·专题一:区块链技术及应用·

# 区块链存在的问题与对策建议

刘 哲[1,2*] 郑子彬[3] 宋 苏[1] 张兆田[1]

(1. 国家自然科学基金委员会 信息科学部,北京 100085;
2. 南京航空航天大学 计算机科学与技术学院,南京 211106;
3. 中山大学 数据科学与计算机学院,广州 510006)

[摘 要] 本文从区块链可扩展性、安全与隐私保护、区块链监管审计及智能合约开发与保障四个方面分析总结了区块链当前存在的问题,阐述了解决相关问题需要研究的基础理论和关键技术;进一步探讨了区块链技术的发展趋势和影响;最后给出了对策建议。

[关键词] 前沿信息技术;区块链;关键技术;发展趋势;对策建议

DOI:10.16262/j.cnki.1000-8217.20200313.003

2019 年 10 月 24 日下午,中共中央政治局就区块链技术发展现状和趋势进行了第十八次集体学习。中共中央总书记习近平在主持学习时强调,区块链技术的集成应用在新的技术革新和产业变革中起着重要作用。要强化基础研究,提升原始创新能力,努力让我国在区块链这个新兴领域走在理论最前沿、占据创新制高点、取得产业新优势。要推动协同攻关,加快推进核心技术突破,为区块链应用发展提供安全可控的技术支撑。要加快产业发展,发挥好市场优势,进一步打通创新链、应用链和价值链。要构建区块链产业生态,加快区块链和人工智能、大数据、物联网等前沿信息技术的深度融合,推动集成创新和融合应用。要加强人才队伍建设,建立完善的人才培养体系,打造多种形式的高层次人才培养平台,培育一批领军人物和高水平创新团队。

为了学习和贯彻习近平总书记在中央政治局第十八次集体学习时的重要讲话精神,国家自然科学基金委员会信息科学部二处分别于 2019 年 11 月 1 日、11 月 22 日召开了区块链基础理论与关键技术研讨会。

## 1 区块链技术存在的问题及关键技术

区块链具有数据透明、防篡改、多方可验证等优点,这些优点使其具有广阔的应用前景。但是,目前区块链技术还存在以下问题亟待解决:

收稿日期:2019-12-17;修回日期:2020-01-16

* 通信作者,Email:zhe.liu@nuaa.edu.cn

刘哲 南京航空航天大学教授、博士生导师,国家青年特聘专家。主要研究领域为密码学、密码工程、物联网安全,区块链等,发表学术会议和期刊文章 80 余篇。曾获得卢森堡国家自然科学基金委杰出博士毕业论文奖、ACM 中国计算机安全新星奖、中国密码学会优秀青年奖、阿里巴巴达摩院青橙奖和多次国际安全会议最佳论文奖,目前主持国家自然科学基金等多项研究课题。担任多个安全和密码类学术期刊的编委,并受国际密码学会邀请担任密码工程顶级会议 CHES 2020 年大会主席。

### 1.1 可扩展性问题

区块链的可扩展性是区块链领域的重要研究问题。以比特币为例,可以通过增大系统的区块大小,或者是缩短出块时间,来提高系统的吞吐率。然而,这样的扩展方案是有上限的,其上限受到网络延迟等因素的制约[1]。如果通过简单地提升某一个指标以提高区块链系统的吞吐率,即使是在实验环境下,其吞吐率的提升也远远无法满足需求,因而比特币系统的可扩展性较差。目前主流的区块链系统中,能够做到无限扩展的几乎没有[2]。未来要想让区块链系统承担起大量的交易和去中心化应用,就必须在兼顾去中心化、安全性的同时,实现可扩展、高性能的区块链系统[3],其关键技术包括:

(1) 区块链共识机制。区块链的本质特点是在多方协同环境中达成共识,现有共识机制在大规模

网络节点下难以满足高吞吐、低延迟的需求，需要研究创新的区块链共识机制。

（2）区块链分片技术。分片是解决区块链扩容问题的主要技术手段，它由传统数据库延伸而来，包括网络分片、交易分片和状态分片等。

（3）区块链跨链交易技术。在多个区块链项目之间研究跨区块链交易技术，比如公证人机制、哈希锁定、分布式私钥控制、跨链智能合约框架等，可提高区块链系统间的互通性。

（4）松耦合数据结构设计。解耦区块链应用场景与底层事务结构与类型，实现不同应用场景下事务统一高效处理；对区块链底层默克尔树进行优化，实现系统账户、事务及状态的高效组织和更新；改进区块链组织与存储结构，方便追溯和高效查询。

（5）区块链密码算法更新。在存在敌手的现实环境中，通过对同一个消息的密文在新老密钥下的周期性更新，实现加密与更新的不可区分性，从而在安全可靠的前提下，达到高效扩展区块链的目的。

（6）链下扩容技术。区块链链上容量是较为有限的，通过将部分链上动作移出到链外可以提高区块链的效率，例如状态通道、闪电网络等技术。一般而言，这些技术通过牺牲一定的可用性以提高计算与存储的可扩展性。

### 1.2 安全与隐私保护问题

区块链的安全性包括系统安全和信息安全两个方面。区块链系统的安全问题可能发生在三个不同的层次：一是网络层，即底层点对点网络的安全，在公有链系统中，通过“女巫攻击”（即伪造多个节点与特定节点通讯的方式），可以使特定节点不能正常工作[4,5]。二是共识层，即共识机制本身的安全，如采用工作量证明的区块链中存在的51%算力攻击，可通过获取大量算力控制特定时段网络区块的打包[6]。三是智能合约层，即区块链上智能合约代码的漏洞，比如以太坊 The DAO 事件，该合约漏洞当时造成了价值数千万美金的加密货币损失[7]。区块链的信息安全的核心是确保系统中用户的各种隐私得到有效保护。区块链隐私保护的关键在于保证不影响去中心化的同时，确保用户的隐私不会因交易公开而暴露。现有的公有链系统中，隐私问题是一个重要挑战，以比特币为例，尽管地址是匿名的，但是在与其他实体的交互过程中容易被反匿名，从而导致用户交易记录的隐私泄露[8]。为实现区块链的安全与隐私保护，须攻关的关键技术包括：

（1）密码算法与安全协议。密码算法是区块链系统的基石，研究点包括满足区块链系统需求的密钥安全存储与防护技术、数字签名、零知识证明、安全多方计算等。

（2）可信身份协同管理技术。区块链身份协同管理技术包括跨区块链、链上链下用户身份的信用评估、认证、检测及管理机制，通过这些机制来保障交易的安全性。

（3）数据隐私保护技术。包括不同形态区块链系统的数据隐私保护方法、交易层数据隐私保护机制等，确保区块链节点数据安全的同时保证数据便于维护。

（4）用户身份隐私保护技术。区块链用户的个人数据隐私保护机制是区块链广泛应用的关键，可避免用户身份泄露而造成用户的损失。

### 1.3 区块链的监管审计问题

由于区块链上用户匿名、信息不可篡改，因而如何“审计”链上行为和数据，确保系统良性发展是区块链技术存在的重要问题。区块链的监管与审计，可以通过分析区块链数据，及时识别用户行为，并预警非法行为，如欺诈行为、链上数据的异常行为等[9,10]。以比特币为代表的区块链采用了一种新的隐私模型，即交易细节全部公开，而用户匿名。此外，比特币区块链系统中包含大量的用户数据，这些数据公开可查，为研究人员对区块链数据进行挖掘分析提供了前所未有的机会。然而，由于用户匿名和去中心化组织导致系统中用户行为不可控，且目前区块链生态中尚缺乏有效的监管，区块链平台成为各种网络犯罪高发地[11-13]。因此，做好非法行为的预警是进一步完善区块链生态的必要条件。区块链的监管与审计关键技术包括：

（1）交易追溯技术。对区块链的交易行为进行追溯，针对恶意或异常交易进行溯源和可视化展示，确保交易行为的健康可持续发展。

（2）异常交易检测技术。针对区块链上的异常或非法交易行为进行检测，提供及时预警，实现区块链的风险控制和安全管理。

（3）非法行为识别技术。识别区块链交易欺诈、合约欺诈、赌博诈骗等非法行为，实现实时监控，及时发现恶意用户或节点，保障区块链的安全运行。

（4）用户身份推测与追踪技术。针对具有异常或非法行为的用户，推测其身份并追踪其轨迹，为打击网络犯罪提供追踪信息，减少利用区块链进行违法犯罪的行为。

### 1.4 区块链智能合约开发与保障问题

一般来说，区块链智能合约的出现标志着区块

链 2.0 时代的到来。凭借着区块链的去中心化、难以篡改等特性，区块链智能合约可以被用于承载去中心化的应用。然而，当前智能合约的发展面临许多问题，如缺乏统一的平台语言、合约可能存在漏洞导致巨大的经济损失等[14,15]。因而，高效地开发安全、可靠的智能合约是促进区块链技术应用发展的重要因素[16]，其中涉及的关键技术包括：

（1）合约一致性证明。保证智能合约与用户期望的一致性，确保合约按用户要求准确执行。

（2）合约设计开发。在智能合约开发过程中，优化其开发、编译及部署运行等问题，设计高效的智能合约，降低计算消耗，节省合约资源开销。

（3）合约漏洞检测技术。对智能合约在部署前进行安全漏洞检测，包括验证技术、测试技术等，防止合约受到恶意攻击。

（4）合约可靠性保障技术。提升智能合约软件代码的可靠性，保障合约在区块链系统中稳定运行。

## 2　发展趋势与影响分析

区块链当前处于发展初期，具有以下发展趋势及影响：

（1）打造全新信息化基础设施，实现价值互联。随着区块链技术在各个行业的应用落地，区块链技术将成为个人与企业信息上链、资产上链、交易上链、各类服务上链的重要支撑，进而发展成一种重要的社会信息化基础设施，实现基于区块链的价值互联与流转。

（2）打通数据孤岛，提升社会效率。在大数据时代，数据成为重要的资产。然而，数据孤岛问题成为数据发挥价值的拦路虎。区块链技术结合分布式机器学习、隐私计算等技术手段，有望成为打通数据孤岛、实现数据在保护用户隐私前提下进行融合计算的重要支撑工具。数据孤岛的打通，将极大地释放数据的价值、实现社会效率的提升。

（3）重构信任格局，重塑行业形象。当前，在某些领域存在公众对企业、行业信任不足的问题，制约行业的发展。区块链技术具有方便追溯、不可篡改等特征，结合其他辅助手段，能够重构社会信任关系格局，将公众对企业的信任转变为对政府可监管、群众可参与的区块链技术的信任，重塑行业形象。

（4）应用金融领域，促进科技发展。区块链具有的不可篡改和解决信任问题的特点使其拥有在金融领域应用的天然优势，可以很好地解决多方协同的记账问题，能够为数字货币和数字资产提供底层技术支撑，也能促进金融产品交易、保险、普惠金融、金融监管等方向的发展。

（5）服务政府部门，提升管理能力。除了在商业上的应用，在政府部门的流程优化上，区块链也拥有较大的应用空间。对政府部门来说，安全保障是政务执行和各项工作正常运转的基础条件，其中包括通信安全、数据安全、信息安全等。而区块链技术可以对链上信息提供溯源依据，从而确保网络上的数据和信息的可信及可靠。区块链有望成为推进国家治理体系和治理能力现代化的一项有力抓手。

（6）变革中介行业，推动新业态诞生。部分中介行业存在的主要原因是打造中心化平台，利用信息不对称赚取利润。随着区块链技术的发展和民众对技术的理解、接受，区块链技术凭借去中介化的特点，结合人工智能等技术，将首先取代部分低价值中介行业，进而实现对中介行业的变革。而围绕区块链平台，将可能诞生新的业务场景和服务模式。

（7）革新法律行业，更新监管模式。区块链因具有分布式、防篡改、可追溯等特点已被成功应用于司法存证，随着区块链技术的发展和行业应用的推广，未来法律行业将面临全新的证据形式，围绕区块链数据的法律服务将成为法律行业的重要组成部分。此外，随着链上数据的积累，基于区块链数据的各类监管、取证将成为未来国家监管的重要一环。现有监管体系结合区块链技术将诞生全新监管模式，促进社会进步。发展基于区块链技术的监管手段，创新监管模式将成为重要研究课题。

## 3　对策建议

为了促进我国区块链技术发展，占领技术制高点，本文提出如下对策建议：

（1）培育自主可控区块链系统，确立区块链生态优势。区块链有机会成为未来的商业基础设施。我国需大力推动自主可控的区块链系统研发，进行核心技术攻关，促进区块链开源社区建设，丰富国产区块链应用生态，占据创新制高点，取得产业新优势。

（2）平衡各方利益，推动产业改革。当前，联盟区块链虽然在各产业中均有一定应用，但距离取代原有商业模式仍有巨大距离。究其原因，很大程度上是产业中的既得利益者不愿参与，因为区块链所

代表的分布式商业模式将减少寡头和中介的既得利益。可以考虑从政府的角度扶持成立产业联盟，促进新商业模式的落地，政府牵头平衡各方利益，从而推动产业改革。

（3）鼓励开源社区，促进技术发展。开放源代码是技术发展的重要手段，当前国内区块链技术产品虽然有一部分进行了开源，但是仍有较大的开放空间。大量的闭源软件限制了技术的发展及创新的速度。国家可鼓励区块链开源社区的发展，如向开源社区提供经费支持、鼓励开源社区交流活动等，促进区块链技术的开源和创新。

（4）加强监管力度，防范金融风险。区块链技术与数字货币等新兴技术需要监管力量来引导其发展。一是引入多方力量共同参与区块链监管技术的研发，改进面向区块链技术的各类监管手段与技术。二是严厉打击披着区块链“外衣”的各类骗局，虽然首次代币融资、加密货币交易所等在中国境内已经被禁止，但在社会上仍有许多打着区块链旗号的融资项目，其中不乏庞氏骗局、蜜罐骗局等，这些骗局严重影响了人民的财产安全和区块链技术的健康发展。三是提前预防 Libra 等超主权货币对我国货币政策和支付体系的冲击，做好提前布局。

（5）协调法规标准，建设符合国情的区块链系统。区块链技术具有永久记录的特性，这与我国现行法律中信息保护的“被遗忘权”相抵触；而现有的金融法律法规，也无法适用于区块链为基础的分布式商业上的金融行为。因此，还需从国家现有国情出发，协调各项政策法规、行业和技术标准与区块链之间的矛盾，保障民众权益的同时促进区块链技术合理发展。

（6）设立专项资金，促进区块链基础理论与核心技术研发。当前各地纷纷出台区块链扶持政策，大部分是从企业角度对各类区块链初创公司进行激励、补贴。但是我国目前区块链技术的基础理论研究及关键技术研究仍然较薄弱，需要重点突破。可考虑围绕区块链关键技术与应用，通过设立应急科学研究项目、重点项目群或重大研究计划项目等方式支持区块链基础理论和关键技术的突破，促进产学研协同健康发展。

**致谢** 感谢研讨会各位专家和领导的建设性意见，为本文提供了很好的素材。

## 参 考 文 献

[1] Bonneau J, Miller A, Clark J, et al. Sok: research perspectives and challenges for bitcoin and cryptocurrencies//Proceedings of the 2015 IEEE Symposium on Security and Privacy. 2015: 104—121.

[2] Pan C, Liu Z, Liu Z, et al. Research on scalability of blockchain technology: problems and methds. Journal of Computer Research and Development, 2018, 55(10): 2099—2110.

[3] Ethereum. Sharding-FAQs[EB/OL]. https://github.com/ethereum/wiki/wiki/Sharding-FAQs.

[4] Otte P, De Vos M, Pouwelse J. TrustChain: a sybil-resistant scalable blockchain. Future Generation Computer Systems, Elsevier, 2017.

[5] Efanov D, Roschin P. The all-pervasiveness of the blockchain technology. Procedia Computer Science, 2018, 123: 116—121.

[6] Li X, Jiang P, Chen T, et al. A survey on the security of blockchain systems. Future Generation Computer Systems, 2017.

[7] Atzei N, Bartoletti M, Cimoli T. A survey of attacks on ethereum smart contracts (sok)//International Conference on Principles of Security and Trust. 2017: 164—186.

[8] Meiklejohn S, Pomarole M, Jordan G, et al. A fistful of bitcoins: characterizing payments among men with no names//Proceedings of the 2013 conference on Internet measurement conference. 2013: 127—140.

[9] Vasek M, Moore T. There's no free lunch, even using Bitcoin: Tracking the popularity and profits of virtual currency scams//International conference on financial cryptography and data security. 2015, 8975: 44—61.

[10] Chen W, Zheng Z. Blockchain data analysis: a review of status trends and challenges. Journal of Computer Research and Development, 2018, 55(9): 1853—1870.

[11] Lischke M, Fabian B. Analyzing the bitcoin network: the first four years. Future Internet, 2016, 8(4): 7.

[12] Tasca P, Hayes A, Liu S. The evolution of the bitcoin economy: extracting and analyzing the network of payment relationships. Journal of Risk Finance, 2018, 19(2): 94—126.

[13] Chen W, Zheng Z, Cui J, et al. Detecting Ponzi schemes on Ethereum: towards healthier blockchain Technology// Proceedings of the 2018 World Wide Web Conference. 2018: 1409—1418.

[14] Chatterjee K, Goharshady AK, Velner Y. Quantitative analysis of smart contracts//European Symposium on Programming. Cham: Springer International Publishing, 2018: 739—767.

[15] Huang Y, Kong Q, Jia N, et al. Recommending differentiated code to support smart contract Update// Proceedings of the 27th International Conference on Program Comprehension. IEEEPress, 2019: 260—270.

[16] Weiqin Z, David L, Pavneet Singh K, et al. Smart contract development: challenges and opportunities. IEEE Transactions on Software Engineering, 2019.

## Problems in Blockchain and Suggestions for Counterplan

Liu Zhe[1,2]　Zheng Zibin[3]　Song Su[1]　Zhang Zhaotian[1]

(1. *Department of Information Sciences, National Natural Science Foundation of China, Beijing* 100085;
2. *College of Computer Science and Technology, Nanjing University of Aeronautics and Astronautics, Nanjing* 211106;
3. *School of Data and Computer Science, Sun Yat-sen University, Guangzhou* 510006)

**Abstract**　This paper analyzed and summarized the current problems of blockchain in terms of four aspects, which were scalability of blockchain, security and privacy protection, supervision and audit for blockchain and development and security of smart contract, with the elaboration of the key technologies that required to be solved for each problem. Then the paper further discussed the development trends and influences of blockchain technology. Finally, several suggestions for counterplan were given.

**Keywords**　advanced information technology; blockchain; key technologies; development trends; suggestions for blockchain counterplan

（责任编辑　齐昆鹏）

·资料信息·

# 我国学者揭示湖泊硅藻生物硅的重要“铝汇”作用

在国家自然科学基金项目（批准号：41772041，41202024，40872042）等资助下，中科院广州地球化学研究所袁鹏研究员课题组在硅藻驱动的硅—铝地球化学共循环机制研究中取得重要进展。相关成果以“Lake Sedimentary Biogenic Silica from Diatoms Constitutes a Significant Global Sink for Aluminium”（湖泊沉积硅藻生物硅构成地球的重要铝汇）为题，于 2019 年 10 月 23 日发表在 *Nature Communications*（《自然—通讯》）上。中科院广州地球化学研究所刘冬副研究员和袁鹏研究员为论文的共同第一作者，袁鹏为通讯作者。论文链接：https://www.nature.com/articles/s41467-019-12828-9。

铝是地壳中丰度最高的金属元素，其循环和归趋不仅与多种成岩成矿作用密切相关，也显著影响着诸多生物地球化学过程。硅藻是一种具有硅质细胞壁（矿物成分为蛋白石）的浮游微生物，广泛分布于各种水体。其通过光合作用吸收二氧化碳的量约占地球生态系统的五分之一，因此，硅藻生物硅的归趋对于理解全球硅、碳等元素循环具有极为重要的意义。硅藻的生命活动及相关生物地球化学过程受到其生长环境中元素浓度的影响。天然淡水湖泊中具有较高的溶解铝浓度（可达微摩尔每升）。然而，对湖泊生物硅在高铝浓度条件下的结构—成分“响应”一直以来缺乏研究认识，制约了对硅藻生物硅的地球化学行为及其效应的深入理解。

袁鹏课题组从我国淡水湖泊中采集了代表性种属的淡水硅藻以提取其生物硅，与在模拟湖泊水体条件下培养所得硅藻的生物硅进行对比研究；运用高分辨微区分析和精细谱学方法，系统研究了湖泊硅藻生物硅中铝的赋存状态和含量。研究发现，铝以类质同象置换硅的形式在硅藻生物硅结构中稳定赋存且含量较高。采用湖泊生物硅沉积率数据测算得出，汇集于湖泊沉积硅藻生物硅中的铝量堪比海洋沉积硅藻生物硅中的铝量，从而揭示出湖泊硅藻生物硅是地球的重要“铝汇”。该研究还指出，湖泊硅藻生物硅的溶解率因其高铝含量而显著降低，这可能是湖泊硅藻“生物泵”作用固碳效率高的重要原因。

鉴于硅藻在全球生物地球化学循环中的重要作用，该研究揭示的“硅藻—矿物基体—溶解铝”之间的独特界面反应机制，为研究硅藻驱动的硅—碳—铝元素循环、硅藻沉积固碳作用乃至硅藻土成矿机制提供了新的依据，对深入理解硅藻生物地球化学行为及其环境效应具有重要意义。

（供稿：地球科学部　陈　曦　初　航　任建国）