计 算 机 研 究 与 发 展
Journal of Computer Research and Development
DOI: 10.7544/issn1000-1239.202220892
61(4): 1018−1037, 2024

能源区块链的跨链服务安全技术研究进展

何云华[1] 罗明顺[1] 胡 晴[2] 吴 槟[3] 王 超[1] 肖 珂[1]
[1](北方工业大学信息学院 北京 100144)
[2](中国兵器科学研究院 北京 100089)
[3](信息安全国家重点实验室(中国科学院信息工程研究所) 北京 100093)
(heyunhua610@163.com)

Research Progress on Security Technology for Cross-Chain Service of Energy Blockchain

He Yunhua[1], Luo Mingshun[1], Hu Qing[2], Wu Bin[3], Wang Chao[1], and Xiao Ke[1]
[1] (*School of Information Science & Technology*, *North China University of Technology*, *Beijing* 100144)
[2] (*China Research Development Academy of Machinery Equipment*, *Beijing* 100089)
[3] (*State Key Laboratory of Information Security* (*Institute of Information Engineering*, *Chinese Academy of Sciences*), *Beijing* 100093)

Abstract Driven by the carbon peaking and carbon neutrality goals of China, the digital transformation of the energy industry is imperative. With the application and development of blockchain in the digital transformation of the energy industry, the concept of energy blockchain has gradually formed a consensus. Energy blockchain is a new industrial form of the deep integration of the blockchain technology and the energy Internet, which can facilitate efficient collaboration between energy entities and provide technical support and services for innovative business models such as green and low-carbon business. The large-scale development of energy blockchain is inseparable from the breakthrough of multi-level cross-chain technology, but the cross-chain service of energy blockchain still faces many problems. We divide the current research status of energy blockchain into five categories, namely energy blockchain architecture, smart contract applications, cross-chain technology, blockchain node management and blockchain privacy protection, and we summarize the related research work in these five directions respectively, sort out the principles, advantages and disadvantages of each research scheme in detail; then, in order to promote the development of the cross-chain service security technology of the energy blockchain, we combine the supervision mechanism and the consensus mechanism to propose a multi-level cross-chain collaborative supervision of the energy blockchain architecture, according to the actual needs of the energy blockchain; finally, we summarize problems that need to be solved in the energy blockchain cross-chain service security technology, and put forward the research prospect of blockchain in the energy field.

Key words energy blockchain; regulatory architecture; cross-chain services; node management; privacy protection

收稿日期: 2022-10-21; **修回日期**: 2023-05-06

基金项目: 国家自然科学基金项目(62272007, U23B2002); 北京市自然科学基金项目(M21029); 云南省区块链应用技术重点实验室开放课题(174009); 北京市教育委员会科学研究计划项目(KM202010009010, KM202010009008); 北京市属高校教师队伍建设支持计划项目优秀青年拔尖人才培育计划(BPHR202203031); 区块链技术与数据安全工业和信息化部重点实验室开放课题(20243222)
This work was supported by the National Natural Science Foundation of China (62272007, U23B2002), the Beijing Natural Science Foundation (M21029), the Open Topics of Yunnan Key Laboratory of Blockchain Application Technology (174009), the Research and Development Program of Beijing Municipal Education Commission (KM202010009010, KM202010009008), the Excellent Young Talents Project of the Beijing Municipal University Teacher Team Construction Support Plan (BPHR202203031), and the Open Topics of Key Laboratory of Blockchain Technology and Data Security, The Ministry of Industry and Information Technology of the People's Republic of China (20243222).

通信作者: 胡晴(huqing_57@163.com)

摘　要　在“双碳”目标推动下，能源产业数字化转型势在必行. 随着区块链在能源行业数字化转型应用和发展，能源区块链概念逐渐形成共识，它是区块链与能源互联网深度融合的产业新形态，可助力能源主体之间的高效协作，为绿色低碳等创新业务模式提供技术支撑与服务. 能源区块链的规模化发展离不开多层次跨链技术的突破，但能源区块链的跨链服务还面临着许多问题. 将目前能源区块链领域的研究现状分为 5 类，即能源区块链架构、智能合约应用、跨链技术、区块链节点管理和区块链隐私保护，针对这 5 个方向分别总结相关研究工作，详细梳理出各研究方案的原理、优势与不足；然后，为促进能源区块链的跨链服务安全技术的发展，根据能源区块链的现实需求，结合监管机制与共识机制提出多层次跨链协同监管的能源区块链架构；最后，总结出能源区块链跨链服务安全技术中亟待解决的问题，并提出区块链在能源领域的研究展望.

关键词　能源区块链；监管架构；跨链服务；节点管理；隐私保护

中图法分类号　TP391

在“双碳”目标推动下，作为碳减排主力的能源产业积极开展数字化转型. 区块链（blockchain）作为当前数字技术自主创新的突破口和“新基建”的重要组成部分，因其具有分布式数据存储、点对点传输、共识机制和加密算法等特点[1]，为能源产业数字化转型提供新契机[2]，助力能源行业高效协作，重塑能源价值链. 能源产业已经开展了区块链的探索和试点. 2017 年，中国中化集团有限公司开展了能源石化交易区块链应用试点；2020 年国家电网开始“国网链”建设，在分布式电力交易、可再生能源电力消纳、安全生产、电费结算和透明化调度管理等方面进行试点和应用；2021 年 5 月，国家电网牵头的全球首个“区块链+碳交易”国际标准获批立项. 美国 LO3 Energy 公司基于以太坊开展了全球第 1 个点对点（peer to peer, P2P）光伏电力交易试点；2020 年，IBM 与欧洲 3 家电网运营商建立区块链新能源平台 Equigy；澳大利亚 Power Ledger 公司将区块链应用到可再生能源行业推动可再生能源的生产、交易和认证. 国际市场调查机构 Alexa Reports 预测，2025 年应用于能源领域的区块链市场价值将达 34.7 亿美元.

由于能源行业的综合性、多样性和数据分散性，能源、信息和资金的流动非常复杂，虽然互联网可以实现信息高速流通，但由于主体信任问题，能源互联网无法实现能源信息和能源的低成本、高效率流动[3]. 众所周知，区块链技术具有去中心化、可追溯、不可篡改等特点，是一种信任实现技术. 区块链目前发展迅速，运用场景广泛. 尽管在有些场景下区块链的引入会带来系统性能降低、共识算法复杂等问题，但是可以结合博弈论、激励机制、共识算法设计与区块结构设计等对区块链系统进行优化，使其性能符合能源行业的要求[4]. 因此，区块链适用于参与主体多、流程长的能源交易场景，能够解决中心化环节的信任问题，并满足场景业务性能要求. 因此，能源区块链的概念被提出并逐渐形成共识. 能源区块链是区块链与能源生产、传输、存储、消费以及能源市场深度融合的能源产业发展的一种新形态，以区块链为底层基础技术，深度融合能源互联网，构建开放合作的主体信任体系，为各类开放融合的创新业务模式提供技术支撑与服务. 能源区块链打破产业链上中下游的信息流、实物流和资金流信息壁垒，促进产业链多方单证、合同、物流和销售等业务的高效协同，将在能源数据共享、分布式电力交易、可再生能源消纳、碳交易监管等应用领域中发挥重要作用.

能源区块链的发展很大程度上依赖于区块链跨链服务技术的突破. 能源区块链要实现同一行业内不同平台的互联，需跨链服务打破平台之间的数据孤岛，实现平台之间的数据共享[5]；能源区块链要实现跨区域互联，需考虑区域内区块链数据上链、查询及业务计算的效率问题，区域内建立独立的区块链是必然趋势，不同区域的独立区块链要实现互联需依赖跨链服务；能源区块链要实现业务或行业数据互通，需考虑不同业务或不同行业所构建区块链的差异，需跨链服务联通差异化的区块链实现数据共享和融合[6]. 因此，区块链跨链服务技术对能源区块链的发展至关重要.

随着能源行业数字化转型的推进，能源区块链逐渐得到关注，能源区块链的研究及跨链服务安全技术也成为了学术界和工业界研究的热点之一，目前已有部分学者就能源领域中区块链的应用方面的研究工作进行了综述[7-11]，但还没有针对能源领域中区块链跨链服务安全技术的进展进行系统性整理. 我们从研究角度分析了相关综述文献与本文的主要区别，如表 1 所示.

本文对近 5 年区块链在能源领域中的相关研究

Table 1 Differences Compared with Existing Reviews

表 1 与现有综述的区别

现有综述	主要工作	与本文的主要区别
Blockchain technology in the energy sector: A systematic review of challenges and opportunities[7]	回顾了 140 个区块链研究项目和初创公司，从中构建区块链在能源应用中的潜力和相关图. 根据活动领域、实施平台和所使用的共识策略，系统地分为不同的类别.	该综述专注于如何使用区块链技术解决去中心化市场、电动汽车充电和电动汽车面临的问题，但是并未考虑安全因素.
Blockchain and energy: A bibliometric analysis and review[8]	通过参考文献的共被引分析，分析了区块链与能源的交叉点. 使用探索性因素分析，确定了 6 个不同的研究方向.	该综述通过共被引分析将区块链在能源领域的研究方向分为 6 类，与本文有相似部分，但是并未考虑跨链技术带来的安全影响.
Integrating blockchain technology into the energy sector — From theory of blockchain to research and application of energy blockchain[9]	回顾了区块链理论，利用可视化文献计量分析方法和 Scopus 数据库，探讨 2014—2020 年能源区块链研究和应用现状.	该综述专注于研究能源区块链未来发展的可能趋势，并总结了区块链的核心技术，认为区块链为能源可持续性提供动力，但同样未考虑跨链技术带来的安全影响.
A comprehensive review of energy blockchain: Application scenarios and development trends[10]	从学术研究、企业和试点项目布局、政府扶持政策 3 个方面对区块链在能源领域的进展进行了概述.	该综述专注于对能源区块链部署提供决策支持，仅初步介绍了部分区块链技术.
A survey of blockchain applications in the energy sector[11]	回顾了区块链技术在能源应用中部署过程，即从能源管理到点对点交易，再到电动汽车相关应用和碳排放交易等.	该综述专注于讨论具体场景下的区块链架构，并分析隐私问题，但是并未考虑安全与监管的需求.

进行梳理，主要集中在电力行业期刊与会议，以及网络安全行业的期刊与会议等，针对 5 个方面做出调研分析：1)能源区块链交易架构，包括单场景交易架构和多场景交易架构等；2)智能合约应用，包括能源交易、电力规划、可再生能源消纳、电力定价和能源数据共享等；3)跨链技术，包括常见的跨链技术应用和跨链技术在能源区块链的探索工作；4)区块链节点安全管理，包括区块链节点接入认证、区块链节点权限管理和区块链节点行为审查；5)区块链隐私保护，包括数据隐私保护与智能合约隐私保护. 此外，为促进能源区块链跨链服务安全技术的发展，本文提出多层次跨链协同监管的能源区块链架构，并指出当前技术发展遇到的关键问题，为下一步研究指明方向.

1 基础知识

本节对能源区块链跨链服务安全技术所涉及的区块链相关知识与跨链技术相关知识进行介绍，并提出能源区块链国网链架构，明确能源区块链跨链服务安全技术的概念.

1.1 区块链相关知识

区块链是通过去中心化的方式集体维护一个可靠数据库的技术方案，由一串使用密码学方法产生的数据块即区块组成，每一个区块都包含了上一个区块的哈希(Hash)值，从创世区块(genesis block)开始连接到当前区块，形成块链[12]. 被纳入新基建的区块链，以数据不可篡改、可公开监管、便于查证的特性，广泛应用于有多方参与的系统中，为多方交互的信息(行为、数据等)提供可靠的存证[13].

起初区块链是以比特币为代表的数字货币应用的底层技术，其应用场景包括支付、流通等. 随着以太坊加入智能合约功能，使得区块链拓展到股权、产权的登记和转让、证券及金融合约的交易和执行等金融领域. 伴随可扩展性和效率的提高，区块链应用范围目前已拓展到身份认证、公证、审计、物联网、医疗、能源等领域[14]，将成为未来社会的一种最底层的协议.

节点是区块链架构的关键组成部分，承担同步数据、参与共识、验证区块、执行交易等作用. 根据区块链节点的准入机制以及数据读写权限和管理权限的不同，区块链可以分为公有链(public chain)[15]、私有链(private chain)[16]与联盟链(consortium chain)[17]. 公有链中，网络上的任何区块链节点都可以自由加入系统，由于数据读写权限并未设置，链上节点可以任意查看区块链上的信息，因此公有链开放性好. 比特币系统、以太坊系统等最著名的区块链系统均为公有链. 私有链所有节点属于同一个组织，只有获得管理员批准的计算设备才可以加入系统，因此私有链安全、隐私性较好. 目前我国各大银行内部运行的区块链系统大多属于私有链. 联盟链节点属于有紧密联系的若干组织或个人，介乎于公有链与私有链

之间，由一组管理员来共同协调管理. 因此联盟链是开放性与安全隐私的折中. 目前我国金融界的跨企业区块链系统大多属于联盟链.

1.2 跨链技术相关知识

跨链技术是实现价值区块链互联网的关键，是实现区块链可扩展性和连接性的桥梁. 当前对跨链技术的研究主要有 4 种策略：公证人（notary schemes）机制[18]、侧链中继（sidechains, relays）机制[19]、哈希时间锁定（Hash time lock）机制[20]和分布式私钥控制（distributed private key control）技术[21]. 目前主流的跨链技术及其代表项目如表 2 所示.

1）公证人机制本质上是一种中介机制，即把受信任的第三方当作中介，以验证和转发双方的跨链消息. 公证人机制的优点是可以灵活地支持具有不同结构的各种区块链，缺点是存在集中化的风险.

典型公证技术为瑞波提出的 Interledger 协议[22]，Interledger 协议使 2 个不同的记账系统可以通过第三方“连接器”或“验证器”互相自由地传输货币. 记账系统无需信任“连接器”，因为该协议采用密码算法用连接器为这 2 个记账系统创建资金托管，当所有参与方对交易达成共识时，便可相互交易. 该协议移除了交易参与者所需的信任，连接器不会丢失或窃取资金，这意味着，这种交易无需得到法律合同的保护和进行过多的审核，大大降低了门槛. 同时，只有参与其中的记账系统才可以跟踪交易，交易的详情可隐藏起来. “验证器”是通过加密算法来运行，因此不会直接看到交易的详情. 理论上，Interledger 协议可以兼容任何在线记账系统，而银行现有的记账系统只需小小的改变就能使用该协议. 从而使银行之间可以无需中央对手方或代理银行就可直接交易.

2）在侧链中继机制中，侧链是指完全具有链功能的另一个区块链，可以主动感知主链信息并采取相应的动作. 中继链是侧链和公证机制的结合，具有验证跨链消息和转发跨链消息的能力.

典型的侧链应用为 BTC Relay[23]，BTC Relay 把以太坊网络与比特币网络通过使用以太坊的智能合约连接起来，可以使用户在以太坊上验证比特币交易. BTC Relay 通过以太坊智能合约创建一种小型版本的比特币区块链，但智能合约需要获取比特币网络数据，比较难实现去中心化. BTC Relay 进行了跨区块链通信有意义的尝试，打开了不同区块链交流的通道.

3）哈希时间锁定机制是闪电网络中提出的一种资产原子交换技术，它提供哈希值的原始值以在指定的时间内实现资产的原子交换，但是该技术只能实现资产交换，不能进行信息传递，因此其使用场景受到限制.

4）分布式私钥控制技术是指通过对分布式私钥实现锁定和解锁操作，把加密货币资产锁定到基于区块链协议的内置资产模板的链上，再部署智能合约解锁来创建出新的加密货币资产.

根据上述 4 种策略的相关工作，目前的跨链工作主要集中在资产交换和跨链通信[24-26]. 很少有信息交换过程中的真实性、实时性和跨链写入互斥的相互研究.

1.3 能源区块链国网链架构

作为数字时代的“信任机器”，区块链技术是数字赋能，驱动数字经济高质量发展的关键支撑. 以国家电网公司为代表的国有企业把握科技创新，加强创新主体与跨界创新的持续融合，不断突破地域和组织界限，为推动科技创新活力、发展我国数字经济、抢占全球数字经济发展制高点作出贡献.

为专注区块链专业研究与建设，国网区块链科技（北京）有限公司于 2019 年 8 月 22 日正式成立，开启了构建以“区块链+大数据+人工智能”为核心驱动的区块链行业生态建设之路. 截至目前，公司以自主研发的区块链底层技术服务平台为基础，依托司法信用“天平链”、能源电力“国网链”、“央企联盟链”3 大区块链基础设施，实现区块链在新能源云、电力交易、优质服务、综合能源等业务场景的融合.

Table 2 Cross-Chain Technology Comparison

表 2 跨链技术对比

跨链技术	信任模型	互操作性	跨链资产交换	跨链资产转移	多币种智能合约	代表项目
公证人机制	多数公证人诚实	所有	支持	支持（需要长期公证人信任）	困难	Ripple
侧链中继机制	链不会失效或受到 51% 攻击	所有（需要所有链有中继）	支持	支持	困难	Cosmos/ Polkadot
哈希时间锁定机制	链不会失效或受到 51% 攻击	只有交叉依赖	支持	不支持	不支持	Lightning network
分布式私钥控制技术	链不会失效或受到 51% 攻击	所有	支持	支持	支持	WanChain

其中“国网链”是国内最大的能源区块链公共服务平台，创造性地提出“一主两侧多从”的主体架构，如图 1 所示. “国网链”分为主链、数据侧链、交易侧链、网省从链、堆栈从链 5 部分. 截至目前，“国网链”已在国网北京、青海、辽宁等多个省电力公司部署应用，在共享储能、电力交易等 25 个具体业务场景落地实践，上链数据超 1 亿条.

2 能源区块链的研究现状

2.1 基于区块链的能源交易架构

基于区块链的能源交易架构在国内外都已经开展了不少研究工作，根据基于区块链的能源交易场景的不同，把能源区块链交易架构分为单场景交易架构和多场景交易架构.

1) 单场景交易

针对单场景交易，Yan 等人[27]提出了一种基于微电网的区块链架构，便于用户在微电网中进行碳配额交易和权衡交易速度、微电网收益与分销网络限制. 该架构中区块链网络中的拟议参与者是配电系统操作员和微电网. 微电网是通过配电系统操作员与同行进行能源和碳排放交易的市场参与者. 位于微电网中的智能电表记录交易、调度交易并将交易存储在区块链中. 配电系统操作员使用微电网可用的通信网络管理交易. 微电网和配电系统操作员都参与区块链验证和共识过程. 因此，配电系统操作员和微电网交换交易、创建数据块，并将它们存储在区块链中.

具体流程如图 2 所示：①微电网将交易数据发送到市场清算智能合约；②市场清算智能合约向配电系统操作员发送交易数据；③配电系统操作员清算市场并向市场清算智能合约发送清算结果；④市场清算智能合约向微电网发送清算结果；⑤市场清算智能合约向交易确认智能合约发送清算结果；⑥交易确认智能合约查询智能电表以获取实时数据；⑦交易确认智能合约为每个微电网清算付款.

除该架构外，Yang 等人[28]为物联网辅助智能家居构建了一种基于区块链的新型交易式能源管理架构，使智能家居能够与能源互联网系统中的电网和其他用户进行交互；Abishu 等人[29]在此基础上提出了新的共识机制，利用了实用拜占庭容错(practical Byzantine fault tolerance, PBFT)和信誉共识(proof of reputation, PoR)的优势保证了能源交易的高可靠性、高吞吐量、低延迟和网络强扩展性；Zhang[30]提出一种基于信誉风险评估的共识机制，实现对分布式能源交易的交易方信誉管理. 然而，面对如今能源区块链日渐复杂的趋势，单一的交易场景已经无法满足现状.

2) 多场景交易

一些研究人员也在多场景交易方面进行了研究. 在多能源交易方面，Deng 等人[31]提出一种电力和热力分配市场的实时 P2P 交易架构，如图 3 所示.

该结构有助于打破不同能源市场的壁垒. 其中区块链技术专为分布式 P2P 交易而设计，区块中记下的信息是一段时间内交易费用的总和，中央运营商在不知道每个产消者的详细价格和数量的情况下，获得所有产消者的费用总和并完成产消者之间的价值转移.

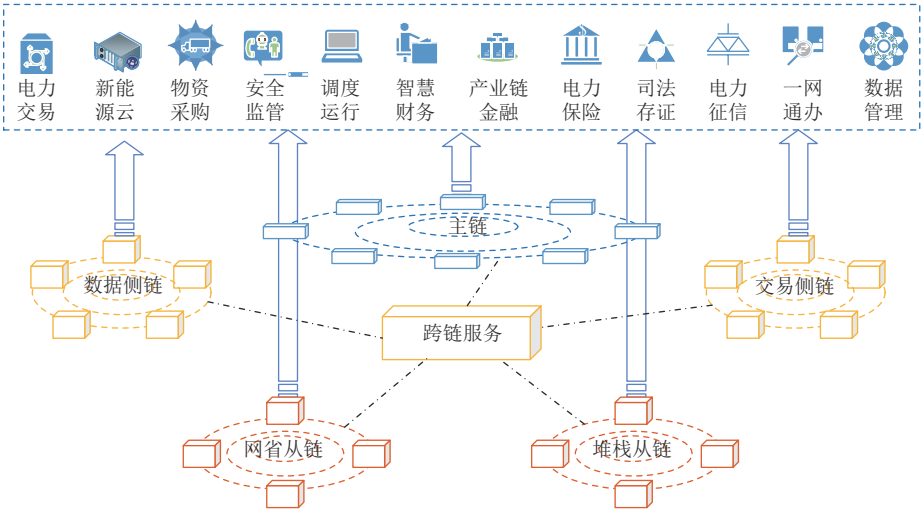


Fig. 1 Architecture of state grid blockchain

图 1 国内网链架构

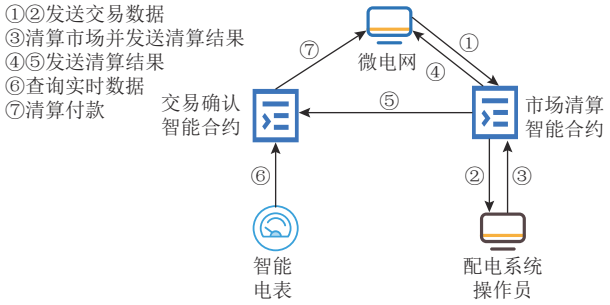


Fig. 2 Transaction process

图 2 交易流程

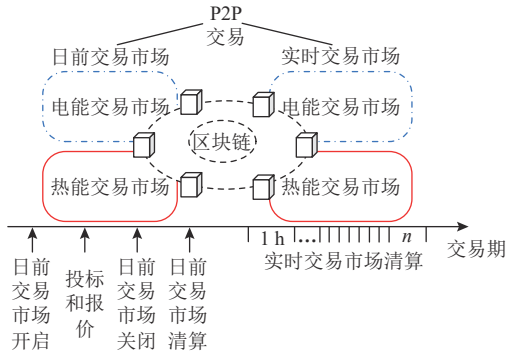


Fig. 3 Electricity trading and heating energy trading of energy blockchain

图 3 能源区块链电力交易与热能交易

Hamouda 等人[32]开发了一个综合交易能源市场框架，将大型电网的大容量发电、输电和较小的互联电网集群有效结合，既保护了公共事业公司的利益，又有利于客户和分布式发电所有者；龚钢军等人[33]设计了区块链聚合商与多个微网群联盟交易架构，针对包含冷热电联供系统的微网及聚合商 2 类节点，以多能互补为基本原则建立考虑碳配额机制及环境标识因数的节点模型；Yang 等人[34]为 P2P 能源交易架构提供了交易市场信用评级，能够根据用户行为评级进行交易撮合；Abdella 等人[35]则为整个能源区块链框架设计了性能评估功能，对区块链的延迟、可扩展性、系统吞吐量等指标进行评估.

然而，虽然目前针对多场景能源交易区块链的研究已有一些进展，但是多链架构未考虑跨平台、跨区域、跨业务的层次化跨链服务，也很少考虑跨链监管和共识的问题. 表 3 简要总结了基于区块链的能源交易架构研究现状.

2.2 能源区块链智能合约应用

智能合约能够用于实现各类能源交易相关的应用，是能源区块链得以推广应用的关键. 目前，能源区块链智能合约应用主要包括能源交易、电力规划、可再生能源消纳、电力定价和能源数据共享.

1）能源交易

能源交易、电力规划是智能合约应用较多的场景. 在能源交易场景中，van Leeuwen 等人[36]搭建了一个基于区块链的综合能源管理平台，为微电网社区提供双边交易. 通过采用区块链和智能合约技术，提议的分布式算法可以以安全、可验证的方式执行，确保市场参与者的独立性和匿名性. 在这些设置中，智能合约的作用至关重要. 智能合约是部署在区块链

Table 3 Research Status of Energy Trading Architecture Based on Blockchain

表 3 基于区块链的能源交易架构研究现状

类型	代表工作	描述	支持与电网/充电站交易	支持与对等用户交易	支持多类能源交易	其他机制	存在不足
单场景交易架构	Yan 等人[27]	基于微电网的区块链架构	是	否	是	激励	单一交易架构不适用我国能源交易现状
	Yang 等人[28]	基于区块链的新型交易式能源管理架构	是	是	否	隐私保护	
	Abishu 等人[29]	结合实用拜占庭容错（PBFT）和信誉证明（PoR）的共识机制	是	否	否	共识机制	
	Zhang[30]	基于信誉风险评估的共识机制	是	否	否	信用评估	
多场景交易架构	Deng 等人[31]	电力和热力分配市场的实时 P2P 交易架构	是	否	是	市场调度、隐私保护	未考虑层次化跨链服务、跨链监管和共识
	Hamouda 等人[32]	综合交易能源市场框架	是	否	否	增强需求响应	
	龚钢军等人[33]	区块链聚合商与多个微网群联盟交易架构	是	否	是	激励、智能合约	
	Yang 等人[34]	P2P 能源交易架构的市场信用评级	否	是	否	定价机制、信用评级	
	Abdella 等人[35]	对区块链框架进行了性能评估	是	否	是	共识机制	

上的一段计算机代码，可以在其他节点调用时执行某些功能. 智能合约接管了这个中央聚合器的功能，从而有效地充当虚拟聚合器. 在这个过程中，智能合约执行 3 种功能：①执行部分交叉方向乘子法 ADMM（alternating direction method of multipliers）算法；②与其他节点交换信息；③授予其他节点进行下一个操作的权限. 该平台内智能合约的功能如图 4 所示.

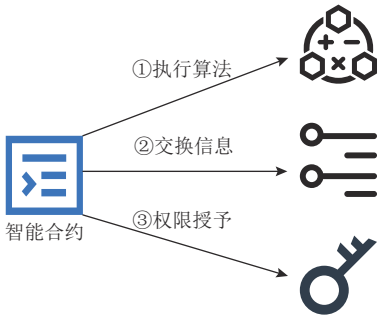


Fig. 4 Functions of smart contracts

图 4 智能合约的功能

Li 等人[37]提出采用智能合约技术实现整个微电网交易的流程，包括报价、匹配、电力转移、交易结算、分析统计和安全检查；穆程刚等人[38]将配售能源交易机制编写成智能合约，设计了一种考虑市场供需关系与网络约束的交易撮合模型；沈泽宇等人[39]提出基于区块链的分布式能源交易方案，将写有交易规则的能源交易智能合约部署上链，实现电力过网费差异的挂牌交易机制、可再生能源认证机制和信用管理机制等功能.

2）电力规划

在电力规划场景中，Kaur 等人[40]使用智能合约实现电网负载和供需的平衡. 本文通过智能合约检测供需差距情况，然后给供电端、用电端发送正或负响应需求，供电端、用电端计算其能源容量并传回智能合约，智能合约根据能源容量结果来制定用电端的激励策略. 该文提出的框架为参与者提供了一种可信且安全的媒介，可以实时交流和分享他们的能源数据. 此外，该框架还支持区块链的自治和去中心化平台，用于使用智能合约监控和执行交易. 通过使用设计的智能合约，参与实体可以为有效的需求响应管理做出贡献，以保持更高的电网稳定性，而无需依赖中心化的第三方执行有效的交易机制. 该文中智能合约的主要函数如图 5 所示.

Yang 等人[41]在分布式电力调度中，采用智能合约来实现供需调度策略确定后的储能租赁费管理和用电端的补偿费管理；Couraud 等人[42]提出采用智能

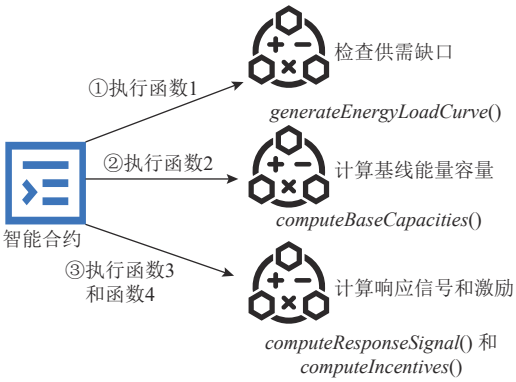


Fig. 5 Main functions of smart contracts

图 5 智能合约的主要函数

合约实现新型家庭能源管理系统的实时电力调度算法，在满足电力市场供需要求的同时，最大限度地提高住宅用户生产能源的用电量；黄伟等人[43]使用智能合约将系统分散式调度的运行模型等系统协议和规则转化为自动执行的程序，使得调度计算过程智能化、程序化、透明化.

3）其他应用场景

智能合约实现可再生能源消纳、电力定价和能源数据共享场景等工作也有少量的研究报道. 在可再生能源消纳场景中，Li 等人[44]提出使用智能合约使得可再生能源消纳规范化，实现高效的信息交互和协调管理. 在电力定价场景，Dabbaghjamanesh 等人[45]提出使用智能合约实现一种微电网的电力定价策略，根据电力需求为电力买家提供不同的报价；Zhang 等人[46]提出采用智能合约实现 P2P 能源交易的供需定价过程，该过程包括用户注册、竞价上传、查询、定价更新和交易触发等功能. 在能源数据共享场景，Wang 等人[47]提出了一种基于区块链的电网数据共享方案，通过智能合约实现细粒度数据访问控制，智能合约依赖于可信硬件的可信执行环境来保证安全性.

综上所述，能源区块链智能合约应用主要使用智能合约实现能源场景中的各实体之间的交互与协同，通常只考虑单一区块链场景，较少考虑多链场景，以及跨链合约部署和跨链合约计算的问题. 表 4 简要总结了能源区块链智能合约应用研究现状.

2.3 能源区块链跨链技术

跨链技术是实现价值区块链互联网的关键，是实现区块链可扩展性和连接性的桥梁. 当前对跨链技术的研究主要有 4 种策略[48]：公证人机制、侧链中继机制、哈希时间锁定机制与分布式私钥控制技术.

Table 4 Research Status of Smart Contract Application in Energy Blockchain

表 4 能源区块链智能合约应用研究现状

场景	代表工作	描述	匹配交易	信息管理	权限授予	分析统计	均衡调度	存在不足
能源交易	van Leeuwen 等人[36]	将智能合约作为虚拟聚合器	否	是	是	否	否	只考虑单一区块链场景，较少考虑多链场景，以及跨链合约部署和跨链合约计算的问题
	Li 等人[37]	采用智能合约技术实现整个微电网的交易	是	是	否	是	否	
	穆程刚等人[38]	将配售能源交易机制编写成智能合约	是	是	否	否	否	
	沈泽宇等人[39]	将写有交易规则的能源交易合约部署上链	是	否	否	否	否	
电力规划	Kaur 等人[40]	智能合约实现电网负载和供需平衡，制定用电端的激励策略	否	否	否	否	是	
	Yang 等人[41]	智能合约实现储能租赁费管理和用电端的补偿费管理	是	是	否	否	是	
	Couraud 等人[42]	智能合约实现新型家庭能源管理系统的实时电力调度算法	是	否	否	否	是	
	黄伟等人[43]	智能合约将系统调度运行模型等转化为自动执行的程序	是	是	否	否	是	
可再生能源消纳	Li 等人[44]	智能合约使可再生能源消纳规范化	否	是	否	否	是	
电力定价	Dabbaghjamanesh 等人[45]	智能合约根据电力需求为电力买家提供不同的报价	是	否	否	否	否	
	Zhang 等人[46]	采用智能合约实现 P2P 能源交易的供需定价过程	是	是	否	否	否	
能源数据共享	Wang 等人[47]	通过智能合约实现细粒度数据访问控制	否	是	是	否	否	

本节我们将从常见的跨链技术应用与跨链技术在能源区块链的探索工作 2 方面展开综述.

1) 常见的跨链技术应用

Garoffolo 等人[49] 提出了一种类似比特币的区块链系统的结构, 它允许在不知道其内部结构的情况下与不同类型的侧链进行创建和通信. Garoffolo 等人[49] 认为主链是一个区块链平台, 它支持使用一些原生资产硬币(例如比特币、Horizen 等)的基本支付功能; 侧链是一个附加的特定领域平台, 也使用硬币资产(但不限于此). 而且认为侧链并不意味着使用任何特定的数据结构或共识算法, 主链结构与侧链结构完全无关, 主链结构可以是另一个去中心化的区块链, 一些由预先定义的权限维护的中心化数据库, 或者一个任意的应用程序. 同时, Garoffolo 等人[49] 使用 zk-SNARKs 构建侧链使用的通用可验证传输机制, 且设计的多链模型如图 6 所示.

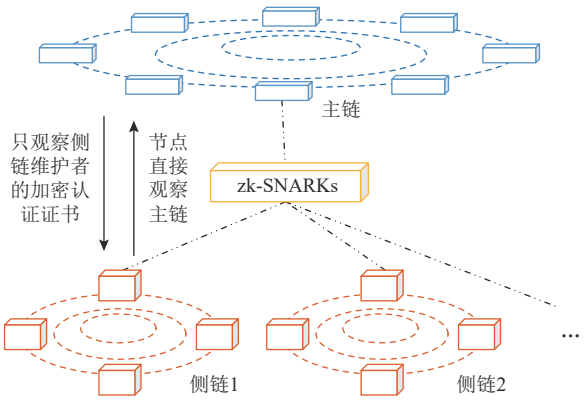


Fig. 6 Cross-chain model

图 6 跨链模型

Ghosh 等人[50] 提出了公有链和私有链之间的信息跨链方法, 从公有链到私有链时采用跨链共识协议来控制信息的准入, 从私有链到公有链时通过联合签名来实现信息的确认; Thyagarajan 等人[51] 提出了一种跨币转化的通道来提升跨链资产转化效率, 并通过设计链式签名技术保证通道中节点支付给下

一节点数字货币后能获得同等价值的数字货币.

大多数的跨链技术都应用在不同区块链的资产转化与资产留置上，以中心化形态为主，不能适应多层次跨链服务需求，而且较少考虑安全性.

2) 跨链技术在能源区块链的探索

在能源交易区块链的跨链技术方面也开展相关研究工作. 例如，Wang 等人[52]提出了一种基于跨链技术的日前协同电力—碳—可交易绿色凭证(tradable green certificate, TGC)市场框架及其实施方法，每日协同市场被设计为顺序运行，以反映碳排放和 TGC 生产的时间属性，并在电力市场中引入了惩罚因素，以表明来自碳市场和 TGC 市场的市场间影响. 此外，本文利用跨链技术形成协调 3 个市场的统一框架，并重新设计每个市场的链结构以适应框架.

余维等人[53]提出一种异构能源区块链的跨链方法，通过中继技术实现了能源索引交易中继链(主链)到能源平行链(侧链)的信息传递，具体架构如图 7 所示. 但是较少涉及跨链信息传递安全性和跨链合约计算问题.

此外，He 等人[54]提出了一种跨链信息传递方法，保证跨链信息的真实性、实时性和链间写互斥性；黄伟等人[43]提出了一种主从链技术以实现综合能源系统调度，将大量的计算工作分配给从链计算，主链仅记录计算结果并验证其正确性，但未给出具体的设计方案.

综上所述，能源交易区块链的跨链技术大多以中继链或侧链方式为主，关于跨链信息准入、跨链信息传递安全、跨链合约部署和计算安全等问题较少考虑. 表 5 简要总结了国内外能源区块链跨链技术研究现状.

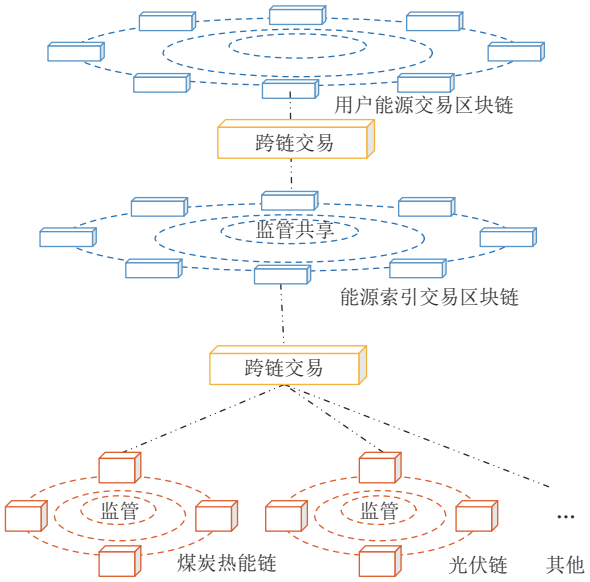


Fig. 7 Energy blockchain cross-chain architecture

图 7 能源区块链跨链架构

2.4 能源区块链节点安全管理

节点安全是区块链安全的重要组成部分，能源交易区块链节点是区块链维护和跨链技术执行的实体，节点不合作或恶意行为会给区块链系统造成拒绝服务、宕机、隐私泄露等严重的后果，因此需要对区块链节点进行安全管理. 目前，区块链节点安全管理的研究工作主要分为接入认证、权限管理和行为审查.

Table 5 Research Status of Energy Blockchain Cross-Chain Technology

表 5 能源区块链跨链技术研究现状

技术	代表工作	描述	跨链资产转化	跨链信息传递	跨链合约计算	存在不足
常见的跨链技术应用	Garoffolo 等人[49]	提出了一种存在父子关系的主侧链	否	是	否	不能适应多层次跨链服务需求，而且较少考虑安全性
	Ghosh 等人[50]	提出了公有链和私有链之间的信息跨链方法	否	是	否	
	Thyagarajan 等人[51]	提出了一种实现跨币转化的支付通道网络	是	否	否	
跨链技术在能源区块链的探索工作	Wang 等人[52]	利用跨链技术形成协调 3 个市场的统一框架，并重新设计每个市场的链结构以适应框架	否	是	否	较少考虑跨链信息传递安全、跨链合约部署和计算安全等问题
	余维等人[53]	通过中继技术实现了能源索引交易中继链到能源平行链的信息传递	否	是	否	
	He 等人[54]	提出一种基于区块链的共享充电平台跨链可信信誉方案	否	是	是	
	黄伟等人[43]	提出主从链技术实现综合能源系统的计算工作调度	否	是	否	

1）区块链节点接入认证

接入认证是指对接入区块链系统的节点进行身份认证，包括注册、证书分发、身份认证等工作.

Novo 等人[55]提出了一种基于区块链的用于管理物联网设备的新架构，提出的框架如图 8 所示.

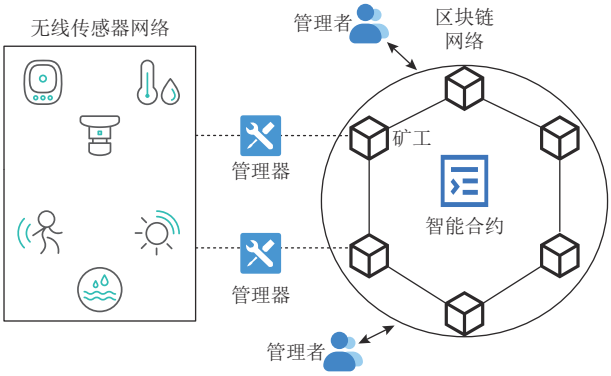


Fig. 8 Access control system

图 8 访问控制系统

该架构利用智能合约实现区块链系统用户的注册、撤销、查询规则和接入策略，从而实现对节点接入进行记录和管理. 该合约定义了访问控制系统中允许的所有操作且该合约是唯一的，不能从系统中删除. 管理器与智能合约交互，可以定义系统的访问控制策略.

Cui 等人[56]提出一种基于区块链的多个传感网络的身份认证方案，在每个传感网络内建立本地区块链，整个网络建立公共区块链，通过设计本地区块链和公共区块链的认证交互流程来实现传感器节点的注册、证书生成和身份认证；Feng 等人[57]提出一种基于区块链的 5G 无人机网络跨域认证机制，每个域内建立私有链，通过联盟链连接各个域内的私有链，域内私有链记录域内无人机的身份信息，联盟链记录所有无人机的身份信息，用户访问域间无人机时通过联盟链中转到无人机所在的域进行认证. 能源交易区块链的接入认证研究工作报道得较少.Che 等人[58]提出了一种基于联盟链的能源分布式交易认证方案，通过包含证书授权（certificate authority, CA）功能的匹配单元进行链下认证，验证发电单元（generation unit, GU）和用电单元（power unit, PU）的身份并颁发证书，并构建证书撤销列表，认证后的节点可以进入区块链网络对能源交易进行确认.

能源交易区块链的接入认证研究工作较少，未考虑跨链或跨域的节点接入认证问题，而且也未考虑跨链节点的特殊性和重要性，跨链节点的可信度直接影响区块链系统的安全性.

2）区块链节点权限管理

权限管理是指对接入区块链系统的节点所具备的权限进行限制和管理，包括节点访问权限、数据访问和操作权限等. Liu 等人[59]提出了一种名为 fabric-IoT 的物联网访问控制系统. 该系统基于 Hyperledger Fabric 区块链框架和基于属性的访问控制（attributed based access control, ABAC），包含 3 种智能合约，分别是设备合约、策略合约和访问合约. 设备合约提供了一种方法来存储设备产生的资源数据的统一资源定位符（uniform resource locator, URL），以及一种查询方法. 策略合约为管理员用户提供管理 ABAC 策略的功能. 访问合约是实现普通用户访问控制方法的核心程序. 结合 ABAC 和区块链技术，fabric-IoT 可以在物联网中提供去中心化、细粒度和动态的访问控制管理. 系统的架构如图 9 所示.

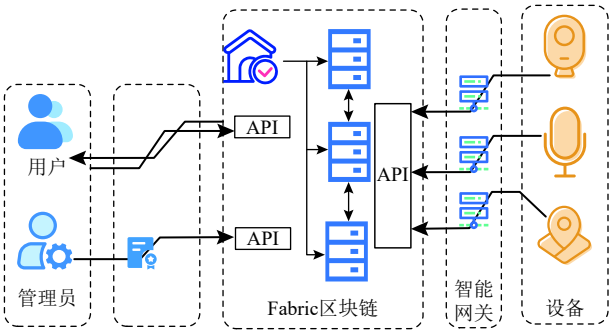


Fig. 9 Architecture of fabric-IoT

图 9 fabric-IoT 架构

Yu 等人[60]提出了一种密文策略基于属性加密（ciphertext-policy attribute-based encryption, CP-ABE）的访问控制方案，将通过 CP-ABE 加密后的数据记录到区块链上，用户根据属性相关联的规则实现对区块链数据的细粒度访问控制；为了进一步保障访问控制的安全性，Huang 等人[61]提出了一种基于信誉的物联网设备工作量证明机制（proof of work, PoW），将节点的信誉值与 PoW 机制关联，PoW 机制的难度根据每个节点的信誉值自适应调整，节点进行非法操作时，其信誉值降低，其 PoW 任务难度增加，该方案通过增加攻击成本来鼓励节点的合作行为. 能源交易区块链也开展了少量关于节点的权限管理的工作. Yang 等人[62]使用 CP-ABE 方案建立了一种基于区块链的 P2P 能源交易访问控制机制，对区块链上的交易数据设置属性关联访问权限，从而实现交易数据的隐私保护.

能源交易区块链的权限管理研究工作较少，未

考虑跨链场景下的节点权限管理, 以及节点操作权限管理.

3) 区块链节点行为审查

行为审查是指对于节点的行为进行跟踪与监督, 包括行为特征提取、行为识别跟踪和异常审查等. Goyat 等人[63]提出了一种基于区块链的物联网传感器节点行为监控方案. 所有传感器节点的注册和认证过程由区块链执行, 完成认证过程后, 所有关键参数都存储在由簇头控制的不可篡改密钥机制(untamperable key mechanism, UKM)中. 簇头将收集到的信息从其成员广播到区块链, 将这些感测到的大量数据与云共享, 以获得更可靠的存储, 关键参数进一步被记录在区块链上, 以提高所获得数据的不变性和透明度, 通过认证撤销过程消除故障传感器节点. 文献 [63] 的网络架构如图 10 所示.

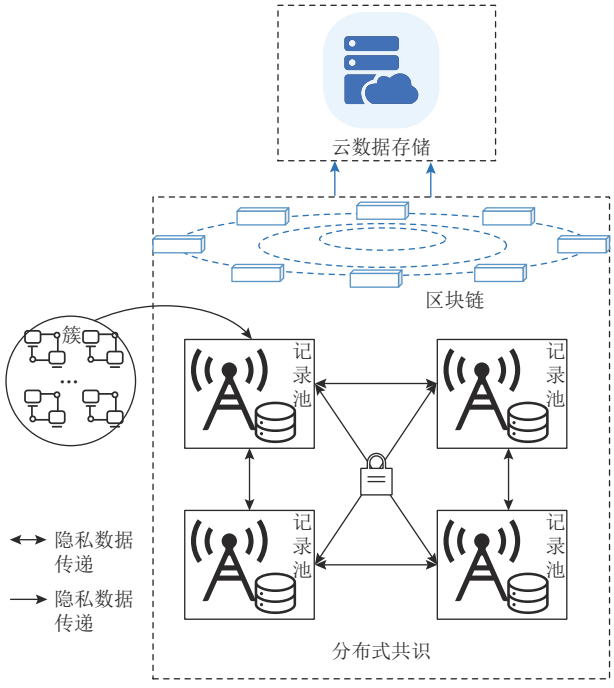


Fig. 10 Architecture of network

图 10 网络架构

Michalski 等人[64]提出一种利用节点特征主动探测区块链节点的机器学习方法, 该方法通过提取节点特征来量化节点的行为, 并使用监督学习算法依据节点的行为特征发现并跟踪节点; Peng 等人[65]在疫苗生产中提出了一种双层区块链结构的节点行为审查方案, 通过双层区块链将公共数据与私有数据分隔, 主审查节点验证公有数据备份的正确性, 预备审查节点用于替换主审查节点或恢复丢失的数据, 审查节点对验证的公有数据备份进行审核和发布, 从而实现对公有区块链数据的审查同时保护私有数据的隐私. 能源交易区块链的行为审查研究工作较少. Li 等人[66]提出了一种基于区块链的能源交易审查方案, 区块链会记录交易并对交易进行审核, 当出现交易争议时, 可实现对恶意能源卖家行为进行惩罚.

综上所述, 能源交易区块链的行为审查研究工作刚刚起步, 未考虑跨链场景下的节点行为管理, 以及审查数据的隐私保护. 表 6 简要总结了国内外能源区块链节点管理技术研究现状.

2.5 能源区块链隐私保护

随着《中华人民共和国网络安全法》《中华人民共和国数据安全法》《中华人民共和国个人信息保护法》等相关法律的实施, 如何在保护隐私的前提下开展能源区块链的数据共享与应用是未来需要研究的重要课题. 现有区块链应用的隐私保护研究主要包括: 区块链数据隐私保护和合约隐私保护.

1) 区块链数据隐私保护

区块链数据隐私保护是指采用隐私保护技术, 使得区块链系统中存储的数据或交易不能推断出用户身份、偏好、交易金额及位置等敏感信息.

Gai 等人[67]提出了一种将物联网与边缘计算和区块链相结合的新方法, 称为基于区块链的边缘互联网模型. 所提出的模型充分利用边缘计算和区块链的优势以及差分隐私(differential privacy, DP)技术来建立隐私保护机制, 所提出的隐私保护模型如图 11 所示.

Gai 等人[67]利用区块链的特性, 使用一种可追溯的机制来解决边缘计算中的任务分配问题, 在区块链系统中使用差分隐私技术以防止区块上的信息受到基于数据挖掘的攻击, 达到保护区块数据隐私的目的.

Ping 等人[68]提出一种电车充电区块链的充电交易隐私保护方法. 与集中式协调机制不同, 所提出的基于 ADMM 的算法中的充电站不需要将有关其自身和现场电动汽车的那些敏感信息暴露给中央协调器, 而只需要有限的信息, 在充电功率配额交易期间保护了交易数据隐私; Guan 等人[69]提出了一种基于区块链的隐私保护能源交易方案, 通过 CP-ABE 方法将分布式交易加密后发送给仲裁节点检查, 再发给记账节点打包上链, 由于交易被设置了访问控制, 交易双方的隐私得到保护; 赵丙镇等人[70]提出了基于区块链的电力交易数据隐私保护方法, 通过概率公钥加密算法实现区块链交易用户真实身份的隐藏, 采用 Pedersen 承诺和零知识证明技术, 实现监管机构

Table 6 Research Status of Energy Blockchain Node Management

表 6 能源区块链节点管理的研究现状

技术	代表工作	描述	实现原理	能源领域	多链场景	存在不足
区块链节点接入认证	Novo 等人[55]	提出了一种区块链节点接入认证智能合约	智能合约	否	否	未考虑能源交易跨链或跨域的节点接入认证问题
	Cui 等人[56]	基于区块链的多传感网络（Multi-WSN）的身份认证方案	多链结构	否	是	
	Feng 等人[57]	基于区块链的 5G 无人机网络跨域认证机制	智能合约	否	否	
	Che 等人[58]	基于联盟链的能源分布式交易认证方案	控制公私钥	是	否	
区块链节点权限管理	Liu 等人[59]	一种基于属性的访问控制合约方案	智能合约	否	否	未考虑能源交易跨链场景下的节点权限管理、节点操作权限的管理
	Yu 等人[60]	基于 CP-ABE 的区块链访问控制方案	密文策略基于属性加密	否	否	
	Huang[61] 等人	采用基于信誉的 PoW 共识机制提升访问控制的安全性	基于信誉的 PoW 共识	否	否	
	Yang 等人[62]	基于 CP-ABE 方案建立基于区块链的 P2P 能源交易访问控制机制	密文策略基于属性加密	是	否	
区块链节点行为审查	Goyat 等人[63]	基于区块链的物联网传感器节点行为监控方案	审查节点数据	否	否	未考虑能源交易跨链场景下的节点行为管理、审查数据的隐私保护
	Michalski 等人[64]	使用机器学习算法依据节点的行为特征发现并跟踪节点	机器学习	否	否	
	Peng 等人[65]	疫苗生产应用中基于双层区块链结构的节点行为审查方案	多监管节点	否	是	
	Li 等人[66]	基于区块链的能源交易审查方案	定时承诺	是	否	

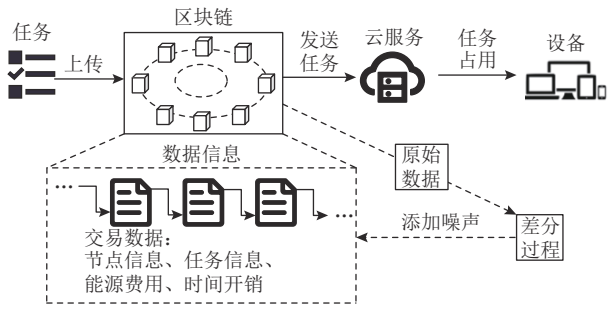


Fig. 11 Privacy protection model of transaction data

图 11 交易数据的隐私保护模型

对交易监管的同时对交易金额的隐私保护.

以上区块链数据隐私保护方法通过上链数据的扰动或加密处理实现隐私保护，但未考虑隐私保护的开销过大、处理后数据的查询及共享的问题.

2）智能合约隐私保护

智能合约隐私保护是指采用隐私保护技术，防止智能合约在执行过程中造成用户的敏感数据泄露.

Cheng 等人[71]利用可信硬件的可信执行环境（trusted execution environment, TEE）执行智能合约以处理机密用户数据，合约计算流程如图 12 所示，但

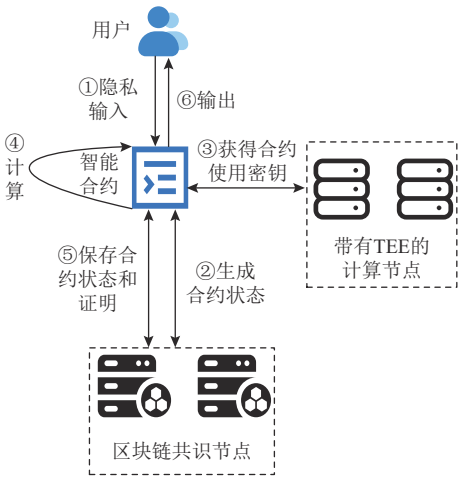


Fig. 12 Contract calculation process

图 12 合约计算流程

是可信硬件的使用会产生额外的硬件造价开销.

Unterweger 等人[72]试图开发能够运用于能源领域的隐私保护智能合约并部署到以太坊区块链上，但是发现即使采用链下预计算和链上 gas 开销优化，也存在开销较大的问题；Abdelsalam 等人[73]提出了一种基于区块链的隐私保护电力节能机制，该机制在

智能合约进行电力调配计算时不共享用电消费者的用电量，仅共享功率变化百分比(percentage power change, PPC)，从而达到保护用电消费者隐私的目的.

以上智能合约的隐私保护方式通常开销较大或者通用性不强，较难应用于融合多类能源交易场景的能源区块链中. 表 7 简要总结了国内外能源区块链隐私保护技术研究现状.

3 能源区块链的跨链架构

根据能源区块链的发展现状，我们发现目前能源区块链发展受限的原因之一，是目前的架构不能适应多层次跨链服务需求，且未考虑层次化跨链服务、跨链监管和共识. 因此，本文根据能源区块链跨平台、跨区域、跨业务的特点，考虑节点、交易及合约的差异性，提出多层次可监管的能源区块链跨链架构.

3.1 多层次可监管的能源区块链跨链架构

虽然区块链的多场景交易架构已经存在，但能源区块链为了实现更大范围的互联，不仅涉及多场景交易，还需考虑跨平台、跨区域、跨业务的层次化跨链服务，不同层级跨链服务在架构设计中应存在差异.

目前，区块链多链协作生态的构建与发展还不成熟，而且存在较多合规性和安全性问题，又因为能源交易具有特殊性，即能源交易不只是纯粹的交易，往往还是国家战略的组成部分，关系着国家的经济命脉与民生大计，并与国家安全紧密相连，实现对能源交易的监管约束尤为重要，且对多链协作生态构建与健康发展也尤为重要.

此外，单一的监管模式不适用能源区块链多链协作生态，因为能源区块链多链协作生态涉及跨平台、跨区域和跨业务互联，存在较多差异较大的节点、交易及合约. 为应对能源区块链节点与交易和合约的差异性，可对能源区块链节点采用多类别的监管模式，但该监管模式也可能会出现监管效果局部好、全局差的问题，而且能源区块链共识机制的设计同样会影响局部和全局监管的效果. 因此，如何耦合共识机制实现多层次协同高效监管，是亟待解决的关键问题.

综上所述，在能源区块链跨链架构设计时应考虑监管的问题，包括能源区块链的节点监管、数据监管和合约监管；在新的架构下，共识机制也需要作出相应的调整，以适应多层次跨链和多级监管功能设计的需求.

3.2 能源区块链监管架构组成

图 13 给出了本文提出的多层次跨链协同监管的能源区块链架构，与目前国网链提出的“一主两侧多从”架构不同，本文提出的架构由 1 条主链与多条跨平台或跨区域的侧链构成，将为能源生产者、能源储备输送商、各类能源运营商、能源消费用户、监管机构等提供多方共建的信任环境. 该架构可以实现多个现存能源交易平台间、不同能源交易区域间甚至不同能源业务或行业间的数据安全共享、多级协同监管. 多级协同监管机制耦合链内、链间及全网的多层级共识机制，实现对参与能源交易各方身份信息及能源交易过程的全面监管.

以下以混合的分布式能源交易场景为例，说明架构的组成和运作方式. 本文架构的 1 条侧链或多条侧链可对应一个能源区块链交易平台，能源区块链

Table 7 Research Status of Energy Blockchain Privacy Protection

表 7 能源区块链隐私保护研究现状

技术	代表工作	描述	实现原理	用户身份隐私	交易数据隐私	合约计算隐私	能源领域	存在不足
数据隐私保护	Gai 等人[67]	将物联网与边缘计算和区块链相结合来建立隐私保护机制	差分隐私	否	是	否	否	未考虑隐私保护的开销过大、处理后数据的查询及共享问题
	Ping 等人[68]	电车充电区块链的充电交易隐私保护方法	减少共享的数据	是	是	否	是	
	Guan 等人[69]	一种基于区块链的隐私保护能源交易方案	使用访问控制	否	是	否	是	
	赵丙镇等人[70]	基于区块链的电力交易数据隐私保护方法	概率公钥加密、承诺方案和零知识证明	是	是	否	是	
智能合约计算隐私保护	Cheng 等人[71]	利用 TEE 执行智能合约	TEE	否	否	是	否	通常开销较大，较难应用于能源区块链
	Unterweger 等人[72]	尝试开发运用于能源领域的隐私保护智能合约	隐私保护智能合约	是	是	否	是	
	Abdelsalam 等人[73]	基于区块链的隐私保护电力节能机制	减少使用的数据	否	是	否	是	

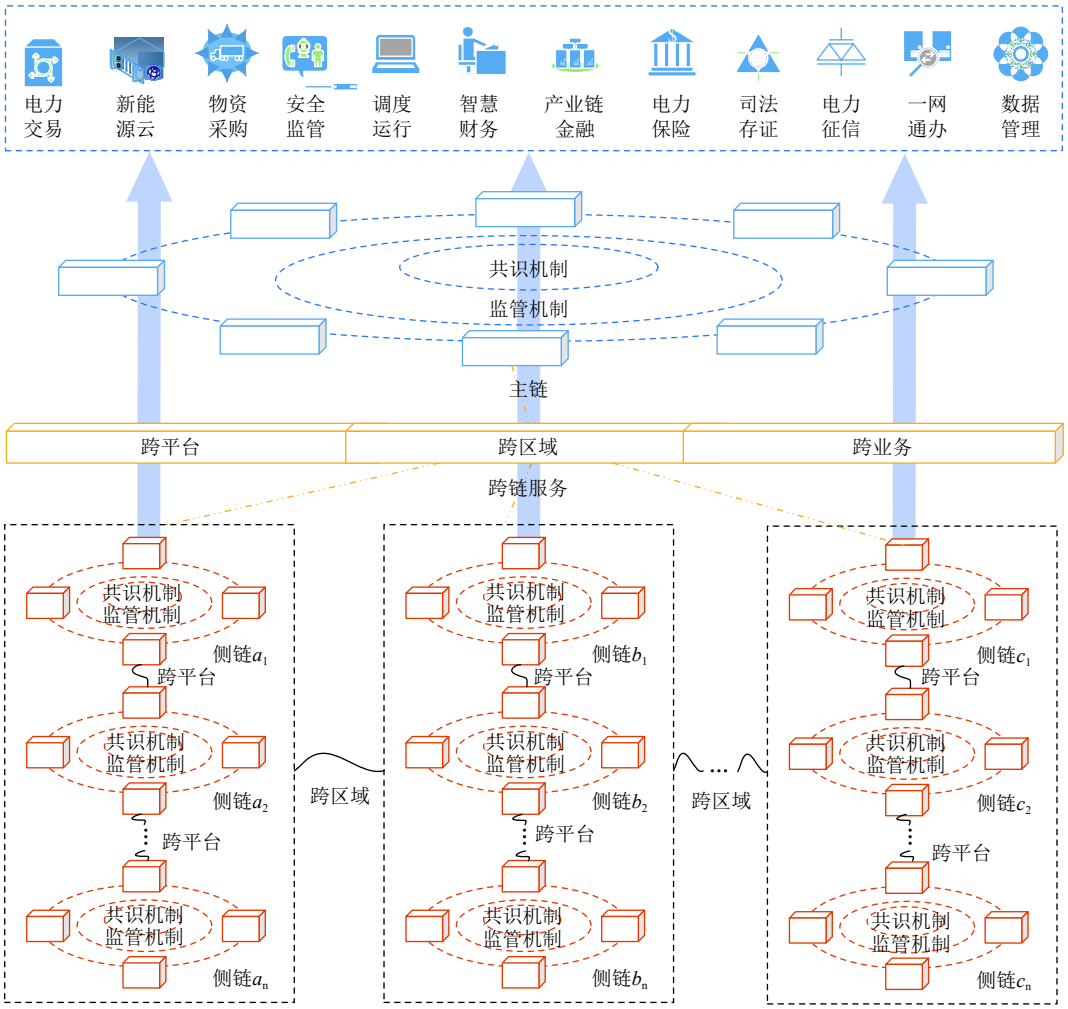


Fig. 13 Our proposed energy blockchain cross-chain architecture

图 13 本文提出的能源区块链跨链架构

交易平台为能源消费者和能源供应商提供交易撮合服务，参与交易的各方均将身份信息保存至区块链上；跨链服务可联通多个能源区块链交易平台，实现跨平台、跨区域交易撮合. 平台根据交易意向中的能源供需数量、交易价格、交易时间等信息创建交易合约，若消费者或生产者在交易过程中未按照交易意向规定需求或供给能源，则监管机构可根据链上信息对违约者实施惩罚措施，以实现对交易过程的监管. 当交易完成后，由监管机构对整个交易结果进行确认；确认无误后，将交易信息打包至能源区块链存储. 各个侧链中的共识机制根据自身的业务需求设定，侧链之间的跨链共识机制在基于信誉的共识机制上进行改进，主链与侧链之间的跨链共识应采用高效的共识算法.

3.3 跨平台、跨区域、跨业务的多级协同监管机制

本文提出跨平台、跨区域、跨业务的多级协同监管机制，将监管从单一区块链的单类能源交易扩展到多平台、多区域乃至多业务范围的监管，更接近于实际能源交易的监管需求，从而实现能源区块链的节点监管、数据监管和合约监管.

以混合的分布式能源交易场景为例，说明监管机制的大致流程. 本文方案拟采用穿透式监管的方式，对能源区块链中参与交易的各方向上穿透监管，核查其身份信息的真实性与交易的合规性；对能源区块链上的每笔能源交易向下穿透监管，核查交易的能源量、交易金额、交易时间等数据；通过耦合跨链服务和共识机制，实现整个能源区块链跨平台、跨区域、跨业务的有效监管. 监管架构考虑目前能源领域区块链技术应用情况，可实现公有链与联盟链、联盟链与私有链、联盟链间安全可靠的数据流通与有效的监管.

3.4 链内、链间及全网共识的多层级共识机制

本文提出链内、链间及全网共识的多层级共识机制，根据跨链监管需求和现有共识机制的特点，设

计能源区块链的链内、链间及全网共识的多层级共识机制，以达到跨平台、跨区域、跨业务能源交易高效共识和监管的目的.

以下以混合的分布式能源交易场景为例，说明链内、链间及全网共识的多层级共识机制的设计. 目前，能源交易区块链大多未涉及跨链，链内共识算法通常采用基于信誉的共识机制来改进，通过可信的记账节点来完成交易确认和打包上链，本文方案可兼容现有平台链内的共识算法，也可根据平台特点推荐使用与平台相匹配的共识算法或改进现有共识算法. 链间共识算法考虑能源区块链跨平台和跨区域交易场景，跨平台交易场景应考虑算力优势攻击，共识算法设计应确保来自统一平台的节点数量不超过参与共识节点数量的 1/3；跨区域交易场景应考虑安全和效率问题，可采用安全顶会 ACM CCS 上提出的 RapidChain 共识算法[74]，利用时间分片技术，随机建立分片和更替挑选委员会，不必频繁重构委员会，提升了共识的效率，实现能源交易信息在全网分散安全存储，达到了链间信息安全共享的目的. 全网共识算法考虑由各链的监管节点来实现，需结合监管业务设计与监管需求相关的共识算法，例如可采用改进的权益证明（proof of stake, POS）共识机制[75]，为不同等级的监管节点赋予不同的权值，使高效的监管助力能源区块链全网共识.

4 关键问题与发展方向

从目前国内外已有的电力行业优秀期刊与会议以及网络安全行业的期刊与会议来看，区块链在能源中应用的已有不少研究工作，但是目前的大部分工作专注于区块链技术在能源领域的应用以及智能合约在能源领域的实现等，虽然有少部分文献针对此过程的能源数据隐私与合约的计算隐私，但是由于跨平台、跨区域、跨业务的需求，需要引入跨链技术为能源区块链提供跨链服务. 由于跨链技术的引入，能源区块链的隐私与安全要求进一步提高，但目前针对能源区块链跨链场景下的跨链技术、跨链节点安全管理和跨链隐私保护的问题研究较少，能源区块链共识算法也是值得研究的目标.

为促进能源行业数字化转型，推动能源区块链项目落地，能源区块链需要可验证、高可信、高安全的跨链服务，本节提出能源区块链跨链服务安全技术的关键问题与发展方向.

4.1 安全高效的能源区块链跨链技术研究

针对能源区块链，虽然跨链技术助力区块链多链协作生态的构建，但也带来了跨链信息传输与合约计算的安全问题，同时跨链效率与安全性也对能源区块链性能造成影响.

跨链技术是跨链服务的关键，现有的跨链技术大多用于实现资产转化，较少考虑跨链信息传递安全和跨链合约计算安全，导致传递信息不准确或计算结果不正确，如何实现和验证信息传递安全和合约计算安全是亟待突破的难题.

目前的跨链技术大多数的研究工作集中在资产交换上，主要在跨链效率、安全性、兼容性等方面进行改进. 然而，能源区块链除了资产交换之外，还涉及信息跨链传递、合约跨链部署及计算，需设计相应的跨链技术实现这些功能. 能源区块链的跨链技术还处于起步阶段，目前还不存在高效、安全和兼容的方案.

跨链信息传递时，应考虑传递信息的准入、跨链传递信息的真实性和实时性、链间写互斥性等问题；跨链合约部署时，应考虑协同制定合约内容与需求的匹配性，以满足能源业务合约的功能需求；跨链合约计算时，应考虑合约计算过程的正确性与计算结果的完整性. 另外，跨链信息传递、跨链合约部署、跨链合约计算的安全方案应该是公开可验证的.

4.2 安全动态的跨链节点管控技术研究

在能源区块链跨链交易时，跨链节点作为跨链技术执行的主体，其不合作和恶意行为将导致跨链服务的不可用和质量差的问题，因而实现跨链节点的安全管控尤为重要.

跨链节点需要完成跨链数据访问、数据中转、数据发送及接收处理、信息审核确认等任务，这些任务之间有较大差异，而且某些任务可能涉及多人协作，因而需按类别和重要性进行分级协作管理，实现管理技术的可信任；跨链节点管理的重点是权限管理和行为审查，两者相互联系且随时间动态变化，因而管理技术还应考虑整体的动态优化调整机制；另外，跨链节点管控还应考虑链间写互斥性和链间数据隐私保护等安全问题. 因此，如何实现可信任的跨链节点权限和行为安全动态管控，是具有挑战性的关键问题.

跨链安全方案最终的执行实体是跨链节点，跨链节点的不合作和恶意行为将导致区块链系统的拒绝服务、宕机等问题，因此跨链节点的管控至关重要. 然而，目前关于跨链节点的管控研究工作几乎没

有，仅有少量区块链节点管控的相关工作，主要集中在接入认证、访问控制、行为审查方面，而且这些研究工作未考虑跨链节点的跨链特点和重要性.

跨链节点安全管控应考虑跨链节点的可信任问题，并根据信任度来进行节点的分级权限管理，从而实现细粒度的访问控制；另外，跨链节点行为审查可能会泄露多条链的隐私，因此跨链节点行为审查还应考虑保护跨链的隐私问题.

4.3 安全轻量的跨链数据及合约隐私保护技术研究

隐私问题是目前制约区块链技术规模化应用的主要因素之一，而且隐私在跨链数据共享和合约计算应用场景中将更加难以保护，在能源区块链的发展中也不得不面临这个问题.

跨链数据共享会涉及数据的频繁查询和访问，因而需设计轻量级的跨链数据隐私保护算法，在保证数据隐私安全的同时，实现数据的快速检索和高效访问控制；跨链合约可能涉及对大量数据的处理和计算，但合约的运行环境和编程语言较难实现开销较大的运算，因而需设计轻量级跨链合约隐私保护算法，在保证合约计算隐私安全的同时，提升大规模协作计算的效率. 因此，如何设计轻量级的跨链数据共享及合约计算的隐私保护算法，是亟待解决的关键问题.

能源区块链在实现数字化协作生态的同时，带来了区块链数据和智能合约隐私泄露的风险，而且跨链技术的运用会联通多链的数据及合约，也带来了更大的隐私泄露风险和危害. 现有的隐私保护方案大多开销较大，较难适应区块链分布式环境，而且未考虑跨链隐私泄露的问题. 另外，隐私保护技术会对数据查询与共享、合约部署与计算的效果造成一定的影响.

因此，在数据隐私保护设计时，应考虑设计轻量级的跨链数据高效查询与共享方案；在合约隐私保护设计时，应考虑设计轻量级的跨链合约协同部署与计算方案.

4.4 安全适配的能源区块链共识算法研究

共识算法是区块链系统中的核心机制之一，在能源区块链网络中，共识节点通过算法交换信息达成共识，维护区块链系统的数据一致性，共识算法也是未来的重要研究方向.

由于跨链场景的存在，以及链内、链间及全网共识的多层级共识机制，共识算法需要满足各场景业务的性能需求. 能源区块链场景复杂多样，如能源交易、电力规划、可再生能源消纳、电力定价和能源数据共享等，通用的共识算法往往不能完全满足能源区块链各场景的需要，需针对各场景研究高适配的能源区块链共识算法，并在安全性、一致性、可用性、分区容忍性等层面对共识算法进行评估分析，解决了目前区块链系统的引入带来的效率降低问题. 因此，如何设计安全适配的能源区块链共识算法，是亟待解决的关键问题.

共识算法的设计需考虑拜占庭容错问题、CAP定理和DSS猜想. 拜占庭容错问题意味着即使某些节点出错或存在恶意行为，拜占庭容错系统也能够继续运转. CAP定理即在一个分布式系统中，一致性(consistency)、可用性(availability)与分区容错性(partition tolerance)这3个要素最多只能同时实现2个要素. DSS猜想即去中心化(decentralization)、安全性(security)、和可扩展性(scalability)，在区块链系统中最多只能在这3个特性中选2个实现. 在能源区块链跨平台、跨区域、跨业务的跨链场景下，各链共识算法各异，通用的共识算法并不能兼顾所有场景下的业务需求与性能需求，为能源区块链共识算法的选择带来难题.

因此，在能源区块链共识算法设计时，应考虑设计链内、链间及全网共识的多层级共识机制方案，并针对各场景业务设计安全适配的能源区块链共识算法.

5 总　　结

随着能源行业数字化转型的推进，能源区块链逐渐得到关注，能源区块链的研究以及相关跨链解决方案也成为了学术界和工业界研究的热点之一，而能源区块链的发展很大程度上依赖于跨链服务技术的突破. 本文针对能源区块链的5个方面分别展开调研，即能源区块链架构、智能合约应用、跨链技术、区块链节点管理和区块链隐私保护，分析了这些安全技术的研究现状，并考虑这些技术在能源区块链跨链交易场景下的可行性，并提出多层次跨链协同监管的能源区块链架构，总结国内外能源区块链跨链服务安全技术研究所面临的关键问题，分析出未来可能的研究方向.

作者贡献声明：何云华负责论文总体规划、指导论文撰写；罗明顺调研与分析文献；胡晴整理文献；吴槟负责图形制作；王超指导论文撰写；肖珂负责论文的审核与修订.

参 考 文 献

[1] Xu Min, Chen Xingtong, Kou Gang. A systematic review of blockchain[J]. Financial Innovation, 2019, 5(1): 1−14

[2] Brilliantova V, Thurner T W. Blockchain and the future of energy[J]. Technology in Society, 2019, 57: 38−45

[3] Yan Yong, Chen Xingying, Wen Fushuan, et al. From energy Internet to energy blockchain: Basic concept and research framework[J]. Automation of Electric Power Systems, 2022, 46(2): 1−14 (in Chinese)
(颜拥, 陈星莺, 文福拴, 等. 从能源互联网到能源区块链: 基本概念与研究框架[J]. 电力系统自动化, 2022, 46(2): 1−14)

[4] She Wei, Bai Menglong, Liu Wei, et al. The architecture, application and development trend of energy blockchain[J]. Journal of Zhengzhou University: Natural Science Edition, 2021, 53(4): 1−21 (in Chinese)
(佘维, 白孟龙, 刘炜, 等. 能源区块链的架构、应用与发展趋势[J]. 郑州大学学报: 理学版, 2021, 53(4): 1−21)

[5] Liu Chang, Mei Yu, Zhang Xu, et al. Research on epidemic data sharing model based on cross-chain mechanism[C]//Proc of the 10th Int Conf on Communications, Signal Processing, and Systems. Berlin: Springer, 2022: 424−430

[6] Wang Weidong, Li Xiaofeng, Zhao He. DCAF: Dynamic cross-chain anchoring framework using smart contracts[J]. The Computer Journal, 2022, 65(8): 2164−2182

[7] Andoni M, Robu V, Flynn D, et al. Blockchain technology in the energy sector: A systematic review of challenges and opportunities [J]. Renewable and Sustainable Energy Reviews, 2019, 100: 143−174

[8] Ante L, Steinmetz F, Fiedler I. Blockchain and energy: A bibliometric analysis and review[J]. Renewable and Sustainable Energy Reviews, 2021, 137: 110597

[9] Wang Qiang, Su Min. Integrating blockchain technology into the energy sector—From theory of blockchain to research and application of energy blockchain[J]. Computer Science Review, 2020, 37: 100275

[10] Teng Fei, Zhang Qi, Wang Ge, et al. A comprehensive review of energy blockchain: Application scenarios and development trends[J]. International Journal of Energy Research, 2021, 45(12): 17515−17531

[11] Bao Jiabin, He Debiao, Luo Min, et al. A survey of blockchain applications in the energy sector[J]. IEEE Systems Journal, 2020, 15(3): 3370−3381

[12] Fu Liyu, Lu Gehao, Wu Yiming, et al. Overview of research and development of blockchain technology[J]. Computer Science, 2022, 49(S1): 447−461,666 (in Chinese)
(傅丽玉, 陆歌皓, 吴义明, 等. 区块链技术的研究及其发展综述[J]. 计算机科学, 2022, 49(S1): 447−461, 666)

[13] Mahmudnia D, Arashpour M, Yang R. Blockchain in construction management: Applications, advantages and limitations[J]. Automation in Construction, 2022, 140: 104379

[14] Zhou Liyi, Qin Kaihua, Torres C F, et al. High-frequency trading on decentralized on-chain exchanges[C]//Proc of the 42nd IEEE Symp on Security and Privacy. Piscataway, NJ: IEEE, 2021: 428−445

[15] Leng Kaijun, Bi Ya, Jing Linbao, et al. Research on agricultural supply chain system with double chain architecture based on blockchain technology[J]. Future Generation Computer Systems, 2018, 86: 641−649

[16] Cao Bin, Wang Xuesong, Zhang Weizheng, et al. A many-objective optimization model of industrial Internet of things based on private blockchain[J]. IEEE Network, 2020, 34(5): 78−83

[17] Qiao Rui, Luo Xiangyang, Zhu Sifeng, et al. Dynamic autonomous cross consortium chain mechanism in e-healthcare[J]. IEEE Journal of Biomedical and Health Informatics, 2020, 24(8): 2157−2168

[18] Dai bingrong, Jiang Shengming, Li Dunwei, et al. Evaluation model of cross-chain notary mechanism based on improved PageRank algorithm[J]. Computer Engineering, 2021, 47(2): 26−31 (in Chinese)
(戴炳荣, 姜胜明, 李顿伟, 等. 基于改进 PageRank 算法的跨链公证人机制评价模型[J], 计算机工程, 2021, 47(2): 26−31)

[19] Singh A, Click K, Parizi R M, et al. Sidechain technologies in blockchain networks: An examination and state-of-the-art review[J]. Journal of Network and Computer Applications, 2020, 149: 102471

[20] Dai Bingrong, Jiang Shengming, Li Chao, et al. A multi-hop cross-blockchain transaction model based on improved hash-locking[J]. International Journal of Computational Science and Engineering, 2021, 24(6): 610−620

[21] Deng Liping, Chen Huan, Zeng Jing, et al. Research on cross-chain technology based on sidechain and Hash-locking[C]//Proc of the 2nd Int Conf on Edge Computing. Berlin: Springer, 2018: 144−151

[22] Neisse R, Hernández-Ramos J L, Matheu-Garcia S N, et al. An Interledger blockchain platform for cross-border management of cybersecurity information[J]. IEEE Internet Computing, 2020, 24(3): 19−29

[23] Frauenthaler P, Sigwart M, Spanring C, et al. ETH Relay: A cost-efficient relay for ethereum-based blockchains[C]//Proc of the 3rd IEEE Int Conf on Blockchain. Piscataway, NJ: IEEE, 2020: 204−213

[24] Ou Wei, Huang Shiying, Zheng Jingjing, et al. An overview on cross-chain: Mechanism, platforms, challenges and advances[J]. Computer Networks, 2022, 218: 109378

[25] Zhong Cong, Liang Zhihong, Huang Yuxiang, et al. Research on cross-chain technology of blockchain: Challenges and prospects[C]//Proc of the 2nd IEEE Int Conf on Power, Electronics and Computer Applications. Piscataway, NJ: IEEE, 2022: 422−428

[26] Zhang Jianbiao, Liu Yanhui, Zhang Zhaopian. Research on cross-chain technology architecture system based on blockchain[C]//Proc of the 8th Int Conf on Communications, Signal Processing, and Systems. Berlin: Springer, 2019: 2609−2617

[27] Yan Mingyu, Shahidehpour M, Alabdulwahab A, et al. Blockchain for transacting energy and carbon allowance in networked microgrids[J]. IEEE Transactions on Smart Grid, 2021, 12(6): 4702−4714

[28] Yang Qing, Wang Hao. Privacy-preserving transactive energy management for IoT-aided smart homes via blockchain[J]. IEEE

Internet of Things Journal, 2021, 8(14): 11463−11475

[29] Abishu H N, Seid A M, Yacob Y H, et al. Consensus mechanism for blockchain-enabled vehicle-to-vehicle energy trading in the Internet of electric vehicles[J]. IEEE Transactions on Vehicular Technology, 2021, 71(1): 946−960

[30] Zhang Yi. Distributed energy intelligent transaction model and credit risk management based on energy blockchain[J]. Journal of Information Science & Engineering, 2021, 37(1): 55−66

[31] Deng Lirong, Zhang Xuan, Sun Hongbin. Real-time autonomous trading in the electricity-and-heat distribution market based on blockchain[C/OL]//Proc of the 2019 IEEE Power and Energy Society General Meeting. Piscataway, NJ: IEEE, 2019[2022-09-23]. https://ieeexplore.ieee.org/abstract/document/8973842

[32] Hamouda M R, Nassar M E, Salama M M A. A novel energy trading framework using adapted blockchain technology[J]. IEEE Transactions on Smart Grid, 2020, 12(3): 2165−2175

[33] Gong Gangjun, Zhang Xinyu, Zhang Zhening, et al. Multi-microgrid co-governance transaction model based on dynamic cooperation game of blockchain[J]. Proceedings of the Chinese Society of Electrical Engineering, 2021, 41(3): 803−819 (in Chinese)
(龚钢军, 张心语, 张哲宁, 等. 基于区块链动态合作博弈的多微网共治交易模式 [J]. 中国电机工程学报, 2021, 41(3): 803−819)

[34] Yang Jiawei, Paudel A, Gooi H B. Blockchain framework for peer-to-peer energy trading with credit rating[C/OL]// Proc of the 2019 IEEE Power and Energy Society General Meeting. Piscataway, NJ: IEEE, 2019[2022-08-13].https://ieeexplore.ieee.org/abstract/document/8973709

[35] Abdella J, Tari Z, Anwar A, et al. An architecture and performance evaluation of blockchain-based peer-to-peer energy trading[J]. IEEE Transactions on Smart Grid, 2021, 12(4): 3364−3378

[36] van Leeuwen G, AlSkaif T, Gibescu M, et al. An integrated blockchain-based energy management platform with bilateral trading for microgrid communities[J]. Applied Energy, 2020, 263: 114613

[37] Li Zugang, Chen Shi, Zhou Buxiang. Electric vehicle peer-to-peer energy trading model based on SMES and blockchain[J]. IEEE Transactions on Applied Superconductivity, 2021, 31(8): 1−4

[38] Mu Chenggang, Ding Tao, Dong Jiangbin, et al. Development of decentralized peer-to-peer multi-energy trading system based on private blockchain technology[J]. Proceedings of the Chinese Society of Electrical Engineering, 2021, 41(3): 878−890 (in Chinese)
(穆程刚, 丁涛, 董江彬, 等. 基于私有区块链的去中心化点对点多能源交易系统研制 [J]. 中国电机工程学报, 2021, 41(3): 878−890)

[39] Shen Zeyu, Chen Sijie, Yan Zheng, et al. Distributed energy trading technology based on blockchain[J]. Proceedings of the Chinese Society of Electrical Engineering, 2021, 41(11): 3841−3851 (in Chinese)
(沈泽宇, 陈思捷, 严正, 等. 基于区块链的分布式能源交易技术 [J]. 中国电机工程学报, 2021, 41(11): 3841−3851)

[40] Kaur K, Kaddoum G, Zeadally S. Blockchain-based cyber-physical security for electrical vehicle aided smart grid ecosystem[J]. IEEE Transactions on Intelligent Transportation Systems, 2021, 22(8): 5178−5189

[41] Yang Xiaodong, Wang Guofeng, He Haibo, et al. Automated demand response framework in ELNs: Decentralized scheduling and smart contract[J]. IEEE Transactions on Systems, Man, and Cybernetics: Systems, 2020, 50(1): 58−72

[42] Couraud B, Robu V, Flynn D, et al. Real-time control of distributed batteries with blockchain-enabled market export commitments[J]. IEEE Transactions on Sustainable Energy, 2021, 13(1): 579−591

[43] Huang Wei, Zuo Xinya, Liu Yiming. Multiple blockchains based dispatching architecture for integrated energy system[J]. Proceedings of the Chinese Society of Electrical Engineering, 2021, 45(23): 12−20 (in Chinese)
(黄伟, 左欣雅, 刘弋铭. 基于多区块链结构的综合能源系统调度构架 [J]. 电力系统自动化, 2021, 45(23): 12−20)

[44] Li Yinan, Yang Wentao, He Ping, et al. Design and management of a distributed hybrid energy system through smart contract and blockchain[J]. Applied Energy, 2019, 248: 390−405

[45] Dabbaghjamanesh M, Wang Boyu, Kavousi-Fard A, et al. Blockchain-based stochastic energy management of interconnected microgrids considering incentive price[J]. IEEE Transactions on Control of Network Systems, 2021, 8(3): 1201−1211

[46] Zhang Min, Eliassen F, Taherkordi A, et al. Demand–response games for peer-to-peer energy trading with the hyperledger blockchain[J]. IEEE Transactions on Systems, Man, and Cybernetics: Systems, 2022, 52(1): 19−31

[47] Wang Yuntao, Su Zhou, Zhang Ning, et al. SPDS: A secure and auditable private data sharing scheme for smart grid based on blockchain[J]. IEEE Transactions on Industrial Informatics, 2021, 17(11): 7688−7699

[48] Li Fang, Li Zhuoran, Zhao He. Research on the progress in cross-chain technology of blockchains[J]. Journal of Software, 2019, 30(6): 1649−1660 (in Chinese)
(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)

[49] Garoffolo A, Kaidalov D, Oliynykov R. Zendoo: A zk-SNARK verifiable cross-chain transfer protocol enabling decoupled and decentralized sidechains[C]//Proc of the 40th IEEE Int Conf on Distributed Computing Systems. Piscataway, NJ: IEEE, 2020: 1257−1262

[50] Ghosh B C, Bhartia T, Addya S K, et al. Leveraging public-private blockchain interoperability for closed consortium interfacing [C/OL]//Proc of the 40th IEEE Conf on Computer Communications. Piscataway, NJ: IEEE, 2021[2022-08-02].https://ieeexplore.ieee.org/abstract/document/9488683

[51] Thyagarajan S A K, Malavolta G. Lockable signatures for blockchains: Scriptless scripts for all signatures[C] //Proc of the 42nd IEEE Symp on Security and Privacy. Piscataway, NJ: IEEE, 2021: 937−954

[52] Wang Yun, Xie Haipeng, Sun Xiaotian, et al. A cross-chain enabled day-ahead collaborative power-carbon-TGC market[J]. Energy, 2022, 258: 124881

[53] She Wei, Gu Zhihao, Yang Xiaoyu, et al. A model of multi-energy complementation and safety transaction on heterogeneous energy blockchain[J]. Power System Technology, 2019, 43(9): 3193−3201 (in Chinese)
(佘维, 顾志豪, 杨晓宇, 等. 异构能源区块链的多能互补安全交易模型[J]. 电网技术, 2019, 43(9): 3193−3201)

[54] He Yunhua, Zhang Cui, Wu Bin, et al. A cross-chain trusted reputation scheme for a shared charging platform based on blockchain[J]. IEEE Internet of Things Journal, 2022, 9(11): 7989−8000

[55] Novo O. Blockchain meets IoT: An architecture for scalable access management in IoT[J]. IEEE Internet of Things Journal, 2018, 5(2): 1184−1195

[56] Cui Zhihua, Fei Xue, Zhang Shiqiang, et al. A hybrid blockchain-based identity authentication scheme for multi-WSN[J]. IEEE Transactions on Services Computing, 2020, 13(2): 241−251

[57] Feng Chaosheng, Liu Bin, Guo Zhen, et al. Blockchain-based cross-domain authentication for intelligent 5G-enabled Internet of drones[J]. IEEE Internet of Things Journal, 2022, 9(8): 6224−6238

[58] Che Zheng, Wang Yu, Zhao Juanjuan, et al. A distributed energy trading authentication mechanism based on a consortium blockchain[J]. Energies, 2019, 12(15): 2878

[59] Liu Han, Han Dezhi, Li Dun. Fabric-IoT: A blockchain-based access control system in IoT[J]. IEEE Access, 2020, 8: 18207−18218

[60] Yu Guangsheng, Zha Xuan, Wang Xu, et al. Enabling attribute revocation for fine-grained access control in blockchain-IoT systems[J]. IEEE Transactions on Engineering Management, 2020, 67(4): 1213−1230

[61] Huang Junqin, Kong Linghe, Chen Guihai, et al. Towards secure industrial IoT: Blockchain system with credit-based consensus mechanism[J]. IEEE Transactions on Industrial Informatics, 2019, 15(6): 3680−3689

[62] Yang Wenti, Guan Zhitao, Wu Longfei, et al. Autonomous and Privacy-preserving energy trading based on redactable blockchain in smart grid[C/OL]//Proc of the 2020 IEEE Global Communications Conf.2020[2022-08-15].https://ieeexplore.ieee.org/abstract/document/9322167

[63] Goyat R, Kumar G, Saha R, et al. Blockchain-based data storage with privacy and authentication in Internet-of-things[J]. IEEE Internet of Things Journal, 2022, 9(16): 14203−14215

[64] Michalski R, Dziubałtowska D, Macek P. Revealing the character of nodes in a blockchain with supervised learning[J]. IEEE Access, 2020, 8: 109639−109647

[65] Peng Shaoliang, Hu Xing, Zhang Jinglin, et al. An efficient double-layer blockchain method for vaccine production supervision[J]. IEEE Transactions on NanoBioscience, 2020, 19(3): 579−587

[66] Li Meng, Hu Donghui, Lal C, et al. Blockchain-enabled secure energy trading with verifiable fairness in industrial Internet of things[J]. IEEE Transactions on Industrial Informatics, 2020, 16(10): 6564−6574

[67] Gai Keke, Wu Yulu, Zhu Liehuang, et al. Differential privacy-based blockchain for industrial Internet-of-things[J]. IEEE Transactions on Industrial Informatics, 2019, 16(6): 4156−4165

[68] Ping Jian, Yan Zheng, Chen Sijie. A two-stage autonomous EV charging coordination method enabled by blockchain[J]. Journal of Modern Power Systems and Clean Energy, 2021, 9(1): 104−113

[69] Guan Zhitao, Lu Xin, Yang Wenti, et al. Achieving efficient and privacy-preserving energy trading based on blockchain and ABE in smart grid[J]. Journal of Parallel and Distributed Computing, 2021, 147: 34−45

[70] Zhao Bingzhen, Chen Zhiyu, Yan Longchuan, et al. Privacy protection of power business transaction data based on blockchain framework[J]. Automation of Electric Power Systems, 2021, 45(17): 20−26 (in Chinese)
(赵丙镇, 陈智雨, 闫龙川, 等. 区块链架构的电力业务交易数据隐私保护[J]. 电力系统自动化, 2021, 45(17): 20−26)

[71] Cheng R, Zhang Fan, Kos J, et al. Ekiden: A platform for confidentiality-preserving, trustworthy, and performant smart contracts[C]//Proc of the 4th IEEE European Symp on Security and Privacy. Piscataway, NJ: IEEE, 2019: 185−200

[72] Unterweger A, Knirsch F, Leixnering C, et al. Lessons learned from implementing a privacy-preserving smart contract in ethereum [C/OL]//Proc of the 9th IFIP Int Conf on New Technologies, Mobility and Security. Piscataway, NJ: IEEE, 2018[2022-08-11].https://ieeexplore.ieee.org/abstract/document/8328739

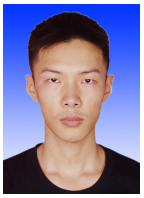
[73] Abdelsalam H A, Srivastava A K, Eldosouky A. Blockchain-based privacy preserving and energy saving mechanism for electricity prosumers[J]. IEEE Transactions on Sustainable Energy, 2021, 13(1): 302−314

[74] Zamani M, Movahedi M, Raykova M. RapidChain: Scaling blockchain via full sharding[C]//Proc of the 25th ACM Conf on Computer and Communications Security. New York: ACM, 2018: 931−948

[75] Leonardos S, Reijsbergen D, Piliouras G. Weighted voting on the blockchain: Improving consensus in proof of stake protocols[J]. International Journal of Network Management, 2020, 30(5): e2093

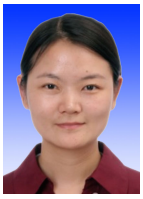
He Yunhua, born in 1987. PhD. Member of the IEEE. His main research interests include security and privacy in cyber-physical systems, bitcoin based incentive mechanism, security and privacy in vehicle ad hoc networks.

何云华, 1987 年生. 博士. IEEE 会员. 主要研究方向为网络物理系统中的安全和隐私、基于比特币的激励机制、车辆自组织网络中的安全和隐私.



Luo Mingshun, born in 1999. Master candidate. His main research interest includes blockchain technology and security.

罗明顺, 1999 年生. 硕士研究生. 主要研究方向为区块链技术、安全.



Hu Qing, born in 1985. PhD. Her main research interest includes advanced persistent threats and IOT security.

胡　晴, 1985 年生. 博士. 主要研究方向为高级持续威胁、物联网安全.

Wu Bin, born in 1980. PhD. His main research interests include covert communication, blockchain technology and network protocol analysis.

吴　槟, 1980 年生. 博士. 主要研究方向为隐蔽通信、区块链技术、网络协议分析.

Wang Chao, born in 1987. PhD. His main research interests include Internet of vehicles communication technology and Internet of things security.

王　超, 1987 年生. 博士. 主要研究方向为车联网通信技术、物联网安全.

Xiao Ke, born in 1980. PhD. His main research interests include the research and development and teaching work of wireless communications, Internet of things, and embedded systems.

肖　珂, 1980 年生. 博士. 主要研究方向为无线通信、物联网、嵌入式系统的研发和教学工作.