

# 基于区块链与 RISC-V 实现物联网数据互联

郝向宇<sup>1</sup>, 柳耀勇<sup>1</sup>, 肖青<sup>1</sup>, 习熹<sup>1</sup>, 任晓明<sup>2</sup>

(1.芯昇科技有限公司, 江苏南京 210018; 2.中国移动研究院, 北京 100053)

**摘要:** 针对物联网特点与痛点, 提出以区块链技术为核心、结合物联网技术并运用 RISC-V 架构实现区块链功能下沉至终端。通过芯片承载区块链的功能使得每一个终端成为区块链的节点, 基于区块链的分布式这一特点, 满足物联网终端节点功用。通过芯片从源头解决上链数据的可信, 针对现有的区块链功能进行轻量化改造, 使其符合芯片的硬件特性。通过 RISC-V 的模块化、高性能、可自定义的指令集实现芯片对于区块链功能的承载。经过合理的分析与例证, 能够利用终端作为区块链节点的方式去解决物联网多样化的应用场景, 满足安全可信的同时提高性能, 降低成本。

**关键词:** 区块链; RISC-V; 物联网; 功能下沉

中图分类号: TN919; TP302.1

文献标识码: A

DOI: 10.16157/j.issn.0258-7998.212091

中文引用格式: 郝向宇, 柳耀勇, 肖青, 等. 基于区块链与 RISC-V 实现物联网数据互联[J]. 电子技术应用, 2022, 48(9): 114–118.

英文引用格式: Hao Xianyu, Liu Yaoyong, Xiao Qing, et al. Achieve IoT data interconnection based on blockchain and RISC-V[J]. Application of Electronic Technique, 2022, 48(9): 114–118.

## Achieve IoT data interconnection based on blockchain and RISC-V

Hao Xianyu<sup>1</sup>, Liu Yaoyong<sup>1</sup>, Xiao Qing<sup>1</sup>, Xi Xi<sup>1</sup>, Ren Xiaoming<sup>2</sup>

(1.Xinsheng Technology Company Limited, Nanjing 210018, China;

2.China Mobile Communications Research Institute, Beijing 100053, China)

**Abstract:** Aiming at the characteristics and pain points of the Internet of Things, it is proposed to take the blockchain technology as the core, combine the Internet of Things technology and use the RISC-V architecture to realize the sinking of the blockchain function to the terminal. The function of carrying the blockchain through the chip makes each terminal become a node of the blockchain, and the distributed characteristics of the blockchain are used to meet the terminal node functions of the Internet of Things. The chip is used to solve the credibility of the data on the chain from the source, and the existing blockchain functions are light-weighted to make it conform to the hardware characteristics of the chip. Through RISC-V's modular, high-performance, and customizable instruction set, the chip carries the blockchain function. After reasonable analysis and examples, the terminal can be used as a blockchain node to solve the diversified application scenarios of the Internet of Things, which can improve performance and reduce costs while satisfying security and credibility.

**Key words:** blockchain; RISC-V; Internet of Things; function sinking

## 0 引言

根据统计和预测, 2020 年全年中国物联网连接数量达到 40 亿, 到 2025 年将增长至 80.1 亿次, 5 年增长 2 倍左右。全球物联网市场支出将从 2020 年 7 420 亿美元增长至 2024 年的 1.138 万亿美元, 复合年均增长率为 11.3%<sup>[1]</sup>。大量的连接数意味着数据价值作用凸显, 我国推动数字经济发展的一个关键方式是合理利用价值化数据, 加快推进数据价值化进程是发展数字经济的本质要求<sup>[2]</sup>。但数据要素的价值实现依赖于对数据资源的深度整合开发和利用, 而“数据孤岛”妨碍了数据的整合、共享与互通。

为了解决“数据孤岛”的问题, 推动数据的整合共享与利用, 推进数字经济发展, 国内诸多专家进行了多方的研究与探索<sup>[3-7]</sup>。然而, 研究方向集中在大数据应用、数据挖掘、数据可视化等显性方面, 而从数据源头出发进行物与物的数据共享互联有助于实现真正的物联网终端应用场景。

物联网的蓬勃发展带来了终端的多样性, 这也造成物联网应用的碎片化, 碎片化的应用恰恰与区块链的去中心化思想一致, 利用区块链能够满足物联网碎片化应用的需求。终端与数据作为物联网的两大基石, 通过数据与数据的交换能够产生数据的价值, 终端与数据的安

全、可靠、可信是靠芯片发挥关键的作用。芯片与区块链的结合，能够从数据源头构建更安全可信的物联网。芯片自主安全的目标需要开源的 RISC-V 内核，其在性能、DSP 指令、缓存配置、算法执行性能上能够满足区块链应用的要求，进而通过区块链与 RISC-V 实现数据价值的作用，推动数字经济的发展。

## 1 区块链技术与 RISC-V

## 1.1 区块链技术

区块链是新一代信息技术的重要组成部分，是分布式网络、加密技术、智能合约等多种技术集成的新型数据库软件，通过数据透明、不易篡改、可追溯，有望解决网络空间的信任和安全问题，推动互联网从传递信息向传递价值变革，重构信息产业体系<sup>[8]</sup>。

区块链是一种链式结构，由每个区块连接而成，如图 1 所示，每个区块包含区块头和区块体，区块头中的 Hash 参数为前一区块哈希，该哈希参数使得各个区块首尾相连形成链状结构。所有的链上信息都包含在区块体中。若中间某区块中交易信息被修改，则其后所有区块头的 Hash 都需要修改，因此链块式数据结构会使块数据难以篡改。

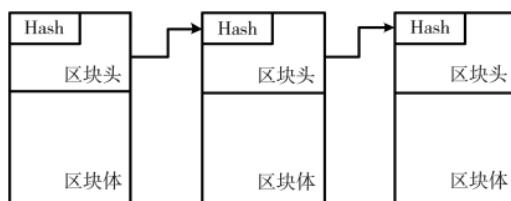


图 1 区块链链式结构

## 1.2 RISC-V

RISC-V 是由加州大学伯克利分校(UCB)提出的一种开源精简指令集架构<sup>[9]</sup>，作为一个新生的开源指令集架构，它具有精简、模块化设计、开源等优点，可以根据需求定制自定义 customer 指令<sup>[10]</sup>，大大简化了处理器的设计，也因此涌现了很多优秀的开源设计。RISC-V 的与众不同之处在于它的模块化，它的核心是以 RV32I 的基础 ISA，模块化来源于可选的标准扩展，根据应用程序的需要，硬件可以包含或不包含扩展<sup>[11]</sup>。这种特性使得 RISC-V 具备了袖珍化、低功耗的特点，对于嵌入式应用至关重要。对于物联网的作用非比寻常，使得 RISC-V 为物联网带来显著的灵活性和成本优势<sup>[12]</sup>。

2 区块链赋能物联网

## 2.1 区块链融入物联网架构

在现有的物联网架构体系中，“云管端”是广泛被认可的架构。“云”指的是云计算，通过引入云计算构建标准化和开放性的综合平台；“管”指的是信息传送通道，是真正意义上的多网融合；“端”指的是与管道连接的终端设备，作为服务载体覆盖最终客户<sup>[13]</sup>。

区块链的加入使得传统的物联网架构“云管端”变成“云链管端”，如图 2 所示。区块链技术实现云上数据可信存储、可信交互、可信计算。通过可信的方式帮助企业实现数据的价值，有利于数据交易、金融监管的参与，同时通过确保数据的可信，解决企业数据共享与控制的矛盾，构建对等、统一的多边协作生态。

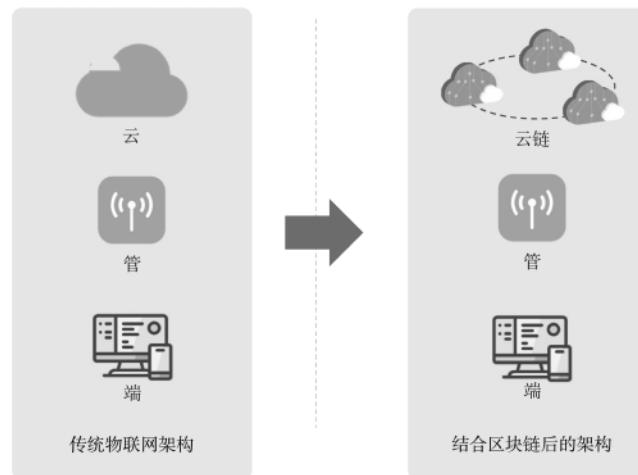


图 2 结合区块链技术后的物联网架构

区块链功能融入至物联网形成区块链物联网能力，如图 3 所示。

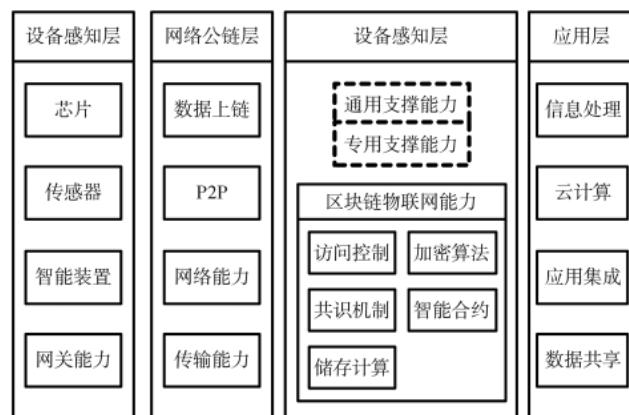


图 3 区块链物联网融合架构图

在此架构下现阶段区块链技术存在 3 个痛点：

(1) 区块链解决了链上数据的可信，没有解决终端测数据可信的问题。数据产生、数据分发、数据使用的闭环暂未形成，在数据产生的阶段需要带有区块链的功能。

(2)数量级不足,区块链相比于物联网,区块链服务器的数量远不及终端的数量,若要匹配相应的能力,需要大量服务器,成本较高。

(3) 区块链没有有效地与终端结合,终端的多样性使得物联网应用场景是非常复杂的,区块链目前难以支撑多样化的场景。

## 2.2 区块链功能下沉

基于上述痛点问题需要将区块链功能下沉,通过区块链、数据、芯片三者结合的方式(即区块链芯片)解决痛点。区块链芯片承载区块链功能提供数据价值服务,嵌入芯片的终端作为区块链节点,简化流程,提高效率,芯片保证上链数据的可信。

众所周知,区块链是相对复杂的流程,对于服务器的性能也有较高的要求。物联网终端的芯片具有物联网的低功耗、轻量化的特点,其算力与性能较低,存储空间较小。若作为区块链节点承担区块链的能力就需要对区块链的核心功能针对物联网场景进行轻量优化。优化方式如下:

(1) 区块链业务流程针对物联网场景进行简化,优化掉不必要的流程。例如通过优化智能合约的方式来降低其部署和执行带来的消耗。

(2) 物联网终端在业务中通常上传数据频次很低,例如智能燃气表每天上报数据次数在个位数,不需要高的TPS(系统吞吐量,即每秒系统处理的数量)。因此针对物联网场景,不需要在TPS上增加成本,弱化对于高TPS的追求,注重可信和安全问题。

(3) 对区块链数据结构进行优化,简化数据结构。保留与认证和溯源有关的必须字段,删除共识算法非必要字段。比特币结构相比于Fabric与以太坊在结构上更加精简,这里以比特币区块数据结构为例,由于物联网业务无需采用工作量证明这种共识算法,可以对其有关字段进行删除,对数据结构进行简化,如图4所示。

(4) 区块链储存的区块设计相应的规则能够定期删除,保证区块的大小不占用太大空间,满足芯片存储空间的能力。同时为了保证数据可溯源,将删除的区块备份至服务器中。

判断连续分布的区块是否满足预设的删除条件,将满足预设条件的区块生成新的区块,删除满足条件的区块,将生成的功能区块加入链中,形成优化后的链,如图5所示。

## 2.3 终端作为区块链节点

根据上述区块链功能优化后下沉到终端侧,终端具

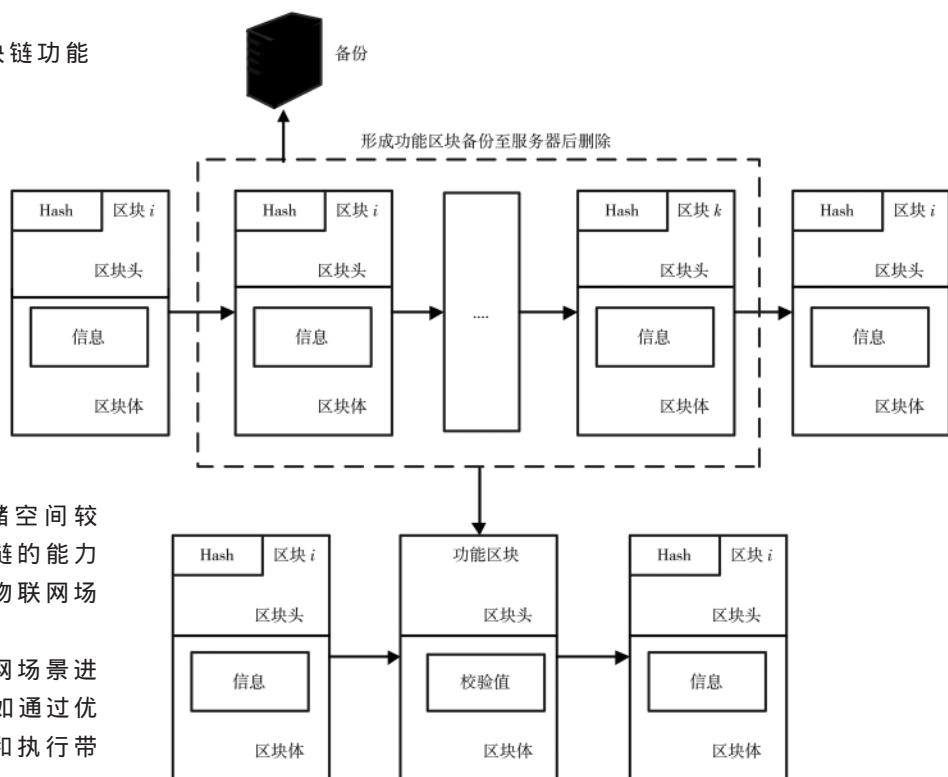


图5 区块根据预设规则定期删除

备区块链能力,能够作为区块链节点。其逻辑架构如图6所示。

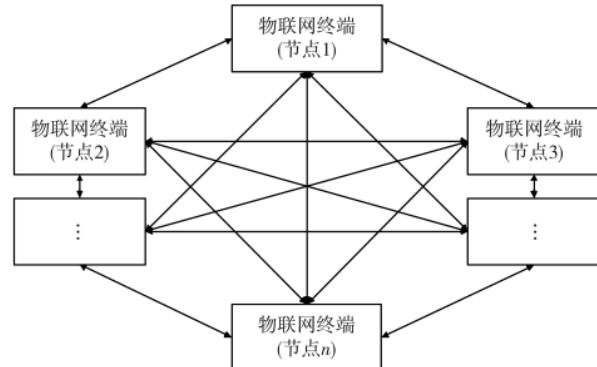


图6 终端作为区块链节点架构图

通过芯片的区块链功能实现去中心化,终端成为节点,在物联网实现公有链终端接入的理想应用效果。下沉到芯片层面更有利于更广泛的推广。在这个架构中区块链的节点不再是单一的服务器,终端成为轻量级的带有区块链功能的节点,提高物与物的联结效率。通过丰富的终端节点支撑物联网复杂、多样化的应用场景。

## 3 RISC-V 对区块链与物联网的作用

### 3.1 区块链功能对于终端芯片提出的要求

在此架构下,区块链功能与特点对终端芯片提出了较高的要求,区块链的能力由芯片实现。

终端作为区块链节点,需要端侧负责数据的发起或响应。在数据层面需要数据文件进行存储;在网络层面需要支持P2P组网,支持跨节点命令调用与多节点数据同步;在共识层面需支持防“崩溃失效”的共识算法;在合约层需支持至少一种编程语言的智能合约,支持容器技术;在安全层面支持多种数字密码技术,如Hash运算、数字签名、Merkle树、商用密码算法、Key-Value数据库,能够对数据进行加密解密,验证其合法性。综上,区块链功能的实现对于终端芯片的计算能力、存储功能以及安全性具有较高的要求。

### 3.2 RISC-V架构助力区块链功能在芯片侧实现

对于上述要求,RISC-V通过高性能、自定义指令集的优势能够更加容易承载区块链的能力。还有强大的芯片架构优势,利用开源特别的安全设计,将安全的源头抓在芯片中。具体表现在:

#### (1)极简、模块化

RISC-V具有极简、模块化、可拓展的特点,物联网侧芯片具有个性化和差异化的特性,其对功耗要求较低,面积较小。这使得针对区块链功能的定制成为了可能。

#### (2)可扩展性

物联网碎片化的场景应用使得对于芯片的功能丰富度有较高的需求。RISC-V的可扩展性能够满足碎片化场景对芯片功能的丰富度要求,具有很高的发展潜力。

#### (3)安全系数高

RISC-V中开源的RTL代码以及无预测性内存访问使得芯片安全系数提高,保证安全性能。

#### (4)硬件性能优秀

RISC-V模块化的ISA(指令集架构)来源于可选的扩展,根据应用程序需要让硬件包含扩展。编译器在得知扩展后可以生成硬件条件下最佳代码,使得代码读写容易,不增加硬件开销。通过简单又具有影响力的机制,降低成本,提高性能。

#### (5)适用于物联网

新兴领域会有一席之地。特别在物联网范畴,目前ARM具有较高的市场占有率,应用开源的RISC-V能够对ARM起到代替作用,能够保证自主安全,解决芯片“卡脖子”的问题。

上述的几个特点保证了芯片性能、储存能力、安全以及稳定性,进而能够使芯片满足轻量化区块链功能的实现。

## 4 应用预测

芯片承载区块链功能使得终端成为区块链节点进而实现物与物的数据交互,提升效率,扩大区块链应用范围,实现“万物互联”,在应用层面能够实现技术的突破。

### 4.1 车路协同

车路协同的目标是实现车与车、车与路、车与人动态的全方位的实时信息交互,通过无线通信技术与物联

网技术来统筹实现车辆有序安全控制与道路协同联动控制,从而实现车路人三者合理协同,保障交通安全的同时提高通行效率,形成和谐、安全、高效的道路交通体系<sup>[14]</sup>。通过终端芯片算力、通信技术以及区块链功能保证车与路之间高效及时的协同,具体表现在:

#### (1)实时加入无需注册

车是移动的,路是固定的,车与路的协同若需要认证注册,效率则会低下。当车作为终端节点加入到链中时,利用区块链的特性无须联网即可成为用户。通过芯片内置非对称的公钥与私钥,将公钥公开至互联网,汽车进行连接时,其他用户只需通过公钥索引便能够建立连接,通过合理的共识与智能合约实现通信。类似于公有链,能够自由加入与退出,参与链上的数据读写。

#### (2)打破传统安全透明

传统的账户与密码是在用户名与密码匹配验证成功后才能开始对话。车路协同系统包含了大量的数据,随着汽车的不断加入,数据生态会越来越大。芯片与区块链先连接再认证,为车路联网带来可信不可篡改的同时保证透明度与真实性、车主的合法身份、汽车行驶数据与人的行为安全。

#### (3)无需网络即可使用

现代非蜂窝连接技术的发展通过区块链的方式能够让用户通过蓝牙、Wi-Fi等方式实现车路协同连接。利用终端作为节点入链使得即时通信无须注册即可加入,无法篡改截获信息,能够使每一辆车先连接再认证,不需要通过蜂窝网络连接即可实现。这就使得车路协同早日实现得到了充分的技术保证。

## 4.2 机器物与物的联动

目前现有场景中物与物联动模型设备之间的连接与通信是通过中心化的网络和通信代理得以实现的。在物联网场景中,终端类型复杂且数量庞大,这极大增加了组网与运维成本,同时可扩展性、可维护性和稳定性也相对较低。在终端(物)承载区块链功能后,将芯片自身的计算和存储能力通过节点扩散到物联网各个环节中。通过P2P组网技术与混合通信协议处理设备间的通信,有效解决单一节点崩溃失效殃及整个网络的问题。

特别在工业场景中,机器与机器之间的联动,相比于传统的中心化控制方式,通过区块链的分布式协作与RISC-V高效处理能力能够更高效地完成任务且具有更高的宽容度与宽泛的感知范围,如图7所示。

区块链的安全特性保证了机器间交互与通信安全,去中心化的分布方式保证了其独立性,远离第三方的干预。合理的共识算法与智能合约保证机器与机器间能够协同工作,快速解决分歧。通过Pegged Sidechain(楔式侧链技术)提供在层次结构中加入不同行为块的可能<sup>[15-16]</sup>,进而可以使得同一机器根据不同预定义的行为参数进行转换,完成不同的操作行为。通过该方式

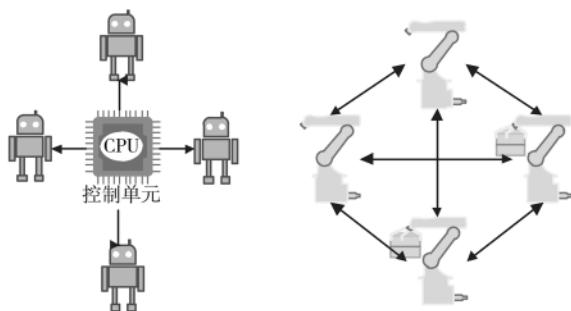


图 7 物与物的中心化控制与分布式协作

能够显著降低成本的同时提高生产效率。

## 5 结论

本文针对当前物联网架构及特点进行分析,当前物联网发展及终端的多样性与区块链的功能特性一致,区块链的功能能够解决当前存在于物联网的一系列问题,物联网传统“云管端”架构变为“云链管端”,总结出现阶段区块链还存在端侧数据不可信、区块链服务器相比于物联网设备数量不足、没有与终端有效结合的问题。提出区块链功能下沉到端侧即芯片中的设想,通过对区块链功能的轻量化设计,使得芯片具备区块链功能,使得终端能够作为区块链节点提高物与物的联结效率。RISC-V在芯片承载区块链功能上发挥了举足轻重的作用,区块链功能要求芯片具备必要的性能。RISC-V的高性能、自定义指令集、模块化、高安全系数、适用于物联网的优势使得区块链功能下沉到端侧能够得以实现。最后展望了能够通过该方案实现具体的应用场景,该方式是对区块链在物联网应用的补充而不是替代,相比于服务器终端的性能依然存在较大的差距。因此,也揭示了未来准备进一步研究的方向。

## 参考文献

- [1] 中国信息通信研究院.物联网白皮书[Z].2020.
- [2] 吴志刚.数据驱动是数字经济发展的本质[J].网络安全和信息化,2020(6):36–39.
- [3] 唐升卫,曾梦迪,顾博川,等.电网智能调度中的大数据及应用场景研究[J].电气时代,2021(6):20–23.
- [4] 董磊.基于物联网、大数据、智能分析的一体化制造过程评价与预测[J].智能制造,2020(11):25–27.

(上接第 113 页)

- [15] 任凤雷,何昕,魏仲慧.基于 DeepLabV3+与超像素优化的语义分割[J].光学精密工程,2019,27(12):2722–2729.

(收稿日期:2021-07-23)

## 作者简介:

李宁(1983-),通信作者,男,硕士,高级工程师,主要

- [5] 王瑞娜.区块链技术在智慧城市建设中的应用研究[J].内江科技,2021,42(7):54–55,116.
- [6] 谢作如,林森焱.用 Node-RED 让物联网数据可视化[J].中国信息技术教育,2019(11):78–81.
- [7] 高晓川.云计算平台下物联网数据挖掘研究[J].电子世界,2021(10):45–46.
- [8] 工信部、中央网信办印发《关于加快推动区块链技术应用和产业发展的指导意见》[J].中国信息化,2021(7):16–19.
- [9] 刘旸,丁涛杰,汤明宏,等.一种 RISC-V 验证系统的设计与实现[J].电子技术与软件工程,2021(13):107–108.
- [10] 吕倩茹.基于网络报文转发应用场景的 RISC-V 定制化设计[D].长沙:国防科技大学,2017.
- [11] LEE S, HUNG Y, CHANG Y, et al. RISC-V CNN coprocessor for real-time epilepsy detection in wearable application [J]. IEEE Transactions on Biomedical Circuits and Systems, 2021, 15(4):679–691.
- [12] 黄平,袁佳,朱静,等.RISC-V 处理器远程监测系统终端设计[J].物联网技术,2020,10(10):12–14.
- [13] 杨鹏.“云管端”同时发力 中国移动 5G 智能电网将“三步走”[J].通信世界,2020(23):18–19.
- [14] 刘伟,黄瑞.面向道路交通的 C-V2X 车路协同应用研究[J].集成电路应用,2021,38(7):34–36.
- [15] KHAN A T, CAO X, LI S. Blockchain technology with applications to distributed control and cooperative robotics: a survey [J]. International Journal of Robotics and Control, 2019, 2(1):36.
- [16] 李芳,李卓然,赵赫.区块链跨链技术进展研究[J].软件学报,2019,30(6):1649–1660.

(收稿日期:2021-08-24)

## 作者简介:

郝向宇(1991-),男,硕士,工程师,主要研究方向:物联网技术、安全技术、区块链技术和应用。

柳耀勇(1986-),男,硕士,工程师,主要研究方向:物联网技术、安全技术、区块链技术和应用。

肖青(1979-),男,硕士,高级工程师,主要研究方向:物联网技术。



扫码下载电子文档

研究方向:高压电缆运维检修及电力计算机视觉技术,E-mail:smart\_3d@126.com。

张彦辉(1984-),男,本科,高级工程师,主要研究方向:高压电缆运维检修技术。

尚英强(1990-),男,博士,工程师,主要研究方向:高压电缆运维检修技术。



扫码下载电子文档

## 版权声明

经作者授权，本论文版权和信息网络传播权归属于《电子技术应用》杂志，凡未经本刊书面同意任何机构、组织和个人不得擅自复印、汇编、翻译和进行信息网络传播。未经本刊书面同意，禁止一切互联网论文资源平台非法上传、收录本论文。

截至目前，本论文已经授权被中国期刊全文数据库（CNKI）、万方数据知识服务平台、中文科技期刊数据库（维普网）、DOAJ、美国《乌利希期刊指南》、JST 日本科技技术振兴机构数据库等数据库全文收录。

对于违反上述禁止行为并违法使用本论文的机构、组织和个人，本刊将采取一切必要法律行动来维护正当权益。

特此声明！

《电子技术应用》编辑部

中国电子信息产业集团有限公司第六研究所