



综述

区块链在蜂窝移动通信系统中的研究现状及发展趋势

左益平¹, 金石¹, 张胜利²

(1. 东南大学移动通信国家重点实验室, 江苏 南京 210096;

2. 深圳大学区块链技术研究中心, 广东 深圳 518060)

摘要: 区块链本质上是分布式数据库, 无需第三方中介机构即可安全更新状态。将区块链技术引入 6G 蜂窝移动通信系统中以保障用户的隐私安全, 减少资源分配和通信服务成本, 支持不同分布式应用, 从而实现移动通信和区块链技术的有机结合, 被预测为 6G 蜂窝移动通信的关键技术之一。从区块链结合物联网 (IoT)、边缘计算、频谱分配、干扰管理方面展开了详细的介绍, 阐述了近年来国际学术界在该方向的最新研究进展, 并在此基础上对 6G 蜂窝移动通信中区块链技术的发展趋势进行了进一步的展望。

关键词: 区块链; 物联网; 边缘计算; 频谱分配

中图分类号: TN929.5

文献标识码: A

doi: 10.11959/j.issn.1000-0801.2019192

Research status and development trend of blockchain in cellular mobile communication system

ZUO Yiping¹, JIN Shi¹, ZHANG Shengli²

1. National Mobile Communications Research Laboratory, Southeast University, Nanjing 210096, China

2. Blockchain Technology Research Center, Shenzhen University, Shenzhen 518060, China

Abstract: The blockchain is essentially a distributed database that can be safely updated without the need for third-party intermediaries. The blockchain technology is introduced into the 6G cellular mobile communication system to ensure the privacy of users, reduce the cost of resource allocation and communication services, and support different distributed applications. In order to realize the organic combination of mobile communication and blockchain technology, it is predicted to be one of the key technologies of 6G cellular mobile communication. From the blockchain combined with internet of things (IoT), edge computing, spectrum allocation, interference management, a detailed introduction was introduced, and the latest research progress of international academic circles in this direction was expounded in recent years, and on this basis, the development trend of blockchain technology in 6G cellular mobile communication was further prospected.

Key words: blockchain, internet of things, edge computing, spectrum allocation

收稿日期: 2019-04-23; 修回日期: 2019-07-19

基金项目: 国家自然科学基金杰出青年科学基金资助项目 (No.61625106); 国家自然科学基金资助项目 (No.61531011)

Foundation Items: NSFC for Distinguished Young Scholars of China (No.61625106), The National Natural Science Foundation of China (No.61531011)

1 引言

大约每一个十年,都会有新一代蜂窝移动通信系统被设计和部署,大大改变了人们工作和生活的方式。1G移动通信网络仅用于语音呼叫;2G移动通信技术是一种数字技术并支持文本消息传递;3G移动技术提供更高的数据传输速率和容量,并支持交互式媒体业务;4G移动通信技术将3G与固定互联网相结合,以帮助无线移动互联网,并且它超越了3G的局限,带宽增加,资源成本降低。5G^[1]相比4G无线传输速率提升10~100倍,峰值传输速率达10 Gbit/s,端到端时延减少至毫秒级,连接设备密度增加10~100倍,流量密度提高1 000倍,频谱效率提升5~10倍,能够在500 km/h的速度下保证用户体验。5G主要从3个维度实现上述指标,即空口增强、更宽的频谱和网络密集化,代表性技术分别对应着大规模MIMO、毫米波通信以及超密集组网。5G尚未正式使用,但其部署已经开始,预计将在2020年出现。然而5G无法解决许多未来需求,例如极高的比特率、超低时延、高能效、抗阻塞性和无线充电等,所以现在有很多国家已经开始关注6G^[2-3]领域了。

6G既要在5G“大带宽、低时延、广联接”这3个应用场景上实现更好的通信基础服务,又要实现更多的应用场景的突破。6G时代才是真正的万物万联时代,因为从目前来看,5G在广联接也就是IoT的应用还不太理想,6G可能会在这个场景上扩展,向着海陆空一体化融合网络的方向发展。目前,中国、美国、欧洲、韩国、日本、芬兰等国家和地区已陆续着手B5G或者6G技术的研发。不过现在还未得到统一的6G定义,各方都有自己的愿景。美国FCC(Federal Communications Commission)认为6G将进入太赫兹(THz)频段,频段更高,基站的覆盖范围会变小,导致网络更加致密化;6G将使用空间复用技术,6G基站可同时接入数百个甚至数千个无线连接,其

容量将会是5G的1 000倍;美国FCC还认为6G将会采用更智能、分布更强的基于区块链的动态频谱共享接入技术。欧盟认为6G就是5G结合卫星通信/卫星导航,可实现国际上几大主流卫星导航的互通漫游。韩国认为6G技术方案是“太赫兹+去蜂窝化结构+高空无线平台(如卫星等)”,其中,去蜂窝结构是指6G基站未必按照蜂窝状布置,终端未必只和一个基站通信,这种结构能够大大提高频谱效率。日本认为6G应该引入大规模MIMO技术与OAM技术的结合,有望在未来实现40个电波的叠加传输。最近在芬兰开的全球首届6G峰会的主办方、全球最早开始研究6G的科研机构——奥卢大学无线通信中心将即时通信与无限制连接、分布式计算和智能、极高频段材料和天线作为6G的主要研究方向。我国也启动了对6G的研发工作,科学技术部发布了关于国家重点研发计划“宽带通信和新型网络”重点专项,如“大规模无线通信物理层基础理论与技术”以及“太赫兹无线通信技术与系统”等,都是与6G相关的。可想而知,6G蜂窝移动通信系统下会产生海量的无线大数据,资源分配和调度复杂度极高,用户个人信息的安全性和隐私性遭到更多方面的威胁。现有的技术手段还不能完全解决上述一系列问题,所以需要将创新性的技术加入6G中,以解决6G蜂窝移动通信系统的瓶颈问题。

另一方面,区块链作为一项新兴的前沿技术^[4-5],近年来受到了广泛的关注,是因为比特币使用了一个分布式的区块链来跟踪所有的交易,但实际上区块链技术并不局限于比特币一种应用。区块链技术天然地拥有去中心化、分布式、防篡改等优点,所以移动通信领域的研究者期望将其应用于系统的各个层面,期望大幅度提升蜂窝移动通信系统的性能,实现真正意义的万物万联。美国FCC在MWCA2018大会上也提出利用区块链进行动态频谱分配的构想,因此区块链技术被认为是6G的关键技术之一,其基本思想就是



利用区块链技术的去中心化、分布式、防篡改等特点,将区块链技术引入 6G 蜂窝移动通信系统中保障用户的隐私安全,减少资源分配和通信服务成本,从而实现移动通信和区块链技术的有机结合。学术界和工业界正在上述领域开展研究工作,使用区块链去中心化的分布式账本来记录各种无线接入信息的研究刚刚起步,未来可能会进一步激发新技术的创新,甚至改变未来使用无线频谱的方式。

尽管区块链技术融入蜂窝移动通信系统是趋势所在,但是研究都处于构想和初步探索阶段,机遇和挑战并存。追溯历史,蜂窝移动通信系统从 1G 到 5G 的发展,基本上解决了面向个人终端的陆地的网络覆盖问题,实现了信息的传播。未来移动通信向着海陆空一体化发展,加入区块链技术以实现信息价值的转移,IoT、资源的配置、隐私安全等方面一定会出现很多有意思的变化。目前这方面的研究面临诸多挑战,国内外研究者进行了初步构想和探索。本文主要介绍区块链技术应用于蜂窝移动通信技术的最新研究进展,主要包括 IoT、边缘计算、频谱分配、干扰管理。

2 区块链简介

2008 年 10 月 31 号, Nakamoto^[6]第一次提出

了区块链的概念,在随后几年中成为电子货币比特币的核心组成部分,作为所有交易的公共账本。通过利用点对点网络和分布式时间戳服务器,区块链数据库能够进行自主管理,无需第三方机构的辅助。比特币即“区块链 1.0”的设计思想已经成为其他应用程序的灵感来源。2013—2014 年间,程序员 Vitalik Buterin 受比特币启发后提出了以太坊即“区块链 2.0”,它是一个开源的有智能合约功能的公共区块链平台,通过其专用加密货币——以太币提供去中心化的以太虚拟机来处理点对点合约。下面详细介绍比特币、以太坊的基本原理以及区块链技术的发展现状。

2.1 比特币

2.1.1 区块

区块分为区块头和区块体两部分:区块头包含前一个区块的散列值、难度值、当前区块所有交易的 Merkle 根节点的散列值、时间戳和随机数,区块体包含当前区块的所有交易信息。区块链就是按创建的时间顺序进行排列的区块链条,它十分完美地实现了一个安全可靠、不断推进的比特币交易数据库,区块数据结构示意图如图 1 所示。比特币系统大约每 10 min 产生一个区块,该区块包含这 10 min 内未确认的交易以及前一个区块的散列值,因此从第一个区块问世至今就形成了一条完整的区块链。

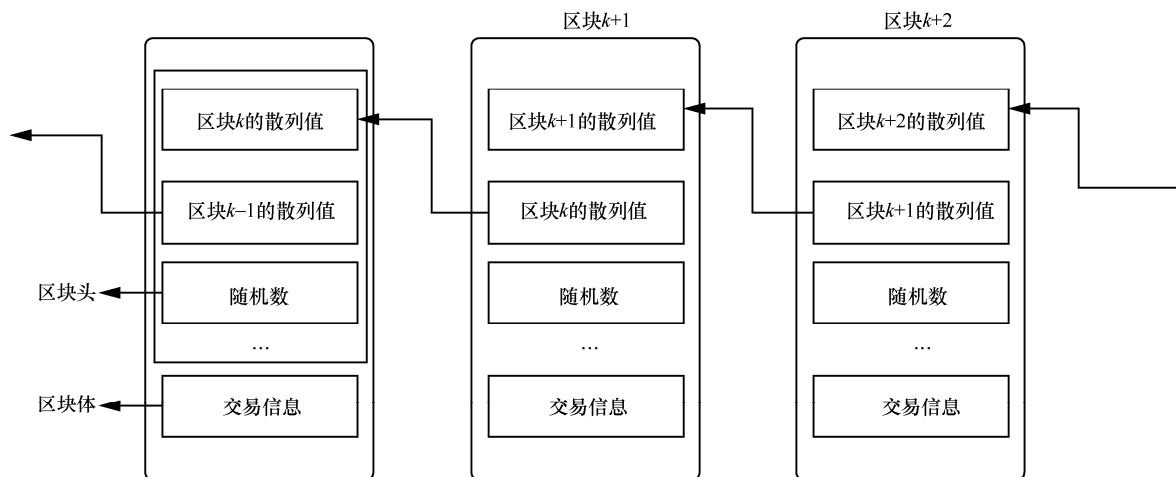


图 1 区块数据结构示意图

2.1.2 PoW

PoW 共识机制的本质是防止低算力的实体随意或恶意发布区块。散列函数的输入为区块头，输出是一个 256 bit 的散列值。比特币系统会把每个区块完成的时间控制在 10 min 左右。如果难度低于 10 min，系统就自动调高难度值，增加散列值开头 0 的位数；如果难度高于 10 min，就适当减少散列值开头 0 的位数，以调低难度值。这个 PoW 的过程被称为挖矿，挖矿流程如图 2 所示，挖矿前要构造好区块，通过不停改变随机数 Nonce 使得区块头的散列值小于目标难度值。

挖矿的本质是争夺记账权，矿工收集、检验和确认过去一段时间内发生的交易。当找到一个符合 PoW 机制的散列值时，矿工就能够将自己封装的区块广播出去，让其他矿工验证该区块。如果有矿工接受该区块并以它为基础继续挖下一个区块，那么该区块中的所有交易单就获得一次确认。每延长一个区块就等价于该区块中的交易多了一次确认。若得到 6 次确认，那么该区块就获得全网的认可，封装到历史区块中。区块链可以记录任意两个节点的交易，且不需要第三方机构就可以在网络中更新节点的信息状态，本质上是分布式数据存储、点对点传输、共识机制、加密算法等技术融合的新型技术。

2.2 以太坊

以太坊就是一个开源的区块链平台，用户可以在该平台上按需创建应用或程序，以实现去中

心化的自治。因此，以太坊是一个开源且去中心化的区块链平台或应用集合。以太坊的原理和比特币基本类似，以太坊最大的创新就是引入智能合约。智能合约就是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。智能合约由矿工执行，执行结果记录在区块链上。基于区块链技术的智能合约不仅可以发挥智能合约在成本效率方面的优势，而且可以避免恶意行为对合约正常执行的干扰。将智能合约以数字化的形式写入区块链中，由区块链技术的特性保障存储、读取、执行整个过程透明可跟踪、难以篡改。同时，由区块链自带的共识算法构建出一套状态机系统，使智能合约能够高效地运行。

2.3 区块链技术的发展现状

在过去 10 年中，区块链技术的发展十分迅猛，区块链不可变的数据组织框架和区块链网络的数据调度及维护方法是推进区块链技术发展的主要动力。从数据组织的角度看，区块链技术采用许多现成的加密技术^[7]，加密地将用户的伪身份与标记的资产交易联系起来，所以区块链能证明资产的所有权。区块链通过“块”的形式将交易集合加密连接到前面的交易目录中来维持交易记录的次序。另一方面，对任意节点具有容忍度的开放网络中，区块链网络中的共识机制创造性地解决了交易记录重复的问题^[8]。与传统的共识机制相比，在没有身份认证和更小消息传输的开销条

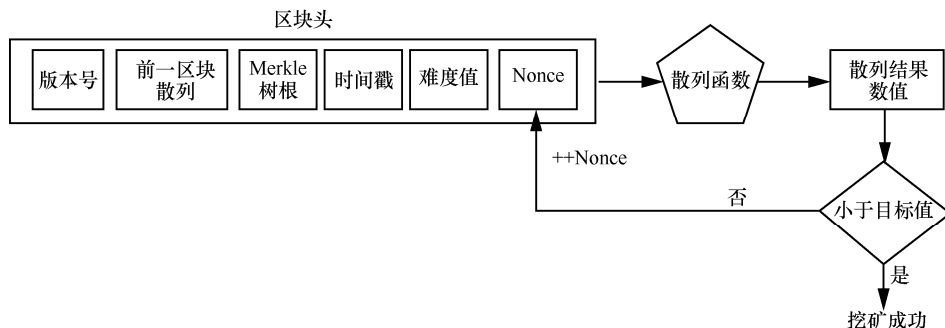


图 2 PoW 挖矿流程



件下, 区块链共识机制能够在大量无信任节点之间提供关于全局分类账—数据状态的共识^[9]。在这个意义上, 区块链可以被看作网络的通用存储器, 并且网络可以被看作包括每个节点的分布式虚拟机 (virtual machine, VM)^[10]。因此, 区块链网络提供了一个通用平台, 用于在分布式的应用程序中执行事务驱动的指令, 例如自组织网络编排^[11]和 P2P 资源交易^[12]。

尽管随着区块链技术已经在快速发展, 但有着更高服务质量需求的区块链应用, 对区块链机制的设计提出了更严峻的挑战。特别地, 区块链网络的性能极大地依赖于所采用的共识机制性能, 与可扩展性非常有限的经典机制相比^[13], 公有区块链网络 (例如比特币) 中的大多数共识机制以处理吞吐量为代价保证了更好的可扩展性。为了实现无信任节点之间分布式同步和确保交易完成, 许多机制也对物理资源 (例如计算能力) 消耗产生了巨大需求^[9]以及需要施加更长的等待时间来确认交易。参考文献[9]对于上述这些问题, 进行了一些简短的调查研究, 目的是在特定方面提高区块链共识机制的性能。

与此同时, 在过去的 10 年中, 区块链已经从不可变的、防篡改的分布式账本进行了进一步扩展。例如参考文献[14-15]讨论了关于比特币范围内的用户端应用 (即钱包)、P2P 网络协议、共识机制和用户隐私的问题。参考文献[16]提供了从金融到物联网的新兴区块链应用的简要总结。此外, 参考文献[17]提供了关于比特币网络中的安全问题的系统调查, 包括对共识机制的攻击以及比特币客户端的隐私/匿名问题。参考文献[18-19]在以太坊网络范围内, 提供了对智能合约的设计、应用和安全性等特殊问题的调查。

3 区块链在 6G 中的应用

6G 蜂窝移动通信系统将会带来超高数据量以及设备的大规模连接, 通过其低时延、高速度

和高容量的覆盖能力, 可以使 IoT 设备获得更加广泛的应用。6G 移动通信网络边缘产生的数据量还在不断增加, 直接在网络的边缘进行数据处理会更加高效, 边缘计算毫无疑问是 6G 中还有发展前景的技术。同时无线频谱一直是稀缺资源, 其需求持续快速增长。另一方面, 随着网络越加致密化, 网络基础设施的投资成本正在不断加大, 如何高效利用频谱资源将会是 6G 的核心挑战。6G 的网络致密化部署将会导致严重的干扰问题, 所以干扰管理问题也是 6G 的关键研究方向。综上所述, 6G 中的 IoT、边缘计算、频谱分配、干扰管理还是特别重要的研究课题。所以本节面向区块链在 6G 移动通信系统的应用, 从 IoT、边缘计算、频谱分配、干扰管理 4 个方面展开详细的介绍, 展示了近年来国际学术界在该方面的最新研究进展。区块链在蜂窝移动通信系统中的研究现状分类见表 1。

3.1 IoT

现在存在的中心化的网络, 包括数据中心的高额维护成本等在内的诸多瓶颈, 并不能适应万物万联的要求。未来 6G 的 IoT 需要一个去中心化的网络架构, 即采用区块链技术。参考文献[20-23]都研究了基于区块链的 IoT 技术, 参考文献[22]分析了在区块链网络中同步的 IoT 设备的通信流量, 因为 IoT 设备需要连接到一个或多个验证器节点以观察或修改账户的状态, 为了与最新的账户状态进行交互, 需要将设备与验证器节点存储的区块链副本同步。介绍了具有不同通信成本和安全级别的同步协议, 使得 IoT 端点与区块链同步, 并且对同步协议产生的流量进行建模和分析。参考文献[22]提出 IoT 设备和区块链网络同步的两种协议, 讨论了 IoT 设备的本地状态到区块链网络的全局状态的转移概率, 受同步协议运行时间、设备睡眠时间、区块的大小等参数的影响。分析和仿真结果表明, 保证同步过程可靠性的无线技术选择取决于区块链参数。而且如果协议执

表 1 区块链在蜂窝移动通信系统中的研究现状分类

研究方向	主要参考文献
物联网 (IoT)	参考文献[22-23]主要讨论了 IoT 设备的局部状态与区块链网络的全局状态保持同步的过程
边缘计算	参考文献[24-27]提出将区块链 PoW 挖矿任务卸载到边缘计算, 构建两阶段的 Stackelberg 博弈和拍卖机制来模拟边缘计算服务器和移动区块链用户的交互过程
频谱分配	参考文献[28]提出基于智能合约的频谱分配方案, 移动网络运营商可以利用其他主要用户未使用的频谱来扩容; 参考文献[29]利用区块链的工作方式模拟了主次要用户之间的频谱租用过程
干扰管理	参考文献[30]提出利用区块链的货币机制和协调协议的贪婪分布式算法实现以前采用中央控制器达到的最优信息分配, 消除了用户间的干扰

行持续时间与平均块生成周期相当, 则保持同步的概率迅速降低。最后发现区块链协议与主要产生上行链路流量的典型 IoT 应用不同, 需要分配大量的下行链路资源。

参考文献[23]分析了具有轻量级 IoT 客户端的区块链系统的时延和通信权衡。区块链技术为 IoT 设备的协调提供了分布式架构, 但是保留区块链分类账本的本地副本对于低功耗和内存受限的设备是不可行的。出于这个原因, 提出用轻量级软件实现, 仅下载有用的数据结构。提出了一种新颖的基于区块链网络的压缩方案, 该方案在周期性更新中压缩区块链数据并进一步降低 IoT 设备的通信成本。参考文献[23]讨论了区块链将同步信息发送到 IoT 设备的下行链路帧长度的分布、帧的传输时间以及利用它们计算通信成本和时延。分析和仿真结果表明, 如果已知账户更新和信道状态的统计信息, 则轻量级客户端可以构建感兴趣的事件列表, 提供可预测的平均通信成本, 该方案可用于设计更高级的区块链轻量级协议。

3.2 边缘计算

现有的针对区块链和边缘计算的研究, 大部分是因为 IoT 与区块链的结合虽然提高了系统的性能, 但是区块链本身的挖矿过程需要很大的算力, 不符合 IoT 设备计算能力相对较低、功耗较低以及零散低带宽的无线连接的特点, 边缘计算

技术可以解决这个问题。

参考文献[24]和参考文献[25]研究的问题相同, 而且都提出了一种解决方案, 具体是将区块链 PoW 挖矿任务卸载到附近的移动边缘计算服务器, 允许移动用户访问和利用边缘的资源或计算服务。然而, 边缘计算服务由边缘服务提供商 (edge services provider, ESP) 部署, 首要目标是最大化自己的利益, 因此使用两阶段 Stackelberg 博弈提供的定价方案来模拟 ESP 和移动用户之间的交互。参考文献[25]对两阶段 Stackelberg 博弈模型进行了更加详细的推导和分析。通过反向归纳得出了博弈的纳什均衡点, 提出了 ESP 分别采用统一和歧视定价的最佳资源管理方案。此外, 在两种定价方案中, Stackelberg 均衡的存在性和唯一性都已经得到了证明。

参考文献[26]采用基于拍卖理论的方案, 其中 ESP 尝试制定实用的分配计算资源策略, 首先, ESP 向移动用户宣布其资源服务, 然后移动用户提交他们对计算资源的估值。最后 ESP 选择给赢得拍卖的用户提供服务, 并通知所有用户当前的分配。对于需求不断的矿工, 提出了一种可以实现最佳矿工收益的拍卖机制。对于有多种需求的矿工, 将矿工收益最大化问题转化为非单调子模块最大化与背包约束问题。然后, 设计了两种有效的机制, 最大限度地提高矿工的收益。实验结果已经证明, 所提出的拍卖机制是真实的、个体



理性的和高计算效率的, 并且能够解决矿工收益最大化问题。

参考文献[27]对参考文献[26]提出的拍卖方案进行了增强, 引入了深度学习的方法, 具体来说, 构建了一个基于最优拍卖解决方案的多层神经网络架构。神经网络首先对矿工的出价进行单调变换, 然后计算矿工的分配和有条件付款规则。使用矿工的估值作为训练数据来调整神经网络的参数, 以优化 ESP 的损失函数。实验结果证明了使用深度学习的好处, 可获得高收益的移动区块链的最佳计算资源拍卖。

上述参考文献提出的区块链和边缘计算结合的算法, 分别通过两阶段 Stackelberg 博弈定价和基于拍卖理论的方案来模拟 ESP 和区块链移动用户之间的交互过程, 以用户的任务量和服务器收取的费用为技术指标, 讨论了用户和服务器为了保证自身利益如何选择最佳的任务和费用策略。可以看出, 边缘计算作为辅助工具可以改进区块链本身的算力复杂度高的缺陷。未来的一个研究方向可以是区块链技术结合人工智能技术对边缘计算的安全隐私性和资源分配等方面进行改善。

3.3 频谱分配

从 1G 到 5G, 为了提高速率、提升容量, 移动通信永远向着更多的频谱、更高的频段扩展。无线频段越高, 单位时间内所能传递的数据量就越大, 覆盖范围越小, 5G 的基站密度比 4G 高很多, 为了提升覆盖范围和网络速率, 将在基站端引入大规模 MIMO 和波束成形技术。5G 已经扩展到毫米波频段 (3~6 GHz), 6G 将使用太赫兹频段 (100 GHz~10 THz), 6G 的基站密集度将会更高。无线频谱是稀缺资源, 其需求正在快速增长, 另一方面, 随着网络更加致密化, 网络基础设施的投资成本正在不断加大。如何高效利用频谱资源将会是 6G 的关键话题之一。美国 FCC 提出 6G 可以采用更智能、分布更强的基于区块链的

动态频谱共享接入技术, 而不再通过集中式的数据库来支持频谱共享接入, 不仅可以降低动态频谱接入系统的管理费用, 提升频谱效率, 还能进一步增加接入等级、接入用户数量等。6G 对原来被 3G/4G 占用的频谱的重新使用, 使得整个移动网络的效率更高。并且借助区块链技术来实现分层次多中心的频谱使用共识和动态分配, 即使是跨牌照协同也成为技术性的可能和商业性的必然。

从基于区块链技术的频谱分配出发, 参考文献[26]提出了基于智能合约的频谱分配方案, 移动网络运营商可以通过聚合其他主要用户未使用的许可频谱来扩展其容量。为了准确识别频谱机会, 移动网络必须部署多个传感器, 或者它可以将此任务卸载到具有感知能力的附近节点, 即所谓的帮助者。但是对于帮助者执行频谱感知的激励是有限的, 所以笔者引入了一种基于智能合约的频谱感知服务解决方案, 促进网络运营商从其附近的帮助者购买频谱服务。参考文献[28]讨论了基于智能合约的主用户频谱感知的检测概率, 恶意节点越多, 频谱检测概率就越低。每秒次要用户的净收益等于总收益减去成本, 净收益必须是正的, 可以推导出最小的频谱效率表达式, 分析了频谱感知帮助者的数目、写入智能合约的数据压缩系数对频谱效率的影响。参考文献[29]利用区块链的工作方式模拟了主次要用户之间租用频谱的过程, 并且设计了相应的同步协议。参考文献[28]和参考文献[29]提出的基于区块链的频谱分配方法, 都比传统拍卖更公平、更安全, 并且节约了部分第三方中介的成本。但是现有文献对于区块链帮助频谱分配方案还都是一些表面的构想, 具体实现和更深入的研究工作还有待后续的科研人员好好探索。

3.4 干扰管理

Gamal 等人^[30]提出了贪婪分布式算法, 利用区块链货币机制和协调协议, 能够实现以前采用

中央控制器达到的最优信息分配,消除了用户之间的干扰。货币机制假设只有一种硬币类型,硬币能从一个发送机—接收机对节点到下一个节点,因为硬币从付款节点1到收款节点2,付款人的发送机对收款人的接收机造成困扰,所以付款人就需要租用付款人的发送机来消除干扰。CM1(协调信息1)是节点 i 愿意接受节点 $i+1$ 的汇款,但要关闭接收机 i ;CM2是节点 i 愿意接受节点 $i+1$ 的汇款,同时使用接收机 i ;CM3是节点 i 不愿意接受节点 $i+1$ 的汇款,节点 $i+1$ 是激活状态,这时从接收机 $i+1$ 端可以看到用户间是无干扰的;CM4是节点 i 不愿意接受节点 $i+1$ 的汇款,节点 $i+1$ 是非激活状态,这时从接收机 $i+1$ 端可以看到用户间的干扰是无法消除的,因为整个回程负载约束失效了。基于上述区块链的货币机制和协调协议,提出了贪婪分布式算法,可以完美实现以前采用中央控制器得到的最优信息分配。

参考文献[30]具有一种硬币类型的货币机制和依赖于2 bit消息的协调协议实现,传输方案基于协作迫零和干扰避免。节点支付硬币是因为在收款人的接收器上造成干扰,所以要出租收款人的发射器消除干扰。在未来的工作中研究如何将所提出的方案扩展到一般网络拓扑,特别是硬币的数量、协调协议的开销以及具有任意拓扑的网络大小的时延标度。区块链技术在干扰管理方面的详细实施,也是一个未来的研究方向。

4 未来发展方向

由本文第3节的分析可知,区块链在蜂窝移动通信领域的应用,主要思想是将区块链技术引入IoT、边缘计算、频谱分配、干扰管理领域。虽然区块链技术应用在蜂窝移动通信系统中的前景很广阔,但是目前还面临着诸多瓶颈问题。首先区块链技术本身存在一些问题,比如区块链技术的可扩展性差,挖矿需要的算力很大,确认交易的时间很长,节点规模、性能、容错性三者之间

难以平衡,目前缺乏统一的区块链技术应用标准等。其次面临的问题是如何将区块链应用到蜂窝移动通信的各种场景中,采用什么样的技术架构,在性能指标、安全性、稳定性等方面缺乏指导性的思路和目标。毫无疑问,区块链技术应用到蜂窝移动通信系统中还有许多工作需要展开和完善。结合已有的研究工作,展望了区块链技术在蜂窝移动通信系统中的应用,可能会出现下述研究方向。

(1) 区块链与IoT结合

当前绝大多数IoT设备基于中心化的分布式架构,边缘节点仍受到中心化的核心节点能力的制约。可以考虑利用区块链的去中心化思想,研究如何把物联网的核心节点的能力下放到各个边缘节点,让核心节点仅控制核心内容或做备份使用,各边缘节点为各自区域内设备服务。并且可以研究如何设计更加灵活的协作模式以及相关共识机制,完成原核心节点承担的认证、账务控制等功能,使得区块链在这种平台架构中扮演公开账本的角色,对IoT设备之间所有的信息交换进行安全、可信和稳定的记录。

(2) 区块链与边缘计算结合

IOT设备有限的计算能力和存储能力是制约区块链应用的重要瓶颈,但边缘计算可以解决这一问题。以移动边缘计算为例,未来可以研究移动边缘计算服务器如何替移动区块链网络下的IoT设备完成计算、存储等任务,并在区块链技术的帮助下保证数据的可靠性和安全性。边缘计算与区块链的融合能提高IoT的整体性能。同时还可以研究如何分配和协调区块链网络下的边缘计算、存储和无线通信等资源。

(3) 区块链与频谱分配结合

如何高效利用频谱资源将会是6G的关键话题之一。美国FCC提出6G可以采用更智能、分布更强的基于区块链的动态频谱共享接入技术,而不再通过集中式的数据库来支持频谱共享接入,不仅可以降低动态频谱接入系统的管理费用,



提升频谱效率,还能进一步增加接入等级、接入用户数量等。区块链的发展可为频谱的分配管理提供新的思路。

(4) 区块链与人工智能结合

到目前为止,6G 所描绘的愿景可以预见到大量的数据交换,需要普遍使用人工智能方法,例如强化学习和深度学习,以智能有效的方式处理数据和管理无线通信资源^[31-32]。显然,这在安全性、隐私性和信任方面构成了重大挑战。在真正庞大的物联网部署中,分布式身份验证是提供可伸缩性的一个关键点,区块链可以解决上述问题,同时人工智能方法也能够确定区块链的最佳参数。所以区块链结合人工智能显著改善 6G 网络的计算、通信和存储性能。这是未来区块链发展的方向之一。

总结已有研究和展望未来,可以发现区块链在 6G 中的应用很广泛,与物联网、边缘计算、资源管理结合,未来区块链在 6G 中的发展向物理层推进,还有与人工智能强强联手的发展趋势。目前这些研究都还刚刚起步,具有广阔的发展前景,面对诸多挑战。

5 结束语

本文首先介绍了区块链技术,包括比特币、以太坊的工作原理以及区块链技术的发展现状,然后详细阐述了区块链应用于蜂窝移动通信技术的最新研究成果,包括物联网、边缘计算、频谱分配、干扰管理。从最新研究进展可以看出,区块链作为 6G 发展的主流技术之一,可以利用自身网络的去中心化、安全性高等特点,对蜂窝移动通信中复杂的资源管理和隐私安全等方面进行颠覆性的改变,将会成为最具潜力的发展方向之一。

参考文献:

- [1] 张静,金石,温朝凯,等. 基于人工智能的无线传输技术最新研究进展[J]. 电信科学, 2018, 34(8): 46-55.
ZHANG J, JIN S, WEN C K, et al. The latest research progress of wireless transmission technology based on artificial intelligence[J]. Telecommunications Science, 2018, 34(8): 46-55.
- [2] CASSARA G A. 6G: the next frontier[M]. Hoboken: Wiley, 2015.
- [3] KLAUS D, HENDRIK B. 6G vision and requirements: is there any need for beyond 5G?[J]. IEEE Vehicular Technology Magazine, 2018, 13(3): 72-80.
- [4] 李董, 魏进武. 区块链技术原理、应用领域及挑战[J]. 电信科学, 2016, 32(12): 20-25.
LI D, WEI J W. Theory, application fields and challenge of the blockchain technology[J]. Telecommunications Science, 2016, 32(12): 20-25.
- [5] 梅海涛, 刘洁. 区块链的产业现状、存在问题和政策建议[J]. 电信科学, 2016, 32(11): 134-138.
MEI H T, LIU J. Industry present situation, existing problems and strategy suggestion of blockchain[J]. Telecommunications Science, 2016, 32(11): 134-138.
- [6] NAKAMOTO S. Bitcoin: a peer-to-peer electronic cash system[R]. 2008.
- [7] MOHR A. A survey of zero-knowledge proofs with applications to cryptography[R]. 2007.
- [8] RAYNAL M. Communication and agreement abstractions for fault-tolerant asynchronous distributed systems[J]. Synthesis Lectures on Distributed Computing Theory, 2010, 1(1): 1-273.
- [9] BANO S, SONNINO A, AL-BASSAM M, et al. Consensus in the age of blockchains[J]. arXiv: 1711.03936, 2017.
- [10] KOSBA A, MILLER A. Hawk: the blockchain model of cryptography and privacy-preserving smart contracts[C]//2016 IEEE Symposium on Security and Privacy (SP), May 22-26, 2016, San Jose, CA, USA. Piscataway: IEEE Press, 2016: 839-858.
- [11] BOZIC N, PUJOLLE G, SECCI S. Securing virtual machine orchestration with blockchains[C]//2017 Cyber Security in Networking Conference (CSNet), Oct 18-20, 2017, Rio de Janeiro, Brazil. [S.l.:s.n.], 2017: 1-8.
- [12] CHATZOPOULOS D, AHMADI M. FlopCoin: a cryptocurrency for computation offloading[J]. IEEE Transactions on Mobile Computing, 2018, 17(5): 1.
- [13] CASTRO M, LISKOV B. Practical byzantine fault tolerance and proactive recovery[J]. ACM Transactions on Computer Systems, 2001, 20(4): 398-461.
- [14] TSCHORSCH F, SCHEUERMANN B. Bitcoin and beyond: a technical survey on decentralized digital currencies[J]. IEEE Communications Surveys Tutorials, 2016, 18(3): 2084-3123.
- [15] BONNEAU J, MILLER A, CLARK J, et al. Sok: research perspectives and challenges for bitcoin and cryptocurrencies[C]//IEEE Symposium on Security and Privacy, May 17-21, 2015, San Jose, CA, USA. Piscataway: IEEE Press, 2015: 104-121.
- [16] ZHENG Z, XIE S. Blockchain challenges and opportunities: a survey[R]. 2016.

- [17] CONTI M, SANDEEP K E, LAL C, et al. A survey on security and privacy issues of bitcoin[J]. arXiv: 1706.00916, 2017.
- [18] ATZEI N, BARTOLETTI M, CIMOLI T, et al. A survey of attacks on ethereum smart contracts[M]. Berlin: Springer, 2017.
- [19] CHRISTIDIS K, DEVETSIKIOTIS M. Blockchains and smart contracts for the internet of things[J]. IEEE Access, 2016(4): 2292-2303.
- [20] DORRI A, KANHERE S S, JURDAK R, et al. Blockchain in internet of things: challenges and solutions[J]. arXiv: 1608.05187, 2016.
- [21] FENG S H, WANG W B, NIYATO D, et al. Competitive data trading in wireless-powered internet of things (IoT) crowdsensing systems with blockchain[J]. arXiv: 1808.10217, 2018.
- [22] DANZI P, KALØR A E, STEFANOVIĆ C, et al. Analysis of the communication traffic for blockchain synchronization of IoT devices[J]. arXiv: 1711.00540v1, 2018.
- [23] DANZI P, KALØR A E, STEFANOVIĆ C, et al. Delay and communication tradeoffs for blockchain systems with light-weight IoT clients[J]. arXiv: 1807.07422, 2018.
- [24] XIONG Z H, ZHANG Y, NIYATO D, et al. When mobile blockchain meets edge computing[J]. arXiv:1711.05938, 2018.
- [25] XIONG Z H, FENG S H, WANG W B, et al. Cloud/fog computing resource management and pricing for blockchain networks[J]. arXiv: 1710.01567, 2018.
- [26] JIAO Y T, WANG P, NIYATO D, et al. Auction mechanisms in cloud/fog computing resource allocation for public blockchain networks[J]. arXiv: 1804.09961, 2018.
- [27] LUONG N C, XIONG Z H, WANG P, et al. Optimal auction for edge computing resource management in mobile blockchain networks: a deep learning approach[J]. arXiv: 1711.02844, 2017.
- [28] BAYHAN S, ZUBOW A, WOLISZ A, et al. Spass: spectrum sensing as a service via smart contracts[C]//IEEE International Symposium on Dynamic Spectrum Access Networks (DySPAN), Oct. 22-25, 2018, Seoul, South Korea. Piscataway: IEEE Press, 2018: 1-10.
- [29] KOTOBI K, BILEN S G. Blockchain-enabled spectrum access in cognitive radio networks[C]//2017 Wireless Telecommunications Symposium (WTS), Apr 26-28, 2017, Chicago, IL, USA. Piscataway: IEEE Press, 2017: 1-6.
- [30] GAMAL A E, HESHAM E G. A blockchain example for cooperative interference management[J]. arXiv: 1808.01538, 2018.
- [31] 王志宏, 杨震. 人工智能技术研究及未来智能化信息服务体系的思考[J]. 电信科学, 2017, 33(5): 1-11.
WANG Z H, YANG Z. Research on artificial intelligence technology and the future intelligent information service architecture[J]. Telecommunications Science, 2017, 33(5): 1-11.
- [32] 王海坤, 潘嘉, 刘聪. 语音识别技术的研究进展与展望[J]. 电信科学, 2018, 34(2): 1-11.
WANG H K, PAN J, LIU C. Research development and forecast of automatic speech recognition technologies[J]. Telecommunications Science, 2018, 34(2): 1-11.

[作者简介]



左益平 (1993-), 女, 东南大学移动通信国家重点实验室博士生, 主要研究方向为移动通信关键技术、区块链技术等。



金石 (1974-), 男, 东南大学移动通信国家重点实验室教授、博士生导师, 主要研究方向为 5G/B5G 移动通信理论与关键技术、物联网理论与关键技术以及机器学习与大数据处理在无线通信中的应用等。



张胜利 (1978-), 男, 深圳大学区块链技术研究中心教授、博士生导师, 主要研究方向为无线网络、区块链关键技术、物理层网络编码等。