区块链技术的应用进展与发展趋势*

何小东 易积政** 陈爱斌
(中南林业科技大学计算机与信息工程学院,长沙 410004)

摘 要:从 2015 年以来,作为比特币底层技术的区块链技术,开始成为继物联网、云计算、大数据和人工智能之后,人们争相研究和应用的热点,并被 Gartner 列为未来十大技术发展趋势之一。区块链具有去中心化、共识机制、不可篡改、智能合约等特性,是一种全新的、去中心化架构的计算范式。本文在分析、比较国内外区块链研究现状和简要介绍区块链关键技术(原理)的基础上,梳理了近几年区块链技术的最新应用进展,分析当前区块链应用面临的主要问题,对区块链未来的应用前景与发展趋势进行展望,进而为未来区块链的研究和应用提供有益的启发和借鉴。

关键词:区块链技术;去中心化;共识机制;不可篡改;智能合约
中图分类号:TP315 **文献标识码**:A doi:10.16507/j.issn.1006 - 6055.2018.12.007

Application Progress and Development Trend of Block Chain Technology*

HE Xiaodong YI Jizheng** CHEN Aibin
(School of Computer and Information Engineering, Central South University of Forestry and Technology, Changsha 410004, China)

Abstract: Since 2015, block chain technology, as the bottom technology of Bitcoin, has become a hot spot of research and application following Internet of Things, Cloud Computing, Big Data and Artificial Intelligence, and has been listed as one of the ten future development trends by Gartner. Block chain has several characteristics, such as decentralization, consensus mechanism, non-tampering, intelligent contract and so on. It is a new and decentralized computing paradigm. After analyzing and comparing research status of block chains at home and abroad, and briefly introducing the key technologies (principles) of block chains, this paper combs the latest application progress of block chain technology in recent years and analyzes the main problems faced by the current application of block chain. The paper further looks forward to the application prospect and development trends of block chain, and devotes itself to providing useful inspirations and references for the research and application of block chain in the future.

Key words: block chain technology; centralization; consensus mechanism; non tampering; smart contract

1 引言

自 2015 年以来,作为继工业革命和互联网之后,可能引发颠覆式产业创新的一种新技术——区块链(Block Chain,简称 BC)技术,在全球经济、金融、物联网以及各个学术领域引发了高度关注。

2018-08-13 收稿,2018-12-10 接受,2018-12-25 网络发表
* 国家自然科学基金(61602528),国家 948 项目(2014-04-09),湖南省科技计划重点研发基金(2016SK2027)资助
** 通讯作者,E-mail:kingkong148@163.com

由此 2015 年被人们称为世界区块链元年。2016 年被称为是中国的区块链元年,2017 年是区块链从实验室走向应用的元年,区块链也从 1.0 时代迈入了 3.0 时代[1],2018 年则是区块链应用与研究高速发展和推进的一年。

那么,究竟什么是区块链呢? 区块链这一概念最早在 2008 年中本聪[2]的比特币白皮书中提出,起源于数字货币——比特币。比特币作为一种加密货币,只是建立在区块链技术上的一种应用,区块链是其底层技术[3],是利用块链式数据结构来验证与存储数据、利用节点共识算法来生成和更新数据、利用密码学原理保证数据传输和访问的安全、利用智能合约来编程和操作数据的一种基础架构与计算范式[4]。简单地说,区块链就是一种去中心化的分布式账本数据库,具有去中心化、不可篡改、共识算法、智能合约四大特点[5]。其开放、自治、数据可追溯等特性,能解决金融、教育、电子政务、文件存储、追溯、防伪等很多领域的技术难点,已成为继物联网、大数据、人工智能之后,产、学、政、资、研的新热点,并被 Gartner 列为十大技术发展趋势。

为全面、系统地了解区块链技术研究、应用及产业等方面的最新进展和发展趋势,本文在比较国内外区块链研究现状和简要介绍区块链关键技术(原理)的基础上,梳理了近几年来区块链的最新应用进展,分析了区块链应用面临的主要问题,展望了区块链未来的发展趋势和应用前景,为后续区块链的进一步研究和应用提供有益参考。

2 区块链的研究现状

鉴于区块链巨大的应用前景,许多国家开始从国家层面设计区块链的研究与发展规划,先后出台了一系列鼓励区块链技术发展和应用的政策[6]。美国、欧盟、日本等发达国家正在积极推动区块链技术理论研究、标准制定、应用落地等相关工作。美国证券交易所已批准公司可以基于区块链技术进行股票交易,并且一些州已对区块链技术立法[7];日本经济产业省召开金融会议,设置专题研究区块链技术的未来发展与影响[8];2017 年 9 月,澳大利亚、英国等多国将区块链纳入国家数字经济战略;2016 年初,英国政府发布《分布式账本技术:超越区块链》研究报告,从国家层面对区块链技术的未来发展及应用进行分析并给出建议[9]。国际上还成立了不少区块链联盟,如 R3 联盟、Hyper Ledger 等。

相比之下,我国的区块链相关技术研究起步较晚,还处于萌芽阶段。但近年来很快上升到国家战略层面,于 2016 年底被写入《“十三五”国家信息化规划》。该规划首次将区块链技术列入需要超前布局的战略性前沿技术。到 2017 年 6 月由工信部指导的首个区块链标准《区块链参考架构》发布;2017 年 9 月,国务院印发的《国家技术转移体系建设方案》指出,要加快区块链科技成果的转移转化;同时,中国人民银行在《中国金融业信息技术“十三五”发展规划》中强调,要加强研究区块链和金融科技;2017 年 10 月,央行推动的基于区块链的数字票据交易平台测试成功;2018 年 5 月,中国计算机学会(CCF)为搭建产业和学界互动的专业平台,推动区块链方面的人才培养和技术应用,率先发起成立了区块链专业委员[10];2018 年 10 月在杭州召开的 2018 年中国计算机大会(CNCC2018)开设了两个区块链专题论坛。

从理论研究现状看,在 CNKI 中检索“区块链”,并在 Web of Science 以“block chain”为检索词进行主题精确检索的结果显示,美国在研究论

文数量上位列第一,其次是英格兰和德国。我国相关研究虽然起步较晚,但数量增长较快,相关研究论文数量 2015 年仅有 15 篇,2018 年已剧增至 2794 篇。目前仍处于研究起步期,主要是以会议论文为主(73.5%),且大多局限于对技术原理的讨论,尤其集中在比特币环境,理论研究明显落后于实践应用的发展[11]。

3 区块链的关键技术

3.1 区块链加密技术及机制

区块链利用块链式数据结构来验证与存储数据,利用密码学的方式保证数据传输和访问安全,其理论是基于密码学的,主要涉及到哈希(Hash)算法和 Merkle 树。

1)哈希(Hash)算法

哈希(也称为散列)算法将任意长度的输入值变换为具有固定长度的二进制值。这个二进制值称为哈希值(也称为散列值),可用于检验数据的完整性。著名的工作量证明算法(Proof of Work,PoW)[2]、Merkle 树都是哈希算法的应用。区块链不保存原始数据,而是保存该数据的哈希值,Merkle 树中的节点信息经两次 SHA256 哈希运算(输出长度为 256 位)得到[12]。此外,区块链中常用的签名也是由私钥和需要被签名的数据经哈希运算而成。

2)Merkle 树

Merkle 树基于数据哈希构建[13],多用于验证和文件对比,特别是在分布式环境下,可大大减小数据的传输量和计算的复杂度。其数据结构是一棵树,一般为二叉树,也可以为多叉树;其叶子节点是数据块(如文件或文件集合)的哈希值,非叶子节点则是其所有子节点的哈希值。

区块链中的每个区块都包含了记录于该区块的所有交易,Merkle 树对这些交易进行归纳表示,同时生成该交易集合的数字签名(图 1)。

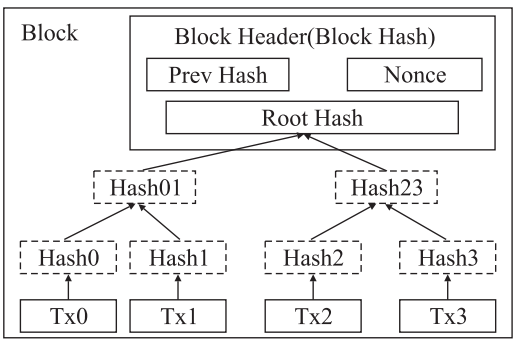

图 1 Merkle 树中的交易哈希[14]

Fig. 1 Transaction hash in Merkle tree[14]

3)时间戳

区块链采用时间戳技术来解决数字货币的“重复支付”问题。即系统给每一笔交易盖上正确的时间戳[14],以此证明在这个时刻这笔交易确实发生,交易中资金的所属权已经转移,之前的资金所有者不能再次使用这笔资金。另外,每一个区块也会盖上正确的时间戳,从而形成一个按时间顺序发展的正确链表。

4)工作量证明(PoW)机制

所谓工作量证明[2],是指要找到一个合理的区块哈希值,需要进行大量计算,若找到这个值,就说明该节点确实经过了大量计算。由于验证只需对结果值进行一次哈希运算,因此,PoW 的验证效率很高。

5)权益证明机制

相比 PoW 浪费大量的算力,权益证明(Proof of Stake,PoS)根据货币持有量和时间来分配相应的利息,仅需要少量计算就能维持区块链的正常运转。但是这种机制存在一点不足,即区块的产生没有消耗大量算力,导致这种机制下的价值来源难以确定。

3.2　区块链的架构

区块链由一系列加盖了时间戳的有效交易区块组成[14]。每个区块都包含了前一个区块的哈希值,是对前一个区块的增强,从创世区块开始逐个链接到当前区块,形成区块链。每一个区块都按照时间顺序在上一个区块之后产生,包含了当前一段时间内的所有交易信息和区块元数据,一旦被确认,几乎不能做修改操作(图 2)。

在区块链中,区块是指一种数据结构,由区块元数据和区块体两部分组成。其中,区块元数据记录的是区块的元数据信息,区块体记录的则是从上一区块产生到此区块创建之间所发生的所有交易。区块链的基本框架如图 3 所示。从下至上包括数据层、网络层、共识层、激励层、合约层和应用层共六层[5];基础数据传输到数据层,在区块主体中组成数据列表,用区块主体中的 Merkle 树记录,区块主体与存储 Merkle 根、父哈希、时间戳等数据的区块头共同形成区块,多个区块通过区块头的数据形成链式结构;网络中的节点收到上传数据后,通过 P2P 网络向全网广播,各节点自动对其验证。

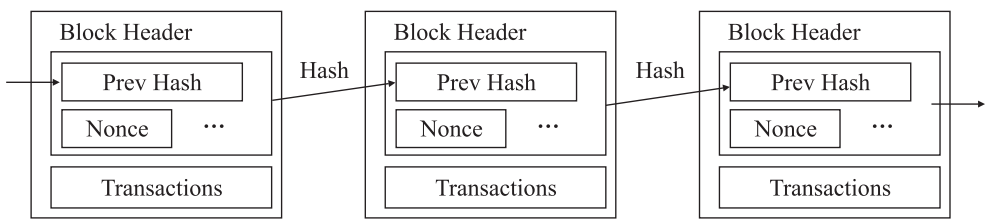

图 2　区块链及其结构[14]

Fig. 2　Block chain and its structure[14]

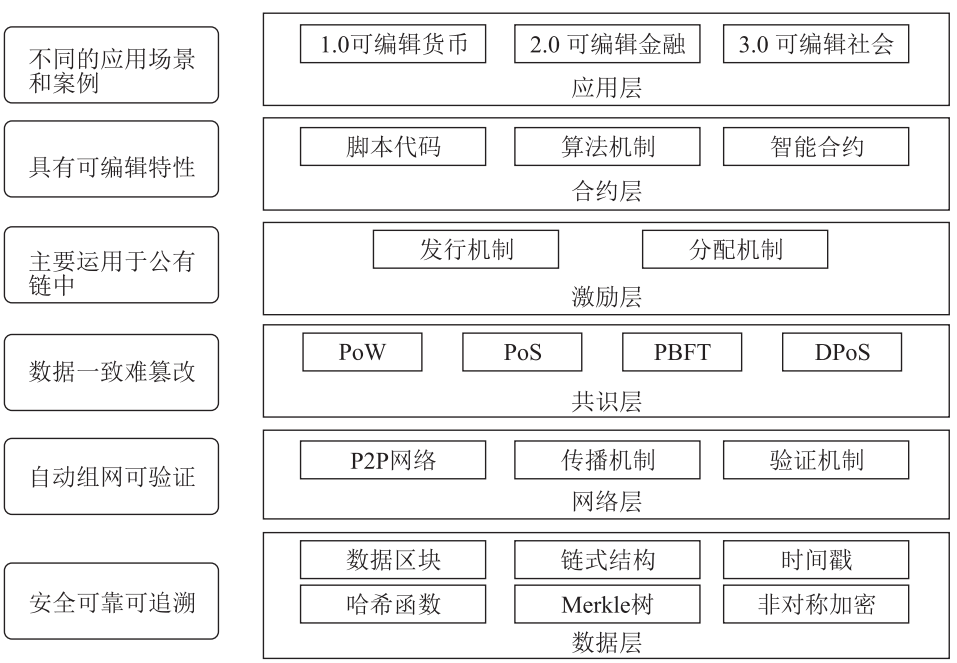

图 3　区块链的基本框架[4]

Fig. 3　Basic framework of block chain[4]

3.3 区块链的建立

中本聪[2]在其比特币白皮书中,详细地介绍了区块链系统的建立过程:

第 1 步:新的交易向全网所有节点广播;

第 2 步:每个节点把收到的交易都写入到一个区块中;

第 3 步:每个节点都在新的区块上进行计算,寻找一个工作量证明解;

第 4 步:某个节点找到工作量证明解时,就把其所在区块向全网进行广播;

第 5 步:其他节点收到这个区块的广播后对其进行验证,只有所有交易都被验证是有效且未被使用的之后,该区块才能被认可;

第 6 步:每个节点通过将此区块的哈希值作为父哈希值来进行下一个区块的计算,表示节点认可了此区块有效。

一般情况下,一笔交易必须经过至少 6 次确认(在此区块之后每产生一个区块就是 1 次确认),才能最终在区块链上被承认是合法交易。6 次确认后要想修改记录,代价太大,所以一般认为区块链上数据不可篡改。

3.4 共识机制

共识机制是指分布式系统中的一致性问题,其核心是在某个协议(共识算法)保障下,在有限的时间内,使得指定操作在分布式网络中是一致的、被承认的、不可篡改的。在区块链系统中,特定的共识算法用于解决去中心化多方互信的问题[3]。为适应不同的应用场景,区块链共识机制集中于优化系统的可扩展性、运行效率和容错等方面。

共识算法通常分为两类。一类是确保各个节点之间的数据绝对一致,用于解决可信节点间网络通信问题的算法,如 Paxos、Raft 算法,以及拜占庭容错算法(BFT)等。另一类则是通过经济利益和算力,鼓励对系统的贡献及提高不可信节点成本的算法,如上述 PoW、PoS 算法等,这类算法通过提供算力或持有权益来平衡利益[14]。

3.5 智能合约

智能合约(Smart Contract)这个术语由密码学家 Nick Szabo[15]提出,是一种计算机协议,用于促进、验证或者执行合约的协商或履行,或使合约条款不必要[16]。智能合约的工作原理与编程语言中的 If – Then 句类似,当满足一个预先编好的条件时,智能合约的相应条款就被触发执行。区块链技术为智能合约的运行提供了可信的执行环境,将其作为一段写在区块链上的代码,一旦某个事件触发合约中的条款,代码即自动执行。智能合约允许在不依赖第三方的情况下进行可信、可追踪且不可逆的合约交易。

目前,较为成熟的以太坊和 Hy-perledger Fabric 框架均包含智能合约,支持图灵完备的语言,在其基础上可实现多种智能合约,包括差价合约、储蓄钱包合约、多重签名合约等,无须依赖第三方或中心化机构,具有较高的效率与准确性。

4 区块链的应用进展

区块链因其实现了去中心化的共识,同时具有优秀的不可篡改、链式存储等安全特性,加上智能合约,使其在各行各业得到了广泛地应用。尤其是在那些参与方众多、交易链条长、中心化效率低、缺少信任的场合,如金融、认证和溯源等,近年来对区块链技术的刚需非常明显。下面归纳了区块链在几个主要领域的应用。

4.1 在银行金融业中的应用

区块链作为一种数字化、安全及防篡改的技术可跨国界而无需中介,以超低费率和几乎瞬时

的方式支付,能创建一个更直接的支付流,为全球的现金交易服务。瑞士的 UBS 银行和英国的巴克莱银行采用区块链来加速推动后台系统功能以及清结算能力;Thought Machine 集团开发了基于私链技术以及加密总账簿的 Vault OS 系统,各种规模的银行都能使用这个安全的点对点金融系统;R3CEV 公司正在为金融行业开发定制化的区块链应用;百度金融也于近期与其他金融机构联合发布了支持区块链技术的 ABS 项目。

在银行的跨境支付业务中,因为双方信用主体不同,用户需要提交大量的身份证明资料,双方银行也需要向中间机构核对信息。而利用区块链可直接建立付款人与银行、银行与银行之间的信任关系,无须中间代理机构,付款人与银行可通过智能合约约定相关的权利义务,实现实时转账和自动清结算。监管机构也可清晰地审查相关的交易记录,识别洗钱等违法行为。对个人方、银行方和监管方来说,区块链有利于降低成本、提升效率。

环球银行金融电信协会联合全球多家银行启动的全球付款创新项目 SWIFT GPI(Global Payments Innovation)已在研究区块链技术与跨境支付的高度融合。我国招商银行在 2016 年也开发了基于区块链的跨境直联清算系统。而在近期,汇丰银行与 ING 银行为美国农业应用区块链技术,完成了首个实时贸易的融资交易。

4.2 在追溯和防伪中的应用

区块链技术的去中心化、数据可追溯和不可篡改等特性,使它不依赖于统一的中央数据库,用做产品防伪具有天然优势,和存储量大、安全性高、使用方便的 IC 卡芯片相结合形成的防伪系统具有极高的不可伪造性,且成本低廉、易于实施[17]。

此外,区块链技术用于产品追溯,可使产品生产、加工、消费各个环节的参与者都无法掺假,且有可信性。英国的 Provenance 软件公司采用由传感器或 RFID 生成的标签将食材记录在区块链上,保证食材的生产日期等数据的真实可靠,避免了信息提供者可能选择性屏蔽对自己不利的基础信息[18]。阿里应用区块链打造透明可追溯的跨境食品供应链,将区块链技术应用于食品的产供销各个环节,使数据依赖于机器采集和机器信任,从而解决食品安全领域存在的各种难题。

由于区块链中每个区块都带有时间戳,这种时序数据强化了信息的不可篡改性,对产品追溯起到很大作用[19],不仅能保证数据的原始性,也降低了交易追溯的成本。每个区块通过哈希算法生成的哈希值来标识自身的唯一性。如果攻击者想篡改数据,就必须修改所有区块中的数据,对于一个成熟的区块链来说,这是不可能的。

4.3 在文件存储中的应用

目前,绝大多数的文件存储方式是集中存储在本地,或者是使用云存储。后者的数据在中心化的服务商处同样面临着被攻击、滥用和泄露的威胁。而区块链技术通过世界各地的闲置存储和带宽所构成巨大节点网络,可以实现真正的分布式存储。如星际文件系统(IPFS),其文件内容转化为哈希值存储在各个节点中,任何内容的修改都会反映在哈希值上。存储的文件都抽象成特殊的 IPFS 目录供检索,大文件切分成小块,下载时从多个服务器同时获取,不设中心服务器,安全性高、成本降低[20]。参与服务者通过对数据共享的贡献,自动获取并分配相应的收益。据估计,到 2027 年全球 10% 的 GDP 将会通过区块链技术存储[21]。

4.4 在物联网中的应用

物联网技术近几年取得了显著发展,并与互

联网相结合,实现了智能化的管理与操作。包括 IBM 在内的跨国公司已经在物联网投入了海量资源,而区块链技术正成为解决其中核心问题的关键。

对于潜在数量在百亿级的联网设备而言,使用传统的中心化机制解决节点信任问题是不现实的。区块链创建的共识网络则无需信任单个节点。IBM 公司正致力于让每个联网设备都能基于区块链技术实现自我管理,无需人工维护。如:让所有家居物件自发自动地与其他物件或外界进行金融活动,让智能电表通过调节用电量和频率形成更优惠的电费账单等。

另外,区块链的去中心化能为物联网提供安全的环境。一是去信任化以及智能合约增强了物联网中的互信机制;二是时序数据和数据加密可保障物联网中的数据安全[22]。

4.5 在资产版权保护中的应用

对于大量原创内容,确权成本高,维权周期长;加上版权授予和代理的链条长,创作回报周期也长。利用区块链去中心化的记录,结合计算机视觉、自然语言等领域相关技术,能实现低成本的内容确权;利用智能合约能方便作者对作品进行定价和授权,同时自动跟踪、记录每次被使用和交易的情况,并自动分配收益,缩短回报周期。

目前,已经有不少区块链版权平台提供数字资产与版权交易功能,帮助数字资产实现高效流转,激活资产价值。今后,线下实体资产也可在区块链上登记与交易,形成流动的资产网络。

4.6 在身份认证中的应用

传统的线下证件容易遗失、被盗取和伪造,互联网上的用户身份和隐私也存在安全隐患,因为用户数据大多存储在应用商的服务器上,缺少第三方监管,用户身份数据容易泄露或者被滥用,如最近 Facebook 的用户数据泄露事件。利用区块链技术,用户可以拥有唯一的、不可篡改的身份 ID,集合多维度信息,用于验证、授权和交易,降低隐私泄露风险[23]。

微软、IBM 等机构已在合作研发去中心化的身份识别系统(Decentralized IDs,DID)。我国中钞区块链技术研究院也推出了中钞络谱系统,对数字身份、可信数据、数字凭证等进行可信登记,向调用这些信息的第三方提供身份、时间戳、凭证登记等,可验证、审计和追溯,在政府监管和司法鉴定等场景中有较好的应用[14]。我国公安部已经把区块链技术应用于案件管理,存储身份证据链,将区块链贯穿身份录入的全过程。

4.7 在教育领域中的应用

当前人们对某一特定学科的精通程度,需要由受认可的大学颁发文凭或证书来证明。这种证书证明方式具有一定的缺陷,如文凭造假、精英教育的不公平性等。为此,美国的 Holbertson 软件技术培训学校将区块链技术应用于认证学历证书,确保学生声称在学校通过的课程都是实际被鉴定合格的。同时避免人工检查,减少纸质文件,节约了时间和成本。基于区块链的教育系统保证每个人的考试成绩及课程设置都被永久且不可更改地记录和存储下来。

4.8 在供应链管理中的应用

在供应链领域,可应用区块链记录参与各方的商品日期、位置等信息,形成一个不可篡改的公共账本,生产方、监管方和公众都能追踪相关信息,这在跨境物流等对安全性要求高的场景尤为重要。采用区块链,交易会被永久性、去中心化地记录下来。如 Provenance 公司已为原材料和产品建立可追溯系统,Skuchain 公司则为 B2B 交

易和供应链市场研发了一个区块链产品。

阿里巴巴和京东也在研发区块链供应链系统。其中阿里巴巴联合政府、行业协会、质检机构等打造了一个全球溯源计划,可追踪进口商品的生产、通关、运输等全链路;而京东则联合清华大学等成立了中国安全食品区块链溯源联盟[19],用于食品的追踪和安全合作。

5 区块链应用面临的问题

作为近年来兴起的新技术,区块链虽然得到了快速发展,其应用场景和领域也非常广泛,但区块链技术总体还处于发展的初期,存在诸多问题和挑战。除了政策和公众认知方面,区块链还在安全、资源和效率等方面存在一些可能制约其应用和发展的问题。

5.1 安全问题

1)**51% 攻击问题**。节点只要掌握全网超过 51% 的算力,就能成功篡改和伪造区块链数据。以比特币为例,据统计中国大型矿池的算力已占全网总算力的 60% 以上,理论上这些矿池可以通过合作实施 51% 攻击,从而实现比特币的双重支付。虽然,实际系统中为掌握全网 51% 算力所需的成本投入远超成功实施攻击后的收益,但 51% 攻击的安全性威胁始终存在[23]。

2)**隐私保护问题**。区块链系统内各节点并不完全匿名,而是通过地址标识(如比特币公钥地址)来实现数据传输。虽然地址标识并未直接与现实世界的实体身份关联,但区块链数据是完全透明的,随着抗匿名身份识别技术的发展,可实现部分重点目标的定位和识别。另外,在完全去中心化的环境中,因缺乏有效的安全机制,可能因数据透明造成隐私泄露[24]。

3)**链外数据输入问题**。在区块链 2.0 乃至 3.0 时代,基于区块链的智能合约更加完备,为区块链增加了应用领域,但同时也增加了与现实世界数据交互的机会,大量来自链外的数据输入可能会给区块链的应用带来安全隐患。如使用区块链进行产品溯源应用时,在理论上还无法证明,可避免从源头的仿冒产品以“正品”的数据被写入区块链[24]。

4)**性能与加密安全问题**。为了提升性能,区块链在加密安全方面可能会做一些让步。如为提升交易处理性能,而在非可信环境中使用非拜占庭容错(BFT)的一致性算法,将给区块链的应用带来了安全隐患。

5.2 资源与效率问题

1)**资源浪费问题**。区块链产业属于高能耗型产业,基于 PoW 共识机制的区块链系统依赖区块链节点贡献的算力,但只有部分算力得到了奖励,其他算力都是在做无用功,资源浪费很大,影响了其在各个领域的推广应用。

2)**区块膨胀问题**。区块链要求系统内每个节点都保存一份备份,这对于海量数据存储来说要求过高。以比特币为例,完全同步自创世区块至今的区块数据需要约 120GB 存储空间,适用于更大规模的解决方案还有待研发[25]。

3)**交易效率低问题**。交易效率主要受到区块产生时间和区块大小的影响,同样以比特币为例,其交易速度为 7 笔/秒,这将限制区块链在一些高频交易场景(如金融业)中的应用,不便进行实时交易。

5.3 其他问题

1)**新共识机制问题**。这种新共识机制能使各自治节点激励相容、能自发地实施区块数据的验证和记账,提高区块链系统内部对非理性行为的验证效率,从而抑制各种安全性攻击。

2)**算力瓶颈问题**。区块链的安全性和不可篡改性是由 PoW 共识机制的强大算力所保证的,任何对于区块数据的攻击或篡改,都必须重新计算该区块以及其后所有区块的 SHA256 难题,并且计算速度要使得伪造链长度超过主链。将区块链与人工智能技术相结合,发挥人工智能优势,并采用新的共识机制,能进一步提高区块链的算力。

3)**与云平台结合问题**。目前云计算提供商已提出 BaaS(Blockchain as a Service)和 BaaP(Blockchain as a Platform)服务,且许多区块链开源项目都支持在公有云上直接部署。

4)**统一标准问题**。目前相关技术与行业还未有统一标准,具体包括:基础标准、业务和应用标准、过程和方法标准、可信和互操作标准、信息安全标准等,其中信息安全标准最为重要[24]。

6 区块链的发展趋势

随着基础理论、方法、技术和平台的进一步发展成熟,区块链将伴随大数据、云计算、物联网和人工智能的兴起,迎来新一轮的技术革命浪潮,将更加深刻地改变未来数字经济社会的价值形态,并带来更广阔的应用前景。但同时也应看到,区块链仍然有一系列问题有待解决。如:安全性问题、可扩展性问题、还有在完全去中心化的自治环境中,如何建立有效的安全应急及责任机制等。

6.1 技术方面

我国学者在区块链的技术研发方面已经取得了不少有影响的研究成果。以太坊、北航链等区块链平台已开始进入实用阶段。未来预计将在可扩展性、加密算法、隐私保护能力等方向有较大发展。

1)**增加可扩展性**。可扩展性是指区块链系统处理高业务量的能力,它决定了区块链在各个行业的应用深度。在考虑去中心化和安全的前提下,区块链的可扩展性主要受制于三个方面[14]:一是分布式区块链网络的节点传输延迟,因为整个网络同步的效率取决于网络中延迟最长的节点;二是账本区块的一致性问题,影响区块链吞吐量的核心参数是区块容量和区块间隔时间,如果区块间隔时间过小,可能会由于不同节点来不及完全同步最新的区块广播而产生不同的新区块,从而造成严重的分叉问题,影响区块链的实际可用性;三是受节点性能限制,目前主流的公有链如比特币、以太坊等仍然使用 PoW 共识机制,节点需要消耗大量的计算资源来进行哈希运算以竞争记账权,从而影响效率。

2)**使用抗量子加密算法**。随着量子计算技术的发展,区块链的非对称加密机制将有被破解的可能性,即通过由主流非对称加密算法生成的公钥地址来反推出账户的私钥。如果成功,整个区块链体系的安全基础就会崩溃[4]。

3)**进一步提升隐私保护能力**。随着区块链应用的广泛推广,如何保护区块链数据的隐私将变得十分重要。而比特币、以太坊等公有链完全公开化的账本,已难以满足人们在应用场景中对隐私的更高需求。为此,在新兴的区块链中,将使用无须泄露数据即可证明数据真实性的所谓“零知识证明”技术,即证明者(被验证者)能够在不向验证者提供任何有用信息的情况下使其相信某个论断是正确的协议。2017 年以太坊平台在拜占庭分叉过程中,就引入了使用同态加密的零知识证明技术 zkSNARKs。

4)**智能合约智能化**。智能合约及其应用逻辑大多根据预定义场景或“IF –”类型的条件来

响应规则,但不能实现具有一定自主决策功能的“智能化”。未来的智能合约将能根据未知场景的“WHAT – IF”推演、计算实验和自主决策等功能实现“智能化”[26]。

5)**提高智能合约的安全性**。智能合约的本质是算法合同,即当事双方同意依据一定的计算机算法来确定合同的内容、订立并履行合同的行为。智能合约是“代码即合约”,其合约代码常蕴含着法律关系和利益交易,因此在可信和执行安全方面有更高的要求。对一个被触发执行的合约程序,要保证程序运行的正确性和合约参与方的机密性。未来将有望采用一些新的密码计算技术(如全同态加密技术(Fully Homomorphic Encryption,FHE))来保证区块链中数据的隐私以及在不可信环境中计算的正确性。

6)**多种共识机制进行融合与优化**。如前所述,共识机制被用于解决分布式系统一致性问题。为适应不同的应用场景,未来的区块链共识机制将集中于优化系统的可扩展性、运行效率和容错性等,主要通过将各种共识机制进行融合实现[27]。如在分层/分片方案中,最上层的主链使用 PoW 机制,以确保全局共识的有效性,而在相对小范围的分片中,则使用 PoS 或者拜占庭容错 BFT 算法[23],以实现更高效率的共识,如以太坊就计划引入基于校验器管理和约(VMC)分片方案。

7)**采用并行化技术**。并行化在传统分布式系统中被用于解决吞吐量问题,这在未来的区块链方案中有两种实现方式:一是将节点和交易分区来进行并行化处理;二是使用有向无环图 DAG(Directed Acyclic Graph)将区块生成过程并行化。在 DAG 中,每个单元允许包含多个父单元(不允许成环),从而容纳更多交易并更快得到确认。

8)**研究算力更加“有用”的共识机制**。质数币(Prime coin)提出,把寻找下一个符合条件质数的过程作为“工作量证明”,这样就可能提供一种新的共识机制,即要求各节点在共识过程中,找到素数的最长链条(如双向双链),而不是无意义的 SHA256 哈希值[28]。

6.2 应用方面

麦肯锡研究报告指出,区块链是最有潜力触发第五轮颠覆性革命浪潮的核心技术,未来区块链的各种新应用场景将不断涌现[29]。

1)组建区块链大联盟,制订行业标准。目前 R3CEV 正联合 40 多家国际领先银行,建立行业监管及相应的技术标准。

2)区块链应用从单纯的数字货币过渡到广泛的社会领域。Capital One 及 Visa 已对金融科技公司进行区块链方面的战略投资;而 UBS、花旗、德意志及巴克莱也成立了区块链实验室,以测试不同的区块链应用场景。

3)从“区块链 3.0”升级到“应用 on 区块链”,即全部业务逻辑均在区块链上运行,避免可信数据输入问题。

4)传统业务正以各类智能合约的形式,从数据中心迁移到区块链的各个记账节点,实现真正的“去中心化”。

5)用区块链把物理世界及人的关联关系,纳入整个区块链生态系统中。这个生态系统可以存储个人各种数据乃至人类思想和意识。

6)基于区块链构建一种新型的价值传递体系。所有参与方通过付出“成本”来获取激励,维持关键数据及业务规则的共识,并以此来作为检验区块链应用是否能真正解决需求的标准。

参考文献

[1]SWAN M. Blockchain:Blueprint for a New Econo-

my[M]. CA:O' Reilly Media Inc. ,2015.

[2]NAKAMOTO S. Bitcoin:A Peer-to-Peer Electronic Cash System[EB/OL]. 2009-10-06. https://bitcoin. org/bitcoin. pdf.

[3]单进勇,高胜. 区块链理论研究进展[J]. 密码学报,2018,5(5):484-500.
SHAN J Y,GAO S. Block Chain Theory Research Progress [J]. Journal of Password,2018,5(5) : 484-500.

[4]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.
YUAN Y, WANG F Y. Development Status and Prospect of Blockchain Technology [J]. Journal of Automation,2016,42(4):481-494.

[5]谢辉,王健. 区块链技术及其应用研究[J]. 信息网络安全,2016(9):192-195.
XIE H,WANG J. Block Chain Technology and Its Application [J]. Information Network Security, 2016(9):192-195.

[6]HAMIDA E B,BROUSMICHE K L,LEVARD H, et al. Blockchain for Enterprise:Overview,Opportunities and Challenges[EB/OL]. [2018-02-08]. https://hal. archives-ouvertes. fr/hal-01591859/.

[7]YLI-HUUMO J,KO D,CHOI S,et al. Where is Current Research on Blockchain Technology? -A Systematic Review[EB/OL]. [2018-02-08]. http://journals. plos. org/plosone/article? id = 10. 1371/journal. pone. 0163477.

[8]唐文剑. 区块链国内外发展快速扫描[J]. 金融电子化,2016(3):66-68.
TANG W J. Rapid Scanning of Block Chain Development at Home and Abroad [J]. Financial Electronization,2016(3):66-68.

[9]Government Office of Science. Distributed Ledger Technology:Beyond Blockchain[EB/OL]. 2017-09-15. https://www. gov. uk/government/uploads/system/uploads/attachment-data/file/492972/gs-16-1-distributed-ledger-technology. pdf.

[10]中国计算机学会. 中国计算机学会成立区块链专业委员会[J]. 中国计算机学会通讯,2017,14(6):43-50.
CCF. The China Computer Federation Established the Block Chain Professional Committee [J]. Communication of the Chinese Computer Federation,2017,14(6):43-50.

[11]韩秋明,王革. 区块链技术国外研究述评[J]. 科学进步与对策,2018,35(2):154-160.
HAN Q M,WANG G. Overseas Research Review on Block Chain Technology [J]. Scientific Progress and Countermeasures,2018,35(2):154-160.

[12]WOLRICH G M,YAP K S,GUILFORD J D,et al. Instruction Set for Message Scheduling of SHA256 Algorithm:US8838997B2[P]. 2012-09-28.

[13]SZYDLO M. Merkle Tree Traversal in Log Space and Time[J]. Lecture Notes in Computer Science,2004,3027:541-554.

[14]何蒲,于戈,张岩峰,等. 区块链技术与应用前瞻综述[J]. 计算机科学,2017,44(4):1-7.
HE P,YU Y,ZHANG Y F,et al. A Review of Block Chain Technology and Application Prospects [J]. Computer Science,2017,44(4):1-7.

[15]WIKIPEDIA. Smart Contract[EB/OL]. 2017-03-18. https://en. wiki pedia. org/wikw/Smart Contract.

[16]CASSANO J. What are Smart Contracts? Cryptocurrency's Killerapp[N/OL]. (2014-09-17)[2016-10-23]. https://www. Fastcompany. con/3035723/app-econom/smart-con-Tract

scould-be-crypto currencys-killer-app.

[17]安瑞,何德彪,张韵茹,等. 基于区块链技术的防伪系统的设计与实现[J]. 密码学报,2017,4(2):199-208.
AN R,HE D B,ZHANG Y R,et al. Design and Implementation of Anti-Counterfeiting System Based on Block Chain Technology [J]. Journal of Cryptography,2017,4(2):199-208.

[18]金评媒. 区块链将被应用于食材跟踪保证食材品质[EB/OL]. 2016-08-07. http://www. jpm. cn/article-13731-1. html.
JPM. Block Chain will be Applied to Food Tracking to Ensure Food Quality [EB/OL]. 2016-08-07. http://www. jpm. cn/article-13731-1. html.

[19]王继业,高灵超,董爱强,等. 基于区块链的数据安全共享网络体系研究[J]. 计算机研究与发展,2017,54(4):742-749.
WANG J Y,GAO L C,DONG A Q et al. Research on Data Security Sharing Network System Based on Block Chain [J]. Computer Research and Development,2017. 54(4):742-749.

[20]杨龙飞,琴琴,杨天,等. 区块链的关键技术、应用与挑战[J]. 中国计算机学会通讯,2018,14(6):43-50.
YANG L F,QIN Q,YANG T,et al. Key Technologies of Block Chains and Their Applications and Challenges [J]. Communication of China Computer Society,2018,14(6):43-50.

[21]ROMAN KORIZKY. World Economic Forum Survey [EB/OL]. 2016-02-21. http://www. coinfox. info/news/3184-world-economic-forum-survey-10-of-global-gdp-may-be-stored-with-blockchain-technology-by-2027.

[22]赵阔,邢永恒. 区块链技术驱动下的物联网安全研究综述[J]. 信息网络安全,2017(5):1-6.
ZHAO K,XING Y H. Overview of Internet of Things Security Driven by Block Chain Technology [J]. Information Network Security,2017(5):1-6.

[23]朱岩,甘国华,邓迪,等. 区块链关键技术中的安全性研究[J]. 信息安全研究,2016(12):1090-1097.
ZHU Y,GAN G H,DENG D,et al. Security Research in Key Technologies of Block Chain [J]. Information Security Research,2016(12):1090-1097.

[24]刘敖迪,杜学绘,王娜,等. 区块链技术及其在信息安全领域的研究进展[J]. 软件学报,2018,29(7):2092-2115.
LIU A D,DU X Y,WANG N,et al. Block Chain Technology and Its Research Progress in the Field of Information Security [J]. Journal of Software,2018,29(7):2092-2115.

[25]EYAL I,GENCER A E,SIRER E G,et al. Bitcoin-NG: A Scalable Blockchain Protocol [C]. Santa Clara:USENIX,2016:45-59.

[26]ETHEREUM. A Next Generation Smart Contract and Decentralized Application Platform [EB/OL]. 2015-11-12. https://github. com/ethereum/wiki/wiki/White-Paper.

[27]WIKIPEDIA. Blockchain(Database)[EB/OL]. 2016-09-15. https://en. wikipedia. org/wiki/Blockchain_(Database).

[28]PRIMECOIN. Advantages of Primecoin [EB/OL]. 2016-02-09. http:// prime-coin. io/.

[29]MCKINSEY. Blockchain in Insurance-Opportunity or Threat? [BE/OL]. 2016-07-25. http://www. mckinsey. com/industries/financial-services/our-insights/blockchain-in-in-surance-opportunity-or-threat.