

区块链赋能物联网自动化设备可信数据交互机制

王侠

杭州精鼎玻璃制品有限公司，浙江省杭州市，310000；

摘要：在新一轮科技革命的推动下，物联网与自动化设备广泛渗透于工业、医疗、交通等领域，其数据价值日益凸显。然而，物联网系统普遍存在数据可信度不足、交互过程易篡改、设备身份难验证等痛点，制约了其规模化与深层次发展。区块链技术凭借去中心化、不可篡改、可追溯等优势，为构建物联网中自动化设备之间的可信数据交互机制提供了新思路。本文从信任建立、数据共享与隐私保护三个维度出发，深入剖析区块链如何融合物联网体系，探索其在身份认证、智能合约执行和异构设备数据协调中的应用路径，提出一套具备实用性与前瞻性的可信交互机制方案，旨在为建设高效、安全、透明的物联网生态提供理论支持与实践指导。

关键词：区块链；物联网；自动化设备；可信交互；数据安全；智能合约；分布式身份

DOI：10.69979/3029-2727.25.08.030

引言

本文从技术机制与应用场景双重维度，深入探讨区块链如何为物联网自动化设备构建可信数据交互机制，并在实践中解决系统信任缺失、隐私泄露和协议分散等关键问题。

1 构建物联网自动化系统的信任基石：区块链机制解析

1.1 分布式账本重塑数据可信结构

传统物联网系统中的数据流转依赖中心节点进行管理与验证，存在单点故障、高维护成本和中心节点易遭攻击等风险。而区块链以分布式账本为核心，通过共识机制实现多节点协同记账，每一条数据的产生、验证与存储都由网络中多个节点共同完成，从而极大地增强了数据的可信度与容错能力。

在自动化设备协作场景中，设备上报的状态信息、操作日志或任务反馈可以直接写入区块链中。由于区块链的“不可篡改”特性，任何设备篡改历史数据都会立即被其他节点识别并拒绝，显著降低了数据伪造的风险。此外，链上数据具有时间戳和签名验证能力，能够为后续的安全审计和责任追溯提供技术依据。

1.2 智能合约推动设备协作自动执行

智能合约作为区块链上的可编程协议，允许各类设备在满足某些条件时自动触发预定义的操作。在物联网自动化系统中，这意味着设备之间的协作可以无需人工介入，实现逻辑上的自治与执行效率的极大提升。

例如，在智能制造场景中，当一个传感器检测到原材料存量低于阈值时，可以自动触发仓库补货任务，由

机器人系统响应执行，并将整个流程同步记录于区块链中。这种去中介化的逻辑执行不仅降低了运营成本，也提升了系统响应的实时性与可靠性。

1.3 分布式身份系统保障设备接入安全

在物联网中，不同设备类型、供应商和接入方式形成高度异构的网络结构，传统身份验证机制难以统一管理。区块链支持构建基于加密公钥的分布式身份系统（DID），每个设备在注册时可生成唯一身份标识，并与链上数据绑定，杜绝了伪冒和非法接入的可能。

通过结合零知识证明和链上身份记录，自动化设备可以在不泄露具体信息的情况下完成身份验证。这种机制打破了设备与平台之间的信任鸿沟，为跨组织协作提供了根基，有助于实现设备的可信接入与统一管理。

2 区块链支持下的可信数据交互路径设计

2.1 多层数据共享结构提升交互效率

在物联网的环境里，自动化设备常常生成很多高频率的不规整数据，比如图片、声音、记录数据和即时控制命令这些，要是所有这些数据都存到区块链上就会遇到很大的运算困难和链上资源不够的问题。所以搞一个多层的数据共享结构就变成了既有效率又要安全的重要办法。这个结构中，设备这边先把数据传送到本地的边缘计算节点，边缘节点会把数据汇总、降低复杂度和压缩，把重要信息抽出来然后算它们的哈希摘要。然后这些哈希摘要还有部分元数据信息就会被写到区块链上面，实现关键信息上链保存证据；而那些原始数据就存在链下比如本地数据库、自己公司的云或者公私混合云里。链上的数据就负责信任证明和权限管理的事情，

链下的数据可以保持更快处理速度和储存效率。

为了让数据交换的时候隐私和权限管理得到保障，系统里引入了智能合约用来规定数据该怎么访问。把谁能访问、什么时间能访问、用户是谁这些都放进合约里之后，系统就能自动识别哪些访问是合规的然后通过，还能拦住那些没权限的和非法的访问，这样整个系统就更安全更灵活了。所有参与方的数据使用情况也会实时写到区块链里面，这样就形成了完整的数据使用追踪链条，让透明度和责任划分变得更清楚。比如智慧物流、智能安防、工业检测这些需要数据共享又快又可靠的领域，这种主要靠链下配合的模式已经有很多成功案例，既能打破不同平台之间的障碍，又能保证数据可以控制地流转同时系统运行得既高效又稳定。

2.2 信任中继节点实现跨链数据流通

随着物联网发展的越来越广，很多公司和单位都用了自己的私有链、联盟链或者公有链系统，因为这些系统用的加密方式、共识协议这些技术不一样导致不能直接通信。所以不同平台之间协作效率很低，数据孤岛的问题变得越来越严重。这时候就需要信任中继节点这个技术来解决不同链之间的数据不通的问题。这个信任中继节点就像中间人那样，主要负责把数据接收过来、验证真伪、打包后再传出去。这样既不会破坏原来区块链的结构，又可以搞一套标准化的流程，帮助各个链之间更好的传递信息和价值。

中继节点一般都用几个机构联合起来的方式或者很多不同单位一起参与管理的方式，需要多个信任的机构一起来运行和维护，防止被某个单独控制，避免了中心化的危险。在跨链传输信息的时候，中继节点会用多个签名一起认证的方法对要传的数据进行检查，只有当大部分签名都同意的情况下，才会认为这个数据没问题然后传到另一条链上去；同时用了一种叫Merkle树的结构来做数据验证，保证整个数据包都是完整没有改过的，不会出现数据被修改或者有错误的情况。另外还有中继节点可以当监测器和指挥员，和智能合约一起管理不同链上的数据对应、同步和触发操作，这样大大提高了系统之间的协作能力和自动化程度。

在自动化工厂、跨地区的能源调配或者多平台城市基建系统里，这个机制能很好解决不同厂商和平台之间的系统隔阂，让设备就算技术标准不同还可以数据互相连接和共同操作，这样为以后建立全球范围内互相连接的物联网协作网络打下很好基础。

2.3 数据生命周期管理助力可信存证

物联网里数据生命周期管理最主要是要保证数据

从收集到保存整个过程里完整、能被验证和可以查来源，避免各个阶段数据被篡改、丢失或者没有授权的操作。区块链因为它有时间戳和链式结构这些不能被修改的特点，所以在管理数据生命周期方面有先天优势。每个数据产生开始就用哈希算法处理和时间标签记下来发生时间、地点、来源设备这些原始数据，这些信息都被固定在区块里写完就不能改。系统能按照区块链上的记录去查每个数据的历史记录，找到是谁的责任，并对有问题操作追究责任。

具体操作生命周期管理的时候，主要分成五个步骤就是数据生成、验证、传输、使用还有归档。在生成数据这个环节，设备或者传感器先把原始数据存到本地缓存里，然后弄个链上的摘要数据。到了验证数据阶段，这时候系统要通过交叉验证加上智能合约的那些规则，检查数据是不是真实的再看能不能进到共享流程里去。传输数据的过程中，区块链上会随时记录下数据传送、谁访问了、调用了什么这些事，比如访问的人是谁、做了什么操作、具体时间这些，最后组合成完整的审计日志。在使用数据的时候，区块链还能用提前设定好的合约管住数据往哪里流、用来干什么、能用多久这些方面，避免数据被乱用到不该用的地方。最后归档数据的话，区块链上记录的那些数据指针还有谁有权限访问的信息还能一直保存着，这样后面需要审计、再利用或者打官司的时候就有合法证明了。

在金融风控、知识产权保护、高端制造流程管理等这些需要很高数据准确性的场合下，区块链技术的数据生命周期管理可以很大程度提高系统对重要数据的保护能力，成为了建设合规安全又有价值的数字资产体系关键支撑。

3 应用场景探索与未来发展路径

3.1 智能制造场景下的应用示范

在智能制造领域里，自动化生产线变得越来越复杂，各个制造步骤之间非常依赖数据传递得快和反应准确。从设备运行状态的监控、质量检查的记录，到工艺参数的设置和原料来源追踪，每个步骤都会产生很多有用的数据。不过这些数据分布在各种系统里，比如企业自己的ERP、MES、SCADA系统，还要和上下游企业的数据库对接，容易出现数据孤岛、信息传递慢和被篡改的可能。这时候区块链技术用上，就能系统性地解决这些麻烦事情。

通过搭建区块链的系统来记录制造过程中的数据，这样就能对整个生产过程进行可靠记录。把每个关键的操作动作都记录到区块链上，比如设备什么时候启动、

刀具磨损程度、质检的数据参数、操作人员是谁这些，这样就形成了可以验证而且不容易被改动的生产记录。拿汽车零件生产来说的话，每当数控机床调用程序的时候，加工每个零件的参数还有是否合格的结果都能马上记到区块链里，然后把物料上的编号、供应商的信息都通过哈希算法绑定在一起，这样从最开始到最终产品每个环节的数据都能被追踪到。

还有就是区块链加上智能合约一起用，可以让制造过程自己动起来反应。比如说如果哪个机器突然不转了，系统就能从区块链上的数据看出来会影响多大地方，然后自动发通知报障、叫备用机器过来或者重新分配生产线的话。管生产的人只看区块链里的一条数据就能知道全部生产情况，这样企业的反应能更快，维护也有效率，最后做到制造透明化、生产过程让人信得过这样。

3.2 智慧城市设备协同中的价值体现

智慧城市最重要是建立一个用数据推动的高合作性治理系统，包含了交通、安全、能源、环境、医疗等很多方面。城市里智能设备装得到处都是，类型很多样，数据互相传得很快，但是现在系统里设备通常是不同公司产的，各个控制系统彼此缺少信任，很难搞出统一又有效率的合作模式。特别是在重要地方比如城市交通管理、检查公共安全的时候，设备之间不能马上分享可靠的数据，这样会让信息重复太多、反应变慢，甚至出现安全问题。

当区块链技术被用到了智慧城市里，设备身份管理和数据交换的方法就能得到很大改进。每个设备连到城市物联网的时候，首先会生成一个独特的身份标识（DI D），然后在区块链上注册就能获得接入权限，这样就可以防止那些“幽灵设备”和可能的攻击行为。这个身份系统用了加密技术和区块链上的时间记录，既确保每个设备都是唯一的，又能让认证过程变得隐私和安全。

在智慧交通方面，区块链和智能合约技术能够用来建立不需要中心控制的信号灯网络。各个路口的红绿灯通过自身传感器收集车流量和行人多少的数据，然后通过区块链的共识方法将这些信息传到整个城市的交通管理中心，这样就生成了即时全面的道路情况图。这个系统依靠区块链上的规则可以自己改变红绿灯时间、重新规划导航路线，这样就不会出现中心服务器的卡顿问题，让调度更灵活。如果有车祸发生时候，涉及的汽车、监控设备和调度信息都会被记录在区块链上，这样能给后面查事故原因、判断谁的责任还有评估城市管理质量给出证据支持。

3.3 面向未来的技术融合发展趋势

虽然区块链技术物联网自动化设备应用方面虽然有很多可能性，但在实际使用中还是存在技术上的一些问题。比如现在主流的公共链处理交易的能力根本不够工业物联网的频繁的数据交换需要，而且储存数据在链上价格贵，反应速度慢，还有共识方式消耗资源太多这些因素都限制住了区块链技术在很多设备一起协作的场景里的应用拓展。所以接下来区块链技术肯定需要和更多高科技结合起来，这样才能建立更加聪明、灵活还能扩容的‘区块链+’物联网系统。

首先和边缘计算结合可以很大程度提高响应速度还有减少网络的负担。因为物联网里的计算任务不需要都传到云端，而是在边缘设备那里先处理下，然后把关键数据存到区块链里，这样就能做到计算在前面处理，记录在链上保存，变成一个有效的方法。这种结构可以用在比如工业设备故障检查、环境监测预警这些需要很快反应的情况

第二点，智能合约里面加入人工智能算法的话，可以让规则建模和决策优化变得更加复杂。AI 算法不但可以发现行为模式和数据里有异常情况，还能让合约逻辑动态变得更优，这样自动化水平就提高了。比如在城市节能的系统里面，AI 合约会根据历史用电量和天气预报的模型，来调整建筑物的用电方法，既保证人们舒服的条件下又能减少资源被浪费掉。所以说未来区块链加物联网的结构会从单一技术转向多方面的系统结合，在安全和可信赖前提下做到智能自动、灵活配合以及生态互相连接，这样就能带领新数字基础建设的路线方向。

4 结语

区块链技术作为重构信任机制的关键创新，为物联网自动化设备之间构建安全、高效、透明的交互环境提供了有力支撑。通过分布式账本、智能合约与分布式身份系统的综合运用，不仅解决了设备身份不明、数据易篡改等痛点，还极大拓展了物联网的跨平台协作能力与行业适应力。面向未来，区块链与其他新兴技术的融合将持续推动物联网系统从连接走向智能、从数据走向价值，为万物互联的智能时代奠定坚实基础。

参考文献

- [1] 张涵, 么新鹏, 范颂, 等. 基于深度学习与区块链的物联网入侵检测[J]. 信息技术, 2025, (05): 122-129.
- [2] 赵小虎, 刘析琳, 王越. 区块链赋能的可信云计算资源分配方法[J]. 计算机工程与设计, 2025, 46(05): 1318-1326.
- [3] 王昌文. 区块链技术重塑数据安全新防线[N]. 中国改革报, 2025-04-20(004).