doi:10.3772/j.issn.1002-0470.2021.01.006

区块链技术应用于物联网:发展与展望①

叶欣宇②* 李 萌③*** 赵铖泽* 司鹏搏*** 孙 阳* 张延华***

(*北京工业大学信息学部 北京 100124)

(**先进信息网络北京实验室 北京 100124)

摘 要 近年来,随着数字货币的日益兴起和商业应用,区块链技术越来越受到政府部门、工业界以及学术界的关注和认可。与此同时,移动通信网络的快速发展和广泛覆盖,促使物联网(IoT)逐渐走入日常生活,极大程度地提升了工作效率与生活品质。然而,物联网场景中仍存在能效性低、数据传输安全性差等问题,使用区块链技术可有助于促进物联网更好地发展和普及。本文对区块链技术在物联网中的应用进行了系统性综述,首先介绍了背景知识和相关研究,其次提出了区块链的基础架构模型,并且详细阐述了区块链技术应用于物联网各场景的发展现状以及相关特征,最后讨论了一些挑战及未来发展趋势。

关键词 区块链;数字货币;物联网(IoT);共识机制;智能合约

0 引 言

随着社会的发展演变,中心化组织架构对经济的发展有一定的阻碍,包括隐私保护问题、成本问题以及所有权问题等。在数字货币领域,分布式架构的成本和效率比中心化架构更有优势。为了能够寻求高可信的去中心机构来发展数字货币,区块链技术应运而生。区块链的概念始于2008年,是由Nakamoto[1]在比特币论坛中发表的论文中提出的,它是一种去中心化的分布式账本技术,并在比特币和其他加密货币中成功应用。区块链的核心思想在于去中心化,通过运用非对称加密技术、时间戳、共识算法、经济激励以及点对点(peer-to-peer, P2P)分布式网络,在没有第三方可信任机构的情况下,互不信任的双方可以运用比特币直接进行电子交易[2]。

正是由于区块链技术的产生,带动了数字加密货币的兴起。区块链技术是数字加密货币的底层技术基础,能够为数字加密货币领域重塑信任,从而大大降低交易成本和交易门槛,提高经济运行的效率。以比特币为代表的数字加密货币,是区块链最为成功的应用场景。它通过运用区块链去中心化、去信任化的特点,并结合P2P网络、共识算法和密码学技术,帮助其解决了双重支付问题和拜占庭将军问题[3]。与传统的中心机构相比,基于区块链的数字加密货币领域形成了一种软件定义的信用,这标志着国家算法信用由集中化向去中心化的根本性转变。基于此,数字化平台在区块链技术的帮助下,其基础功能和应用将得到颠覆性改造,从而对经济社会产生更强大的推动力。

随着数字加密货币的发展,区块链技术在不断地扩大完善,将其应用于更广阔的领域,可以带来更显著的优势。区块链具有去中心化、去信任、不可篡改、公开透明、匿名性和民主化等特点[4]。首先是去中心化,它实现了一种点对点的直接交互,使得高效率、大规模、无中心化代理的信息交互方式成为了现实;其次是去信任,在跨境支付等金融交易中,可以在没有可靠第三方机构的情况下,让交易以点对点的方式正常运行,缩短了支付周期,降低了交易费

① 国家自然科学基金(61901011)和北京市教育委员会科技计划(KM202110005021)资助项目。

② 女,1997年生,硕士生;研究方向:区块链,物联网,网络资源管理;E-mail:332184646@qq.com

③ 通信作者,E-mail:limeng720@bjut.edu.cn

(收稿日期:2020-03-20)

用;第三是不可篡改,信息经过验证并添加到区块链后,便会永久存储,可用于农产品溯源、进口商品溯源等方面,用户可以追踪到真实的商品生产、储存、出仓等信息;第四是公开透明,区块链系统是公开的,除了交易各方的私有信息被加密外,每个参与者都可以访问所有的交易记录,以便查看每笔交易的去向;第五是匿名性,可以确保在公开交易数据的同时,更好地保护数据来源的私密性,从而杜绝非法盗取和倒卖交易数据的不良现象;最后是民主化,系统中的交易验证,是通过多方参与者共同做出的决策,任何人为的干预是不起作用的。

区块链技术已为金融等领域带来深刻的变革,但其作为底层应用技术,仍具有较强的普遍适用性。一些研究工作也对区块链技术进行了回顾总结(如文献[5-11])。Zheng 等人[5]从基础架构、特点、应用、未来研究挑战等方面对区块链进行了全面的综述。Lin 和 Liao[6]对区块链的安全问题和挑战进行了讨论。Conti 等人[7]对区块链所面临的安全和隐私问题进行了调查,包括可能的攻击和应对措施。Tschorsch 和 Scheuermann[8]对去中心化数字货币的特点、基本结构及应用进行了详细的叙述。Li 等人[9]对区块链的安全威胁进行了调查,并列举了相关的真实攻击案例。Sankar 等人[10]对区块链中已经提出的共识协议进行了分析,并验证了满足协议提出的特性方面的可行性和有效性。Mukhopadhyay 等人[11]调查和比较了当前主要加密货币使用的挖掘技术,并评估了每种挖掘策略的优势、劣势和可能的威胁。

虽然现有的工作已经对基于区块链的数字加密货币领域进行了广泛的研究,但随着社会的发展,更多的领域将会融入区块链技术。在第五代通信技术的发展与普及过程中,物联网(Internet of Things, IoT)迎来爆发式的增长环境。如今,物联网领域在智慧城市、交通、能源、金融、家居、医疗等方面都有具体的应用案例,然而,物联网却始终面临限制行业发展的数据隐私性和安全性问题。区块链技术作为新兴网络技术,可以作为有效解决这些问题的方法之一。但是,当前对区块链技术应用于物联网领域的研究较少,大部分都是讨论区块链在金融领域的应用。本文调查了可以应用于物联网的最先进的区块链技术,介绍了采用区块链技术提高物联网环境的性能、效率和安全性的研究。此外,本文还对未来相关领域的研究方向进行了适当深度和广度的探讨,确定了基于区块链的物联网领域的三个方面,重点关注背景知识、物联网中的区块链、挑战及未来发展趋势。本文的讨论和探索可以让读者对这一领域有个全面的了解,并为后续研究提供更多的思路和方向。

1 区块链基础架构模型

区块链是一个基于 P2P 网络,整合了密码学、共识算法、智能合约等关键技术的去中心化的分布式网络,按照时间顺序以密码学方法将数据块以链表形式连接起来,每一个数据块中包含了验证的交易信息,根据区块链技术不可篡改和不可伪造的特点,能够对这些信息进行安全存储和溯源。随着人们对区块链认识的不断加深,其技术范围和应用范围也不断扩大。

区块链的基础架构模型如图 1 所示。一般来说,区块链系统由数据层、网络层、共识层、激励层、合约层和应用层组成。

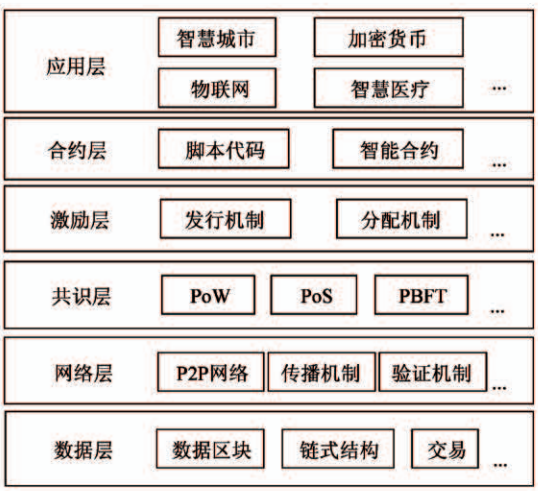

图 1 区块链基础架构模型

1.1 数据层

数据层中双方之间的交易被验证并打包到一个块中,块头包含父区块的哈希值(Hash),能够链接

到前一个块，从而形成一个有时间顺序的区块主链，如图 2 所示。区块头中封装了前一区块的哈希值、时间戳、随机数、Merkle 根和当前区块的哈希值。区块体中包含当前区块中的所有交易，并通过 Merkle 树的哈希过程生成唯一的 Merkle 根记入区块头中，并且通过哈希值，参与者可以找到交易对应的区块。

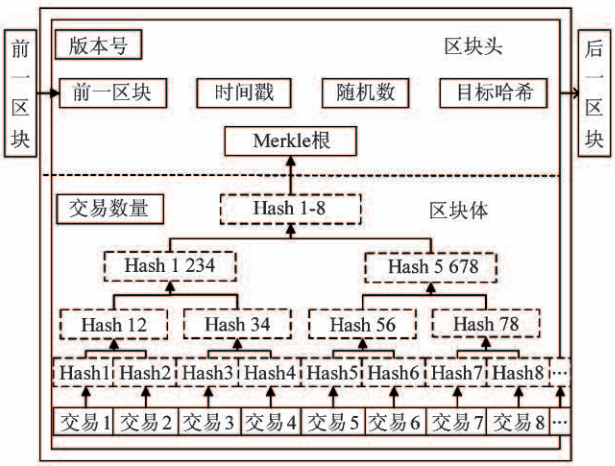

图 2　数据区块

1.2　网络层

网络层定义了区块链中使用的网络机制。此层的目标是传播从数据层生成的数据并对数据的有效性进行验证。网络机制一般采用 P2P 网络，如图 3 所示。其中，对等点都是参与者，都可对区块链系统进行管理和维护，对系统中的交易进行验证。P2P 网络中的每个节点的地位对等，不存在任何中心化的特殊节点，当有交易生成时，由生成该交易的节点向邻居节点进行广播，邻居节点经过验证后，只转发有效的交易。

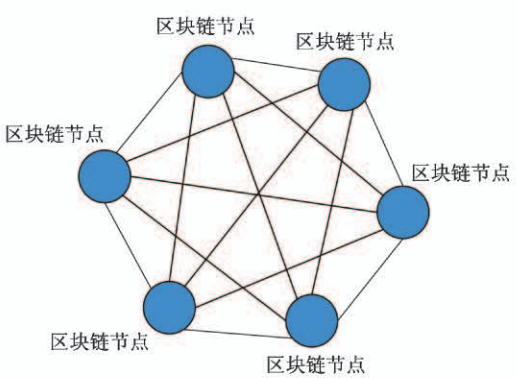

图 3　P2P 网络

1.3　共识层

共识层是为了解决分布式系统的一致性问题，使区块链中的各节点可以在去中心化的系统中对交易的有效性达成共识。共识层由共识算法组成，主要的共识机制包括 3 种，即工作量证明机制（proof of work，PoW）、权益证明机制（proof of stake，PoS）和实用拜占庭容错算法（practical byzantine fault tolerance，PBFT）。

比特币系统中运用 PoW 共识机制，每个矿工（节点）运用各自计算机的算力，通过反复运行哈希函数找到一个随机数（挖矿），这个值很难生成，但是其他人很容易验证。当双哈希值小于或等于目标哈希值时，随机数被确定，先找到这个随机数的节点将会获得区块记账权并得到系统给予的比特币奖励。由于 PoW 的计算量大，其计算能力相对于网络总计算能力（小于 51%）是有限的，因此可以防止恶意节点的攻击。

PoS 共识机制是拥有最高权益的节点获得区块记账权，权益指节点所拥有的特定货币数量，称为币零（货币数量乘以持有时间）。PoS 仅依靠权益和币零，不需要消耗额外的资源，解决了 PoW 共识机制中算力和资源浪费的问题，并且能够更快速地达成共识，提高了交易效率。因此，比特币后的许多数字货币均采用 PoS 进行共识。

PBFT 共识过程中的每个区块都由随机选出的主节点生成，当正常工作的节点超过全网结点的 $\frac{2}{3}$ 时，系统正常运行，可保障数据的安全性和一致性。

1.4　激励层

激励层中集成了经济激励，鼓励节点参与区块链的安全验证工作，这对于维护区块链系统的安全性至关重要。为了鼓励节点参与，通常将比特币、以太币作为奖励，发放给成功找到随机数并将区块添加在链上的节点。除了奖励外，存款和罚款都被引入到区块链中以保护外包计算。

1.5　合约层

合约层将可编程特性带入区块链，封装了各类脚本代码以及由此生成的智能合约，是区块链系统灵活编程和操作的基础。在以太坊中，智能合约作为功能强大的脚本，是一组状态响应规则，用于在用

户之间自动转移数字资产。

1.6 应用层

应用层封装了区块链的各种应用场景和案例,包括物联网、知识产权、智慧城市等,这些应用为社会带来深刻变革。虽然区块链技术仍处于起步阶段,但学术界和工业界都在努力将这项有前途的技术应用到更多领域。

2 区块链技术在物联网中的应用

随着区块链技术的蓬勃发展,其在个人数据管理、智慧医疗、智能电网、智能交通、智能家居和边缘计算等物联网领域存在广泛的应用场景。本节将详细介绍区块链技术在物联网各领域中的实际应用和技术特点。

2.1 区块链+个人数据管理

随着大数据的到来,产生的数据量也随之指数增长。在这个数据集中化的时代,用户的个人数据容易遭到泄露和入侵,并且数据的存储和访问方式也存在安全隐患和漏洞。如何能让用户有效传输、存储和管理个人数据,是当前面临的重要问题。区块链技术的去中心化分布式存储方式,可以很好地解决这些问题,能够让用户自己建立节点,加入区块链网络进行数据同步,用户可以随时随地查询数据,并对数据进行加密管理,保障数据的安全性。

2.1.1 个人数据存储

近年来,随着物联网设备的广泛使用,其收集到的用户数据呈井喷式增长。由于多数物联网设备的设计是集中式网络架构,如何能在安全存储数据的同时保持数据的完整性,是面临的一个难题。区块链的去中心化、不可篡改的特点使其成为用户存储个人数据的理想选择。目前,许多研究已经运用区块链技术来进行个人数据存储。

个人数据存储是对个人敏感数据信息进行管理和部署,如今,云存储已成为大多数个人用户或企业用户工作和生活所必须的存储方式,通常以密文的形式将隐私数据存入其中,用户需要用第三方密钥来进行数据访问。若第三方不可信时,用户的隐私将受到威胁。为了解决云存储存在的问题,可以将区块链与云服务器结合起来,构建基于以太坊区块链技术的安全云存储系统[12],如图4所示。数据所有者通过智能合约在区块链网络中存储数据密文,同时上传加密文件存储至云服务器中,数据用户访问加密文件需获得内容密钥方对加密文件进行解密。

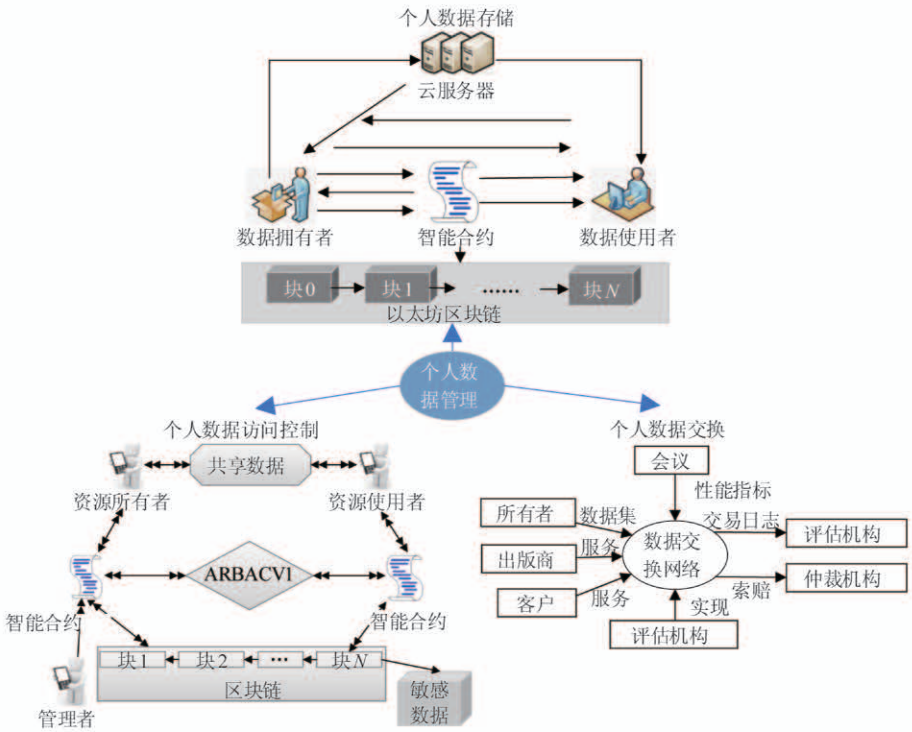

图4 个人数据管理体系模型

当前,还存在由于数据泄漏所造成的存储不平衡问题,为了解决该问题,并针对区块链网络在稳定性和可用性方面的不足,研究人员提出了一种基于自定义遗传算法和禁忌搜索算法的启发式算法[13]。这种启发式算法能够在节点较少的情况下,获得与遗传算法和禁忌搜索算法相同的存储适应度,使得区块链网络的安全性大幅提升。

2.1.2 个人数据访问控制

如上文所述,用户的个人数据大多都存储在数据中心,通过集中式访问控制服务器来对数据进行访问,即便当前中心机构采取了更强的加密方案,但一旦有恶意节点进入系统,便可访问到所有数据,这将严重威胁到用户的信息安全。运用区块链技术的去中心化、去信任、匿名性等特点,可以作为构建可行数据访问控制平台的基础,实现可信的访问,用户可以自己决定谁有资格访问其数据。因此,运用区块链技术能够有效地实现用户数据的安全访问和有效使用。

目前,大多数数据库系统和企业信息系统都是基于角色的访问控制技术,该权限管理系统运行稳定。但是,由于角色访问控制简单,其灵活性和细粒度控制有时不能满足实际访问控制的需求。为了满足需求,可以将基于角色与基于属性的访问控制相结合,得到基于属性角色的访问控制模型[14],并将该模型通过智能合约集成到区块链中,如图 4 所示。资源所有者通过加密方式将共享数据上传到共享数据服务中心,敏感的私有数据可以直接上传到区块链,并为它们设置适当的访问策略,当用户请求访问数据时,必须通过智能合约启动相应的权限请求,请求同意后方可进行数据访问。

随着使用物联网设备产生的有价值数据的增加,用户对分级访问控制的需求也在增加。最近研究表明,在无法确认第三方完全可信的情况下,集中式云无法为用户提供满意的分级访问控制服务。然而,使用基于区块链的分布式密钥管理体系结构可以更好地保护访问隐私[15],该结构采用了雾计算来减少延迟,并通过在云服务器中运行的多区块链来实现跨域访问。

同时,在传统的云存储系统中,可能会产生密钥滥用、隐私数据泄露以及单点故障等问题,影响用户的正常访问。在结合星际文件系统和以太坊区块链所产生的框架中[16],数据所有者可以通过指定访问策略,对共享数据加密并为用户分发密钥。在访问控制列表的维护中,以太坊智能合约起到很大作用,系统通过与智能合约的结合与交互,使文件上传和传输的时间不受限制,提高了系统的访问控制能力。

2.1.3 个人数据交换

随着智慧城市的发展,用户对数据的需求度随之增高,数据交换市场逐渐进入人们的视野。数据所有者可以通过数据交换市场,将数据进行共享和出售。但当前的数据交换市场是集中式的,所有交易都需要通过可信任的第三方进行,并向第三方支付一些费用。这种通过第三方进行交易的方式存在安全隐患,并有极大可能发生单点故障。为了解决这种问题,可以使用区块链技术建立去中心化的数据交换市场。

区块链能够使互不信任的实体达成共识并保持完整性,而无需任何可信第三方。根据其去中心化和不可篡改的特性,可以开发安全可靠的数据共享系统[17],用于保证共享数据的实时性并在区块链网络中提供交易隐私。同时,对于医院、银行等拥有大数据集的组织来说,维护数据服务需要特殊的信息技术,通过区块链技术构建去中心化的数据交换系统[18]可以有效解决此问题。如图 4 所示,在该系统中,用户节点通过 P2P 网络进行数据交换,解决了数据交换过程中的隐私安全问题。但区块链系统吞吐量小的问题,会影响数据交换的速率,以区块链为中心的交换协议中[19],提出了新的 P2P 网络层来解决该问题,并使用了以信息为中心的体系结构来优化信息交换。

此外,随着对物联网数据交换要求的增多,涌现出一批致力于连接各种分布式数据源的物联网数据交换平台,服务提供商可以通过平台搜索和交换他们需要的数据集。但是,由于对这种集中式平台的不信任,大多数用户不愿意将自己的数据集放入平台共享,这样无法满足实际需求。因此,研究人员提出了一种基于区块链的物联网数据可信交换分散解决方案[20],利用以太坊区块链和智能合约实现了一

个透明的系统原型,将数据交换的可信任度大幅提升。

综上所述,在个人数据管理中运用区块链技术,可以安全地存储用户的数据信息,并且能够公开透明地访问数据。同时,在数据交换中无需可信任第三方,即可实现可靠的数据交易。虽然区块链技术在个人数据管理中有很好的优势,但是其数据交易吞吐量仍是一个有待解决的问题。相比于中心机构,区块链处理交易的速度过于缓慢,会严重影响交易的进行。因此,提升区块链的吞吐量将是未来重点研究的方向之一。

2.2 区块链+智慧医疗

随着物质生活水平的提高,健康越来越被大众所关注,医疗信息化也成为大势所趋。当前,多数医疗机构都建立了电子医疗管理系统,患者的各项数据指标存储对于有效治疗疾病非常重要。然而,各医疗机构间的数据都分散在各自系统中,数据存储格式各不相同,且需要中心化的管理机构进行授权和管理,无法有效地实现数据共享。区块链技术的诞生,改变了这种数据集中存储,通过在医疗机构和研究机构之间建立联盟区块链,被授权加入区块链的节点使用相同的结构来存储数据,同时可以访问其他节点中的数据,从而减少访问期间数据审查和审核的时间。区块链的匿名性和完善的授权策略,可有效降低数据共享的潜在风险。

2.2.1 健康数据共享和存储

在患者治疗过程中,需要创建、存储和访问大量医疗数据。通常,每个医院都无法获取患者在其他医疗机构就诊的病历数据,这会影响患者的治疗效率。因此,实现各医院之间的数据共享是非常有必要的,并且要保证数据的隐私性和完整性。区块链技术可以促进医疗数据的共享和存储,并将患者的医疗数据以安全可靠的方式共享并存储在区块链上。

随着智能可穿戴设备走进人们的生活,其收集到的个人健康数据为医疗保健提供了巨大的价值。为了解决数据共享的安全隐私问题,研究人员创建了以用户为中心的基于区块链的健康数据共享系统[21]。通过部署移动应用程序,使智能设备收集到的健康数据同步到云上,并将记录证明存储在区块链中,这在保证数据隐私和完整性的同时,实现了数据共享。同时,有研究提出可以在此基础上加入机器学习技术,实现共享个人连续动态健康数据[22],使用机器学习技术的数据质量检测模块来控制数据质量,能够使用户安全地拥有管理他们个人健康数据的权利。

并且,区块链增强方法[23]可以防止恶意攻击,一个许可的区块链只允许授权的个人和医疗服务提供者加入网络,同时使用一个私钥和公钥用于安全数据交换,且所有协议都由智能合约管理和执行,从而实现数据安全。

此外,有研究提出基于区块链的可验证数据完整性的个人健康记录共享方案[24],如图5所示。该方案包括三个实体,即患者、用户和云服务器。患者对个人健康记录进行加密并上传至云服务器。通过区块链系统,可部署智能合约并为用户生成和分发属性私钥,其密钥使用区块链进行管理,由此用户可以使用私钥来进行数据的访问。云服务器用于存储患者上传的数据关键字索引,且索引集在智能合约中的存放提高并保证了数据完整性验证的效率。

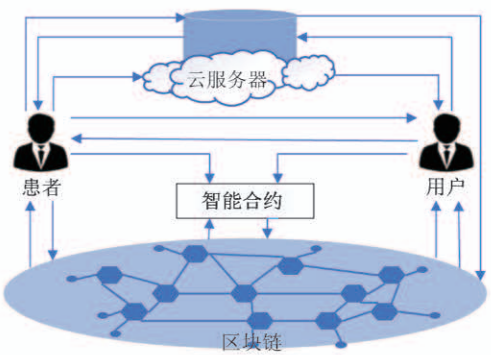

图5 基于区块链的个人健康记录共享模型

2.2.2 健康数据访问控制

传统的医疗系统中,患者的医疗数据由医疗机构存储,患者对自己的医疗数据没有控制权,也无法知道医疗数据是否未经授权就被使用。医疗数据中包含患者自身的个人隐私,大多数患者都希望可以授权管理自己的医疗数据,防止被篡改和盗用。区块链去中心化和防篡改的特性能够让患者对医疗数据进行访问控制。

个人健康记录(personal health records, PHRs)是每个人的隐私,也是诊疗时的可靠参考[25]。然而,PHR 在紧急情况下有时不能起到期望的作用。在传统的急救系统中,病人无法同意急救人员进入其 PHR,这样会使医生很难接管病人。此外,现有设备无法对 PHR 记录进行安全管理,例如决定谁何时可以访问这些信息。因此,设计人员开发出基于区块链技术的应急访问管理系统[26],如图 6 所示。该系统采用了超级账本编码器,患者使用智能合约为急诊医生等用户定义了包括紧急状态和时间期限的访问控制策略,用户通过 API 接口来请求数据访问,通过共识确认所有访问过程的准确性,最终所有的访问记录将存储在分类账中。

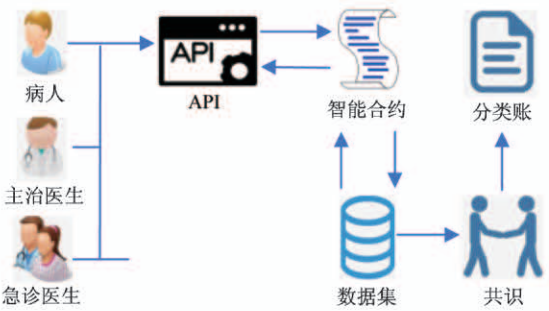

图 6　基于超级账本结构的 PHR 应急访问管理系统

实现个人健康数据访问控制,还可以构建基于区块链的电子健康应用架构[27-28]和数据记录管理系统[29]等。与传统的系统相比,使用区块链技术,可防止单点故障和拒绝服务攻击,为患者提供全面的记录管理,在跨服务商和服务点访问信息方面也提供了便利。

区块链平台是解决医疗数据共享、存储和访问问题的有效手段。使用区块链技术,不同医疗机构采用分布式多中心的互联,提供数据存储、传输及分析等能力,在保证隐私的同时高效利用数据资源。医生通过访问电子病历,为患者提供更高质量的医疗服务。基于医疗数据的快速流转和统计分析,支持了社会和企业的发展决策,提高了健康服务的效率和质量,为个人健康提供更有力的技术支撑。但总体来看,区块链医疗项目大多处于初创期,真正大规模使用的案例还比较少。同时,由于区块链平台的建设需要依托强大的资源,消耗高昂的成本,因此,如何能在降低开销的同时使区块链技术更加成熟完善地应用于医疗机构仍是需要解决的问题。

2.3　区块链 + 智能电网

智能电网是将传感测量技术、无线通信技术等现代先进技术与物理电网高度集成而形成的新型电网。智能电网在为电力供应商和用户提供便利的同时,也为安全和智能领域带来了新的挑战。因此,运用区块链技术的分布式电网系统是智能电网的发展趋势。区块链技术充分促进了高可信和高效的分布式电网系统的实现,同时还增强了智能电网系统的稳定性和数据安全性。

2.3.1　电力能源交易

在分布式电力交易系统中,如何在众多用户之间实现安全可靠的电力交易是一项重要的目标。运用区块链技术可以建立一个公开透明、可信任的电力交易系统,使用户进行安全交易。

随着分散式可再生能源的应用,生产者和消费者之间将不断进行电力交换,用户能源交换的种类需求也随之增加。因此,未来的电网应该是使用分布式能源管理软件相互连接的双向通信模式[30]。其中,除了可以通过交易双方直接达成共识进行电力交易,还可以通过能源拍卖方式[31],拍卖方将能源信息发布到基于区块链的拍卖系统,投标者从中获取信息并进行投标,运用智能合约管理拍卖过程,最终中标者获得能量并进行付款,拍卖数据将存入区块链中。

同时,在确保交易安全性方面,多重签名和匿名加密消息流实现了去中心化能源交易系统的概念验证[32],使同行能够匿名协商能源价格并安全地执行交易,也使智能电网有望提供更复杂的能源交易。

当前,一种称为 Helios 的太阳能分配系统[33],可以进行自动能源交换,如图 7 所示。Helios 模型分为能源网格、中间件控制器和智能合约。能源网格由太阳能电池板、交流电源、智能电表和电池等设备组成。智能合约用于监视和核算能源交换,使生产者可以在有限的地理区域内自动进行能源交易。中间件控制器将能源网格与智能合约互连,来调用智能合约并从能源网格接收数据。

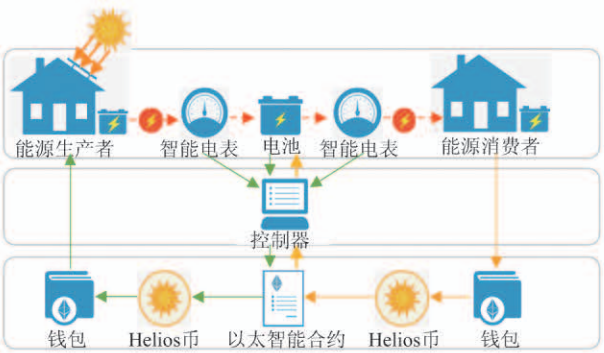

图 7　Helios 模型高级架构

2.3.2　增强智能电网的数据安全性

在智能电网系统中,数据安全性对电力公司及其客户至关重要,客户希望掌握他们电器的用电情况,从而避免高额支出。此外,有误的数据可能会导致电网系统中心做出错误的判断,使系统出现混乱或产生经济损失。区块链具有去中心化、不可篡改和去信任的优点,能够增强智能电网的数据安全性。

为了实现电网弹性,区块链将信任商品化,智能合约使客户和能源提供商之间直接进行多方交易[34],消除了与第三方互动的需求,有助于降低能源交易成本,提高交易数据的安全性,从而促进能源交易。此外,使用许可区块链边缘模型也可以确保智能电网性能并提高数据保护能力[35]。

在智能电网中,每个家庭都安装了一个智能电表以实时监测用电数据,公共机构能够根据这些数据提供更好的智能家庭服务。但当数据泄露时,攻击者可以通过分析用户的用电情况来推测个人生活规律等隐私。为了解决此问题,研究人员提出一种基于区块链的高效数据聚合方案[36],以在智能电网中保护用户的隐私。在每个时间段内,根据电表中用户用电数量与平均值之间的差异来选择挖掘节点,并通过该节点将用户的数据记录在区块链上,保证数据的完整性。同时使用区块链的匿名性来隐藏用户的真实身份,保证用户用电数据的安全性。

未来,区块链技术会驱动更多分布式电网基础设施建设,同时也会激发更多资源投入赋能分布式电网的技术和能源交易市场,实现可靠、高效的匹配能源供需。但同时,区块链应用于智能电网需要部署大批电网设施,消耗大量分布式电力资源,并且鉴于电网上所涉及的节点的绝对数量,可能会带来很高的风险,这些问题还需要进行改进和解决。

2.4　区块链 + 智能交通

智能交通能够为驾驶员和乘客提供舒适和便利,改善交通和出行效率,并提高车辆道路安全性。然而,在当前智能交通系统中,无法实现高效安全的车辆通信管理和信息共享。利用区块链技术的去中心化、不可篡改和公开透明的特点,可以建立一个分布式的安全、可信的智能交通系统。

2.4.1　分布式智能交通架构

传统的交通管理控制中心可以方便进行交通的监测和管理,但在实现实时数据共享以及车辆通信过程中,会产生延时、单点故障等其他不可控因素。为了克服这些问题,可使用区块链技术来建立安全且去中心化的智能交通网络。

车载自组网(vehicular ad-hoc networks, VANETs)是组成智能交通系统的重要部分。整个网络没有固定的基础设施,每个节点都能以任意方式动态地保持与其他节点的联系,从而提高道路交通的安全与高效。但这种动态性和无固定基础设施,在网络安全方面无法做到保障。因此,可以使用软件定义的 VANET 来安全管理动态 VANET[37],再结合区块链技术,对整个网络进行分布式控制。对比集中式控制平台而言,这样能够防止恶意节点攻击,提高系统性能。此外,为了提高 VANET 中电动汽车交互的安全性,定义区块链启发的数据硬币和能源硬币为用于车辆应用的新加密货币[38]。通过数据贡献频率和能量贡献量完成工作量证明,实现车辆间的分布式共识。

在 VANETs 环境下,数据安全存储和传输是需要解决的重要问题。采用基于区块链的分布式交易存储方案[39]能够解决数据安全存储问题,每个交易的内容分为多个部分,并以分布式方式存储在不同的云服务器上,交易的哈希值存储在区块链中,用户可以通过区块链上的同源哈希值来访问交易,获取道路信息。数据安全传输问题可以采用基于分布式区块链的动态密钥管理系统[40]来解决,如图 8 所示。路边单元(road side unit, RSU)将消息通过接口上传到安全管理器(security managers, SM),每个 SM 在安全域中管理加密的材料,将分散的 SM 网络

部署在区块链结构中，可对密钥传输过程进行身份验证，使密钥能够安全传输。

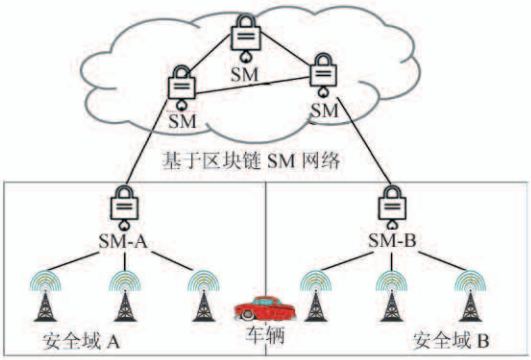

图 8　基于区块链的动态密钥管理系统

2.4.2　车辆通信管理

车辆之间通过共享与道路相关的信息，可以提高交通的安全和效率。但是，由于可能存在恶意车辆提供错误信息，会对交通造成严重后果，使得车辆之间无法做到相互信任。为了解决信任问题，设计分布式系统对于信任管理更有效。因此，采用区块链技术的公开透明和不可篡改的特性，可建立去中心化交通信任管理系统。

在车辆行驶过程中会接收到其他车辆或 RSU 发送的消息，但无法评估消息的可信度，而信誉系统被证明是解决上述问题的有效方法[41-42]。车辆根据路况对接收到的信息的可信度进行评级，并将这些评级打包成一个“块”，大多数车辆验证通过后，将块存储在区块链中。根据存储在区块链中的评级，车辆能够计算消息发送者的声誉值，并根据此值来评估消息的可信度，由此可使车辆收集到安全可靠的路况消息。

如图 9 所示，针对车辆信任和隐私问题，还有研究人员提出了一种基于区块链的信任管理方案[43]。该方案模型包括三部分，即信任机构、RSU 和车辆。RSU 和车辆通过信任机构申请进入 VANETs，RSU 在其通信范围内收集车辆的聚合包，以评估消息的可信度并更新车辆的信誉值，并将更新后的信誉数据打包到一个块中并与其他 RSU 进行共识，验证块的正确性，最终存储在区块链中，实现 VANETs 中消息的同步和可信度的提升。此外，该方案还实现了有条件的隐私保护，由于信任机构可以使用区块链中的公共地址跟踪匿名恶意车辆的身份，从而保护了用户的隐私。

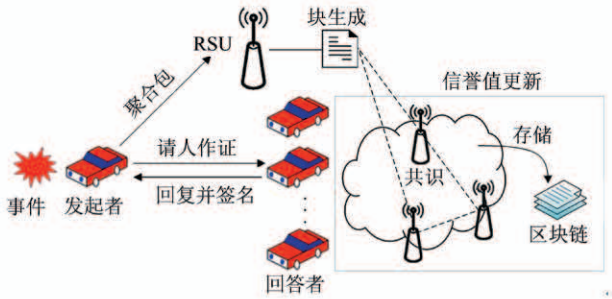

图 9　基于区块链的信任管理模型

2.4.3　电动汽车充电管理

为了发展绿色交通系统，电动汽车已引起广泛关注，并在多个国家或地区投入使用。充电站为电动汽车提供电力资源，同时，车主需支付相应的费用。运用区块链和智能合约技术可以促进电动汽车和充电站之间进行高效安全的电力交易和实时费用结算。

电动汽车充电能源来源于智能电网，为了降低电网中的功率波动水平和电动汽车用户的总充电成本，可建立一个安全自主的交易平台，并将基于区块链的自适应电动汽车充放电调度算法应用于该平台中[44]。电动汽车将充放电指令发布并传输到智能电网公共区块链交易平台，使用该算法处理订单，匹配后的订单由网络中的对等节点进行处理和验证，最终双方以分布式方式保存确认的订单。

此外，充电站中运营着多个充电桩，并从电网或微电网获取能量，电动车向充电桩发送充电请求，双方进行电力交易，但其双方之间的不透明且不信任性，使得交易存在潜在的安全和隐私问题，为了解决此问题，每台电动车内置的智能电表用于记录能耗金额，并验证交易是否完成来进行授权支付[45]。电动汽车与充电桩之间的交易信息存储在区块链中，保证交易数据的安全可靠性。

对于需要在工作时间内进行充电的电动出租车，如何在已接单的情况下，根据其订单位置选取合适的充电站进行充电，是亟待解决的问题。图 10 是电动出租车的充电引导场景[46]。服务器节点分布在联盟区块链网络中，出租车将充电需求发送给充

电站运营商,运营商的服务器节点计算总能源需求。同时,服务器节点收集各快速充电站的充电桩使用情况和周边道路信息,根据这些信息,在与其他服务器节点达成共识的情况下为电动出租车推荐最优的快速充电站。

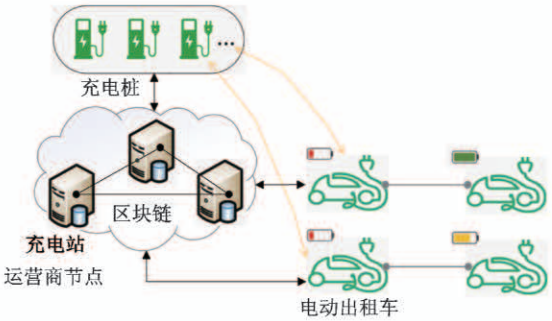

图 10　基于区块链的电动出租车在线预约服务充电架构

智能交通与区块链技术等尖端科技相结合可改善道路安全、缓解交通拥挤、降低能源消耗,还能提升运输系统的能效、加强交通资讯的整合,以及更好地配合交通管理与监控。但是,当前智能交通的发展依然存在很多的挑战,一方面,交通设备的重新搭建需要花费大量的人力和物力,并且与 RSU 进行交互的过程会增加网络的通信和计算开销;另一方面,车辆无法做到完全匿名,用户可能被盗取真实信息。因此,如何能够减少花销并保证车辆网络的隐私安全和有效的信任管理仍是具有挑战性的问题。

2.5　区块链 + 智能家居

随着物联网技术的发展,家居的智能化和联网化趋势愈发明显,智能设备需要相互通信以提供更多的服务。在基于区块链的智能家居架构中,可以对用户的隐私信息进行保护,并且智能家居的所有者可以使用区块链来管理设备之间的通信,智能合约部署在区块链上,可以规定设备访问和其他动作的权限。

智能家居设备信息安全性相对较低,用户的隐私安全遭到威胁。然而,区块链技术可以为其安全问题提供更好的解决思路。当前,研究人员构建一种基于区块链的智能家居架构[47-48],该架构通常由本地设备、覆盖网络和云存储组成。覆盖网络是一个 P2P 网络,它的组成节点是智能家庭管理器(smart home manager, SHM)。当本地设备生成交易向其他设备共享、请求或存储敏感数据时,SHM 处理所有交易。通过对这些数据进行加密,并使用共享密钥与本地设备和云存储进行本地通信,可以对用户敏感数据进行隐私保护。

此外,智能家居设备能够提供远程访问功能,用来获取图像、音频等信息,但这也存在一定的风险,攻击者可以利用易受攻击的设备对用户和组织进行监视或执行其他非法活动。因此,研究人员设计出基于区块链的远程用户身份验证系统来解决此问题[49],如图 11 所示。组用户在组管理器中注册之后,通过交易 Tx_{access} 将其请求发布到区块链上,家庭网关用于监视区块链中记录的请求,并将结果数据回复给用户,同时组管理器可以跟踪异常交易 Tx_{unusal},防止恶意用户的破坏。

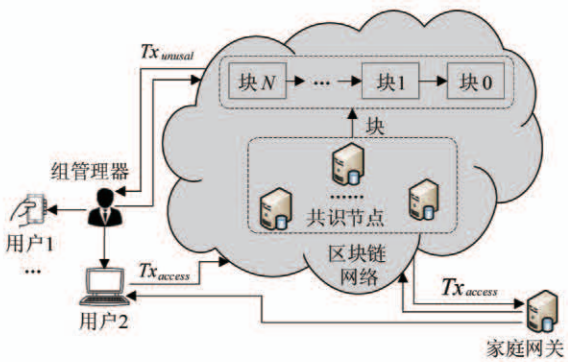

图 11　基于区块链的安全认证系统架构

在智能家居中使用区块链技术,能够远程控制大多数家用电器,保证每一件家居数据的安全与真实性。但如何使家居中记录固定信息的功能根据需求及时升级,从而实现实时动态信息的控制和记录,以及提供更为有效的行为规范和访问策略的隐私保护,是需要思考和解决的问题。

2.6　区块链 + 边缘计算

边缘计算是将数据放在靠近用户的边缘设备中进行存储、计算、传输,而不用将数据放到云上,减少网络资源浪费和传输延时,如图 12 所示。由于数据计算服务器具有分散性,边缘计算的网络一般是分布式的。因此,为确保数据计算安全性,需要在移动环境中部署区块链,运用区块链的去中心化,形成安全可靠的边缘计算分布式网络。

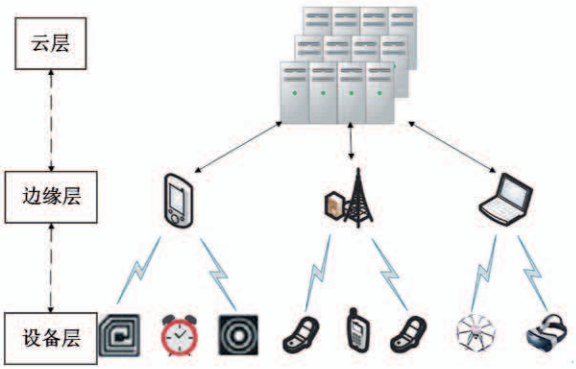

图 12 边缘计算架构

在边缘计算中,边缘层将收集到大量终端物联网设备的数据,并通过服务器对数据进行处理。然而,由于数据的安全和信任性无法确认,当收集到不可靠的数据时,若直接对数据进行计算处理,会导致严重问题。使用区块链技术可有效解决上述问题,当边缘设备收集数据后,将其存入数据库或分布式文件系统中,并将关键数据及其哈希值同时存储到区块链中,当进行数据调用等操作时,将在具有智能合约的可信环境中进行,从而实现高级信任管理,保障数据的安全性[50]。

区块链技术与移动边缘计算(mobile edge computing, MEC)结合,能够在视频传输领域实现高效的视频转码和数据传输[51]。用户能够通过区块链向视频提供商和小区基站付费来享受视频流服务,视频提供商也可以通过区块链向基站支付使用缓存和计算资源的费用,将一些视频放到接近用户的基站上,方便用户更快速地获取视频资源。

此外,在车联网中,由于车辆的资源有限,车与车之间数据共享和分析需要使用 MEC 来提供额外的算力及数据存储,同时结合区块链技术,可保证系统的隐私安全性[52]。在该系统中,RSU 使用数据存储智能合约将收集和验证的数据块添加到区块链中。每个数据请求者通过信息共享智能合约找到最佳数据提供者后,向最近的 RSU 发送数据请求,数据提供者将做出有关数据共享授权的决定,实现了车辆间的分布式数据存储和安全 P2P 式共享。

边缘计算与区块链融合能提高物联设备整体效能,终端设备的数据放入边缘服务器进行计算,同时在区块链技术的帮助下保证数据的可靠性和安全性,为物联网发展提供更多可能性。但二者融合需要解决安全、计算资源分配不均等问题。若有冒充的终端设备与边缘服务器交互时,容易产生安全问题。此外,终端设备本身的算力较弱,若请求边缘服务器进行挖矿过程,其中的资源如何分配,这些问题都有待解决。

3 区块链技术面临挑战及未来发展趋势

区块链作为拥有广阔前景的新型技术,在广泛部署在物联网的多个领域之前,仍然面临着许多重大的研究挑战。本节将讨论区块链技术面临的挑战和问题,并展望了区块链技术在未来的发展趋势。

3.1 面临挑战

3.1.1 安全与隐私

安全与隐私是区块链面临的最重要的问题。虽然区块链具有匿名性,可以通过加密技术对用户数据进行设密,只有用户自己可以对数据进行访问和处理。但由于区块链系统内的各个节点并不是完全匿名的,只是使用假名。尽管区块链中的每个用户拥有的地址假名并不会与真实世界中的用户相关联,但用户存储在区块链中的数据是公开透明的,通过分析其上的数据,可以跟踪用户活动或分析用户个人习惯,尤其是随着链上数据往来的增多,其关联性将或多或少地泄露个人隐私,如果这些交易信息被恶意挖掘及利用,将给用户隐私带来严重的威胁。若结合区块链分析的信息和一些外部信息,并使用一些反匿名身份甄别技术,还有可能会揭示用户的真实身份,一旦用户的真实身份被暴露,就会产生隐秘信息的泄露问题。因此,匿名性的不完善是区块链所面临的严重的潜在安全威胁,确保真正的匿名性是非常重要的。

3.1.2 吞吐量

在物联网中应用区块链技术时,数据交易通常处理速率较低。因此,提升交易吞吐量是区块链技术面临的另一个重要问题。在区块链系统中,比特币的交易吞吐量为每秒约 7 笔交易,以太坊的交易吞吐量为每秒约 15 笔交易。以比特币为例,由于比特币中是将多笔交易放入一个区块后再一起进行处

理,并且每 10 分钟才能打包一个区块,每生成 6 个块后才能进行交易最终确认。这种交易验证过程保护了区块链的安全性,但同时降低了系统的性能,使交易时间延长。与传统的金融系统每秒可达百万甚至千万笔交易相比,区块链的吞吐量远不能满足用户的实际需求。因此,需要设计适当的方案来增加区块链系统的吞吐量,同时保证系统足够的安全性。

3.1.3 能源效率

区块链是高能耗需求的技术,无论是比特币还是以太坊网络,每笔交易的签名与验证、每个区块的哈希运算以及复杂的共识过程等都涉及大量的能源消耗。在区块链的 PoW 共识过程中,这种消耗尤为突出。在使用“挖矿”求解哈希值过程中,需要消耗大量的计算机算力来进行比特币挖掘。根据 2017 年 6 月发布的白皮书,比特币网络中的能源消耗量可以供 700 个普通的美国家庭一年使用,这造成了严重的资源浪费。因此,研究区块链系统节能的共识机制具有重要的意义。

3.1.4 激励和惩罚机制

区块链网络中,需要节点来进行数据的验证。然而,节点的运行有一定的成本,这就需要激励机制来激励这些节点为验证数据做出贡献,确保交易的顺利完成。各个节点之间存在着竞争博弈,对交易过程中节点的贡献程度如何划分并给予相应的奖励,并且使区块链系统中的节点能够自发开展区块数据验证及记账工作,是激励机制需要考虑的问题。另一方面,区块链系统中也需要惩罚机制,在进行交易的过程中,当有恶意节点意图破坏规则,获得不正当的奖励时,系统发现之后,应立即进行相应的惩罚。例如,一个节点获得的经济激励只能在较长的确认时间之后才能使用,若在确认时间内发生中毒交易,将立即收回恶意节点的经济激励。

3.1.5 监管问题

区块链技术诞生是依据去中心化的特点,所以在它的运作机制中并没有监管部门的参与。但随着数字货币的迅速发展,区块链潜在的监管问题也逐渐显现。以比特币为例,它容易被作为非法交易的途径,为洗钱、勒索等犯罪活动提供安全稳定的资金渠道,是金融欺诈的一个手段。另一方面,由于区块链不可篡改、匿名性等特性,一些违法分子将自身的敏感有害信息上传到区块链系统中进行存储,警方无法通过其涉及违法犯罪交易的发送方地址来确定发送方的真实身份,给国家的安全和稳定带来了严重的危害。因此,在保持区块链“自治”优势的前提下,融入现实世界的监管体系是区块链取得广泛应用的必经之路。

3.1.6 成本问题

在区块链共识过程中,需要多个节点同时参与记账,但多个节点进行数据传送的过程需要消耗大量的资源,并且比特币挖矿过程中需要花费的成本非常高。另外,尽管区块链可以应用于智能电网、智能交通等场景,使其应用性能得到大幅提升,但同时为了满足区块链技术的要求,会消耗大量的人力物力来进行设备的重建。区块链虽然节约了中心化成本,但其自身消耗的大量成本问题需要进行改善,应该设计低成本低能耗的共识机制,并且将设备使用的相关零件进行比对,选择成本最低性能最好的,由此来改进成本问题。

3.2 未来发展趋势

当前,世界各国都高度重视区块链技术的发展,我国也提出要把区块链作为核心技术自主创新的重要突破口,加快推动区块链技术和产业创新发展。展望未来,区块链将与人工智能、物联网等前沿技术深度融合,发展新兴产业;与智慧城市结合,给城市建设、改善民生带来新的希望;与供应链融合,实现高效率的供应链管理。但区块链技术应用于这些实际业务时,仍存在诸多问题,为了解决这些问题,未来的区块链技术还需在以下几个方面进行研究和发展。

3.2.1 共识机制

共识机制是影响区块链系统性能的关键,现有的共识机制存在资源消耗大、成本高及吞吐量低等问题。因此,共识机制的未来研究可以从如下几个角度考虑:(1)在共识失败的概率处于很小范围内的前提下,实现在少部分可信节点中选取主节点的共识算法,提高共识速率;(2)将两种及以上算法通过拓扑结构结合,充分发挥各类共识算法的优势,实现安全、效率和去中心化之间的动态平衡;(3)考虑

竞争资源的结合,将多种资源结合竞争,从而解决51%攻击问题;(4)在特定安全性的前提下,减少网络广播的共识算法。

3.2.2 智能合约

The DAO 被攻击事件中,攻击者利用系统中智能合约的两个代码漏洞创建子合约盗取了 360 万个以太币。由于公有链的智能合约出现漏洞和错误时,无法像集中式平台一样关闭系统进行系统补丁和升级,一旦有攻击者通过漏洞对系统进行攻击时,会造成严重的经济损失。因此,在智能合约制定时,增加审核流程,同时可以考虑把以往应用在芯片设计或者军事控制系统上的形式化验证方法,应用到区块链的智能合约中,以数学证明的方式尽可能避免人为错误。未来,智能合约的高阶形态将能对接现实世界的法律系统。

3.2.3 跨链

随着区块链应用深化,医疗、交通、物流追溯等领域的企业,大多都会建立各自的区块链系统。未来这些众多的区块链系统间的跨链协作与互通是区块链技术演进的必然结果。目前较有影响力的跨链技术是 Polkadot 和 Cosmos,将来这些跨链技术将融合起来,彼此互通形成跨链联盟,底层由跨链协议支撑,所有公链通过加入联盟来实现多链分工合作的区块链网络,最终实现区块链间的“万链互联”。

3.2.4 公有链与联盟链融合

未来,区块链技术的发展趋势应当是公有链和联盟链的不断融合,在公链的基础上架设联盟链,实现优势互补。底层是公链,形成全球或全国范围的基础设施,被所有用户所信任,同时公链本身进行了分层,有完全开放的层级,也有需要身份认证的层级。联盟链则可以接入公链的认证层级,从而实现与其他数据主体的数据交互和交易。这样,将会使区块链技术日益完善,尽早实现商业落地。

3.2.5 链外交易

当前较流行的链外交易通道是比特币社区采用的闪电网络和以太坊社区采用的雷电网络,通过将小额交易转移到链外进行,既提高了加密货币的可扩展性和用户隐私性,也降低了交易手续费和主链压力,主链只需处理最终的交易清算结果。但这种交易方式可能出现链内和链外信息不对等的情况,例如,在数字票据应用场景中,若发生人为篡改,则无法保证链外真实数字票据的承兑情况与最终上链数据一致。因此,未来可借助物联网等技术手段,在链外信息数字化上链过程中,减少人为干预,保证相关信息真实可靠。

3.2.6 部分存储

区块链网络中每个节点都存储着所有历史交易数据,这虽保证了数据的公开透明性,但会带来数据隐私问题和性能问题。因此,很多平台采用了只存储部分交易数据的解决方案。超级账本 1.0 的多通道技术从性能和隐私两个角度考虑,使每个通道仅存储与通道节点有关的交易;以太坊 2.0 的分片技术将全网交易数据按片数等分,使得每个分片存储的交易数据尽可能均衡。未来,随着交易量和数据量的剧增,区块链节点由全量存储到部分存储将会成为一个趋势。

以上,就是区块链技术在未来可能的发展趋势,总体来说区块链技术的发展演变中还存在很多未曾改变但在不断调整的规则,当这些规则逐渐完善时,区块链应用将会真正落地,为人们生活带来深远的影响。

4 结 论

本文对区块链技术在物联网的多种领域的应用现状进行了综述,对区块链的背景和相关调查研究进行了讨论。同时,本文分别从个人数据管理、智慧医疗、智能电网、智能交通等方面详细总结了区块链技术在物联网各领域的应用。此外,本文给出了区块链技术在物联网应用中面临的一些重要研究挑战和未来发展趋势,包括安全和隐私、吞吐量、能源效率、激励和惩罚机制等。

综上所述,当前,区块链技术应用的研究非常广泛,所面临的挑战和发展趋势也不可忽视。本文通过对区块链技术的基础架构进行系统介绍,围绕其在物联网不同场景中的应用进行总结,并对区块链技术存在的问题和未来发展提出展望。通过本文对区块链技术在物联网领域应用的综述,以及提出的

各领域中仍存在的问题,希望能够为相关研究提供更多可参考的价值。在物联网快速发展中,随着人们需求的增多以及技术的成熟性,区块链技术可以为物联网在不同的应用环境中带来更多安全隐私、数据可控、方便快捷的优势。通过本文的总结和探索,为区块链技术的发展和实施开辟新的途径。

参考文献

[1] Nakamoto S. Bitcoin: a peer-to-peer electronic cash system [EB/OL]. https://bitcoin. org/bitcoin. pdf: Bitcoin, 2008

[2] Yang R, Yu F R, Si P, et al. Integrated blockchain and edge computing systems: a survey, some research issues and challenges [J]. *IEEE Communications Surveys and Tutorials*, 2019, 21(2): 1508-1532

[3] 袁勇,王飞跃. 区块链技术发展现状与展望[J]. 自动化学报,2016,42(4): 481-494

[4] Xie J, Tang H, Huang T, et al. A survey of blockchain technology applied to smart cities: research issues and challenges[J]. *IEEE Communications Surveys and Tutorials*, 2019, 21(3): 2794-2830

[5] Zheng Z, Xie S, Dai H, et al. An overview of blockchain technology: architecture, consensus, and future trends [C]//2017 IEEE International Congress on Big Data, Honolulu, USA, 2017: 557-564

[6] Lin I C, Liao T C. A survey of blockchain security issues and challenges[J]. *International Journal of Network Security*, 2017, 19(5): 653-659

[7] Conti M, Kumar E S, Lal C, et al. A survey on security and privacy issues of bitcoin[J]. *IEEE Communications Surveys and Tutorials*, 2018, 20(4): 3416-3452

[8] Tschorsch F, Scheuermann B. Bitcoin and beyond: a technical survey on decentralized digital currencies[J]. *IEEE Communications Surveys and Tutorials*, 2016, 18(3): 2084-2123

[9] Li X Q, Jiang P, Chen T, et al. A survey on the security of blockchain systems[J]. *Future Generation Computer Systems*, 2017, 107: 841-853

[10] Sankar L S, Sindhu M, Sethumadhavan M. Survey of consensus protocols on blockchain applications [C]// 2017 4th International Conference on Advanced Computing and Communication Systems, Coimbatore, India, 2017: 1-5

[11] Mukhopadhyay U, Skjellum A, Hambolu O, et al. A brief survey of cryptocurrency systems [C]//2016 14th Annual Conference on Privacy, Security and Trust, Auckland, New Zealand, 2016: 745-752

[12] Wang S, Wang X, Zhang Y. A secure cloud storage framework with access control based on blockchain[J]. *IEEE Access*, 2019, 7: 112713-112725

[13] Liu T, Wu J, Li J, et al. Secure and balanced scheme for non-local data storage in blockchain network [C]// 2019 IEEE 21st International Conference on High Performance Computing and Communications; IEEE 17th International Conference on Smart City; IEEE 5th International Conference on Data Science and Systems, Zhangjiajie, China, 2019: 2424-2427

[14] Ding X, Yang J. An access control model and its application in blockchain[C]//2019 International Conference on Communications, Information System and Computer Engineering, Haikou, China, 2019: 163-167

[15] Ma M, Shi G, Li F. Privacy-oriented blockchain-based distributed key management architecture for hierarchical access control in the IoT scenario [J]. *IEEE Access*, 2019, 7: 34045-34059

[16] Wang S, Zhang Y, Zhang Y. A blockchain-based framework for data sharing with fine-grained access control in decentralized storage systems [J]. *IEEE Access*, 2018, 6: 38437-38450

[17] Chowdhury M J M, Colman A, Kabir M A, et al. Blockchain as a notarization service for data sharing with personal data store[C]//2018 17th IEEE International Conference on Trust, Security and Privacy in Computing and Communications/12th IEEE International Conference on Big Data Science and Engineering, New York, USA, 2018: 1330-1335

[18] Chen J, Xue Y. Bootstrapping a blockchain based ecosystem for big data exchange[C]// 2017 IEEE International Congress on Big Data, Honolulu, USA, 2017: 460-463

[19] Sedky G, Mougy A E. BCXP: blockchain-centric network layer for efficient transaction and block exchange over named data networking[C]//2018 IEEE 43rd Conference on Local Computer Networks, Chicago, USA, 2018: 449-452

[20] Huang Z, Su X, Zhang Y, et al. A decentralized solution for IoT data trusted exchange based-on blockchain[C]// 2017 3rd IEEE International Conference on Computer and Communications, Chengdu, China, 2017: 1180-1184

[21] Liang X, Zhao J, Shetty S, et al. Integrating blockchain for data sharing and collaboration in mobile healthcare applications [C]//2017 IEEE 28th Annual International Symposium on Personal, Indoor, and Mobile Radio Communications, Montreal, Canada, 2017: 1-5

[22] Zheng X, Mukkamala R R, Vatrapu R, et al. Blockchain-based personal health data sharing system using

cloud storage[C]//2018 IEEE 20th International Conference on e-Health Networking, Applications and Services, Ostrava, Czech Republic, 2018: 1-6

[23] Ito K, Tago K, Jin Q. i-Blockchain: a blockchain-empowered individual-centric framework for privacy-preserved use of personal health data[C]//2018 9th International Conference on Information Technology in Medicine and Education, Hangzhou, China, 2018: 829-833

[24] Wang S, Zhang D, Zhang Y. Blockchain-based personal health records sharing scheme with data integrity verifiable[J]. *IEEE Access*, 2019, 7: 102887-102901

[25] Huang J, Qi Y W, Asghar M R, et al. MedBloc: a blockchain-based secure EHR system for sharing and accessing medical data[C]//2019 18th IEEE International Conference on Trust, Security And Privacy In Computing And Communications/13th IEEE International Conference On Big Data Science And Engineering, Rotorua, New Zealand, 2019: 594-601

[26] Rajput A R, Li Q, Ahvanooey M T, et al. EACMS: emergency access control management system for personal health record based on blockchain[J]. *IEEE Access*, 2019, 7: 84304-84317

[27] Pussewalage H S G, Oleshchuk V A. Blockchain based delegatable access control scheme for a collaborative E-Health environment[C]//2018 IEEE International Conference on Internet of Things and IEEE Green Computing and Communications and IEEE Cyber, Physical and Social Computing and IEEE Smart Data, Halifax, Canada, 2018: 1204-1211

[28] Hossein K M, Esmaeili M E, Dargahi T, et al. Blockchain-based privacy-preserving healthcare architecture [C]//2019 IEEE Canadian Conference of Electrical and Computer Engineering, Edmonton, Canada, 2019: 1-4

[29] Azaria A, Ekblaw A, Vieira T, et al. MedRec: using blockchain for medical data access and permission management[C]//2016 2nd International Conference on Open and Big Data, Vienna, Austria, 2016: 25-30

[30] Tanaka K, Nagakubo K, Abe R. Blockchain-based electricity trading with digital grid router[C]//2017 IEEE International Conference on Consumer Electronics, Taibei, China, 2017: 201-202

[31] Hahn A, Singh R, Liu C, et al. Smart contract-based campus demonstration of decentralized transactive energy auctions[C]//2017 IEEE Power and Energy Society Innovative Smart Grid Technologies Conference, Washington, USA, 2017: 1-5

[32] Aitzhan N Z, Svetinovic D. Security and privacy in decentralized energy trading through multi-signatures, blockchain and anonymous messaging streams[J]. *IEEE Transactions on Dependable and Secure Computing*, 2018, 15(5): 840-852

[33] Kounelis I, Steri G, Giuliani R, et al. Fostering consumers´energy market through smart contracts[C]//2017 International Conference in Energy and Sustainability in Small Developing Economies, Funchal, Portugal, 2017: 1-6

[34] Mylrea M, Gourisetti S N G. Blockchain for smart grid resilience: exchanging distributed energy at speed, scale and security[C]//2017 Resilience Week, Wilmington, USA, 2017: 18-23

[35] Gai K, Wu Y, Zhu L, et al. Permissioned blockchain and edge computing empowered privacy-preserving smart grid networks[J]. *IEEE Internet of Things Journal*, 2019, 6(5): 7992-8004

[36] Guan Z, Si G, Zhang X, et al. Privacy-preserving and efficient aggregation based on blockchain for power grid communications in smart communities[J]. *IEEE Communications Magazine*, 2018, 56(7): 82-88

[37] Zhang D, Yu F R, Yang R. Blockchain-based distributed software-defined vehicular networks: a dueling deep Q-learning approach[J]. *IEEE Transactions on Cognitive Communications and Networking*, 2019, 5(4): 1086-1100

[38] Liu H, Zhang Y, Yang T. Blockchain-enabled security in electric vehicles cloud and edge computing[J]. *IEEE Network*, 2018, 32(3): 78-83

[39] Zheng D, Jing C, Guo R, et al. A traceable blockchain-based access authentication system with privacy preservation in VANETs[J]. *IEEE Access*, 2019, 7: 117716-117726

[40] Lei A, Cruickshank H, Cao Y, et al. Blockchain-based dynamic key management for heterogeneous intelligent transportation systems[J]. *IEEE Internet of Things Journal*, 2017, 4(6): 1832-1843

[41] Yang Z, Zheng K, Yang K, et al. A blockchain-based reputation system for data credibility assessment in vehicular networks[C]//2017 IEEE 28th Annual International Symposium on Personal, Indoor, and Mobile Radio Communications, Montreal, Canada, 2017: 1-5

[42] Lu Z, Liu W, Wang Q, et al. A privacy-preserving trust model based on blockchain for VANETs[J]. *IEEE Access*, 2018, 6: 45655-45664

[43] Liu X, Huang H, Xiao F, et al. A blockchain-based trust management with conditional privacy-preserving announcement scheme for VANETs[J]. *IEEE Internet of Things Journal*, 2019, 7(5): 4101-4112

[44] Liu C, Chai K K, Zhang X, et al. Adaptive blockchain-based electric vehicle participation scheme in smart grid platform[J]. *IEEE Access*, 2018, 6: 25657-25665

[45] Su Z, Wang Y, Xu Q, et al. A secure charging scheme for electric vehicles with smart communities in energy blockchain[J]. *IEEE Internet of Things Journal*, 2019, 6(3): 4601-4613

[46] Jin Z, Wu R, Chen X, et al. Charging guiding strategy for electric taxis based on consortium blockchain[J]. *IEEE Access*, 2019, 7: 144144-144153

[47] Dorri A, Kanhere S S, Jurdak R. Towards an optimized blockchain for IoT[C]//2017 IEEE/ACM 2nd International Conference on Internet-of-Things Design and Implementation, Pittsburgh, USA, 2017: 173-178

[48] She W, Gu Z, Lyu X, et al. Homomorphic consortium blockchain for smart home system sensitive data privacy preserving[J]. *IEEE Access*, 2019, 7: 62058-62070

[49] Lin C, He D, Kumar N, et al. Homechain: a blockchain-based secure mutual authentication system for smart homes[J]. *IEEE Internet of Things Journal*, 2020, 7(2): 818-829

[50] Ma Z, Wang X, Jain D K, et al. A blockchain-based trusted data management scheme in edge computing[J]. *IEEE Transactions on Industrial Informatics*, 2020, 16(3): 2013-2021

[51] Liu Y, Yu F R, Li X, et al. Decentralized resource allocation for video transcoding and delivery in blockchain-based system with mobile edge computing[J]. *IEEE Transactions on Vehicular Technology*, 2019, 68(11): 11169-11185

[52] Kang J, Yu R, Huang X, et al. Blockchain for secure and efficient data sharing in vehicular edge computing and networks[J]. *IEEE Internet of Things Journal*, 2019, 6(3): 4660-4670

Blockchain technology applied to the Internet of Things: development and prospect

Ye Xinyu*, Li Meng*,**, Zhao Chengze*, Si Pengbo*,**, Sun Yang*, Zhang Yanhua*,**

(*Faculty of Information Technology, Beijing University of Technology, Beijing 100124)

(**Beijing Laboratory of Advanced Information Networks, Beijing 100124)

Abstract

In recent years, with the increasing rise and commercial application of digital currency, blockchain technology has attracted attention and obtained recognition from government departments, industry and academia. At the same time, the rapid development and extensive coverage of mobile communication network have prompted the Internet of Things (IoT) to gradually enter daily life, which has greatly improved work efficiency and quality of life. However, there are still some problems in the IoT scenario, such as low energy efficiency and poor data transmission security. The blockchain technology can help to promote the better development and popularization of the IoT. In this paper, we systematically review the application of blockchain technology in the IoT. Initially, the background knowledge and related researches are introduced. Then, we propose an infrastructure model of blockchain, and elaborate the state-of-the-art and related features of blockchain technology applied in various scenarios of the IoT. Finally, some challenges and future development trends are discussed.

Key words: blockchain, digital currency, Internet of Thing (IOT), consensus mechanism, smart contract