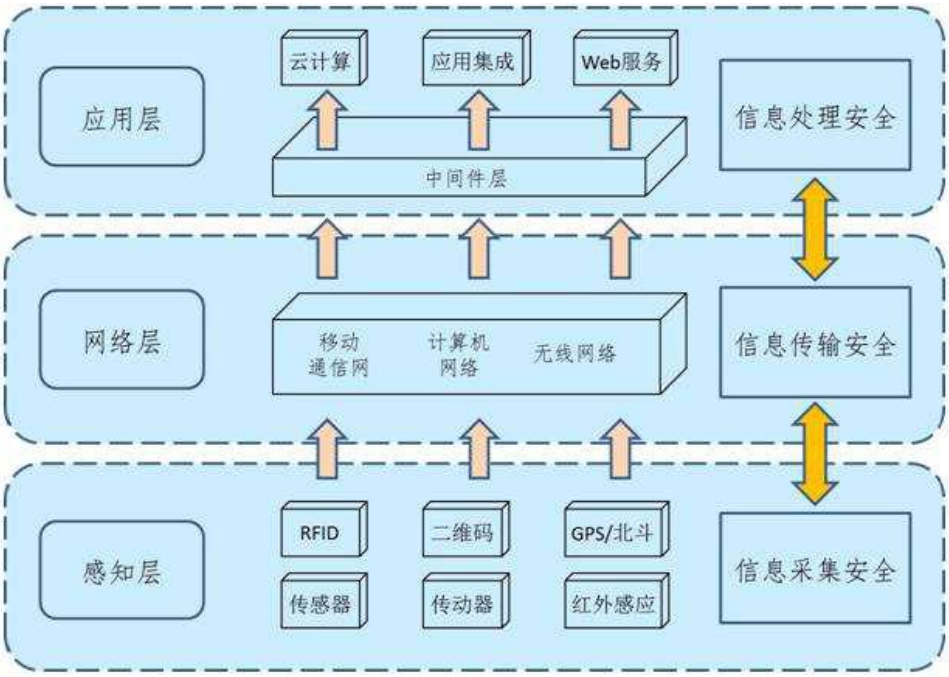


图 1 物联网架构

物联网应用中，有三项关键技术

1. 传感器技术：这也是计算机应用中的关键技术。到目前为止绝大部分计算机处理的都是数字信号,需要传感器把模拟信号转换成数字信号，计算机才能处理。

2. RFID 标签：一种传感器技术，RFID 技术是融合了无线射频技术和嵌入式技术为一体的综合技术，RFID 在自动识别、物流管理有着广阔的应用前景。

3. 嵌入式系统技术：是综合了计算机软硬件、传感器技术、集成电路技术、电子应用技术为一体的复杂技术。经过几十年的演变，以嵌入式系统为特征的智能终

端产品随处可见；小到人们身边的 MP3,大到航天航空的卫星系统。嵌入式系统正在改变着人们的生活，推动着工业生产以及国防工业的发展。

物联网用途广泛，如图 2 所示，遍及多个领域，智能交通、环境保护、政府工作、公共安全、平安家居、智能消防、工业监测、环境监测、路灯照明管控、景观照明管控、楼宇照明管控、广场照明管控、老人护理、个人健康、花卉栽培、水系监测、食品溯源、敌情侦查和情报搜集等多个领域。

图 2 物联网主要应用领域

值得一提的是，物流是物联网技术最重要的应用领域之一，物联网技术是实现智慧物流的基础。物流业作为国民经济发展的支柱性产业，要实现进一步增长，满足越来越高的物流需求，实现智慧物流，必须依赖于物联网技术的全面应用。目前，物联网在物流业相对成熟的应用主要集中在四个方面：产品的智能可追溯网络系统、物流过程的可视化智能管理网络系统、智能化的企业物流配送中心及企业的智慧供应链。

1.2 万物互联的定义

万物互联的定义：主要体现就是我们把分布式物品运行、流通、记录给互联起来，让物品的数据（-运行数据-流通数据）互联起来搭建一个分布式针对各个各业的数据获取模型，实现工业企业低成本地拥抱互联网，生产、支付、流通、售后等服务可视、可控；譬如说：用户可以随时随地了解物品流通过程，了解成本、产地；设备供应商在线进行设备售后服务；服务商在线进行评估、诊断、分析和建议，共同保障物品的安全、高效运行。

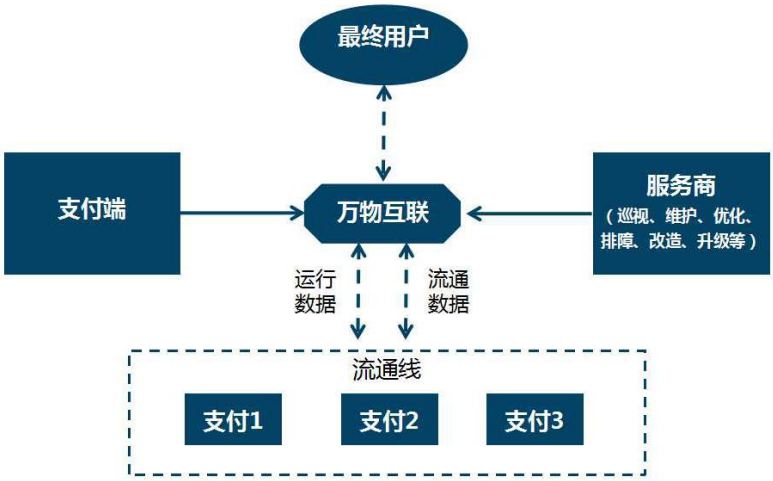


图 3 万物互联运行逻辑

万物互联的几个主要的特征包括：

（1）设备运行数据化

（2）海量数据实时采集、高速传输、云端存储、动态展现

（3）数据远程在线分析

（4）多方协同工作

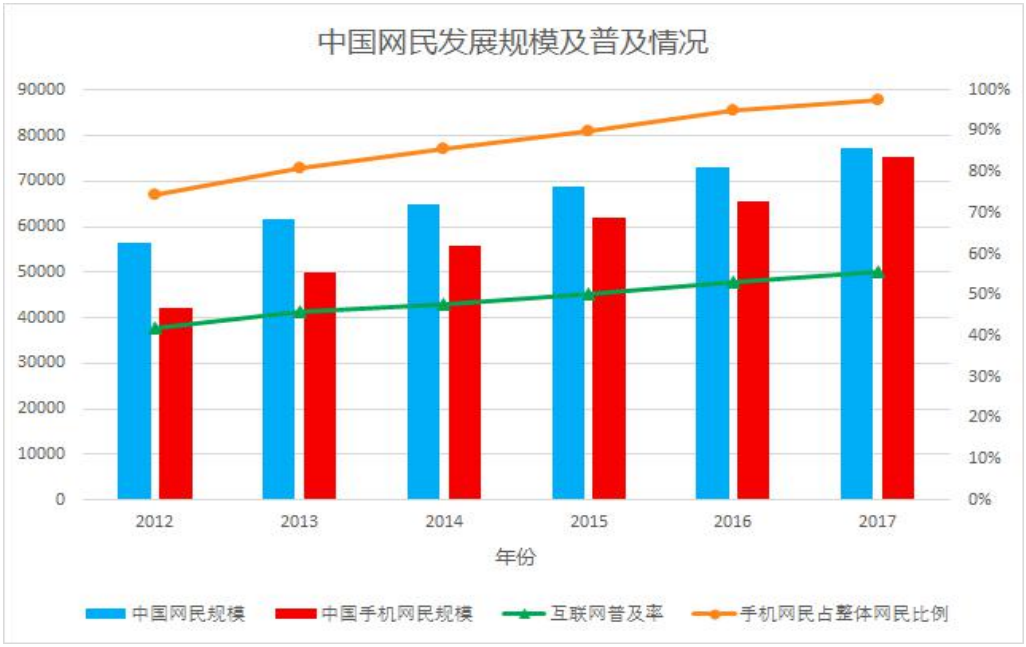
（5）为设备巡检、预测性维护、故障诊断、生产线优化、改造、升级提供数据支持。

1.3 物联网市场分析

物联网被全球公认为继计算机、互联网、移动互联网之后世界信息产业的又一次信息化浪潮，将给人类的生活质量、生产效率带来巨大升级，具有十分广阔的市场前景。物联网行业发展，无论是近年来的实际强劲表现还是投资人的乐观预期，都在告诉我们物联网的时代正快速到来。其主要原因如下：

1.3.1 物联网深度融入生活场景，爆发条件成熟

近年来，互联网获客成本提高，以物互联时代正式开启。互联网用户总数趋于饱和，获客成本快速增加。据 CNNIC 统计，在经历前几年的快速增长后，我国网民总数和移动互联网用户数量增速已趋于缓和。2017 年全国网民规模总数为 7.72 亿人，其中移动互联网用户超过 7.53 亿人。用户总数正趋于饱和，对互联网公司而言意味着获客成本的迅速提升。



数据来源：中国互联网络信息中心(CNNIC)

图 4 中国网民发展规模及普及情况

在以数据称王的当下，线上数据获取渠道的逐渐枯竭促使互联网企业纷纷将注意力转至线下，而物联网技术作为连接线下和线上的最终途径正成为他们投入的重要方向。在创新技术的驱动下，可穿戴设备、智慧零售、共享经济等以物联网为主要工具的商业模式正取代工业物联网成为物联网商业化的主流，甚至是引领未来几年物联网快速发展的新生力军。

物联网正处于飞速增长阶段，一个全球化的智能互联时代已经到来。根据 IDC 的统计，到 2020 年该数字将达到 12899 亿美元，年复合增长率约为 15.02%。根据全球移动通信系统协会（GSMA）发布的报《Spectrum for the Internet of Things》，2015 年全球物联网规模为 0.89 万亿美元，预计到 2020 年全球物联网市场规模将达到 1.9 万亿美元，按此计算，2015 至 2020 年全球物联网市场规模年均复合增长率为 16.38%。作为物联网软件和数据传输的载体，2016 年全球物联网安装设备已达到 148.66 亿台，而五年后全球设备数量将超过 300 亿台，年复合增长率达 20.2%。

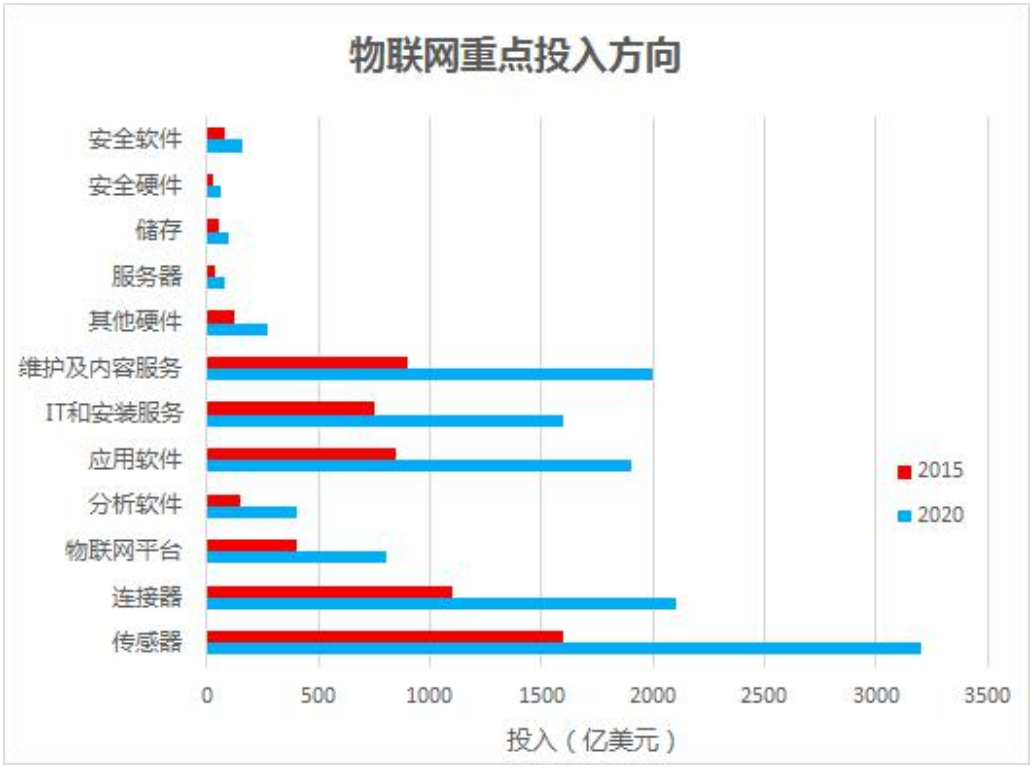
图 5 全球物联网连接设备数

2014 年国内物联网产业规模为 6200 亿元，同比增长 24%，M2M 连接数超 7300 万，同比增长 46%，占全球 M2M 连接数的 30%，继续保持全球第一大市场地位。在过去的几年中，我国物联网产业复合增长率超 30%，增长势头强劲。根据中国产业信息网预测，未来五年国内物联网市场将从 2016 年的 9300 亿元人民币增长到 2020 年的 18300 亿元，整体规模将以倍数增加。

图 6 全球物联网连接设备数

1.3.2 从传感器成本的下降到低功耗广覆盖技术的出现

传感器成本的下降使物联网大规模应用成为可能。传感器是物联网感知层的设备，包括温度传感器、压力传感器、麦克风等等。据 IDC 统计，2015 年全球对传感器的投入占对物联网总投入的四分之一，而到 2020 年，对传感器方面的投入将突破 3151 亿美元，远超其他技术。传感器作为物联网的底层配件，是支撑整个物联网运行的关键设备，投入量越大意味着未来可获取的数据越多。而对于物联网运营商而言，大规模投入传感器的基础仍在于其成本的持续下降。



资料来源：IDC

图 6 全球物联网投入方向

传感器行业竞争加剧，价格有明显下降趋势。由于传感器行业所遵循的摩尔定律，即集成电路上可容纳的元器件的数目，每隔约 18 个月便要增加一倍，性能也将提升一倍，但同时价格维持不变。因此在过去十年间，一些传感器的价格猛降了 100 倍。此外，MEMS 技术的出现使得芯片成本进一步下降。近几年全球传感器出货量大幅增长，但行业营收却增长不大。根据 IC Insights 预测，2016 年-2020 年所有半导体传感器的平均售价的年复合增长率将达-5%，而前五年大约是-2.5%。技术的持续更新和市场的竞争饱和将成为传感器持续降价的主导因素。在这样的条件驱动下，物联网的大规模部署将成为必然趋势。

低功耗广覆盖技术的出现使物联网链接更为持久广泛。目前物联网的主要连接方式还是以 WiFi、蓝牙及 ZigBee 等技术为主，应用于室内和短距离数据传输场景。据统计，目前短距离连接的极限是 WiFi 和蓝牙的 200 米，这意味着大范围的室内场景和远距离数据传输场景对物联网技术的应用将因此而受限。随着物联网连接环境和物品种类的不断扩大，经济活动对物联网的应用在通信技术的连接范围提出了更高的要求。然而，由于当下作为远距离通信主要手段的 2G\3G\4G 技术能耗高，同时更适用于庞大数据量传输，在低频次应用场景中并不具备高效性，因而进一步推动了市场对低功耗远距离传输技术的需求。

近年来，低功耗广域网技术快速兴起，以功耗低、距离远等特点迅速吸引了市场的注意。低功耗广域网技术可分为非 3GPP 组织主导的基于非授权频段的 LoRa 和 Sigfox 等技术，和 3GPP 组织主导的基于授权频段的 eMTC、NB-IoT 和 EC-GSM 等技术。此前，Semtch 公司的 LoRa 技术和 Sigfox 公司的 Sigfox 技术已经率先开始商业化，但因为存在信号干扰等问题，始终没能得到广泛应用。2016 年，3GPP 组织正式推出 eMTC 和 NB-IoT 标准技术，基于授权频段的突出优势迅速吸引大量厂商跟进。

因为技术的演变，使得物联网的应用场景更为广泛。低功率广域网技术已在智能计表、地质勘测等领域首先展开应用，并逐渐与垃圾站、消防用品等低频次城市资产相结合，在智慧城市这一领域将物联网的连接范围进一步扩大。随着配套设施的完善，低功率技术将有望进入更多实体经济领域。通过发挥广域数据传输和低功率节能特性，远距离资产跟踪（如共享单车等）和小型设备通信（如可穿戴设备等）将成为 LPWAN 对物联网整个产业的新的开拓方向。同时更多的长尾物品将因为这类技术的成熟陆续加入物联网的连接范畴，使数据源的量级得到进一步提升。

互联网饱和导致向物联网的转变、物联网关键器件的技术突破与成本降低构成了物联网未来持续增长的动力来源。

1.4 物联网发展瓶颈

1.4.1 孤岛效应

物联网的项目众多，发展迅速，但是由于信息技术水平，安全性防范，标准化的制定严重落后，大部分的项目都还是处于初期概念验证（PoC）阶段，究其原因，就是存在大量的孤岛。

（1）数据孤岛：物联网企业的数据往往都各自存储和定义。每个行业的数据都无法和其他领域的数据进行连接互动，形成一个个数据孤岛。简单说就是数据间缺乏关联性，数据库彼此无法兼容，同时也导致不同物流企业对用户数据重复收集，数据价值无法在用户体验上达到最大化。

（2）信息孤岛：在物联网经济深入私人领域的同时，也造成了企业对用户信息了解的难题。互联网上大量信息甄别成本巨大，传统企业对用户信息获取渠道单一，同时用户征信孤岛中关于对客户的征信的描述在各类行业中的信息标签并不一致，这些都导致了信息孤岛化。

（3）用户征信孤岛：物联网企业虽然对用户在其产皮 内使用的数据有所记

录，但无法判定新用户的综合信用水平。由于需要对用户征信保密，而且不同领域的使用者有不同的使用权限，所以企业无法判定每个用户的个人综合信用，这导致了用户征信孤岛化。

1.4.2 中心化运作模式存在明显弊端

物联网数据是参与物联网中所有商品、服务的经济化数据轨迹，由于现行物联网发展现状，孤岛无法消除。物联网独立化运营也即是中心化运作模式会带来明显弊端，让行业数据、用户信息数据、征信体系无法连接使用。这些弊端在形态上又分为两种：分散中心化和集成中心化：

（1）分散中心化弊端：表现为由单独的物联网参与企业独立管理用户数据、信息和征信体系，但是由于各行业规范不一，数据篡改难度简单，无法保证数据真实性，企业无法使用户规范使用服务，也无法了解用户关键信息、使用轨迹和平台流向。同时，用户的数据在物联网之间无法产生直接关联。

（2）集成中心化弊端：表现为集成平台型物联网企业和供应链企业统一运营管理数据，但是由于集成体系下的运营商众多，在利益分配不均的基础上很难形成真正的高效互联，使信息共享困难重重，集成运营商很难从各大运营商的前后台中获取真实的数据。同时，用户数据得不到有效性保护，如遭遇攻击篡改，后果不堪设想。

物联网当中的信息孤岛效应与中心化的运作模式会在一定程度上减缓未来物联网的发展速度，但随着区块链技术的发展与逐渐普及，这一问题将得到完美的解决。

1.5 区块链简介

区块链是一种按照时间顺序将数据区块以顺序相连的方式组合成的一种链式数据结构， 并以密码学方式保证的不可篡改和不可伪造的分布式账本。一般说来，区块链系统由数据层、网络层、共识层、激励层、合约层和应用层组成。其主要特征为：

（1）去中心化：由于使用分布式核算和存储，不存在中心化的硬件或管理机构，任意节点的权利和义务都是均等的，系统中的数据块由系统中具有维护功能的节点来共同维护；

（2）开放性：系统是开放的，除了交易各方的私有信息被加密外，区块链的数据对所有人公开，任何人都可以通过公开的接口查询区块链数据和开发相关应用，

因此整个系统信息高度透明；

（3）自治性：区块链采用基于协商一致的规范和协议（比如一套公开透明的算法）使得整个系统中的所有节点能够在去信任的环境自由安全的交换数据，使得对“人”的信任改成了对机器的信任，任何人为的干预不起作用。

（4）信息不可篡改：一旦信息经过验证并添加至区块链，就会永久的存储起来，除非能够同时控制住系统中超过 51%的节点，否则单个节点上对数据库的修改是无效的，因此区块链的数据稳定性和可靠性极高。

（5）匿名性：由于节点之间的交换遵循固定的算法，其数据交互是无需信任的（区块链中的程序规则会自行判断活动是否有效），因此交易对手无须通过公开身份的方式让对方自己产生信任，对信用的累积非常有帮助。

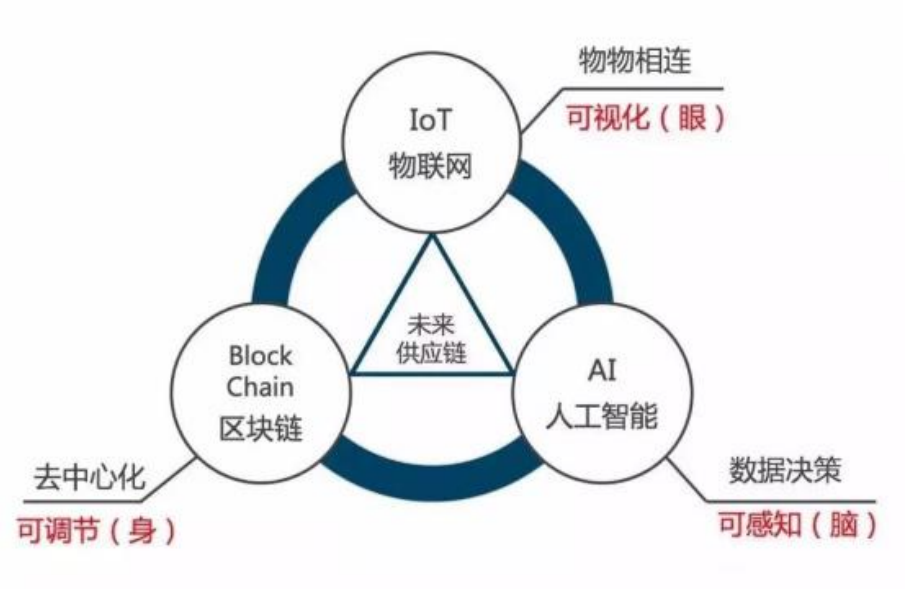


图 7 全球物联网投入方向

仔细梳理不难发现，借助区块链技术作为创造信任的机器，可以有效解决物流市场中交易主体间的诚信机制建立问题；借助区块链技术在支付交易系统中的高效率交易优势，可以有效提高物流市场交易效率；借助区块链技术分布式的技术特征，可以有效提升物流市场治理能力和行业管理水平。

1.6 区块链与物联网撮合

区块链技术和物联网行业发展存在着充分的“合作空间”。一方面，物联网行业的商业模式，在某种程度上恰恰并不进行共享，他们通过中心化聚合资源，然后统一分配出去，更像是一种聚合经济。然区块链的本质，却是不再强调集中，把分散化的社会资源，用点对点的方式，让参与者各自以不同的方式付出和受益。另一方面，区块链的精要是弱控制、分中心、自治机制、网络架构和耦合连接，通过分布

式的节点支撑起真正的点对点沟通，做到去中介化的信任。总的来说，区块链带给物联网行业的改变有如下几个方面：

从中心化到去中心化，构建物联网行业生态圈。区块链的真正价值在于促进各行各业的中心化机构之间达成共识、构建联盟，形成多个中心组成的商业生态圈，这样的生态系统突出中心的职能，大大简化了中心化机构运营成本。比如在跨境汇款领域，通过借助区块链去中心化的网络进行全球范围内的货币流通和国际金融结算，同时还可以允许用户向世界上任何人进行转账而不需要支付高额的服务和交易费用，可以实现实时汇款，不仅大幅节约成本，同时也极大提升了跨境汇款的效率。

从不信任到信任，共享行业信任危机成为过去式。区块链的去信任化特性，基于互不信任的原则，整个系统的运作是公开透明的，通过“签名”机制和利用“少数服从多数”的朴素方式，却能够从机制上保障信用。比如在物流平台上，通过区块链技术的运用，用户可以随时查看真实商品流通记录和各大线路的运力配置，不必担心数据造假。

从不安全到安全，打消用户信息担忧。首先，用户数据以块链结构存储，具有自校验性，篡改之后可以迅速发现。其次数据在多个节点都有相同的备份，即使某个节点上的数据被修改，也可以从其他节点上自动恢复过来，从机制上杜绝了黑客的数据篡改袭击。借助区块链技术，用户能够随时随地查看物联网中的真实不可篡改信息。

区块链是第一个能够真正做到去中介化信任的技术，这意味无须经过任何第三方的共享经济成为可能，还能通过借助智能合约技术自动执行满足某项条件下的操作，也能够使得更多物品安全，大幅降低契约建立和执行的成本。比物流企业的数据信息，在区块链技术帮助下会共享准确的、可信的、可量化的数据指标，通过权威的第三方征信机构可以获得更权威可信的用户信息分析和建议。

第二章 物数链的作用

2.1 “物数链”的定义

物数链全称物联网数据区块链，是利用区块链技术对物联网参与方产生的数据进行记录、储存。通过利用 TOKEN 和智能合约获取物联网参与方不可逆转的商品流通记录。由于物数链是全开放式的，允许各种物联网创新型企业基于物数链的基础发行智能合约和专用 TOKEN,促进各领域互通形成物联网大数据，达到更高效的数据整合，打造一流的去中心化物联网生态圈，推动各主体间的商业创新和协同合作，也让用户通过 TOKEN 奖励机制更好地推进物联网“共建、共有、互联、互通”。

（1）物联网平台将链接各大物联网产业数据接口，以去中心化数据结构形成生态圈。具体而言，物数链或者其他物联网参与方会利用物联链的技术发布新的智能合约，接入用户愿意提供的各项数据（身份数据、关系数据、偏好数据、行为轨迹数据、征信数据），并且将所有行业中的个人数据链接至区块链的服务层应用中，基于共享账本、数字资产和鉴证服务反馈分析后形成群体数据集。毫无疑问，多个行业主体之间的交互将产生海量数据，在协同交互过程中扩散和流动，多形态的数据跨领域融合形成物联网大数据（包括用户行为数据、用户信用数据）。

（2）各大物联网行业运营商可以利用综合用户数据，进行跨领域合作和营销创新。多维度的用户行为数据将带给运营商更全面的画像，可以提供新角度新视野的营销灵感。还可以关联全行业用户的信用评分，开放供应商用户征信体系，去粗取精完善整个行业的信用规范以期提供更优质的服务。总的来说，就是可以实现基于物联网产生数据的智能分析和生态圈的行业应用及服务。

（3）引入代币机制，激励各行业用户共同参与。代币（Token）是在共同维护区块链系统安全运行的前提下的可以流动的加密的数字权益证明，是对系统中参与者的酬劳和激励，它随时随地可被验证、被交易、兑换，在以区块链为交易和流转的基础设施中，也具有匿名性、无缝的流转性、快速交易、可跨国交易的特点。

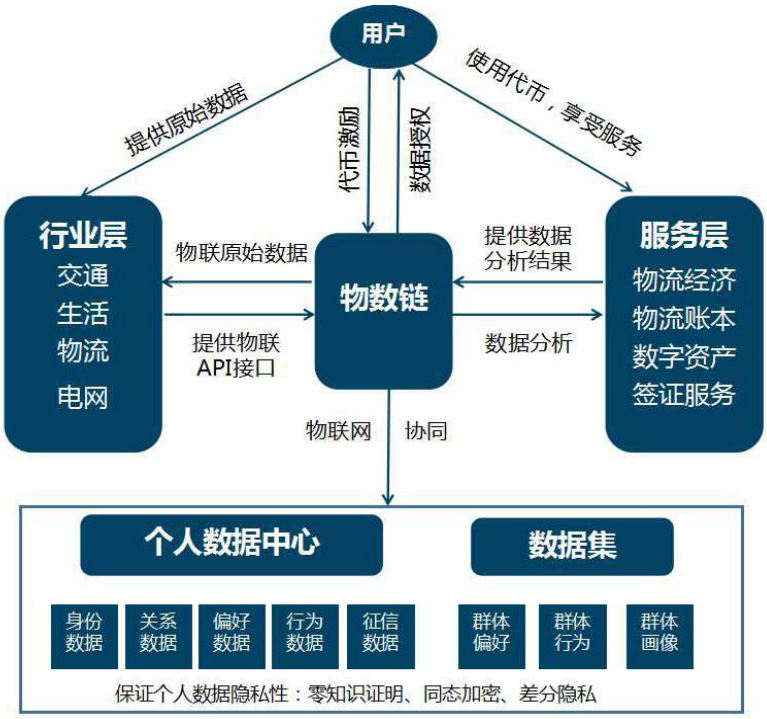


图 8 去中心化的物数链数据结构

区块链技术与物联网数据相结合的全新服务平台，为物联网参与者提供一个商品流通性透明真实，质量可靠，源头可溯的数据一体化网络，由于区块链技术的引入，“物联网”平台上的每一种服务都具有物联网特性的生产交易数据形成去中心化的数据轨迹，每一种行为都被完整记录，形成数据轨迹并记录在平台里，由于去中心化内容不可篡改，消费更加放心，流通更加便捷，支付更加安全。随着“物数链”技术的成熟，一种新的商品流通性与区块链融合的新生态物数链正在形成，会为消费者创造更优质的消费体验服务。为物联网的真正形成，发展提供有效数据保障。

2.2 物数链的优势

物数链充分融合区块链技术与物联网万物互联原理，能够进一步突破物联网的瓶颈，充分发挥区块链的技术优势，两者的完美融合，让物数链拥有了以下几点完美的特点，如图 9 所示：

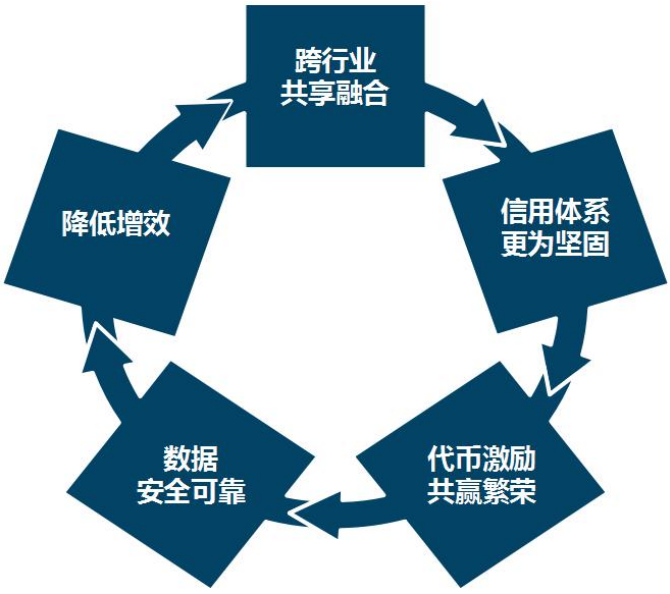


图 9 物数链平台特点

（1）去中心化结构消除数据孤岛，跨行业数据融合共享。平台提供统一的数据市场平台，打破各个行业间数据交互分享的壁垒，支撑跨行业数据应用开发的门槛。让数据易采集、易存储、易理解、易处理、有价值。针对逻辑性的信息孤岛，我们可以采用制定数据规范、定义数据标准、建设维护元数据的方式。针对物理性的信息孤岛，我们可以在合适的时机，对企业的主要业务流程进行整合，根据这样的流程，结合战略，把不同的业务系统串接起来，使数据相互形成联系。

（2）降低成本，高效物联。平台提供完善的标准体系、用户知识库以及用户、开发者社区，助力物联网生态建设。区块链可以为这个共享行业生态圈网络提供容纳性的、可信任的基础设施。可以降低中心化设备的运营和信用成本，提高运营效率和行业资产利用率。

（3）更为安全可靠的数据，不可篡改，隐私完全归属于用户。数据通过区块链的加密方式、身份验证、授权机制等技术存储于去中心化资源上，除了用户本人任何机构和个人都无法接触用户的原始数据。数据只有在用户同意授权下能够被有限地开放。在密码学的差分隐私加密下，应用可以对用户的部分数据进行大数据等研究，但无法解析个人数据，更不能查看，复制，篡改数据。

（4）智能合约让信用体系更为坚固。在平台中所有行业契约型的约定都实现智能化，利用智能合约自动执行双方所达成的契约，排除了人为的干扰因素，从制度上防止任何一方的抵赖。LDBC Token 可以保障所有约定的可靠执行，避免篡改、抵赖和违约。将社会中的零散数据转变为数字智能资产进行确权。

（5）统一正向激励参与者，共赢生态繁荣。代币体制让个体行为价值化、货币

化，可以有效地激励行业发展良性循环，凡是对物联网生态圈做出价值贡献的任何个体行为，即使是用户自发的、自愿的和小微的行为，都可以以 Token 的形式价值化和货币化，被激励。也即是通过基于 Token 激励模型设计，可以在一个统一维度上的正向激励所有产业参与者，从而所有人通力合作共创和共赢生态繁荣。

2.3 物数链数据模型

物流链将打造一个开放的物联网数据系统，物联网参与者提供数据的同时，平台通过流式计算框架形成每个行业独特的数据模型（指对各类用户行为、征信数据特征的抽象组织），每个供应商都可以通过平台获得这些数据模型以对接本行业用户信息。并且，用户的每次行为在物数链会自动化匹配到数据模型上，以不停地完善模型构造。

比如，物流领域数据模型，就是指描述物流行业物品的符号记录，包括用户可以完整回溯商品从原材料、到加工、到制作、到运输、到销售、配送位置、信用记录，等每一个环节的信息，每一个静态行为、动态特征和约束条件构成的数据点将经过计算框架形成模型。

而当供应商商拥有这些数据模型后，由于加密标识使得这些独特的用户信息更不易被盗取或者被其他供应商查阅，更好地做到了匿名、安全、可靠、唯一。

整体来看，物数链大数据平台又细分为数据运行平台与观测服务平台。

2.3.1 数据运行平台

物数链运行大数据，是指货物参与物联网中的周期中，所生产的生产、交易、支付、流通等行为数据。物数链以物品的流通行为为基础，叠加各行业相关业务信息，围绕各行业资源共享范围和授权使用范围，建设协同区块链大数据架构。

在当前物联网政策法规不健全、行业信息系统相对独立的现实情况下，平台采取“物理分散、逻辑集中”的方式，以统一平台开放数据交换接口的方式推动数据共享和开放，是最具可行性的。整个物数链协同大数据平台由 7 个部分组成，包括内部应用和外部数据对接、数据类别、数据应用平台、数据物数链交换平台、数据存储处理架构等，具体如图 10 所示

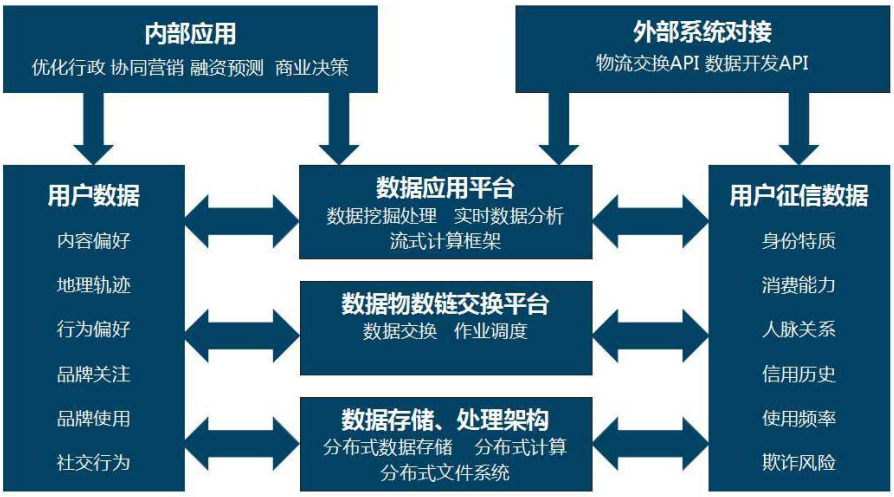


图 10 物数链平台特点

具体来看，主要内容有：

（1）用户行为数据：用户在共享产品或服务的使用时间周期内的行为数据，包括内容偏好、地理轨迹、行为偏好、品牌关注、品牌使用和社交行为等数据；

（2）用户征信数据：用户在共享产品或服务的使用时间周期内的评分体系相关数据，多维度包括身份特质、消费能力、人脉关系、信用历史、使用频率和欺诈风险等数据。并且用户的行为数据是显著影响征信数据的形成，这些极具价值的隐私数据都将通过加密技术进行编码，匿名化的信息权限由用户掌握。

（3）外部系统对接：主要由平台公开基础源码给各物联网行业，允许其他物联网企业基于物数链进行智能合约的发布。

（4）数据应用平台：通过自主建模和数据挖掘技术，挖掘数据形成自动报表或其他展现形式为数据分析服务。然后通过流式计算框架进行实时数据分析。

（5）数据物流交换平台：包括①数据交换作业调度中的数据抽取、转换、加载、大文件传输和数据源适配器，以方便数据调度。②数据交换作业管理、监控和日志统计等。

（6）数据存储、处理架构：通过分布式存储、分布式计算和分布式文件系统来存储、处理海量的结构和非结构化的数据。通过区块链技术达到去中心化。

（7）内部应用：对于各物联网行业来说，应用领域主要有：①优化行政效率、②协同营销，跨行业跨领域合作营销、③融资预测、④辅助商业决策。

2.3.2 观测服务平台

参与物联网中的物品数据的观测，即物联网参与者使用产品或服务时会贡献各

类行为数据，包括内容、地理轨迹、行为偏好和社交行为等数据。由物联网数据平台对该观测数据进行分析并上传物联网行为的加密数据，使物联网参与者行为数据整合提供精准的用户人群画像，使物联网企业信息收集与信息管理有正向帮助。

2.4 物数链数据优势

物数链定位于未来工业 4.0 的核心支撑平台、物联网大数据及区块链面向智慧工业过程提供集数据采集、存储、计算、分析及高级可视化于一体的数据基础，用户可利用物数链提供的组态合约、智能合约。物数链数据体系主要服务于广大物联网参与方，除此之外，随着物联链数据的发展还会将业务扩展到其他领域，充分发挥平台的优势。在未来制造行业中扮演着推动智能制造发展、主导智慧工业发展方向、构建制造业新秩序的角色。物数链快速、低成本地拥抱互联网，实现生产过程的可视、可控；唤醒沉睡的零碎数据；打破信息孤岛，实现数据共享；让你的数据创造价值，从而促进生产运行更高效。

（1）数据追溯体系

数据追溯体系，是指可以对用户行为或征信体系进行正向，逆向或不定向追踪的数据完善系统。只要用户在物数链上产生经济行为，数据追溯系统将会一直采集用户行为习惯，一直到形成每一个用户的独特数据链，完善数据模型系统。此系统的开放是为各供应商打通了一条更为深入了解用户信息的通路，以解决信息杂音太多、不对称、不透明的问题。

（2）全开放性体系

区块链系统具有开放性。基于区块链技术的物数链系统中，除了交易各方的私有信息被加密外，区块链的数据对所有人公开，任何人都可以通过公开的接口查询区块链数据和开发相关应用，因此整个系统信息高度透明。因此，在物联网中，平台建立了一个数据获取源头开放体系，在保护数据私密信息的前提下，消费大数据的使用者可以通过平台查看数据获取的来源。

（3）智能合约机制

智能合约是区块链平台的基础。借助智能合约，可以在处理交易时安全地应用规则。可以使用它们自动执行验证步骤，对过去包含在已签署的物理合约中的条件进行编码。

智能合约意味着区块链交易远不止代币买卖，将会有更广泛的指令嵌入到区块链中。传统合约是指双方或者多方协议做或不做某事来换取某些东西，每一方必须

信任彼此会履行义务。而智能合约无须彼此信任，因为智能合约不仅是由代码进行定义的，也是由代码强制执行的，完全自动且无法干预。基于物联链中增加其他智能合约，更好的推进生产环节、支付环节、贸易环节的数据共享和数据获取。

2.5 物数链 TKOEN 体系

为了鼓励更多物联网参与者为这样一个公共性系统提供计算、存储、数据资源，物数链每个区块产生一定量的物流数据区块链（LDBC）作为为物数链提供资源的激励，使用 LDBC 可以参与记账人选举、转账、发布和使用物流数据资源等。

LDBC 是物数链基础代币， TOKEN 由物数链全球基金会发行，并且可以在平台使用。

1.用户可以使用 LDBC 基于物联链进行物流数据交换。

2.用户在物数链其他支持 LDBC 智能合约上使用。

3.物数链上其他 TOKEN 都需要消耗一定的 LDBC。

4.拥有 LDBC 代表在物数链的权利证明，参与相关投票。

根据“物数链”的运行机制，节点会组成了一个个的物联网网络，而且这些节点能够互相交换 LDBC，当完全节点创造了一个区块，并将交易放入这个区块之后，将写满交易的区块链接在已有的区块链上，系统会奖励一定量的 LDBC。这一过程称之为挖矿。

2.5.1 去中心化治理

在去中心化治理系统中，任何决定都要在一个固定时间内完成投票，这个时间根据提议内容不同而发生改变。当且仅当收集到足够高权益的投票，提议才会执行，否则提议将会关闭。在去中心化自治系统中，并不是权益高者的一言堂，权益低者可以联合在一起制衡权益高者。

去中心化自治内容包括但不限于交易所注册、币种注册、统计函数、抵押代币范围等，这些升级可以通过自治系统参与者共同投票参与决定。

第三章 物数链与区块链技术高度耦合

3.1 物数链

物数链的目的是基于链上元协议（on-chain meta-protocol）、脚本、智能合约、跨链协同、分布式储存概念进行整合和提高，使得开发者能够创建任意的基于共识的、可扩展的、标准化的、特性完备的、易于开发的和协同的数据展现及数据储存平台。通过建立终极的抽象的基础层-内置有图灵完备编程语言的区块链-使得任何人都能够创建合约和去中心化应用，并在其中设立他们自由定义的所有权规则、交易方式和状态转换函数。

3.2 物数链账户

在账户系统中，状态是由被称为“账户”（每个账户由一个 20 字节的地址）的对象和在两个账户之间转移价值和信息的状态转换构成的。LDBC 的账户包含四个部分：

- 随机数，用于确定每笔交易只能被处理一次的计数器
- 账户目前的余额
- 账户的合约代码
- 账户的存储（默认为空）

LDBC 是物数链内部的主要加密燃料，用于支付交易费用。一般而言，有两种类型的账户：外部所有的账户（由私钥控制的）和合约账户（由合约代码控制）。外部所有的账户没有代码，人们可以通过创建和签名一笔交易从一个外部账户发送消息。每当合约账户收到一条消息，合约内部的代码就会被激活，允许它对内部存储进行读取和写入，和发送其它消息或者创建合约。

3.3 消息和交易

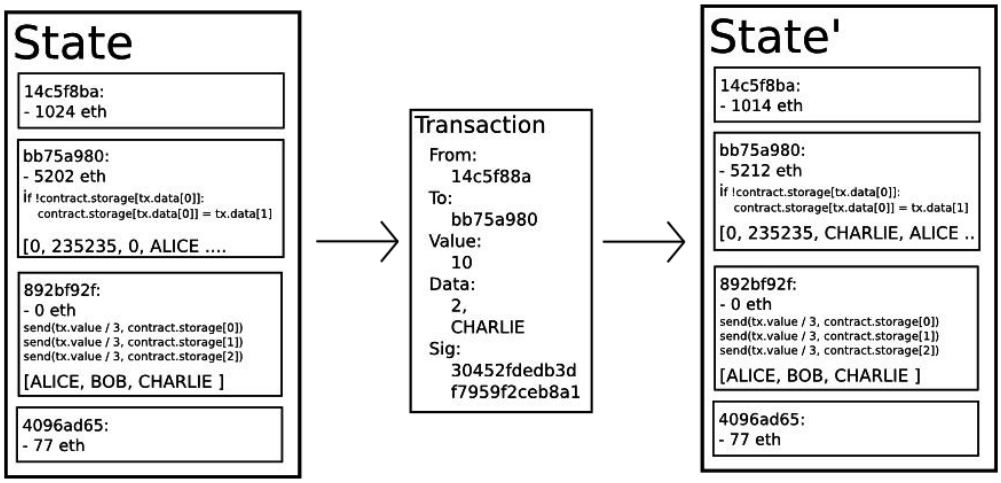
第一，消息可以由外部实体或者合约创建，然而比特币的交易只能从外部创建。第二，消息可以选择包含数据。第三，如果消息的接受者是合约账户，可以选择进行回应，这意味着物数链消息也包含函数概念。

物数链中“交易”是指存储从外部账户发出的消息的签名数据包。交易包含消息的接收者、用于确认发送者的签名、币账户余额、要发送的数据和两个被称为 STARTGAS 和 GASPRICE 的数值。为了防止代码的指数型爆炸和无限循环，每笔

交易需要对执行代码所引发的计算步骤-包括初始消息和所有执行中引发的消息-做出限制。STARTGAS 就是限制，GASPRICE 是每一计算步骤需要支付矿工的费用。如果执行交易的过程中，“用完了燃料”，所有的状态改变恢复原状态，但是已经支付的交易费用不可收回了。如果执行交易中止时还剩余燃料，那么这些燃料将退还给发送者。创建合约有单独的交易类型和相应的消息类型；合约的地址是基于账号随机数和交易数据的哈希计算出来的。

消息机制的一个重要后果是物数链的“头等公民”财产-合约与外部账户拥有同样权利，包括发送消息和创建其它合约的权利。这使得合约可以同时充当多个不同的角色，例如，用户可以使去中心化组织（一个合约）的一个成员成为一个中介账户（另一个合约），为一个偏执的使用定制的基于量子证明的兰波特签名（第三个合约）的个人和一个自身使用由五个私钥保证安全的账户（第四个合约）的共同签名实体提供居间服务。物数链不需要关心合约的每一参与方是什么类型的账户。

3.4 物数链状态转换函数



物数链状态转换函数：APPLY(S,TX) -> S’，可以定义如下：

1 检查交易的格式是否正确（即有正确数值）、签名是否有效和随机数是否与发送者账户的随机数匹配。如否，返回错误。

2 计算交易费用:fee=STARTGAS * GASPRICE，并从签名中确定发送者的地址。从发送者的账户中减去交易费用和增加发送者的随机数。如果账户余额不足，返回错误。

3 设定初值 GAS = STARTGAS，并根据交易中的字节数减去一定量的燃料值。

4 从发送者的账户转移价值到接收者账户。如果接收账户还不存在，创建此账户。如果接收账户是一个合约，运行合约的代码，直到代码运行结束或者燃料用完。

5 如果因为发送者账户没有足够的钱或者代码执行耗尽燃料导致价值转移失败，恢复原来的状态，但是还需要支付交易费用，交易费用加至矿工账户。

6 否则，将所有剩余的燃料归还给发送者，消耗掉的燃料作为交易费用发送给矿工。

例如，假设合约的代码如下：

```
if !contract.storage[msg.data[0]]:
contract.storage[msg.data[0]] = msg.data[1]
```

需要注意的是，在现实中合约代码是用底层虚拟机代码写成的。假设合约存储器开始时是空的，一个值为 10 个币，燃料为 2000，燃料价格为 0.001 个币并且两个数据字段值为[2, ‘CHARLIE’] [3]的交易发送后，状态转换函数的处理过程如下：

1 检查交易是否有效、格式是否正确。

2 检查交易发送者至少有 2000*0.001=2 个币。如果有，从发送者账户中减去 2 个币。

3 初始设定 gas=2000,假设交易长为 170 字节，每字节的费用是 5，减去 850，所以还剩 1150。

4 从发送者账户减去 10 个币，为合约账户增加 10 个币。

5 运行代码。在这个合约中，运行代码很简单：它检查合约存储器索引为 2 处是否已使用，注意到它未被使用，然后将其值置为 CHARLIE。假设这消耗了 187 单位的燃料，于是剩余的燃料为 1150 – 187 = 963。

6. 向发送者的账户增加 963*0.001=0.963 个币，返回最终状态。

如果没有合约接收交易，那么所有的交易费用就等于 GASPRICE 乘以交易的字节长度，交易的数据就与交易费用无关了。另外，需要注意的是，合约发起的消息可以对它们产生的计算分配燃料限额，如果子计算的燃料用完了，它只恢复到消息发出时的状态。因此，就像交易一样，合约也可以通过对它产生的子计算设置严格的限制，保护它们的计算资源。

3.5 代码执行

物数链合约的代码使用低级的基于堆栈的字节码的语言写成的，被称为“物数链

虚拟机代码”。代码由一系列字节构成，每一个字节代表一种操作。一般而言，代码执行是无限循环，程序计数器每增加一（初始值为零）就执行一次操作，直到代码执行完毕或者遇到错误，STOP 或者 RETURN 指令。操作可以访问三种存储数据的空间：

●堆栈，一种后进先出的数据存储，32 字节的数值可以入栈，出栈。

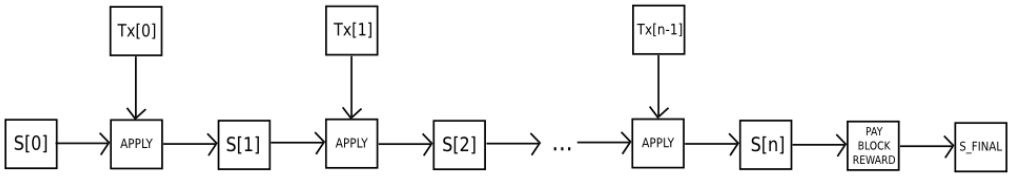
●内存，可无限扩展的字节队列。

●合约的长期存储，一个秘钥/数值的存储，其中秘钥和数值都是 32 字节大小，与计算结束即重置的堆栈和内存不同，存储内容将长期保持。

代码可以象访问区块头数据一样访问数值，发送者和接受到的消息中的数据，代码还可以返回数据的字节队列作为输出。

虚拟机代码的正式执行模型令人惊讶地简单。当物数链虚拟机运行时，它的完整的计算状态可以由元组(block_state, transaction, message, code, memory, stack, pc, gas)来定义，这里 block_state 是包含所有账户余额和存储的全局状态。每轮执行时，通过调出代码的第 pc（程序计数器）个字节，当前指令被找到，每个指令都有定义自己如何影响元组。例如，ADD 将两个元素出栈并将它们的和入栈，将 gas（燃料）减一并将 pc 加一，SSTORE 将顶部的两个元素出栈并将第二个元素插入到由第一个元素定义的合约存储位置，同样减少最多 200 的 gas 值并将 pc 加一，虽然有许多方法通过即时编译去优化，但物数链的基础性的实施可以用几百行代码实现。

3.6 区块链和挖矿



虽然有一些不同，但物数链的区块链在很多方面类似于比特币区块链。它们的区块链架构的不同在于，物数链区块不仅包含交易记录和最近的状态，还包含区块序号和难度值。物数链中的区块确认算法如下：

1 检查区块引用的上一个区块是否存在和有效。

2 检查区块的时间戳是否比引用的上一个区块大，而且小于 2 分钟。

3 检查区块序号、难度值、 交易根，叔根和燃料限额（许多以太坊特有的底层概念）是否有效。

4 检查区块的工作量证明是否有效。

5 将 S[0]赋值为上一个区块的 STATE_ROOT。

6 将 TX 赋值为区块的交易列表，一共有 n 笔交易。对于属于 0……n-1 的 i，进行状态转换 S[i+1] = APPLY(S[i],TX[i])。如果任何一个转换发生错误，或者程序执行到此处所花费的燃料（gas）超过了 GASLIMIT，返回错误。

7 用 S[n]给 S_FINAL 赋值, 向矿工支付区块奖励。

8 检查 S-FINAL 是否与 STATE_ROOT 相同。如果相同，区块是有效的。否则，区块是无效的。

物数链确认效率远超比特币相提并论。原因是状态存储在树结构中（tree structure），每增加一个区块只需要改变树结构的一小部分。因此，一般而言，两个相邻的区块的树结构的大部分应该是相同的，因此存储一次数据，可以利用指针（即子树哈希）引用两次。一种被称为“帕特里夏树”（“Patricia Tree”）的树结构可以实现这一点，其中包括了对默克尔树概念的修改，不仅允许改变节点，而且还可以插入和删除节点。

应用一般来讲，物数链之上一个完美的例子是为解决物流信息共享问题而设的自我强制悬赏。通过独创的环形计算（annular calculate）将数据分享做成一个标准化共识，改进区块链的识别和共识奖励。

3.7 改进版幽灵协议

幽灵协议提出的动机是当前快速确认的块链因为区块的高作废率而受到低安全性困扰；因为区块需要花一定时间（设为 t）扩散至全网，如果矿工 A 挖出了一个区块然后矿工 B 碰巧在 A 的区块扩散至 B 之前挖出了另外一个区块，矿工 B 的区块就会作废并且没有对网络安全作出贡献。此外，这里还有中心化问题：如果 A 是一个拥有全网 30%算力的矿池而 B 拥有 10%的算力，A 将面临 70%的时间都在产生作废区块的风险而 B 在 90%的时间里都在产生作废区块。因此，如果作废率高，A 将简单地因为更高的算力份额而更有效率，综合这两个因素，区块产生速度快的块链很可能导致一个矿池拥有实际上能够控制挖矿过程的算力份额。通过在计算哪条链“最长”的时候把废区块也包含进来，幽灵协议解决了降低网络安全性的第一个问题；这就是说，不仅一个区块的父区块和更早的祖先块，祖先块的作废的后代区块

也被加进来以计算哪一个区块拥有支持其的最大工作量证明。物数链付给以“叔区块”身份为新块确认作出贡献的废区块 87.5%的奖励，把它们纳入计算的“侄子区块”将获得奖励的 12.5%，不过，交易费用不奖励给叔区块。

物数链实施了一个只下探到第五层的简化版本的幽灵协议。其特点是，废区块只能以叔区块的身份被其父母的第二代至第五代后辈区块，而不是更远关系的后辈区块（例如父母区块的第六代后辈区块，或祖父区块的第三代后辈区块）纳入计算。这样做有几个原因。首先，无条件的幽灵协议将给计算给定区块的哪一个叔区块合法带来过多的复杂性。其次，带有物数链所使用的补偿的无条件的幽灵协议剥夺了矿工在主链而不是一个公开攻击者的链上挖矿的激励。最后，计算表明带有激励的五层幽灵协议即使在出块时间为 15s 的情况下也实现了了 95%以上的效率，而拥有 25%算力的矿工从中心化得到的益处小于 3%。

费用因为每个发布到区块链的交易都占用了下载和验证的成本，需要有一个包括交易费的规范机制来防范滥发交易。比特币使用的默认方法是纯自愿的交易费用，依靠矿工担当守门人并设定动态的最低费用。因为这种方法是“基于市场的”，使得矿工和交易发送者能够按供需来决定价格，所以这种方法在比特币社区被很顺利地接受了。然而，这个逻辑的问题在于，交易处理并非一个市场；虽然根据直觉把交易处理解释成矿工给发送者提供的服务是很有吸引力的，但事实上一个矿工收录的交易是需要网络中每个节点处理的，所以交易处理中最大部分的成本是由第三方而不是决定是否收录交易的矿工承担的。于是，非常有可能发生公地悲剧。

然而，当给出一个特殊的不够精确的简化假设时，这个基于市场的机制的漏洞很神奇地消除了自己的影响。论证如下。假设：

1 一个交易带来 k 步操作, 提供奖励 kR 给任何收录该交易的矿工，这里 R 由交易发布者设定， k 和 R 对于矿工都是事先（大致上）可见的。

2 每个节点处理每步操作的成本都是 C (即所有节点的效率一致)。

3 有 N 个挖矿节点，每个算力一致(即全网算力的 1/N)。

4 没有不挖矿的全节点。

当预期奖励大于成本时，矿工愿意挖矿。这样，因为矿工有 1/N 的机会处理下一个区块，所以预期的收益是 kR/N , 矿工的处理成本简单为 kC. 这样当 kR/N > kC，即 R > NC 时。矿工愿意收录交易。注意 R 是由交易发送者提供的每步费用，是矿工从处理交易中获益的下限。 NC 是全网处理一个操作的成本。所以，矿工仅

有动机去收录那些收益大于成本的交易。

然而，这些假设与实际情况有几点重要的偏离：

1.因为额外的验证时间延迟了块的广播因而增加了块成为废块的机会，处理交易的矿工比其它的验证节点付出了更高的成本。

2.不挖矿的全节点是存在的。

3.实践中算力分布可能最后是极端不平均的。

4.以破坏网络为己任的投机者，政敌和疯子确实存在，并且他们能够聪明地设置合同使得他们的成本比其它验证节点低得多。

上面第 1 点驱使矿工收录更少的交易，第 2 点增加了 NC; 因此这两点的影响至少部分互相抵消了. 第 3 点和第 4 点是主要问题；作为解决方案我们简单地建立了一个浮动的上限：没有区块能够包含比 BLK_LIMIT_FACTOR 倍长期指数移动平均值更多的操作数。具体地：

blk.oplimit = floor((blk.parent.oplimit * (EMAFACTOR – 1) + floor(parent.opcount * BLK_LIMIT_FACTOR)) /EMA_FACTOR)

BLK_LIMIT_FACTOR 和 EMA_FACTOR 是暂且被设为 65536 和 1.5 的常数，但可能会在更深入的分析后调整。

3.8 计算和图灵完备

需要强调的是物数链虚拟机是图灵完备的； 这意味着虚拟机代码可以实现任何可以想象的计算，包括无限循环。物数链虚拟机代码有两种方式实现循环。首先，JUMP 指令可以让程序跳回至代码前面某处，还有允许如 while x < 27: x = x * 2 一样的条件语句的 JUMPI 指令实现条件跳转。其次，合约可以调用其它合约，有通过递归实现循环的潜力。这很自然地导致了一个问题：恶意用户能够通过迫使矿工和全节点进入无限循环而不得不关机吗？ 这问题出现是因为计算机科学中一个叫停机问题的问题：一般意义上没有办法知道，一个给定的程序是否能在有限的时间内结束运行。

我们的方案通过为每一个交易设定运行执行的最大计算步数来解决问题，如果超过则计算被恢复原状但依然要支付费用。消息以同样的方式工作。为显示这一方案背后的动机，请考虑下面的例子：

一个攻击者创建了一个运行无限循环的合约，然后发送了一个激活循环的交易给矿工，矿工将处理交易，运行无限循环直到燃料耗尽。即使燃料耗尽交易半途停

止，交易依然正确（回到原处）并且矿工依然从攻击者哪里挣到了每一步计算的费用。

一个攻击者创建一个非常长的无限循环意图迫使矿工长时间内一直计算致使在计算结束前若干区块已经产生于是矿工无法收录交易以赚取费用。然而，攻击者需要发布一个 STARTGAS 值以限制可执行步数，因而矿工将提前知道计算将耗费过多的步数。

一个攻击者看到一个包含诸如 send(A,contract.storage[A]); contract.storage[A] = 0 格式的合约然后发送带有只够执行第一步的费用的而不够执行第二步的交易（即提现但不减少账户余额）。合约作者无需担心防卫类似攻击，因为如果执行中途停止则所有变更都被回复。

一个金融合约靠提取九个专用数据发布器的中值来工作以最小化风险，一个攻击者接管了其中一个数据提供器，然后把这个可变地址调用机制设计成可更改的数据提供器转为运行一个无限循环，以求尝试逼迫任何从此合约索要资金的尝试都会因燃料耗尽而中止。然而，该合约可以在消息里设置燃料限制以防范此类问题。

图灵完备的替代是图灵不完备，这里 JUMP 和 JUMPI 指令不存在并且在某个给定时间每个合约只允许有一个拷贝存在于调用堆栈内。在这样的系统里，上述的费用系统和围绕我们的方案的效率的不确定性可能都是不需要的，因为执行一个合约的成本将被它的大小决定。此外，图灵不完备甚至不是一个大的限制，在我们内部设想的所有合约例子中，至今只有一个需要循环，而且即使这循环也可以被 26 个单行代码段的重复所代替。考虑到图灵完备带来的严重的麻烦和有限的益处，为什么不简单地使用一种图灵不完备语言呢？事实上图灵不完备远非一个简洁的解决方案。为什么？请考虑下面的合约：

C0: call(C1); call(C1);

C1: call(C2); call(C2);

C2: call(C3); call(C3);

…

C49: call(C50); call(C50);

C50: (run one step of a program and record the change in storage)

现在，发送一个这样的交易给 A，这样，在 51 个交易中，我们有了一个需要花费 250 步计算的合约，矿工可能尝试通过为每一个合约维护一个最高可执行步数并且对于递归调用其它合约的合约计算可能执行步数从而预先检测这样的逻辑炸弹，

但是这会使矿工禁止创建其它合约的合约（因为上面 26 个合约的创建和执行可以很容易地放入一个单独合约内）。另外一个问题点是一个消息的地址字段是一个变量，所以通常来讲可能甚至无法预先知道一个合约将要调用的另外一个合约是哪一个。于是，最终我们有了一个惊人的结论：图灵完备的管理惊人地容易，而在缺乏同样的控制时图灵不完备的管理惊人地困难- 那为什么不让协议图灵完备呢？

3.9 挖矿的去中心化

物数链现在的目的是使用一个基于为每 1000 个随机数随机产生唯一哈希的函数的挖矿算法，用足够宽的计算域，去除专用硬件的优势。注意每单个用户使用他们的私人笔记本电脑或台式机就可以几乎免费地完成一定量的挖矿活动，但当到了 100%的 CPU 使用率之后更多地挖矿就会需要他们支付电力和硬件成本。ASIC 挖矿公司需要从第一个哈希开始就为电力和硬件支付成本。所以，如果中心化收益能够保持在(E + H) /E 以下，那么即使 ASICs 被制造出来普通矿工依然有生存空间。另外，我们计划将挖矿算法设计成挖矿需要访问整个区块链，迫使矿工存储完成的区块链或者至少能够验证每笔交易。这去除了对中心化矿池的需要；虽然矿池依然可以扮演平滑收益分配的随机性的角色，但这功能可以被没有中心化控制的 P2P 矿池完成地同样好。这样即使大部分普通用户依然倾向选择轻客户端，通过增加网络中的全节点数量也有助于抵御中心化。

3.10 扩展性

扩展性问题是常被关注的地方，与比特币一样，物数链也遭受着每个交易都需要网络中的每个节点处理这一困境的折磨。比特币的当前区块链大小约为 20GB，以每小时 1MB 的速度增长。如果比特币网络处理 Visa 级的 2000tps 的交易，它将以每三秒 1MB 的速度增长（1GB 每小时，8TB 每年）。物数链可能也会经历相似的甚至更糟的增长模式，因为在物数链之上还会有很多应用，而不是像比特币只是简单的货币，但物数链全节点只需存储状态而不是完整的区块链历史这一事实让情况得到了改善。

大区块链的问题是中心化风险。如果块链大小增加至比如 100TB，可能的场景将是只有非常小数目的大商家会运行全节点，而常规用户使用轻的 SPV 节点。这会增加对全节点合伙欺诈牟利（例如更改区块奖励，给他们自己 BTC）的风险的担忧。轻节点将没有办法立刻检测到这种欺诈。当然，至少可能存在一个诚实的全节点，并且几个小时之后有关诈骗的信息会通过 Reddit 这样的渠道泄露，但这时已经

太晚：任凭普通用户做出怎样的努力去废除已经产生的区块，他们都会遇到与发动一次成功的 51%攻击同等规模的巨大的不可行的协调问题。物数链会使用两个附加的策略以应对此问题。首先，因为基于区块链的挖矿算法，至少每个矿工会被迫成为一个全节点，这保证了一定数量的全节点。其次，更重要的是，处理完每笔交易后，我们会把一个中间状态树的根包含进区块链。即使区块验证是中心化的，只要有一个诚实的验证节点存在，中心化的问题就可以通过一个验证协议避免。如果一个矿工发布了一个不正确的区块，这区块要么是格式错，要么状态 S[n]是错的。因为 S[0]是正确的，必然有第一个错误状态 S[i]但 S[i-1]是正确的，验证节点将提供索引 i，一起提供的还有处理 APPLY(S[i-1],TX[i]) -> S[i]所需的帕特里夏树节点的子集。这些节点将受命进行这部分计算，看产生的 S[i]与先前提供的值是否一致。另外，更复杂的是恶意矿工发布不完整区块进行攻击，造成没有足够的信息去确定区块是否正确。解决方案是质疑-回应协议：验证节点对目标交易索引发起质疑，接受到质疑信息的轻节点会对相应的区块取消信任，直到另外一个矿工或者验证者提供一个帕特里夏节点子集作为正确的证据。

3.11 综述

去中心化应用上述合约机制使得任何一个人能够在一个虚拟机上建立通过全网共识来运行命令行应用（从根本上来说是），它能够更改一个全网可访问的状态作为它的“硬盘”。然而，对于多数人来说，用作交易发送机制的命令行接口缺乏足够的用户友好使得去中心化成为有吸引力的替代方案。最后，一个完整的“去中心化应用”应该包括底层的商业逻辑组件和上层的图形用户接口组件。物数链客户端被设计成一个网络浏览器，但包括对“LDBC” Javascript API 对象的支持，可被客户端里看到的特定的网页用来与物数链交互。从“传统”网页的角度看来，这些网页是完全静态的内容，因为区块链和其它去中心化协议将完全代替服务器来处理用户发起的请求。最后，去中心化协议有希望自己利用某种方式使用 LDBC 来存储网页。

3.12 结论

物数链协议围绕去物流数据分享去中心化存储，去中心化计算以及数十个类似概念建立的协议和去中心化应用，有潜力从根本上提升物流行业的效率，并通过首次添加经济层为其它的 P2P 协议提供有力支撑，最终，同样会有大批与金钱毫无关系的应用出现。

物数链协议实现的任意状态转换概念提供了一个具有独特潜力的平台；与封闭

式的，为诸如数据存储，或金融等单一目的设计的协议不同，从设计上是开放式的，并且我们相信它极其适合作为基础层服务于在将来的年份里出现的极其大量的物流行业和非行业协议。

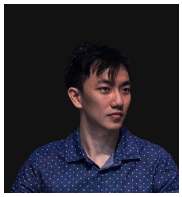
第四章 物数链发展规划及治理结构

4.1 发展规划：

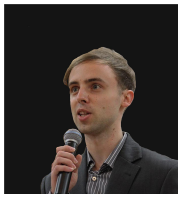
4.2 治理结构简介

物数链平台由管理运营委员会，物数链基金会，监督委员会组成。物数链基金会是物数链最高决策机构，通过制定良好的治理结构，致力于”物数链”的开发建设和治理透明度倡导及推进工作，促进开源生态社会的安全、和谐发展。管理运营委员会将管理“物数链”平台的一般事宜和特权事项，主要考虑开源社区项目的可持续性、管理有效性，项目的应用落地，由美国云网区块链科技股份有限公司、核心团队，运营团队共同组成。监督委员会董事会部分成员和活跃的投资人构成，主要就是对物数链日常管理进行监督。

4.3 团队简介



Yanomiyabi 环形计算发明者，区块链应用专家，参与多家日本交易所的底层开发。



Stephen Temple 麻省理工大学天才少年，多项区块链专利获得者。

Cheong Ben 新加坡物联网应用专家，日裔，物数链的理论开创者。新加坡科学设计大学博士。

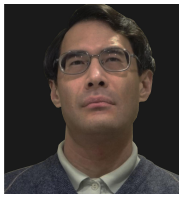
Haitao Feng 原百度区块链底层技术专家，多年底层开发经验。

Xiaoming Peng 原产贸送 CEO，物流数据专家。

顾问名单：

Rachel Wilson，教授，数据安全专家。比特币社区早期成员。

Michael Graetzel，教授，光和纳米技术行业领袖级人物。



Shinichi Mochizuki，教授，日本京都大学教授，数学家，远阿贝尔几何”领域中的领袖级人物。

第五章 物数链发行计划

5.1 发行方案

物数链网络包含自身的内置货币 LDBC，LDBC 扮演双重角色，为各种数据交易提供主要的流动性，提供支付交易费用的一种机制，是物数链的权益证明。

发行模式如下：

●通过发售活动、算力配置及数据分享，物数链 10 年产生约 90 亿枚 LDBC，预挖 55 亿枚 LDBC 将完全用来支付开发者和研究者的工资和悬赏，以及投入生态系统的项目。

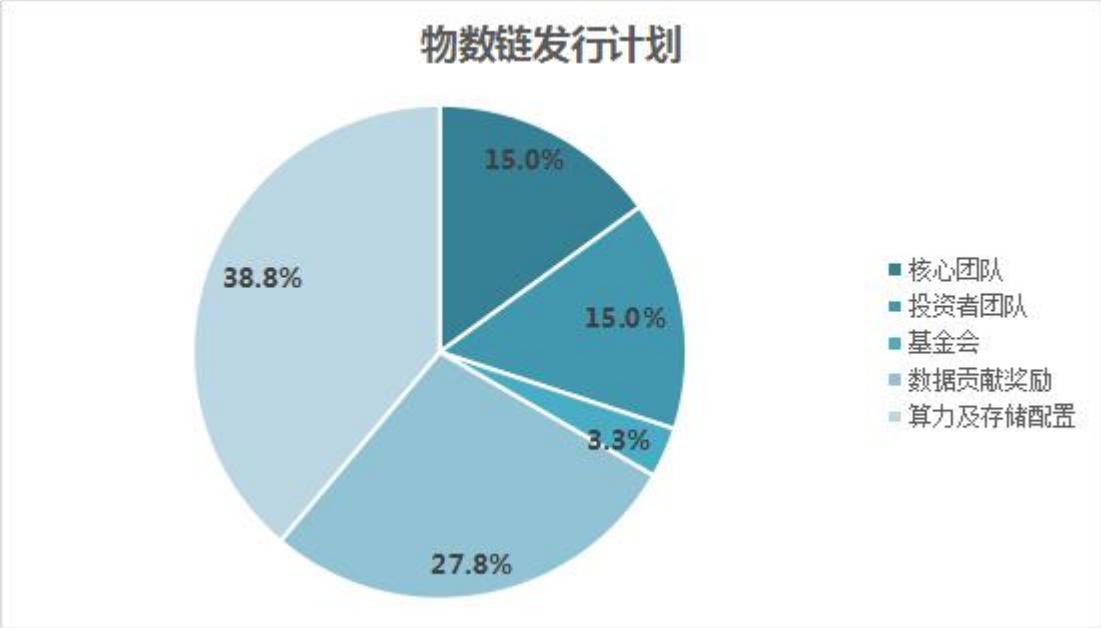
●27 亿 LDBC 将被分配给项目开发的早期贡献者及私募机构，

●23 亿 LDBC 将作为数据贡献奖励封存在基金会账户中，待 2019 年环形计算标准上线后再进行解封。

●5 亿 LDBC 将作为基金会用于奖励开发者以及社区初期建设奖励。

●自上线时起每年都将有 3.5 亿枚 LDBC 被矿工挖出，10 年共挖出 35 亿枚 LDBC

发行分解永久线性增长模型降低了在比特币中出现的财富过于集中的风险，并且给予了活在当下和将来的人公平的机会去获取货币，同时保持了对获取和持有物数币的激励，因为长期来看“货币供应增长率”是趋于零的。随着时间流逝总会发生因为粗心和死亡等原因带来的币的遗失，假设币的遗失是每年货币供应量的一个固定比例，则最终总的流通中的货币供应量会稳定在一个等于年货币发行量除以遗失率的值上（例如当供应量达到 11x 时，每年有 0.11x 被挖出同时有 0.11x 丢失，达到一个均衡）。除了线性的发行方式外，和比特币一样的 LDBC 的的供应量增长率长期来看也趋于零。



发行代币数量：90 亿枚

15%——初创核心团队

15%——投资者团队

3.3%——基金会

27.8%——数据贡献奖励 20%

38.9%——用于算力及存储配置

5.2 其他细则

1、LDBC 将作为物数链基础交易费。

2、发布子链与智能合约，需要 LDBC 进行抵押（抵押的物数链只能用于子链或者智能合约的运行消耗）。

3、子链运行持续消耗 LDBC。

为打造一个健康的物数链生态，所有基于物数链的运转，需要支付一定的 LDBC，包括但不限于主链为子链的数据证明、TOKEN 的交易等。为了平衡支付的 TOKEN 始终在一个合理的区间，不会随着 LDBC 的增值而超出合理范围，系统会根据社区投票来调整基准费率。

4、子链基础货币和 LDBC 的智能兑换。

主链的基础货币为 LDBC，接入物数链的所有子链，可以支持自己的基础 TOKEN，把基础 TOKEN 看作是 LDBC 的智能资产；子链亦可发行合约代币，称之为 IOU 资产。物数链底层系统为智能资产提供与 LDBC 的兑换功能。子链若要发行智能资产，需要支付一定数量的 LDBC，初始比例由发行商自己设定。

第六章 风险提示

6.1 核心协议相关的风险

代币和应用程序基于物数链协议开发，因此任何物数链核心协议发生的故障，不可预期的功能问题或遭受攻击都有可能导致 LDBC 或应用以难以意料的方式停止工作或功能缺失。此外，物数链协议中账号的价值也有可能以跟 LDBC 相同方式或其它方式出现价值上下降。

6.2 购买者凭证相关的风险

任何第三方获得购买者的登录凭证或私钥，即有可能直接控制用户的 LDBC，为了最小化该项风险，用户必须保护其电子设备以防未认证的访问请求通过并访问设备内容。

6.3 司法监管相关的风险

区块链技术已经成为世界上各个主要国家的监管主要对象，如果监管主体插手或施加影响则应用或 LDBC 可能受到其影响，例如法令限制使用，销售，电子代币诸如代币有可能受到限制，阻碍甚至直接终止应用的发展。

6.4 应用缺少关注度的风险

平台应用存在没有被大量个人或组织使用的可能性，这意味着公众没有足够的兴趣去开发和发展这些相关分布式应用，这样一种缺少兴趣的现象可能对系统和应用造成负面影响。

6.5 相关应用或产品达不到标准的风险

平台自身或购买者的预期的风险应用当前正处于开发阶段，在发布正式版之前可能会进行比较大的改动，任何自身或用户对应用或代币的功能或形式(包括参与者的行为)的期望或想象均有可能达不到预期，任何错误地分析，一个设计的改变等均有可能导致这种情况的发生。

6.6 代币挖矿攻击的风险

就如其它去中心化密码学代币和加密代币一样，用于应用的区块链也容易受到挖矿攻击，例如双花攻击，高算力比例攻击，“自利”挖矿攻击，过度竞争攻击，任何成功的攻击对 LDBC 来说一种风险，尽管非常努力地提升系统的安全性，但以上所述的挖矿攻击风险是真实存在的。

6.6.1 无法预料的其它风险

密码学代币是一种全新且未经测试的技术，除了本白皮书内提及的风险外， 此外还存在着一些团队尚未提及或尚未预料到的风险，此外，其它风险也有可能突然出现，或者以多种已经提及的风险的组合的方式出现。

第七章 免责声明

该文档只用于传达信息之途，并不构成本项目买卖的相关意见。以上信息或分析不构成投资决策。本文档不构成任何投资建议，投资意向或教唆投资。

本文档不组成也不理解为提供任何买卖证券的行为，也不是任何形式上的合约或者承诺。且本文档由原版翻译而已，一切均以原文为准。

相关意向用户明确了解本项目的风险，投资者一旦参与投资即表示了解并接受该项目风险，并愿意个人为此承担一切相应结果或后。

运营团队不承担任何参与本项目项目造成的直接或间接的损失。