区块链技术在政府部门的应用综述

任 明[1] 汤红波[1] 斯雪明[2] 游 伟[1]
(国家数字交换系统工程技术研究中心 郑州 450001)[1]
(数学工程与先进计算国家重点实验室 郑州 450001)[2]

摘 要 随着比特币价值的不断攀升,其背后使用的区块链技术在全球范围内迅速引起了各个行业的广泛关注,同时也引起了各国政府的高度重视。特别是以美国为代表的一些国家在政府和权力机构的支持下,已经开始尝试将此项技术应用于专用信息平台建设、装备物资运转和系统控制等多个方面,认为此项技术的分布式、可追溯、不易篡改等特性能够在匿名数据的收集、数据的完整性校验、智能设备的互联通信等多个方面发挥重要作用。同时,目前也有不少国家政府机构对区块链技术的应用仍然保持谨慎的态度,认为此项技术仍然面临着安全保密、应用的通用性等诸多问题。通过介绍和分析政府部门中区块链技术的应用情况,指出目前该项技术在政府部门应用的过程中面临的挑战。最后,针对这些问题,并结合现在学术界已有的工作提出相应的解决方案。

关键词 区块链,非金融应用,政府应用,安全,挑战
中图法分类号 TP393 **文献标识码** A **DOI** 10.11896/j.issn.1002-137X.2018.02.001

Survey of Applications Based on Blockchain in Government Department

REN Ming[1] TANG Hong-bo[1] SI Xue-ming[2] YOU Wei[1]
(China National Digital Switching System Engineering and Technological R&D Center, Zhengzhou 450001, China)[1]
(State Key Laboratory of Mathematical Engineering and Advanced Computing, Zhengzhou 450001, China)[2]

Abstract As the value of Bitcoin continuously rises, the blockchain technology applied behind it has promptly drawn widespread attention throughout the world, and it has also attracted the attention of governments at the same time. In particular, some countries, represented by the United States, under the support of the governments and the power institutions, have begun to try to apply this technology in various aspects, including the construction of specific information platforms, the operation of equipment supplies, and the control of systems. They think that the features including distribution, traceability and difficult tampering, etc of this technology could give full play to advantages of many aspects such as anonymous data collection, data integrity verification, interconnected communication of intelligent equipments, etc. In the meantime, the government institutions of many countries still maintain a cautious attitude towards the application of blockchain technology and they think that this technology is still faced with lots of problems including security and the universality of application, etc. Through the introduction and analysis of applications of the blockchain technology of government departments, the challenges confronted by current blockchain technology in the applications of government departments were pointed out. Lastly, for these problems, corresponding solutions were brought forward through combing the existing work in the academic field.

Keywords Blockchain, Non-financial applications, Applications in government department, Security, Challenges

1 引言

随着比特币[1]的价格在交易市场的持续上涨,区块链[2]作为其支撑技术,逐渐吸引了大量国内外学者和企业商人的关注,其应用从最初的单纯的数字货币应用[3]迅速扩展至银行[4]、医疗、保险、版权存证、共享经济、物联网[5]、大数据等诸多领域。不论是在国内还是国外,区块链都已经有了“落地”的应用尝试。区块链技术本身也以其特有的分布式[6]、可追溯[7-8]和不易篡改[9-11]等性质,为不同组织、机构和部门在非信任环境下达成共识[12-13]以及建立起可信数据库提供了可行方案。面对市场上的这项新兴技术,各国政府显然不会无视它的发展。目前,以美国为首的科技强国已经开始在政府

到稿日期:2017-12-04 返修日期:2018-01-10 本文受东南大学移动国家重点实验室开放研究基金资助课题(2013D09)资助。
任 明(1990-),男,硕士生,CCF会员,主要研究方向为区块链技术的应用、区块链系统性能优化,E-mail:mu571@sina.com;汤红波(1968-),男,教授,博士生导师,主要研究方向为移动通信网络、新型网络体系结构,E-mail:thb@ndsc.com.cn(通信作者);斯雪明(1966-),男,教授,博士生导师,CCF会员,主要研究方向为密码学、数据科学、计算机体系结构、网络安全、区块链;游 伟(1984-),男,博士,讲师,主要研究方向为密码学及5G网络安全。

和权力机构中尝试应用区块链技术,其中的一些案例已经有所进展。与此同时,仍然有部分国家对这项技术可能存在的安全问题持谨慎态度。

本文结合区块链的技术特征,对非金融领域(特别是目前政府部门已经开始实施的应用情况)进行了分析,并探讨了未来可能的技术发展方向。

2 非金融领域应用中的区块链技术

区块链技术最早出现于比特币——一种 P2P 架构下的数字加密货币[14]。随着比特币和其他数字货币的不断发展,专家学者和企业商人都不再满足于仅将这项技术应用于银行和金融行业[15],人们发现区块链可以在数据存证和数据完整性校验等方面提供有效的解决方案[16]。目前,无论是在物联网领域,还是在公证、医疗、房地产领域[17],均存在着很多的中介机构,其中高昂的中介成本和信息安全隐患都驱使企业尝试在他们的应用产品中使用区块链技术。下面结合 3 个比较典型的场景案例进行说明。

(1)物联网

物联网将网络身份赋予实际物体。现在,手机和电脑已经可以通过网络进行互联;而在未来,汽车、房屋、电器也都可能会加入到网络中,它们将能够被远程操控。例如,当出现电力紧张或者电流过高时,通过使用区块链技术中的智能合约,可以自动实现网络中电器节电模式的启动或者不同电器的交替使用[18]。区块链可以解决阻碍物联网发展的成本和诚信问题。对于物联网公司来说,开发专用的智能设备会花费巨额成本,区块链技术可以取代云和服务器的集群,使物联网能够将基础设施的建设外包给成本较低区域的企业;同时,通过智能合约的调用,网络上产生的交易或者事物处理信息可以根据用户之间提前约定好并写入区块链网络的内容自动执行,而无须在事件发生后担心反悔、抵赖和篡改信息等情况的出现,从而解决了不同用户和智能设备之间的信任问题[19]。

(2)数据存证

Everledger 是一家从事区块链技术的初创公司,其主要业务是使用区块链技术的可溯源特性对钻石进行检测和认证。通过钻石的切割面、颜色、克拉数、证书编号等几十个数字指纹的记录,对从矿石开采到钻石的加工再到商家与消费者之间的交易这一系列过程进行数据的存证,其目的是解决钻石检测中的冲突和保险欺诈行为。区块链技术能够用于数据存证这一特点已经得到了业内的广泛认可。但是在实际的应用中,目前只有钻石和保险的相关应用得到了推广,这是由所需认证数据的价值决定的。因此,在结合不同行业的应用时,需要重点考虑认证的成本问题。

这种存证方式同样适用于供应链场景。与钻石的认证一样,针对某些特定产品,可以对它们的技术研发、原料来源、生产过程、仓库存储、物流信息等多个方面的数据进行存证,从而能够有效防止这些产品的信息在整个生命周期内被恶意篡改,并且可以追溯源头,对可能出现的产品质量、操作失误等问题留存证据。

(3)医疗记录

目前,在医疗方面,区块链技术主要用于保存个人的医疗信息,即在区块链上为患者建立起电子病历。此举旨在使病人能够掌握自己的医疗记录和患病历史,而不是简单将这些信息分别存储在各个单独的医院内。医院在面对病人时,也可以从区块链网络上获取到该患者的详细病史记录,从而更加全面地了解对方的情况,做出更加准确的诊断。在这一过程中,由于病人信息具有一定的隐私性[20],一些公司在产品的设计过程中会进行加密处理,通过生成数字指纹的方式防止医疗数据被泄露给第三方的无关人员。

3 区块链技术在政府部门应用中的优势

比特币在诞生和发展的过程中借鉴了密码学[12,21]、分布式系统、博弈论等多个领域的技术,其中起核心支撑作用的区块链技术也可以被看作是对这些技术的整合与综合运用。区块链的本质是一个透明、可追溯、不易篡改的分布式账本数据库,其在设计上普遍采用了较为成熟的密码学算法[22-23],以保证其安全防护性能。对于各国的政府部门来说,安全保障是一切技术手段、执行政务和各项工作正常运转的基础条件之一。通信安全、数据安全、信息安全,包括密码安全,都是其中的典型代表。而使用区块链的一个重要原因是,这项技术能够使位于全球范围内不同地区的节点在非信任的环境下建立起有效的共识机制[24-27],使诚实节点之间达成一致,并为可能存在的伪造信息提供溯源依据,从而使网络上的数据和信息可信、可靠。区块链技术以其分布式的结构,通过全网节点的共同参与维护、共同记录存储数据的方式,可以有效应对传统数据库由于完全中心化管理带来的安全风险。同时,在数据的完整性保护和可靠性提升方面,区块链技术的出现可以为新时代、信息化社会环境下的可靠数据传输和存储[28-29]带来新的、更好的解决方案[30-31]。

4 美国政府对区块链技术的应用

美国政府在科学技术的发展方面一直对新技术的开发及应用表现出足够的兴趣。区块链作为一项新兴的热门技术,出现后随即引起了美国政府的高度重视。当地时间 2017 年 9 月 19 日,美国参议院通过了一项给美国提供 7000 亿美元资金的国防开支计划,这其中就包含了一项涉及国防部从事区块链研究任务的修正案,其研究工作被描述为“一份关于区块链技术和其他分布式数据库技术的潜在进攻和防御的网络应用,以及一项针对国外力量、极端组织以及犯罪网络利用这些技术的研究报告评估”[32],其目的是更好地保护网络安全。虽然从提案到该项研究任务被正式开始执行仍有很多工作要完成,但是不难看出,美国政府和其涉及的权力机构在区块链技术方面的研究工作已经开始向实际应用转化。

4.1 特殊信息的收集

2015 年,美国反腐反恐技术支持办事处 CTTSO 在其官方文件 Bid3692 中明确提到了区块链技术,认为其能够改善美国政府收集信息的方式。而当时令美国官方感兴趣的正是区块链技术所拥有的匿名性特征。区块链采用数字加密手段,对包括使用者身份信息在内的多种数据进行了信息隐藏,使得安全的匿名通信成为可能。特别是在比特币网络[33]中,美国政府利用交易双方身份的匿名性,通过使用比特币激励

的方式,对情报提供者予以奖励。虽然这种方式属于对区块链技术较为基础的应用,但是由于比特币用户账号的生成无须认证,一个用户随时可以拥有多个无直接关联的账号,并且通过账号并不能对用户的真实身份信息进行核查,信息的提供者不受地域、国别等属性的限制,可以在任何时间、任何地点通过为美国政府提供其所需信息得到比特币奖励,而不用担心身份或者行踪被其他国家的政府或军队锁定而暴露目标。因此,美国政府可以通过以美元换取比特币的方式,利用比特币这一平台向提供特殊信息的人员支付奖励资金;而信息的提供者在获得奖励资金之后可以再兑换成所在地区的法定货币。使用比特币作为信息交易的支付中介和激励载体,可以让获取信息资金的流转过程难以被溯源,从而有效地保护了美国政府情报机构的身份信息和人员的安全。但是,区块链这种匿名特性在保护用户信息的隐私与安全的同时,也为非法行为提供了便利。例如,暗网中知名的"丝绸之路"与"阿尔法湾"等交易平台就是利用比特币或其他数字加密货币在网络中交易双方拥有的身份匿名性特征,进行军火走私、毒品交易、奴隶买卖等一系列非法活动。有力打击这些非法性质的活动,反向追踪对手的真实身份信息,同样也是包括美国在内的各国政府与世界维和组织需要面对的重大考验之一。

4.2　基于区块链技术的信息平台

据报道[34],2017 年 5 月 25 日,美国印第安纳科技与制造公司(ITAMCO)宣布其已经获得美国国防高级研究计划局(DARPA)的第一期资金,该资金被用来为美国国防部(DoD)创建一个使用超级账本区块链协议的通信平台。该平台将会在 ITAMCO 现有的使用了 256 位 AES 加密协议的加密聊天应用(Crypto-Chat application)的基础上,结合区块链技术,提升现有平台的工作效率、鲁棒性与安全性。按照设计,通信平台将基于分布式的基础架构,使用 P2P 的通信方式和端到端的加密模式,允许来自任何地方的用户传送安全信息或者处理来自多个分布式数据库通道的通信信息,即提供跨多个通道的安全保护机制。平台的用户可以通过应用程序将信息的创建与信息的收发分离,利用平台上分布式的可执行合约代码进行通信。该公司的研究和开发总监 Joel Neidig 相信,该平台可以有效地促进美国情报人员与五角大楼之间的信息传递以及各分散单位与总部之间的沟通。这项计划分为 3 个阶段进行:第一阶段以小型企业创新研究计划(SBIR)的方式进行,该计划通过竞争的形式鼓励美国国内小型企业从事联邦项目的研究与开发工作。2017 年 5 月初,美国国土安全部公布,他们向 13 家小型企业提供了 970 万美元的资金支持,用以奖励他们在区块链等技术方面的创新。第二阶段预计在 2018 年中期开始,包括平台程序的开发、测试和对原型机的评估工作。第三阶段包括应用平台功能的完全实现和商业化应用。

随着区块链技术越来越受到关注,使用该技术进行安全防御的方式也在逐步增加。美国政府此举是希望借助区块链技术的防篡改特性与其使用的数字加密技术,为指挥系统与一线工作人员之间的信息交互提供更为安全、可靠的平台,并确保人员之间通信信息的准确性。

4.3　关键系统控制

美国国防部的国防高级研究计划局已经开始借助区块链技术来确保关键系统信息的完整性,并将尝试创建更多的信息服务。

信息的完整性是区块链技术吸引美国政府机构注意力的一个重要方面。信息的完整性是指,数据被访问时不会被访问者修改或篡改,不会由于系统错误或第三方的干扰而被损坏。

在数字化环境中,信息都是以电子数据的形式存储的,对于企业和政府机构,特别是美国在全球范围内的武装行动而言,数据安全和信息的存储是至关重要的。DARPA 的目标是通过使用基于区块链技术的新系统来提升数据的完整性保障,并防止机密数据和信息遭受黑客的入侵和破坏。这种考虑同时也是 4.2 节中信息平台构建的基础之一。

2016 年 9 月,DARPA 向 IT 安全公司 Galois 和从事区块链安全技术的 Guardtime 公司提供了一份价值 180 万美元的合同,用来建立一个基于区块链的数据完整性监控系统。其中,Galois 公司被认为是形式验证(Formal Verification)行业的领导者,该公司提供了证明系统在所有情况下都能够按照预期方式工作的相关技术,该技术不仅进行测试和评估,而且使用了数学的方式进行验证;Guardtime 创建了无钥签名基础设施(KSI),该系统旨在为电子数据、设备和人员提供可扩展的基于数字签名的身份验证。Guardtime 的基础设施已经被用于保护爱沙尼亚的 IT 系统和英国能源基础设施的安全。使用基于区块链的技术,可以有效保证高敏感数据的可靠性与完整性。美国政府希望通过部署该系统,有效防止任何针对重点数据库和设备的窃听、破坏事件。DARPA 的区块链项目经理 Timothy Boother 曾经表示[35],美国无论在什么时候使用武器装备,数据的完整性都非常重要。这其中包括了对核武器以及卫星的指挥与控制。

5　其他国家政府对区块链技术的应用

作为世界超级大国,美国对区块链技术的关注度很大程度地影响到了其他相关国家。事实上,其他国家在政府机构对区块链技术的应用方面既有相似之处,也有不同方面的考虑。从目前已有的信息来看,同样在世界范围内具有巨大影响力的俄罗斯在区块链技术的发展方面相对保守,对此项技术的应用尚在起步阶段。

5.1　北约——网络防御平台及通用化应用

DARPA 并不是唯一正在尝试寻求利用区块链技术解决问题的政府组织,北大西洋公约组织(NATO)也在计划实施基于此项技术的解决方案。北约曾在 2016 年 4 月宣布当年的重点创新目标是要加速转型,寻求最先进的技术解决方案以支持北约包括指挥、控制、通信、计算机、情报、监视与侦察在内的 C^4ISR 系统[36]以及其他方面对网络能力的需求。除此之外,北约各成员国也在寻求更多领域的通用化应用,例如物流、采购以及财务等。

在北约组织内的装备管理与物流方面,智能化与数据的安全保障是重点问题。不论是装备设施还是后勤物资,从研究测试、工厂生产到交付使用、退役报废的整个生命周期内,

不仅要对生产厂商、使用单位、存储状况等基础信息进行记录备案，还要对装备研发过程中的设计方案、测试结果等技术信息与物资在运转过程中的使用情况等相关数据进行安全、可追溯的存储。传统的纸质及电子介质在装备移交、物流网络通信、系统维护等多个方面难以实现有效的数据安全保障，缺乏有效的监管措施，系统的运行效率不易得到保证。通过引入区块链技术，可以实现多方共同参与和维护的分布式、可追溯、可控可监管的数据网络系统，使装备设施管理、后勤物资调配等诸多方面的数据更加安全、可靠；通过使用这项技术，可以使信息之间的交互与调用更加灵活，数据在传输过程中即可进行智能认证，从而有效地确保系统的高效运行，提升数据使用的便捷性。此项技术同样可以应用于政府部门人员的档案管理工作，通过区块链技术记录工作人员的任职履历，形成多方共同存储、共同维护的电子人力资源档案，以技术手段解决目前普遍存在的人员信息繁琐、复杂的弊端，并且可以消除伪造人员信息的情况。

5.2 澳大利亚——基于区块链的物联网系统

澳大利亚虽然不是北约的成员国，但其在政治、经济与军事发展上与美国休戚相关，特别是在军事技术与装备发展方面与美国关系密切。2017 年 6 月，装有宙斯盾级 Aegis 监控系统的霍巴特级导弹驱逐舰在阿德莱德被交付给澳大利亚政府，标志着澳大利亚海军进入了电子战时代。澳大利亚希望更好地将陆地车辆、海军舰艇、飞机等武装力量连接起来，形成智能互联的物联网系统，实现从获取敌方信息到作出反应并展开行动的流程自动化。这其中就引入了区块链技术。相比于美国对这项新兴技术的信任，澳大利亚政府部门则表现出更多关于安全性的担忧。全球知名的武器装备供应商洛克希德马丁公司已经宣布将区块链技术的特征集成到其数据系统中，用以应对网络和武器操作系统中可能会遇到的威胁[37]。此举与美国相似。事实上，洛克希德马丁公司也与 Guardtime 公司签订了合同来开发新的安全系统，成为了第一家与美国政府合作并将区块链技术纳入其发展范围的军事技术承包商。澳大利亚政府对基于区块链技术的安全系统可能存在的网络安全漏洞问题表示担心。这是因为洛克希德马丁公司的系统长期以来一直在为澳大利亚的防空驱逐舰和空军基地的维护设施提供服务，此次该公司引入的区块链技术令澳大利亚政府部门持谨慎态度。

5.3 俄罗斯——引入加密算法

俄罗斯在区块链技术的应用方面处于落后地位。该国政府与澳大利亚政府一样，在对新技术的应用方面持谨慎态度，国防机构内的保守观点使得这项新兴技术无法在短期内迅速被引入。俄罗斯 Voentelecom 公司的 CEO 亚历山大·达维多夫透露，只有在将俄罗斯加密算法引入区块链技术并能够确保该技术的全面安全性之后，俄罗斯才会在民营和国家机构中使用这项技术，并在未来将其应用到俄罗斯国防力量上，而这个过程可能将耗时 7～10 年。Voentelecom 是俄罗斯的一家电信公司，主要向俄罗斯政府机关、管理部门和权力机构提供通信服务。由此可见，俄罗斯虽然短期内不会在政府部门的应用中引入区块链技术，但是未来很有可能会在该项技术应用中通过使用自己的加密算法来提升加密等级，确保通信与数据算法的安全性。

6 区块链技术在政府部门应用中面临的问题

区块链技术的发展速度较快，国内外的不少组织机构、学者以及企业都在对它进行研究和开发利用，这也从客观上说明了其价值已经得到了各行各业的广泛认可。但是不可否认的是，此项技术的发展并不成熟[38]，仍然有很多问题有待解决[39-40]，特别是在与不同领域的应用相结合的过程中。针对不同行业的特点，区块链技术仍然面临着许多问题，在实现其技术运用的过程中还存在不少挑战[41]。本节将结合区块链技术在政府部门中应用时所面临的 3 个问题作具体说明。

(1)安全保密

世界顶级安全专家、世界级黑客 Benjamin Kunz Mejri 在 2017 中国互联网安全大会上曾经说过“没有攻不破的系统”，任何技术的安全性都是相对的。区块链技术在政府部门办公应用体系中应用的场景多为核心、涉密程度较高的环境，一旦出现安全漏洞，将造成重要信息和数据资料的泄露，后果不堪设想。因此，安全问题是政府部门应用方面需要解决的首要问题。这里的安全问题既包括区块链技术可以应用的对象，也包括此项技术本身[42]。

区块链技术包含共识机制、加密算法、智能合约和分布式系统等多个模块的内容，系统的正常运转需要对各个模块进行合理、高效的组合运用。因此，区块链的安全问题既有可能来自他国政府的主动攻击，也有可能来自系统内部设计[43]所存在的缺陷。例如，不完善的加密算法可能带来安全漏洞[44]，不恰当的共识机制可能会造成关键时刻出现系统崩溃的现象。由于在应用中采用了分布式架构，任何参与者都可以在任何地点对区块链上的数据进行监听和读取，因此可能会造成秘密信息的泄露；也有可能会由于网络上存在恶意节点而导致数据被破坏或者存在伪造的信息在网络上传播。

另外，对区块链技术在被正式引入政府办公系统之前的保密性评估与认证，目前还没有专门的机构负责，在应用的性能测试方面还缺乏明确的标准和依据。虽然美国国防部与 Galois 公司在信息平台的开发过程中进行了合作，但目前仅是部分授权，仍然缺少权威机构或组织专门对此类事务进行有效监管。因此，由于行业的特殊性，在目前的条件下，政府部门和一些特殊行业的区块链技术应用还很难大规模地推广。

(2)通用型应用与特殊性应用相结合

在金融、数据存证等领域，目前已经开发出了不少区块链技术的商用产品，政府机构内的开发者和使用者在开发具有行业特色的特殊性应用时，也应该关注技术相对成熟、通用性较强的产品。

国际上较大的区块链开源社区包括以太坊[45]和超级账本[46-47]项目等，不少金融、证券行业的区块链应用[38,48]都是由它们衍生出来的，并且已经有了不少成功的案例。如果能够将这些发展较为成熟的应用与政府工作的特点相结合，将会在应用的开发过程中有效节约成本和时间，并且能够在应用的稳定性方面得到一定的保障[49-50]。目前，通用型应用与政府办公特殊性应用相结合的相关工作开展得并不顺利。各

国政府和权力机构在与企业合作的过程中往往会选择之前有过合作的大型公司,而对中小型创业公司的产品缺乏信任,甚至是直接忽视了它们的存在。因此,一些更加新颖、更具创造力的应用设计通常很难得到足够的重视;而且现在还缺少适当的机制和评价体系对创业公司的产品进行全方面的评估,那些运行同样稳定且性能可能更加优良的应用产品很难被发现。换句话说,当前已有的政府与企业的合作模式还较为单一,无法完全做到择优选用。

(3)大文件数据的存储

目前,区块链作为账本数据库,存储的数据类型多为文本,单个文件的数据量都不是很大。随着技术的不断发展,政府机构在办公中使用的文件资料格式也在发生改变,不仅仅局限于文本数据,未来更多的可能是以视频材料为代表的多媒体资源,但这些文件通常所占存储空间较大,在目前的区块链系统结构下很难完成存储。例如,以太坊虽然在理论上可以进行视频文件的存储,但因为要涉及将文件分段并分别计算哈希值,随之产生的数据量也相对较大,费用成本高昂,所以目前其只能作为技术手段的验证,并不适合大规模应用。

7　对未来应用的思考

随着区块链技术在世界范围商用领域的迅速发展,应用案例也在逐步增多。但是,如上文所述,其自身发展尚不完善,还有不少可以改进的方面,特别是在与特殊领域相结合的过程中,必须要考虑到行业的特殊性,做出与之相适应的优化。针对目前区块链技术在与政府工作事务相结合的过程中所面临的问题,在此探讨未来可以改进的方向。

(1)在政府部门和一些特殊行业中,有必要在使用区块链技术的同时采取访问权限控制和网络信息监管等措施。可以对区块链采用数据访问权限分级和通信信息的实时监控,这一点在前文提到的美国政府部门设计的信息平台中有所涉及。他们通过信息生成与信息传输相分离的方式,可以在发现伪造信息之后对信息来源进行有效追溯,并随即采取相应的打击措施;而安全信息并不会受到影响,可以在网络中正常传输,从而避免了可能发生的通信冲突。未来可以结合不同的系统,针对不同级别的领导机构获取信息的权力与必要性[51],对链上的数据进行分级管理与存储,通过零知识证明等方式,使链上记录的数据只对相关人员可见,从而加强对重点信息的保护,提升数据与系统的安全性。同时,在应用部署之前,开发人员也应当对系统进行足够长时间的性能测试与漏洞检查,从而将内部问题可能造成的系统风险降到最低。

需要说明的是,采取访问控制等手段并不违背区块链技术本身的使用初衷。区块链的透明性特征在政府机构和部分有特殊职能的行业应用中并不具备优势,反而会带来不必要的安全隐患,可追溯性特征也是如此。在这些领域内,并不是所有的信息都需要或者被允许溯源,对于机密性较强的信息,即使记录在案,政府部门和权力机构仍然不希望网络中不相关的人员进行查看或者修改。因此,对数据进行分层存储与访问权限的分级管理,也可能会成为区块链技术在这些特殊领域应用的特点之一。

(2)区块链技术的应用离不开各国政府和权威机构的支持与配合。不同于其他行业,权威性在包括政府部门在内的一些领域中必不可少,大部分的工作都需要得到高级部门或者机构的批准与授权。在此前提下,通用性较强的应用完全可以借鉴商业领域的成功案例,在完善安全防御措施及提升安全等级的前提下对已有的应用案例做适当程度的修改,这样不仅能够减少重复开发造成的资源与时间的浪费,而且能够保证系统的稳定性。同时,美国国防部对中小型企业提供资金支持与奖励的做法值得其他国家借鉴,此举有助于提升技术应用的创新性。通过与商业公司合作的方式,能够加速重点课题的研究进度,早日实现不同行业对区块链技术的实例化应用。

目前还存在一些未得到实例验证的技术[52](如跨链技术[53])包括以太坊、超级账本项目等区块链技术大型研究社区在内的不少组织、机构和公司都在对其进行研究,并分别提出了各自的解决方案的架构设计。在政府部门的应用中,从当前已有的设计来看,跨链技术的实现是未来区块链在该领域发展运用过程中必须要解决的问题之一。在北约国家试图建立的装备设施与物资管理系统中,跨链技术可以很好地满足不同性质部门和机构之间的通信需求,甚至可以满足物联网之间的通信需求。而在信息化的时代背景下,智能设备将被越来越多地引入反恐维和等武装行动中,其背后需要可靠的通信手段作为保障。因此,在电子信息干扰的环境下,上级机构能够通过远程管理等手段准确无误地掌握下级动向并传达命令,能够使己方人员的智能设备之间保持安全通信,将成为未来完成政府部门任务的基础保证之一。在信息交互中引入区块链跨链技术,很有可能对现在已有的安全防御系统带来强烈的冲击。不仅如此,鉴于在政府部门中安全性占据着重要地位,特别是在核心机密数据保护方面,各个国家都在加密方式上投入了大量的人力与物力,俄罗斯等国家更是开发了自己的国家加密算法以应对可能出现的黑客攻击。而区块链技术对于数据的保护作用已经基本得到了验证,随着它的加入,很可能出现新一轮的安全防御与攻击问题。如何应对这些伴随着新兴技术而来的安全问题,也需要各国政府与军事化武装力量进行认真的考虑与解决。

(3)在大文件数据的存储方面,已经有人提出使用 IPFS (Inter Planetary File System)[54]。这是一项针对 HTTP 协议的改进方案。按照 HTTP 协议,当对某台服务器上的某个文件进行查找时,首先要查找的是存放文件服务器的 IP 地址,然后再通过服务器去访问文件所在的路径;而 IPFS 查找的是文件的内容。在 IPFS 网络中,每个节点都有唯一的哈希指纹,每个文件也有一个唯一的哈希指纹,文件被切割成多个小块后再存储于节点哈希值与文件哈希值最相近的多个节点上。查找文件时,通过文件的哈希值在节点网络中逐级询问,直到最终找到存储文件的节点。相比于泛洪算法,这种方式可以有效避免网络信息的阻塞。由于区块链需要全网范围内的共识,通常情况下系统吞吐量会受到限制,因此其不太适合

存储较大的文件。同为 P2P 网络结构的 IPFS 网络，可以为区块链系统解决文件存储问题提供参考方案。在实际应用中，可以在区块链上存储文件的哈希值，用户可以通过使用客户端在对文件的哈希值进行查找之后，再利用 IPFS 网络获取目的文件。

结束语 区块链技术以其分布式、可追溯、不易篡改等特性引起了各国政府的广泛关注。以美国政府为代表的世界科技强国已经在实践中有了许多区块链技术方面的尝试，但同时也面临着很多随之而来的问题，其中包括安全保密问题、政商合作与监管问题等。各国政府在引入区块链技术的同时，也在尝试解决它带来的新的技术挑战。通过目前已有的尝试可以看出，区块链技术在政府部门和一些特殊领域有着广阔的应用空间与巨大的发展潜力，其未来的发展需要政府部门在增加支持与配合力度的同时，对区块链技术进行具有行业特色的改进，同时对商业应用领域较为成熟的技术进行透彻分析并加以利用，以提升具有行业特色应用的安全性与稳定性。

参 考 文 献

[1] ANTONOPOULOS A M. Mastering Bitcoin[M]. USA:O'Reilly Media,2014.

[2] Wikipedia. Blockchain (database) [EB/OL]. [2017-10-3]. https://en. wikipedia. org/wiki/ Blockchain_(database).

[3] GERVAIS A,RITZDORF H,KARAME G O,et al. Tampering with the Delivery of Blocks and Transactions in Bitcoin[C]// ACM Sigsac Conference on Computer and Communications Security. New York:ACM,2015:692-705.

[4] PORRU S,PINNA A,MARCHESI M,et al. Blockchain-Oriented Software Engineering:Challenges and New Directions [C]// International Conference on Software Engineering Companion. Piscataway,NJ:IEEE Press,2017:169-171.

[5] CHRISTIDIS K,DEVETSIKIOTIS M. Blockchains and Smart Contracts for the Internet of Things[J]. IEEE Access,2016,4:2292-2303.

[6] KYPRIOTAKI K N,ZAMANI E D,GIAGLIS G M. From Bitcoin to Decentralized Autonomous Corporations: Extending the Application Scope of Decentralized Peer-to-Peer Networks and Blockchains [C]// Proceedings of the 17th International Conference on Enterprise Information Systems(ICEIS2015). Barcelona,2015:284-290.

[7] NEISSE R,STERI G,NAI-FOVINO I. A Blockchain-based Approach for Data Accountability and Provenance Tracking[EB/OL]. [2017-6-14]. https://arxiv. org/ abs/1706. 04507.

[8] SZYDLO M. Merkle Tree Traversal in Log Space and Time[J]. Lecture Notes in Computer Science,2004,3027:541-554.

[9] WOLRICH G M,YAP K S,GUILFORD J D,et al. Instruction set for message scheduling of SHA256 algorithm:US8838997B2 [P]. 2012-09-28.

[10] HABER S,STORNETTA W S. How to time-stamp a digital document [J]. Journal of Cryptology,1991,3(2):99-111.

[11] BAYER D,HABER D,STORNETTA W S. Improving the Efficiency and Reliability of Digital Time-Stamping [M]// Sequences II:Methods in Communication,Security,and Computer Science. New York:Springer. 1993:329-334.

[12] 杨保华，陈昌. 区块链原理、设计与应用[M]. 北京：机械工业出版社，2017：34-62.

[13] KRAFT D. Difficulty control for blockchain-based consensus systems[J]. Peer-to-Peer Networking and Applications,2016,9(2):397-413.

[14] NAKAMOTO S. Bitcoin:A Peer-to-Peer Electronic Cash System[EB/OL]. [2008-11-1]. https:// bitcoin. org/bitcoin. pdf.

[15] R3. About R3[OL]. http://www. r3cev. com/about.

[16] ZYSKIND G,NATHAN O,PENTLAND A S. Decentralizing Privacy:Using Blockchain to Protect Personal Data[C]// Proceedings of the 2015 IEEE Security and Privacy Workshops (SPW 2015). San Jose,CA:IEEE,2015:180-184.

[17] SWAN M. Blockchain Thinking:The Brain as a Decentralized Autonomous Corporation [J]. IEEE Technology and Society Magazine,2015,34(4):41-52.

[18] BOGNER A,CHANSON M,MEEUW A. A Decentralised Sharing App running a Smart Contract on the Ethereum Blockchain [C]// Proceeding of ACM International Conference on the Internet of Things. New York:ACM,2016:177-178.

[19] KIM K J,HONG S P. Study on Rule-based Data Protection System Using Blockchain in P2P Distributed Networks[J]. International Journal of Security and Its Applications,2016,11(10):201-210.

[20] KOSBA A,MILLER A,SHI E,et al. Hawk: The blockchain model of cryptography and privacy-preserving smart contracts [C]// Symposium on Security and Privacy. New York: IEEE Computer Society,2016:839-858.

[21] LAMPORT L. Time,Clocks,and the Ordering of Events in a Distributed System [J]. Communications of the ACM,1978,21(7):558-565.

[22] MERKLE R C. Protocols for Public Key Cryptosystems[C]// IEEE Symposium on Security and Privacy. New York: IEEE Computer Society,1980:122-133.

[23] MERKLE R C. A Digital Signature Based on a Conventional Encryption Function [C]// Conference on Advances in Cryptology-crypto,1987:369-378.

[24] PEASE M,SHOSTAK R,LAMPORT L. Reaching Agreement in the Presence of Faults[J]. Journal of the ACM,1980,27(2):228-234.

[25] FISCHER M J,LYNCH N A,PATERSON M S. Impossibility of Distributed Consensus with One Faulty Process[J]. Journal of the ACM,1985,32(2):374-382.

[26] CASTRO M,LISKOV B. Practical Byzantine Fault Tolerance [C]// Proceedings of the 3rd USENIX Symposium on Operating Systems Design and Implementation. Berkeley:USENIX Association,1999:173-186.

[27] VUKOLIC M. The Quest for Scalable Blockchain Fabric:Proof-of-Work vs. BFT Replication[C]// International Federation for Information Processing. New York:Springer International Pub-

lishing,2016:112-125.

[28] BAILIS P,FEKETE A,FRANKLIN M J,et al. Coordination Avoidance in Database Systems[J]. Proceedings of the VLDB Endowment,2014,8(3):185-196.

[29] WILKINSON S,BOSHEVSKI T,BRANDOFF J,et al. Storj:A Peer-to-Peer Cloud Storage Network(V0. 2)[EB/OL]. [2016-11-15]. https://storj. io/storj. pdf.

[30] HARI A,LAKSHMAN T V. The Internet Blockchain:A Distributed,Tamper-Resistant Transaction Framework for the Internet[C]// ACM Workshop on Hot Topics in Networks. New York:ACM,2016:204-210.

[31] CORBETT J C,DEAN J,EPSTEIN M,et al. Spanner:Google's globally-distributed database[C]// Usenix Conference on Operating Systems Design and Implementation. Berkeley: USENIX Association,2012:251-264.

[32] HIGGINS S. $700 Billion Senate Defense Bill Calls for Blockchain Cybersecurity Study[EB/OL]. [2017-9-19]. https://coindesk.com/700-billion-senate-defense-bill-calls-blockchain-cybersecurity-study.

[33] KOKORISKOGIAS E,JOVANOVIC P,GAILLY N,et al. Enhancing Bitcoin Security and Performance with Strong Consistency via Collective Signing[J]. Applied Methematical Modelling,2016,37(8):5723-5742.

[34] CUMMINGS D. Blockchain Messaging App Under Development For The US Military[EB/OL]. [2017-5-27]. https://www.ethnews. com/blockchain-messaging-app-under-development-for-the-us-military.

[35] RUUBEL M. Guardtime Federal and Galois Awarded DARPA Contract to Formally Verify Blockchain-Based Integrity Monitoring System[EB/OL]. [2016-9-13]. https://guardtime. com/blog/galois-and-guardtime-federal-awarded-1-8m-darpa-contract-to-formally-verify-blockchain-based-inte.

[36] Industry Relations. NCI Agency innovation challenge[EB/OL]. [2016-4-25]. https://www. ncia. nato. int/NewsRoom/Pages/160425_Innovation. aspx.

[37] NATOLI C,GRAMOLI V. The Balance Attack or Why Forkable Blockchains Are Ill-Suited for Consortium[C]// 47th Annual IEEE/IFIP International Conference on Dependable Systems and Networks (DSN). Denver:IEEE Press,2017:579-590.

[38] LI W T,SFORZIN A,FEDOROV S,et al. Towards Scalable and Private Industrial Blockchains[C]// ACM Workshop on Blockchain. New York:ACM,2017:9-14.

[39] EYAL I,SIRER E G. Majority is not Enough:Bitcoin Mining is Vulnerable[C]// Proceedings of 18th International Conference on Financial Cryptography and Data Security. Berlin: Springer,2014:436-454.

[40] LEWENBERG Y,SOMPOLINSKY Y,ZOHAR A. Inclusve Blockchain Protocols[J]. Financial Cryptography and Data Security,2015,8975:528-547.

[41] EYAL I,GENCER A E,SIRER E G,et al. Bitcoin-NG:A Scalable Blockchain Protocol[C]// Proceedings of the 13th USENIX Conference on Networked Systems Design and Implementation. Berkeley:USENIX Association,2016:45-59.

[42] KARAME G. On the Security and Scalability of Bitcoin's Blockchain[C]// 2016 ACM Sigsac Conference on Computer and Communications Security. New York:ACM,2016:1861-1862.

[43] GERVAIS A,KALAME G O,WUST K,et al. On the Security and Performance of Proof of Work Blockchains[C]// ACM Sigsac Conference on Computer and Communications Security. New York:ACM,2016:3-16.

[44] YUAN C,XU M X,SI X M. Research on a New Signature Scheme on Blockchain[J]. Security and Communication Networks,2017(2017):1-10.

[46] Welcome to Hyperledger Fabric[EB/OL]. (2017-10-15). https://hyperledger-fabric.readthedocs.io/en/release.

[45] BUTERIN V. Ethereum:A Next Generation Smart Contract and Decentralized Application Platform[EB/OL]. https://github. com/ethereum/wiki/wiki/White-Paper.

[47] HYPERLEDGER. About the Hyperledger Project[EB/OL]. https://hyperledger. org/about.

[48] HYPERLEDGER. Projects[EB/OL]. https://hyperledger. org/community/projects.

[49] DINH T T A,WANG J,CHEN G,et al. BLOCKBENCH:A Framework for Analyzing Private Blockchains[C]// 2017 ACM International Conference on Management of Data. New York:ACM,2017:1085-1100.

[50] COOPER B F,SILBERSTEIN A,TAM E,et al. Benchmarking cloud serving systems with YCSB[C]// ACM symposium on Cloud Computing. New York:ACM,2010:143-154.

[51] AI-BASSAM M. SCPKI:A Smart Contract-based PKI and Identity System[C]// ACM Workshop on Blockchain. New York:ACM,2017:35-40.

[52] BACK A,CORALLO M,DASHJR L,et al. Enabling blockchain innovations with pegged sidechains[EB/OL]. [2014-10-22]. http://blockstream. com/sidechains. pdf.

[53] WANG H,CEN Y,LI X. Blockchain Router:A Cross-Chain Communication Protocol[C]// International Conference on Informatics,Environment,Energy and Applications. New York:ACM,2017:94-97.

[54] BENET J. IPFS-Content Addressed,Versioned,P2P File System[EB/OL]. [2014-7-14]. https://ipfs. io/ipfs/QmR7GSQM93Cx5eAg6a6yRzNde1FQv7uL6X1o4k7zrJa3LX/ipfs. draft. pdf.