区块链应用场景落地面临的挑战及应对策略研究

张 昊
（中国科学技术信息研究所，北京 100038）

摘 要：为加快推进区块链应用场景向纵深发展，释放区块链技术潜在价值，本文对区块链技术落地存在的点对点网络实现困难、并发处理能力不足、数据存储能力不强、跨链互通困难等技术性因素进行分析，同时对监管不到位、隐私保护存在隐患等非技术性因素进行总结，提出推动区块链技术应用进一步深化的策略。

关键词：区块链；智能合约；分片技术；有向无环图；技术标准
中图分类号：C01 **文献标识码**：A DOI：10.3772/j.issn.1009-8623.2022.02.003

区块链技术诞生于 2008 年，是集成了已有的多种成熟技术的革命性创新技术，已成为各国竞相发展的战略性技术。近年来，随着区块链技术的地位逐渐提高，解决区块链应用落地遇到的技术性难题，推动区块链服务于实体经济与产业升级，成为释放区块链技术能力的关键。

1 区块链概念与特性

区块链技术是分布式的网络数据管理技术，利用分布式账本、非对称加密、点对点传输等较为成熟的技术，具有数据多方维护、交叉验证、全网一致、不易篡改等特性。区块链技术以应用为导向，缘起于 2008 年中本聪创立并启动的比特币金融系统。经过十多年的更迭，比特币已经成为市值最高的数字货币，总市值超过 1 万亿美元，而依托区块链技术，全球数字加密货币的总市值也已超过 2 万亿美元。

由于区块链技术具有透明、可信、可溯源、难以篡改、匿名等特性，可以确保数据安全与隐私，能够以去中心化的方式解决互联网信息不对称、多个协作主体之间缺乏信任以及交易流程效率低下等问题[1]，该技术逐渐突破数字加密货币应用，向人们社会生活的更多领域拓展。

国内近年来涌现出诸多区块链技术深层次应用。蚂蚁金服旗下的蚂蚁区块链发布 ODATS 联盟链跨链方案，能够实现用户低成本、安全和跨平台的交互操作。腾讯云推出的区块链即服务平台 TBaaS 能够极大地降低企业实现区块链底层技术的成本。根据《全球区块链产业发展全景（2020—2021）》，京东智臻链 BaaS 平台提供的防伪追溯功能已有超 13 亿条上链数据。国外区块链项目中，由 Meta 等巨头联合发起的 Libra 项目，由巴克莱、纳斯达克等银行和金融机构联合发起的 Utility Settlement Coin 项目，由摩根大通发起的 JPMCoin 项目等，均以数字货币为依托，致力于向世界推销具有支付功能的金融基础设施。因此，区块链技术在提升社会生产力、改变生产关系等方面具有广阔前景，有望成为促进传统商业模式升级的重要底层工具。此外，随着元宇宙概念的不断成熟，区块链技术作为元宇宙的重要组成部分和核心技

作者简介：张昊（1996—），男，研究实习员，主要研究方向为人工智能技术发展、区块链发展战略研究。
项目来源：2021 年度中信所创新基金青年项目“区块链应用场景落地面临的挑战及应对策略研究”（QN2021-11）。
收稿日期：2021-12-24

术，对产生虚拟世界的数字资产、完成虚拟社会经济系统的构建具有不可或缺的作用。但当前区块链技术诱发了诸多数字资产犯罪，成为实施洗钱、非法集资、金融诈骗等行为的常用工具。

2　区块链落地困难因素

区块链技术从产生开始就存在缺陷。当前区块链应用存在“不可能三角”，即无法同时保证“去中心化”“安全性”及“交易处理性能”，通过已有手段只能同时实现其中两个。该理论并没有经过严格的论证，而是业内对实际情况下的区块链应用进行总结后得出的结论。目前，尚未出现将三方面同时做得出色的公链，“不可能三角”仍未被打破，也成为了制约区块链大规模应用的壁垒。例如，比特币去中心化程度最高，但处理效能低下，仅适合特定场景应用；EOS、数字政务、数字发票等提高了并发处理能力，但降低了去中心化水平。此外，区块链技术还存在非技术性问题。

2.1　技术性因素

区块链技术架构主要包含数据层、网络层、共识层、激励层、合约层和应用层（见图 1）。目前，区块链的不同层级均存在风险挑战，下面具体就关键风险进行分析。

2.1.1　可扩展性不足

缺乏可扩展性已经成为限制区块链技术大规模应用的最重要因素，对于金融、存证、溯源等依赖高性能处理的应用场景来说，区块链的处理能力明显不足。当前运行的公链中，最核心的是比特币、以太坊以及 EOS。比特币系统吞吐量（TPS）约为 7，即每秒能处理 7 笔交易。以太坊的理论 TPS 为 2 048，其在世界范围内分布众多节点，保证了去中心化程度，但由于需要保证网络同步率，以太坊的实际TPS仅为7~15。EOS作为区块链3.0的有力竞争者，TPS 达到 3 000~4 000，远高于比特币与以太坊，但处理能力仍无法达到大规模应用的需求，同时 EOS 仅有 21 个超级节点，节点数目远低于其他公链，未实现去中心化，在抵御黑客攻击上也存在劣势。

此外，区块链还面临粉尘攻击和空块攻击等问题。DOS 攻击主要通过降低区块链交易处理效率进行，影响共识效率和交易吞吐量 [2]。日蚀攻击通过攻击比特币网络，用 40% 的算力就可以达到 51% 的攻击效果 [3]。

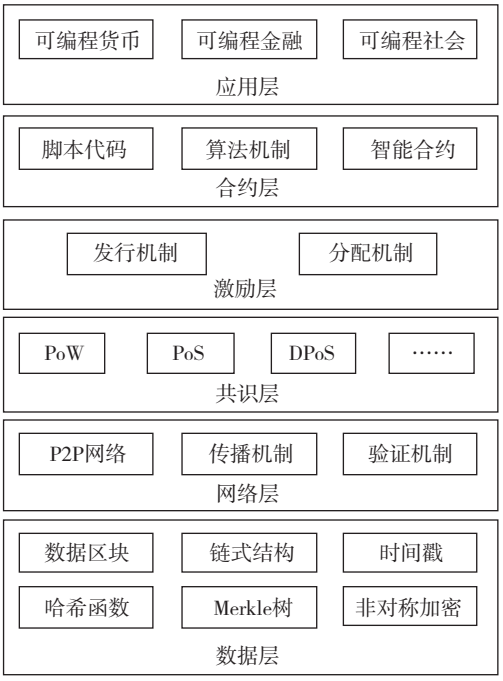

图 1　区块链技术架构图

2.1.2　智能合约安全性存疑

智能合约是区块链技术的核心，是保障各类交易稳定运行的自动化工具，但目前仍有诸多因素影响智能合约的安全性。人为因素方面，智能合约的编写与生成完全依赖程序员，开发人员的编程水平将直接影响合约的功能完整性及条款严密程度，同时，由于无法确保开发人员自身的合规性，合约中可能出现人为主观意识的叠加，导致漏洞被不法分子利用，造成严重损失 [4]。此外，当前编程脚本语言成熟度不高，合约中不可避免地会出现整数溢出、函数调用错误等程序错误，此类案例已屡见不鲜（见图 2）。The DAO 是以太坊著名的项目，在 2016 年筹集了 1.5 亿美元，是当时世界上最大规模的众筹，而 2016 年 6 月 18 日，黑客利用 The DAO 中递归和资产销毁两个漏洞进行了 200 多次攻击，造成超过 360 万枚以太币的损失。2018 年 4 月 22 日，黑客通过整数溢出漏洞攻击了 BEC 的 Token 合约，释放了大量 Token，致使 BEC 的价格几乎归零。2018 年 5 月 29 日 EOS 节点远程代码执行。2020 年 9 月 27 日，Kucoin 库币被黑客入侵，损失数亿资金。

2020 年 12 月 21 日，英国加密货币交易所 EXMO 发生重大安全漏洞，导致平台冻结所有提款。此外，智能合约涉及法律有效性的问题，作为自动执行的约定，其并不具备法律效力，在出现问题时尚不能作为法律凭证。此外，长期存在的双花攻击（恶意节点掌握全网 50% 以上的算力，就可以生成比主链更长的侧链）[5] 和 DOS 攻击（通过填充多余的请求使主机系统或者主机网络资源过载，从而阻止合法服务的实现）[6]，也成为区块链技术难以消除的隐患。

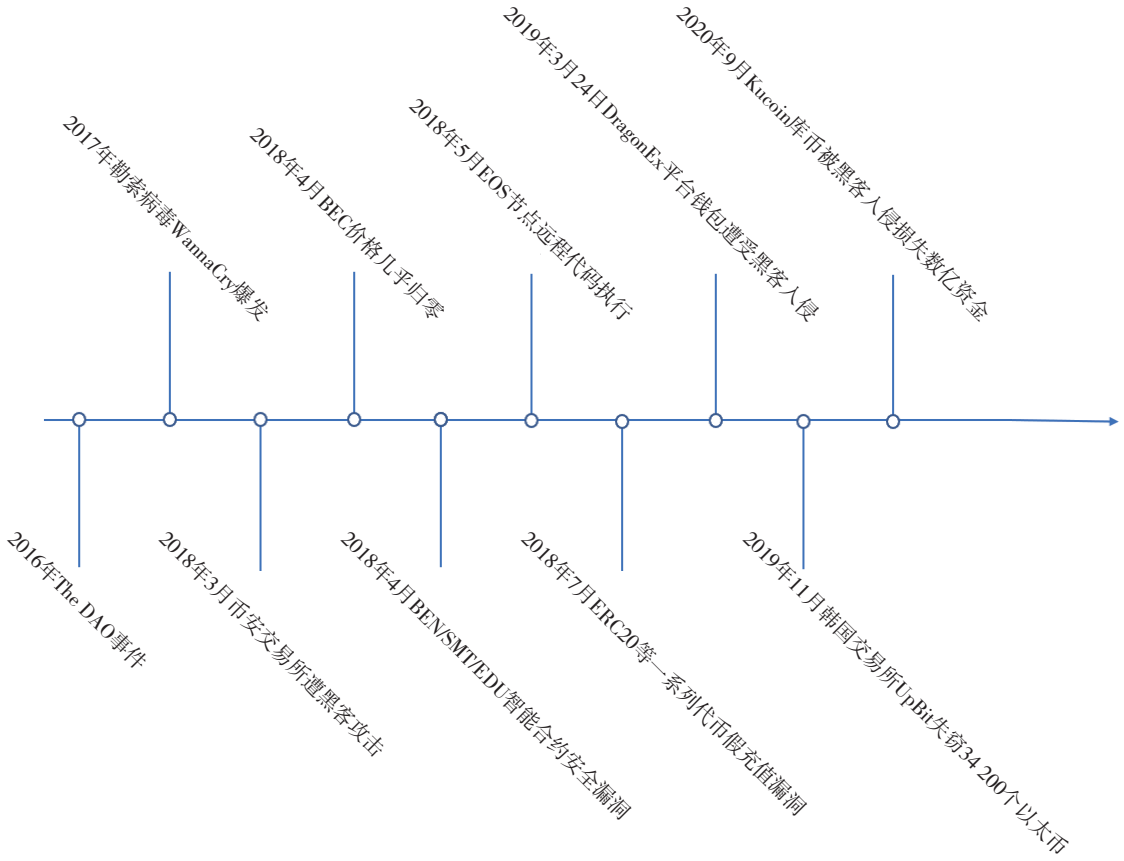

图 2　各大区块链系统漏洞及发生时间

总体来讲，当前智能合约的角色是一套自动化流程与方法，而鉴于目前智能合约存在的安全隐患和更多自动化流程的选择，其不可替代性仍有待商榷。

2.1.3　区块链技术缺乏针对用户私钥灾难的救赎机制

区块链技术体系的突出特点是公钥私钥唯一性。用户成为区块链系统中节点的唯一方式是公钥和私钥的匹配，私钥的唯一性也带来硬风险。一旦用户忘记或丢失私钥，则再也无法获取电子钱包中的数字资产。若私钥失窃，数字资产被转移后，由于区块链交易不可撤回，被盗窃财产也无法追回。因此，面对资产损失风险，当前区块链尚不存在救赎机制。这种过于单一的安全措施也制约了区块链技术的进一步应用。此外，部署现代公钥加密基础设施已经花费了近 20 年的时间 [7]。随着量子计算技术的发展，一些专家甚至预测，在未来 20 年左右的时间里，将建造足够大的量子计算机，以破解目前使用的所有公钥方案 [8]。

2.2　非技术性因素

一是区块链存在的意识形态风险。区块链从诞生起的最终目的就是实现完全去中心化，这也成为区块链技术意识形态的核心，尤其是随着去中心化概念的不断发展，涌现出众多模仿比特币的完全去中心化区块链项目。但正如前文分析，“不可能三角”的存在导致完全去中心化的系统无法在现实世

界落地，无论系统如何发展，最终的结果不是由中心化权力机构接管，就是由于缺乏强有力的协调机制而分裂或下线，即使是比特币、以太坊这些长时间活跃的项目也遭遇过多次硬分叉。因此，以形成完全去中心化的系统为目标成为当前区块链发展的意识形态陷阱。

二是监管和法律体系保障不到位。区块链作为集成性的创新技术，正在不断影响行业发展和社会管理方式，但新技术必然存在技术标准缺乏和监管体系不完善的短板。目前社会各界都在积极探索建立区块链的技术标准，其中以行业企业为主，例如苏州、南京等企业发布《区块链基础技术规范》，中国电子技术标准化研究院正在制定《信息技术区块链和分布式记账技术参考架构》，国家标准稳步推进。但总体上看，区块链技术监管仍无法赶上技术发展速度，监管需求不断紧迫。

现有法律体系能够对线下资产进行较为明确的划分，但区块链系统内涉及众多数字资产，一旦在交易系统中出现纠纷，当前体系下对保障不同主体利益的规定仍较为模糊，大多数法律问题都停留在研究阶段，交易双方的法律权益无法被保障，只能依靠智能合约完成约定。在未来，私人数字资产的认可度仍需进一步讨论；另一方面，需继续研究如何确保执法机构在维护受害人法律权益时，能够以强有力的方式对被执行人进行约束。

3　解决措施

3.1　技术措施

目前尚未出现能较好解决“不可能三角”的方式，各类优化模式都是牺牲某一方面优势来获取区块链性能提升。

3.1.1　分片技术

分片技术最初出现于数据库领域，即将大型数据库分散为数据分片，储存在不同服务器中，以降低服务器的访问压力，提升整体效能。比特币的闪电网络（Lightning Network）、以太坊的雷电网络（Raiden）和赛勒网络（Celer Network）都属于这一领域。

分片技术在多个较小的节点组之间分摊处理运行成本，通过并行工作可最大限度地提高性能，同时使每个节点所需的通信、计算和存储显著减少，从而允许系统扩展到大型网络。然而，现有的基于分片的区块链协议仍然只能部分地获得分片的潜在好处，这给这些协议的吞吐量和延迟带来了一个主要瓶颈。除了有限的可扩展性之外，这些协议由于故障韧性较低或故障率高导致安全性较弱，这限制了它们对主流支付系统的适用性。

3.1.2　以太坊 Layer 2 方案

随着用户量和交易量不断增长，以太坊性能缺陷愈发明显。一方面由于 TPS 过低，用户在交易高峰期等待时间过长、网络拥堵等问题严重；此外，伴随小额高频交易和长尾项目的出现，以太坊过高的手续费（Gas Fee）阻碍了诸多交易的发展。在以太坊 2.0 迟迟无法面世的情况下，Layer 2 成为目前以太坊的最佳扩容方案。Layer 2 建立在区块链 Layer 1 的基础上，同时共享主链的安全性，通过将主链的部分数据处理任务分配到 Layer 2 平台上，降低主链的数据处理压力，从而提升整体交易速度和吞吐量。

当前 Layer 2 方案主要有 Plasma、Rollups 和 Sidechains，但由于不同方案之间实现逻辑不同，实践中的安全性、扩展性和去中心化程度也不尽相同（见表 1）。

3.1.3　有向无环图（DAG）技术

相较于链式结构来说，有向无环图是树状结构，并具有较多优点。一是图有多个出度，可同时处理多个相连节点，同时支持并行计算，将区块链的同步记账改为异步记账，在节约计算资源的同时大幅提升交易速度。二是有向无环图各节点之间无需等待同步，扩展性强，尤其适用于物联网项目。三是有向无环图可使作恶难度加大，相比于链式结构，有向无环图中的恶意篡改需要同时修改节点的出度和入度，作恶成本更高。此外，由于有向无环图允许用户账本之间存在短时间的数据不同步，因此有向无环图各节点的交易量越大，则交易处理越快[9]。

有向无环图的重点项目有 IOTA、Byteball、TrustNote 、Nano 等，不同项目之间的节点分类和对抗双花问题等系统性问题出现的方式也不尽相同（见表 2）。

虽然有向无环图的安全性和一致性仍需要检验，但该技术的创新给区块链技术的广泛应用带来了新的可能。

表 1　不同 Layer 2 方案特征比较

	Plasma	Rollups	Sidechains
实现逻辑	不在主链保存原始交易数据、专门的验证节点和“欺诈证明”	在主链保存原始交易数据、专门的验证节点和“有效证明”	与主链相互独立、自行负责安全性和共识实现过程
安全性	低	中	低
可扩展性	高	中	高
去中心化程度	低	中	低

表 2　不同有向无环图重点项目特征比较

	IOTA	Byteball	TrustNote
代币	IOTA	Byte	TTT
共识机制	PoW 权重累加	12 名公证人	去中心化 TrustME 共识
智能合约	不支持	声明式合约	高级声明式合约
奖励机制	无	交易引用和公证	交易引用和挖矿
节点分类	全节点 轻节点	全节点 轻节点	超级节点 全节点 轻节点 微节点
交易费	无	有	有
双花问题	PoW 权重比较	MainChain 定序	MainChain 定序
低交易量问题	中心化协调	弱中心化公证人	TrustME 公证人

3.2　政策建议

（1）围绕重大战略部署，加快推出区块链技术标准。

要集中优势资源突破大数据核心技术，在前沿技术研发、数据开放共享、隐私安全保护等方面做好前瞻性布局。应推进国家标准体系建设，在区块链技术的知识产权领域循序渐进地参与、制定、引领相应技术标准，更好地推动人工智能技术等新一代技术与区块链的深度融合。

（2）加快底层技术攻关步伐，打造优质区块链技术联盟。

一是大力发展区块链底层技术，加快推进区块链底层核心关键技术研发，如共识机制、跨链技术等，开展产品研发和测试。政府部门可从科研立项、研发费用补贴等方面支持区块链底层技术研究。加强与国内公司合作，模拟建立应用场景，进行完善的技术储备。二是培育良好技术生态。调动政府、科研院所、领军企业等的资源，共同为区块链发展培育良好科研环境。三是打造优质区块链技术联盟，充分整合分散资源，支持开源开放，构建软硬件协同的生态系统。推动新一代基础设施建设，以保护公民现实世界的数字镜像和数字资源的产权为目标，研发区块链基础设施，如区块链操作系统等。

（3）制定相关政策细则，回应基本法律问题。

为回应和引导区块链技术应用的规范化发展，应明确规定区块链技术应用数据的法律效力，进一步制定规则、指引等指导意见，如在司法领域，可明确区块链技术的适用性，出台相关指导意见，将区块链技术发展关键环节与法律法规相关要素整合，引导区块链技术在产业和行业中的合理、合法应用。

（4）加强国际国内同业交流，培育区块链技术人才。

区块链技术的推广需要监管部门、金融机构和互联网企业的通力协作，需要根据区块链技术的发展与创新动向及时调整发展战略和应用标准，积极参与国际区块链联盟组织的研究交流和标准讨论，加强国际国内的同业交流与合作，力争加入国际区块链系列产品的研究和开发。国内可成立专门实验室，推进区块链技术的研发以及与不同行业的融合应用。应尽早建立培养、招募和储备区块链人才的制度，设立专门的人才培养制度，引进专业师资和专家团队，联合培养人才，为区块链技术开发、应用及推广提供人才储备和智力支持。

（5）提升对区块链技术认知能力，改善行业治理。

一是监管部门应加强对区块链的全面认知，建立区块链类型管理制度，将公有链、联盟链、私有链进行明确界定，实施分类管理制度。二是积极引导社会公众，一方面加强对区块链技术的宣传引导，使公众认识到区块链技术的优势特点，建立对技术本身的信心，认识其应用的重要意义。另一方面要充分认识区块链技术的发展现状，不盲目夸大技术的颠覆作用，谨防 NFT、DeFi 等新晋区块链应用形成的泡沫。注意防范区块链对传统机构管理、商业运营模式的冲击，以及操作陷阱、技术垄断等潜在风险。营造行业良好氛围，为区块链等颠覆性技术营造良好的传播环境，鼓励不同行业机构联合开展区块链技术合作研究。■

参考文献：

[1] Yang L. The blockchain: state-of-the-art and research challenges[J]. Journal of Industrial Information Integration, 2019, 15(C) : 80-90.

[2] 韩璇，袁勇，王飞跃 . 区块链安全问题：研究现状与展望 [J]. 自动化学报，2019，45（1）：206-225.

[3] Heilman E, Kendler A, Zohar A, et al. Eclipse attacks on Bitcoin's peer-to-peer network[EB/OL]. (2018-10-05) [2021-10-01]. https://www.usenix.org/system/files/conference/usenixsecurity15/sec15-paper-heilman.pdf.

[4] 孙国梓，王纪涛，谷宇 . 区块链技术安全威胁分析 [J]. 南京邮电大学学报（自然科学版），2019，39（5）：48-62.

[5] 房卫东，张武雄，潘涛，等 . 区块链的网络安全 : 威胁与对策 [J]. 信息安全学报，2018，3（2）：87-104.

[6] Chen L, Jordan S, Liu Y K, et al. Report on Post-Quantum Cryptography[R/OL]. (2018-10-05) [2021-10-01]. https://www.nist.gov/publications/report-post-quantum-cryptography.

[7] Zhang R, Xue R, Liu L. Security and privacy on blockchain[J]. ACM Computing Surveys, 2019, 52(3):1-34.

[8] Mosca M. Cybersecurity in an era with quantum computers: will we be ready?[J]. IEEE Security & Privacy, 2018: 38-41.

[9] 斯雪明，徐蜜雪，苑超 . 区块链安全研究综述 [J]. 密码学报，2018，5（5）：458-469.

Research on Challenges and Countermeasures of Blockchain Application Scenario Landing

ZHANG Hao

(Institute of Scientific and Technical Information of China, Beijing　100038)

Abstract: In order to accelerate the in-depth development of blockchain application scenarios and release the potential value of blockchain technology, this paper analyzes the technical factors existing in the implementation of blockchain technology, such as difficulties in point-to-point network implementation, insufficient concurrent processing capacity, weak data storage capacity, difficulties in cross chain communication, and summarizes the non-technical factors such as inadequate supervision and hidden dangers in privacy protection. Finally the paper puts forward strategies to further deepen the application of blockchain technology.

Keywords: blockchain; smart contract; sharding technology; directed acyclic graph; technical standard