基于区块链的工业互联网安全防护研究与实践

陈惠玲
公诚管理咨询有限公司　广东广州　510610

摘　要：在数字化时代的发展中，工业互联网已成为新一代信息技术与工业制造领域融合的典范，更是引领工业变革与升级的动力。但随着其快速演进的步伐，工业互联网面临的数据安全挑战越来越严峻，传统安全防护体系的局限性愈发明显。在这个背景下，基于区块链技术的工业互联网安全防护的方案应运而生，并成为工业信息安全领域的焦点。区块链技术以其去中心化、数据防篡改等优势，为工业互联网建立一道更坚固的安全屏障，确保工业数据的保密性、真实性、持久性，为工业互联网的稳定、长远发展保驾护航。

关键词：区块链；工业互联网；安全防护

引言

工业互联网平台以独特的特性，成为安全风险的高发地。该平台的安全防护体系直接关系到工业生产的稳定运行，更影响企业信息的保密、经济发展的动力，甚至触及社会稳定的根基与国家安全的屏障。安全防护保障不是单个环节，单一层面上问题的解决，必须是全方位地、多层次地从技术、管理等方面进行全面的安全设计和建设，因此，我们需要从它的应用特点和防护策略展开研究与实践。

1. 区块链技术在物联网安全防护工作中的应用特点

1.1 去信任化：重构物联网设备间的可信协作机制

区块链的“去信任化”并非完全消除信任，而是通过技术手段将传统中心化信任转化为系统内生信任。在物联网环境中，数以亿计的智能设备需要实时交互（例如工业传感器群、智能家居设备群），传统依赖中心服务器认证的模式存在单点故障风险。区块链通过三个核心设计解决这一问题：

1）分布式信任锚点：所有设备共享同一份加密账本，每笔数据变更需经过 PoW/PoS 等共识机制验证（例如某工厂的温度传感器数据上链需获得半数以上节点确认），避免单设备作恶；

2）密码学护城河：结合非对称加密与哈希算法，既保障设备身份真实性（每个智能电表拥有唯一数字身份证），又确保数据历史不可篡改（如篡改某次水质监测记录将导致哈希值连锁失效）；

3）智能合约仲裁者：预设规则自动执行（例如当车载传感器检测到异常震动时，区块链自动触发保险理赔流程），消除人工干预引发的信任争议。

1.2 去中心化：构建物联网安全的韧性防线

物联网的传统中心化架构如同“将所有鸡蛋放在一个篮子里”——云端服务器一旦被攻破，数十亿设备将面临集体沦陷风险。区块链通过三层分布式设计重塑安全范式：

1）数据存储去中心化：将设备数据分散存储在边缘节点（如智能工厂的每台机床既是数据生产者也是存储节点），攻击者需同时攻破 51% 节点才能篡改数据，防护成本呈指数级上升；

2）传输链路动态化：采用 DAG（有向无环图）结构替代传统链式结构，实现多路径并发传输（例如自动驾驶车队信息可同时通过 5G 基站、路侧单元、邻近车辆三条链路验证），即使局部节点失效仍能保障系统鲁棒性；

3）身份认证网格化：通过轻量级 Merkle 树验证协议，让每个智能电表都可作为临时认证节点（某智慧城市项目借此将路灯系统的非法接入识别率提升至 99.6%）。

典型案例是德国某汽车制造商建立的去中心化车联网：车辆数据不再上传至总部服务器，而是通过区块链在区域节点间同步。当黑客试图伪造某辆车的刹车信号时，系统会立即与周边 200 米内车辆数据进行交叉验证，攻击行为在 0.3 秒内被识别隔离。这种架构使系统防御从“城堡模式”转变为“蜂群模式”，大幅提升物联网系统的抗毁伤能力。

区块链技术的去中心化应用优势，可以最大化提升数据的安全传输效率和响应速度，通过摆脱传统中心化结构的数据存储方式，物联网系统中的数据具备多重安全保障，不

再依赖于单一的节点进行安全传输与存储[1]，如下图。

图 1 多项节点传输

区块链技术的实际应用，助力物联网安全防护人员科学规避中心化节点带来的潜在风险，更确保各个节点能高效履行自身的信息安全传递职责，如，身份验证和不同节点之间的高效同传，更为物联网系统的整体安全性能提升注入强大的动力和支持。

2. 基于区块链技术的工业互联网安全防护策略

2.1 密码技术革新：构筑去中心化安全基石

密码技术始终是信息安全领域的基础，能确保数据的私密性、完整性、真实性。但在工业互联网这一复杂的环境中，传统的安全防护措施因其固有的限制，如，防护目标的专一性和参与角色的局限性，很难应对逐渐增长的安全挑战。因此，要建立一套全新的密码技术体系，来应对这些挑战。首先，实现管理的简化和高效化，通过转变传统的证书管理方式，采用无证书的理念，大幅度减少管理的复杂性，并提升整个系统的安全性和运行效率。由于工业互联网中大数据的存储和查询需求逐渐凸显，新体系必须支持去中心化的数据查询制度，也就是即使在没有中心节点的情况下，也能迅速检索和处理数据，来有效应对大数据时代的各种挑战[2]。另外，优化通信性能，通过降低通信宽带的需求并减少数据传输的延迟，提升实时通信的效率，为工业互联网中的各种应用提供更顺利的用户体验。

为应对这些挑战，基于区块链的新一代密码技术体系需实现以下突破：

1）无证书化身份管理：采用基于区块链的“去中心化标识（DID）”技术，设备可通过生成唯一加密密钥对自主管理身份，无需第三方认证机构介入，大幅降低管理复杂度。

2）轻量化加密算法：针对物联网终端的低算力特点，设计适配的轻量级密码协议（如国密 SM9），在确保安全性的同时降低通信带宽占用，实现毫秒级加密响应。

3）跨域认证协同：通过区块链构建分布式信任网络，不同安全域的设备可基于智能合约自动验证彼此身份。比如某工厂的传感器数据需与物流公司共享时，双方可以直接调用链上合约来完成密钥协商，从而打破信息孤岛。

2.2 经济安全治理：区块链重塑工业互联网金融生态

根据麦肯锡预测，2025 年全球物联网经济规模将达 11 万亿美元，设备数量突破 750 亿台。这一指数级增长背后，传统的集中式数据管理暴露出两大隐患：中心化金融风险，如支付平台一旦被攻击，可能导致数亿用户交易中断；数据垄断与滥用，平台方可能利用用户行为数据牟利，侵犯隐私权。

区块链技术通过三大机制重构物联网经济安全框架：

1）分布式账本透明化：所有交易记录由全网节点共同维护，例如智能电表可将用电数据实时上链，供电力公司与用户交叉核验，杜绝“数据黑箱”问题。

2）智能合约自动化执行：在供应链金融中，货物抵达指定位置后，区块链自动触发货款结算，减少人工干预导致的履约纠纷。

3）通证激励合规性：通过发行合规数字通证（如央行数字货币 CBDC），物联网设备可自主完成小额支付。例如，电动汽车在充电桩充电后，通过链上通证自动扣费，全程无需银行介入。

区块链技术的融合应用，能大幅度提升物联网金融的运行效率，更能彻底打破传统信息集中处理模式的束缚，为用户提供更稳定、安全的金融交易环境，如下图。

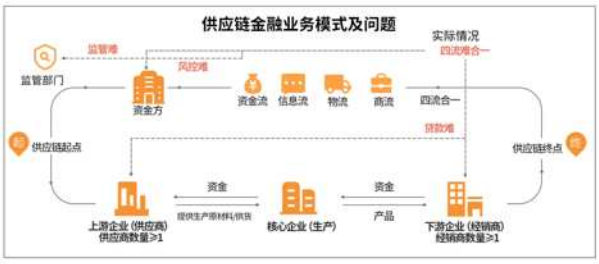

图 2 供应链金融业务应用模式

现有的实践案例有：蚂蚁链的“物联网 + 区块链”金融方案已应用于 30 万物流车辆，实现每秒处理 10 万笔交易，错误率低于 0.001%。

2.3 数据完整性保护：哈希链构建防篡改屏障

工业互联网中，传感器数据若被恶意篡改，可能导致设备误判甚至引发安全事故。区块链技术通过哈希链式存储与共识验证双重机制，可为数据完整性提供三重防护：

1）结构防篡改：每个数据块包含前序区块的哈希值（类似 DNA 链式结构），任何数据修改都会导致后续哈希值失配；

2）多节点存证：数据同步存储于全球数万个节点，攻击者需同时修改超 51% 节点才能篡改记录，理论成本高达数十亿美元（以比特币网络为例）；

3）时间戳溯源：区块生成时间被精准记录，可追踪数据操作全生命周期。

该制度则赋予区块链在数据真实性和完整性保护方面的卓越能力，能迅速识别出任何对数据的非法修改，且从源头上防止数据的恶意篡改或破坏 [3]。

在现实的应用场景，如某航空发动机厂商将 2000 个传感器的实时监测数据上链，利用智能合约设定阈值告警。当某节点数据异常时，系统 3 秒内定位故障点，较传统方式提速 90%。

2.4 跨域通信安全：分布式信任打破协作壁垒

工业互联网经常涉及跨企业、跨行业的数据交换，传统中心化通信通常面临两大痛点：信任建立成本较高，不同主体之间需要反复验证对方资质；传输链路脆弱，中心服务器一旦宕机，全域通信就会中断从而发生“事故”。

区块链的去中心化通信架构通过以下方式提升安全性：

1）端到端加密直连：设备间基于区块链身份直接通信，数据经加密后点对点传输，避免经第三方服务器转存。例如，医疗设备可通过私有链共享患者数据，医院无需依赖云服务商。

2）智能合约规则约束：在车联网中，车辆与交通信号灯的交互规则被写入链上合约。如果交通信号灯发送错误指令，合约将自动拒绝执行并触发警报。

3）抗 DDoS 攻击韧性：分布式节点设计使得攻击者难以定位单一目标。实测显示，基于区块链的通信网络遭受 DDoS 攻击时，服务恢复时间缩短至传统系统的 1/5）。

在技术前瞻性方面，华为的案例可以充分体现，其提出的“区块链切片”方案，将跨域通信网络划分为多个安全子链，既能隔离风险，又可实现子链间可信交互，目前已在 5G 基站协同管理中试点应用。

3. 结束语

工业互联网的蓬勃发展正推动社会进入万物互联时代，而安全威胁的复杂化要求防护策略从“被动防御”转向“主动免疫”。因此，更需要迫切研究区块链技术的安全防护策略，可通过密码技术革新、经济模型重构、数据完整性保障与跨域信任建立，为工业互联网构建起多层安全护盾。未来，随着零知识证明、同态加密等技术与区块链的深度融合，工业互联网安全将迈入“可验证、可自愈”的新阶段，为数字中国建设筑牢技术基座。

参考文献：

[1] 马娟 , 等 . 工业互联网设备的网络安全管理与防护研究 [J]. 中国工程科学 ,2021,23(02):81–87.

[2] 白宇 . 基于区块链技术的工业互联网安全防护效果研究 [J]. 自动化应用 ,2023,64(16):231–234.

[3] 马刚 . 基于区块链技术的工业数据安全防护的研究 [J]. 网络安全技术与应用 ,2022(05):76–78.

作者简介：

陈惠玲（1982—），女，广东汕头人，本科学士，工程师，现就职于公诚管理咨询有限公司，任信息系统项目管理师、行业主管、一级专家，从事通信建设及信息化项目管理相关工作 16 年；主要研究方向为通信工程建设、信息系统项目管理。