区块链对信息系统开发和应用的影响

The Impact of Blockchain on Information System Development and Application

李梓童[1]

摘要 区块链是一项变革性的新兴技术，具有去中心化、数据时序性、集体维护等特点，表现出在信息系统中实现大规模协作的潜力，将会对信息系统的开发与应用带来重大变革。本文通过使用文献调查、规范分析、实证分析等研究方法，首先对区块链和信息系统作简要介绍，再从规划、分析、设计、实施四个角度探讨区块链在信息系统开发过程中的影响，接着从促进资源共享、简化信任背书、精简执行流程三个角度分析区块链在节约人力成本方面的影响，最后从信息安全、时空效率、耗能问题角度分析区块链带来的新的问题，旨在为区块链在信息系统领域的发展提供有利的理论支持。
关键词 区块链，信息系统，开发与应用，影响

Abstract Blockchain is a revolutionary emerging technology with the characteristics of decentralization, data timing and collective maintenance showing the potential for large-scale collaboration in information systems, and will bring great changes to the development and application of information systems. This paper begins with a brief introduction to blockchain and information systems, then discusses the influence of blockchain in the development process of information system from the perspectives of planning, analysis, design and implementation. After that, it analyzes the impact of blockchain on saving labor costs from three perspectives: promoting resource sharing, simplifying trust endorsement, and streamlining the execution process. Finally, new problems brought by blockchain are analyzed from the perspectives of information security, space-time efficiency and energy consumption. This paper aims to provide favorable theoretical support for the development of blockchain in the field of information systems.

2008 年，化名“中本聪(Satoshi Nakamoto) ”的学者发表论文《Bitcoin: A peer-to-peer electronic cash system》[1]，此后，区块链逐渐成为科技领域的热点。

区块链可看成由“分布式账本”组成的系统，在去中心化的理念下，每个账本都有写入信息（创造价值）的权力。每一个数据包（交易信息）发出，经过一定的激励和竞争后，如果该数据包得到了系统的认可（其后接上了一定数量的新块），该数据包或进入总链，否则便被丢弃。同时账本（节点）上存在大量的信息冗余，以保证数据的安全性。

现在，区块链已走出金融领域，在科技、政治、贸易等其他领域发挥重要作用。它对信息社会产生的影响是巨大的：改变了信息的组织方式和传递方式，通过分布式架构促进了信息的共享，采用数字化的手段形成了自信任的体系，在无形之中创造了价值，等等[2]。

信息系统是一门历史悠久的学科，技术层面上看可以分为信息的输入、信息的处理、信息的输出三部分，在不同的应用场合有不同的实现方式和功能类型。区块链技术的出现，为信息系统注入了新鲜的血液：区块链所代表的新的数据组织方式（高冗余分布式存储），对

[1] 中国人民大学信息学院， 北京 100872

传统信息系统的数据组织方式产生了冲击。建立在分布式系统上的共识机制，影响着信息系统的数据确认方式。新的数据结构对应新的保护措施，这是信息系统在应用区块链技术时不得不考虑的问题。如此种种，都说明区块链正改变着信息系统的开发思维和应用方式。由此，本文意图对这一问题进行深入分析与整理：区块对信息系统的开发与应用产生了什么样的影响？

1 文献综述

本文针对区块链的相关内容进行了文献的搜集与整理，结果发现，目前区块链领域的研究可大体分为区块链在某一领域中的应用和区块链安全性能分析两类。

1.1 区块链在某一领域中的应用

这些研究针对不同领域各自的特点，对应区块链技术自身的特征，分析区块链在这些具体语境中的实施情况。

例如，黄俊飞、刘杰在《区块链技术研究综述》中提到区块链在金融领域的应用。区块链脱胎于比特币，作为新兴的金融科技，金融行业是其最重要的应用领域，在数字货币、金融交易、资产管理等方面都有广泛的应用[3]。

同样是金融领域，傅晓阳在《区块链技术应用探索》中提到兴业银行成功将区块链应用于汽车金融、承兑汇票等业务场景和见证代管业务的“倚天鉴”电子合同平台等[4]，推动了区块链在金融领域的应用。

在数据保护领域，由于区块链具有执行匿名交易的能力，这为数据或隐私的保护提供了透明机制。例如，Lazarovich A. 在《Invisible ink: blockchain for data privacy》提出了基于区块链审计的的隐形墨水系统，说明了区块链技术在数据保护方面的应用[5]。

除了上述提到的金融应用和数据保护领域外，区块链技术还在车联网、电力交易、智能交通、物联网等领域都得到应用。这些区块链领域内的研究大多为给出一个具体的应用场合，讨论区块链在其中的使用前景。

1.2 安全性能分析

区块链的安全性是现在该技术所面临的重大问题，现有许多文献对区块链的安全问题做出总结、提出其可能存在的隐患，或阐述相关的安全监测模型、以期提高区块链的安全性。

例如，在《区块链技术发展现状与展望》中，袁勇、王飞跃提出量子计算的发展可能会使区块链依赖的哈希函数、公钥加密算法、零知识证明技术的安全性受到威胁，从而影响整个区块链的安全性[6]。

在《区块链安全问题：研究现状与展望》一文中，韩璇等人列举了区块链可能存在的种种安全问题，如跨链操作问题、监管技术缺失、代码漏洞、P2P 安全漏洞、安全性假设不可靠等[7]。虽然区块链会为信息系统应用带去一定的便利性，同时也为其埋下安全隐患。

在《区块链的安全检测模型》中，叶聪聪、李国强、蔡鸿明等人提出一种根据区块链的结构来评估和检测安全性的方法。当一个区块后连接 6 个区块后，可认为该区块达到稳定状态，通过分析每个区块链达到稳定状态的概率来评估安全性[8]。

通过文献资料的查阅分析，可以看出学术界研究的重点是区块链在不同领域中的应用及其安全方面的问题，因此本文结合相应的调查，探讨区块链对信息系统开发和应用的影响。

2 研究方法

2.1 文献调查法

文献研究法主要指搜集、鉴别、整理文献，并通过对文献的研究形成对事实的科学认识的方法。在研究区块链对信息系统开发和应用的影响时，通过搜集和总结有关文献，逐渐形成对此问题的科学认识。

2.2 规范分析法

规范分析涉及已有的事物现象，对事物运行状态做出是非曲直的主观价值判断。在本文撰写过程中，通过主观价值判断，从正面影响和负面影响两个角度来考虑区块链对信息系统应用产生的影响。

2.3 实证分析法

实证分析指着眼于当前社会或学科现实，通过事例和经验等从理论上推理说明。在研究过程中，分析有关事实案例，总结得出区块链对信息系统开发与应用的影响。

3 区块链、信息系统简介

区块链：一般来说，区块链系统由数据层、网络层、共识层、激励层、合约层和应用层组成[5]。从技术角度看，它是一种构建在点对点网络上，利用链式结构来验证和存储数据，利用分布式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性，利用由代码组成的智能合约来编程和操作数据的分布式基础架构与计算范式[9]。

信息系统：信息系统是一个以人为主导，吸取经验和遵照规律并重，利用适合的信息技术以及相应设备，根据相应的业务模型和数学模型，进行信息的收集、传输、加工、储存、更新和维护，以提高组织的效益和效率为目的，支持组织的高层决策、中层控制、基层运作的集成化的人机系统[10]。

4 区块链对信息系统开发的影响

4.1 区块链对信息系统开发的影响

信息系统开发可分为规划、分析、设计、实施四个阶段，本节主要从这四个阶段讨论区块链对信息系统开发的影响。

4.1.1 规划

规划阶段，开发者应首先考虑系统应用需求、区块链本身特点（时序性、不可篡改、去中心化信用、智能合约自动执行，虽有技术层面的安全保障但并非绝对安全，分布式数据高冗余存储带来额外的空间消耗等）和现实条件（如资金、时间、人力等）制约，判断是否应当使用区块链或在多大程度上采用区块链的体系架构。

例如，若开发的信息系统其子模块便已具有较大的数据规模，再进行子节点拷贝所有数据区块的存储方式会占用大量的空间、产生很高的成本，此时便应斟酌是否采用区块链技术；若开发的信息系统数据规模较小，且在信任、价值等“敏感”领域有较高的精度要求，便可考虑采取区块链技术进行开发。

规划阶段，区块链为信息系统开发人员提供了另一种选择，但需注意区块链技术不是适

合于所有信息系统的，具体问题具体分析才是上策。

4.1.2 分析

假设在规划过程中已确定采用区块链技术，分析阶段便应对区块链技术的运用作进一步细化，分析信息系统的需求与区块链使用之间的联动关系。例如，根据数据的使用频率、规模大小、保密等级分析哪些应该写入数据区块，根据区块链的使用场合判断应采取公共链、联盟链还是私有链，根据数据处理的具体要求分析智能合约的结构等等，确定区块链架构的方向并划定相应的运用范围。

4.1.3 设计

设计阶段，需要根据分析得出的需求具体化区块链的细节，为最后的实施做准备。在这一阶段，开发者需具体从数据层、网络层、共识层、激励层、合约层等六个层面考虑区块链的建设。例如，从数据层角度，根据特定需求给出相应的数据结构；从网络层角度，结合通道安全性进行设计；从共识层角度，根据算力限制和规模等条件选择共识方式，等等。

4.1.4 实施

在实施应用区块链技术的信息系统时，开发者需要根据实际情况搭建区块链体系。其中，需要考虑的内容包括而不限于下列因素：区块链平台的选择，目前世界上的区块链平台种类丰富，开发者可以根据限制条件和具体应用场合进行选择；二是程序迁移的问题，目前区块链的主要应用领域是金融与货币，在别的领域进行代码迁移或升级时是否有足够好的兼容性；同时，还需预留一定的时间进行风险管理，对信息系统进行测评和完善。

5 区块链对信息系统应用的影响

信息系统应用中，区块链一方面起到了节约人力成本的积极作用，另一方面也带来了新的问题。

5.1 节约人力成本

区块链的出现减少了“人”在信息系统操作中的低技术型劳动，从而达到节约成本，提高效率的目的。接下来将从促进资源共享、简化信任背书、精简执行流程三个角度作进一步阐述。

5.1.1 促进资源共享

区块链促进了信息系统的资源共享。这种资源共享表现在两方面，一是不同领域、相同层级的信息系统之间的资源共享，二是同一领域、不同层级的信息系统之间的资源共享。

区块链广泛使用数字签名、非对称密钥等加密技术，灵活地在数据存储和流通中运用密码学手段进行数据保护，使得区块链上节点可以在数据安全的环境里进行数据交换；区块链的底层架构是开放的体系，通过共识算法实现数据传输，可以使本区块链与其他区块链进行对接或较为方便地增加新的节点。由于这两个原因，使用了区块链技术的信息系统在应用时具有较大的灵活性，信息系统中节点的资源共享更加方便。

一是不同领域、相同层级的信息系统之间的信息传递，便是本区块链与其他区块链进行对接的过程。例如，政府金融监管部门可以通过引入基于区块链的点对点数据授权共享机制，为广大互联网金融产品提供更为完整的可信数据分析产品，实现了金融监管部门信息系统与互联网金融产品信息系统这些独立系统之间的资源共享[11]。

二是同一领域、不同层级的信息系统之间的资源共享，便是在一个大的系统下其子系统的信息传递的过程。例如，DongChang Zhao 提出区块链在汽车租赁系统中的应用[12]，整个汽车租赁行形成一个父系统，而每个汽车租赁单位形成一个子系统，记录单辆汽车租赁的细节内容，父系统易于增删子系统、实现汽车租赁的统筹管理。

从以上两个方面考虑，区块链因其链式架构的灵活性和加密技术的安全性，在信息系统应用中起到了促进资源共享的积极作用，提高了信息传递的效率和信息解读的便利性，增强了信息系统的灵活度。

5.1.2 简化信任背书

区块链的一大革新，便在于其“创造”了信任。由于区块链的分布式架构、不可篡改和共识机制等因素让抵赖和造假的成本巨大，使得最终的交易结果可以被信任。也就是说，它用数字化的手段建立了信任机制。自动化信任机制的产生，使得信任背书这过去需要走访多方、手续繁复的过程大大精简了。

未应用区块链的系统中，如果要对数据进行存证，往往需要当事人亲自到合法的鉴定机构办理相关手续后才能形成有效证明。不仅过程耗费人力物力，而且很多数据难以形成有效的证明。区块链的诞生将这一过程数字化、大大减少了人力成本，不仅如此，还能从技术上杜绝数据的篡改和删除，具有很强的公信力。

以银行业为例，由于涉及资金的流转，银行之间必须通过反复互相校对来确保各自账本的一致性，为此付出了大量的人工成本和时间成本，提高了交易的手续费。而由于区块链的出现，银行之间可以利用分布式账本实现即时同步、更新不可篡改的数据，使利益相关的多方无需进行额外的工作就能保证其数据的一致性，极大地降低了成本。类似的利益相关多方互不信任场景并不罕见，区块链信任自动化的机制减少了繁冗的手续。

5.1.3 精简执行流程

精简执行流程主要从智能合约角度实现。区块链的智能合约在程序层面上自动执行，减少了人在其中的工作量，加快信息处理和反馈的速度，从而提高信息系统的运行效率。

以商业社会为例，“交易迟滞”是商业社会中延缓交易速度的重要原因，造成交易迟滞的原因有商业合同签订流程延迟、合同执行不一致而受阻、打款流程反复等[13]。而区块链中智能合约的存在可以较好地提高交易的效率：由于智能合约高度数字化的特性，一旦符合条件即自动执行，大大减少了如打款、谈判、寄送、签署等需要人工进行的工作量，从而提高了信息系统的运行效率。

5.2 新产生的问题

区块链并不是十全十美的，它虽然可以提高信息系统的效率，但同时也带来了新的问题。接下来将从信息安全、时空效率、耗能问题作进一步阐述。

5.2.1 信息安全

区块链技术通过公钥加密、数字签名、哈希函数等密码学组件实现信息系统的隐私保护需求，但这并不意味着区块链的安全设施是功不可破的。例如 PoW 共识机制下的区块链面临 51%算力攻击的威胁，其非对称性加密机制也随着密码学、计算技术和数学的进步而变得脆弱，以及智能合约存在漏洞，等等，这些因素都会引发安全事故，导致使用区块链技术存储信息时由于区块链自身架构的缺陷和外部攻击等原因，数据的保密性、完整性和可用性受损。

例如 2016 年 6 月，区块链物联网公司 Slock.it 发起的众筹项目 The DAO 智能合约存在

漏洞，被黑客利用使得 300 多万以太币资产被分离、以太坊被迫进行硬分叉。在这一过程中，信息系统的安全性受到打击，数据的完整性被破坏。

不仅如此，即便区块链本身暂未发现安全问题，其产生的价值也可能为不法分子所觊觎，引起信息系统的破坏。例如，2017 年 5 月，比特币勒索病毒 WannaCry 全球范围内爆发，至少 30 万名用户受害，影响到金融、能源、医疗等众多行业。区块链技术的产物比特币因其具有的价值被不法分子作为交易的筹码，导致大量不同领域的信息系统中数据的可用性被破坏。

对于传统信息系统，系统安全往往通过单向加密来实现，安全性能更大程度上需要“人”发挥作用，而在区块链背景下，则对智能合约、51%算力攻击等都需纳入考虑范围之内。

5.2.2 时空效率

信息系统应用中，人们希望尽可能降低数据存储空间。而在区块链的架构下，每个节点都有一份完整的数据拷贝，且数据规模随着链的不断增长有增大的趋势，形成大量的冗余，这会对信息系统的空间利用率产生不可忽视的影响。

例如，比特币网络中，2018 年十月数据已超过 200GB，而且还在进一步增加。比特币网络由于其节点中数据结构量度较小，即便每个节点都有一份数据拷贝也尚在可接受的范围之内。而对于其他信息系统，若应用区块链技术，节点中包含的数据类型可能就千变万化，再做一份数据拷贝，产生的数据规模可能会非常的大，造成存储的困难。

另外，对数据操作时间而言，交易场合中区块链的交易效率是另一个痛点。如比特币区块链在每秒内处理的交易数仍是个位数，显然无法满足其他金融系统高频交易的需求。

5.2.3 耗能问题

若应用区块链的信息系统采用 PoW 这样用算力来决定共识的算法，高耗能也就成了另一个问题。PoW 机制中，机器贡献的算力主要用于寻找合适的随机数使之产生满足要求的哈希值，除此之外没有其他社会价值的输出。例如，目前比特币在挖矿竞争中吸收了大量的算力资源，比特币生态圈内企业有资本密集型的高耗能企业发展趋势。若其他规模较大、节点较多的信息系统应用区块链技术且采用 PoW 共识机制，在算力和电力资源上的消耗也是值得考虑的。

6 结束语

本文主要探讨了新兴技术区块链对信息系统开发与应用的影响。在信息系统开发过程中，区块链的影响主要表现在：规划时根据需要判断是否采用区块链及多大程度采用区块链；分析时进一步细化需求；设计时根据需求给出区块链的框架；实施时考虑搭建区块链的现实因素。在信息系统应用中，区块链的影响主要表现在两方面：一是节约人力成本，促进资源共享、简化信任背书、精简执行流程；二是带来新的问题，如信息安全问题、时空效率问题、耗能问题。

在撰写区块链对信息系统应用的影响时，主观判断较强，缺乏具有权威性的宏观统计数据支持（如中国范围内银行系统中高级信息系统的区块链技术覆盖率等），具体情况有待相关部门的进一步公布。

区块链的诞生为信息系统带来了机遇，同时也带来了挑战。在将区块链技术融合到信息系统当中时，政府应建立健全区块链在信息系统开发应用中的相关制度，各个行业应加快建立行业内联盟和跨界联合的相关机制，区块链从业者应增强相应的安全意识和规范意识。

7 参考文献

[1]Nakamoto S．Bitcoin: A peer-to-peer electronic cash system［EB/OL］.［2017-11-23］. https: // bitcoin.org/bitcoin.pdf.
[2]Swan M. Blockchain thinking: the brain as a decentralized autonomous corporation. IEEE Technology and Society Magazine, 2015, 34(4): 41−52.
[3]黄俊飞,刘杰.区块链技术研究综述[J].北京邮电大学学报,2018,41(02):1-8.
[4]傅晓阳.区块链技术应用探索[J].中国金融,2018(02):73-74.
[5]Lazarovich A． Invisible ink: blockchain for data privacy ［D］. Massachusetts: Massachusetts Institute of Technology，2015: 36-40.
[6]袁勇,王飞跃.区块链技术发展现状与展望.自动化学报, 2016, 42(4): 481−494.
[7]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(01):206-225.
[8]叶聪聪,李国强,蔡鸿明,顾永跟.区块链的安全检测模型.软件学报,2018,29(5):13481359. http://www.jos.org. cn/1000-9825/5500.htm.
[9]赵刚.区块链技术的本质与未来应用趋势[J].人民论坛·学术前沿,2018(12):61-69.
[10]左美云.信息系统开发与管理教程[M].北京：清华大学出版社，2013：7-10.
[11]王毛路,陆静怡.区块链技术及其在政府治理中的应用研究[J].电子政务,2018(02):2-14.
[12]Dongchang Zhao, Guorui Jia, Huanhuan Ren, Chuan Chen, Rujie Yu, Peng Ge and Shaohui Liu. Research on the Application of Block Chain in automobile industry [C], 2018 IOP Conf. Ser.: Mater. Sci. Eng. 452 032076.
[13]景宏文.论区块链技术对商业活动效率的提升[J].纳税,2017(15):102+104.