项目编号：2020YFB1005500 密级：公开

**国家重点研发计划项目** 2021 **年度**

**课题技术进展报告**

课题名称：

项目名称： “以链治链”的监管架构与关键技术研究

所属专项： 云计算和大数据

项目管理专业机构：科学技术部高技术研究发展中心

执行期限：  2020年11月 至 2023年 10月

2021年10月18日

[科技报告编号] 公开范围[延迟期限]

科 技 报 告

报 告 名 称：\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

支 持 渠 道：\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

编 制 单 位：\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

编 制 时 间：\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

编写说明

一、课题负责人负责组织研究人员编写科技报告，并按相关计划管理的要求审核和提交。

二、科技报告一般包括封面、基本信息表、目录、插图清单、附表清单、正文、附录和参考文献等部分。

三、报告内容应客观真实、准确完整、层次清晰。本领域的专业读者依据这些描述能重复调查研究过程、评议研究结果。

科技报告基本信息表

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 1.报告名称 | | 中文（不超过40字）：XXX课题年度报告（2021年） | | | | | | |
| 英文：Annual Technology Report on XXXX（2021） | | | | | | |
| 2.报告作者及单位 | | 中文： | | | | | | |
| 英文： | | | | | | |
| 3.使用范围（公开和延期公开，延期公开需明确延期时间）  原因： | | | | | | 4.编制时间（YYYY-MM-DD）  2021-10-18 | | |
| 5.报告编号（单位机构代码+课题编号+/顺序号，XXXXXXXXX -- NNNNUUNNNNNN/NN） | | | | | | | | |
| 6.备注（须注明的特殊事项，如延期公开报告的查询权限、免责声明、报告与其它工作或成果的联系等） | | | | | | | | |
| 7. 摘 要 | 中文（600字左右）： | | | | | | | |
| 英文（不超过2500个字符）： | | | | | | | |
| 8. 关 键 词 | 中文（3-8个，以分号隔开）： | | | | | | | |
| 英文（3-8个，以分号隔开）： | | | | | | | |
| 9.支持渠道 | 项目名称 | | |  | | | | |
| 主管部门 | | |  | | | 计划名称 |  |
| 项目编号 | | |  | | | 应用领域 |  |
| 承担单位 | | |  | | | | |
| 合作单位（不超过5家） | | |  | | | | |
| 总经费（万元） | | |  | | | 国拨经费（万元） |  |
| 项目负责人 | | |  | | | | |
| 起始日期 | | |  | | | 截止日期 |  |
| 10.联系人 | 姓名 | |  | 单位 |  | | | |
| 电话 | |  | E-Mail |  | | | |

**目 录**

# 插图清单

# 附表清单

# 引言

课题X总的研究目标是。

本年度，课题的研究内容主要包括以下2个方面。（各任务描述各自合同规定的阶段或年度研究任务的目标、内容、方法等要点。）

1. 协助课题牵头单位构建“以链治链”跨链监管架构；
2. 进行加密数据搜索研究

形成《课题年度技术进展报告》1篇。

# 研究概述

## 研究背景及意义

。

## 课题三与其它课题的关系

。

## 课题三研究内容

### 拟解决的关键科学与技术问题

在大规模区块链业务中，用户数量大、交易模式多，分布式监管难以审计跨链的密态内容。链上数据持续增加对访问模式和搜索模式提出了更高的要求。本研究旨在不侵犯数据隐私内容的前提下完成数据的精准审计，设计支持链码的数据加密方案，转化目标问题，在加密数据上完成复杂计算任务的求解。

### 拟开展的主要研究内容

设计支持链码的同态加密、差分隐私等数据加密方案，抽取数据审计的共性计算操作，构建合规属性集，在加密数据上完成复杂计算任务的近似求解，完成具有自适应安全等级或多关键字的密文搜索与查询等技术研究，并开展加密数据统计分析研究。

针对基于差分隐私的数据保护方案，设计链上数据的前期去隐私化处理机制，实现支持噪声动态注入的链上数据统计分析；基于混淆电路的隐私保护方案，完成安全计算协议自适应生成方案。

## 研究技术路线（任务技术路线）（文字+至少1张图）

本研究的目标是结合智能合约的底层特点，设计支持链码的同态加密、差分隐私等数据加密方案，抽取数据审计的共性计算操作，构建合规属性集，对目标问题进行相应转化，在加密数据上完成复杂计算任务的近似求解；利用混淆电路自动化生成安全计算协议，在不侵犯数据隐私内容的前提下完成数据的精准审计。

如图1.1是本研究的技术路线图，研究成果包括数据加密方案，加密数据近似求解，去隐私化机制和密文搜索、分析与查询。数据加密方案通过同态加密和差分隐私实现，支持链码。基于差分隐私的数据保护方案是链上数据去隐私化处理机制的基础，这种处理机制支持噪声动态注入的链上数据统计分析。提取链上数据审计的共性计算操作，构建合规属性集，进行加密数据的复杂计算任务的近似求解。

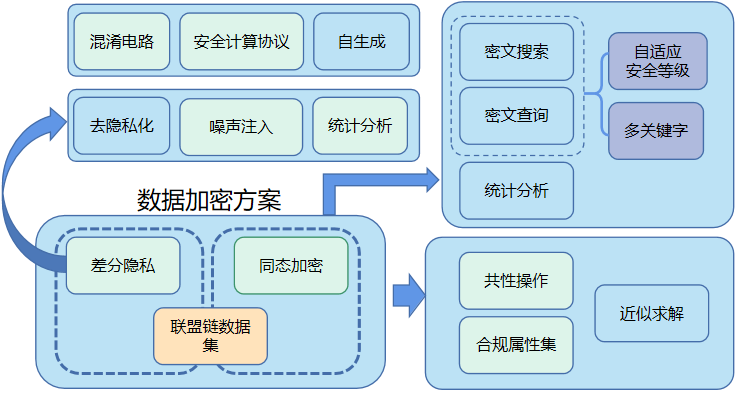


图1.1 密态内容审计方法研究技术路线

# 2.BOSSA：一种可检索证明和复制证明的去中心化系统

## 2.1现有系统存在的问题

云计算作为一种新的计算范式，为普通用户提供了一种便捷的途径使用强大的计算资源和存储资源。用户可以将其数据外包给云服务提供商，以摆脱复杂的本地数据管理。虽然前景看好，但将数据外包给远程服务器会引起严重的安全问题。这种行为剥夺了数据所有者的物理控制权。关键问题之一是确保数据的正确性。恶意服务器可能为了节省存储资源而丢弃很少访问的数据，或者为了维护声誉而故意掩盖数据丢失事故。此外，云服务商通常将数据与几个副本存储在一起，以确保高可靠性[1]，如果发送数据丢失，它在其服务级别协议(SLA)[2]中承担有限责任。最近腾讯云[3]发生了数据安全的事故，其他的云服务[4]也表示云服务是不能完全可信的。

可检索证明[5]，[6]，[7]，[8]，[9]，[10]，[11]，[12]以及复制证明[13]，[14]，[15]，[16]，[17]，[18]，[19]是两种典型的加密方法，允许服务器证明原始文件以及所有副本都正确存储在服务器上。可检索证明和复制证明的解决方案可以让用户不必时刻在线进行数据完整性和可检索的审计，但是这些方案在很大程度上依赖于半可信的第三方审计(Third Party Audit，TPA)来执行公共验证。但是这种方法有以下两个缺点:

（1）合谋攻击（Collusion Attack）：一般文献设定TPA不会和云服务商S合谋。但是在实际中，这种强假设会轻易被利益驱动所破坏，一旦云服务商和TPA合谋后可以轻易地给出假的数据证明。而且，从用户的角度看，这种合谋是不可感知的。

（2）腐化攻击（Corruption Attack）：持续在线的TPA容易受到未知意外的单点故障攻击，如地区停电、DDoS黑客攻击等。

我们将这些安全问题归因于TPA过于中心化的控制。构建一个分布式的审计框架可以从根本上解决上述问题。区块链由于其不可篡改和不可否认的特性，在电子投票[20]、拍卖[21]和公平交易[22]等领域被广泛用于取代第三方。用区块链取代TPA使得用户可以跟踪整个审计过程。因此，用户能够验证证据检索和备份的每一步。此外，区块链的去中心化提高了单点故障的容忍度。区块链是抵御共谋攻击和腐化攻击有前景的解决方案。此外，对于旨在保证数据可靠性的数据副本服务，云服务商可以故意删除副本以节省存储资源，而无需担心被监控到。受分布式存储网络(Distributed Storage Network，DSN)的启发，分布式存储网络试图构建一个点到点网络，允许单点买卖空闲存储资源，分布式数据备份使攻击者更难做出恶意行为，因为数据传输、存储和删除的每一步都是记录和可跟踪的。

## 2.2 BOSSA方法及系统详细技术方案

我们提出了基于区块链的外包存储和审计(BOSSA)方案，这是一个可检索证明和复制证明的通用框架。BOSSA 将原始数据单独存储在服务器上，并将相应的副本存储在位于区块链的分布式网络的节点(也称为BOSSA中的农民)上，并通过智能合约检查它们的完整性。BOSSA可以自然地防御共谋攻击和腐化攻击，同时提供可视化的数据复制。BOSSA并不深度依赖像[23]这样的特定共识机制，这使得BOSSA可以部署在图灵完备的区块链的离线网络上[24]，[25]。BOSSA解决了以下三个挑战：

（1）时间限制证明：简单地将现有的可检索证明方案与区块链相结合无法实现我们的预期目标，区块链只支持简单的功能。区块链不能主动提出审计，只能根据收到的交易被动做出反应。该属性允许对手逃避审计。为了防止这种消极行为，我们利用区块以近似固定的速率上链的特性，提出了一个时间限制证明，迫使云服务商和农民节点提供数据可用性证明。

（2）激励机制：BOSSA组织农民节点存储用户数据的副本。但是农民节点并不完全可信，可能会随意离开网络，导致副本丢失，破坏副本的可靠性。为了解决这个问题，我们设计了一个激励机制来激励在必要时刻提供数据副本的节点。我们定义了一种奖励机制，在这种机制下，如果农民能够定期提供备份数据的有效证据，他们就会得到定期奖励。同时，部分奖励被暂时冻结，直到农民承诺的服务期满，这一设计在动机上阻碍了农民离开网络。为了进一步激励农民节点共享数据副本，我们定义了一个称为贡献率的度量，并将农民节点冻结的奖励与贡献率联系起来，只有贡献率为100%的农民才能得到所有的冻结奖励。

（3）隐私保护：像Ethereum这样的区块链平台大多以明文存储交易，任何参与者都能够检索交易的信息，包括智能合约的输入、中间计算结果等。对于一个建立在原生区块链网络的审计系统，区块链的开放性使对手能够记录证据并恢复原始数据。为了防止这种隐私泄露，我们结合了隐私增强技术来生成证明，同时确保它们的正确性。

### 2.2.1系统模型

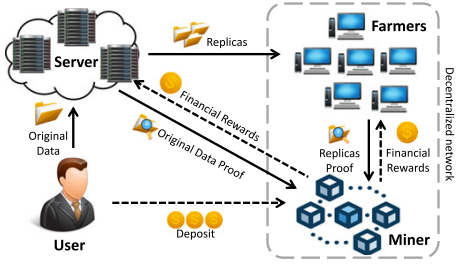


图2.1 BOSSA系统模型

如图2.1是BOSSA的系统模型。系统中包含以下实体：云服务商S，云服务用户U，分布式网络的两类节点：矿工M和农民F。矿工维护整个区块链网络，并执行智能合约。农民是加入到区块链网络中出租空闲存储资源的节点。在本系统中，服务商从用户中获得原始数据，用于数据分析，比如预测和推荐。为了节省服务商的存储资源，服务商将数据副本外包给农民，利用农民的空闲存储资源存储数据备份。用户委托矿工分别审计服务商的原始数据和矿工的备份数据。

BOSSA的核心功能流程如图2.2所示。

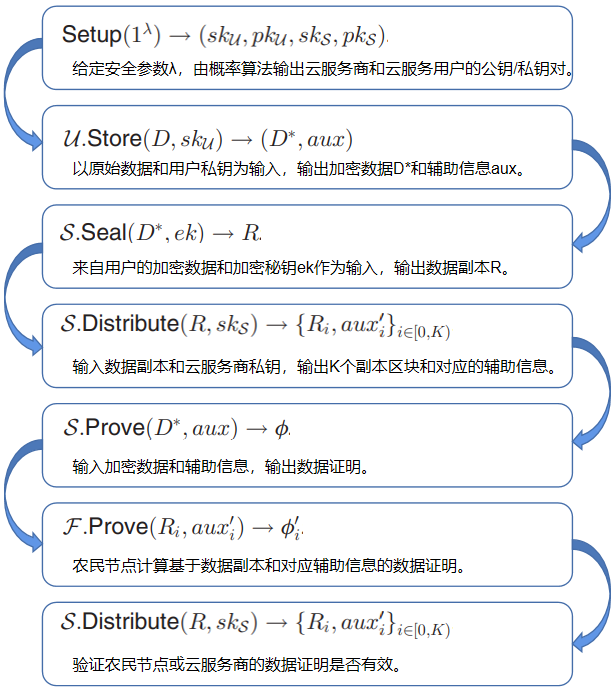


图2.2 BOSSA系统核心功能流程

### 2.2.2威胁模型

根据以前的工作[13]，[14]我们以理性的云服务商为研究对象，其行为大多数时候遵守规则，除非恶意行为能带来更多的收益，例如删除很少访问的数据块以节省存储资源。区块链网络可以视为一个可信的公共实体。区块链的大部分算力由诚实的矿工掌握，他们会如实地执行智能合约[46]。区块链网络中的任何节点都可以了解网络内部状态和区块链收到的消息。

来自分布式网络的农民节点出租他们的空闲磁盘空间来存储云服务用户的数据副本。我们假设有大量的农民节点，他们的数量足以存储所有用户的副本。如果农民失去了储存数据副本的兴趣，他们可能会不负责任地离开网络。因此，有必要保证副本的可用性，激励农民诚实地保存用户数据副本直到服务器满。

### 2.2.3 系统构建

BOSSA系统为数据完整性审计和数据备份提供了一个新的范例，它使用区块链网络定期审计服务器并存储数据副本。具体来说，为了确保服务器正确存储数据，BOSSA采用了传统的PoR方案，但用区块链代替了TPA。由于区块链只能被动地接收事务，不能向服务器发出质询，因此限时证明用于强制服务器主动提供证明。此外，BOSSA的另一个重要组成部分是在区块链网络中的节点(农民)之间存储副本。向农民节点发送数据备份会产生数据隐私、可靠性和可检索性安全担忧。在BOSSA中，服务器对数据副本进行编码和加密，以保证隐私和可靠性，激励证明鼓励农民节点保持了副本的完整性。此外，农民因提供有效数据证据(诚实地存储数据副本)，他们的回报取决于他们是否能在用户需要的时提供数据副本，这是通过贡献率来衡量的。100%贡献率的农民，可以取回自己所有的报酬。

### 2.2.4 审计算法

审计算法的设计和实现使用了一些密码学工具。如图2.2是BOSSA的功能流程。

1. 在Setup阶段，用户使用椭圆曲线加密算法，初始化秘钥对，并生成云服务商的密钥对。云服务商密钥对将随外包数据发送给云服务商。
2. 用户预处理数据后，再发送给云服务商。用户使用纠删码对原始数据编码，得到处理后的数据D\*。
3. 为保证数据副本的可用性，并保护用户隐私。需要对数据副本进行密封。如图2.3是对数据的密封示例。我们密封了22个区块中的22个（黄色区块和深灰色区块）。浅灰色区块为带有两个零填充的原始数据区块，暗灰色的区块由密封算法（Seal Algorithm）第一阶段生成，黄色区块由密封算法的第二阶段生成。我们省略了加密过程。这些数据的每一列都会外包给不同的农民节点。
4. 云服务商将过程（3）中的数据分为K块，生成不同的块副本和对应的辅助信息。并分发给不同的农民节点。
5. 云服务商和农民节点提供数据的可用性证明。

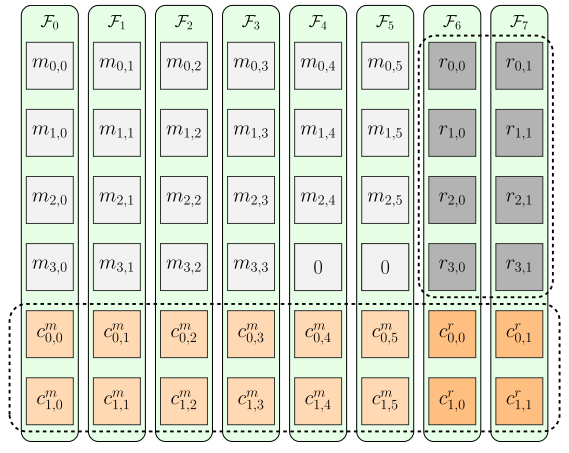


图2.3 数据密封示例

## 2.3本方法的优点

首先，本研究利用Block以近似固定的速率上链的特性，提出了一个时间限制证明，迫使云服务商和农民提供数据可用性的证明。以此解决恶意节点逃避审计的问题。

其次，设计了一个激励机制来激励农民为用户在任何时候提供数据检索服务。在这种机制下，如果农民能够定期提供数据备份的有效证据，就会得到定期奖励。同时，部分奖励被暂时冻结，直到农民服务期满。为了进一步激励农民共享数据副本，我们定义了一个称为贡献率的度量，并将农民的冻结奖励与贡献率联系起来，这样只有贡献率为 100%的农民才能取得所有的冻结奖励。

第三，Ethereum等区块链平台以明文存储交易数据，任何参与者都能够检索交易的信息，包括智能合约的输入、中间结果等。对于建立在原生区块链上的审计系统，区块链的开放性使攻击者能够记录证据并恢复原始数据。为了防止这种隐私泄露，我们结合了隐私增强技术来生成证明，并确保证明的正确性。

# 区块链网络安全保障：攻击与防御

## 问题现状

随着区块链的快速发展与普及，其潜在的安全漏洞逐渐暴露出来。2020 年 7 月底，西班牙加密货币交易平台 2gether 遭攻击，损失约140万美元[1]。最近，在以太经典（ETC, Ethereum classic）平台上爆发的一起51%攻击导致大约价值 560 万美元的加密货币被双倍消费[2]。由此可见，区块链技术的漏洞可能导致无法挽回的财产损失和隐私泄露。目前，国内研究者针对区块链安全问 题进行了系统的综述[3-6]，但这些工作与本文的侧 重点和覆盖面有所差别。例如，文献[3]侧重于宏观 层面的区块链技术发展；文献[5-6]侧重于介绍区 块链威胁和漏洞相关研究，没有详细调研针对区块 链威胁的具体防御措施。

## 研究内容

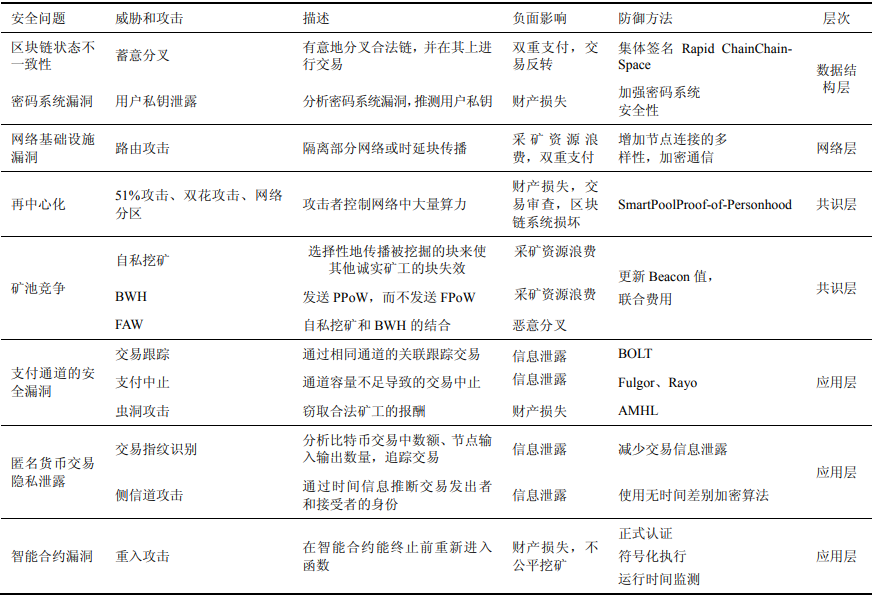
如表1，是区块链数据结构层、网络层、共识层、应用层面临的安全威胁。区块链的基本组成部分为区块。在交易过程中，不断有新的区块链接到区块链中，而链接过程存在区块链状态不一致和分叉的威胁。另外，区块链底层高度依赖密码算法，攻击者可以利用密码系统的漏洞造成用户私钥泄露，从而引发财产损失等安全问题。

在网络层，区块链网络的基础网络基础设施漏洞和自身 P2P 网络结构是引发安全问题的主要原因。

区块链的实现很大程度上得益于共识层的设计。在这一层中，区块链在一个分布式去中心化的账本上运行，链中的所有节点通过共识机制保持统一运行状态。目前，共识层中的大多数安全威胁都是随着矿池的出现而产生的。

在应用层，近期研究主要集中在提高性能和拓宽区块链系统的应用潜力上[7,8]，与之密切相关的安全问题包括支付通道的隐私和安全问题，匿名货币交易隐私泄露，智能合约漏洞等。

表1 区块链安全威胁和防御方法



本研究针对对于区块链潜在的安全问题，提出了对应的安全策略。

在数据层面，区块的不一致性会引起区块链结构分叉等问题，而保证一致性会影响到区块链系统的运行效率，从而削弱可伸缩性。然而，为提高性能而设计的新方案可能会面临更严重的不一致性问题。为了提高交易的一致性同时保证高吞吐量，Syta等[9]提出了一种可扩展的集体签名协议Cosi来提高交易的确认效率。另一个提高区块链吞吐量的解决方案是分片[10,11] 机制，它将处理交易的开销分割为多个较小的节点组。

在网络层，为了防止路由攻击，从部署的角度划分，可以实行短期和长期对策[12]。短期对策更容易部署，不需要对协议进行任何更改。如果节点所有者能增加节点连接的多样性，攻击将变得极其困难。从长远来看，对比特币通信进行加密可以防止信息泄露。

在共识层，为了解决共识协议（例如工作量证明或权益证明）的再集中化问题，Borge等[13]提出了全新的个人身份证明机制（PoP, proof-of-personhood）并设计了一种名为 PoPCoin 的加密货币。

在应用层，近年来，大量工作致力于分析和提升链下支付通道的安全性。但是如何在保证效率的情况下设计出匿名性好的加密货币系统是目前学术界和工业界的一大挑战。智能合约的安全从多个方面加强，包括自动形式化验证、字节码级别验证、时检测重入攻击等。

## 研究优势

本文调研关于区块链安全漏洞的最新进展外，并详细介绍了目前最先进的防御方法，系统地调研了区块链系统的安全性问题。作为一个集成框架，区块链系统可分为4层：数据结构层、网络层、共识层和应用层。本文从区块链系统结构角度出发，深入分析数据结构层、网络层、共识层和应用层的安全漏洞、攻击原理以及对应的防御措施。

## 参考文献

[1] GOGO J. European Bitcoin exchange hacked for $1.4 million, claims it cannot afford to repay users [EB/OL]. Bitcoin.com, 2020-08-04.

[2] HAIG S. 51% attack bleeds more than $5M from Ethereum classic [EB/OL]. Cointelegraph, 2020-08-06.

[3] 袁勇, 王飞跃. 区块链技术发展现状与展望[J]. 自动化学报, 2016, 42(4): 481-494.

[4] 祝烈煌, 高峰, 沈蒙, 等. 区块链隐私保护研究综述[J]. 计算机研究与发展, 2017, 54(10): 2170-2186.

[5] 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.

[6] 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): 8-19.

[7] DECKER C, WATTENHOFER R. A fast and scalable payment network with bitcoin duplex micropayment channels[C]//Symposium on Self-Stabilizing Systems. Berlin: Springer, 2015: 3-18.

[8] LUU L, NARAYANAN V, ZHENG C, et al. A secure sharding protocol for open blockchains[C]//Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security. New York: ACM Press, 2016: 17-30.

[9] SYTA E, TAMAS I, VISHER D, et al. Keeping authorities “honest or bust” with decentralized witness cosigning[C]//2016 IEEE Symposium on Security and Privacy. Piscataway: IEEE Press, 2016: 526-545.

[10] GAO S, LI Z, PENG Z, et al. Power adjusting and bribery racing: Novel mining attacks in the bitcoin system[C]//Proceedings of the 2019 ACM SIGSAC Conference on Computer and Communications Security. New York: ACM Press, 2019: 833-850.

[11] CORBETT J C, DEAN J, EPSTEIN M, et al. Spanner: Google’s globally distributed database[J]. ACM Transactions on Computer Systems, 2013, 31(3): 1-22.

[12] APOSTOLAKI M, ZOHAR A, VANBEVER L. Hijacking bitcoin: routing attacks on cryptocurrencies[C]//2017 IEEE Symposium on Security and Privacy. Piscataway: IEEE Press, 2017: 375-392.

[13] BORGE M, KOKORIS-KOGIAS E, JOVANOVIC P, et al. Proof-of-personhood: redemocratizing permissionless cryptocurrencies[C]//2017 IEEE European Symposium on Security and Privacy Workshops. Piscataway: IEEE Press, 2017: 23-26.