工程科学学报
Chinese Journal of Engineering

网络安全等级保护下的区块链评估方法

朱岩 张艺 王迪 秦博涵 郭倩 冯荣权 赵章界

Research on blockchain evaluation methods under the classified protection of cybersecurity

ZHU Yan, ZHANG Yi, WANG Di, QIN Bo-han, GUO Qian, FENG Rong-quan, ZHAO Zhang-jie

引用本文:
朱岩, 张艺, 王迪, 秦博涵, 郭倩, 冯荣权, 赵章界. 网络安全等级保护下的区块链评估方法[J]. 工程科学学报, 2020, 42(10): 1267-1285. doi: 10.13374/j.issn2095-9389.2019.12.17.007
ZHU Yan, ZHANG Yi, WANG Di, QIN Bo-han, GUO Qian, FENG Rong-quan, ZHAO Zhang-jie. Research on blockchain evaluation methods under the classified protection of cybersecurity[J]. *Chinese Journal of Engineering*, 2020, 42(10): 1267-1285. doi: 10.13374/j.issn2095-9389.2019.12.17.007

在线阅读 View online: https://doi.org/10.13374/j.issn2095-9389.2019.12.17.007

工程科学学报, 第 42 卷, 第 10 期: 1267−1285, 2020 年 10 月
Chinese Journal of Engineering, Vol. 42, No. 10: 1267−1285, October 2020
https://doi.org/10.13374/j.issn2095-9389.2019.12.17.007; http://cje.ustb.edu.cn

网络安全等级保护下的区块链评估方法

朱　岩[1)✉], 张　艺[1,2)], 王　迪[1)], 秦博涵[1)], 郭　倩[1)], 冯荣权[3)], 赵章界[4)]

1) 北京科技大学计算机与通信工程学院, 北京 100083　2) 中国科学院软件研究所, 北京 100190　3) 北京大学数学科学学院, 北京 100871
4) 北京信息安全测评中心, 北京 100101

✉通信作者, E-mail: zhuyan@ustb.edu.cn

摘　要　等级保护(简称等保)是我国信息安全的基本政策, 随着区块链技术在各行业中的应用日趋广泛, 有必要同步推进区块链系统的等级保护测评工作, 这将有利于推动该技术在我国的持续健康发展. 有鉴于此, 依据等保第三级的应用和数据安全要求, 给出了区块链系统中对等网络、分布式账本、共识机制和智能合约等核心技术的具体测评要求及实施方案, 并从等保 2.0 规定的控制点出发, 分别对当前区块链系统运行数据与基于日志流程的安全审计机制进行了归纳与分析. 通过上述评估与分析可知区块链系统在软件容错、资源控制和备份与恢复等方面满足等保要求, 而在安全审计、身份鉴别、数据完整性等方面则有待进一步改进.

关键词　区块链; 网络安全等级保护; 对等网络; 共识机制; 评估与分析

分类号　TP306

Research on blockchain evaluation methods under the classified protection of cybersecurity

ZHU Yan[1)✉], *ZHANG Yi*[1,2)], *WANG Di*[1)], *QIN Bo-han*[1)], *GUO Qian*[1)], *FENG Rong-quan*[3)], *ZHAO Zhang-jie*[4)]

1) School of Computer and Communication Engineering, University of Science and Technology Beijing, Beijing 100083, China
2) Institute of Software Chinese Academy of Sciences, Beijing 100190, China
3) School of Mathematics Sciences, Peking University, Beijing 100871, China
4) Beijing Information Security Test and Evaluation Center, Beijing 100101, China
✉ Corresponding author, E-mail: zhuyan@ustb.edu.cn

ABSTRACT　A blockchain is a cryptographic distributed database and network transaction accounting system. In the current era of major technological changes, blockchain technology, with its cryptographic structure, peer-to-peer (P2P) network, consensus mechanism, smart contract and other mechanisms, is decentralized, tamper-proof, and traceable and has become a hot spot in the development of informatization. Classified protection is one of the basic policies of information security in China. The implementation of the information security level protection system can not only guide various industries in performing security management in accordance with the equivalent security standards, but also ensure that supervision and evaluation institutions follow the laws and regulations, which is of significance to network security. As the application of blockchain technology in various industries is becoming more extensive, it is necessary to simultaneously promote the national classified protection of blockchain security assessment, which contributes to the sustainable and healthy development of blockchains in China. According to the revised assessment methods of grade protection, in addition to the status of universality requirements, evaluation specifications should be formulated for specific technologies and fields (such as cloud computing, mobile Internet, Internet of Things, industrial control, and big data). In view of the particularity of

收稿日期: 2019−12−17
基金项目: 国家科技部重点研发计划资助项目(2018YFB1402702); 国家自然科学基金资助项目(61972032); 北京市经济和信息化局资助项目(HTBH_20200901_573)

blockchain technology, China has initiated the formulation of blockchain evaluation specifications, but has not applied the level protection standards to the formulation of blockchain evaluation specifications. Therefore, the assessment requirements and enforcement proposals are specified for the blockchain's core technologies, such as P2P network, distributed ledger, consensus mechanism, and smart contracts, according to the application and data security layer requirements at Level 3. Moreover, the current running data of blockchains and their security audit mechanism based on the log workflow were summarized and analyzed respectively in compliance with the control points specified in classified protection 2.0. Our investigation indicates that blockchains can satisfy the requirements of evaluation items in three aspects, namely, software fault tolerance, resource control, and backup and recovery. However, further improvements are needed for other aspects, including security audit, access control, identification and authentication, and data integrity.

KEY WORDS blockchain; classified protection of cybersecurity; peer-to-peer network; consensus mechanism; assessment and analysis

区块链是一种密码学化的分布式数据库和网络交易记账系统, 可不依赖于可信第三方提供安全的电子交易服务[1]. 在当前科技重大变革的时代, 区块链技术凭借其密码化结构、P2P 网络、共识机制、智能合约等机制, 具有去中心化、防篡改、可追溯等特性, 成为当前信息化发展的热点. 区块链的应用已延伸到医疗[2]、版权[3]、法律[4]、媒体、资产管理[5] 等多个领域.

当前, 与互联网相连的计算机系统都有可能遭受来自世界范围的攻击, 这不仅会影响系统的正常使用, 甚至会影响信息化社会的稳定与国家安全. 我国信息安全等级保护[6](简称等保)制度的实施, 不仅能引导各行业按照等保标准进行安全管理, 还可以使监管、测评机构有法可依、有章可循, 对网络安全具有重要意义. 随着等级保护 2.0 时代[7] 的到来, 信息安全等级保护制度也正式更名网络安全等级保护制度[8]. 《中华人民共和国网络安全法》[9] 第二十一条、第三十一条规定我国实行网络安全等级保护制度, 国家对关键信息基础设施在网络安全等级保护的基础上实行重点保护.

区块链技术起源于国外, 在我国正处于发展阶段, 其测试评价工作也正在同步推进. 按照等级保护修订思路和方法, 除了具有普适性的通用要求外, 还应针对特定技术及领域(如云计算、移动互联、物联网、工业控制、大数据等)制定测评规范. 鉴于区块链技术的特殊性, 我国已经启动了区块链测评规范的制定工作, 例如, 中国区块链测评联盟出台了“区块链与分布式记账信息系统评估规范”. 然而, 上述工作并没有将等级保护标准应用于区块链测评规范制定中.

针对目前仍然鲜有参照等保 2.0 标准开展区块链测评研究的现状, 而国家关键信息基础设施的安全保护等级至少为第三级, 因此本文将以“等保三级”的应用和数据安全要求为依托, 以区块链功能组成为单元提出安全评估要求, 并结合具体区块链进行分析. 上述工作通过对区块链进行系统化的测评, 将有利于推动区块链技术在我国的持续健康发展.

1 等级保护概述

等级保护是我国关于信息安全的基本政策. 基本思想是对不同的保护对象分等级, 以便按照标准进行管理和监督. 等级保护工作在国外早已纷纷开展: 美国国防部 20 世纪 80 年代成立国家计算机安全中心, 90 年代公布的橘皮书带动了国际的安全评估工作; 随后, 欧洲借鉴橘皮书的经验, 公布了欧洲白皮书, 并首次提出信息安全的保密性、完整性、可用性, 国际的信息安全研究再上新台阶; 1996 年, 美国政府同加拿大及欧共体吸收了包括欧洲白皮书、加拿大的 CTCPEC 以及国际标准化组织 ISO:SC27WG3 的安全评估标准在内的各国先进经验, 制定了通用安全评估准则(CC).

我国在充分借鉴他国前提下, 从信息系统建设、管理和使用等方面入手, 建立计算机信息系统安全等级保护制度[10], 并制定安全评估标准. 国家标准《GB/T 22239—2019 信息安全技术 网络安全等级保护基本要求》在开展信息安全等级保护工作的过程中起到了非常重要的作用[11]. 为了进一步完善等级保护的适用性、时效性、可操作性, 近年来出现的网络新技术, 包括移动互联网、云计算[12]、大数据[13]、物联网[14] 和工业控制五个领域, 分别依据 GB/T 22239—2019 修订的思路和方法进行面向领域的等级保护标准制定.

1.1 安全等级保护的定级标准

安全等级的划分是根据等保对象在国家安全、经济建设、社会生活中的重要程度, 遭到破坏后对国家安全、社会秩序、公共利益及公民、法人和其他组织的合法权益的危害程度等因素确定. 表 1

表 1　定级要素与安全等级的关系

Table 1　Relation between grading elements and safety level

程度 Degree	公民、法人、其他组织 Citizens, corporations and other organizations	社会秩序、社会公共利益 Social order, public interest	国家安全 National security
损害 General damage	第一级 Level 1	第二级 Level 2	第三级 Level 3
严重损害 Significant damage	第二级 Level 2	第三级 Level 3	第四级 Level 4
特别严重损害 Especially significant damage	第三级 *Level 3	第四级 Level 4	第五级 Level 5

* Classified protection 1.0 is level 2.

给出了定级要素与安全等级之间的对应关系，其中，从第一级到第五级等级保护对象遭到破坏后所产生的损失依次增加.

1.2　等保 2.0 版与 1.0 版应用层控制点对比

等级保护 2.0 的标准是在等级保护 1.0 的基础上重新确立并发展的. 在应用层面上，如表 2 所示，等级保护三级 2.0 通用标准将原有 1.0 标准中的应用安全、数据安全及备份恢复两个层面合并为应用和数据安全；将通信完整性、通信保密性纳入网络和通信安全层；此外，在 1.0 基础上增加了剩余信息保护和个人信息保护两个控制点.

2　区块链框架

目前，主流的区块链系统包括比特币[1]、以太坊[15]和超级账本[16]，并各具特点. 简单地讲，比特币是最早真正意义的去中心化区块链系统，共识采用工作量证明获得记账权. 它只能处理简单的脚本，并不具备图灵完备的智能合约执行能力. 以太坊是一个允许用户按照自己的意愿创建复杂操作并具备图灵完备的智能合约功能的可编程区块链，它的出现将区块链带入了智能合约[17]时代；IBM 的超级账本系统是一种可插拔、可扩展的模块化区块链平台，它的中心化程度较高，支持通用编程语言而不是特定领域语言（DSL）编写智能合约.

上述区块链系统的不同特征无疑增大了区块链测评的难度，然而，无论何种区块链，按照其系统框架均可以划分为网络层、共识层、交易层、合约层，如图 1 所示. 区块链系统的核心部分包括：分布式对等网络（网络层）、共识机制（共识层）、分布式账本（交易层）、智能合约（合约层）等. 有鉴于此，本文将分别针对区块链系统上述各个部分进行测评.

3　分布式对等网络测评

分布式对等网络是仅包含具有等效控制和操作能力节点的计算机网络. 区块链信息系统底层拓扑结构是分布式对等网络，各个节点通过对等网络进行数据通信以支撑上层功能. 网络的五层模型可以分为物理层、数据链路层、网络层、传输层、应用层. 区块链系统小世界模型[18]的 P2P 网络是以 IP 协议、TCP 协议为基础存在于应用层面上的逻辑覆盖网络，特点主要有非中心化、扩展性强及负载均衡[19]，这些特点为区块链系统高效稳定运行提供了强有力的保证.

区块链系统维护一个在启动时可以连接的对等节点列表[20]，在系统新节点接入已有网络时，首

表 2　等级保护 1.0 与 2.0 三级应用层控制点对比

Table 2　Comparison of application layer control points in classified protection 1.0 and 2.0 at level 3

版本 Version	类别 Category	控制点 Control points
等级保护1.0 Classified protection 1.0	应用安全 Application security	身份鉴别、访问控制、安全审计、通信完整性、通信保密性、软件容错、资源控制 Identity authentication, access control, security audit, communication integrity, communication confidentiality, software fault tolerance, resource control
	数据安全及备份恢复 Data security and backup recovery	数据完整性、数据保密性、备份和恢复 Data integrity, data confidentiality, backup and recovery
等级保护2.0 Classified protection 2.0	应用和数据安全 Application and data security	身份鉴别、访问控制、安全审计、软件容错、资源控制、数据完整性、数据保密性、数据备份和恢复、剩余信息保护、个人信息保护 Identity authentication, access control, security audit, software fault tolerance, resource control, data integrity, data confidentiality, data backup and recovery, residual information protection, personal information protection

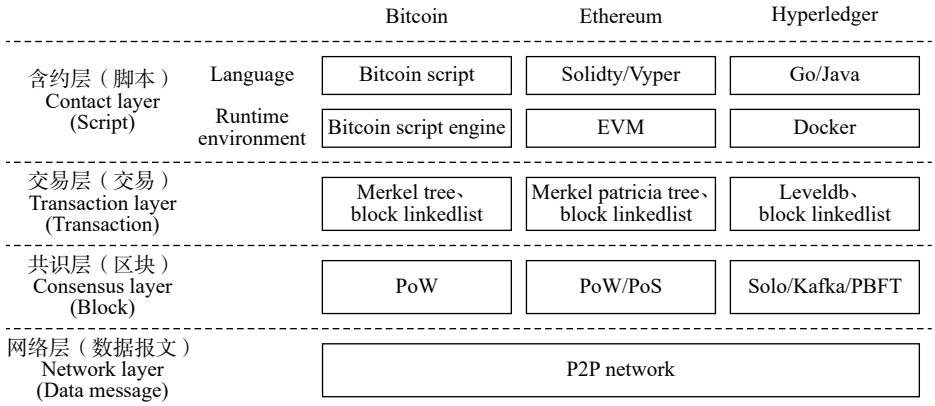

图 1　区块链框架

Fig.1　Blockchain framework

先节点会通过“种子”得到对等节点 IP 列表. 节点间通常采用 TCP 协议与相邻节点建立连接，建立连接时也会有认证“握手”的通信过程用来确定 P2P 协议版本、软件版本、节点 IP、区块高度等. 为了能够被更多节点发现，新节点会将带有自身 IP 地址的信息发送给相邻节点，并要求其返回其已知的对等节点的 IP 地址列表.

表 3 列举了针对区块链中分布式对等网络的测评标准，并对身份鉴别、软件容错、资源控制、数据完整性、审计等五个类别逐项对区块链 P2P 网络[21−22] 进行了分析. 测评项包括：①节点接入控制，② 自我保护与自适应，③并发连接限制，④连接超时限制，⑤单播通讯防篡改，⑥广播通信防篡改，⑦转发通信防篡改，⑧网络状态获取更新和⑨网络节点动态监测.

值得说明的是，已建立连接的节点会定期发送信息维持连接，如果某个节点长达 90 min 没有通信，则结束会话. P2P 网络节点连接不超过 117 个输入连接，向其他节点发起 8 个输出连接，超过数量的 IP 地址会被忽略.

比特币采用 P2P 网络，每个节点邻接边数为 8，如图 2(a)所示我们测量了近 3 个月时间内比特币网络规模的变化情况，可以看出，目前该网络规模可达 60 万个节点，大约需要 7 ~ 10 次转发可实现交易的全网广播，由图 2(b)可知，2009 年之后网络规模呈增长趋势，因此对 P2P 网络的要求日益严格.

区块链网络测评需要对网络规模、节点地理分布、节点中断可用性方面的网络稳定性以及有关传输信息、传播时间等数据进行收集与分析，并总结区块链对等网络的实际使用情况，完成测评工作. 表 3 中提供了针对每个测评项的实施方法及预期效果，同时，给出了区块链系统的测评结果，可以看出，除第②、③、④、⑧测评项通过外，其他 5 项均未达到等保三级要求.

4　共识机制测评

共识机制[23−24] 是区块链系统成员节点在对区块链的操作（如建块、交易验证等）上达成一致确认的方式. 由于区块链是去中心化分布式系统，没有中心化记账节点确保每笔交易在所有节点上的记录一致，因此共识机制的作用就是实现区块链各节点之间的数据一致性和操作同步性，它是区块链系统的关键技术之一.

现有的主流共识技术[25] 主要有工作量证明（PoW）[26−27]、拜占庭容错共识（PBFT）[28−29]、权益证明（PoS）[30] 和授权权益证明（DPoS）[31] 等. 采用了 PoW 协议的区块链，它适用于较大规模网络，也是至今为止最成熟的共识协议. 与之相比，PBFT 则更适用于小型的全连通网络. 区块链可根据需求并结合实际情况（如节点数量、容错性、性能效率等指标）选择适合的共识算法. 本节将对 PoW 协议予以测评.

共识机制的测评以共识算法的资源耗费和共识所达到的效果两方面为核心，测评项主要包括共识资源控制、备份与恢复、共识效果三方面，具体包括：①共识资源控制，②实时备份，③系统热冗余，④共识容错性，⑤共识有效性和⑥共识结果一致性.

PoW 的共识过程如图 3 所示，其目标是所有节点共同建立包含最近交易的新区块，共识主要分为交易收集、候选区块创建、工作量证明（挖矿[32]）、广播区块、区块组装到链和交易回收几个阶段，并由通常的区块链节点（交易节点）与矿工

表 3　分布式对等网络测评

Table 3　Distributed peer-to-peer network assessment

类别 Categories	测评项 Items	实施 Implementation	预期效果 Expected Effectiveness	实际测评结果说明 Description of actual evaluation results	达标 Y/N
身份鉴别 Identification	节点接入控制 Node link control	查看连入区块链是否需要认证 Check if the connection to the Blockchain requires authentication	当节点连入系统时, 对其进行身份认证, 控制节点接入 When nodes are connected, the system authenticates themto restrict node access.	节点接入时没有对身份进行认证 The identity is not authenticated when the node is connected.	否 N
软件容错 Software fault tolerance	自我保护与自适应 Self-protection and self-adaptation	网络不稳定时查看信息传输情况 Inspect information transmission when the network is unstable.	网络抖动对传输不会造成太大影响, 系统运行稳定 Network jitter does not have much impact on transmission. Blockchain runs stably.	网络抖动时, 区块链系统运行稳定 Blockchain system runs stably when network jitter occurs.	是 Y
资源控制 Resource control	并发连接限制 Concurrent connection restriction	查看节点最大连接数目 View the maximum number of connections on nodes	对最大并发连接进行限制, 防止系统资源耗尽 Limit maximum concurrent connections to prevent system resource exhaustion	节点连接不超过117个输入连接, 向其他节点发起8个输出连接. Node connections do not exceed 117 input connections and 8 output connections.	是 Y
	连接超时限制 Connection timeout limit	查看相关网络配置 View related network configurations	自动结束长期无应答的会话防止系统资源占用 Automatically end long-term unanswered sessions to prevent system resource usage.	某个节点超过30 min没有新消息, 则发送心跳消息, 长达90 min没有通信, 则结束会话 If there is no communication for more than 30 minutes, a heartbeat message is sent. End the session if there is no communication for 90 minutes.	是 Y
数据完整性 Data integrity	单播通信防篡改 Anti-tampering of unicast	查看数据传输是否加密防篡改安全 Check whether data transmission is encrypted and tamper-proof	数据在点对点通信过程中不被篡改 Data is not tampered with in the process of point-to-point communication.	不能保障数据在单播通信过程中的完整性 The integrity of data in unicast communication cannot be guaranteed.	否 N
	广播通信防篡改 Multicast communication tamper-proof	能否提供通信多播, 广播功能, 通信过程中数据是否防篡改 Check whether the system can provide communication multicast, broadcast function and tamper-proof data in the process of communication	数据在广播通信过程中不被篡改 Data is not tampered with during broadcast communication.	不能保障数据在广播通信过程中的完整性 The Bitcoin system does not guarantee the integrity of data in the broadcast communication process.	否 N
	转发通信防篡改 Forwarding communication tamper-proof	转发功能及数据防篡改 Data tampering prevention in forwarding communication	数据在某节点通过转发时不被篡改 Data is not tampered with when forwarded by a node.	不能保障数据在转发通信过程中的完整性 The integrity of data in the process of forwarding communication cannot be guaranteed	否 N
安全审计 Security audit	网络状态获取更新 Network status get update	查看日志是否记录节点状态信息 Check whether the log records node status information.	能够为系统的稳定运行提供可信的节点数据 Ability to provide trusted node data for stable operation of the system.	存在单个节点的状态更新记录, 但更新记录不进行全网交换, 无法获取全网状态 There is a status update record for a single node. However, update records are not exchanged in the whole network, the whole network status cannot be obtained.	否 N
	网络节点动态监测 Network node dynamic monitoring	是否对在线节点数量进行统计 Statistics on the number of online nodes	具备对节点动态增加和减少的识别能力 Ability to recognize nodes dynamically increasing and decreasing.	区块链系统具备全网节点数量实时统计能力 The Bitcoin system does not have the real-time statistical ability of the number of nodes in the whole network.	是 Y

节点共同实现, 下述评测内容在此共识过程基础上进行评测.

4.1　共识资源控制（测评项①）

区块链共识机制中矿工不断修改区块头

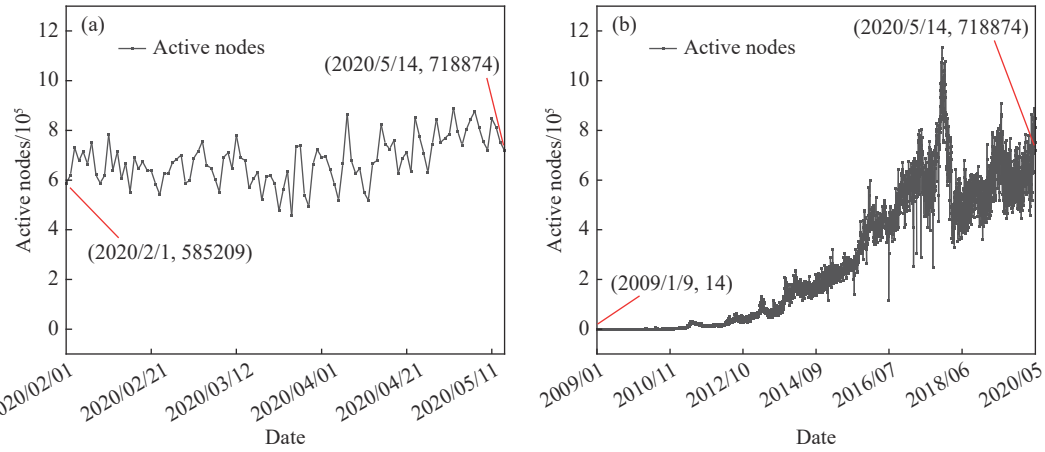

图 2　比特币 P2P 网络规模变化图. (a)近 3 个月比特币网络规模变化图; (b) 2009 年之后比特币网络规模变化图

Fig.2　Scale change of Bitcoin P2P network: (a) scale change of Bitcoin P2P network in last three months; (b) scale change of Bitcoin P2P network since 2009

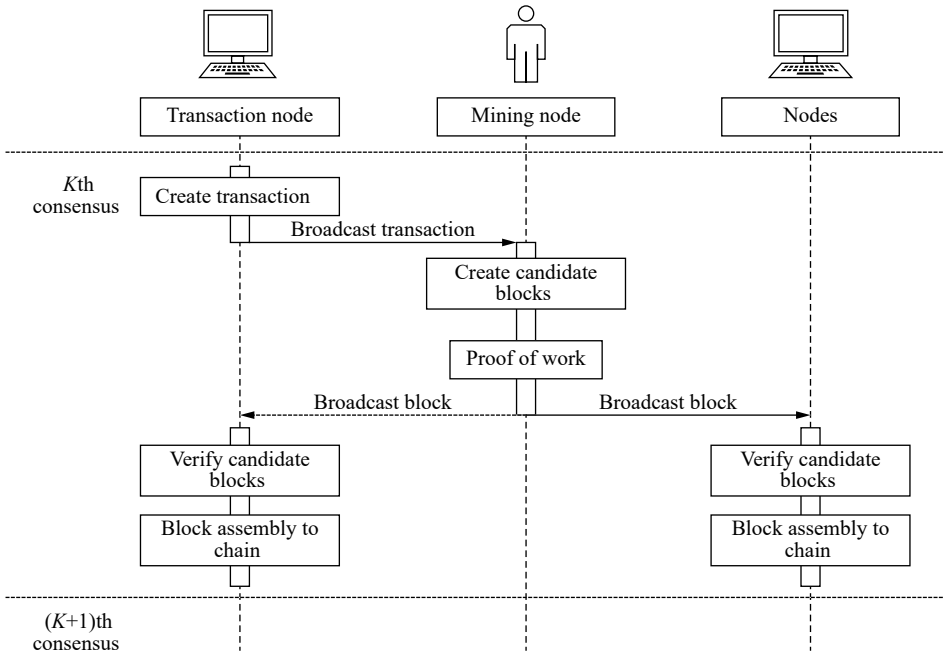

图 3　共识过程时序关系图

Fig.3　Consensus timing diagram

BlockHeader$_n$的随机数N_n, 并计算区块头的SHA 256^{2}哈希值, 直到区块头哈希值小于难度值T_n. 上述关系可由下式表示: SHA 256^2(BlockHeader$_n$) < T_n. 矿工在短时间内消耗大量的计算资源以求得满足要求的随机数, 进而争夺记账权. 若挖矿成功, 则N_n作为该矿工的工作量证明. 该证明生成困难(生日攻击下的平均挖矿计算复杂性为$O\left(\sqrt{2^{256}/T}\right)$), 任何节点可通过上面的公式轻易验证该矿工为成功者. 系统经过十余年的运行, 挖矿难度越来越大, 带来了大量(电力)资源消耗, 这意味着系统运行成本的增加, 共识周期的延长, 严重影响系统稳定性, 因此应将全网平均算力和区块生成时间分布等作为资源控制(测评项①)的测评指标, 下述以比特币为例进行评测分析.

(1)全网平均算力.

算力是衡量在一定的网络消耗下生成新块的单位总计算能力; 全网算力, 即网络中所有参与挖矿的矿机算力综合, 比特币的全网算力是所有参与挖矿的比特币矿机算力的总和. 如图 4 所示我们收集了 2009 年 1 月至 2020 年 5 月的全网平均算力, 并画出了分布趋势图. 可以看出, 随着比特币在线活跃地址数的增加和计算能力的迅捷发展, 比特币全网算力也有了较大的提升.

(2)区块生成时间分布.

假设区块链中一个节点的地址为 A, 且其余额为bal(A), 在挖矿过程中, 该节点不断修改随机数的

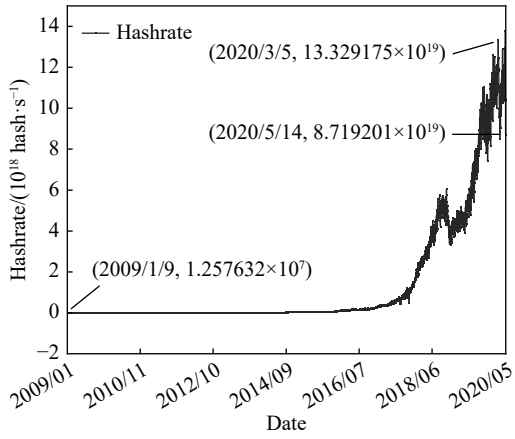

图 4　比特币全网算力图

Fig.4　Bitcoin hashrate historical chart

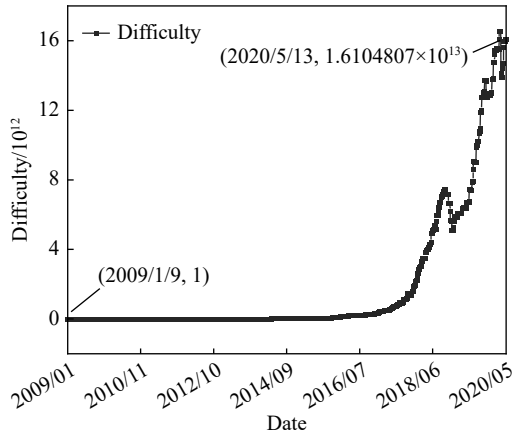

图 5　共识机制难度变化趋势图(比特币)

Fig.5　Consensus difficulty change trend diagram(Bitcoin)

值(通常是逐渐加一),从而使计算结果小于目标阈值才能建造有效区块. 我们将建造一个新的区块时的目标值记作θ,挖矿难度为D,则区块链协议中所有有效区块都需要满足一个条件$U \leqslant \theta \leqslant 1$,式中$U \sim [0,1]$是对区块头数据进行哈希并对得到的值进行归一化后生成的均匀分布的随机变量. 由于哈希函数的特性,很多共识技术都是该式的特殊情况,例如:

①在 PoW 情况下,$\theta = 1/D$;

②在 PoS 情况下,$\theta = \mathrm{bal}(A)/D$;

为了生成一个块,用户需要找到令U满足$U \leqslant \theta \leqslant 1$的数据,即不断更改随机数,并计算包含其的区块头哈希结果U,使其满足$U \leqslant \theta \leqslant 1$,设$N$为用户在找到一个有效块之前需要计算的数据组合数. 由于工作量证明 PoW 间隔很大,所以用户每秒只能迭代r个组合,其中r由用户的挖掘设备确定. 在权益证明 PoS 情况下,搜索空间较小,因此可假设$r = 1$. 用户找到一个有效块所需的时间T与N有关:$T = N/r$,考虑累积概率分布:

$$P\{T \leqslant t\} = P\{N \leqslant rt\} = 1 - P\{N > rt\} =$$

$$1 - (1-\theta)^{rt} = 1 - \exp(\log(1-\theta)^{rt}).$$

当$\theta \ll 1$时,有$\log(1-\theta) \approx -\theta$,代入上式可得:

$$P\{T \leqslant t\} \approx 1 - \exp(-\theta rt).$$

因此,用户找到一个有效块所需的时间T以速率θr呈指数分布. 在 PoW 的情况下,这个速率等于r/D. 在 PoS 的情况下,$r = 1$,速率等于$\mathrm{bal}(A)/D$,生成有效区块的概率等于用户资金余额与流通货币总量的比率,若将整个网络中的所有用户的资金总额视为$\sum_a \mathrm{bal}(a)$,则整个网络的块生成时间以速率$\sum_a \mathrm{bal}(a)/D$呈指数分布. 如图 5 所示我们收集了近些年比特币区块的难度值,并绘制了难度变化曲线图,是一个较为明显的指数分布曲线,拟合方程为$y = -1.44623 \times 10^9 \times (1 - \mathrm{e}^{-0.00228x})$.

针对 PoW 的攻击是敌手[33]以较大优势成为挖矿的获胜者,从而使用记账权改变或伪造交易. 为取得挖矿成功,当前敌手采取的主要攻击包括:

(a)共识过程攻击包括 51% 算力攻击[34]、暴力破解[35]、私自挖矿[36]等. 以 51% 算力攻击为例,它并不是指拥有全网 51% 以上的算力才能成功攻击,而是算力超出 51% 这个门限,敌手计算出正确哈希值的速度就会比全网其他矿工更快,攻击成功率会大大增加.

(b)区块广播过程可受到日食攻击[37]、女巫攻击[38]等因素影响. 其中,日食攻击是敌手通过阻止正常节点通讯的方式影响共识;女巫攻击中敌手会伪装成不同角色的区块链节点监视和干扰正常网络.

资源控制(测评项①)的测评中考虑上述攻击对系统带来的影响,可通过提高资源控制难度保障系统安全. 就区块链系统而言,随着系统节点不断加入,全网总算力剧增,系统网络也愈加庞大,敌手占据全网大部分算力的可能性极小,操控网络难度巨大,因此可保证系统资源可控. 但对于小型区块链系统而言,全网算力较低,敌手可通过资源控制的方式成功攻击系统.

4.2　实时备份(测评项②)

交易的收集阶段过程为:(1)新交易产生后将实时地被该节点通过区块链网络广播至全网;(2)矿工节点收集交易并验证交易的规范性(包括是否前一笔交易属于未花费交易等[39]);(3)如果交易内容的正确性和逻辑性符合要求,则矿工会把交易存入内存的“未确认交易池”. 因此,交易形成后,创建节点会通过 P2P 分布式对等网络实时广播至全网,并由矿工节点收集验证其规范性,进而

放至“未确认交易池”, 实现本地和异地节点的数据备份.

区块组装到链工作的具体过程为: (1)验证挖矿的正确性; (2)验证失败则丢弃区块, 否则将区块附加在已有区块链之后. 节点寻找新区块的父区块, 并链接到父区块完成区块的组装. 每个节点不断地将共识区块写入自己的账本中, 从而达到全网节点具有相同数据副本的实时备份效果[40].

综上, 区块链在交易、区块产生及共识的过程中都达到了全网节点数据备份效果, 测评项②得到保证.

4.3　系统热冗余(测评项③)和共识容错性(测评项④)

区块链系统节点是去中心化并包含少数恶意节点的, 达到 100% 的共识显然很难实现, 因此系统测评应充分采纳统计学中的小概率事件思想: 只要共识度超过 95% 即代表完全共识. 由于目前区块链系统在 2 h 内能以 99.9999% 的概率确认单笔交易, 因此可认为共识容错性(测评项④)达到标准. 依据上述标准, 区块链系统节点是互为冗余的, 少数节点的故障并不影响系统稳定性和可用性, 因此系统热冗余(测评项③)达到要求.

4.4　共识有效性(测评项⑤)

在交易收集阶段, 矿工节点通过规范性验证检查交易中签名正确性、货币是否存在、货币是否二次使用等交易数据内容, 以此保证了被共识交易的有效性(测评项⑤), 然而, 上述验证过程并不能完全保证交易的绝对有效性, 如“门头沟(Mt.Gox)事件”中交易所受到的延展性攻击[41], 因此测评工作应根据最新的 CVE(Common Vulnerabilities & Exposures)漏洞加以展开.

候选区块创建阶段由矿工完成, 具体为: (1)新建候选区块以及 Coinbase 交易(创币交易, 即含挖矿奖励的新交易); (2)从“未确认交易池”中按优先级提取交易并写入前述区块中; (3)计算区块头部信息并将其填充到新创建的候选区块中. 在第一步前矿工可计算本次挖矿可得奖励, 奖励由当前区块奖励与将要打包进区块的交易费用总和两部分组成, 因此, 验证 Coinbase 交易中奖励的真实性和有效性可保证矿工工作的正确性(测评项⑤).

PoW 共识算法根据整个网络的哈希速率动态调整难度值, 当前调整周期为 2 周, 调整值将会写入区块头部并参与下一阶段的工作量证明计算, 从而建立起难度值的延续影响, 保障共识数据区块顺序不变.

当主链高度超过其他分支六块(可实现在 1 h 内能以 99.9% 的概率确认[42] 单笔交易)以上, 分支的区块交易将会被进一步解析, 未处理的交易会被重新放入“未确认交易池”. 分支的交易回收过程能够避免交易丢失进而保证了一定程度上共识的有效性.

综上, 共识机制在不同阶段皆采用了一定的机制验证交易数据的正确性和逻辑性, 保证了共识有效性(测评项⑤)的达标.

4.5　共识结果一致性(测评项⑥)

由 PoW 交易收集、候选区块创建、工作量证明(挖矿)、广播区块、区块组装到链和交易回收几个处理过程可得, 区块链系统的安全性主要受挖矿节点的影响, 已有挖矿算力对系统安全分析的结果表明当严格遵循共识规则的挖矿节点算力超过(微弱)多数时, 可保证系统内所有节点得到相同共识, 共识结果具有一致性(测评项⑥).

如表 4 所示, 文献 [43] 展示了不同的区块链参数选择(区块间隔、公共节点、挖矿池、陈腐块率和区块大小)对区块链网络传输的影响. 通过以上测评, 表 5 总结了 PoW 共识区块链系统在每个测评项的达标情况: 从备份与恢复及共识效果来看, PoW 共识区块链系统均可满足测评项①②③④⑤⑥要求.

表 4　不同区块链参数选择对网络传输影响[43]

Table 4　Impact of parameter selection on network transmission in different blockchains[43]

Parameter	Bitcoin	Litecoin	Dogecoin	Ethereum
区块间隔 Block interval	10 min 10 min	2.5 min 2.5 min	1 min 1 min	10−20 s 10−20 s
公共节点 Public nodes	6000	800	600	4000
挖矿池 Mining pools	16	12	12	13
陈腐块率/% Stale block rate	0.41	0.273	0.619	6.8
区块大小/KB Block size	534.8	6.11	8	1.5

5　分布式账本测评

分布式账本[44] 是在各个成员之间同步共享、序列化、防篡改的分布式数据存储结构, 并可为区块链系统提供运行过程中产生的各种类型数据的写入与查询服务. 针对数字货币交易, 区块链系统

表 5　共识机制测评

Table 5　Consensus mechanism assessment

类别 Categories	测评项 Items	实施 Implementation	预期效果 Expected effectiveness	实际测评结果说明 Description of actual evaluation results	达标 Y/N
资源控制 Resource control	共识资源控制 Consensus resource control	检测计算机中资源使用情况. Check the use of resources in the computer	共识机制消耗计算机资源应该最小化原则 Consensus mechanisms should minimize the consumption of computer resources.	PoW共识机制计算资源耗费较大, 但系统资源可控 PoW consumes a lot of computing resources, but the system resources are controllable.	是 Y
备份与恢复 Backup and recovery	实时备份 Real-time backup	查看节点是否同步了新共识区块 Check whether the node has synchronized the new consensus block	全网节点具有相同的数据副本 All network nodes have the same data replica.	节点实时备份区块链中产生的交易数据 Real-time backup of transaction data generated in Bitcoin system by nodes.	是 Y
	系统热冗余 System hot redundancy	查看节点瘫痪后系统可用性 View system availability after node paralysis	业务连续性未被中断 Business continuity not interrupted.	节点之间互为冗余, 单一或少数节点故障不影响系统稳定性和可用性 Nodes are redundant to each other and single or few node failures do not affect the stability and availability of the system.	是 Y
共识效果 Consensus effect	共识容错性 Consensus fault tolerance	设置异常节点, 查看共识情况 Set exception nodes and view consensus.	存在共识阈值, 使得超过阈值的节点达到共识即代表全网共识完成 There is a consensus threshold, so that the node exceeding the threshold reaches the consensus, which means that the consensus of the whole network is completed.	系统可容纳5%的节点共识错误. 95%以上的节点共识成功即可 The system can accommodate 5% node consensus errors. More than 95% of the nodes are successful.	是 Y
	共识有效性 Consensus Effectiveness	发起非法交易, 查看共识是否失败 Initiate an illegal transaction to see if the consensus failed	非法交易共识失败. 通过对交易进行正确性和逻辑性验证, 使恶意造假交易的代价昂贵, 避免恶意共识 Illegal transaction consensus failed. By verifying the correctness and logic of the transaction, the cost of malicious fraudulent transactions is expensive and avoids malicious consensus.	非法交易不能被共识通过 Illegal transactions cannot be passed by consensus.	是 Y
	共识结果一致性 Consensus consistency	发起合法交易, 查看共识结果是否满足一致 Initiate a legal transaction and see if the consensus result is consistent	忠诚参与方共识结果具有一致性 Loyal participant consensus results are consistent.	对于合法交易区块链系统达成共识后写入区块链 After agreeing on the legal transaction of Bitcoin system, it is written into the blockchain.	是 Y

中的分布式账本被设计用来存储当前时间段内发生的交易信息, 并通过密码学哈希(hash)函数来维护交易信息的完整性和抗抵赖性等功能.

分布式账本的测评是针对区块链中所存储信息的结构、功能及安全机制展开的. 在表 6 中, 我们将测评项划分为软件容错、访问控制、数据完整性、数据保密性和账本功能等 5 个基本方面, 同时, 还把分布式账本特有的抵赖性、同步性、幂等性三个功能点作为账本功能予以重点列出. 据此, 分布式账本的测评项包括: ①账本格式规范性, ②账本访问控制, ③存储完整性, ④存储保密性, ⑤数据抗抵赖, ⑥账本数据同步和⑦账本数据幂等.

5.1　账本格式规范性 (测评项①)

区块链具有严格的结构定义, 每个块[45]由区块头和区块体构成, 如表 7 所示, 并且数据长度有明确的数据格式规范. 区块头包含区块版本 V、难度 D、前区块哈希PreH、默克尔树根 M、随机数 N 和时间戳 T 等信息, 第 n 个区块头可表示为 $\text{BlockHeader}_n := (V_n \| D_n \| M_n \| T_n \| \text{PreH}_n \| N_n)$.

区块体存储了块中的交易数量和交易列表. 图 6 表示了区块链系统的交易结构, 且结构中信息大多有标准长度限制. 交易由交易版本和若干个输入段(Vin)与输出段(Vout)构成, 每个输入段与特定的一个“未花费过的”交易输出通过哈希函

表 6　分布式账本测评

Table 6　Distributed ledger assessment

类别 Categories	测评项 Items	实施 Implementation	预期效果 Expected effectiveness	实际测评结果说明 Description of actual evaluation results	达标 Y/N
软件容错 Software fault tolerance	账本格式规范性 Standardization of ledger	查看账本中的数据格式是否有统一标准 Check whether the data format in the ledger has a uniform standard	交易、区块等数据按照数据格式进行存储 Data such as transactions and blocks are stored in data format.	区块链系统交易、区块等均有统一组织标准 Blockchain system transactions, blocks, etc. have unified organizational standards.	是 Y
访问控制 Access control	账本访问控制 Ledger access control	查看是否存在访问策略监管节点及访问控制策略 Check whether there is an access policy supervision node and access control policy	对账本上的数据资源进行保护, 防止非法访问 Protect the data resources on the ledger against illegal access	作为公有链系统没有完备的访问控制策略 Bitcoin as a public blockchain, there is no complete access control strategy	否 N
数据完整性 Data integrity	存储完整性 Storage integrity	查看数据存储是否存在哈希、指纹等机制保障存储的完整性 Check if there is a hash mechanism in the data storage to ensure the integrity of the storage	存储内容被哈希处理, 完整性得到保障 Stored data is hashed and integrity is guaranteed.	将交易按照默克尔树的形式进行哈希并存储于区块 Bitcoin hashes transactions in the form of Merkel trees and stores them in blocks.	是 Y
数据保密性 Data confidentiality	存储保密性 Storage Confidentiality	查看机密数据的存储是否加密 Check if the storage of confidential data is encrypted	数据存储不是以明文格式 Data is not stored in plaintext format.	数据存储是以明文的16进制形式进行存储, 方便查询和验证 Bitcoin data storage is stored in plaintext in hexadecimal form, which is convenient for query and verification.	否 N
账本功能 Ledgerfunction	数据抗抵赖 Data non-repudiation	查看账本中的交易数据来源是否有效 Check if the transaction data in the ledger is signed	交易被各个参与方签名, 使交易可溯源, 以达到抗抵赖的作用. The transaction is signed by each participant, so that the transaction can be traceable to achieve the role of non-repudiation.	区块链系统通过对交易数据进行签名达到了数据抗抵赖的作用 Bitcoin achieves data non-repudiation by signing transaction data.	是 Y
	账本数据同步 Ledger data synchronization	查看是否有完全节点, 节点间存储账本数据是否一致 Check if there is a full node, store all data in the ledger	全节点中同步了账本中所有的数据, 可以通过全节点得到区块链数据的完整副本 All the data in the ledger is synchronized in the full node. A complete copy of the blockchain data can be obtained from full nodes.	区块链系统中存在同步了账本所有数据的全节点, 并能对同步过程中发现的数据错误予以检测及确认 There are full nodes in the Bitcoin system that synchronize all the data of the ledger.	是 Y
	账本数据幂等 Ledger data idempotentce	查看账本信息中检索同样的数据结果是否一致 Check if the results of retrieving the same data are consistent	在查询相同记录时具有相同的结果, 确保数据的一致性 Ensure data consistency by querying the same records with the same results.	区块链系统存入账本的数据均通过共识, 账本数据具有幂等性 The data of Bitcoin deposited in the ledger has passed the consensus, and ledger data has idempotency.	是 Y

数(SHA256)和签名脚本相衔接, 这种结构也被称为 UTXO(未花费的交易输出).

根据以上分析, 区块链中交易、区块等结构皆有严格的数据项要求和数据项长度规定, 能够保证账本格式规范性和全局一致性, 测评项①达标.

5.2　账本访问控制(测评项②)

区块链平台的开放性使得所有用户均可访问账本数据, 不存在具有监管功能的节点, 因而测评项②未能达到标准.

5.3　存储完整性(测评项③)

区块链中引入了完整的密码学数据认证机制

表 7　区块链头信息及长度限制

Table 7　Information and length limit of Blockchain Header

数据项 Items	用途 Use	大小(字节) Size(byte)
区块版本V Version	区块版本号 Block version number	4
难度D Difficulty Target	用以标注挖矿难度 To indicate the difficulty of mining	4
前区块哈希 PreH Pre-block hash	基于区块中所有交易的256位hash值 Based on the 256-bit hash value of all transactions in the block	32
默克尔树根M Merkletree Root	交易内容hash256值 The value of the transaction content 256-bit hash	32
随机数N Nonce	用以调整当前区块头hash值 To adjust the current block head hash value	4
时间戳T Timestamp	UNIX时间戳A UNIX timestamp	4

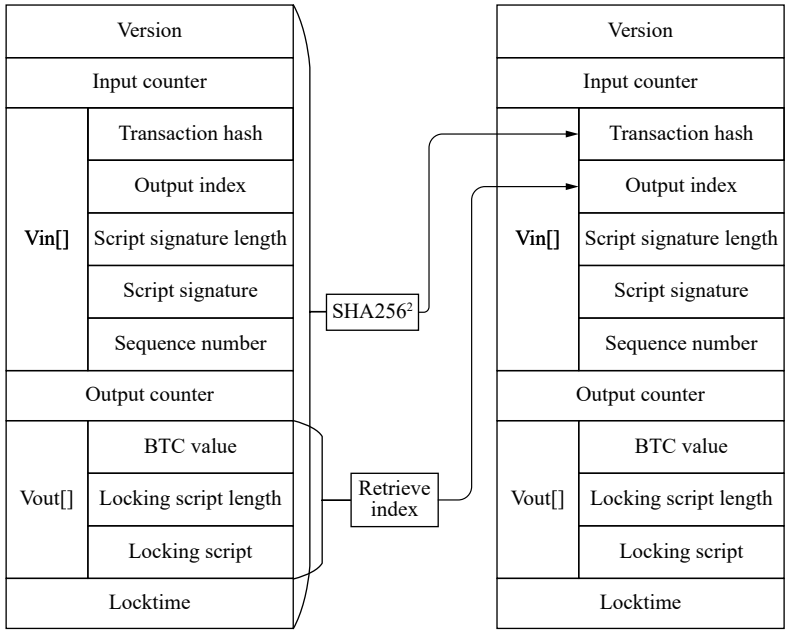

图 6　区块链交易结构

Fig.6　Structure of blockchain transaction

和严格且规范化的数据结构来保证交易、区块数据的不可篡改性，列举如下：

(1)密码学 hash 函数的使用：利用 hash 算法逆向求解困难、输入的雪崩效应、抗碰撞等特性，保证区块数据永久存储且不可篡改.

(2)链式哈希结构[46]：区块头之间通过密码学哈希函数(嵌套 SHA256)进行衔接，保证了区块间数据在时间轴上不可修改、插入、删除等攻击.

(3)树状哈希结构：采用默克尔树结构[47−48]对大量的交易进行封装，并在区块头中放置默克尔树根[49]，保证此区块中交易内容、顺序均不可更改.

综上，区块链中利用大量密码学机制和数据结构对数据进行存储保护，可保证数据区块存储过程的完整性，测评项③达标.

5.4　存储保密性（测评项④）

区块链账本采用 16 进制编码(未加密)方式存储数据以方便用户对数据进行查询验证和追溯，受限于目前公钥加密技术在大规模动态群组下密钥协商、构造、分发、更新、撤销等技术上的不成熟，因此在存储保密性(测评项④)上未能达到等级保护三级要求.

5.5　数据抗抵赖（测评项⑤）

在图 3 所示交易结构中，交易结构 Vin 所含“交易输出索引”字段是指前一交易中所使用输出段 Vout 的序号(即索引号)，“脚本签名”[50]是解锁脚本的不定长数据，只有解锁脚本正确，才能对输

出进行消费,“锁定脚本”定义了支付输出所需的条件(如认证货币所有者身份的公钥信息),在交易信息中,为验证货币的所属关系,前一交易的“锁定脚本”和当前交易的“脚本签名”可分别存储货币所有者的“公钥”与“签名”信息,并可通过前者对后者签名的有效性予以验证,使交易满足测评项⑤中的数据抗抵赖.

5.6　账本数据同步(测评项⑥)

在分布式账本管理方面,区块链系统依赖“完全节点”存储账本所有数据,新加入节点可通过对完全节点克隆得到区块链数据的完整备份,保证了账本数据同步(测评项⑥). 此外,区块链系统能对同步过程中发现的数据错误予以检测及确认,并标注为确认交易和未确认交易两种,图 7(a)给出了近 3 个月时间内比特币和以太坊确认交易数量的变化情况,图 7(b)给出了比特币近三月的未确认交易增长变化情况,可知,有大量的未确认交易存在(约占 20%),这表明区块链能够很好地检测并区分恶意或无效的交易.

5.7　账本数据幂等(测评项⑦)

针对账本数据的查询请求,账本中数据完整性可经过密码学哈希函数验证,hash 函数冲突避免的函数特性,保障了查询结果在所有节点中的一致性,使检索幂等性(测评项⑦)得以实现.

综上,在分布式账本方面进行评测,得到最终结果如表 6 所示,账本访问控制(测评项②)和存储保密性(测评项④)未能达到等级保护三级要求,其它评测项皆符合等保三级标准.

6　合约层分析

智能合约是运行在区块链上的程序或脚本,区块链作为数据的载体存储着事件的关键信息,而智能合约就是在区块链中操作这些数据的规则. 例如,比特币交易使用比特币脚本及签名技术限定未花费交易的所有者;以太坊等区块链平台以计算机程序的方式代替比特币脚本,使得用户可以更加灵活地制定规则.

智能合约被称为运行在区块链上,是因为它不止被一台计算机运行,而且要被参与验证的节点执行并验证. 智能合约运行流程为:(1)执行者发起运行请求,在本地运行并检验可行性;(2)将运行状态广播到区块链网络中,挖矿节点执行智能合约并验证通过后打包到区块中;(3)区块广播到所有节点,参与验证的节点通过执行区块中交易所含有的合约来完成验证.

表 8 列举了针对区块链中智能合约层的测评标准,并对身份鉴别、安全审计、恶意代码防范、数据完整性、数据保密性 5 个类别逐项对智能合约层进行了分析. 测评项包括:①执行身份验证,②行为事件审计,③审计记录,④免受恶意代码攻击,⑤传输完整性和⑥传输保密性.

6.1　执行身份验证(测评项①)

身份验证是智能合约最基础的功能. 为实现身份验证,比特币脚本被分为锁定脚本和解锁脚本,通过密码学数字签名技术,解锁“锁定脚本”的用户就是符合规定可以使用这笔交易的用户. 最常用的脚本如图 8 所示.

图 8 中,解锁脚本以签名和公钥作为输入,通过锁定脚本里设定的操作码以及存储的公钥哈希验证了签名的正确性,从而鉴别了用户身份,测评项①达标.

6.2　安全审计(测评项②和③)

审计[51]是指按照某种规范忠实地记录下系统

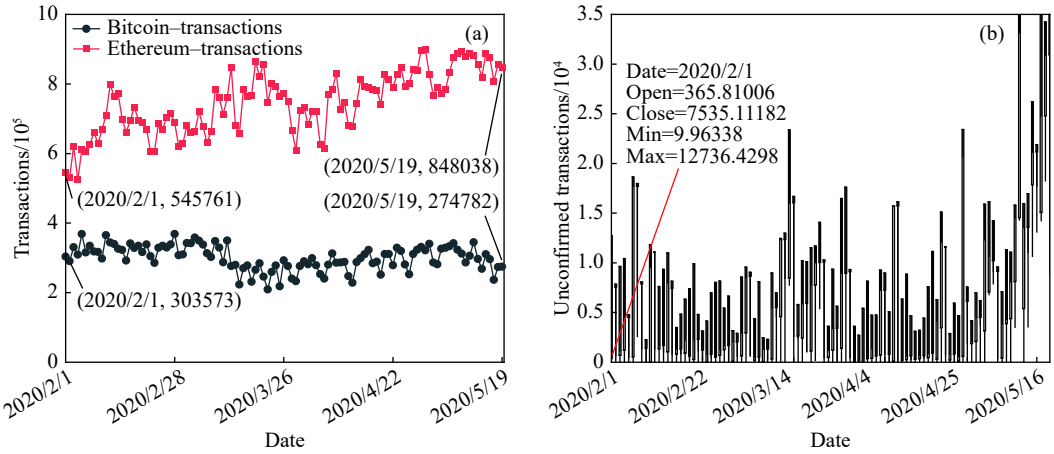

图 7　区块链系统中已确认和未确认交易数量对比(近 3 个月). (a)比特币与以太坊确认交易量图;(b)比特币中未确认交易增长变化图

Fig.7　Comparison between confirmed and unconfirmed transactions in the blockchain systems: (a) diagram of confirmed transactions for Bitcoin and Ethereum; (b) growth chart of unconfirmed transactions for Bitcoin

表 8　区块链合约计算层测评

Table 8　Blockchain contract computing layer evaluation

类别 Categories	测评项 Items	实施 Implementation	预期效果 Expected effectiveness	实际测评结果说明 Description of actual evaluation results	达标 Y/N
身份鉴别 Identification	执行身份验证 Performingentity authentication	查看合约是否许可查看或限定执行者身份 Check if the contract can be viewed or qualify executor's identity	应对登录的用户进行身份标识和鉴别，身份标识具有唯一性，身份鉴别信息具有复杂度 The identification and authentication should be carried out for the logged-in user. The identification is required to be unique and complicated.	在发布交易时，区块链会对执行者身份进行验证，因此可以控制执行合约的身份 When publishing a transaction, the blockchain verifies the executor's identity, thus constraining the execution of contract.	是 Y
安全审计 Security audit	行为事件审计 Behavioral event audit	能否验证智能合约的执行 Check if to verify the execution of smart contract	应启用安全审计功能，审计覆盖到每个用户，对重要的用户行为和重要安全事件进行审计 The security audit function should be enabled to cover every user over significant user actions and security events.	所有参与挖矿节点会验证智能合约执行的正确性 All nodes involved in mining can verify the correctness of smart contract execution.	是 Y
	审计记录 Audit records	是否记录了审计的相关信息 Check if audit information is recorded	审计记录应包括事件的日期和时间、用户、事件类型、事件是否成功等．应对审计记录进行保护，定期备份，避免受到未预期的删除、修改或覆盖等 The audit record should include the date and time of event, the executor, the type of event, the state if the event was successful, etc. Audit records should be protected and backed up regularly to avoid unexpected deletions, modifications or overwrites.	区块中的交易记录了智能合约的执行时间、执行用户、执行的输入与输出 The transactions in the block record the execution time, the executors, the input and output of the smart contract.	否 N
恶意代码防范 Malicious code protection	免受恶意代码攻击 Protection from malicious code	是否有免受恶意代码攻击的机制 Check if there is a mechanism to protect against malicious code	应采用免受恶意代码攻击的技术措施或主动免疫可信验证机制及时识别入侵和病毒行为，并将其有效阻断. It is necessary to adopt the technical measures to avoid the attack of malicious code or the trusted verification mechanism with active immunity to identify the intrusion and virus behavior in time and block it effectively.	通过限定的寻址方式、限定的指令集以及Docker等运行环境或其他机制使得本地计算机及区块链系统不会受到影响 Local computers and blockchain systems do not be affected byrestricted addressing methods, limited instruction sets, operating platforms such as Docker, or other mechanisms.	是 Y
数据完整性 Data integrity	传输完整性 Transmission integrity	查看是否通过校验技术或密码技术保证数据完整性 Check if data integrity is guaranteed by CRC or cryptography	应采用校验技术或密码技术保证重要数据在传输过程中的完整性. Verification technology or cryptography should be adopted to ensure the integrity of important data during transmission.	存在单个节点的状态更新记录 There are status updating records for individual nodes.	是 Y
数据保密性 Data confidentiality	传输保密性 Transmission confidentiality	查看是否通过密码技术保证数据保密性 Check if data onidenticality is guaranteed by cryptography.	应采用密码技术保证重要数据在传输过程中的保密性. Cryptography should be adopted to ensure the confidentiality of important data during transmission.	区块链系统不具备全网节点数量实时统计能力 The blockchain system does not have the real-time statistical ability on the number of nodes in the whole network.	否 N

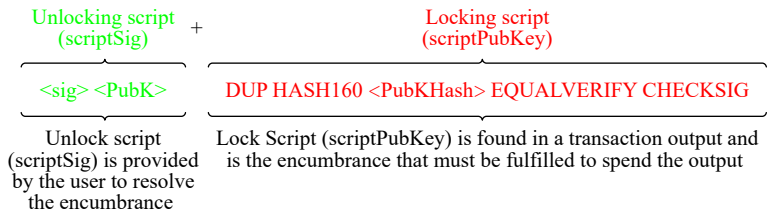

图 8　常用脚本机制

Fig.8　Common scripting mechanism

表 9　区块链系统 error 审计分类

Table 9　Blockchain error audit classification

功能 Function	接口函数 Interface function	输出错误 Output error
初始化错误 Initialization error	AppInit2_Cold()	Winsock库、初始化完整性检测、钱包文件损坏等 Winsock Library, Initial Integrity Detection, Wallet File Damage, etc.
交易错误 Transaction error	CheckTransaction()	检查交易时出错, 如输入输出为空等交易格式错误 Errors in checking transactions, such as empty input and output, etc.
	AcceptToMemoryPool()	验证交易合理性并存入交易池时发生错误, 如输入已经被花费等 Errors occur when validating the reasonableness of transactions and storing them in the trading pool, such as input being spent, etc.
	CScriptCheck()	脚本签名错误 Script signature error
	CheckInputs()	交易输入错误, 如: 交易总输入<总输出 Transaction input errors, such as: total transaction input <total output
	CheckSignature()	检查签名时出错 Error in checking signature
区块错误 Block error	WriteBlockToDisk()	将区块写入磁盘出错, 如文件打开失败 Errors in writing blocks to disk, such as file opening failure
	ReadBlockFromDisk()	从磁盘读出区块出错, 如打开区块文件失败 Error reading block from disk, such as failure to open block file
	DisconnectBlock()	断开区块链接时出错 Error while disconnecting block links
	ConnectBlock()	连接区块时出错, 如资产提交时出错 Error connecting blocks, such as asset submission
	CheckBlock()	检查区块时出错, 如默克尔树根不匹配 Error checking blocks, such as Merkle root mismatch
	ContextualCheckBlockHeader	检查区块头部信息是否出错, 如块的时间戳太早 Check if block header information is wrong, such as block timestamp too early
	LoadBlockIndex()	加载区块索引出错, 如将创世块写入磁盘失败 Error loading block index, such as failure to write Genesis block to disk
共识错误 Consensus error	CheckBlockHeader()	工作量证明失败 Proof-of-work error
	AcceptBlock()	未找到工作量证明 Accepting blocks makes errors, such as failing to find proof-of-work
网络错误 Network error	RecvLine()	socket错误Socket error
	Read()	连接节点数据文件peer.dat读错误 Error in peer.dat reading of connection node data file
	Write()	连接节点数据文件peer.dat写错误 Error in peer.dat writing of connection node data file
	Connect()	连接错误 Connection error
	ProcessMessage()	侦听并处理网络中的不同的消息时出错 Errors in listening for and processing different messages in the network
远程过程调用 Remote procedure call	JSONRPCError	远程过程调用请求、解析、参数等错误 Errors in remote procedure call requests, parsing, parameters, etc.

所发生的所有行为, 方便管理员对系统安全进行实时监控, 及时发现异常违规行为并取证[52]. 通过对某区块链系统开源代码分析, 表 9 列举了其初始化、交易、区块、共识、网络和远程过程调用 6 个功能模块输出的错误和涉及该错误的接口函数, 可见系统关于审计信息的记录是较为详尽的. 智能合约的每一次执行都会被其他节点所验证, 合约中的行为或事件都会被审核, 因此行为事件审计(测评项②)达标.

图 9 为系统日志生成流程, 具体为: (1)给生成的日志信息添加规定格式的时间戳; (2)查看参数中是否要求输出信息中附加 IP 地址; (3)将处理好的日志输出到默认的 debug.log 中, 用户也可自定义将日志信息打印到控制台. 日志文件 debug.log 容量最大值被系统设定, 超出部分将会被丢弃, debug.log 只存最新的审计信息, 由此可知日志信息并不是永久保存、不可更改的.

系统的日志分为 Debug、Warning、Error 三个级别, 目前没有 Fatal 致命错误, 其中 Debug 级日志记录了系统在开发调试和运行时的状态信息; Warning 记录了可能导致错误的告警信息; Error 记录了系统运行过程中的异常错误.

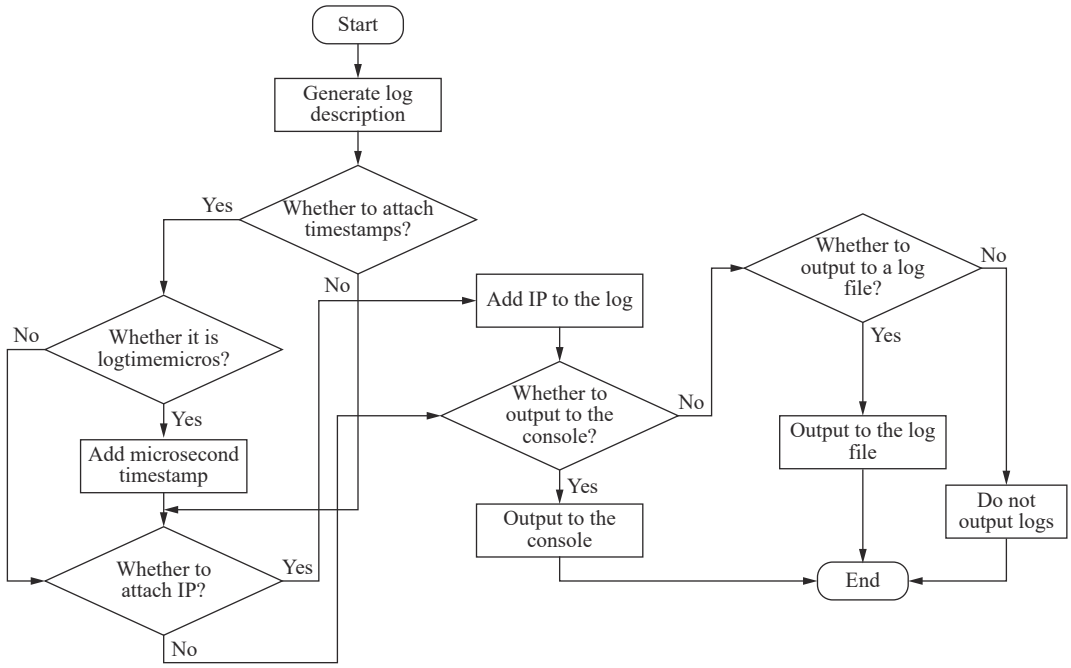

图 9　区块链日志生成流程图

Fig.9　Blockchain log workflow chart

区块链系统中的审计记录在审计格式上不符合等保要求，记录的事件不够具体．其日志可以输出也可以不输出，输出的文件内容可以被篡改甚至清除，因此审计记录（测评项③）未达到等保三级的要求．针对系统审计情况，提出的改进措施如下：

（1）建立分布式区块链系统日志网络，日志作为交易上传到区块链上[53]．

（2）细化日志记录项，审计内容至少包含事件的日期和时间、用户、事件类型、事件是否成功及其他与审计相关的信息．

（1）单节点函数调用及状态日志应以受保护的形式存于本机，避免受到删除、修改或覆盖．

6.3　免受恶意代码攻击（测评项②）

智能合约需要由参与验证的节点执行来保证合约执行结果的正确性，这就需要将不同用户编写的智能合约部署和运行在验证节点上，因此防范恶意代码是非常有必要的．

智能合约的安全问题分为两个方面：（1）智能合约程序本身的安全问题；（2）智能合约程序对执行环境造成的安全问题．根据等保标准，本文仅讨论第二种安全问题，即恶意智能合约代码对验证节点所在的计算机、区块链程序及其他智能合约造成的安全问题．

比特币的脚本系统采用栈式运行环境，寻址规则为直接寻址，且指令相对简单，没有跳转或循环等指令，因此不会对外部环境产生影响．

以太坊智能合约运行在以太坊虚拟机（EVM）中．EVM 是一种沙箱环境，与外界隔离，因此恶意代码不会对外部产生影响．同时，以太坊设计了 gas 机制用来防止恶意代码占用过多计算资源与区块链存储资源．智能合约程序每运行一步会花费一定量的 gas，每修改区块链中的数据，也会按照大小花费一定量 gas．

通过以上测评，表 8 总结了智能合约计算层在每个测评项的达标情况：区块链可以满足测评项①②④，测评项③未达标．由于共识层可以达成共识结果一致性，因此共识层之上的合约层可以验证数据的完整性（测评项⑤达标），但区块链中没有通过密码技术对数据进行加密，因此无法保证数据保密性（测评项⑥未达标）．

7　区块链系统测评结果

本文结合网络安全等级保护 2.0 版本三级通用要求中的应用与数据安全层面控制点，针对区块链在对等网络、分布式账本、共识机制方面提出了评估要求，并结合评估项对三种区块链系统（比特币、以太坊、超级账本）进行了测评，如表 10 所示．由综合测评结果可知，比特币和以太坊的测评达标项同为 19 项，超级账本则为 22 项；超级账本在节点接入控制、网络节点动态监测、账本访问控制三项测评中更加优秀．

综上所述，区块链系统在等保 2.0 三级应用与数据层控制点的测评结果总结如下：

（1）达到等级保护三级要求的测评项为：软件

表 10 区块链系统测评结果总结

Table 10 Summary of evaluation results of blockchain system

	类别 Categories	测评项 Items	达标 √/× 比特币 Bitcoin	以太坊 Ethereum	超级账本 Hyperledger
分布式对等网络测评 Distributed P2P network assessment	软件容错 Software fault tolerance	自我保护与自适应 Self-protection and self-adaptation	√	√	√
	资源控制 Resource control	并发连接限制 Concurrent connection restriction	√	√	√
		连接超时限制 Connection timeout limit	√	√	√
	身份鉴别 Identification	节点接入控制 Node link control	×	×	√
分布式对等网络测评 Distributed P2P network assessment	数据完整性 Data integrity	单播通信防篡改 Anti-tampering of unicast	×	×	×
		广播通信防篡改 Multicast communication tamper-proof	×	×	×
		转发通信防篡改 Forwarding communication tamper-proof	×	×	×
	安全审计 Security audit	网络状态获取更新 Network status get update	×	×	√
		网络节点动态监测 Network node dynamic monitoring	√	√	√
分布式账本测评 Distributed ledgers assessment	软件容错 Software fault tolerance	账本格式规范性 Standardization of ledger	√	√	√
	访问控制 Access control	账本访问控制 Ledger access control	×	×	√
	数据完整性 Data integrity	存储完整性 Storage integrity	√	√	√
	数据保密性 Data confidentiality	存储保密性 Storage confidentiality	×	×	×
	账本功能 Ledger function	数据抗抵赖 Data non-repudiation	√	√	√
		账本数据同步 Ledger data synchronization	√	√	√
		账本数据幂等 Ledger data idempotence	√	√	√
共识机制测评 Consensus mechanism assessment	资源控制 Resource control	共识资源测评 Consensus Resource Control	√	√	√
	备份与恢复 Backup and recovery	实时备份 Real-time backup	√	√	√
		系统热冗余 System hot redundancy	√	√	√
	共识效果 Consensus effect	共识容错性 Consensus fault tolerance	√	√	√
		共识有效性 Consensus effectiveness	√	√	√
		共识结果一致性 Consensus Consistency	√	√	√
合约计算层测评 Contract computing layer assessment	身份鉴别 Identification	执行身份验证 Performing entity authentication	√	√	√
	安全审计 Security audit	行为事件审计 Behavioral event audit	√	√	√
		审计记录 Audit records	×	×	×
	恶意代码防范 Malicious code protection	免受恶意代码攻击 Protection from malicious code	√	√	√
	数据完整性 Data integrity	传输完整性 Transmission integrity	√	√	√
	数据保密性 Data confidentiality	传输保密性 Transmission confidentiality	×	×	×
统计 Statistics	达标个数 Number of qualified items		19 Nineteen	19 Nineteen	22 Twenty-two

容错、备份与恢复、资源控制和恶意代码防范；

（2）未达到等级保护三级要求的测评项有：身份鉴别、访问控制、数据完整性、数据保密性和安全审计.

此外，本文对区块链系统在分布式账本的测评上新增了数据抗抵赖、账本数据同步和账本数据幂三个测评项；在共识机制的测评中提出了共识容错性、共识有效性和共识结果一致性测评要求，区块链系统均能达标. 由此可见，为满足等级保护三级测评标准，区块链技术仍有待提高.

8　总结与展望

本文依据等保第三级的应用和数据安全要求，给出了区块链系统中对等网络、分布式账本、共识机制和智能合约等核心技术的具体测评要求及实施方案，并对比特币、以太坊、超级账本进行了评估和对比，结果表明区块链系统在软件容错、资源控制和备份与恢复等方面满足等保要求，而在安全审计、身份鉴别、数据完整性等方面则有待进一步改进. 根据《中华人民共和国网络安全法》、《GB/T 22239—2019 信息安全技术 网络安全等级保护基本要求》等的要求，近年来很多关键性计算机技术都已经进行了等级保护测评标准的制定，而区块链等级保护的测评也势在必行，建设满足我国现实需求和中国特色的区块链技术是区块链发展的必然要求，区块链等级保护标准的制定也将为我国信息基础构架和社会信息系统合规管理提供支持.

参　考　文　献

[1] Nakamoto S, Bitcoin: a peer-to-peer electronic cash system[J/OL]. *Bitcoin Online* (2008-10-31)[2019-12-17] https://bitcoin.org/bitcoin.pdf

[2] Mettler M. Blockchain technology in healthcare: the revolution starts here // 2016 *IEEE 18th International Conference on e-Health Networking, Applications and Services* (*Healthcom*). Munich, 2016: 1

[3] An R, He D B, Zhang Y R, et al. The design of an anti-counterfeiting system based on blockchain. *J Cryptol Res*, 2017, 4(2): 199
（安瑞, 何德彪, 张韵茹, 等. 基于区块链技术的防伪系统的设计与实现. 密码学报, 2017, 4(2): 199）

[4] Tian H B, He J J, Fu L Q. A privacy preserving fair contract signing protocol based on block chains. *J Cryptologic Res*, 2017, 4(2): 187
（田海博, 何杰杰, 付利青. 基于公开区块链的隐私保护公平合同签署协议. 密码学报, 2017, 4(2): 187）

[5] Wijaya D A. Extending asset management system functionality in bitcoin platform // 2016 *International Conference on Computer, Control, Informatics and its Applications* (*IC3INA*). Tangerang, 2016: 97

[6] Tian Z H, Wang B L, Ye Z W, et al. The survey of information system security classified protection // *Electrical Engineering and Control*. Springer, Berlin, Heidelberg, 2011: 975

[7] Xia B. *Cybersecurity Law and Classified Protection of Cybersecurity* 2.0. Beijing: Publishing House of Electronics Industry, 2017
（夏冰. 网络安全法和网络安全等级保护2.0. 北京: 电子工业出版社, 2017）

[8] Guo Q Q. *Book of Cybersecurity Law and Classified Protection of Cybersecurity*. Beijing: Publishing House of Electronics Industry, 2018
（郭启全. 网络安全法与网络安全等级保护制度培训教程(2018版). 北京: 电子工业出版社, 2018）

[9] Deng R Y, Yu M L, Ding Y, et al. Safeguarding cyberspace security by law and building a cyber power——Interpretation of cybersecurity law of the People's Republic of China and National cyberspace security strategy. *E-Government*, 2017(02): 2
（邓若伊, 余梦珑, 丁艺, 等. 以法制保障网络空间安全构筑网络强国——《网络安全法》和《国家网络空间安全战略》解读. 电子政务, 2017(02): 2）

[10] Zhu J F, Zhao Y J, Yang H, et al. The evolution of classified protection idea. *Inform Security Commun Privacy*, 2011(4): 70
（朱继锋, 赵英杰, 杨贺, 等. 等级保护思想的演化. 信息安全与通信保密, 2011(4): 70）

[11] Ma L, Zhu G B, Lu L. Baseline for classified protection of cybersecurity (GB/T 22239—2019) standard interpretation. *Netinfo Security*, 2019, 19(2): 77
（马力, 祝国邦, 陆磊.《网络安全等级保护基本要求》(GB/T 22239—2019)标准解读. 信息网络安全, 2019, 19(2): 77）

[12] Gao Y, Huang X K, Li X W. Cloud computing security requirements and measurement practices in the classified protection 2.0Era. *J Inform Security Res*, 2018, 4(11): 987
（高员, 黄晓昆, 李秀伟. 等保2.0时代云计算安全要求及测评实践. 信息安全研究, 2018, 4(11): 987）

[13] Huang Z, Chen X, Wen S H, et al. Security testing frame and technology of big data. *Commun Technol*, 2017, 50(8): 1810
（黄钟, 陈肖, 文书豪, 等. 大数据安全测评框架和技术研究. 通信技术, 2017, 50(8): 1810）

[14] Wang N, Liu Z J. The internet of things security protection level of the research. *Netinfo Security*, 2011(6): 5

(王宁, 刘志军. 物联网安全中的等级保护研究. 信息网络安全, 2011(6): 5)

[15] Wood G. Ethereum: a secure decentralised generalised transaction ledger. *Ethereum Project Yellow Paper*, 2014, 151: 1

[16] Androulaki E, Barger A, Bortnikov V, et al. Hyperledger fabric: A distributed operating system for permissioned Blockchains // *Proceedings of the Thirteenth EuroSys Conference* (*EuroSys* 2018). Porto, 2018: 1

[17] Kosba A, Miller A, Shi E, et al. Hawk: The blockchain model of cryptography and privacy-preserving smart contracts // 2016 *IEEE Symposium on Security and Privacy* (*SP*). San Jose, 2016: 839

[18] Zhu Y, Gan G H, Deng D, et al. Security architecture and key technologies of blockchain. *J Inform Security Res*, 2016, 2(12): 1090
(朱岩, 甘国华, 邓迪, 等. 区块链关键技术中的安全性研究. 信息安全研究, 2016, 2(12): 1090)

[19] Antonopoulos A M. *Mastering Bitcoin: Unlocking Digital Cryptocurrencies*. California: O'Reilly Media, Inc, 2014

[20] Ben Mariem S, Casas P, Donnet B. Vivisecting blockchain P2P networks: Unveiling the bitcoin IP network // *ACM CoNEXT Student Workshop*. Crete, 2018

[21] Gencer A E, Basu S, Eyal I, et al. Decentralization in bitcoin and ethereum networks // *International Conference on Financial Cryptography and Data Security*. Berlin, 2018: 439

[22] Donet J A D, Pérez-Sola C, Herrera-Joancomartí J. The bitcoin P2P network // *Proceedings of the* 1*st Workshop on Bitcoin Research* (*in Assocation with Financial Crypto* 14). Berlin, 2014: 87

[23] Du M X, Ma X F, Zhang Z, et al. A review on consensus algorithm of blockchain // 2017 *IEEE International Conference on Systems, Man, and Cybernetics* (*SMC*). Banff, 2017: 2567

[24] Gramoli V. From blockchain consensus back to byzantine consensus. *Future Generation Comput Syst*, 2020, 107: 760

[25] Nguyen G T, Kim K. A survey about consensus algorithms used in blockchain. *J Inform Process Syst*, 2018, 14(1): 101

[26] Fullmer D, Morse A S. Analysis of difficulty control in bitcoin and proof-of-work blockchains // 2018 *IEEE Conference on Decision and Control* (*CDC*). Miami Beach, 2018: 5988

[27] Taylor D. *An Analysis of Bitcoin and the Proof of Work Protocols Energy Consumption, Growth, Impact and Sustainability* [Dissertation]. Glasgow: University of Strathclyde, 2018

[28] Castro M, Liskov B. Practical Byzantine fault tolerance // *Proceedings of the Third USENIX Symposium on Operating Systems Design and Implementation* (*OSDI*). New Orleans, 1999: 173

[29] Borran F, Schiper A. A leader-free byzantine consensus algorithm // *International Conference on Distributed Computing and Networking*. Berlin, 2010: 67

[30] Saleh, F. Blockchain without waste: proof-of-stake. *Economics Networks eJ*. http://dx.doi.org/10.2139/ssrn.3183935

[31] Bach L M, Mihaljevic B, Zagar M. Comparative analysis of blockchain consensus algorithms // 2018 41*st International Convention on Information and Communication Technology, Electronics and Microelectronics* (*MIPRO*). Opatija, 2018: 1545.

[32] Kiayias A, Koutsoupias E, Kyropoulou M, et al. Blockchain mining games // *Proceedings of the* 2016 *ACM Conference on Economics and Computation*. ACM, 2016: 365

[33] Levine M. Scientific method and the adversary model: Some preliminary thoughts. *Am Psychologist*, 1974, 29(9): 661

[34] Dey S. A proof of work: Securing majority-attack in blockchain using machine learning and algorithmic game theory. *Int J Wireless Microwave Technol*, 2018, 8(5): 1

[35] Heusser J. SAT solving-An alternative to brute force bitcoin mining[J/OL]. *Technical Report*(2013-02-03)[2019-12-17]. https://jheusser.github.io/2013/02/03/satcoin.html

[36] Eyal I, Sirer E G. Majority is not enough: Bitcoin mining is vulnerable. *Commun ACM*, 2018, 61(7): 95

[37] Heilman E, Kendler A, Zohar A, et al. Eclipse attacks on bitcoin's peer-to-peer network// *Proceedings of the* 24*th USENIX Conference on Security Symposium* (*SEC'*15). Washington D.C., 2015: 129

[38] Douceur J R. The sybil attack // *International Workshop on Peer-to-Peer Systems*. Berlin, 2002: 251

[39] Chohan, Usman W. The double spending problem and cryptocurrencies. *Inf Syst Economics eJ*, http://dx.doi.org/10.2139/ssrn.3090174

[40] Decker C, Wattenhofer R. Information propagation in the bitcoin network // *IEEE P2P* 2013 *Proceedings*. Trento, 2013: 1

[41] Decker C, Wattenhofer R. Bitcoin transaction malleability and MtGox // 19*th European Symposium on Research in Computer Security*. Wroclaw, 2014: 313

[42] Zhu Y, Guo R Q, Gan G H, et al. Interactive incontestable signature for transactions confirmation in bitcoin blockchain // 2016 *IEEE* 40*th Annual Computer Software and Applications Conference* (*COMPSAC*). Atlanta, 2016: 443

[43] Gervais A, Karame G O, Wüst K, et al. On the security and performance of proof of work blockchains // *Proceedings of the* 2016 *ACM SIGSAC Cnference on Computer and Communications Security*. New York, 2016: 3

[44] Sekiguchi K, Chiba M, Kashima M. *The Securities Settlement System and Distributed Ledger Technology*. Bank of Japan Research Laboratory Series, 2018

[45] Bowden R, Keeler H P, Krzesinski A E, et al. Block arrivals in the Bitcoin blockchain[J/OL]. *arXiv preprint*(2018-01-23)[2019-12-17]. https://arxiv.org/pdf/1801.07447.pdf

[46] Son K T, Thang N T, Dong T M, et al. Blockchain technology for data entirety. *Sci Research*, 2019, 6(6): 68

[47] Merkle R C. Protocols for public key cryptosystems // 1980 *IEEE Symposium on Security and Privacy*. Oakland, 1980: 122

[48] Szydlo M. Merkle tree traversal in log space and time // *International Conference on the Theory and Applications of Cryptographic Techniques*. Interlaken, 2004: 541

[49] Jakobsson M, Leighton T, Micali S, et al. Fractal Merkle tree representation and traversal // *Cryptographers' Track at the RSA Conference*. San Francisco, 2003: 314

[50] Delgado-Segura S, Pérez-Solà C, Herrera-Joancomartí J, et al. Bitcoin private key locked transactions. *Inform Process Lett*, 2018, 140: 37

[51] Stanciu N. Importance of event log management to ensure information system security. *Metalurgia Int*, 2013, 18(2): 144

[52] Kreps J, Narkhede N, Rao J. Kafka: a distributed messaging system for log processing // *Proceedings of the NetDB*. Athens, 2011

[53] Aniello L, Baldoni R, Gaetani E, et al. A prototype evaluation of a tamper-resistant high performance blockchain-based transaction log for a distributed database // 2017 13*th European Dependable Computing Conference* (*EDCC*). Geneva, 2017: 151