可信区块链推进计划
TRUSTED BLOCKCHAIN INITIATIVES

区块链溯源应用白皮书（1.0 版本）

可信区块链推进计划

2018 年 10 月

版权声明

牵头编写单位：

中国信息通信研究院

智链数据科技（南通）有限公司

百度在线网络技术（北京）有限公司

参与编写单位：北京泛融科技有限公司 航天信息股份有限公司

浙江蚂蚁小微金融服务集团股份有限公司 北京孚链科技有限公司

中链科技有限公司 联通大数据有限公司

上海分布信息科技有限公司 合肥达朴汇联科技有限公司

北京太一云技术股份有限公司 西安纸贵互联网科技有限公司

全链通有限公司 深圳银链科技有限公司

编写组成员：魏凯 卿苏德 张奕卉 董宁 张增骏 郭晶 肖伟 魏菱 李翔 王晋军 程思进 尹春天 梁志华 彭赟 周适 赵立超 林进峰 裴超 华正皓 张焱 郭艳来 付珊珊 张一博 王智慧 史聪莉 高莉 刘毅 母振宇

目录

序言

自 2010 年以来我国食品安全流通追溯体系开始启动建设。2012 年 6 月，国务院印发了《国务院关于加强食品安全工作的决定》，其中明确提出了计划用三年时间使我国食品安全治理整顿工作取得明显成效。国家多溯源体系的关注从政策上提出了具体要求，根据商务部表述，“十三五”（2020 年）末，争取让肉类蔬菜流通追溯系统覆盖到所有百万人口以上城市，并涵盖肉菜、禽畜、水果、水产品、食用菌、豆制品等各类食药品。而鉴于我国目前愈演愈烈的产品安全现实，未来 300 个地级市也将启动溯源认证的建设并规范追溯体系认证的相关资质。

随着互联网金融向纵深发展，区块链技术及其应用成为人们日益关注的热点，开放、可信、去中心化、共享，区块链的这些核心思想被大家广泛认可。现在，区块链技术已经从概念走向了实际应用，越来越多的领域开始在区块链的技术中看到新的机遇，溯源作为大家近来关注的重点方向，区块链在溯源应用中发挥了重要的价值。

该白皮书主体是围绕溯源的现状和存在的问题，分析区块链技术如何与溯源深入契合，如何利用区块链技术，保障溯源的安全透明、高效可信，探索适合的应用落地模式，助力行业的茁壮发展。第一章着重概述溯源，分析溯源的背景、概念和目标。第二章通过介绍新兴技术在溯源领域的应用，探讨区块链与溯源相结合的可行性。第三章分析基于区块链的溯源应用实现，提出区块链助力溯源应用的总体框

架。第四章剖析区块链+溯源的应用案例，通过具体的场景来分析区块链+溯源的落地方案。第五章提出区块链+溯源应用的未来展望。

该白皮书是可信区块链推进计划在溯源领域的第一个白皮书，由于编写时间仓促，该白皮书存在一定的不足，欢迎业内各界人士一起沟通交流讨论。

一、溯源概述

1.1 溯源的背景

随着社会的进步和发展，“毒奶粉、地沟油、瘦肉精、假疫苗、侵权官司、产权归属”等事件层出不穷，持续爆出的食品安全和信息来源问题令公众焦虑不已，消费者对于食品安全的信任降至最低点，对于各种知识产权，信息来源的归属问题持怀疑态度。食品安全关系到经济建设和社会稳定，关系到每个人的健康和幸福。产权归属和信息来源关系到人们的财产经济问题，也牵涉到社会的信任和监管运营问题。追本溯源，寻找到信息真正的根源是解决当下这些问题的一个有效措施。

1.1.1 食药畜牧

食药畜牧是为人类提供营养的物质，一直以来在国民经济中有着重要的地位和作用，主要包括为人类提供肉、奶、蛋类等可食用的食物，促进相关行业和产业的经济和文化发展等，但是在传统农业畜牧业里，产业链非常长，从种植到人们可以食用的环节，中间历经多个环节，这些环节大多都是割裂、无序的，食品到达最终可食用的环节，中间的过程大多无法得知，无法追溯，加之现在出现的许多假冒伪劣商品，导致消费者对于现在的食品都持怀疑态度，不敢轻易食用，而且同样的产品由于各种方式的包装，导致价格不一，高低差距很大，人们不知道如何抉择，选择什么价位的食品，

不了解哪个食品提供的信息是真实可靠的，在生态农业建设中还有更多更深层的问题，比如供需不平衡。

1.1.2 知识产权

知识产权是指人们就其智力劳动成果所依法享有的专有权利，是一种无形财产或者一种没有形体的精神财富，是创造性的智力劳动所创造的劳动成果，包括专利、版权和商标权。随着科学技术在社会经济中发挥着越来越重要的作用，知识产权已成为市场竞争力的核心要素之一。然而，在当下的互联网生态中，知识产权三权不清，运营动力不足，价值评估困难，供需不平衡，侵权现象严重，纠纷频发，而且还存在着举证困难、维权成本过高等诸多问题。

知识产权的生命周期可以分为研发、生产、授权、运营、保护、维权、失效等阶段，分别会面临确权、用权、维权的问题。在研发、生产、授权阶段，由于时间周期长、科研课题交错、涉及的参与方往往比较多，权利、权属、权益三权不清，极大地降低了知识产权生产者的积极性。在知识产权运营阶段，由于三权不清、长周期的研发、生产、授权阶段数据无法回溯，知识产权价值难以评估，导致运营效率低下。在保护、维权阶段，同样由于历史数据无法回溯、历史权属不清、举证艰难、维权成本高而效率低。

当前信息互联网模式下，版权的一些新的运营模式也难以支撑。比如版权通证化、著作权合作编写、版本分支化、故事多元化

等，由于传统确权模式无法确认三权、无法追溯三权，导致些商业模式无法实现。

1.1.3 数字凭证

发票电子化自从2013年发展至今，仍然存在着许多问题。从监管方面看，对不同形式的电子发票服务平台无有效监管，发票全生命周期状态监管困难，红字发票恶意冲红存在较大税收流失风险，发票虚开不能杜绝；从使用上看，发票使用状态无统一管理，存在重复报销风险，发票流转过程中，提供发票服务的平台较多，用户归集困难，使用不方便；数据共享方面，提供电子发票服务的平台众多，不能形成统一标准，存在数据孤岛问题。以上诸多问题导致目前电子发票发展受阻，无法实现全程电子化。

1.1.4 供应链

供应链是由物流、信息流、资金流共同组成的，是指围绕核心企业，从配套零件开始，制成中间产品以及最终产品，最后由销售网络把产品送到消费者手中，将供应商、制造商、分销商直到最终用户连成一个整体的功能网链结构。

供应链行业存在如下以下几个方面的问题：一是信息不透明，各方信任成本高：供应链由众多参与主体构成，不同的主体之间存在大量的交互和协作，而整个供应链运行过程中产生的各类信息被离散的保存在各个环节各自的系统内，信息缺乏透明度。二是中小企业融资

难：资金流是企业的血液，企业资金流的状况将会决定企业的命运，而中小企业的现金流缺口经常会发生在采购、经营和销售三个阶段，中小企业亟需提高融资业务各个环节的业务可信度。三是供应链整体效益下降：在现行机制下，企业缺乏便捷的渠道为其他企业实时更新内部数据，缺少统一外部规范，且缺乏针对企业的激励机制。当所有企业都以自身利润最大化为目的运转时，系统的效率不能达到最优，进一步造成了供应链整体效益的下降。四是供应链中的溯源数据造假：目前在供应链中已有的溯源模式包括条形码、RFID 射频识别技术、扫描二维码等，各种溯源方式中一般采用中心化模式对数据进行统一管理，导致数据容易被篡改，且各种模式下标签必须手动处理，造成了溯源数据真实性难保障等问题。

1.2 溯源的概念

溯源，是一种追溯根源行为，通常是指物品或者信息在生产、流通及传输的过程中，利用各种采集和留存方式，获得物品或者信息的关键数据，如流通和传输的起点、节点、终点，数据类别，数据详情，数据采集人，数据采集时间，并通过一定的方式，把数据按照一定的格式和方式进行存储。通过正向、逆向、定向方式查询存储的相关数据，就可以对物品及信息进行追溯根源。

1.3 溯源的目标

溯源可以实现所有批次产品从原料到成品、从成品到原料 100%的双向追溯功能。溯源最大的特色就是数据的安全性，每个人工输入的环节均被软件实时备份。

溯源系统建立后，一旦发生相关事故，监管人员就能够通过该系统判断企业是否存在过失行为，企业内部也可借助该系统查找是哪个环节、哪个步骤出现了问题、责任人是谁，避免了由于资料不全、责任不明等给事故处理带来的困难，使问题得到更快解决。

1.3.1 应用角度的溯源目标

从内部管控的目标来看：

（1）企业为维护自己的产品品质、树立品牌形象，需要严格管控企业内、产业链内产品的生产、包装、仓储、运输、经销过程，避免产品在流程中出现违规行为、造假行为，通过溯源可以追溯到全流程行为和数据，进行过程监控、安全问题责任追究，加强薄弱环节的监管。

（2）企业根据溯源数据，不断优化生产流程，标准化生产规范，提高产品品质和产量。

从外部品牌维护的目标来看：

（1）通过溯源系统，向用户展现产品的真实产业链流转行为和数据，达到溯源溯真目标，实现产品安全消费，满足用户的知情权，提升用户的信任度，拒绝以假乱真，提升自己的品牌形象。

（2）通过自己固化的产业链流程，特有的产品内部信息，严格的溯源数据采集环节，提升造假难度，打击假货，提高产品附加值和市场竞争力。

从社会监督、责任追究、事故控制来看：

（1）通过溯源系统，企业向社会公开自己的生产、包装、仓储、运输、经销流程，并且提供可查询的数据，接受社会监督。

（2）当产品发生问题时，社会、政府、执法机构可以通过溯源系统追溯产业链各环节数据，定位问题发生的环节和责任方，同时产业链参与方也可以通过溯源数据自证清白。

（3）来源可追溯、去向可跟踪，通过溯源系统可以查找到产品发生问题的环节，同时可以跟踪从出问题环节流转出去的产品去向，及时追踪产品进行召回等行为，避免事故进一步扩大。

1.3.2 技术角度的溯源目标

从技术角度看，溯源系统具有如下目标：

（1）溯源数据的采集，需要技术手段丰富、采集灵活、数据准确、效率高，对现有生产工艺改造代价小，成本低。

（2）溯源数据采集需要进行严格的权限控制，只有流程中必要的环节和授权角色可以上传数据，控制数据的录入、修改、删除权限，最好不提供修改、删除权限。

（3）溯源数据在产业链参与角色间进行共同维护、同时在产业链内外和面向社会、消费者进行分享，所以需要控制数据记录和呈现范围。

（4）由于溯源涉及到数据共享、共同维护，所以数据的安全变得非常重要，一个是数据存储的安全性，一个是使用的安全性，需要严格的备份机制和访问权限控制。

二、新兴技术赋能溯源应用

2.1 区块链概述

区块链(Blockchain)是一种由多方共同维护,使用密码学保证传输和访问安全，能够实现数据一致存储、难以篡改、防止抵赖的记账技术，也称为分布式账本技术(Distributed Ledger Technology)。典型的区块链以块链结构存储数据。

典型的区块链系统中，各参与方按照事先约定的规则共同存储信 息并达成共识。为了防止共识信息被篡改，系统以区块(Block)为单位存储数据，区块之间按照时间顺序、结合密码学算法构成链式 (Chain)数据结构，通过共识机制选出记录节点，由该节点决定最新区块的数据，其他节点共同参与最新区块数据的验证、存储和维护，数据一经确认，就难以删除和更改，只能进行授权查询操作。

2.2 区块链在溯源中的运用

如今，伴随着区块链的兴起与发展，人们也开始更加了解区块链给各个领域带来的价值与前景。溯源通过结合区块链技术手段和区块链治理思想的方式，实现了区块链在溯源中的重大价值，主要体现在：

（1） 技术方面，通过区块链为溯源平台提供了很好的技术基础，保障了数据的真实可追溯；

（2）应用方面，智能合约在应用层面会成为帮助解决溯源的关键问题，提供更加有价值的信息和服务；

（3）生态层面，区块链技术可以真正打造多中心、按劳分配、价值共享、利益公平分配的自治价值溯源体系。

2.3 其他新兴技术的运用

2.3.1 物联网和边缘计算

- 物联网

物联网是通过智能感知、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，把物联网的分布式设备作为数据的来源地，只统计和验证它们所观测到的特征，综合起来加以利用。

- 边缘计算

边缘计算是在靠近物或数据源头的一侧，采用网络、计算、存储、应用核心能力为一体的开放平台，就近提供最近端服务。在边缘结点处理这些数据将会带来极小的响应时间、减轻网络负载、保证用户数据的私密性。

2.3.2 大数据和人工智能

- 大数据

溯源需要对海量技术的处理，精炼抽象出关心的数据。与此同时庞大的区块链数据集合，包含着溯源数据的全部历史。所以随着

区块链溯源的应用迅速发展，会进步一扩大数据的规模和丰富性。依托大数据技术能够满足上述需求。

- 人工智能

利用人工智能技术对数据源的相似度进行识别，如图片版权，通过人工智能识图技术将目标图片与源图进行比对从而判断是否被盗用是可行的。

2.3.3 其他

除了以上一些技术的应用外，溯源在发展过程中还有很多技术的开发和应用，例如：

- 分布式爬虫

分布式爬虫技术有助于提升数据获取的效率，同时能够及时发现相关数据是否在别处被使用。

- 分布式存储

由于区块链全节点保存了所有数据，涉及到海量的数据存储，因此对区块链单个节点的存储能力有很大的需求，而分布式存储正是为了解决海量数据的存储问题。

三、基于区块链的溯源应用架构

区块链技术给互联网深化发展带来巨大的想象空间，引发互联网上传统信任机制的改变，区块链技术应用于溯源系统中的数据存储，由于其天生的特征，存储的数据难以删除和更改，提供了一种区别于原来溯源系统中心化数据存储的新信任机制，因此极大的提高了溯源系统的可信度。

根据数据溯源的产生和使用过程，要能够很好地管理数据溯源信息，首先需要有一个统领全局的架构。由于区块链技术的可追溯性和防篡改性，与溯源需求正好契合，结合区块链的溯源架构能够满足实际生产的要求。

3.1 溯源应用的数据建模

数据溯源技术关键在于数据模型的构建，它决定了数据起源的获取、存储以及后期的使用等各种操作。数据溯源的模型图如下：

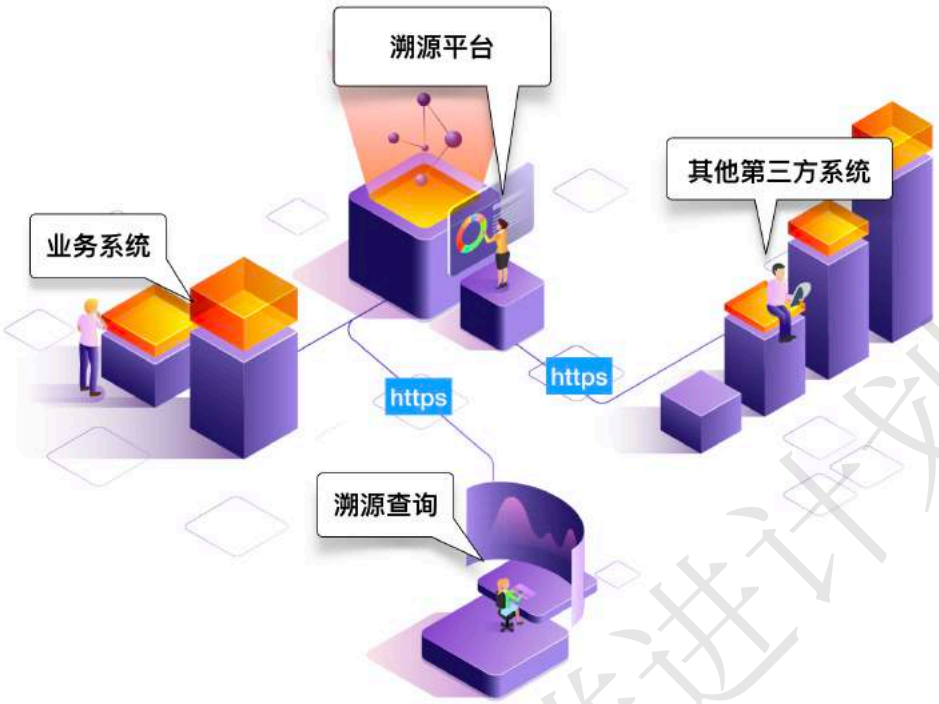

图 3-1 数据溯源模型图

1、不同应用和不同业务具有的业务数据和业务字段千差万别，溯源平台该如何适应这种变化呢？这就需要对不同业务和不同应用的数据进行抽象建模，并对数据接入进行规范。

2、对于溯源平台来说，可以把不同应用和业务的整个过程划分不同的阶段，并对不同阶段的业务数据进行分组。这样就可以针对不同阶段，不同组的数据进行溯源。

3、溯源方在查询数据的时候，通过数据特征标识获取到数据的全链路历史版本。

3.2 溯源应用的全生命周期管理

溯源应用的业务从开始到结束的整个过程就是该溯源应用的生命周期。要正确的对业务应用进行溯源追踪，需要对溯源应用的生命周期进行管理。

在如今的供应链体系中，一个特定商品的供应链包括从原材料采购到制成中间产品及最终产品，最后由销售网络把产品送到消费者手中，将供应商、制造商、分销商、零售商，直到最终用户串成一个整体。

例如大米溯源案例中，大米的整个过程包括选种，播种，收割，再到销售，最后到消费者食用的这些阶段，这些阶段的信息都会记录在溯源的应用系统中，当需要进行查询或者追踪时，消费者或者其他人可以从其中任何一个阶段进行数据查询，追踪，消费者在拿到粮食时，可以根据粮食身份证在“区块链大农场”区块链上查询是否存在相关的信息，真实存在的粮食身份证会展示出这袋粮食的品种信息、种植农户的信息、在田间详细的作业信息、每个关键生长阶段的数据信息、收割检验信息、加工过程信息、物流信息等，真正做到信息的溯源和防伪。

3.3 溯源应用的总体架构

溯源应用的总体架构图如图 3-2 所示：

图 3-2 溯源应用的总体架构图

溯源应用总体架构分为五个层级结构，描述了溯源应用当中典型的功能模块。

- 应用层：应用层可以是溯源数据的来源端，也可以是溯源服务的接收端。从线下到线上数据从来都是风险，需要物联网设备作为可信的信息化数据手段。同时还有相应企业与个人涉及的前端应用。
- 服务层：服务层为溯源应用提供核心区块链相关服务，保证了服务的高可用性、高便捷性。可信的分布式身份服务 DID 作为物或人的认证标识，可靠的数据接入，精准的数据计算，安全的元数据管理，这些服务是溯源应用提供能力的保证。
- 核心层：核心层是区块链系统的最重要的组成部分，将会影响整个系统的安全性和可靠性。共识机制与 P2P 网络传输是区块链的核心技术，保证了网络的安全性和分布式一致性。

在溯源的场景中，有许多企业商业数据，所以隐私保护也是溯源架构中必不可少的一环。

- 基础层：基础层提供了基本的互联网基础信息服务，主要是为上层架构组件提供基础设施，保证上层服务可靠运行，物联网 IoT 设备决定了数据来源的可靠性，区块链保证了数据的真实性，最后将数据安全的存储、分析和计算，提供高效、精准的数据服务。
- 管理层：管理层是溯源应用落地过程中必不可少的重要组件。权威质检中心为溯源应用数据提供了最权威的信用背书，认证了实物的可用性，也为对应的数据赋予相符的价值。溯源数据中心收集整个溯源信息流作为数据“原料”，监控中心监控数据在流转中的异常，提供了流转数据过程的可靠性。最后通过可视化展示的溯源信息即为全流程的真实的，由区块链作为价值背书的数据。还有一些辅助功能，包括配置管理、权限管理、策略管理、监控中心等保障了溯源应用的生产可用。

四、基于区块链的溯源应用案例

4.1 食药畜牧

在传统农业、畜牧业中的产业链很长，从种植、养殖到消费环节过程繁杂，在每个交易场景下都处于本位利益，市场割裂无序。从消费者角度出发，过程缺乏有效直观可信的绿色溯源途径，对于纯绿色农产品品质无法保障，从而出现劣币驱逐良币现象，致使生态链中的各相关方利益得不到保障，如种/养殖户、食品加工、保险机构等。在医疗领域，各医院病例无法互通，对患者来说不主动提供或想不起来曾经就诊的病历，医生就无法获知病人准确的信息，这会在一定程度上阻碍诊疗的进行，有时甚至会耽误病情治疗。

4.1.1 大米溯源案例

（一）案例介绍

“区块链大农场”平台是要通过溯源信息解决食品安全问题，实现快捷便利流通以及提高农民真实收入。利用的物联网设备包括智能化的育苗大棚、水田环节采集设备、虫情测报仪、作物长势监控设备、视频监控设备等，覆盖了粮食生产的各个环节，可采集到空气环境、作物生态参数、水环境参数、气象环境参数、视频等多种信息，实时获取的信息直接上链，能够提供真实的第一手数据。种植阶段的这些数据经过离线分析还会反馈给生产现场为作物生长提供合适水、肥等环境。

通过区块链技术构建区块链大农场的实践，解决了以下问题：

（1）食品安全问题：建立了一套生产可追踪溯源产品的体系标准，实现全过程可追踪，运用物联网、区块链、智能制造等技术的组合，保证粮食是放心粮。同时，产生的体系标准可以在其他领域复制和推广。

（2）提高土地经济效益：建立具有可追踪溯源属性的电商平台，区块链技术可以实现从生产到销售，从线下到线上的全程数字化追踪和记录，且数据无法篡改。通过全过程的数据价值采集和激活，不仅实现商品真实溯源，还将区块链大农场每亩土地产出提升了 1500 元以上。

（3）科研价值： 通过区块链大农场的落地，产业链相关各方，如区块链、物联网领域的专家、科院院校、政府等建立了良好的合作平台与沟通机制，为区块链大农场的推广以及其他行业的应用开发积累了经验。

（二）案例方案

智链（ChainNova）设计了“区块链大农场”平台基础架构，区块链技术在整个“区块链大农场”平台架构中处于底层，而整个“区块链大农场”的业务还嵌入了实时计算、大数据处理、人工智能等模块。此外，由于大农场将会产生巨大的数据量以及并发数据，必须有高效的实时计算和大数据平台来承载对接 IoT，而为了让用户更好的认知整个溯源历史，同时在大数据的基础上做了数据可视化等。

智链“区块链大农场”溯源平台的整体架构图如 4-1 所示下：

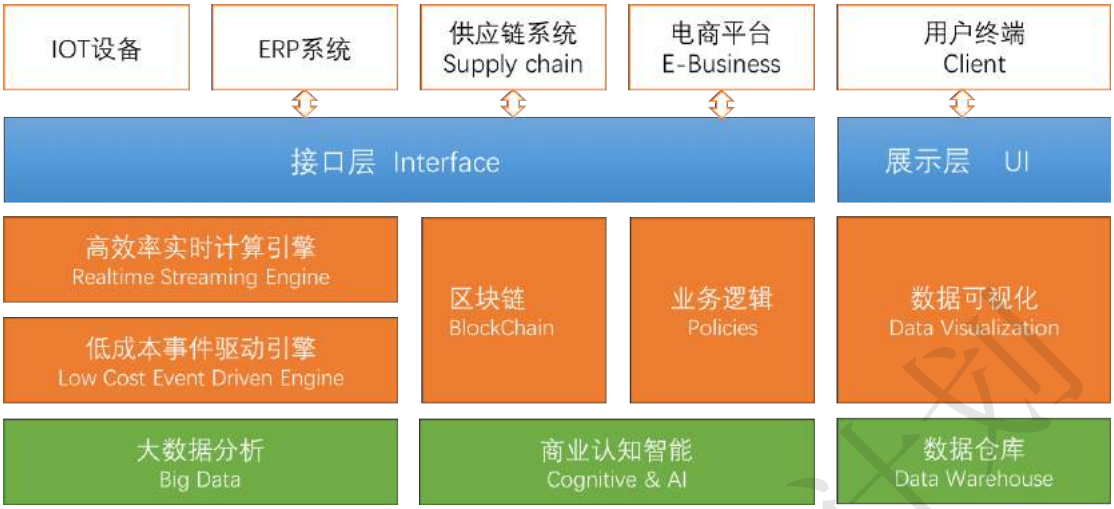

图 4-1 “区块链大农场”溯源平台架构图

根据目标和设计原则智链打造了一款通用的溯源平台，并对上链的数据进行了建模，制定了一套数据上链标准。根据数据上链的标准，可以对上链的数据项进行灵活的配置。

为了满足各种来源的数据进行上链，智链溯源平台设计了可以支持多种数据源的上链，可以是离线数据，也可以是 IoT 设备的数据，也可以是来自其他业务系统的数据等。针对实时数据，智链提供了实时处理引擎和处理规则引擎，如何计算实时数据，只需要配置处理规则，不需要编写任何代码就能够完成。而且实时数据处理规则是实时生效的。该溯源平台还能够适应业务字段的变化。因为定义了一套数据规范，所以智链的溯源平台可以支持多种行业的产品溯源，比如：农业产品，工业产品，等等。

（三）案例价值

目前区块链大农场平台主要用于北大荒高度组织化的“基地+农户”的经营模式上，北大荒 1,296 万亩黑土地，覆盖 3 万+农户，40

万+种植工人，9 种 IOT 采集标准，112 个电子表单，63 个种植标准，23 个风险点阈值，1639 个细节字段，55 个关键节点的农业大数据与区块链结合，激活北大荒农业大数据的沉睡价值。

（1）全流程的关键业务数据上链，做到信息公开透明

“区块链大农场”把区块链技术应用到从种植品种选择开始到最后送到消费者手中的所有环节中，大的环节包括粮食种植、粮食收割、粮食加工、粮食仓储、粮食运输等，每个环节都有很多细分的过程，每一个过程产生的数据都会记录在区块链的账本数据中，智能合约内部逻辑会实现每个过程数据之间的关联性，最终生成一个唯一的粮食身份证。物联网数据直接上链，提供真实的第一手数据。

（2）链上链下结合，确保信息真实的情况下还能保证品质

“区块链大农场”涉及到物联网设备采集标准，作业电子表单，种植标准，风险点阈值，包括细节字段和关键节点，这些流程和标准规范化链下的粮食生产过程，提升每个步骤产出的质量，包括链下粮食生产的质量，也保证了上链粮食数据的品质。

（3）海量数据存储优化确保系统稳定运行

“区块链大农场”可以管理上万亩土地，部署在土地里的物联网设备实时收集不同类型的数据，不同农时作业时产生的数据也会实时上链，产生了海量的数据，存储到大农场平台的数据仓库。

（4）智能合约让种植生产流程良性循环

区块链整合了不可篡改种植和销售的各种数据，基于这些数据基础上实现的智能合约能够反馈销售结果到种植环节，优良的粮食品质能够给种植这些粮食的农户带来更好的收益，对改进粮食种植有积极的作用，也能在农资贷款等提供数据的支撑，促进粮食种植的良性循环。

（5）共识机制确保数据的一致性并且不可篡改

“区块链大农场”底层的区块链技术实现的共识机制包括交易背书、交易排序、交易验证记账等多个步骤，每个步骤都需要对请求进行签名和验证，只有多个背书节点对交易结果进行背书，满足了背书策略并且在排序服务节点之间达成共识后排序产生的区块经过记账节点验证通过后才能记录到账本中，任何一个步骤出现错误都会导致交易失败，经过这些步骤后每个记账节点记录的账本都是一致的。“区块链大农场”基于PKI体系验证用户的身份，对提交请求进行数字签名的验证，保证数据的安全性和不可篡改性，让数据更加透明，大大提高消费者信任度。

4.1.2 畜牧养殖溯源案例

（一）案例介绍

畜牧业区块链溯源是通过对畜牧生命体征监控，数据实时上链，链上记录牲口的健康状态和基本信息，检疫信息，饲养信息，人员信息等；链上溯源可输入牲口的ID进行查看牲口的基本信息，运动轨迹，近期照片，同时查看链上哈希、区块高度、存证时间等

信息。平台通过传感设备采集的数据对牲口健康状态进行健康预警实现精细化养殖管理等服务。同时借助区块链技术解决了传统溯源系统在信息交互、数据保真、用户可信度方面存在的沉疴弊病，利用区块链平台数据不可篡改的特性，使得用户对产品流通各环节溯源校验的信任度大大提升，优化了公众监督的条件，提升了用户感知，提升溯源行业服务水平。

（二）案例方案

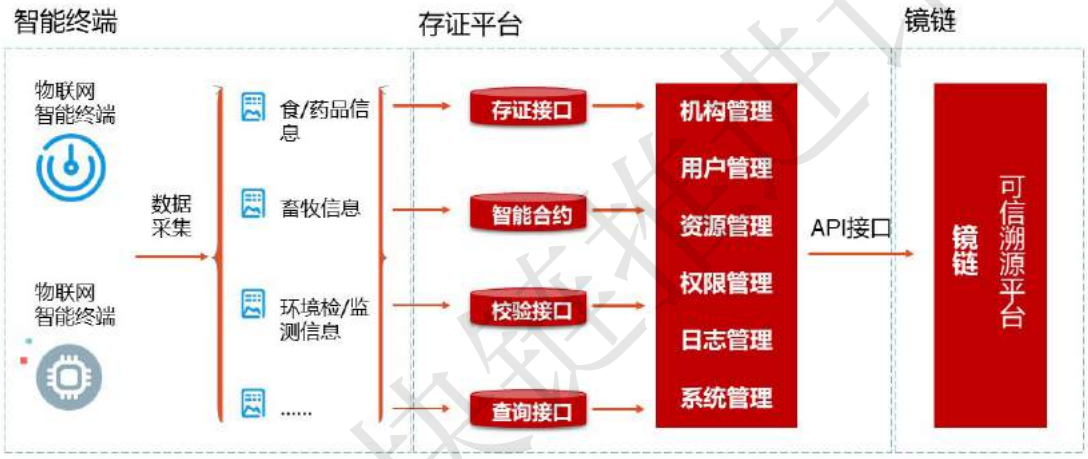

图 4-2 畜牧业区块链溯源平台业务流程

如图 4-2 所示，畜牧业区块链溯源平台采用 NB-IoT 网络，为每一头牛羊佩戴物联网终端，终端设备编号，即条码，做为牛羊唯一标识，对牛羊从出生到出栏的整个过程包括牛羊基本信息、牧场信息、牧民信息、生长信息 、位置信息、活动轨迹信息、视频图像信息、卫生防疫、检验检疫等进行全程记录，建立完整的电子档案，借助区块链技术可追溯、防篡改的特性，结合大数据平台能力和深度学习算法，实现畜牧基本信息管理、牛羊实时定位、偷盗报警、轨迹回放、电子围栏、远程看护、健康监测。

养殖企业可开放平台 API 端口，用于屠宰后肉品溯源跟踪。消费者通过手机终端扫描肉品包装上的溯源二维码、或通过网站、微信公众号、短信、客服等方式即可实现对产品全程的生态牧场、绿色有机羊生长过程、生产加工、流通销售溯源信息的查看，确认购买到的是绿色有机散养牛羊。

（三）案例价值

（1）远程放牧

牧主收到拆除告警，结合实现定位，及时找到牲口，避免了防止牛羊走失和偷盗的发生，减 少和避免牧民、畜牧企业的偷盗丢失损失

（2）绿色溯源

对于养殖企业，平台提供标准化 API 接口，同时设备支持序列号二维码导出，二维码含设备关联牲口信息、检疫信息、牧民信息、轨迹等信息的访问入口，用于屠宰后肉品溯源跟踪。消费者通过手机终端扫描肉品包装上的溯源二维码、或通过网站、微信公众号、短信、客服 等方式即可实现对产品全程的生态牧场、绿色有机羊生长过程、生产加工、流通销售溯源信 息的查看，确认购买到的是绿色有机散养牛羊。

（3）保险理赔

已经投保保险的牛羊，如若发生意外死亡，则结合运动轨迹跟踪信息及拆除报警功能，能清晰判定牲畜为意外死亡而非人为骗保，有效避免保险理赔纠纷。

4.1.3 中国食品链平台溯源案例

（一）案例介绍

中国食品链平台从食品领域出发，以食品安全溯源为出发点，通过区块链技术手段和区块链治理思想结合的方式，建立一个面向全球的安全可信、可追溯的食品生产和流通体系，推动中国食品行业转型升级。

中国食品链平台通过“技术+制度”的实现方式，将食品原产地的生产企业、加工企业、物流企业、电商平台和销售企业、各类社区以及终端消费者集聚在中国食品链生态体系中，建立链上和链下共治的中国食品产业的信用体系。

中国食品链平台通过“技术+制度”的实现方式，将食品原产地的生产企业、加工企业、物流企业、电商平台和销售企业、各类社区以及终端消费者集聚在中国食品链生态体系中，建立链上和链下共治的中国食品产业的信用体系。

（二）案例方案

（1）中国食品链生态服务体系

中国食品链中国食品链平台是以区块链技术为基础设施，结合区块链治理思想，打通食品产业供应链上下游节点，建立起绿色开放的食品生态信用网络，从而构建全程透明、高效协同的可信区块链生态环境，真正赋能实体经济发展。

1）食品防伪溯源服务

通过为广大中小微食品企业提供便利优质的区块链平台接入服务，并提供公开、透明的防伪溯源信息、数字帐户、身份验证、异步通信以及跨越多个 CPU 内核或集群的程序调度，实现多中心化应用的纵向和横向扩展。

2）产地直供服务

通过为中高档小区终端消费者提供绿色、有机、健康、安全的食品直供服务，真正实现从生产者到终端消费者的端到端（P2P）直供服务。

产地直供平台服务旨在降低管道费用，重构食品供应链生态体系，所有参与节点企业均享有激励收益，助力开启价值互联网时代。

3）生态信用网络

中国食品链将通过链上的各个节点对食品行业的绿色生态资源，如林场、牧场、农田、池塘等进行环境监测和流程监控，并将土壤质量、水资源生态数据与土地产权、使用权相联结，并引入评级、评估机构、金融机构对相关资源进行估值和提供资金支持。中国食品链通过对源头土地及生态资源的确权，最终确保食品溯源上链的安全性，提高农民和相关从业者保护优质土地资源的积极性。

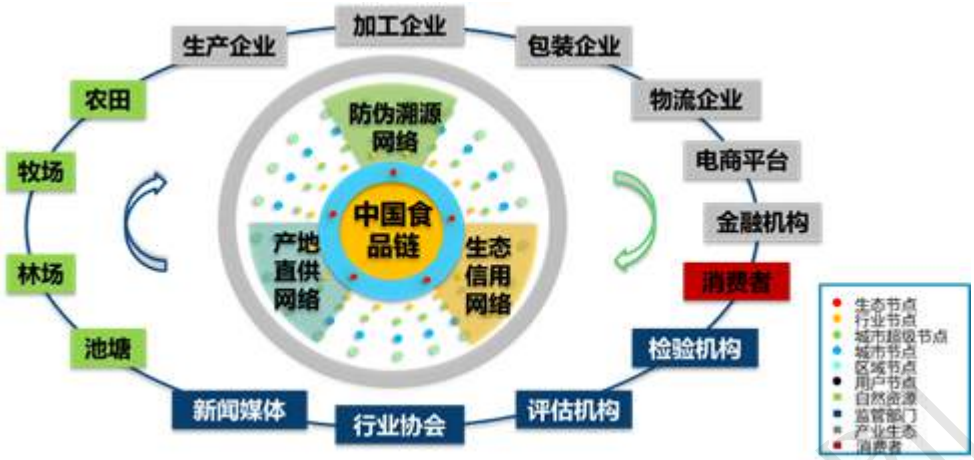

图 4-3 中国食品链生态网络体系结构图

（2）中国食品链平台架构

中国食品链平台拥有完全自主开发的高效底层平台 CFOS，平台架构设计以数据存证和通证模型为两个主要的核心，安全可靠地集成了通过权威第三方测试的超导网络，拥有多项专利产权，平台在保证上层应用的性能需求同时，对接口进行抽象和封装，支持用户更灵活的构建应用。

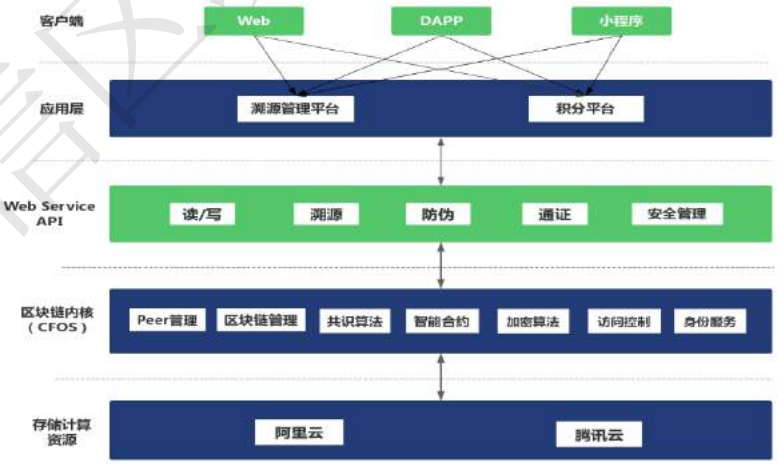

图 4-4 中国食品链平台架构图

（3）平台应用成果

平台已经完成对赣南脐橙、新疆大枣、五常大米、青海黑枸杞、安华云茶等产品的信息上链溯源，正在筹备更多产品的上链溯源，以这些产品以及企业为基础，逐步构建起食品行业信用体系，解决食品安全问题。

（三）案例价值

（1）全民监督，保障食品安全

中国食品链将食品行业的各个参与者类联为一体，在全球范围内共同分享溯源数据，为食品安全提供科学依据，共同监督流通环节，运用物联网和区块链技术，实现数据链下可信采集与链上信息不可篡改，确保食品生产流通全流程的安全可靠。

（2）共建共治，规范市场经济秩序

中国食品链平台打破了企业之间的信息壁垒，有效地降低了企业信用成本。在维护企业品牌建设基础上，促进企业的快速转型和升级，优化资源分配，响应国家供给侧结构性改革，推动全球食品经济持续、健康发展。

（3）降低企业成本，提高企业效益

中国食品链基于区块链技术进行点对点交易，省略第三方甚至是第四方、第五方广告代理公司，摆脱中间环节机构层层剥削，降低企业流量成本；凭借自身优势为食品建立起一套完整的身份机制，在食品溯源和查询时，对食品质量给出可信赖的判断，不再需要第三方认证机构或者权威中心对食品进行鉴定和认可，削减这一环节的成本，从而降低整体交易成本；发生食品安全事故时，区块

链网络可以在短时间内追踪到受污染的食物来源，精准召回不合格的批次产品，避免下架所有的同类产品，有效地节约了人力、物力和财力，提升企业业务效率，增加企业收益。

（4）增加农民收入，助力精准扶贫

中国食品链通过土地确权、精准扶贫，并联通大型物流企业、供销社、大型电商和高档生活社区为农民提供多样化直销模式，在发展绿色食品产业的同时，大大增加了农民的收入。

4.1.4 苹果溯源案例

（一）案例介绍

甘肃天水“花牛苹果”是与美国蛇果、日本富士相媲美的世界三大著名品牌名果之一。但目前市场上存在大量假借“天水苹果”以次充好的售卖现象，为了重塑并扩大天水花牛苹果的品牌形象及影响力，纸贵科技与甘肃天水市林业局合作，提供了基于区块链的果品溯源产品，让生产者、供销商及消费者等主体可以看到每一个果品的生产销售过程，让果品从生产到销售环节都做到流程透明。各参与节点将其采集数据记录到区块链的共享账本中，实现果品上下游企业全部纳入追溯体系中，构建来源可查，去向可追，责任可究的全链条可追溯系统。

（二）案例方案

在天水苹果案例当中，纸贵科技应用了一物一码、纸贵许可链 Zig-Ledger、分布式身份标识（DID）等诸多先进的区块链技术，为果品的全流程溯源提供了坚实的底层技术支撑。

（1）“一物一码”技术独具创新，在苹果上通过日晒形成了独一无二的二维码标识，实现了果品与数字身份的一一对应。用户通过手机扫码，可以查看苹果的区块链证书，从而获取苹果的生产和物流相关信息。

（2）Zig-Ledger 作为天水苹果溯源的底层区块链网络，包括区块链底层系统、SDK、浏览器、运维平台等部分，在资产登记和流转，共识机制，隐私保护，行为监管，跨链交互等方面做出许多重要改进，更适用于商业级应用场景。

（3）纸贵科技在天水苹果溯源场景中引入 DID（Decentralized Identity，分布式身份标识）和可验证声明技术，为每一件商品注册唯一 DID，将产品信息写入 DID 描述文件中，各环节参与方通过 DID 为产品签发和校验可验证声明，实现天水苹果全生命周期信息可信上链。

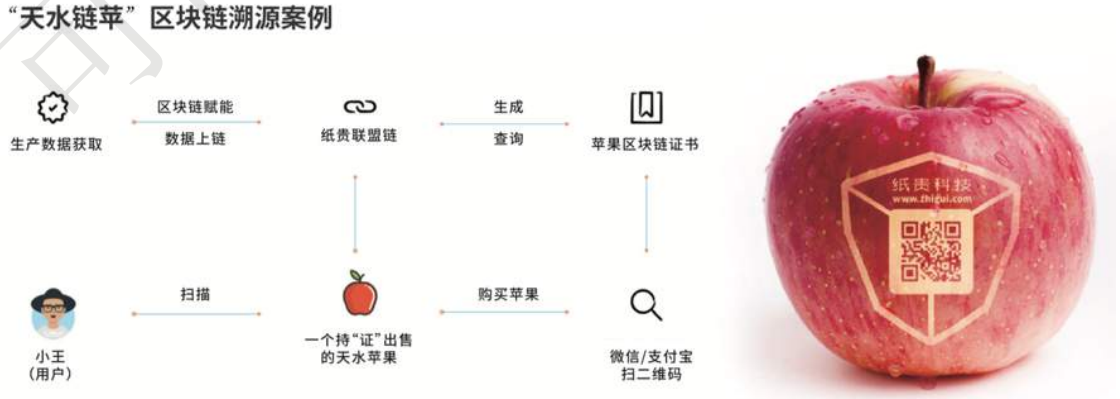

图 4-5 “天水链苹”区块链溯源图

（三）案例价值

（1）苹果关联数据上链，信息可追溯：

通过区块链不可篡改、可追溯的特性，各参与节点将苹果原产地、植保、采摘存放、品检、包装、物流等每一环节的具体信息进行上链，记录在区块链的共享账本中，并提供专业的电子存证证据，让每一颗天水苹果都有“身份认证”。

（2）提高农民收入，积极响应精准扶贫号召：

果品相关信息全部上链，打破了传统生产、销售、消费等环节的信息不对等现象，减少批发商、渠道商、零售商等不透明利润分成，最大额度让利给农民，让农民提高收入，也是政府积极响应精准扶贫的创新型举措。

（3）提升消费者满意程度，保障消费者权益：

为顾客提供果品信息溯源，商品真伪查询的平台，保证信息透明，保障消费安全，让消费者购买和食用更加放心。

（4）创新监管机制，提高政府公信力：

将天水苹果的品牌优势和纸贵科技在区块链技术上的优势相结合，让品牌感染力和用户的满意度都得到提升；进一步协助政府制定相应管理标准和规范，创新监管服务机制，通过共建产品溯源示范区，帮助政府提升质量监督管理效率，提升公信力。

4.2 知识产权

无论是美国发起的 301 调查，还是频频发生的专利纠纷，在国际竞争中，无论是进攻还是防守，各国都不约而同的举起知识产权这把武器，知识产权在一定程度上代表了一个国家和一个企业的科技水平，而我国专利质量参差不齐、版权、商标侵权严重，如何很好的杜绝侵权行为、鼓励大家创造更有价值的知识产权是一个紧迫而严峻的任务，通过建设基于区块链的溯源系统，在知识产权源头存证、确权，在运营和维权阶段能够正本清源，进而提高知识产权创造的积极性和运营效率。

4.2.1 图腾版权溯源案例

（一）案例介绍

百度图腾是百度区块链原创图片服务平台。该产品采用自研区块链版权登记网络，配合可信时间戳、链戳双重认证，为每张原创图片生成版权 DNA，可真正实现原创作品可溯源、可转载、可监控。作为百度搜索公司首个区块链落地项目，图腾旨在为原创生产者提供版权认证、分发传播、变现交易、监控维权以及 IP 资产管理的全链路服务，在提升版权确权和维护各环节效率的同时，重塑版权资产价值链、帮助版权人获得多元价值。

图 4-6 百度图腾

（二）案例方案

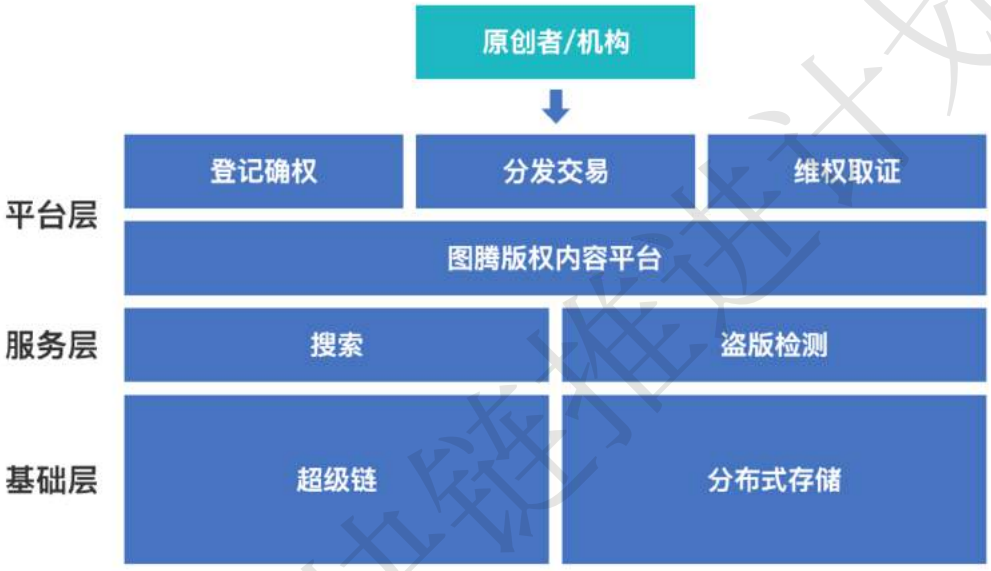

图 4-7 图腾的技术架构图

（1） 基础层：基于百度超级链技术构建版权链，版权链用于记录版权行业登记确权、维权线索、交易等需要公信力或透明性的信息，版权链由百度、内容机构、确权机构、维权机构等节点共同维护和账本同步，具有强大的公信力。庞大的版权内容信息则是存储于百度分布式存储系统中。版权链和分布式存储系统中的内容可相互关联访问；

（2） 服务层：构建搜索、盗版检测等基础服务。搜索：针对上链的版权内容，根据资源类型，构建文本、图片、视频等多种类

型的搜索系统，为原创内容购买者提供一个需求匹配的便捷入口。盗版检测：基于百度强大的技术背景和丰富的网络资源，利用成熟的分布式爬虫系统，对全网资源进行采集。基于智能 AI 技术，构建文字、图片、视频的重复检测系统，利用强大的算法和过硬的技术，即便内容发生了部分修改也能被追踪和发现；

（3） 平台层：为内容生产者提供登记确权、分发交易、维权保护等核心产品功能。百度图腾以 XuperChain 区块链技术作为基石将人工智能、分布式存储、分布式爬虫、图片检索、大数据和云计算等主流技术完美地结合起来，使系统具备了区块链版权登记、图片检索、图片智能识别以及智能推荐的能力，逐步打造完整的版权登记、版权分发结算、版权监控维权的体系。

从区块链技术的分类来看，图腾采用的是 XuperChain 的联盟链服务，所谓联盟链，就是有若干个机构共同参与管理的区块链，每个机构都运行一个或者多个节点，其中的数据只允许系统内不同的机构进行读写和发送交易指令，并且共同来记录交易数据。

（三）案例价值

图片版权行业由图片的生产者、用图方以及代理机构组成。当前行业各方的痛点如下：

对于图片的生产者和机构来讲，图片版权市场的信息不透明、不对称，盗版现象猖獗屡禁不止，维权、确权成本较高是他们难以翻越的鸿沟。因为信息不透明、不对称，使得他们难以判断自己作

品的价值，同时由于维权、确权成本较高，使得他们面对猖獗的盗版现象只能望洋兴叹。这在很大程度上扼杀了他们的创作热情；

对于自媒体平台或者作者、站长、商业产品等用图方来讲，用图成本高、图片全面性、时效性、本土化不足，版权界定模糊是让他们头疼的事情。也就是说会承受花高价格却买中盗版图的风险。这也在一定程度上打消他们尊重版权的积极性。对于代理机构来讲，销售图片的售卖渠道扩展困难，行业整体技术缺失是其面临的首要困难。

综上所述，各方的核心诉求均体现在需要一套安全可靠、信息透明、供需直接对接、维权确权流程优化的体系来解决行业的痛点。区块链的本质分布式账本，具有公开、透明、永久保存、不可篡改等特点，与版权保护的场景非常契合。

4.2.2 地理标志溯源案例

（一）案例介绍

地理标志产品，是指产自特定地域，所具有的质量、声誉或其他特性本质上取决于该产地的自然因素和人文因素，经审核批准以地理名称进行命名的产品。因此当本地的地理商标注册成功之后，就等于为城市贴上了一个标签，有了“名片”，大大增加了当地品牌甚至是当地的知名度，当打响了知名度，无论是企业还是当地经济都会得到飞跃般的提升，然而也因此引来了更多的造假者，对地标企业和当地品牌造成了很大的困扰，地方政府和企业每年为此需

要付出高昂的费用，通过建设溯源系统，可以对地理标志产品溯源溯真，增加造假难度，在一定程度上可以解决地标产品造假问题。

但是，传统的溯源系统，系统由一个企业建设，数据存储在一个中心的系统中，数据不具有权威性、不具有可信度，系统维护商可以随时修改溯源数据。中心的溯源系统会成为一个新的权力中心、滋生腐败，通过建设基于区块链的溯源系统，可以解决上述问题。

（二）案例方案

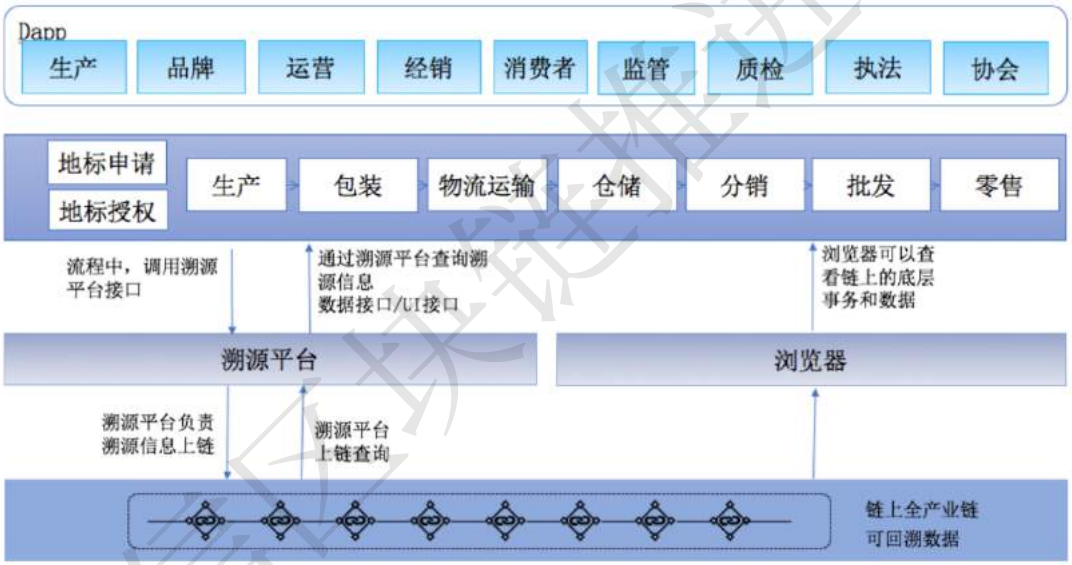

图 4-8 地理标志溯源平台架构图

孚链科技基于区块链的地理标志溯源平台由三层组成，底层为知识产权产业公链，中间层为行业定制化的溯源平台，上层为面向用户的 DApp。

知识产权产业公链是由孚链科技打造的国内第一条具有公信节点的半许可产业公链，聚焦于知识产权领域，为专利运营，商标版权保护、存证，地理标志产品溯源、防伪等提供服务，致力于打造

一个知识产权垂直领域的公链生态，为行业内的企业、用户提供一个公平、透明、互信的价值网络，提升行业的发展效率。

定制化溯源平台，提供溯源一站式解决方案，首先溯源平台封装了上链细节，为客户提供简单、易用的 rest api，可以很容易接入和获取溯源信息。其次溯源平台提供定制化服务，用户可以自定义溯源流程、信息、规则。再次，溯源平台降低了溯源接入门槛，使溯源工作不在繁琐，信息记录、检索都提供 api 和 UI 接口，实现 0 代码接入。

产业链中间环节，通过相应 DApp 扫描产品识别码（二维码等）即可获得授权，进行溯源数据上传，或者通过企业 ERP、供应链等系统调用平台提供的接口上传数据。消费者通过相应的 DApp 扫描产品识别码即可获得产品的原材料、生产、加工细节，完整生命周期流转信息，产品原始信息、品牌故事、是否正常流转等，从而判断产品是否为真。

（三）案例价值

（1）传统溯源价值，来源可追溯、去向可跟踪，企业内部管控，质量、流程改进优化，政府可监管，用户可信任。

（2）基于区块链的地理标志溯源平台，通过数字身份认证，确保上链数据的来源可靠，通过智能合约预设产业链流转流程，智能判断上链逻辑是否正确。

（3）符合品牌运营业务逻辑的产业链流转数据上链后，由于区块链上的数据分布式存储、不可篡改，杜绝了可能的作弊环节，确保链上数据真实可信，也即溯源数据真实可信。

（4）溯源平台的定制能力，降低了企业溯源项目的建设成本，丰富的 API 和接口形式，方便企业快速接入，也降低了开发商的上链门槛。

4.2.3 电信数据溯源案例

（一）案例介绍

大数据在交易和共享过程中存在着被第三方复制、留存、转卖的风险，造成数据权属不易证明，各方权益无法得到保障。如数据提供方担心使用方获得数据后，未经许可传播给其他人或非法组织牟利，造成数据泄漏；数据使用方担心买到的数据是非法数据，引起法律纠纷。为解决在大数据交易和共享过程中数据权属和溯源的问题，需要构建一个可靠的系统为交易和共享的参与方和数据提供保障。

（二）案例方案

联通大数据溯源系统以区块链和数字水印作为核心技术，通过建立数据的唯一标识，登记权属信息、记录交付路径、水印加注检测，实现数据的起源、路径管理和权属证明，不仅对数据提供方和使用方进行了确权鉴定，也对数据的流转和交易过程提供可信的路径记录和查询，为大数据流通共享和交易提供了技术保障。

图 4-9 联通大数据溯源系统架构

系统技术架构总体分为五个部分，分别是平台管理、技术层、功能层、表示层、数据接入。

（1）平台管理：对整个系统进行用户身份、行为的管理和审计，对系统运行状态的监控和告警。

（2）技术层：依赖的底层技术，包括区块链和数字水印技术。

（3）功能层：针对确权和溯源两个目标，实现系统的主要功能。

（4）表示层：为不同角色的用户提供多个维度的数据视图，帮助了解数据质量和使用情况。

（5）数据接入：数据交互接入，包括对实时数据流、批量数据按不同传输协议和方式的数据读取和写入。

从功能方面，系统从四个方面完成数据的确权和溯源：

（1）节点管理：联盟链的各个节点通过平台认证授权，审核通过后，才能加入或退出网络。各机构组织组成利益相关的联盟，共同维护系统的健康运转。

（2）确权管理：建立数据提供方和使用方的身份标识，对流转的数据建立唯一标识，按用户角色和数据的类别和级别，建立相应的权属映射关系。将该映射关系构成区块并广播全网。

（3）溯源管理：不同角色的用户可查询当前区块链上的用户和数据的关系，也可按数据的标识查询数据的使用和流转情况。

（4）水印管理：对流转数据进行特征识别，并对数据的使用方的身份信息和数据标识生成数字水印，加注到流转的数据当中，实现链上的权属关系与链下数据的关联。

通过以上四个方面，各方作为节点构成大数据流通或交易的联盟链，并将各方与数据的关系形成映射广播至整个网络中，以数据的唯一标识作为交易对象，并将交易记录广播。同时为实现链上权属关系和链下大数据的关联，使用数字水印技术将交易用户身份和数据标识隐藏写入到大数据当中。需要进行用户与数据的确权证明时，可通过查询链上记录，同时识别大数据中的数字水印信息，进行比对验证实现证明。

（三）案例价值

（1）数据确权。将数据提供方和使用方的身份信息、以及数据标识生成数字水印后隐藏在大数据中，并将相应的提供方和使用的

对数据的权属关系进行上链。通过区块链的不可篡改、去中心化特性，保证了数据提供方和使用方对数据权属关系的可信性。

（2）数据溯源。利用区块链的可追溯特性，对数据的流通路径进行查询追溯，或对数据的提供方和使用方进行追溯。当发生数据泄露或恶意传播时，可追溯数据泄露者。

（3）促进大数据流通和交易。通过区块链与数字水印相结合，从技术手段上解决了数据确权和溯源的可行和可信的问题，将会积极地促进大数据流通共享和交易，使得数据提供方和数据使用方都将更有依据、更有信心地进行数据流通、数据交易和数据使用。

4.3 数字凭证

数字凭证就是互联网通讯中标志通讯各方身份信息的一串数字，提供了一种在互联网上验证通信实体身份的方式，数字凭证不是数字身份证，而是身份认证机构盖在数字身份证上的一个章或印（或者说加在数字身份证上的一个签名），人们可以在网上用它来识别对方的身份。由于互联网电子商务系统技术使得顾客在网上购物时能够极其方便地获得商家和企业的信息,但同时也增加了对某些敏感或有价值的数据被滥用的风险。为了保证互联网上电子交易及支付的安全性，保密性等，防范交易及支付过程中的欺诈行为，必须在网上建立一种信任机制。这就要求参加电子商务的买方和卖方都必须拥有合法的身份，并且在网上能够有效无误的被进行验证。

4.3.1 电子发票溯源案例

（一）案例介绍

本方案构建电子发票联盟链，利用区块链技术解决目前电子发票在流转过程中共享难、归集难，报销难、监管难等问题，实现对电子发票流转全过程的管理。

对于各第三方平台(如发票开具或者财务平台)，通过区块链技术使得各平台可以做到在服务分离的情况下，达到互联互通信息共享的目的。

对于加入网络的税局等监管部门，可以通过监管节点获得电子发票全流程信息，实现税局等监管部门对电子发票低成本、高效率、可信赖的穿透式监管。

对于个人或受票企业来说，基于区块链技术实现了电子发票全流程管理，用户可以安全便捷地使用电子发票，极大地降低了使用成本、提高了工作效率。

（二）案例方案

图 4-10 电子发票流转应用网络图

基于区块链的电子发票流转应用网络如上图所示，第三方服务商（包括第三方平台和大企业自建平台）、ERP 厂商作为联盟链的节点，税务机关作为监管方加入区块链，统一制定区块链的运行标准和合约条件，区块链上的各节点和加入者都必须按照事先制定的交易规则参与和运行，共同维护联盟链，解决各电子发票服务商之间的数据互通问题，通过区块链对电子发票的开具、流转、报销和存档等全流程的发票状态进行记录和存取，有效解决电子发票的重复报销等问题。企业通过第三方服务商提供的服务进行电子发票开具，第三方服务商向联盟链写入电子发票信息，ERP 厂商可从链上读取电子发票信息，并记录电子发票状态信息，税局作为监管方查看所有信息，实现对电子发票全流程的穿透式监管。

方案用到的关键技主要包括同态加密、属性基加密等隐私保护方案、基于分片的可扩展共识机制、海量数据存贮与检索、异构网络下的互联互通等。通过设计“PKI+IBC”相互融合的密码安全方案，实现系统安全和用户隐私保护。

（三）案例价值

（1）为电子发票全程无纸化提供了基础条件，可以有效防止重复报销，打印报销等问题。

（2）为受票方提供多种手段发票查验功能，减少纳税人因发票查验繁琐的带来的工作负担，提升税局服务形象。

（3）开通受票方入链渠道，使的发票后期流转更通畅。

（4）为消费者提供丰富的前端工具，方便消费者发票归集、查验、报销等工作。

（5）税局通过区块链建设，可以对电子发票进行全程追溯和审计，对电子发票服务平台进行有效监管。

4.3.2 艺术品溯源案例

（一）案例介绍

艺术品一般被认为是一种可靠而安全的价值存储。几个世纪以来，艺术品一直是家庭投资组合的一个组成部分，并且在过去的几十年内交易量持续稳步增长。投资者和财富管理机构对艺术品的兴趣正在上升，年轻一代的买家也渴望拥抱艺术。

然而，投资艺术品一直是大多数人无法企及的，主要原因有两个：首先艺术品交易掌握在少数中心化的拍卖行和银行手中，不透明的运作导致高企的交易费用；其次，艺术品市场充斥赝品，艺术品鉴定难度大，技术都掌握在专家或者专门鉴定机构手中，大多数人在交易过程中会难以避免的买到赝品，造成巨大损失。高昂的交易费用和赝品风险阻碍了艺术品交易市场以更快的速度往前发展。

达朴汇联结合区块链去中心化以及可溯源的特点针对艺术品交易的两个痛点设计了一个艺术品溯源交易平台，通过交易记录、用户信用和鉴定奖励等方法实现了艺术品交易低成本和防赝品等功能。

（二）案例方案

基于区块链的艺术品溯源交易平台参与方包括平台方、艺术品交易链上的交易方和鉴定机构（或鉴定专家）。每件艺术品在链上都有唯一的 ID，有真伪信用值；每个交易方在链上有相应的诚信度信用值；每个鉴定机构或鉴定专家在链上有相应的专业水平信用值。跟传统艺术品拍卖平台一样，艺术品提供方将艺术品挂到平台上公开拍卖，需求方可在平台上竞价。竞拍成功后，区块链矿工会将交易记录到链上，平台收取交易费用，交易费用转成通证部分返还竞拍方，部分支付给矿工作为记账费用。这样保证在平台上交易的艺术品的流转过程有据可查，当一件艺术品再次交易时，其流转记录可作为该艺术品的真伪信用的一个证明。在艺术品流转的过程中的任意环节，该艺术品的当前主人都可支付费用委托鉴定机构或

鉴定专家对该艺术品进行鉴定，每次鉴定都作为一个交易记录（包括鉴定机构或专家的名称、信用等信息）记录到链上。每次鉴定都会生成一定数量的通证作为对平台的贡献值奖励给委托鉴定的艺术品主人。鉴定机构或专家也可以主动免费参与到鉴定过程，这样可以由鉴定机构或专家获得鉴定贡献的通证奖励。交易手续费返还的通证或鉴定奖励的通证都可在本案例的平台上用于艺术品交易、手续费或鉴定费的支付等。每次鉴定的结果都可作为该艺术品真伪信用的证明。每次鉴定为真的艺术品将根据鉴定机构或专家的技术水平信用值增加该艺术品交易链条上以前所有交易方的诚信信用值和艺术品本身的真伪信用值，反之则将扣除艺术品主人和艺术品的信用值。当被鉴定过的艺术品再次被鉴定时，则将根据最后一次鉴定的鉴定机构或专家的信用值增加链上该艺术品以前与本次鉴定结果相同的鉴定者的信用值，但是扣除与本次鉴定结果不同的鉴定者的信用值。平台定期会根据链上参与方的信用值奖励或处罚相应的通证。

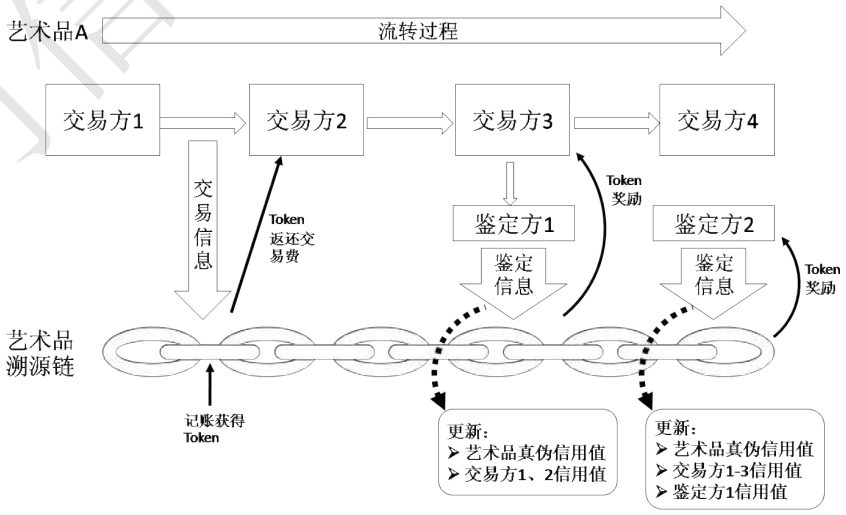

图 4-11 艺术品交易溯源流程图

本案例核心在于区块链主链的设计，采用达朴汇联自主研发的Delegated（Proof-of-Stake + Proof-of-Contribution）的共识机制，除了选中的权益代表记账可以获得奖励之外，为平台作贡献还可以生成奖励，在本案例体现为鉴定贡献。引入贡献共识机制可以使交易方、平台方与鉴定方之间可以找到平衡，从而克服别的PoS，DPoS体系中的大者恒大的问题，从而为社区的自发成长创造一个坚实的基础。

为了保障在复杂网络中快速共识的一致性问题。Delegated (PoS + PoT)委派权益和贡献代表制引入到了主链的共识机制。每轮将由愿意参与选举的通证持有者选出若干个节点轮流记账。为达到这个目标，每个股东可以将其投票权授予一名代表。获对应通证权益票数最多的前若干位代表按每10秒中轮流产生区块。被选出记账的节点将使用上一个区块的时间戳作为伪随机种子进行随机打乱记账顺序。每经过360个区块，主链网络将重新选择节点参加记账。在这共识机制里，所有委派的代表将收到他所打包的区块的交易费的10%以及区块奖励的5%作为报酬。而剩余的交易费将交给每块对应的代表。代表根据给其投票的权益人放入的权益比例转交给权益人。每轮所有代表获得同样的区块奖励，扣除代表报酬后，也根据其投票的权益人放入的权益比例转交给通证的实际拥有者。

如果一个节点被选中为代表却因为网络延迟等原因没能及时广播他们的区块，他将失去该轮次所有的奖励，同理他背后的权益持有者也将失去相应的奖励。同时排在当前代表之后的代表将会继续

负责区块构造，系统会按之前的代表次序选择若干名之后的一名代表填补空缺。每一个代表必须抵押一定的通证来参与区块构造。如果他们错过了太多的区块，那么系统将会推荐股东去换一个新的代表。如果任何代表被发现恶意签发无效的区块，那么代表所抵押的通证将被没收，并且该代表将无法参加任何后续的区块构造。

在主链平均每 10 秒产生一个区块。基于 DPOS 的共识机制特性，在一个区块被产生并广播后，即可认为区块中包含的交易已被最终确认。所以对于小额交易，当接收到区块，即 10 秒左右便可以认为交易已被确认。在一些极端情况下，如网络拥堵、恶意区块构造者进行分叉攻击等情况发生时，当节点连续丢失两个区块，便可以认为自己有大概率处于一个分叉上。当节点连续丢失三个区块，就可以基本确认自己处于分叉上。所以节点用户可以基于不同商业类型安全度的需求，等待三个以上连续确认的区块来确保自己的交易被最终确认。

当区块链出现分叉时，虽然通证权益代持者事实上在两个分叉上都能获得利益。但由于贡献的唯一性，贡献节点用户无法在同一时间下将一份贡献同时提供给两个分叉上的不同用户。为了保证自己的利益被系统记录在区块中，贡献节点用户必会优先选择最多权益认可的分叉。在这种情况下，随着贡献节点集中涌入其中一个分叉，而大部分块又由贡献节点制造，其他分叉最终会出现出块困难而获得最多权益认可的分叉成为链最长的分叉，其他分叉会因无人使用而被舍弃。

（三）案例价值

本案例设计的艺术品交易链，交易费用通过通证返还的策略可大大降低艺术品交易的成本，并且通过鉴定和信用相结合，并辅助以通证激励的方式大大降低赝品流通概率（或增加赝品流通成本）。由于交易链条上任何一个环节都有可能有鉴定者参与，造假被发现的概率大大增加。鉴定机构或鉴定专家会受到其他鉴定者监督，考虑到其专业技术信用值和通证激励，会尽量避免与艺术品主人合作造假的可能性。

4.4 供应链

产品从原材料采购，加工，生产，质检，物流，经销商，零售商一直到用户手里，经过了大量环节，不同的环节离散、孤立的保存相关的信息，造成信息孤岛，信息流转不畅，信息缺乏透明度。在经济一体化的背景下，产品流通往往呈现出跨区域（甚至是跨国）、周期长等特征，加重了信息流转不畅的状况。利用区块链将供应链参与各方链接起来，安全的实时共享数据，信息不可篡改，参与主体不可抵赖，从而实现了正品溯源，有效监管，提高供应链效率等显著价值。

4.4.1 危化品信息流溯源案例

（一）案例介绍

由于供应链流程中涉及到的参与方是具有不同经济利益的独立实体，相互间形成了企业间的“数据孤岛”，这种利益上的冲突常常会导致成员间产生互不信任，造成各自为政，在组织上也是如此，比如国内一些大型零售企业内部仍然是作坊式的管理模式,各个部门单独进货,各有各的进货渠道，这不仅加大了进货成本，而且是整个企业失去了抵御市场变化的能力，没有发挥资源复用的优势。

另一方面，供应链系统的地域和时间跨度大,对信息化依赖程度高。供应链系统连接多个生产企业、运输企业、配销企业、采购企业及用户，多个参与方使用一套可信的账本数据，将会减少企业对数据的信任成本，所以区块链技术将是供应链整合的实现的理想技术手段。

（二）案例方案

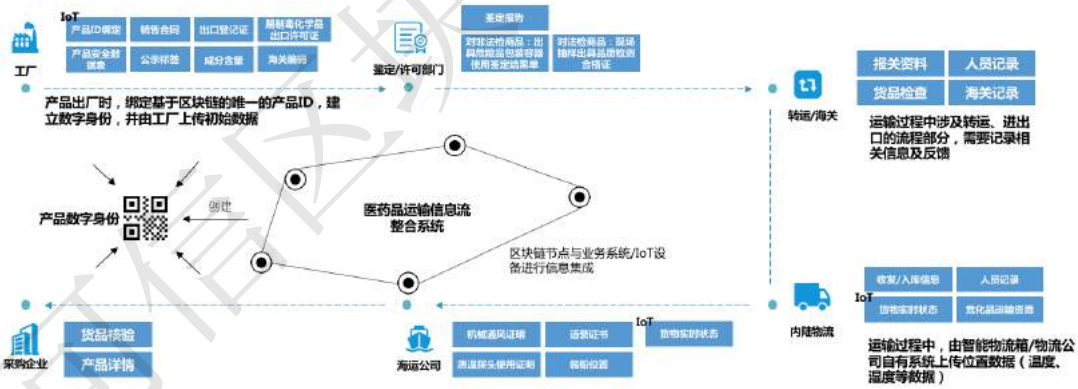

图 4-12 分布科技危化品供应链信息流整合流程

在分布科技的供应链解决方案中，危化品供应链方案整合了全流程信息流，产品在工厂出产并检测质量无误后，即为产品绑定基于区块链的唯一数字 ID，并加以 IoT 设备保证全流程数据的透明可信，在经过危化品鉴定部门，海关等国家机关检测后，把检测、鉴

定报告信息加密存储在区块链当中，并使用零知识证明、CL 签名等方式让指定验证方有权查看报告，保护数据隐私和安全性。由于物流信息化技术的完备，在海陆物流运输途中，可通过传感器设备实时监控温度、湿度等数据，保证货物处在合理区间内，并将物流状态信息、地理位置，证书等数据上传至区块链。最终采购企业在货品核验时，可查验货物从出厂到收货的全流程、多维度可信数据，通过区块链的技术背书而非人为信任，加以 IoT 技术，保证了原始信息数据的真实可信，以及物品与信息数据的一一对应，极大的增加生产企业的作恶成本，同时降低了采购企业和全社会的信任成本。

（三）案例价值

数据确权，由于区块链的分布式账本特性，各个参与者同时记录、共享账本数据。在供应链信息流中使用区块链技术，可使信息在上下游企业之间公开。由此，需求变动等信息可实时反映给链上的各个主体。

增强信任关系，降低上下游企业间的信任成本。结合区块链技术，供应链上下游企业之间的交易及信息流都运行在区块链上，区块链不可篡改的特性决定了，保证了信息流的真实有效，解决了危化品供应链流程中，数据流程信息数据不可信，多方不信任的问题。

4.4.2 跨境商品溯源案例

（一）案例介绍

跨境商品的供应链相比国内商品的供应链而言，更加复杂。跨境商品要从原产地工厂到代理商，海外仓、原产国海关、国际物流、国内保税区、保税区海关，国内物流、快递配送，直到消费者手中，中间经过了大量的环节，参与方众多，流程长，信息不对称的情况更加严重。这就造成了跨境商品容易造假，供应链效率低下等突出问题。

蚂蚁区块链帮助天猫国际搭建跨境商品供应链网络，跟踪进口商品全链路，将众多海外品牌商、海外质检机构、中检集团、跨境电子商务商品质量国家监测中心等机构引入进来，汇集生产、运输、通关、报检、第三方检验等信息，给每个跨境进口商品打上“身份证”。消费者只要扫描商品上的二维码，即可查询到跨境商品的完整信息，包括商品详情、质检报告、供应链溯源等信息，从而确保消费者买到的商品是正品，买得放心。目前天猫国际的跨境商品供应链已覆盖奶粉、保健品、化妆品，汽车用品等品类，未来将覆盖全球 63 个国家和地区，3700 个品类，14500 个海外品牌。

（二）案例方案

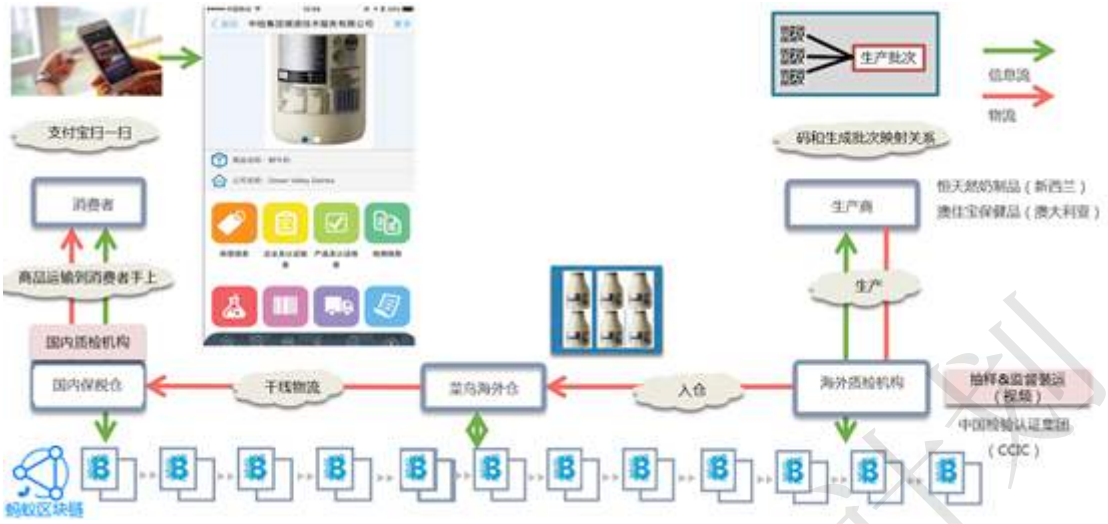

图 4-13 跨境商品供应链网络图

跨境商品供应链网络是蚂蚁区块链搭建的一个跨境的联盟链网络，其中境外的共识节点部署于澳大利亚。联盟链的参与方包括原产地企业、海外质检机构、海外仓、保税仓、国内质检、天猫国际、菜鸟物流等企业和机构。海外商品经过张贴/印刷定制的二维码，实现对商品“一物一码”的唯一标识，同时将商品二维码与质检的检查单位和物流的运输单位进行关联。商品在流转过程中由各对应主体将操作信息使用标明身份的“私钥”进行数字签名并附上时间戳写入区块链，一旦写入区块链，相关数据即不可篡改，不可抵赖。消费者收到商品后，使用手机扫描二维码，收到提示后刮开二维码上的暗码并输入，即可查询到跨境商品的全流程溯源信息。

（三）案例价值

（1）商品防伪

商品经过“一物一码”的标识，并且将全过程流转的信息写入区块链。区块链上信息不能随意篡改，商品从生产到运输再到最后

销售，每一个环节的信息都被记录在区块链上，可以确保商品的唯一性。造假商品很难具备合乎特定规则的商品标识和全流程溯源信息。

（2）有效监管

商品从生产到销售，每一个环节的主体都以自己的身份（私钥）将信息签名写入区块链，信息不可篡改，身份不可抵赖。万一出现纠纷，可以很快的定位出问题的环节，从而进行举证和追责。

（3）供应链协同

区块链上的数据高效的在跨境商品供应链不同参与主体之间进行共享，达到统一凭证、全程记录、及时高效，能够有效解决多方参与、信息碎片化、数据流通难等问题，从而降低供应链成本、提高效率。

4.4.3 冷链溯源案例

（一）案例介绍

冷链是特殊的供应链系统，泛指冷藏冷冻类食品药品的生产、储藏、运输、销售等各个环节中始终处于规定的低温环境，以保证其质量的一套系统工程。

中链科技有限公司和某大型肉类协会及某大型冷链公司合作，针对冷链溯源业务的定制化需求分别提供针对各自业务特点的解决方案，打造基于区块链的全程冷链溯源平台。由于区块链具有打破信息垄断，实现数据共享的特点，解决了传统的溯源技术中标准不一致、

无法体系化，原材料提供商、生产厂家、物流方等多方彼此隔离难以互信的难题，打造多方参与的生态。系统通过智能合约实现资源的整合和各方效益的最大化，构筑新型合作共赢的生态场景。

（二）案例方案

中链科技冷链溯源解决方案采用区块链、RFID 和传感技术，以及云计算、大数据等技术手段，打造冷链物流环境环境监测及溯源平台，平台主要包括以下功能：

可信溯源：中链区块链冷链溯源解决方案打造冷链溯源生态体系，将冷链关键环节的各方作为节点，实现原料、生产、仓储、批发、零售等各个环节的生产数据、产品数据、卫星定位数据、冷链物流数据、物流运输过程中温度、湿度、光线等数据经哈希后全程入链存证，打造可信存证基础设施平台，为溯源提供可信数据支撑。

实时监控：在冷链商品的流通过程中，对流通领域内的温度、湿度等信息进行全天候的实时监控，严格保障冷链商品的环境参数在规定范围内。

预警管理：冷链商品运输中，一旦发现环境中的温度、湿度等参数超标，系统会自动对异常情况进行预警，及时采取有效防范措施。

查询服务：平台面向各方用户提供高效查询服务，可面向生产商、经销商、零售商、终端消费者等提供不同类型的信息查询服务，让经销商实时掌握冷链商品运输中的状态，让终端消费者买到放心商品。

除以上功能外，平台还提供运输过程中的冷链商品交接管理、实时 GPS 定位、报表分析及管理、用户管理、资产管理、产品档案管理、人员身份管理等功能。

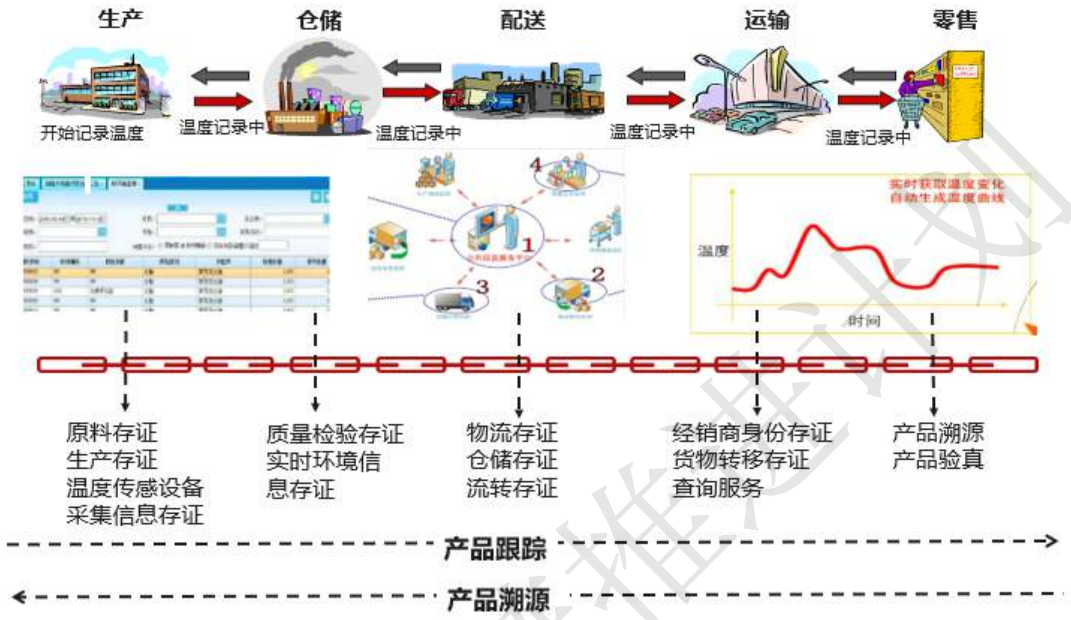

图 4-14 区块链冷链溯源公共服务平台

冷链物流中的温度和时间是必须考虑的两个重要因素，且贯穿于储藏和输配送的整个过程中。系统基于射频识别技术（RFID）及传感技术进行冷链物流环境监测，可实时监测物品在储藏、运输阶段的环境参数，并通过监控中心判断是否符合标准，以便及时调整，减少损失。系统采用 RFID 标签取代传统的环境监控方法，标签内部装有天线 RFID 芯片、温度传感器、湿度传感器以及光线传感器。标签安放在合适的位置后，传感器将实时采集所处环境的温度、湿度、光照信息，并将信息写入标签的芯片内，按规定的时间间隔将信息传输到阅读器中。阅读器通过无线网络上报到监控中心，由监控中心存储并分析收到的数据，如有异常情况，则及时报警，采取措施。其过程中所

有的温度、湿度及光线信息全程入链存证，防止数据被删除和篡改，为冷链溯源平台提供了可信数据支撑。

（三）案例价值

基于区块链的冷链溯源系统在建设过程中，打造可信冷链溯源联盟链，将生产企业、冷链物流公司、监管部门、冷链仓储机构、监测机构等部门纳入联盟网络，通过区块链网络进行数据共享和传输，保障各方信息实时同步，有效避免了由于信息造假、篡改等问题为平台带来的失信隐患，打造了各方互信共享的可信冷链溯源生态。

五、未来展望

毋庸置疑，区块链将成为下一代互联网应用的基础设施，已在全球范围的多个领域得到的广泛应用，区块链在数据权属登记上有广阔的应用前景，能够极大的促进商业活动的良性发展。同时，在全球范围内已有多个国家对区块链及其应用场景立法，以促进其良性、快速的发展。

5.1 政策层面

习近平总书记在在中国科学院第十九次院士大会、中国工程院第十四次院士大会上的讲话指出“以人工智能、量子信息、移动通信、物联网、区块链为代表的新一代信息技术加速突破应用”，对区块链应用给予了极大的肯定。多地政府以专项基金、资源形式予以大力支持，促进区块链应用的快速落地。

最高法关于互联网法院审理案件若干问题的规定，法释【2018】16 号文件中指出“当事人提交的电子数据，通过电子签名、可信时间戳、哈希值校验、区块链等证据收集、固定和防篡改的技术手段或者通过电子取证存证平台认证，能够证明其真实性的，互联网法院应当确认”，给予了区块链技术在商业活动中的明确定位，为区块链的发展提供了坚实的后盾。

区块链中的交易是将本次交易的输出作为下一次交易的输入，天然就具有“溯源”的效果，同时“不易篡改”的特性能够有效的保证记录数据的准确性、完整性，能够极大地提升多个机构间的业务推进

效率，同时解决了传统场景下集中制管理对于数据层面的欺诈行为。区块链溯源可以应用在产品、金融等众多领域，作为基础技术体系解决商业应用中的诸多问题。同时，区块链的 PKI 体系，通过非对称加密算法能够极大的提升用户数据的隐私保护作用。

5.2 应用层面

近年来“假货”成为线上线下蔓延泛滥的经济现象，在高效物流的便利背后，食品安全问题也引起大众关注。区块链溯源在食药领域的应用能够有效的提升产品质量的控制，以传统的反欺诈、风控为业务风险控制手段，结合区块链上对数据的追溯、留痕的特点能够有效的约束各参与方行为，建立可信的产业链生态，保证了产品质量，有效的提升产业的竞争力。

区块链溯源同时还能帮助金融行业有效防止金融欺诈事件。金融欺诈产生的主要是因为基础资产的真实性无从验证或极难验证，导致资产流转成本高、流动性差的问题。而这些问题则极大的阻碍了资产流转业务的发展，传统风险控制手段结合区块链应用能够将基础资产透明化、提升业务效率、降低企业流动性资产成本支出，助理金融产业的快速发展。

5.3 技术层面

区块链是一整套算法及加密体系的结合，属于底层的可信数据建设基础设施，可以在众多领域得到广泛的应用，但其本质上是不能解

决业务层面的反欺诈、反洗钱、风险评估等业务、金融风险，即使用了区块链并不等于所开展的业务就是合规的、安全的，但是安全的业务环境应该构建在区块链网络上且将是大势所趋。