GRG Chain 运通链

戴汝为院士
倪光南院士 **联合推荐**
廖湘科院士

# 运通链白皮书

## 运智汇，通天下，链未来

广电运通区块链科技有限公司

2018 年 10 月

# 前言

2016 年 3 月，谷歌阿尔法狗以 4:1 战胜当时的围棋世界冠军李世石，使得人们意识到机器智能正在接近，甚至在某些方面已赶超人类智能，一个人工智能的时代正在全面加速来临。

而也恰恰在差不多相同时间，以太坊发布第一版本“Homestead（家园）”，一个“永不停息的世界计算机”- 基于区块链的图灵完备智能合约平台诞生。

这两个表面上看似不相关联的事件，其相互作用产生的影响却蕴藏着无穷的可能，对未来将产生深远的影响。它们标志着人类社会正在步入一个全新的数字经济时代。在这个时代，机器智能将与人类智能紧密结合，机器智能将参与过往只有人类参与的大规模协作。大规模协作的基础是信任机制，而区块链作为重构数字经济时代信任机制的基础设施，对生产关系的改善，生产力的提高将起重大作用。

2016 年也被认为是中国区块链的元年，从这一年开始区块链技术在中国各行业中受到了极大的重视。首先是 2016 年 1 月人民银行宣布将来要使用法定数字货币，之后许多国内的组织机构也开始进行区块链相关投资。同时，高校、大型机构和中小创业公司都纷纷组建专业团队研究区块链相关技术，研发区块链平台；另一方面，区块链的研讨班、论坛等活动也如雨后春笋般涌现。

然而，区块链的应用目前大多还仅停留在概念炒作阶段，很多关注点均聚焦于虚拟货币方面的应用，进而出现了“利用 ICO 进行非法

集资”、“空气币、传销币大行其道”等市场乱象。由于区块链技术仍然处于初级阶段，在安全性和性能上并不能支撑很多传统应用。而另一方面，很多人在区块链的热潮中盲目跟随，为区块链而区块链，把区块链用于很多不适合于区块链的应用场景，或者是用于传统中心化模式运行良好的应用场景，致使不但没有获得预想的效果，反而造成不良后果。业界也频频出现区块链技术没有落地场景的声音。

我们认为，区块链作为一种通过去中心的模式建立信任的机器信任技术，需要与基于人工智能的智能设备结合，才能真正发挥其机器信任的价值。有鉴于此，运通区块链将聚焦于智能设备的区块链应用，致力于构建一个全国独有的服务于智能设备的区块链平台。我们这里首先定义什么是智能设备。在这个白皮书中，我们把智能设备的范围缩小到具有人机交互能力的，采用人工智能技术的机器和终端，例如ATM、无人零售机器、无人售票终端、自动识别身份的闸机、以及广义上的具人机交互能力的机器人，都属于我们定义的智能设备的范畴。

未来，运通区块链将以智能设备区块链平台为基础，联合集团内外的合作伙伴，通过人工智能技术提升生产力，并利用区块链技术改善生产关系，共同打造全新的涵盖新零售、大文旅、大健康、新政务、新物流、新金融的惠民生态，区块链将成为链接这个惠民生态的信任枢纽，提供公平的分配和激励机制，提升透明性和可问责机制。让区块链技术真正落地，使其价值落到实处，真正能给民众体验得到。

# 编委会成员

**顾问团队**：黄跃珍，叶子瑜，罗攀峰，罗一明，梁添才

**研究撰写**：吕坤，邹均等

**排版设计**：左炜

# 目录

# 1 区块链技术的机遇与挑战

## 1.1 区块链带来的社会变革

区块链技术为近几年兴起的一项重要科技创新，涵盖了计算机网络、密码学、分布式系统、金融学、博弈论等诸多学科的知识。作为一种分布式记账的底层核心技术，其能够有效改变传统中心化的交易模式，实现去中心化的点对点价值传输与协作。它甚至被认为是社交网络之后的第五次颠覆式创新，是央行纸币信用之后的第四个里程碑，是未来价值互联网的基石。

2008 年，中本聪（Satoshi Nakamoto）首次提出比特币的概念。其后，人们把比特币的底层基础技术总结为区块链技术。区块链主要通过共识机制、密码学、时间戳等技术，将一段时间内的交易信息打包成数据区块，按时间顺序连接形成一种链式结构，并最终形成去中心化的共享账本。数据区块通常包含前一区块哈希值、交易信息等关键数据。前一区块哈希值确保了区块之间的顺序连接关系，任何想要篡改数据区块的行为，都将导致区块连接关系断开，因而极易被识别和剔除。交易信息是系统进行交易处理的核心，其中定义了交易的发起者、接收者、发起者的签名信息等。根据区块链系统的架构模式、运行机制、账本数据维护方式等特征，其具有的主要特性为去中心模式建立信任、可靠分布式数据库、不可篡改共享账本。

去中心模式建立信任：区块链系统中没有中心化的权威机构，各节点拥有相同的权利和地位，其运行规则完全公开透明，节点之间并

不需要完全的相互信任，每笔交易都需要节点之间达成共识才能写入区块链账本中。由于区块链账本交易数据完全公开，各共识节点直接平等协作，因此在系统规则范围内，节点之间无法相互欺骗。

可靠分布式数据库：账本数据在各节点都有完整拷贝，各节点自己管理自己的数据库，整个系统没有单点故障，比传统中心化的数据库具有较强的健壮性和安全性。

不可篡改的共享账本：区块链的账本通过共识机制在系统范围内形成共享账本，账本中的数据区块通过哈希指纹的形式形成链式结构，在系统容错范围内，区块链账本数据无法被篡改。共享账本提供透明性和公正性，使得对账、清结算能够自动执行。

正如美国区块链科学研究所的梅兰妮斯万所说，区块链技术的发展可以大致分为 1.0、2.0 和 3.0 三个阶段。其中，区块链 1.0 指以比特币为代表的虚拟货币时代，号称“可编程虚拟货币”，保证价值安全的转移；区块链 2.0 发展为智能合约的广泛使用，区块链被应用于货币市场和金融市场，号称“可编程金融”；区块链 3.0 则是超越金融外的应用，即在政府、健康、科学、文化和艺术方面有所应用，号称“可编程组织和社会”。区块链技术的发展与应用使人类社会从简单的信息互联升级为价值互联，它有望从各个方面对人们的生活产生积极影响。

## 1.2 区块链技术面临的挑战

区块链技术能够在一定程度上通过算法模型解决信任问题，形成一种价值互联，给我们带来了很多现实问题的解决方案以及未来应用

的想象空间，但是现有的区块链系统在系统架构、共识机制、数据存储及交易效率等方面还存在诸多问题。区块链技术在基础理论与实际应用方面仍面临巨大挑战。区块链的“不可能三角”的问题就引起了广泛关注，即去中心化、安全性、扩展性之间的矛盾难以彻底解决，需要从基础理论和工程实践两个层面去做出突破和权衡，使区块链系统达到理想的应用状态。

### 1.2.1 系统架构

区块链系统根据其应用需求及实现机制的不同，通常被分为公有链、联盟链、私有链三类架构模型：

公有链：面向社会公开，全球范围内任何节点都可以不经授权地加入或退出区块链网络。同时，账本数据由所有区块链节点共同参与维护，一般依赖代币激励机制维护系统的良性运转。该类系统去中心化程度较高，但是系统共识效率往往低于联盟链和私有链。

联盟链：一般应用于达成同盟协议的机构之间，完成多机构协作。该类系统严格控制节点的加入和退出，且只有通过授权的成员节点才能参与账本数据的共识维护，要求具备严格的节点身份审查和权限控制机制。该类系统去中心化程度低于公有链，但系统运行效率较高。

私有链：一般应用在机构内部，运行规则由机构自行设定，中心化程度较高。其多用于机构内部治理，账本数据不公开，适用性较差。

事实上，如何权衡好去中心化程度和系统运行效率之间的矛盾正逐步成为区块链领域的热门话题。区块链不可能三角也逐渐成为阻碍区块链技术快速发展应用的难题，需要对其进行突破。

### 1.2.2 共识机制

现有的公有链系统大多采用PoW、PoS等最终一致性的共识机制。PoW 共识机制通过挖矿的方式争夺记账权，只有获得记账权的节点才能获取最终的区块奖励。然而，巨大的挖矿算力竞争带来巨大电力等资源消耗的同时，似乎并没有给人类社会带来任何的积极影响。例如，目前的比特币拥有全球大部分的数字货币挖矿算力，使其余使用该类共识机制的区块链系统很难获得足够强大的算力来确保系统的安全性。同时，由于该类算法通常依据最长链原则达成数据账本的最终一致性，是一种弱一致性算法。因而，该类交易通常需要等待多个确认，交易确认周期较长，如比特币交易一般需要等待 6 个确认，每个确认的平均时间约为 10 分钟，并不适用于高频交易的场景。而在 PoS 共识机制中，拥有的代币及其币龄越高的节点拥有的权利越大，越容易挖矿产生新区块。该算法能够在一定程度上解决算力依赖及能源消耗问题，但也存在公平性问题，例如 PoS 的初次分配问题，会出现“穷者越穷，富者越富”的情况，更严重的是，PoS 机制使得作恶的节点可以不用顾虑损失的在不同分叉上同时出块，因此存在安全隐患。

现有的联盟链系统则多采用 PBFT 等传统的拜占庭容错算法。PBFT 算法是 Miguel Castro 和 Barbara Liskov 于 1999 年提出来的一种拜占庭容错算法，该算法能够在分布式系统中存在有恶意节点的情况下，实现正确节点就某个输入达成一致，其通常包含多轮共识协商的过程。该类算法多采用轮流记账的方式提高共识效率并消除算力竞争，

进而避免了资源浪费，因而多被应用于多方协作的联盟链系统。PBFT 算法不仅可以解决区块链系统中交易序列化的问题，还能够提供 f=⌊(n-1)/3⌋的容错能力，其中 n 为节点总数，f 为可容纳拜占庭节点的最大数量。然而，该算法在多个阶段都需要节点间的两两交互，造成较高的通信负载，进而影响共识性能，扩展性比较差，一般参与共识的记账节点不能超过一二十个，否则性能将快速递减。

### 1.2.3 数据存储

目前区块链数据存储的主要挑战在于全节点存储数据量庞大、数据增长速率过快，以及数据存储过程中的数据隐私保护等方面。由于每个区块链全节点都保存有完整的历史账本数据备份，所以存储数据量庞大及数据增长速率快。例如，截止 2018 年 6 月持续运行了 8 年的比特币系统，每个全节点都需要存储约 170G 的完整数据账本，而且这一数据仍在快速增长。同时，由于存储在区块链账本中的数据通常保持公开透明，如何保证重要数据的隐私性也成了区块链面临的一大挑战。

针对区块链的数据存储难题，目前大多区块链系统通过仅存储数据的哈希指纹的形式来降低数据存储量，而原始数据仍存储于链外。由于原始数据并不直接保存在区块链系统中，所以该类系统在降低数据存储量的同时能够做到一定程度的隐私数据保护。然而，该类区块链系统也存在无法利用区块链中的数据直接进行处理分析的能力，系统的运行还需要与外部系统协调配合，在一定程度上降低了区块链系统的可扩展性和安全性。此外，由于每个节点仍保存完整的账本备份，

所以整个系统的数据存储量依旧会随着区块链节点的增加及系统的持续运行而不断增大。

### 1.2.4 交易效率

在区块链技术受到热烈追捧的同时，其交易效率问题也备受争议。比特币、以太坊等公有链平台取得广泛应用与成功的同时，受限于共识机制、节点通讯等因素，区块链网络吞吐量较低，如比特币只能达到约 7 笔/秒的交易处理速率，而以太坊也只能达到约 15 笔/秒的交易处理速率。而在社会实际生产实践中，交易系统的处理能力往往需要达到几千笔甚至几万笔每秒，系统的交易效率正逐步成为制约区块链系统商业化应用的瓶颈。

虽然目前国内外对于区块链交易效率的改进上也进行了一些有益的探索，如采用 DAG、限制共识节点数量等方式，但是目前仍没有理想的解决方案。在实际生产环境中，应该结合自身的实际应用场景，对系统整体架构方案进行调整，提高系统的交易效率以满足应用未来的高频交易需求。

## 1.3 区块链应用面临的挑战

正如未央网作者李赫在文章《从歪曲的比特币谈区块链应用及误区》中开篇所提到的“区块链源于 IT 技术，但主要应用于非 IT 行业，由于行业的专业性和技术的复杂性在区块链应用时共存，导致出现了两个世界：一个是程序员的世界，这里的人在大肆谈论着去中心化、价值传输网络、第五范式，但是却不懂行业特点和细节，应用很难具

体落地；另一个是行业人士的世界，这里的人熟悉合规处理，清楚行业流程，却被区块链的概念弄得晕头转向”，可见区块链技术要实现真正的落地引用，除了 IT 技术外，还要融合商业逻辑。在实现区块链应用落地的过程中，主要还存在以下挑战：

（1）去中心化的阻力

现有的中心化体系经过不断的修正，已有序地运作多年，形成了稳定的运作结构。近几年随着互联网的发展，更是涌现了如 BATJ 等“巨无霸”般的中心，人们已习惯于通过中心化的系统来处理、解决事情。而区块链技术作为新兴的 IT 技术，一方面受制于“不可能三角”的问题暂未出现有效的解决方案，未能如中心化系统般有效地解决实际商业场景中的“大规模、高并发”的应用要求；另一方面由于使用区块链构建的系统未经市场考验，人们对其系统的运行稳定性仍然存疑，在实际问题的解决上更倾向于引入中心化的体系进行处理。

（2）被歪曲的理解

一提到区块链，大部分人的第一印象是“ICO”、“发币”，进而可能会联想到 “割韭菜”等负面报道，造成这个的原因，一方面是由于前期币圈的过度炒作，另一方面也是由于区块链这种新兴技术对很多人来说还不容易理解。还有一方面原因是区块链作为一种全新的技术，目前离成熟还需要一定的时间，而需要让用户认可和行业的加持则需要更长的时间投入。因此，尽管区块链技术将来可以给人们的生活带来颠覆性的变化，但由于前期的市场乱象及未形成大范围的应用，故人们大多对区块链还存在着一些误解。

（3）法律法规有待更加明确

区块链作为一项新兴技术，目前大部分国家仍未出台相应的法律法规去对行业进行规范与明确区块链上存证信息、智能合约等信息的法律地位，这就造成即使区块链具有可信、溯源、存证、不可篡改等特性，但由于缺乏国家法律法规的保护，在出现相应的诉讼、仲裁问题时，区块链上存储的数据信息可能不能起到真正的效力。故区块链技术需实现落地商用，需要政府出台相应的政策和法规予以保护。在中国，最近一个月最高法院出台司法解释，认可通过区块链技术收集的证据的“真实性”，无疑是在向有利于区块链推广应用的方向发展迈出了一大步。

# 2 使命：打造智能设备价值互联网络，赋能智慧惠民生态

## 2.1 智能设备与区块链

随着物联网时代的到来，为了使人们能够享受更为便捷高效的服务，越来越多的智能设备被接入互联网，如自动售票机、自动售货机、服务机器人等。然而，人们似乎都没有意识到自己使用这些设备的时候会产生许多有价值的数据。随着大数据技术的发展与应用，数据即价值似乎已经成了人们的一种普遍共识。在注重数据隐私保护的同时，人们也正尝试利用智能设备产生的数据获取更多的经济收益。然而，目前并没有能够使智能设备平台便捷接入，并以较低的成本不断进行数据价值交换的综合性平台。

目前，大多数智能设备通过网络光纤等方式接入到其运营商的中心服务器，以获取设备运行维护的实时数据，从而实现提高设备的维护效率。极少有智能设备对用户使用数据进行进一步综合分析利用，在线支付、人工智能等技术的发展使得智能设备还能获取实际使用者的数字身份信息，通过对这些数据的进一步分析使用，可以实现智能设备对用户进行消费数据权益发放、定向广告推送等功能，进而实现更高的数据价值。同时，现有的智能设备多采用中心化的网络连接及认证体系，该类系统存在认证权利集中、数据篡改、单点故障等问题。即使是相同类型的智能设备，由于生产厂商的不同，设备身份标识及安全防护级别也不相同，设备之间难以实现互联互通且设备往往面临

被入侵的风险，如近几年发生的黑客远程操控智能设备的事件越来越多。未来随着智能设备的逐步普及使用，实现智能设备的分布式互联、自动化管理、设备全方位安全保障已经成为一种趋势。

区块链技术具有安全、去中心化、无需中心信任和不可篡改等特性，能够使各参与方以较低的成本实现价值互联和价值传递。智能设备天然就是分布在不同场景中，集中化的管理很难保证效率和安全。智能设备生态中有多个相互有弱信任关系角色，像设备制造商、运营商、供货商、场地租赁方、消费者等。因此区块链的去中心化信任建立对智能设备网络尤为重要。区块链技术能够很好的解决单点故障等问题，基于区块链技术的设备身份认证、数据价值传递，将能够使智能设备的接入和价值融合更加安全、灵活。因此，探索为智能设备打造高性能的区块链平台，能够使智能设备从传统的服务提供者转变为价值数据的提供者和消费者，将有助于形成完整智能设备生态体系，实现多方共赢。

## 2.2 智能设备区块链

运通区块链公司将利用区块链技术，结合智能设备的发展状况打造一个高性能的智能设备区块链平台，它采用一种融合架构模型，并利用终端安全认证、DPOC-BFT 共识算法等关键技术，构筑安全高效的智能设备价值传输体系，进而实现智能设备的去中心化自治。

智能设备区块链将围绕智能设备，以公有链和联盟链结合的方式形成一种混合链模型，利用公链保证系统的安全开放，在面向消费者（C 端）的场景中提供信任机制和激励机制；同时针对特定的应用场

景，采用联盟链的形式确保联盟成员身份的安全可靠，以及在 B 端场景中联盟数据的隐私安全。由于智能设备之间的差异，在实际生产环境中，我们无法确保智能设备的硬件条件。根据前期调研实践的结果分析，目前自助柜员机（ATM）等智能设备拥有较多的硬件资源，但是它目前也正在操着削减硬件成本的方向发展。而对于自动售货机等一类智能设备，其拥有的硬件资源较少。考虑不同智能设备的现状，运通区块链采用一种智能设备节点映射的机制，对于硬件资源不足的节点，采用该机制将其接入网络并映射至全节点，由该全节点代其行使全部的权限和义务，使其拥有其余全节点智能设备的所有权益。同时，为确保系统的稳定高效运行，首次引入 DPOC-BFT 的共识机制，在保持系统开放的同时，利用 DPOC 算法选出超级节点，并利用改进的 BFT 算法使超级节点之间实现强一致性，避免系统分叉。

运通区块链将致力于打造一个安全、高效、稳定、可扩展的智能设备区块链平台，提供便捷的智能设备认证接入、跨链交易、安全隐私保护等功能，打造完整的智能设备区块链生态体系。运通智能设备区块链的使命，就是通过大家的努力，让社会更信任、让设备更智能、让生活更安全。

## 2.3 智能设备区块链带来的变革

随着人们对于便捷生活的追求，智能设备必将渗透到人们生活的各个角落，而每一个接入运通区块链平台的智能设备都将成为价值互联网世界的一个入口。每一个智能设备将不再是孤军奋战的个体，而是像人类社会一样的社群，通过贡献自己的“力量”推动社群的发展壮

大，而社群的发展又将给它们带来直接收益。在这种互惠互利的模式下，推动智能设备社群向健康高效的方向发展，使智能设备为人类提供更为便捷高效服务。

未来，运通区块链将围绕智能设备区块链平台，联合合作伙伴、开源社区、极客等一道共同打造涵盖新零售、大文旅、大健康、新政务、新物流、新金融的惠民生态，为民生的改善，构建更诚信的商业体系和社会贡献力量。

# 3 运通智能设备区块链(IDBC)

运通智能设备区块链（IDBC：Intelligence Devices BlockChain）依托广电集团强大的智能设备研发和生产能力，聚焦于区块链技术与智能设备的融合，致力于构建智能设备区块链的基础设施与生态环境，以区块链技术改善惠民生态中的分配机制和激励机制等生产关系格局，以智能设备提升惠民生态中各行业的生产、流通效率。

## 3.1 设计理念

运通智能设备区块链 IDBC 是基于区块链开源技术和广电集团在金融电子、人工智能、轨道交通等方面的核心技术和多年项目经验累积的基础上研究设计的安全高效的企业级区块链基础设施平台。运通智能设备区块链 IDBC 的设计秉承以下理念：

**（1）混合链构想。**尽管现有公有链发展迅速，技术也日臻成熟，但是其完全开放的设计使得交易数据对区块链网络中所有实体都是可见和透明的，这种特性对许多传统数据敏感性的行业（如金融业、制造业、服务行业等）存在风险。此外，监管机构对于交易数据的监管和审计要求也需要数据具有一定的开放权限。如何在数据可信、安全、开放之间取得平衡，靠现有的单一公链、私链、联盟链难以达成目标。因此，混合链成为了新的发展方向。IDBC 首次将公有链和联盟链融合起来应用于智能设备生态领域。通过公链提供可信公开数据的查证、智能设备接入认证等服务；通过联盟链提供会员企业的系统准入、身份鉴别、隐私保护、数据隔离等服务，保障成员间交易的安全。

公有链和联盟链之间通过侧链技术和智能合约跨链技术进行数据交互和价值锚定。

**（2）终端安全认证**。IDBC 链设计的初衷，是将各种智能终端设备接入区块链网络。智能终端提供原始数据的采集、过滤、加工；区块链负责将处理后的数据链式存储和传输，保障数据的不可篡改和分布式存储。二者完美结合有效的将线下线上数据标准化和一体化，这也是物联网+区块链范围的延展。对于上链终端设备的安全认证，将会是考验系统架构体系安全的关键一环。IDBC 首次引入 ODIN 标识和 PPK 协议，结合传统的 CA 证书体系和 TLS 协议，全方位、多维度的解决各种不同类型终端的唯一地址标识和身份认证的问题。

**（3）开放接口**。智能设备区块链 IDBC 的接口将会以统一化、标准化的方式对外开放，公链本身也将开源。我们将秉承开源的思想，积极投身开源社区的工作。此外，智能设备区块链将专注于底层区块链平台的建设和智能设备接入标准的制定，与各行业的合作伙伴携手合作，共同打造基于智能设备的区块链可信基础设施和生态圈。

**（4）数字经济体系。**由于区块链生态体系大多是以一种分布式多方协作的形式运转，其完整生态的建设往往离不开数字经济的支撑。通过对生态中的贡献者进行奖励、对破坏者进行处罚等方式，数字经济体系有助于在生态内形成一种正向的行为导向。完善的数字经济体系能够有效增强区块链生态的凝聚力和运行效率，使参与者（投资者、开发者、维护者、使用者等）形成高效的数字经济循环模型。由于系统运行规则写在达成共识的代码中，对于生态中的任何人都公开透明，

其在一定程度上可被认为是区块链生态的运行法则。数字经济体系建设将有助于运通区块链打通智能设备生态的各个环节，将新零售、大文旅等子生态连接起来，形成有机整体，使各参与方通力合作，在贡献力量的同时获取收益，形成正向激励，有效改善生态内的生产关系。

## 3.2 总体架构

运通智能设备区块链 IDBC 创新的采用混合链架构，充分利用公链和联盟链的优点，采用层次化的架构设计，将区块链基础设施和上层应用、设备接入层进行隔离，这种高内聚低耦合的设计可以充分将各个功能模块化、提高运行效率、保障系统安全。系统架构图如下：

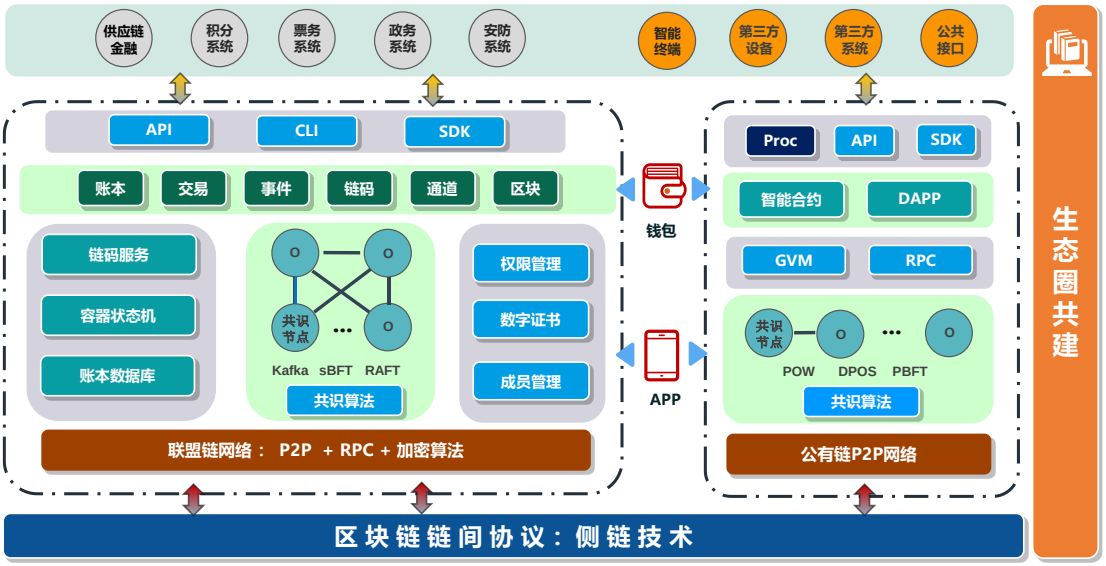


图 3-1 IDBC 架构层次

### （1）业务应用层

业务应用层采用开放的 RESTful 接口风格，可以对接各种智能设备终端、第三方系统，可以实现终端身份认证、终端标识管理。智能终端可以进行采集数据上链等，其所有生态建设行为都将获得奖励。

由于 IDBC 采用了联盟链和公链的混合架构，不仅智能终端设备

可以设置厂商的准入规则，平台还可以扩展到多种行业应用场景，比如供应链金融、积分管理系统、政务系统、物联网设备、人工智能等。

**（2）接口层**

IDBC 混合链中的公链和联盟链虽然使用了不同的基础框架，但是都支持包括 API、SDK、CLI 等形式的接口调用方式。应用程序接入方可以灵活的选择接入方式，通过接口层与区块链进行交互。

针对智能设备终端的运算资源有限、元器件功耗较低、安全监控要求高的特性，IDBC 使用了定制版的智能设备驻留程序 Proc。驻留程序以守护进程的方式运行在后台，且将区块链终端的功能最小化，以适配智能终端运行的软硬件环境。驻留进程提供了设备接入的身份认证模块、数据采集与上链、运维监控等基本功能。

**（3）区块链层**

IDBC 混合链中的基础设施，包括了公链和联盟链两套底层链。公链采用 DPOC-BFT 的共识算法、由网络节点投票选举出出块节点。智能合约运行在改进的 GVM 虚拟机上、通过 RPC 调用提供服务、支持多种分布式应用 DAPP 开发。

联盟链基于 Hyperledger 基础上搭建，采用 KAFKA、SBFT、RAFT 等共识算法，支持联盟成员单位的准入管理、证书体系、权限管理；通过账本数据库和容器状态机，为上层应用开发链代码定制和管理。同时多通道机制、CA 证书、交易事件、链代码模块、容器虚拟化等功能在处理敏感数据和保护隐私的同时，也能够提高系统的交易吞吐量，有效的支撑了企业级应用的构建。

### （4）链间协议层

区块链底层采用了 Gossip、Kademlia 等协议构建 P2P 网络体系，侧链协议允许价值在公链和联盟间进行转移，通过双向锚定将其在联盟链中锁定，同时在公链中释放，反之亦然。通过侧链技术，可以实现安全数据存储于联盟链中，再结合多重签名等机制，实现链间的价值转移。联盟链的准入、权限管理、高并发能力实时响应客户请求；公链的公信力机制让客户的数字资产得到安全保障。

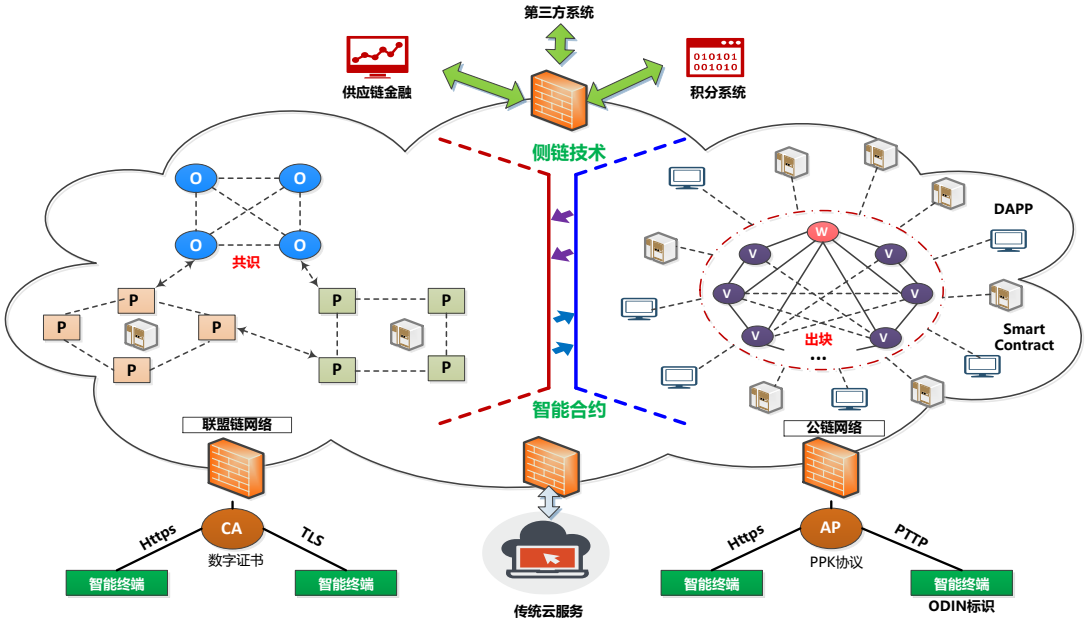


图 3-2 IDBC 网络拓扑图

图 3-2 是运通智能设备区块链 IDBC 的网络拓扑结构。左侧演示了联盟链组网架构和成员组成；右侧演示了公链网络组网架构和成员组成。联盟链和公链之间使用侧链技术和智能跨链合约进行价值锚定和数据交互。

智能终端设备可以通过 CA 证书的方式使用 TLS 和 HTTPS 协议与区块链网络交互；或者通过 ODIN 标识、通过 AP 节点代理，使用 PTTP 和 PPK 协议与区块链网络交互。此外，对于视频、音频、图片等不适

合链上流转的多媒体数据，仍然可以存储于传统云服务器，而将数据对象的摘要信息上链存储和流转。

第三方系统接入方面，IDBC 混合链提供 RESTful 标准的调用接口，利用联盟链自身的特点，为企业级的传统应用（比如供应链、积分、政务、票务等）切入区块链提供了无限的空间。智能终端层、传统应用层和区块链层之间使用防火墙进行安全隔离防护。

## 3.3 功能特性

运通智能设备区块链 IDBC 主要提供区块链底层技术和链上服务管理平台两大方面的服务。通过调研大量的业务模型和具体案例，结合自身实际应用需求，在设计 IDBC 的时候主要考虑要实现的功能特性包括智能设备准入、用户数字身份识别、并发交易秒级确认、海量数据存储、智能合约管理、权限控制、可视化运维等。

**（1）智能设备准入**

由于智能设备的硬件的功能型号各异，接口不一，常规接入需要大量重复的二次开发。IDBC 提供了一种网络节点映射机制可以将智能设备安全接入区块链网络并被其他节点感知，同时获得设备在网络的唯一标识。在该机制中，每一台智能设备通过身份注册协议，可映射成为区块链网络中的一个节点，进而参与整个智能设备链的账本验证及维护。该节点可以是轻量节点，也可以是竞选成为 BP（Block Producer）节点。智能设备可以通过该节点在区块链网络中共享用户的使用数据，在数据被消费使用后获取奖励。

**（2）用户数字身份识别**

随着人工智能技术的发展与演化，以生物特征识别（人脸、指静脉、掌纹、声纹）为代表的人工智能技术已经逐渐添加到各类智能设备中，如刷脸支付、指纹识别等。在智能设备生态中，对于需要进行终端用户身份认证应用场景下，IDBC 将利用生物特征识别等人工智能技术手段，辅助以动态二维码等便捷的认证形式，通过智能设备的用户身份识别终端对用户现实身份进行识别与认证，并将其转化为一种匿名的区块链数字身份参与区块链生态活动中。目前，运通区块链已经针对用户数字身份识别进行了技术攻关和应用验证，证明了技术实施的可靠性并申请了多项发明专利。

**（3）并发交易秒级确认**

由于 IDBC 公链开放给所有用户使用，故单位时间内交易处理能力直接决定了公链能否进行规模使用。IDBC 通过对签名算法、共识机制、消息广播、账本结构等环节的优化改造，可实现 3,000+/s 的交易处理能力和 1 秒内的交易快速确认，满足大部分实际场景的用户体验。后续 IDBC 团队将聚焦结合侧链及链下交易的方式进一步提升系统单位时间内的交易处理能力。

**（4）海量数据存储**

在以往区块链记账模式下，系统长时间的运行后，历史数据不断累积，运行一个全节点的成本与运行时间成正比例增长。IDBC 借鉴 IPFS 存储方式，创建一个持久且分布式存储和共享账本的网络，根据应用需求自主设置要存储或公开的账本片段，IDBC 激励模型会根据节点提供给全网使用的账片段容量来给予相应的权益。节点需要验证

指定交易时，可以快速的从多个相邻节点并行同步不同区间的账本数据，从而有效解决全节点的海量数据存储的问题。

**（5）智能合约管理**

智能合约是一种旨在以信息化方式传播、验证或执行合同的计算机协议。智能合约允许在没有第三方机构信任背书的情况下进行可信交易，这些交易可追踪且不可逆转。为了提升用户体验，减少中间环节，IDBC 在智能合约的管理上提供一站式的服务，支持合约上传、一键部署、合约升级、状态查询、合约的废弃和清理等功能。

**（6）权限控制**

在权限控制方面 IDBC 主要完善了两方面的内容：一、对数据内容的权限控制。用户可以对本节点产生的有价值数据做控制，从而设置某些数据可以免费开放访问，或是某些数据需要付费使用以及私密不开放数据。二、对分组内用户的权限控制。用户可以自建分组来做进行组织隔离，不同分组间的用户不能互相访问对方的数据，组内的成员可根据实际需求授予不同的操作权限，如管理员、普通成员等。

**（7）可视化运维**

提供包括智能合约管理软件、区块链浏览器、区块链节点监控服务、网络实时监控模块、日志统计模块、告警与通知模块等一系列配套的可视化工具和服务，以便于商用系统的管理与维护。

## 3.4 技术创新

### 3.4.1 智能设备接入

IDBC 智能设备区块链的初衷是整合各种智能终端设备作为原始数据的提供方来接入到区块链网络，通过提供服务及分享数据的方式来体现衡量自身的贡献值，从而在区块链激励模型中获得相应的收益。

IDBC 引入的 PPK 协议是一种由国内开源团队自主研发的融合了 IPFS、区块链等技术的 P2P 协议，并建立了一套完全开放、开源的 ODIN 运行机制，为每一个生产价值数据的智能设备提供一个作为区块链唯一标识的 ODIN 号。所有接入到 IDBC 中的智能设备都将通过设备注册协议，将设备唯一 ODIN 号注册至公链中，形成全网唯一且无法篡改的智能设备区块链身份。智能设备在 IDBC 网络上开发出来的数据都会携带自身的 ODIN 唯一标识，ODIN 拥有者具备获取数据资源的访问权限，也可以是通过适当的自定义机制让使其他用户获取数据资源的访问权限，如通过订购、资源传递、数据使用收费等方式获得。

### 3.4.2 共识算法

IDBC 中由于联盟链拥有完备的访问控制机制及联盟特定的运行规则，其区块链节点数量通常不会过多，因而仅在传统的共识算法 RAFT、PBFT 基础上进行适当优化即可投入使用。而对于公链，由于智能设备数量庞大且硬件资源有限，如果所有节点都直接参与共识记账，将对网络资源造成巨大压力。因此 IDBC 提出了一种新型的融合委托贡献和拜占庭容错的共识算法 DPOC-BFT(Delegated Proof of

Contribution- Byzantine Fault Tolerance)，该算法中通过委托贡献协议 DPOC 竞选记账节点，这些节点通过改进后的 BFT 算法达成最终一致性共识。任何节点都可以参与 BP 生产者竞选，竞选者在抵押资产（即数字积分）的情况下，需要贡献自己的硬件基础设施（包括计算能力、存储、带宽），所有节点均可以参与投票，最终竞选排名以得票数与忠实矿工工龄权重求和排序。节点实际得票数计算公式如下：

$$S = (\sum_{i=0}^{n} N_{\mathrm{i}}) \cdot k\% + C \cdot (1-k)\%$$

其中：$S$ 为得票数；$N_i$为第 $i$ 个节点的投票数；$k$ 为数字积分投票权重占比；$C$ 为节点的贡献度（根据智能设备的押金、出块数、打包率综合得出）。系统投票过程中将竞选产生共 $n$ 个超级节点以及若干候补节点，而这些超级节点通过改进后的 BFT 算法产生区块并达成共识，任何一个区块都有其余 BP 超级节点签名。如果 BP 节点在区块验证过程中发现有非诚实或不作为节点，对此节点进行剔除，并由候选节点替换其参与区块链账本共识记账。超级节点的个数 $n$ 将随着智能设备网络的大小来周期性的调节。起始为 7 个节点，当智能设备网络大小发生变化时，动态的在 7 – 101 个之间调节。

### 3.4.3 跨链模式

作为连接不同区块链的关键技术，跨链技术主要实现不同区块链系统之间的信息互通和价值转移。IDBC 将结合传统的跨链模型，设计出一套可以实现联盟链与公链的跨链交互模式，并在价值互连基础上，实现跨链的智能合约调用。传统的三种跨链模式如下：

**（1）公证人模式**。该模式下，不同区块链系统之间通过引入第三方公证人的方式，让价值在各个区块链账本之间间接流通。由于公正人的模式与区块链去中心化的设计理念存在矛盾，故其一直备受争议。

**（2）侧链/中继模式。**该模式通常采用中继的技术手段，对核心主链进行功能和价值上的扩展。中继器本身也可以是一种侧链，主链并不一定知道侧链的存在，通过多重签名等机制可以实现主链资产锁定及侧链锚定、执行等操作，进而实现价值的跨链传输。

**（3）哈希锁定模式。**比特币闪电网络中最早提出利用哈希锁定进行链下快速交易的基本思路，后来其关键技术逐渐发展成为一种区块链跨链的技术手段。该模式并没有实现价值在链间的直接流通，而是通过哈希锁定的方式实现间接的跨链价值转移。

IDBC 主要通过集成哈希锁定的方法来对侧链技术进行创新，将公链作为要锚定的主链，联盟链作为侧链用来接收用户交易请求或是合约调用并对请求做处理。当需要处理跨链资产交换或跨链合约调用时，IDBC 会先锁定公链上的交易发起方的资产，并通过联盟链内置合约将交易中一些非敏感性数据提交到公链记录，然后通过联盟链上交易处理结果加上交易双方的数字签名来解锁公链上锁定的资产。通过这种方式，可以实现混合链上数字资产的自由流通，跨链的合约调用实现了链间交易的自动化触发，减少了中间人环节的介入，为去中心化的跨链交互方式提供了一种可行示例。

### 3.4.4 安全隐私保护

为保障系统数据的安全隐私，IDBC 混合链提供多种不同安全等

级的解决方案，具体如下：

**（1）双重身份验证**

IDBC 是一种集成了公链和联盟链的混合链设计机制，并提供了一种加密机制来对已经公链私钥和联盟链私钥做映射，用户接入 IDBC 时需要提供两套私钥签名才能接入到网络中，如果一旦公链或联盟链私钥丢失或被盗，可以通过另外一个私钥做映射运算推导出丢失的私钥信息，所以也相当于双重备份的机制。

**（2）国密算法**

随着国家对金融安全的高度重视，国际密码局制定标准的国密算法也被广泛应用到各类金融或偏金融的应用系统中。运通区块链凭借母公司多年在金融设备和金融系统领域的技术积累，成功使 IDBC 系统支持国密 SM2/3/4 算法，给用户更多保障，同时满足合规性要求。

**（3）零知识证明**

零知识证明能够在不向验证者提供任何有用的信息情况下，使验证者来相信该结论是正确的。该算法使用户能够充分证明自己是某种权益的合法拥有者，又不把有关的信息泄露出去。运通区块链团队将进一步针对该技术进行研究与运用，使 IDBC 系统进一步提升对用户隐私数据的保护级别，避免信息泄露，同时将进一步探索将其应用于数据存证等多种应用场景。

### 3.4.5 三层激励模型

IDBC 在数字经济模型方面，结合系统公链加联盟链的融合架构特点，在技术上支持三层激励模型。第一层是公链系统原生数字积分

支持，主要用于公链系统的开发、维护、激励等，鼓励更多的人参与到公链系统大生态的运行维护。第二层是通过公链智能合约发行的子生态数字积分，该类数字积分主要由生态项目决定，其可与原生数字积分进行锚定，由市场决定项目的价值。第三层是通过联盟链智能合约发行的联盟数字积分，该类积分可以通过跨链协议与原生数字积分或者公链的子生态数字积分进行锚定，由联盟成员共同决定数字积分的流通形式，在其内部形成完整运作，促进联盟的进一步协调发展。

三层经济模型要求区块链系统能够支持原生数字积分、子生态数字积分和联盟数字积分的发行流通，同时需要跨链协议实现其在不同链之间进行流转。

# 4 运通区块链的应用方案

人类文明发展至今，正处于由工业文明向信息化文明过渡的时期，信息化对人类社会的发展起到了革命性的作用。正如电影《黑客帝国》所展示的场景一样，随着智能设备与物联网技术的发展，未来人类除了在现实生活中拥有一个实体身份外，还将被赋予一个数字化的身份，围绕个人所产生的资产、信用、经历等信息将通过智能设备的采集并进行数据化后存储在个人的数字身份内，这个数字身份将会被存储在一个安全、高效、防篡改的区块链网络中，这就是运通区块链所要打造的智能设备生态链。

数字经济体系连接智能设备生态的各个领域，通过适当的激励措施使生态体系中的参与者获取正向激励，促进整个生态的健康发展。IDBC 中数字积分基本流通路线如下：

- 智能设备：上传真实的用户行为数据并获取一定的积分奖励。设备接入时需抵押一定的积分，当其上传恶意数据时进行押金罚没，从而防止设备恶意上传无效的数据造成网络拥堵。
- BP 节点：打包生成合法的数据区块之后，将获得一定的积分奖励，从而激励更多节点竞争记账，共同维护账本的一致性。
- DAPP 开发者：可以针对这些智能设备开发出个性化的应用，应用部署上线到区块链网络之前需要支付一定的数字积分，并可以从 DAPP 使用者中获取一定的积分作为手续费。
- 数据消费者：在使用数据前需要支付一定的积分给数据生产者，

以获取相应的数据资源。

- 普通用户：可以在使用智能设备之后获取一定的积分奖励，并利用这些积分从设备运营商处兑换商品或服务。

为保证用户数据的隐私性，智能设备将根据应用实际需要选择要上传的数据。同时，对于联盟链，上传的数据也仅对授权成员可见。本章将详细介绍将对运通区块链围绕智能设备区块链展开的，在新零售、大文旅、大健康、新政务、新物流、新金融等领域的应用探索。

## 4.1 新零售生态

“新零售”的概念最早由马云在 2016 年提出，随着科学技术的不断发展，“新零售”由开始时的通过电子商务连通线上与线下的模式逐渐演化成无人零售模式，虽然现在还是以电商模式为主流，但在人工智能、物联网、移动通信等技术的完善与普及后，相信未来无人零售模式才是“新零售”的最终形态。

无人零售主要由智能化后的自动售货设备提供，目前这些自动售货设备大多只停留在为客户提供日常所需的商品销售服务，而每名客户的消费习惯却由于缺乏数据入口而白白流失，未能通过这些智能设备捕捉到每名客户的消费大数据，这是对资源的极大浪费。有鉴于此，运通区块链将运用区块链技术，链接所有的自动售货设备，让每台自动售货设备都成为区块链网络上的一个节点，在用户授权后用于保存上传每名客户的消费信息。具体的应用场景示例如下图：

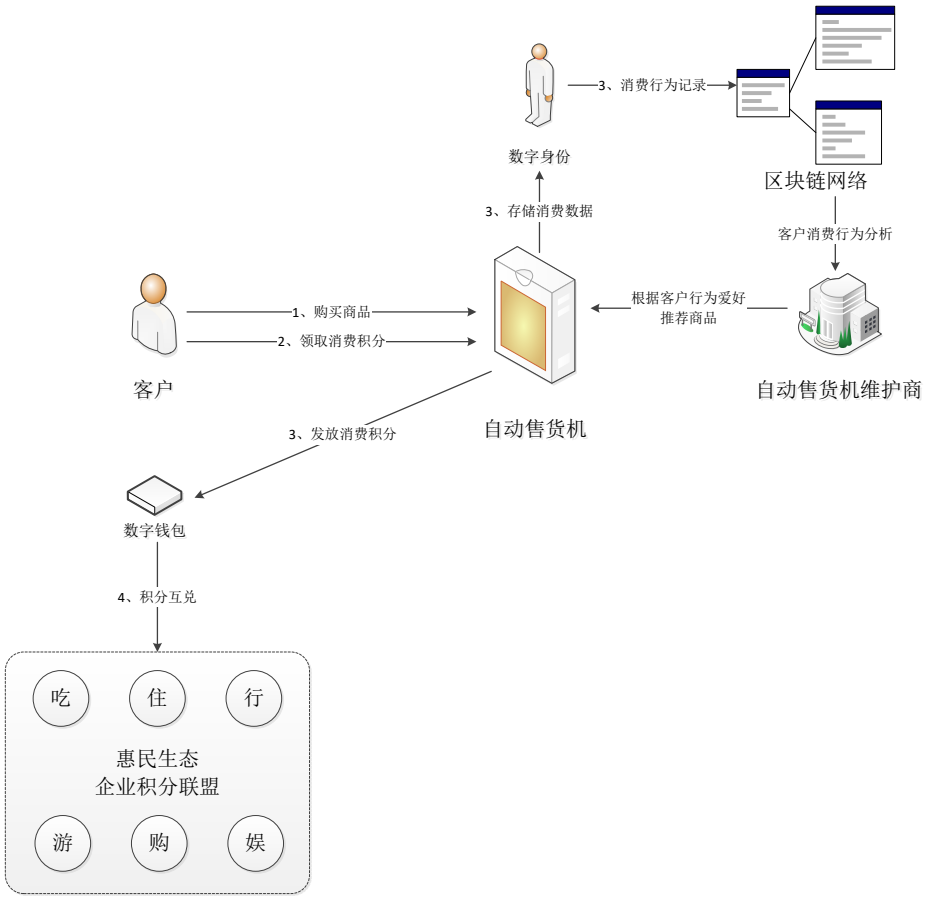


图 4-1 新零售应用方案

同时，在公链上通过智能合约的形式发行新零售生态的积分--消费积分。在每名客户的消费数据如何获取和保存的问题上，运通区块链为每名客户提供一个专属的数字钱包，并通过引入消费积分激励机制，激励客户使用数字钱包消费，从而使得客户在自动售货设备消费后，机器能够准确地记录下客户的消费时间、购买品类等信息，进而形成每个客户的数字化身份信息。在客户再次消费时，机器可根据客户的消费爱好推荐消费商品，缩短客户的选择时间，为客户提供更好的消费体验。而用户体验的提升将有助于使用户更多地使用该类自动售货机，为自动售货机的维护商带来利润收益，进而形成正向激励。

由于消费后赠送的消费积分记录在区块链网络上，具有安全、

不可删改的特性，将其与公链的原生数字积分进行锚定，其价值能够以极为便捷的形式在公链传递。因此，这类消费积分可间接在运通区块链上各个惠民场景进行兑换使用，赋予了消费积分更大的使用价值和发展空间。

## 4.2 大文旅生态

智能设备的产生与不断改进，正给人们的生活与出行带来方方面面的改变，其中旅游行业是改变最大的行业之一。过去，人们需要忍受在景区门口漫长排队等待购票的煎熬；过去，人们需要耗费大量时间通过纸质地图寻找和记录旅游路线；过去，人们为了出行方便需要花费高价参团且对旅行团的服务质量难有清晰的了解。而如今，随着智能设备的出现，人们可通过提前订票及使用自动售票机打印门票，大大缩短了购票等候的时间；通过加入了 GPS 技术的电子地图可以实时、清晰地了解到旅游的路线，基本杜绝了由于路线错误而白白浪费旅游时间的可能；通过互联网化的旅游平台，可以了解到其他旅行者对旅游团的服务的历史评价，甚至可以通过游记来制定自己的出现方案，从而优化旅游体验。由此可见，智能设备与技术正对人们的旅游出行带来了巨大的改变。

然而，虽然目前人们的旅游出行通过智能设备的介入已得到了极大的优化，但仍存在如下问题有待进一步改进：

（1）智能设备大多由景区进行管理，游客的出行数据只能保存在单一或某几个合作的景区的数据库中，由于数据不共享而难以形成用户画像，进而优化旅行者的旅游体验。

（2）旅游过程中的不文明行为屡见不鲜，旅游景区虽加强了监控管理，但却未能对不文明的旅行者形成有效的制约；同时，对于部分文明旅行者的好人好事行为也未得到有效的奖励。

（3）旅行者对旅行团、旅游服务商（如酒店、餐馆等）的评价均存储在部分旅游平台的中心化系统上，而这些旅游平台可以对评价的内容选择性进行显示，评价的真实性存疑，从而会出现部分旅行者通过平台选择了“优质评价”的旅游服务而最终强差人意的情况出现。

针对上述问题，运通区块链提出利用区块链技术赋能智能设备，进一步优化人们旅游体验的大文旅生态方案。首先，运通区块链将通过区块链网络链接自动售票机、自动售货机、景区内的视频监控设备、景区门禁设备、酒店自助入住/退房设备等智能设备系统，通过这些智能设备和人工智能技术精准捕捉人们的旅游行为。其次，运通区块链将引入大数据系统，将个人存储在区块链上的信息进行处理，构建个人在旅游生态上的数字身份活动轨迹。

具体的应用场景示例如下图：

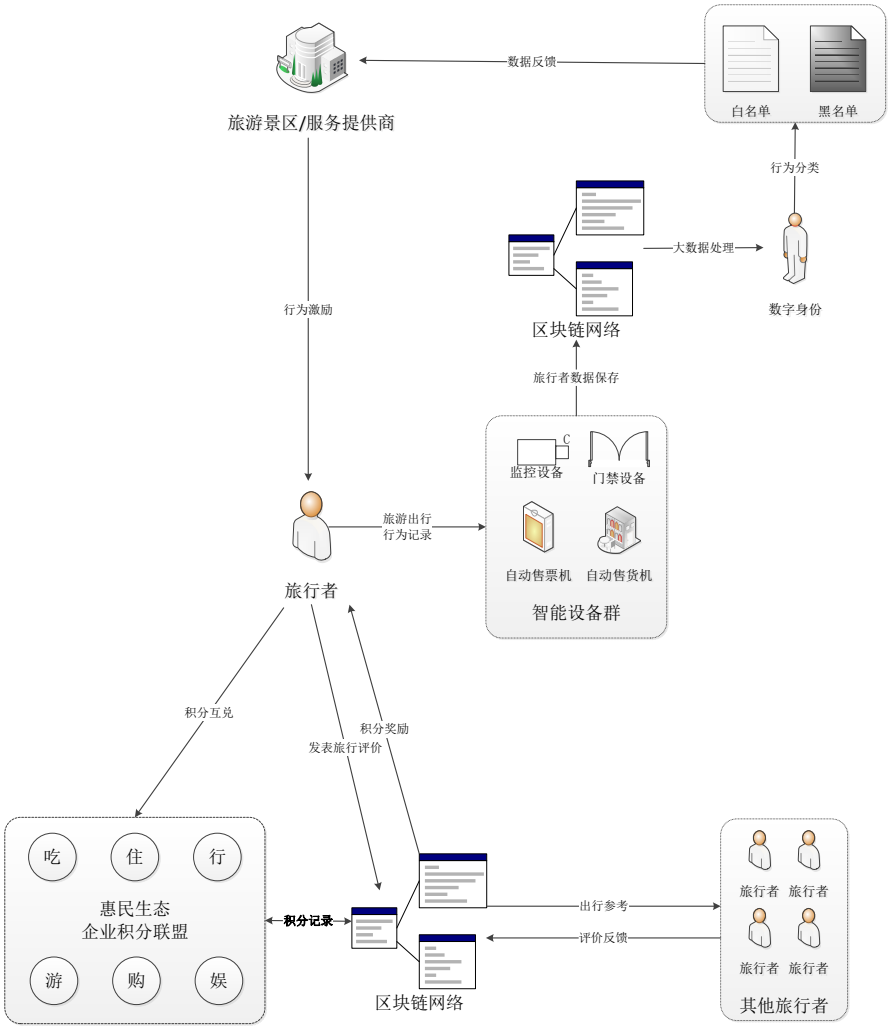


图 4-2 大文旅应用方案

同时，与新零售生态类似，大文旅生态也引入与原生数字积分锚定的旅游积分机制。由于区块链具有可信、不可篡改等特性，个人在旅游过程中的“吃、住、行”等行为轨迹都通过智能设备真实地记录在区块链网络上。对于文明的旅行者，可系统地生成“旅游白名单”，在白名单内的旅行者，各景区或旅游服务商可提供相应的旅游积分奖励，从而激励旅行者在旅游中要做到文明出行；而对于存在不文明行为的旅行者，可系统地生成“旅游黑名单”，通过区块链网络广播至所有的景区和旅游服务商，并罚没数字积分、加价甚至拒绝提供服务等负激励的手段限制不文明旅行者的旅游出行，从而对旅游不文明行

为起到制裁与预防的作用。

在旅游服务评价的问题上，区块链网络天然地存在公开透明、真实不可删改的特性，因此旅行者可将每一次旅游体验的游记、旅游攻略等及对旅游服务商提供的服务评价上传至由运通区块链构建的旅游平台，对优质的游记、旅游评价内容予以旅游积分奖励，其他旅行者可通过支付旅游积分的形式查阅平台上的优质旅游评价，获取相关的出游地的旅游信息及优质旅游攻略。同时，与原生积分锚定的旅游积分可用于获取出行优惠或在运通区块链上参与积分互兑的商家联盟间进行兑换使用，进而可以完善旅游评价体系，为旅行者在出游前提供有效的参考帮助。

## 4.3 大健康生态

中国医疗健康产业市场规模在过去的 5 年中保持了超过 20%的年复合增长率，预计至 2020 年会超过 8 万亿。随着科技的发展，人们开始将人工智能与医疗进行结合，衍生出一系列的智慧医疗应用，如谷歌 AI 运用到乳腺癌的病理识别中，准确率已超过了医生的诊断；Watson 可以在 17 秒内阅读 3469 本医学专著、24.8 万篇论文、69 种治疗方案，和进行 61540 次模拟试验、产生 10.6 万份临床报告等操作，进而得出用户需要的诊断结果；自学式人工智能技术已经可协助预测心脏病发作、皮肤癌筛选等工作。可见智慧医疗已开始走出实验室，走向了人们的生活。针对医疗板块，运通区块链将利用区块链网络，融合人脸识别、人工智能等多项技术，为人们提供远程医疗、数字病历、医药溯源等服务，构建惠民的大健康生态。

### 4.3.1 基于智能设备的便民医疗

“小病在社区，大病到医院”，是我国实行的分级诊疗的要求，虽然从制度上合理利用了医疗资源、缓解了医疗压力，但却由于受时间、空间的制约，未能满足部分人群（如上班族、行动不便的老年人等）的医疗所需。有鉴于此，运通区块链将通过连接到区块链网络的智能设备解决时间、空间上的医疗问题。

首先，运通区块链将在居民小区、写字楼、养老院等区域内布放由 VTM、自动售药机、智能血压计、智能听诊器、智能血糖仪等医疗医用设备构成的智能设备组，让患者获得近距离的医疗服务，大大缩短耗费在看病途中的时间；第二，运通区块链将联合居民小区、写字楼、养老院等附近的医院，通过智能设备提供远程看病的服务；第三，通过区块链技术实现智能设备与附近医院系统的链接，医生在为患者看病后可将药方直接发送至自动售药机，患者直接通过自动售药机付钱拿药，从而完成完整的诊疗过程。具体的应用场景示例如下图：

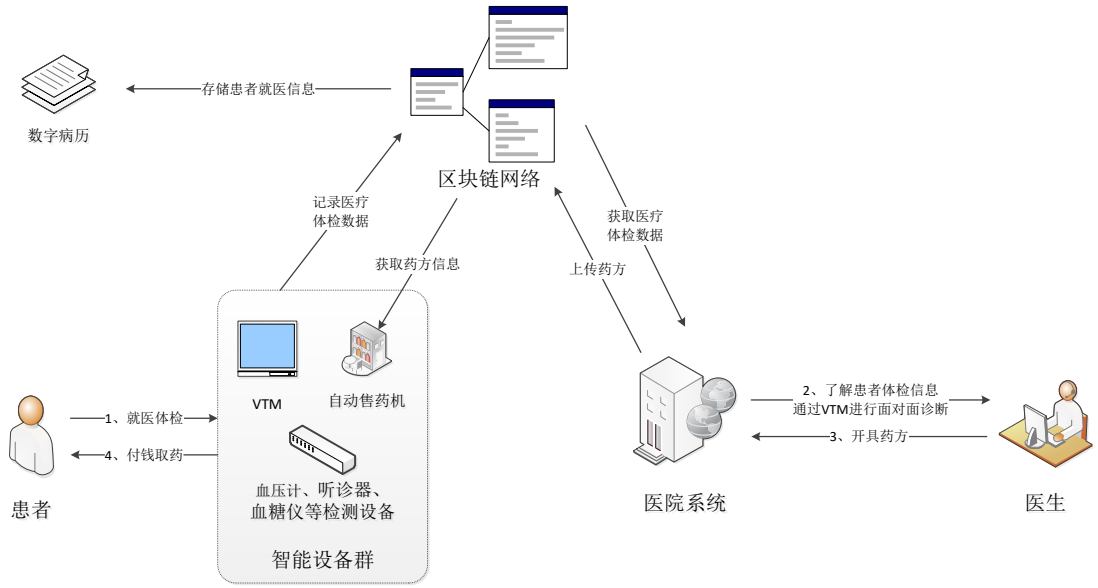


图 4-3 便民医疗应用方案

### 4.3.2 区块链电子病历

当前患者的病历信息都存储在各个医疗部门的中心化数据库或者文件柜中，各医疗机构数据难以共享，对患者在不同的医疗机构就医时造成一定的麻烦，同时也不利于医疗机构对患者过往病历的了解。另一方面，患者医疗信息泄漏事件时有发生，随着基因数据检测手段以及指纹数据应用的普及，若这部分患者的信息一旦泄漏，将会导致灾难性的后果，且作为数据的保存方——医院，一旦患者信息遭到窃取，轻则声誉受损，重则可能需接受法律的制裁。

有鉴于此，运通区块链将利用分布式账本技术，完整、准确地记录下患者的每一次就医情况，医生给患者制订诊疗方案时，可以参考有效、连续的诊疗记录，提高治病效率；另外，使用加密技术对患者病历数据进行加密，只有在患者授权的情况下查看病历，从而保护患者隐私信息。具体的应用场景示例如下图：

（1）病历信息存储

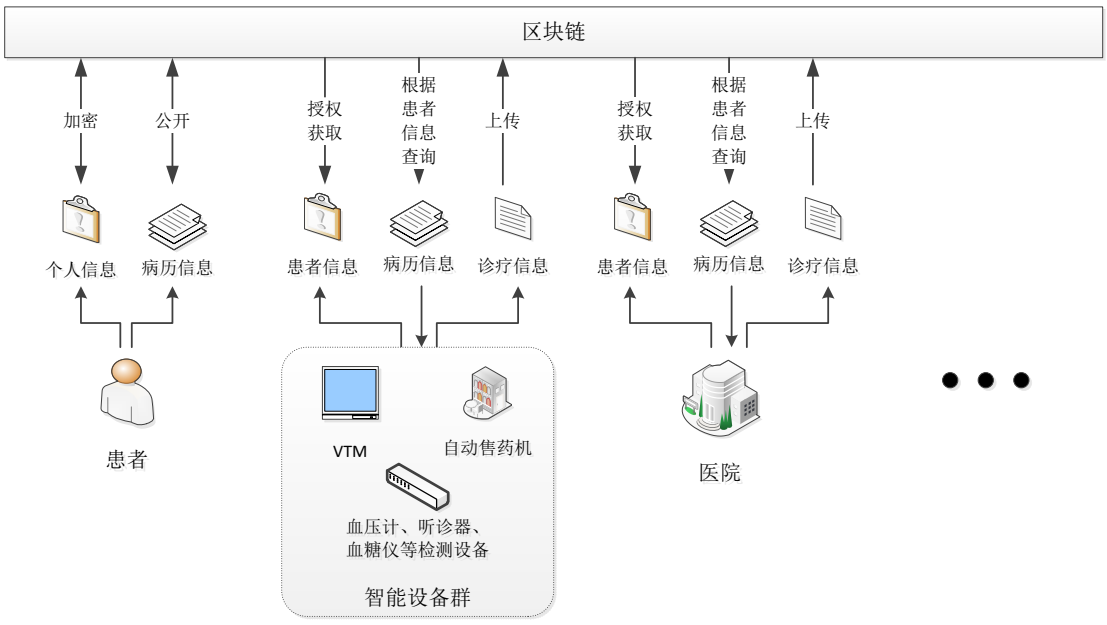


图 4-4 病历信息存储示意图

## （2）就医流程

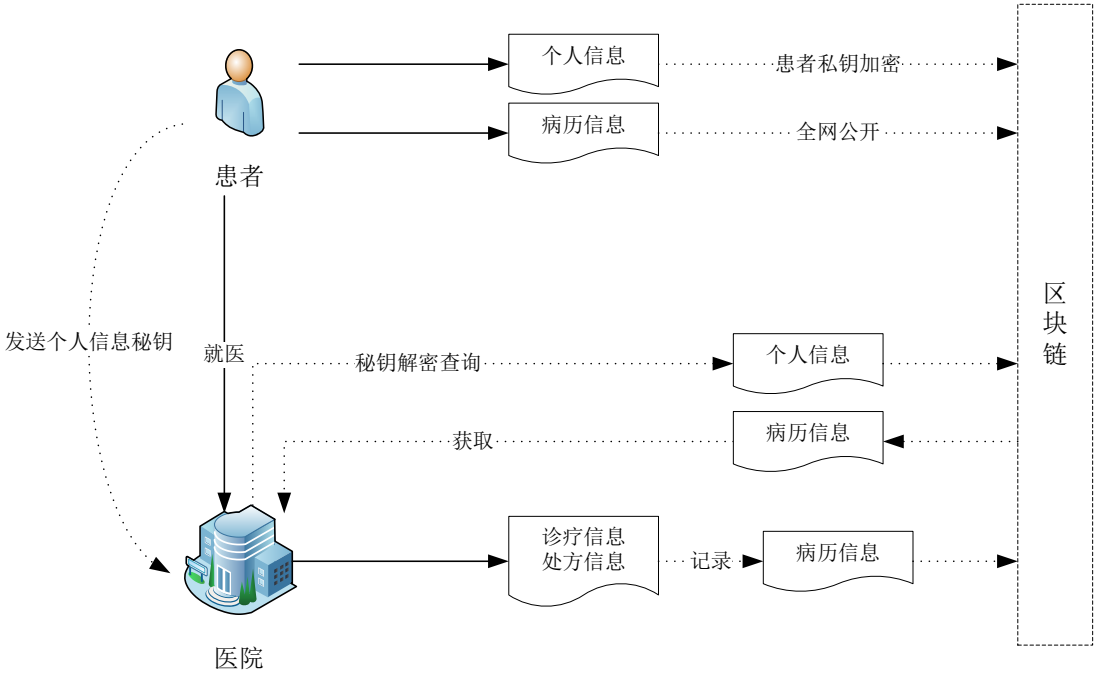


图 4-5　就医流程图

## （3）转诊流程

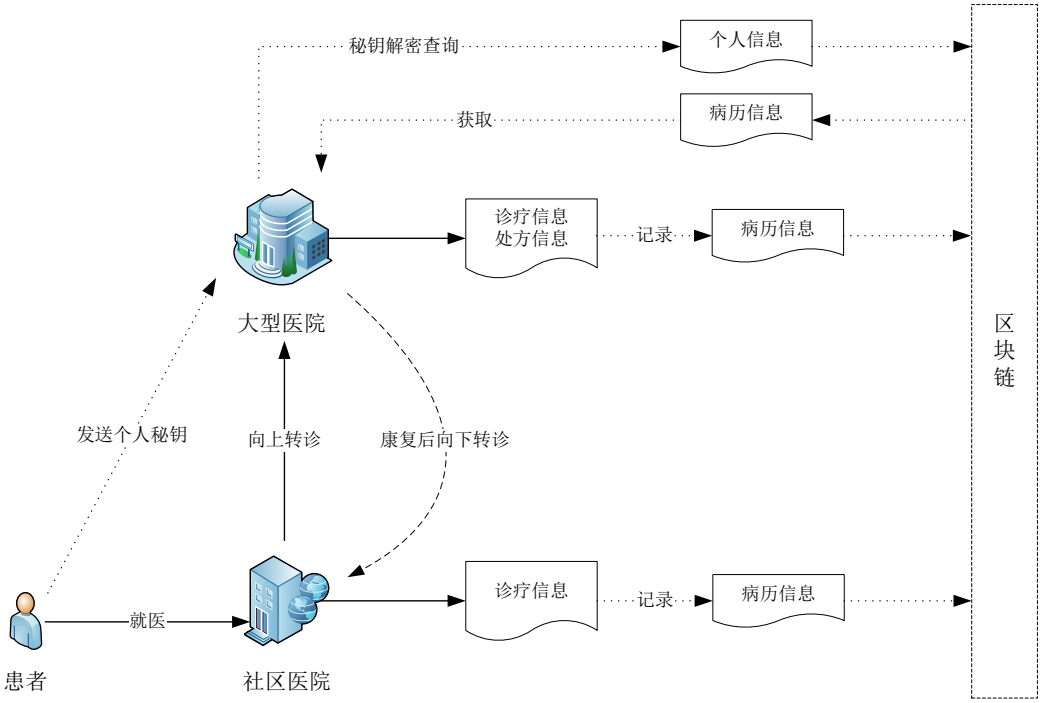


图 4-6　转诊流程图

### 4.3.3 药品溯源

药品是关乎百姓生命健康安全的特殊商品，掺杂使假危害重大。近年来，制售假药、劣药等违法犯罪行为高发，个别不法分子为牟取暴利，疯狂地进行假药生产销售，严重影响了医药市场的正常秩序，给百姓带来了极大的危害。运通区块链将把区块链与药品供应链结合起来，将药厂、物流、仓储、分销等所有的药品信息记录到区块链上，进而最大程度保证患者用药的安全。

具体的应用场景示例如下图：

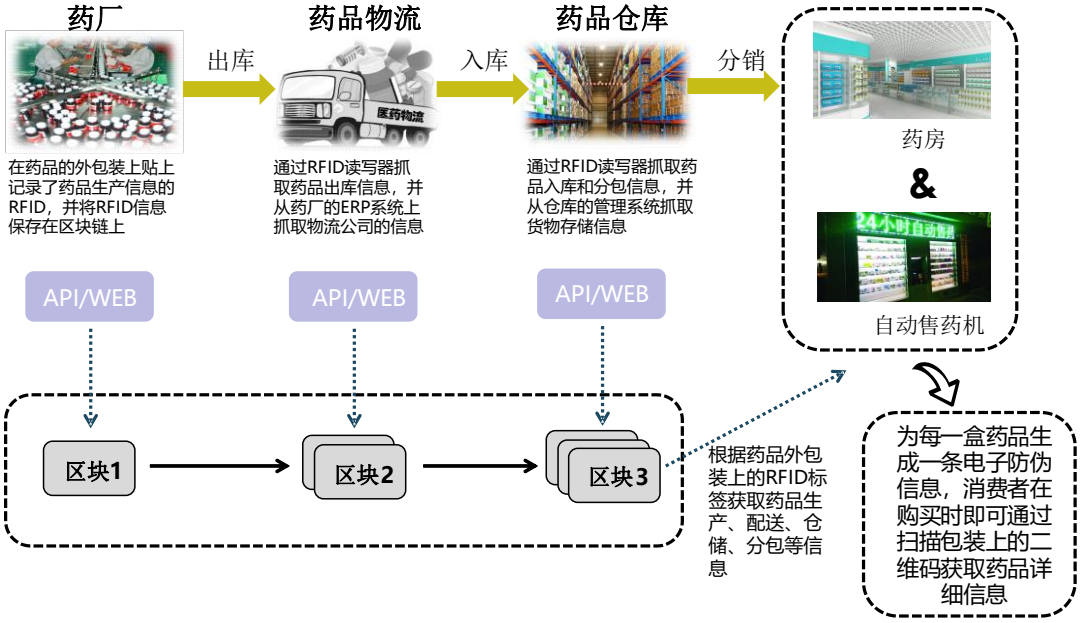


图 4-7 医药溯源应用方案

## 4.4 新政务生态

随着经济社会的发展，特别是计算机互联网时代的到来，我国传统政务系统的弊端日益凸显，存在架构臃肿、效率低下、信息壁垒等问题，阻碍了经济社会的良性发展。近年来，伴随着科技的发展和国家政策的引导，电子政务发展态势迅疾，政务效率已经得到了大幅度

的提高。但是，现阶段以 CBA 平台（Cloud Computing 云计算、Big Data 大数据、Artificial Intelligence 人工智能）为代表的电子政务系统仍然存在着以下问题，是制约电子政务进一步发展的重要瓶颈：

（1）各政务部门间的系统不兼容，个人/企业政务信息难以实时更新、共享，具体弊端表现在跨部门办事时需要通过函调的方式来获取个人/企业在其他政府部门的政务信息，函调所需要时间较长，导致政务办事效率低，让群众来回跑路。

（2）系统的集成化和中心化在简化办事流程的同时也扩散了系统的安全风险，增加了防范外部黑客攻击的成本。

（3）当前的中心化平台在数据跨中心平台交互共享过程中存在着信任、安全和效率之间的矛盾，同时政务信息透明度不高，影响了政府的公信力。

区块链技术的兴起恰好为突破电子政务现阶段的瓶颈提供了契机。运通区块链立足于智能政务终端设备，结合生物识别（人脸识别、指纹识别等）等人工智能技术，采集个人信息、利用 VTM 等智能设备读写个人政务信息、利用区块链存储个人信息与政务信息，从而打造流通于政务系统的个人数字身份。运通区块链打造的政务链平台，将利用区块链技术突破现阶段电子政务的发展瓶颈，具体如下：

（1）运通区块链通过区块链网络连接各个智能政务办事终端，打破终端之间系统不兼容的问题。此外，办事群众在任何一个作为运通政务链节点的部门输入个人信息或上传电子证件时，运通区块链会随即将 VTM 设备所捕捉到的群众身份数据通过分布式记账的方式实

时存储、共享到各区块链节点上，实现信息的实时共享。在这种情况下，办理跨部门事务时可以经过办事群众授权直接从区块链上获取所需的个人政务信息，无需再通过其他部门函调相关信息。

（2）区块链的去中心化和共识机制使得单个或少数个别节点的信息丢失或伪造对整个区块链系统的信息不构成威胁，有效地降低了信息的安全风险，加上密码学加密技术的使用，大大增强了系统防范外部黑客攻击的能力，缩减政府部门在系统安全问题上的相关支出。

（3）区块链的多中心化的账式存储形式实现了信息跨级别、跨部门、跨中心、跨区域的实时共享。在跨平台的数据信息交互共享上兼顾了安全和效率两大问题。同时，系统向个人提供公共节点，公共节点可实时监控政务的办理进度，从而增加了政务信息的透明度，提升政府的公信力。

运通区块链的政务链平台具体应用场景如下：

（1）办事群众在某个政府部门的智能政务终端初次办理事务时，需要通过生物识别设备进行人脸、指纹识别，并与公安系统登记的身份信息进行比对、校验，最终存储在区块链上，形成个人数字身份。

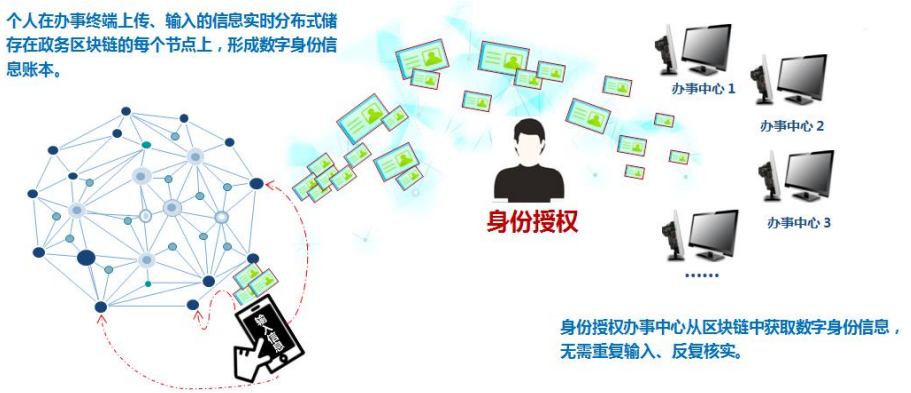


图 4-8　新政务应用方案

（2）随后，办事群众继续输入个人信息及电子证件等信息进行事务办理，政务智能设备将捕捉群众的身份信息进行加密，并实时共享到各个区块链节点上，每个节点都保存了该群众上传的所有政务信息和相关材料，形成独有的、完整的数字身份。

（3）当群众再次办理政务事务时，通过人脸识别和身份证件信息的对比验证后即可访问个人存储于区块链上的数字身份。政府部门在获得办事群众的身份授权后，即可从区块链上调取该群众之前上传的身份数据信息，同时也可以写入新的政务信息存储在个人的数字身份上，从而实现无需重复输入相同信息，减少信息核实的时间和成本，提高了行政的效率与公信力。

## 4.5 新物流生态

商品从生产到销售，都会经历复杂的物流流转过程，人为因素在整个商品流转中参与过多，导致对中间环节的数据可信度存在较大疑问，由此引发的商品溯源问题是目前社会和企业的主要难题。运通区块链将利用区块链技术，依托区块链具有的数据不可篡改、交易可追溯以及时间戳的存在性证明机制，降低物流体系内各参与方数据被篡改风险，并且可实现有效的追责。同时，在物流仓储过程中的仓单管理上，基于运通链生成电子仓单，提高仓单的安全性及流转效率。物流商品溯源以及电子仓单管理的主要流程如下：

（1）物流商品溯源流程

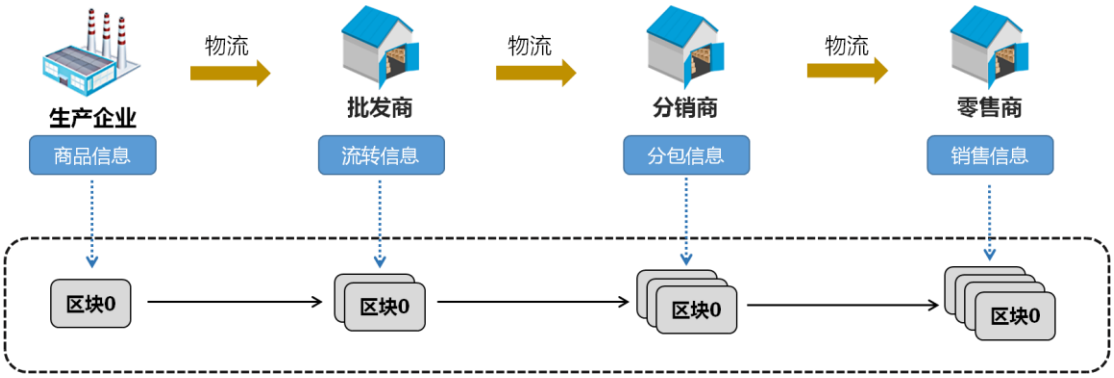


图 4-9 物流商品溯源

（2）电子仓单生成流程

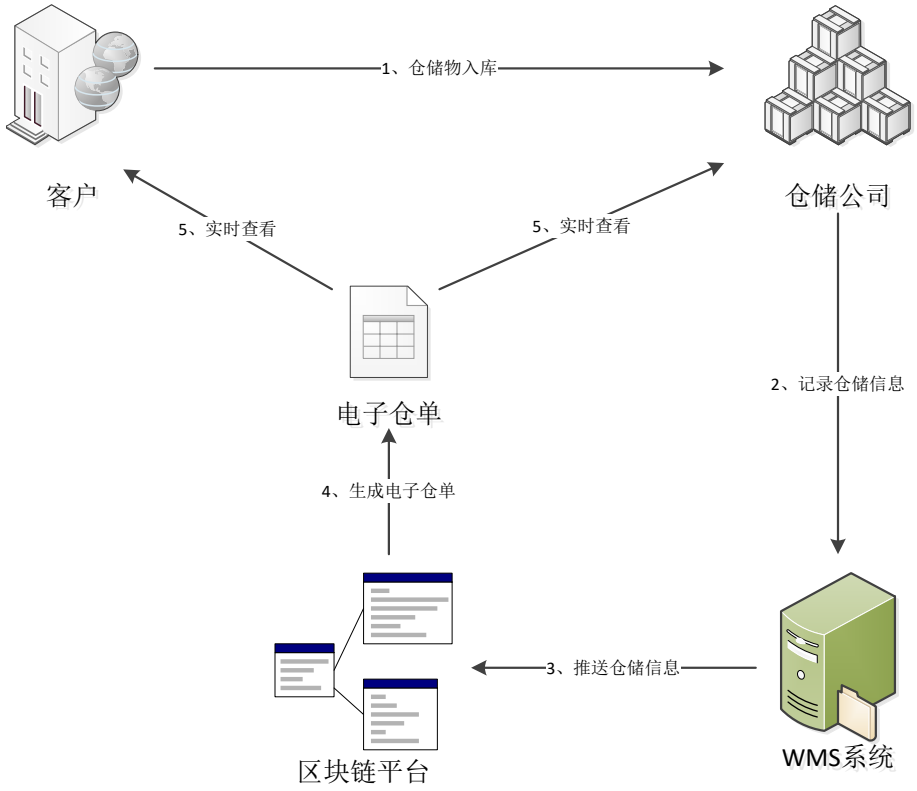


图 4-10 电子仓单生成流程图

## （3）仓单质押流程

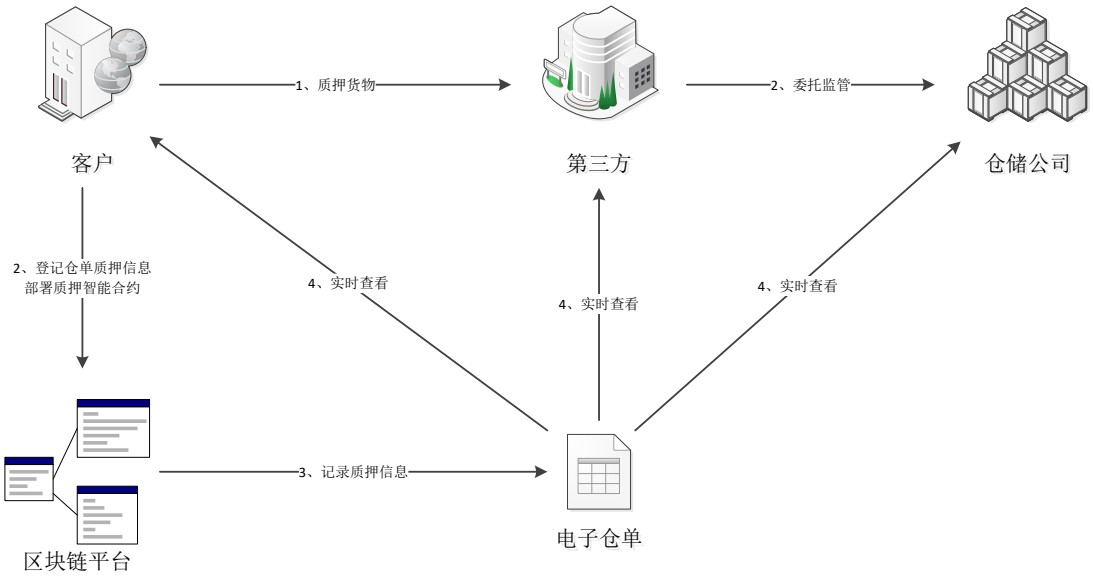


图 4-11 仓单质押流程图

## （4）实施质权流程

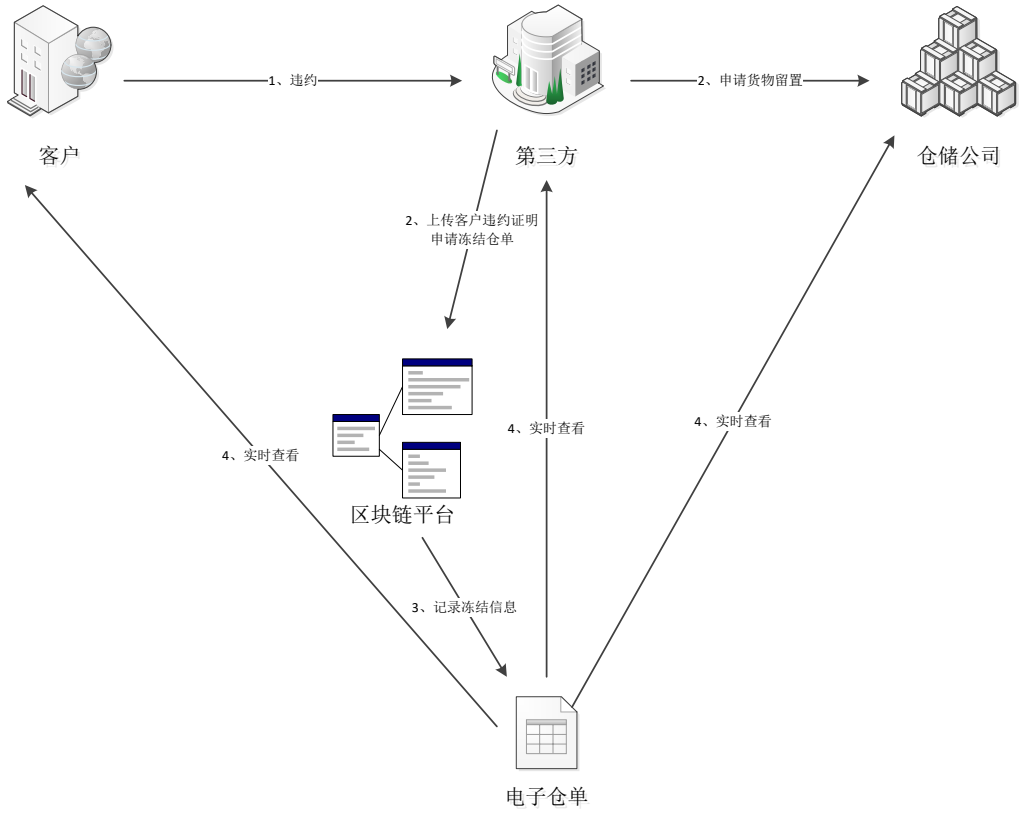


图 4-12 实施质权流程图

## 4.6 新金融生态

基于区块链构建的智能设备公链平台上，链接了众多企业，这些企业中有实力雄厚的行业龙头，也有为龙头企业提供原材料和销售产成品的上下游中小微企业，从而在公链平台上形成了多条不同行业、不同区域的供应链，运通区块链将分行业、区域为公链平台上的企业建立不同的联盟链，为这部分企业提供供应链金融解决方案。

### 4.6.1 供应链金融应用方案

供应链金融业务主要解决供应链条上的“供、产、销”问题，由金融机构为供应链条上的中小微企业提供预付融资、货押融资、保理融资等金融服务。业务的主要参与方有金融机构（如银行、券商、小贷公司、保理公司、P2P 公司等）、核心企业（行业龙头等）、上游供应商、下游采购商、仓储物流企业等。

在传统的供应链金融模式下，主要存在如下痛点问题，导致供应链金融开展较为困难。

（1）金融机构的痛点分析：

- 游离在实体产业外，由于信息不对称造成核信较为困难且成本较高，传统模式下的操作大多仅能通过企业提供的合同、发票、货运单据查验业务的真实性。
- 核心企业配合积极性不高，“萝卜章”事件时有发生。
- 核心企业自建供应链金融平台，瓜分供应链金融市场份额。
- 贷前、贷后需投入大量的人力对供应链上的交易进行尽调核查，但业务收益却不高。

（2）核心企业的痛点分析：

- 配合金融机构开展业务并未能得到收益，但却需承担风险（如承担担保、回购责任等）。
- 担心企业核心信息泄漏，不愿将 ERP 信息向金融机构公开。
- 自建供应链金融平台虽能带来收益，但由于大多企业人员非金融行业出身，缺乏金融风控思维，抗风险能力较差。

（3）上游供应商和下游经销商的痛点分析：

- 中小微企业居多，融资渠道较少，融资成本较高。
- 与核心企业的谈判、交易中处于弱势地位，核心企业可随意延迟支付货款或采购货物，进一步增加了资金的压力。

针对上述问题，运通区块链的解决方案如下：

（1）金融机构的痛点解决方案

- 交易信息由上下游企业提供并经核心企业确认，从提供信息开始至信息最终确认，所有操作均保存在区块链上，任何人均无法对信息进行篡改。
- 利用“挖矿”机制对核心企业进行激励，即核心企业每在系统上确认一笔交易，即等于“挖矿”成功，由系统向核心企业发放积分，积分可换取业务分润。
- 通过区块链技术保证企业间交易的真实性，金融机构可实时监控交易的确认情况，提高尽调核查的工作效率，降低人力成本。

（2）核心企业的痛点解决方案

- 通过“挖矿”获取业务分润收益，提高配合积极性。

- 交易信息由上下游企业录入，核心企业只需配合确认信息即可，无需将自身的 ERP 信息开放予他人。
- 作为参与方直接从金融机构对上下游企业的融资业务中分得收益，无需自建金融平台承担金融政策和经营风险。

（3）上游供应商和下游经销商的痛点解决方案

- 引入核心企业对交易信息进行确认，降低了金融机构的融资风险，从而降低企业的融资成本（风险越大成本越高）。
- 使用智能合约取代人为操作，交易到期后自动执行，杜绝核心企业随意拖欠的情况。

具体业务流程如下：

## （1）预付款融资

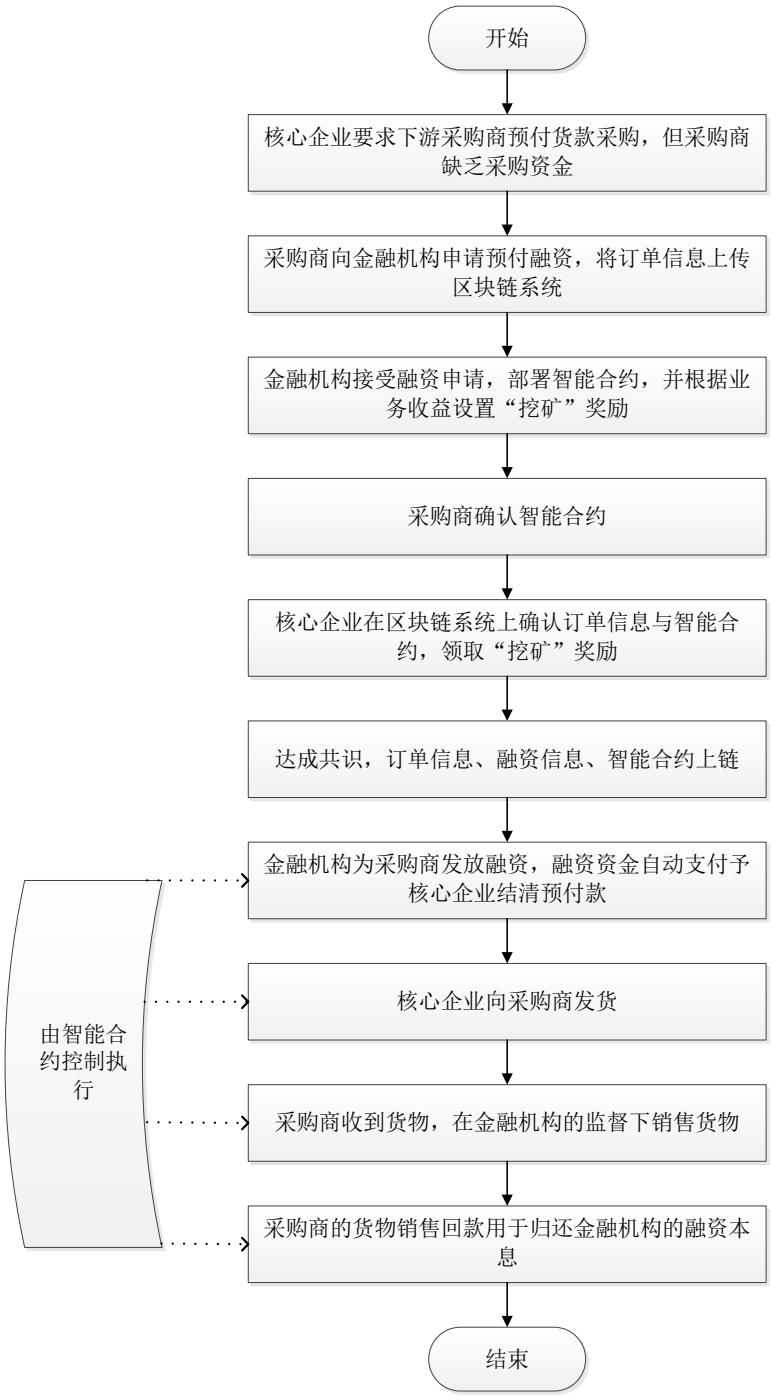


图 4-13　预付款融资流程图

## （2）货押融资

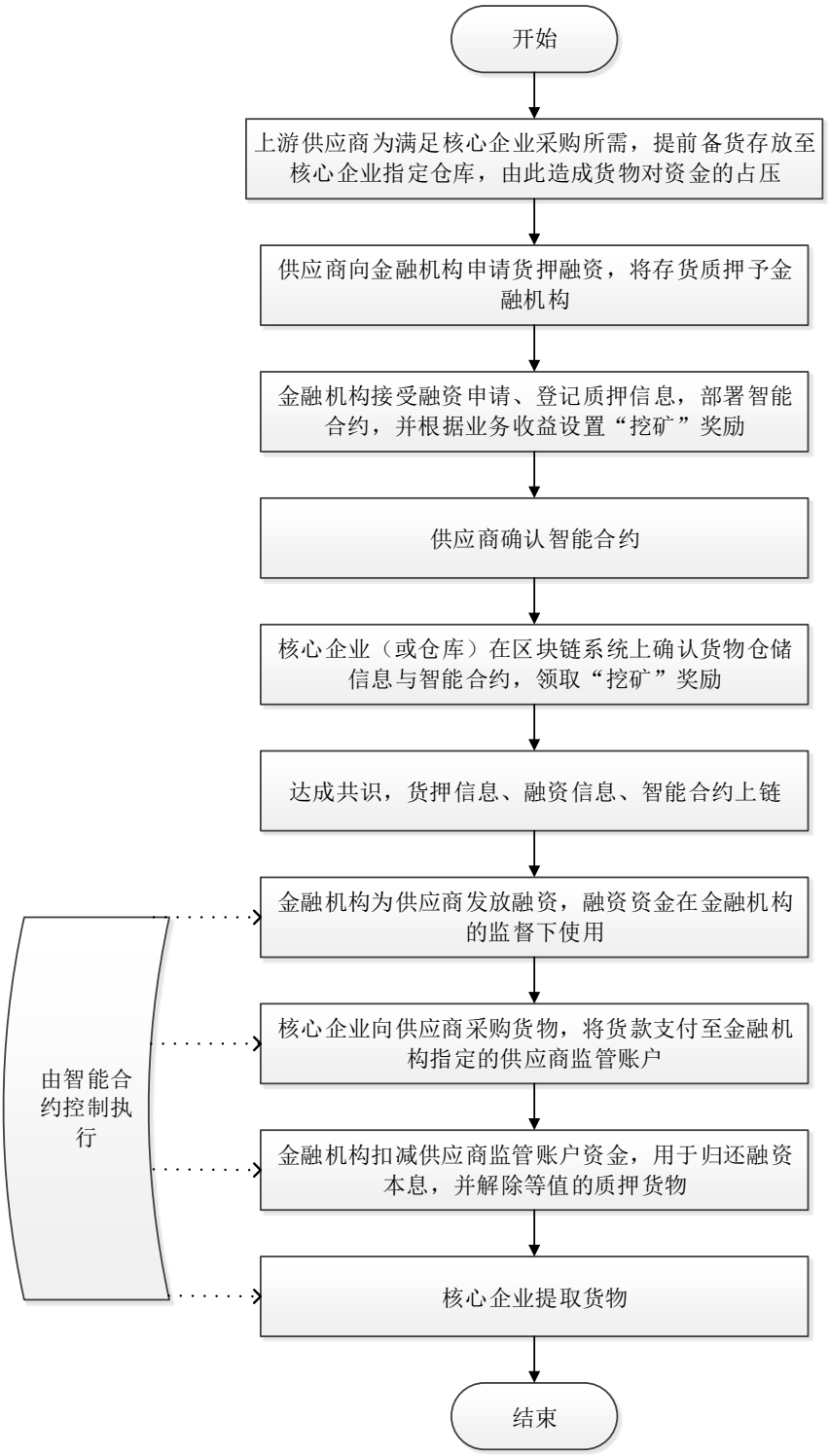


图 4-14　货押融资流程图

（3）保理融资

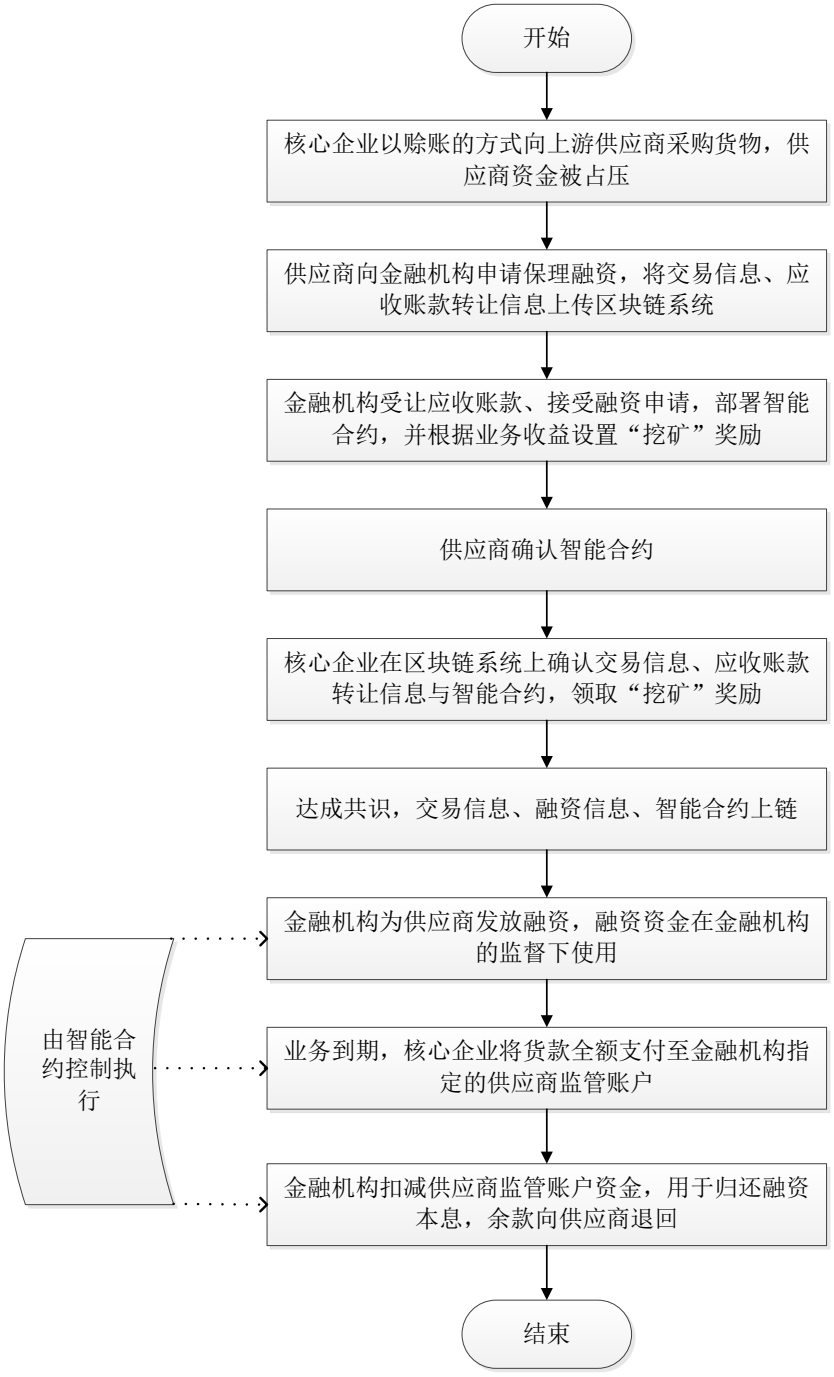


图 4-15 保理融资流程图

### 4.6.2 资产证券化应用方案

供应链金融旨在解决供应链条上中小微企业的“融资难、融资贵”问题，通过引入核心企业的信用增值，可解决“融资难”问题，而“融

资贵”的问题，则可通过供应链金融资产证券化（ABS）向社会募集低成本的资金进行解决。

供应链金融资产证券化是指以供应链金融资产未来将会产生的现金流（还款来源）为偿付支持，通过银行、券商等机构进行结构化设计及信用增级后，在此基础上发行资产支持证券（ABS），该证券可在市场上进行交易。

资产证券化业务涉及的业务参与方较多，主要有资产方（如网络小贷公司、商业保理公司等）、托管银行、管理人（投资银行）、中介机构（如评级机构、会计师事务所、律师事务所等）、ABS 投资人（如券商、基金、银行、信托等）、交易所等。

在传统的业务模式下，主要存在如下痛点问题：

- 参与方众多，往来对账成本高、时效性差。
- 操作流程复杂，人工操作出错概率高。
- 经过多重包装后，底层资产较难追溯，投资人风险高。
- 一笔交易可能同时对应多笔资产，且每笔资产对应不同的外部担保，目前仍未能真正实现担保随同资产的金融债权转让。

针对上述问题，运通区块链的解决方案如下：

- 使用分布式账本技术，各成员间使用同一的账本，消除调解不同账本的操作成本与时间。
- 利用智能合约取代人为操作，实现款项的自动划拨、资产循环购买和自动收益分配等功能，降低操作风险。
- 区块链自带追溯功能，可实现对底层资产的穿透，提升资产

的透明度，降低投资人的投资风险。

- 同时将资产信息和担保信息写入区块，实现资产与担保的同时转让。

具体业务流程如下：

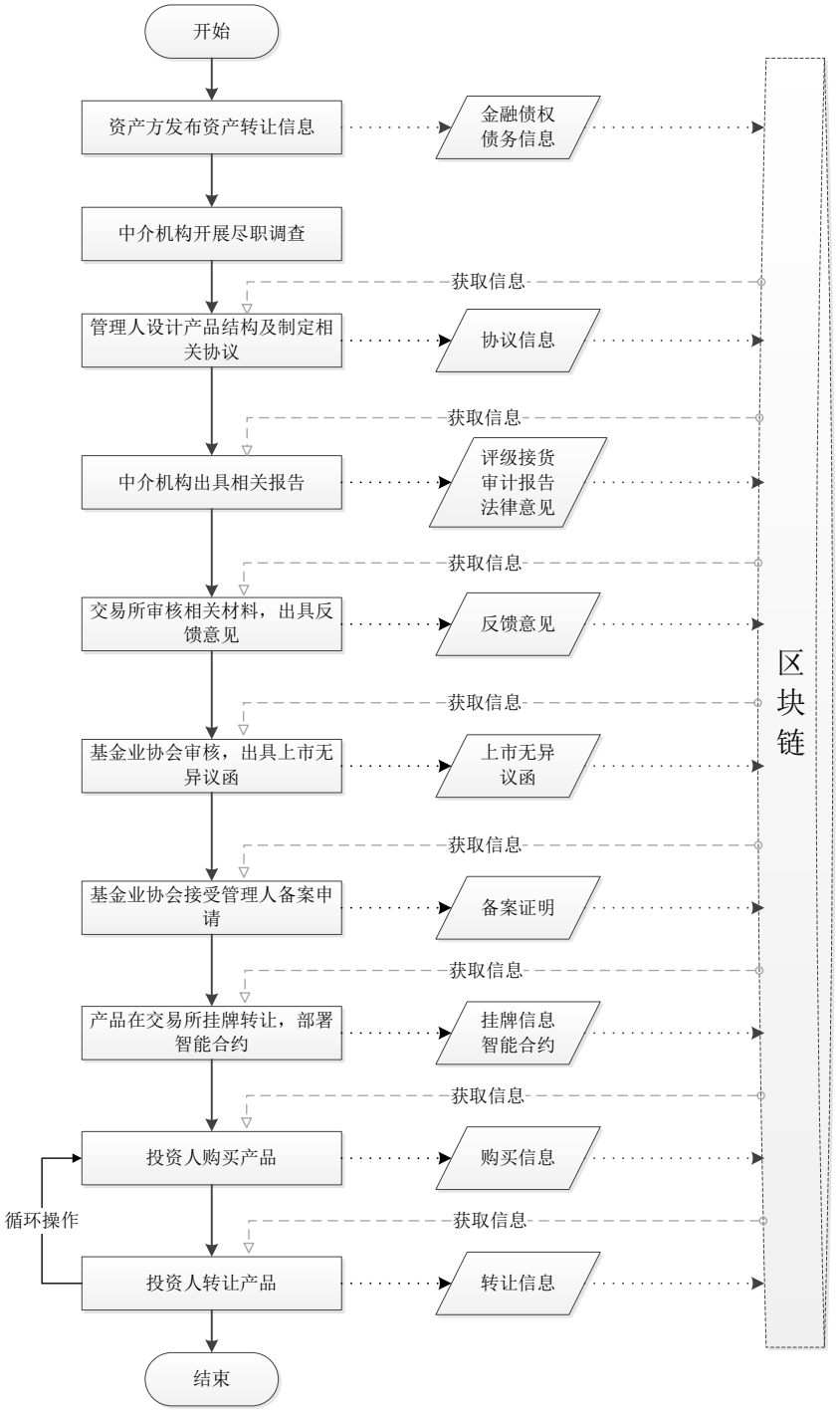


图 4-16　资产证券化业务流程图

# 5 运通区块链未来展望

经过最近几年的技术积累和应用实践，运通区块链坚信利用区块链技术可以解决围绕智能设备的痛点问题。同时，我们注意到区块链技术本身目前仍存在许多挑战，需要我们一步步去攻克技术难题，进而拓展区块链的应用场景，使其成为数字社会的基础设施。今后我们将围绕技术攻坚、行业标准制定、技术普及、智能设备区块链生态体系建设等开展后续工作。

区块链技术作为一项新兴技术，当风行一时的 ICO 被国家明令禁止之后，该技术也引起人们的误解。这类现象主要是目前监管仍存在一定的不明确性以及区块链行业标准仍相对缺失。运通区块链公司将在国家相关政策支持下，积极参与区块链相关行业标准的制定，推动区块链技术走向规范化的发展道路。经过近几年的发展，区块链概念已经被大众所了解，但是区块链底层技术原理及其优势并不被大众所熟悉。运通区块链团队在进行区块链技术攻坚的同时，积极开展区块链相关基础知识普及和技术培训工作，为我国乃至全球的区块链技术推广工作贡献企业力量。

运通区块链已经围绕智能设备链进行了大量的探索，初步实践证明智能设备区块链方案切实可行，但是要完成整个生态的布局及实现，还需要大量的工作，我们将朝着建设智能设备区块链完整的生态方向不断努力。同时，欢迎感兴趣的企业、志同道合的朋友们积极参与到智能设备区块链生态的建设中来，构建一个全新的利国利民的惠民生

态。

我们看到，人类已经步入由人工智能和区块链技术双引擎驱动的数字经济时代，这是一个前所未有的时代，孕育着伟大的变革，将给人类社会的进步和发展带来极大的推动。通过技术重构一个诚信而高效的商业体系和社会体系，让我们的后代生活在一个没有欺诈、智能高效的社会是我们每一位有良知的公民的梦想。而这个诚信体系的构建，将从与智能设备结合的区块链基础平台开始，逐渐形成一个覆盖民生的诚信惠民生态。每一位有幸参与其中的同仁都应该庆幸我们生逢其时，让我们坐言起行，以行动和结果来证明我们不辜负这个伟大的时代。

# 关于我们

广州广电运通区块链科技有限公司，是由全球领先的人工智能设备及系统解决方案提供商-广电运通，联合北京区块链云科技有限公司、绿谷联盟高科技有限公司共同投资成立的高科技公司。

公司在母公司长达 3 年的孕育过程中，参与并承建了“广东省虚拟资产与区块链工程技术研究中心”，助力母公司成为了“广州市区块链产业协会”的首届理事单位、中国区块链技术和产业发展论坛首批成员单位，并与建设银行、广发银行等多家银行成立了金融创新联合实验室；申请了 4 项区块链技术专利和 8 项区块链计算机算著作权；参加“2017 中国金融科技创客大赛”并荣获广州区金奖及全国优胜奖。

运通区块链拥有一支由海外留学背景及丰富工作经验的博士带领的核心研发团队，过半数成员均为博士和硕士。公司领导及主要研发成员均长期从事区块链行业相关的工作，多数骨干具有在银行、国企、大型互联网公司的工作经验。

**广电运通区块链科技有限公司**
地址：广州高新技术产业开发区科学城科林路 9、11 号
邮箱：grgchain-pr@grgbanking.com
网址：www.grgchain.cn

**GRGBanking Blockchain Express Co., Ltd**
Add: 9,11 Kelin Road,Science City, High-tech Industrial Development Zone, Guangzhou, China
E-mail: grgchain-pr@grgbanking.com
Http://www.grgchain.cn

扫一扫
关注运通区块链