密码学报 ISSN 2095-7025 CN 10-1195/TN
Journal of Cryptologic Research, 2018, 5(5): 458–469

E-mail: jcr@cacrnet.org.cn
http://www.jcr.cacrnet.org.cn
Tel/Fax: +86-10-82789618

区块链技术专刊

区块链安全研究综述*

斯雪明[1], 徐蜜雪[2], 苑 超[2]

1. 复旦大学 计算机科学技术学院, 上海 201203
2. 信息工程大学 数学工程与先进计算国家重点实验室, 郑州 450001
通信作者: 徐蜜雪, E-mail: mixue_xu@163.com

摘 要: 区块链是一种去信任化的分布式新型计算范式, 是一种带激励的基于博弈论共识的分布式账本技术. 区块链的出现促进了信息互联网向价值互联网的转化, 加快了可编程货币、可编程金融和可编程社会的产生. 区块链对金融、物联网、征信等领域势必会产生革命性的影响, 在提高生产效率、降低生产成本以及保护数据安全等方面, 区块链将发挥重要的作用. 区块链对数据安全、网络安全将产生积极的影响, 同时区块链本身也面临着严重的安全问题, 受到研究者的广泛关注. 本文将分层介绍区块链的基本技术原理. 重点从算法、协议、使用、实现、系统的角度出发, 对区块链的技术存在的安全问题进行分模块介绍, 讨论区块链面临的安全问题的本质原因, 主要分析协议安全性中的共识算法问题、实现安全性中的智能合约问题、以及使用安全性中的数字货币交易所安全问题. 最后, 分析了现有区块链安全保护措施存在的缺陷, 给出了区块链安全问题的解决思路, 并明确了区块链安全的未来研究方向.

关键词: 区块链; 安全; 智能合约; 分布式系统; 共识算法

中图分类号: TP309.7 **文献标识码:** A DOI: 10.13868/j.cnki.jcr.000256

中文引用格式: 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.

英文引用格式: SI X M, XU M X, YUAN C. Survey on security of blockchain[J]. Journal of Cryptologic Research, 2018, 5(5): 458–469.

Survey on Security of Blockchain

SI Xue-Ming[1], XU Mi-Xue[2], YUAN Chao[2]

1. School of Computer Science, Fudan University, Shanghai 201203, China
2. State Key Laboratory of Mathematical Engineering and Advanced Computing, Information Engineering University, Zhengzhou 450001, China
Corresponding author: XU Mi-Xue, E-mail: mixue_xu@163.com

Abstract: Blockchain is a new type of distributed computing paradigm and is de-trusted. It is a distributed ledger technology (DLT) based on game theory consensus. The emergence of blockchain promotes the transformation of information Internet to value Internet and accelerates the generation of programmable currency, programmable finance and programmable society. The blockchain is bound to have a revolutionary impact on the fields of finance, Internet of Things, credit reporting, etc. In

* 基金项目: 国家自然科学基金创新研究群体科学基金 (61521003)
Foundation: Innovative Research Groups of the National Natural Science Foundation of China (61521003)
收稿日期: 2018-08-11 定稿日期: 2018-09-28

terms of improving production efficiency, reducing production costs, and protecting data security, the blockchain will play an important role. The blockchain will have a positive impact on data security and network security. Meanwhile, the blockchain itself is facing serious security problems, which has attracted extensive attention from researchers. This paper introduces the basic principle of blockchain in modules. Focusing on the algorithm, protocol, application, implementation, and system perspectives, this paper overviews the security problems of the blockchain technology and discusses the essential rationale for them. It mainly analyzes the consensus algorithms in the security of the protocol, the smart contracts in security of implementation, and security issues in digital currency exchanges in practical applications. The defects of existing blockchain security protection measures are analyzed, and the problem of blockchain security is given. Finally, the defects of existing protection measures to blockchain security problems are analyzed, some ideas toward the solutions are given, and the future research directions are clarified.

Key words: blockchain; security; smart contract; distributed system; consensus algorithm

1 前言

区块链起源于中本聪的论文 [1], 在论文中并没有直接提出 “blockchain” 这个词, 而是提到了 “a chain of block”. 2009 年诞生的比特币就是世界上第一个去中心化的数字加密货币, 这之后加密货币一词多指此类设计, 比特币是目前为止区块链最成功的应用, 目前已有上千种以区块链技术作为底层技术的加密货币, 其中的一些加密货币也受到了人们的认可, 例如莱特币、以太币 [2] 等等. 现存的加密货币大多由两种方式产生, 一种是在已有加密货币的基础上做改进, 这种方式中最有代表性的是在比特币基础上做硬分叉, 例如比特币现金 (BCH)、比特币黄金 (BCG) 等等. 另外一种方式就是完全原创的加密货币, 这种方式最有代表性的就是以太币、EOS [3]. 并且大多数的加密货币都有自己的特性, 例如达氏币 [4]、门罗币 [5]、零币 [6] 等以隐私保护为特性; EOS、ZIL [7] 等以交易速率为特性. 当然并不是所有的加密货币都对应着一条区块链, 真正有区块链的加密货币非常少, 大多数的加密货币都仅仅是有一个虚拟的概念. 区块链最开始的应用领域仅仅局限在加密货币, 后来逐渐向更多的金融领域拓展. 随着 2013 年以太坊的诞生, 区块链的应用领域逐渐向其它方面拓展, 其中智能合约与区块链的结合起到了主要的作用. 以太坊的应用中, 以 Cryptokitties 为代表的区块链游戏和发行 TOKEN 是最有代表性的, 然而受到交易速率以及隐私保护方面缺陷的影响, 以太坊的现实应用仍然比较局限. 2015 年, Hyperledger 项目推出, 其中以 IBM 为主要贡献者的 Fabric 项目受到了大家的广泛认可. Fabric 考虑到现实的应用环境, 牺牲了部分去中心化的特性, 在隐私保护与交易速率方面基本满足现实应用需求.

目前区块链的应用领域已经十分广泛, 2018 年由工业和信息化部主编的《2018 年中国区块链产业白皮书》中提到了供应链金融、物联网等 22 个重点应用领域. 当然区块链的应用领域并不仅仅局限在这 22 个领域, 任何高价值数据的管理、流通与共享都可以用区块链. 另外区块链在数据安全、网络安全方面也起到重要的作用. 美国国防部正在尝试利用区块链技术创建一个黑客无法入侵的安全信息服务系统, 北约也在探索使用区块链技术开发下一代军事系统, 以实现北约网络防御平台的现代化, 我军也在积极探索区块链在军事领域的应用价值. 区块链在越来越多的重要场景中被应用, 在这些场景中安全性是非常重要的, 但是目前区块链本身存在严重的安全问题. 从 2016 年的 “The DAO” 事件开始, 区块链上智能合约的安全问题层出不穷. 据不完全统计, 从 2011 年到 2018 年 4 月份, 区块链安全事件中, 共识机制安全事件造成的损失达 3100 万美元, 矿工安全事件损失的金额达 6328 美元, 普通用户安全事件造成的损失达 1.73 亿美元, 智能合约安全事件造成的损失达 12.4 亿美元, 交易平台安全事件造成的损失达 13.44 亿美元, 其他安全事件造成的损失达 1260 万美元.

本文第 2 节将介绍区块链的基本技术原理, 第 3 节对区块链安全的背景知识进行介绍, 主要对区块链安全进行分类, 分为算法安全、协议安全、实现安全、使用安全和系统安全, 并将区块链安全分类与区块链基础架构进行对应. 第 4 节将按照第 3 节中对区块链安全的分类分别对区块链安全问题进行分析. 第 5 节将针对第 4 节中的区块链安全分析讨论并给出相应的区块链安全应对机制以及未来研究方向. 第 6 节

将对全文进行总结.

2 区块链基础技术原理

区块链起源于比特币, 比特币是最简单也是最典型的区块链架构. 后期的区块链也基本延续了比特币的基础架构, 主要由数据层、网络层、共识层、激励层、合约层和应用层构成. 但是随着区块链的发展, 区块链的基础架构已经不完全按照这 6 个模块构建, 一些传统的模块已经被弱化, 甚至被丢弃, 同时一些新的模块也被采用. 例如, 以 Fabric 为代表的联盟链缺少了激励模块, 而增加了相应的身份认证模块; 以 IOTA [8] 和 Byteball [9] 为代表的有向无环图 (directed acyclic graph, DAG) 放弃了传统的单链模式, 采用了图的交易结构. 根据目前区块链的发展趋势, 将区块链的技术框架分为 4 个模块, 具体如图1所示.

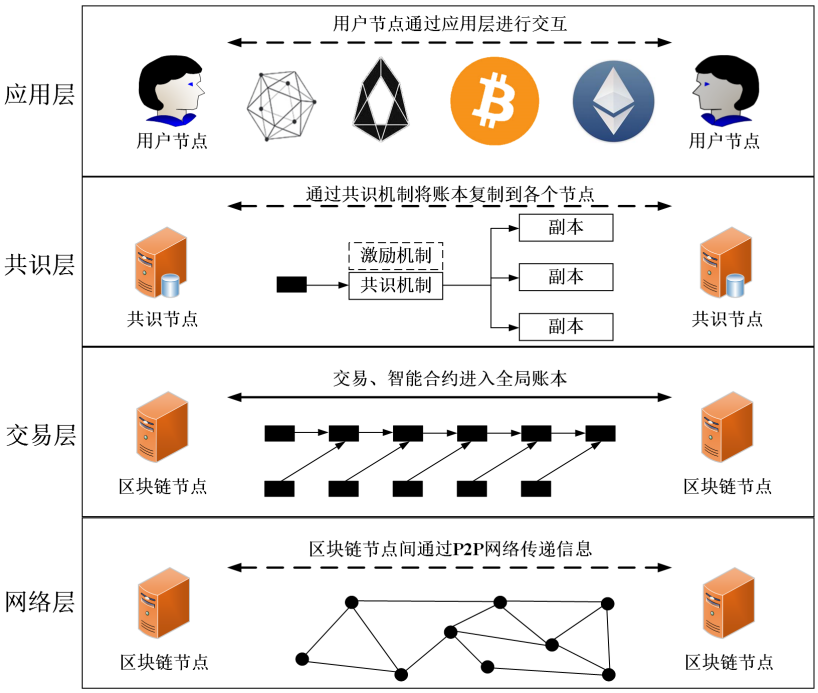

图 1 区块链技术架构

Figure 1 Architecture of blockchain

2.1 网络层

网络层负责区块链节点之间的通信, 主要包括区块链网络的组网方式和区块链节点之间的通信机制. 在组网方式上, 区块链采用对等网络 (peer-to-peer networking, P2P) 的组网技术, 具有去中心化的特性. 不同的区块链节点分布在不同的物理位置, 且所有节点的关系平等, 不存在中心权威节点. 目前规模最大的区块链网络是比特币, 近一年可访问的比特币节点数量平均为 10 589 个, 主要来自美国、德国、中国、法国等国家.

P2P 通信是区块链中一切活动的前提, 根据结构关系可以将 P2P 系统细分为四种拓扑形式 [10]:

(1) 中心化拓扑, 即存在一个中心节点保存了其他所有节点的索引信息, 索引信息一般包括节点 IP 地址、端口、节点资源等. 由于去中心的要求, 目前区块链不会使用中心化拓扑的 P2P 网络.

(2) 全分布式非结构化拓扑, 移除了中心节点, 在 P2P 节点之间建立随机网络, 就是在一个新加入节点和 P2P 网络中的某些节点间随机建立连接通道, 从而形成一个随机的拓扑结构, 比较典型的是 Gnutella. 比特币也采用的是类似的网络结构, 但是, 比特币通常使用像 Torrent Tracker 的 IRC 通道来找到连接到节点的节点.

(3) 全分布式结构化拓扑的 P2P 网络主要是采用分布式散列表 (distributed hash table) 组织网络, 所以也称作 DHT 网络.

(4) 半分布式拓扑吸取了中心化结构和全分布式非结构化拓扑的优点, 选择性能较高的结点作为超级节点, 超级节点需要索引其他部分节点的信息, 网络中流转的包首先在超级节点转发, 然后才是超级节点传递给叶子节点, 这样信息传播速度可以得到保证.

2.2 交易层

交易层是实现区块链系统任务的具体内容部分, 可以在满足共识条件后, 使得两个地址之间完成价值数据的传递. 基于账本和基于 UTXO 的交易模式中, 交易层信息主要包含输入部分、输出部分和交易信息部分. 但是随着对区块链效率的更高要求, NXT 社区提出了有向无环图与区块链结合的方式来存储交易信息, 这个时候更多还是类似侧链的解决思路, 不同的链条存储不同类型的交易, 在之后某个节点需要合并的时候, 几个分支再归并到一个区块. 真正将 DAG 与区块链结合的是 IOTA 的 Tangle 协议, Tangle 里的一个 Bundle 可以包含多个 TX 信息, 其中某些交易可以是价值 TX 包括 token 的收入和支出, 也可以是非价值 TX 包括一段数据. 与比特币区块相比, Bundle 通常 TX 含量非常少, 而且可以被节点独立完成并提交到公共账本中, 下表给出 Bundle 和比特币 Block 的对比.

表 1 Bundle 与 Block 的对比

Table 1 Comparison between Bundle and Block

类目	Bundle	Block
索引	两个前引 bundle 的哈希值	前一区块的哈希值
Nonce	用于 PoW 的遍历, 每个 TX 均存在	用于 PoW 的遍历, 存在 Coinbase 中
输入输出部分	输入或输出的地址	前一笔交易输出对应哈希和输出指数作为输入部分、该笔交易接收者地址或脚本作为输出部分
签名脚本	基于私钥的交易签名或者非价值 TX 的数据片段 (message)	基于私钥的交易签名
交易信息	交易值, 正值代表收入, 负值代表支出	交易值, 只有正值

交易信息不仅可以是代币数量, 也可以是存储信息索引、证书 ID、智能合约代码等. 智能合约是一套以数字形式定义的承诺, 在比特币中智能合约以脚本方式完成简单的延迟交易和条件交易, 在以太坊中的虚拟机中实现了可以编写智能合约的图灵完备脚本语言. 随着区块链体系结构的进步, 智能合约也可能会有新的表现形式.

2.3 共识层

共识层中封装的是相应的共识算法, 正如 TechTarget 的解释 “在计算机科学中, 共识算法是一种用在分布式过程或系统中, 实现单一数据值的协议”, 分布式过程中各个节点表现不一致, 所以共识算法必须要有一定的容错能力. 常见的共识机制有工作量证明共识 (proof of work, PoW)、权益证明共识 (proof of stack, PoS)、实用拜占庭容错协议 (practical Byzantine fault tolerance, PBFT) [11]、授权权益证明共识 (delegate proof of stack, DPoS)、基于 DAG 的共识, Paxos [12] 共识算法以及对 Paxos 改进的共识 RAFT [13] 等.

PoW 可以容忍小于 1/2 的错误节点, 是迄今为止使用最为广泛的共识机制, 但是此类共识要求计算大量的哈希会造成资源浪费问题和中心化问题.

PoS 是针对 PoW 缺陷产生的替代技术, 用户必须具有系统中的一些权益, 每次投票都会消耗掉用户的权益, 这使得如果在使用 PoS 的区块链系统中进行 51% 攻击更加困难. 正如以太坊研究员 Vlad Zamfir 提到的, 在 PoS 中重复 51% 攻击的代价, 可类比为每增长一个攻击区块, 都会毁掉所有矿机.

PBFT 可以容忍小于 1/3 的错误节点, 已经被 Hyperledger Fabric0.6 采用. PBFT 使用了较少的共识参与者, 因此运行非常高效, 但是不足之处在于是中心化程度过高, 不能作为公有链共识.

在 DPoS 共识中, 所有拥有 token 的节点都是权益持有者, 权益持有者按照权益投票选举见证者, 再由见证者代表自己进行投票共识. 通常见证节点采用轮询方式, 一个节点只能产生一个区块, 这样可以防

止“双重支付攻击”, 一旦见证节点做坏, 权益持有者就会投票决定其退出并选择其他更好的见证者.

基于 DAG 的共识算法可以支持高并发的共识, 从结构上提高了区块链的可扩展性, 但是以 DAG 作为基础架构的区块链项目 IOTA, 由于早期采用了中心化协调器来保证系统的可用性, 因此存在一些安全性隐患.

RAFT 是一种可以形式化证明安全性的共识算法, 通过逻辑分离保证状态的一致性, 与 PBFT 相同, RAFT 也被部署在 Fabric0.6 中作为可插拔的组件起作用.

2.4 应用层

应用层包含了区块链的各种应用场景, 各类为加密货币开发的电子钱包、以太坊上搭建的各类区块链应用以及基于 Fabric 开发的各类软件均属于应用层, 应用层开设各类接口以方便用户使用, 并且用户不必了解具体的区块链底层技术. 随着区块链技术的发展, 区块链的应用场景也越来越广泛, 目前除了应用于金融领域, 也开始扩展到娱乐、供应链管理、物联网、医疗、能源、公益和法律等领域. 区块链技术将对人的信任改变为对机器的信任, 使得任何的人为干预不起作用, 这种特点将会大大促进价值互联网在全球范围内的广泛应用.

3 区块链安全背景知识

3.1 区块链安全分类及定义

首先我们借用 ISO 对信息安全的定义给出区块链安全的定义.

定义 1 (区块链安全) 保护区块链系统不因偶然或恶意的原因而受到破坏、更改、泄露.

任何违背区块链安全定义的行为都可以归结为从算法安全层面、协议安全层面、实现安全层面、使用安全层面和系统安全层面进行的破坏、更改和泄露. 其与各层的对应关系如图2所示:

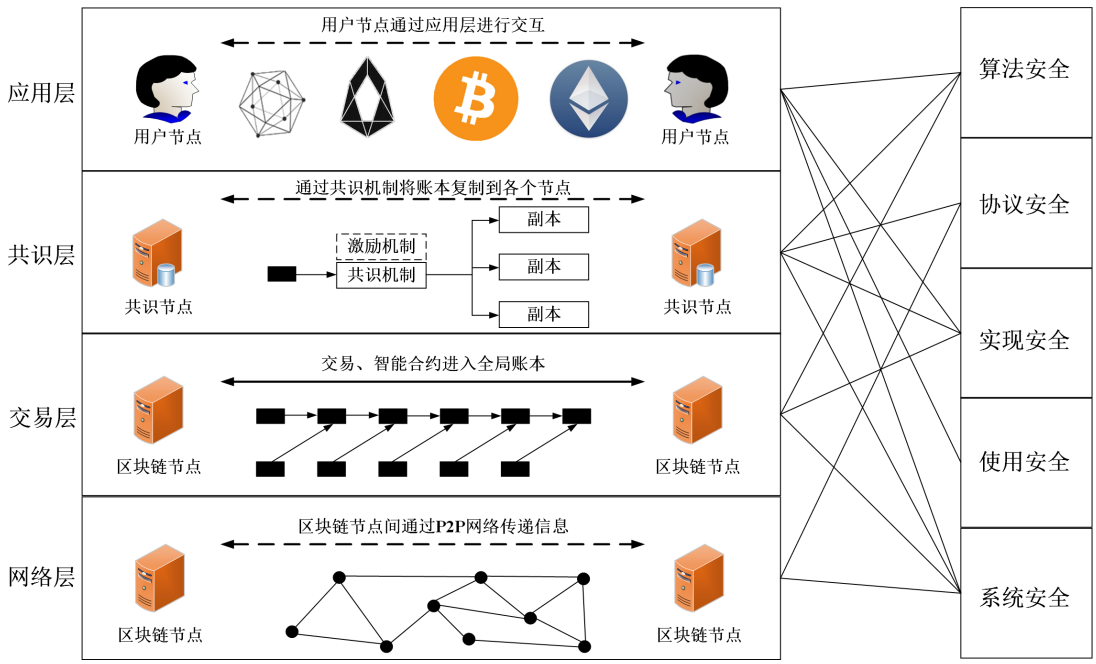

图 2 区块链安全分类

Figure 2 Safety classification of blockchain

算法安全通常是指密码算法安全, 密码算法在交易层主要表现为数据、地址等的展现形式, 既包括用于检验交易的哈希算法、签名算法, 也包括用于某些智能合约中的复杂密码算法; 在共识层, 密码算法通

常是共识算法的子算法, 比如 PoW 中 “猜谜” 的哈希算法, 比如 PoS 中代表权益的签名算法等; 在应用层表现为口令的加密存储等. 为清晰分界我们将网络协议的密码算法安全归结到协议安全内.

协议安全是区块链系统中的协议安全, 协议是通信双方为了实现通信而设计的约定或通话规则, 在网络层不同的区块链系统可以有不同的网络协议, 比特币 P2P 网络应用的是非结构化的 gossip 协议 [14], 另外扩展的比特币网络协议还包括矿池挖矿协议、Stratum 协议等, 以太坊使用的是结构化的 Kademlia DHT 协议 [15]. EOS 采用的是半分布式的网络结构协议, 本质上也是 DHT 类协议. 共识协议是区块链实现数据一致的关键, 很多共识协议的设计需要与网络协议相适应.

实现安全是区块链系统在实现时的安全, 实现漏洞是黑客们最愿意关心的问题, 而通常在进行区块链系统设计时, 是一般在交易层、共识层和应用层进行改造, 因此实现安全性也主要体现在这三个层上.

使用安全定义为用户或者服务器端在使用应用时由于使用方式不当而出现的相关安全问题, 加密资产交易平台是使用安全的短板, 近年来交易平台遭受的攻击在所有安全问题中占据比例最大, 用户、服务器、交易平台也是所有安全问题中最容易被利用的环节.

系统安全是一个整体性概念, 区块链系统从整体来看是一个同构冗余的系统. 系统的安全性受到各级安全性的共同影响, 也受到其组织形式的影响. 算法、协议、实现、使用漏洞与黑客攻击结合, 容易使区块链受到致命的打击, 所以系统安全分布在区块链系统的各个层上.

3.2 区块链安全的优势与劣势

区块链由于其独特的链式结构和底层的 P2P 网络, 其在安全性方面有独特优势, 因此区块链在密钥分发、隐私数据保护等安全领域已经有较多理论成果 [16,17]. 另一方面, 由于其去中心的分布式架构和公有链无准入要求的特点, 区块链在安全方面也存在劣势. 下面分析了区块链在安全方面的优势和劣势.

区块链安全的优势:

(1) 区块链不可更改的特性使得非正常活动痕迹会被永久记录在链上, 加入监管的区块链系统可以对非正常活动进行识别.

(2) P2P 网络节点物理位置分散, 每一个节点 (peer) 大都同时具有信息消费者、信息提供者和信息通讯等三方面的功能. 公私钥都是节点自己生成, 不需要中心化的服务器存储, 与攻击中心化服务器相比, 黑客很难通过攻击某一个节点获得大量用户信息, 从而更改全局账本.

区块链安全的劣势:

(1) 所有信息记录在区块链上, 通过交易历史记录容易形成交易画像, 一旦某用户将真实身份与地址关联关系泄露, 那么其隐私安全将会遭到不同程度的威胁.

(2) P2P 网络节点准入要求极低, 与专业服务器相比安全漏洞多防护能力差, 黑客很容易针对少量关键节点发起网络路由攻击或者直接入侵, 通过日蚀攻击获得利益.

(3) 智能合约安全性验证发展缓慢, 智能合约的部署要求低, 许多初学者也可以部署智能合约, 容易造成大量的安全问题.

4 区块链安全问题分析

区块链作为价值互联网的基础, 凭借其同构冗余的数据存储方式和共享共治的理念, 有效促进了高价值数据的传输和存储. 但是近年来, 以区块链技术为基础的系统, 出现越来越多的安全问题. 本节按照算法安全、协议安全、实现安全、使用安全和系统安全的顺序对区块链安全问题进行分析.

4.1 算法安全性分析

一般来说多数区块链中使用的通用标准密码算法在目前是安全的, 但是这些算法从间接和未来看也存在安全隐患.

首先从间接来看, SHA256 算法对应的 ASIC 矿机以及矿池的出现, 打破了中本聪设想的 “一 CPU 一票” 的理念, 使得全网节点减少, 权力日趋集中, 51% 攻击难度变小, 对应的区块链系统受到安全性威胁.

其次从未来发展看, 2018 年 3 月 6 日, Google 宣布制造了 72 量子比特的量子计算机 “Bristlecone”, 随着量子计算的兴起, 实用的密码体制都存在安全威胁. 根据对传统密码算法和量子计算算法的研究, 量子计算对现有密码体制的威胁如表2 所示.

表 2 量子计算对现有密码体制的影响

Table 2 Influence of quantum computation on existing cryptography

加密算法	类型	作用	安全基础	安全性威胁
AES	对称密码	加密	——	攻击难度减半
SHA256	哈希函数	数据指纹	——	攻击难度减半
RSA	非对称密码	签名、密钥生成	大整数分解	可被完全破解
ECDSA、ECDH	非对称密码	签名、密钥交换	椭圆曲线离散对数	可被完全破解
DSA	非对称密码	签名、密钥交换	离散对数	可被完全破解

另外, 虽然哈希算法在设计时考虑了抗碰撞, SHA 256 等算法在现在也是相对安全的, 但是也存在对哈希算法的碰撞攻击 [18] 和针对 Merkle–Damgård 散列函数 (在区块链中被广泛使用的 SHA-256 也是此类算法) 的长度扩展攻击 [19], 这些攻击方式有可能会对哈希算法造成威胁.

而对于新型密码, 由于其没有经过足够的时间检验和充分的攻防考验, 其在实际应用中更容易成为短板, 比如 Neha Narula 和她的团队在麻省理工学院媒体实验室的数字货币计划中发现 IOTA 哈希算法中的致命漏洞, 使得 IOTA 团队紧急更换算法. 某些未经检验的随机数生成器也可能存在漏洞, 利用生日攻击会产生相同随机数, 进而威胁区块链加密体制.

4.2 协议安全性分析

协议安全在网络层表现为 P2P 协议设计安全, 利用网络协议漏洞可以进行日蚀攻击 [20] 和路由攻击. 黑客利用一个节点的出度受限可以用日蚀攻击将节点从主网中隔离, 出度越多、节点随机化链接程度越高, 黑客的攻击难度就越大. 网络协议的好坏通常决定了信息流转的能力, 由于 P2P 网络结构不同, 以太坊就远比比特币更容易受到日蚀攻击的影响 [21]. BGP(边际网关协议) 攻击 [22] 是一种攻击者控制路由基础设施将区块链网络分块进行的攻击, 分为分割攻击和延迟攻击. 在分割攻击中, 攻击者通过控制 ISPs(互联网服务提供商) 将区块链网络划分为大小两个部分, 并在小网络中进行交易, 交易成功 (提现或提货) 后合并两个网络, 使得原交易被否定从而获利. 在延迟攻击中, 攻击者可以使矿工请求的最新块属于旧块, 从而使其他矿工竞争力增大. 另外针对某些特定服务器、交易网站还可以发起 DDoS 攻击, 目前对于 DDoS 攻击只能依靠收取交易费和浪费算力来控制.

协议安全在共识层表现为共识协议安全. 首先共识协议本身存在安全问题, 由于不同共识协议容错能力不同, PoW 存在 51% 算力攻击, PoS 存在 51% 币天攻击, 而 DPoS 和 DAG 还存在着中心化风险.

其次共识协议还受到外部攻击的影响. PoW 存在的自私挖矿 [23] 和坚强挖矿 [24] 等都是对 51% 攻击的进一步利用. 自私挖矿是 “区块扣留攻击”, 攻击者挖到区块并不公布, 而是继续挖掘, 待到其他人放块之后再放块分叉, 使自己能够保留主链优势 (比另一分叉多至少一个区块) 并且消耗他人算力, 得到多获利的目的. 矿池只需要拥有超过 1/3 的算力就可以实行自私挖矿, 由于自私挖矿不是以破坏系统为前提, 使得这种情况非常普遍又极难分辨. 坚强挖矿是在自私挖矿基础上改进的, 如果将自私挖矿中的保留主链优势替换为分叉使两个链深度相同, 就能使其收益率超过自私挖矿 13.94%, 而且如果自私挖矿和日蚀攻击相结合能够产生更大收益.

PoS 是作为 PoW 的替代技术提出的, 由 Vlad 和 Vitalik 带领研究的 Casper [25] 以及 Jae 带领研究的 Tendermint [26] 是两个标志性的 PoS 方案, 意在解决 PoW 的一些内在问题. 如果用户拥有 10% 的权益 (代币), 那么该用户挖掘下一个区块的可能性就是 10%, 基于权益的证明方式可以使得黑客很难收集到超过 51% 的权益. 但是 PoS 会在 “无利害关系” 上出问题, 如果需要对多个分叉进行投票, PoW 会选择胜出概率更大的一个分叉, 而 PoS 则会如下图所示同时押注. 我们假设用户投票成功得到的权益是 λ, 则 PoS 无利害攻击如图3所示.

一个好的 PoS 共识协议必须通过引入保证金来防止无利害关系的攻击, 另外还需要解决远程攻击 (long range attacks) 和卡特尔的形成 (Cartel formation) 这两个问题 [27]. 远程攻击是指矿工在撤回被锁定的虚拟资产后, 再发起之前生成的历史区块的分叉. 卡特尔是指在区块链上的寡头垄断. 由于 PoS 共识算法的本质是谁 “富有”, 谁就有更大的话语权, 这样少数富有矿工之间的 “协调” 将导致寡头垄断的形成.

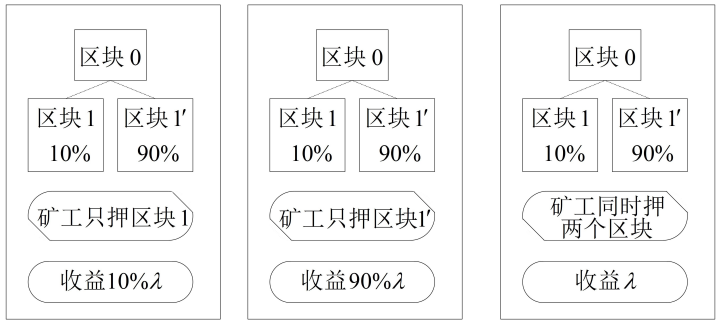

图 3 PoS 无利害攻击
Figure 3 Nothing at stake attack of PoS

DAG 是一种更通用形式的区块链, 通常来说区块链属于线性结构, 相比较于并行结构, 区块链的增长是缓慢的, 而对 DAG 而言只要当前交易的前引交易已经被验证, 那么当前交易就可以并行添加到账本中. 在高并发高可扩展性方面, DAG 比区块链拥有天然的优良特性. 但事实上, 以 DAG 技术为基础的 IOTA 网络目前依靠一个集中的, 封闭的 “协调员” 来保护它免受攻击, 而且团队还没有就何时以及如何移除中心协调器给出明确的指导.

4.3 实现安全性分析

在区块链系统的实现过程中, 由于程序员的主观原因或者留有后门, 会导致区块链的安全性受到损害.

交易层的实现安全性主要受到智能合约漏洞的影响, Ivica 等人将现有的智能合约漏洞分为浪子合约、贪婪合约、自杀合约、死后合约等 [28], 其定义如下:

(1) 浪子合约: 一个合约如果在某时刻被触发后, 能立刻或者经过多次交易将代币转移到任意地址, 那么该合约被称为浪子合约. 浪子合约的出现说明代币的转移违背了原始合约意图.
(2) 贪婪合约: 一个合约如果只能接受代币, 而不能发出代币, 那么这个合约账户将会锁定大量代币, 这种合约被称为贪婪合约. 贪婪合约的触发会使得全网流通的代币数量下降.
(3) 自杀合约: 有些合约允许代币消耗尽时或者被攻击者攻击时, 合约的拥有者可以用后备选项 “杀死” 合约, 但如果一个合约可以被任何人 “杀死”, 那么这个合约就被称为自杀合约. 自杀合约是极脆弱的合约.
(4) 死后合约: 当合约被终止时, 其代码和全局变量将从区块链被清除, 从而阻止其代码的进一步执行. 然而, 所有被终止的合约可以继续收到交易. 虽然这样的交易不能再调用合同的代码, 但是如果代币随它们一起发送, 它会被添加到合约余额中, 从而被无限期锁定. 死后合约和贪婪合约造成的后果相同.

代币的生成代码漏洞极容易摧毁系统的经济生态, 这是出现在共识层的严重安全问题. 代码在开发时可能会出现整数溢出漏洞、短地址漏洞和公开函数漏洞等. 其中整数溢出漏洞案例包括 wxBitcoin 和 bitcoind0.3.11 之前版本可以违背账户利益多生产比特币, 2018 年 4 月的 BEC、SMT 被盗事件. 以太坊的短地址漏洞可以使交易者从交易所获利 256 倍甚至更多. 最近的 Parity 多重签名钱包漏洞则是由于 initWallet 函数不慎设置成公开函数造成的.

应用层的实现安全性问题更多, 比如开发者违规记录用户信息, 应用软件口令未设置最低标准, 交易所的实现安全问题等, 都深刻影响着区块链系统的安全. 15 岁的安全研究人员 Saleem Rashid 对硬件钱包 Ledger 分析发现这些设备中包含一个安全处理器芯片以及一个不安全的微型控制器芯片, 攻击者可以将恶意软件植入微型控制器芯片中, 并在用户接收设备之前破坏设备, 或者从设备中窃取私钥. 这一漏洞将影响所有使用 Ledger 硬件钱包的交易所, 目前来看, 由于区块链还处于起步阶段, 目前缺少适用于加密资产的平台软件标准, 加密资产交易平台实现中除钱包防护问题, 还存在单点登录漏洞、oAuth 协议漏洞等各种问题.

4.4 使用安全性分析

区块链技术一大特点就是不可逆, 不可伪造, 但前提是私钥是安全的. 与以往任何体系不同的是, 私钥是每个用户自己生成并且自己负责保管的, 理论上没有第三方的参与, 所以私钥一旦丢失, 便无法对账户的资产做任何操作. 多重签名某种程度上能解决一部分问题, 但实施起来非常复杂, 而且要设计与之相配套的非常复杂的秘钥管理和使用体系. 区块链系统中钱包的口令也通常是用户的常用口令, 通过撞库攻击黑客很容易恢复出钱包的私钥. 另外有些用户在使用上不小心, 容易将私钥和助记词泄露在博客和视频中. 因此用户的个人行为是使用安全的一大隐患.

在线钱包的设计本是为了更好得管理用户私钥, 但是由于钱包算法固定以及用户思维模式相同, 也会造成安全隐患, brainwallet.org 是因为使用者脑中想象的随机字符产生了碰撞, 进而产生相同地址, 例如 “bitcoin is awesome” 生成的脑钱包地址 14NWDXkQwcGN1Pd9fboL8npVynD5SfyJAE, 有人在 2012 年用这个短语生成该地址后, 向里面转入 500 枚比特币后, 随后在不到一分钟的时间内, 这上面的币就被全部转走.

交易平台常见的隐患有热钱包防护问题、滥用权限问题和内部攻击问题等. 许多交易平台使用单个私钥来保护热钱包, 如果黑客可以访问私钥或者偷取私钥就可以破解热钱包. 而且由于没有完善的风险隔离措施和人员监督机制, 导致部分拥有权限的员工利用监管的机会盗取信息或代币. 2016 年交易平台 ShapeShift 发生的员工盗取敏感信息事件给交易平台造成了 23 万美元的损失. 从 2011 年到 2018 年 4 月, 交易平台安全事故损失约 13.44 亿美元, 占所有区块链安全损失的 1/2, 交易平台安全事件占所有区块链安全事件的 56.67%, 在所有事件中, 有 27% 是直接攻击交易所导致的, 这些黑客还能在后续的攻击中, 对窃取的用户信息 (账户密码、支付信息等) 重复利用, 这种情况的盗窃事件也能达到 14%.

4.5 系统安全性

目前, 黑客攻击对区块链系统安全性造成很大影响. 攻击者可以综合运用网络攻击手段, 对算法漏洞、协议漏洞、使用漏洞、实现漏洞、系统漏洞等各个方面综合利用, 从而达成攻击目的. 另外社会工程学与攻击手段的结合使区块链变得更加脆弱.

Mt.Gox 出现的盗币事件, 就是黑客利用早期比特币允许同区块出现交易链, 而 Mt.Gox 存在为方便交易不经验证即连续转账的漏洞, 转走大量比特币. 另外还有黑客利用网络钓鱼的手段, 在初次发起代币时利用电子邮件散播虚假信息、设置近似域名与近似地址使用户向攻击者账户转账. 另外利用用户终端漏洞, 操纵用户主机挖矿, 消耗主机的资源和电力获利, 2018 年初, 上百款《荒野行动》游戏辅助被植入挖矿木马, 利用游戏机的高性能来挖矿获利.

5 区块链安全问题应对机制

目前国际上基于区块链技术的系统发展迅速. IBM 的超级账本、微软及万象区块链实验室的 BAAS (blockchain as a service)、以太坊智能合约平台等项目快速推进使区块链平台出现了从无到有的飞跃, 平台推进的标准出台、共识机制和算法的突破、功能的强化和接口的丰富将助力区块链应用的加速落地. 区块链技术已经展现出非常好的发展前景, 在这种情况下, 区块链系统的安全问题更加值得我们去探讨, 构建一个更加安全的区块链系统迫在眉睫. 下面将从直接应对措施和根本应对措施两方面对区块链系统的安全性进行叙述.

5.1 直接应对机制

算法安全性是区块链安全系统的基石. 为了防止 ASIC 过度使用造成区块链中心化问题, 设计不利于并行计算的哈希算法势在必行, 可以看到莱特币的 scrypt 算法和暗黑币 X11 算法从增加内存消耗方面提高了 ASIC 开发难度, 随着防并行哈希算法的开发, 区块链虽然不能回归 “一 CPU 一票” 的秩序中, 也可以实现 “一 GPU 一票” 的 GPU 矿工公平状态. 为了防范量子计算的威胁, 哈希算法也必须加强安全强度, 传统密码算法也需要尽早替换为抗量子密码算法, 基于格上困难问题的密码算法和基于纠错码的密码算法都是不错的替代密码算法. 为了防范不成熟密码造成的安全漏洞, 要求区块链开发者对于未经验证的密码算法谨慎使用, 尽量杜绝叠加算法. 另外随机数生成器也可从伪随机向真随机过渡, 基于混沌的随机数发生器 [29] 和基于量子的随机数发生器 [30] 经验证都有很好的统计学表现.

针对协议安全性问题, 为防止网络层攻击, 全分布式非结构化拓扑网络虽然在组织结构不如全分布式结构化拓扑网络利于管理, 但是由于进入网络更随机, 黑客预先生成节点隔离目标节点的成本要更大, 所以建议开发者在进行网络布局时合理改造. 为防止权力的过度集中, 可以设计防 ASIC 挖矿的共识协议, 也可以用密码抽签技术增加共识层数. 为防止 DDoS 攻击, 开发者在设计激励机制时要考虑到 DDoS 攻击的成本问题.

针对实现安全性问题, 我们给出如下几项解决方案和建议.

- 对于开发者必须提出更高的要求, 发布智能合约之前需要对当下出现过的漏洞进行防范, 必须严格的智能合约形式化验证和安全测试, 在产品上线之前也要进行长时间的安全验证.
- 必须制定严格数据标准和产业标准.
- 定期进行代码审计, 包括交易安全审查和访问控制审查等.

针对使用安全性问题, 用户需要更加谨慎保管私钥, 尽量使用安全的冷钱包存储私钥, 口令设置需要与其他口令不同以预防撞库攻击. 开发者可以设计向用户透明的安全私钥管理应用、同时必须对用户口令设置安全的最低标准. 交易平台需要对员工进行安全培训, 严格进行权限管理, 谨慎开放服务器端口, 定期进行安全监测, 建立完善的应急处理措施.

针对系统安全性问题, 除了对以上各种安全措施的综合运用, 还要关注用户自身系统安全性, 包括定期使用更新补丁、启用设备防火墙、禁用路由器中不必要的组件等.

5.2 引入异构的区块链系统

虽然应对方法很多, 但是没能从根本上解决安全问题. 通过长时间研究, 我们认为区块链安全问题的解决根本途径是区块链体系结构的创新. 本节通过对现有区块链系统的同构性质进行说明, 从本质上找到单一漏洞影响系统安全的原因, 从而提出引入异构, 得到应对区块链安全问题的有效机制.

定义 2 (同构系统) 系统同构一般是指不同系统的数学模型之间存在着数学同构. 但是在复杂系统中, 人们常常把具有相同的输入和输出且对外部激励具有相同的响应的系统称为同构系统.

区块链系统就是这样一个同构的系统, 如果按照既定的程序对输入进行运行, 那么将会得到相同输出, 下面我们将在各个层次上对其同构性进行描述.

- 同构的网络结构: 区块链中用的 P2P 网络结构类型虽然不同, 但是都是同构的网络结构. 即对于某个节点在某时刻进入现有网络, 其链接方式是固定的.
- 同构的交易组织验证形式: 对于同样输入的交易信息, 不同节点产生的交易内容相同, 系统不同节点进行验证的方式结果也相同.
- 同构的共识机制: 对于同一个外部激励, 不同节点产生的响应相同, 如果是一个区块信息, 那么只要节点不做坏, 那么得到的结果要么是同时接受, 要么是同时拒绝.
- 同构的应用系统: 对于同样的操作方式和输入参数, 不同节点上的应用系统的反应是相同的.

同构系统最严重的问题是对于某个漏洞, 一旦被利用, 那么整个系统都会被破坏, 因此应该对区块链系统进行异构的改造, 才能有效应对区块链的安全问题. 对区块链系统进行异构改造, 必须使系统对原同构系统逻辑中定义的外部激励产生与原来相同的结果, 但是对于逻辑中未定义的外部激励产生响应. 我们定义这样一组构件 $\{g_1(x), g_2(x), \cdots, g_n(x)\}$, 与原同构系统逻辑中定义的外部激励集合为 $\mathrm{Out} = \{O_1, O_2, \cdots, O_m\}$, 逻辑中未定义的外部激励集合 $\mathrm{Out}' = \{O'_1, O'_2, \cdots, O'_m\}$. 所以异构区块链系统构件需要满足如下条件:

$$g_1(O_i) = g_2(O_i) = \cdots = g_n(O_i), O_i \in \mathrm{Out} \tag{1}$$

对任意 O'_i, 存在 s, t 使得

$$g_s(O'_i) \neq g_t(O'_i) \tag{2}$$

该构件集合对刺激产生的最终输出, 是对所有输出的择多判决. 这种区块链系统进行异构化改造, 能够使对构件中单一漏洞的利用被系统识别出来, 并且单一漏洞也无法对系统产生破坏性影响, 从而大大提高区块链系统的安全性和稳固性.

区块链的安全问题是影响区块链发展的核心问题. 区块链系统开发中存在扩展性、去中心化和安全性的不可能三角, 由于前提条件是去中心化的, 安全性的提高必然使得扩展性下降. 所以异构化的结果必然伴随存储开销和处理开销的增加. 但是从需求的角度看, 数据价值越高的领域对信息安全的要求就越高, 安全在区块链系统中是不可舍弃的. 因此对于异构区块链的研究方向是: 在增加异构的同时, 需要尽可能少地增加系统开销.

6 总结

本文从区块链安全问题分析和防治的角度出发, 首先指出现有区块链的分层方式与之前不同, 分为了网络层、交易层、共识层和应用层, 并且进行了分层介绍. 然后, 对区块链安全进行了定义和划分, 分为算法安全、协议安全、实现安全、使用安全和系统安全, 指出各类安全与区块链分层之间的对应关系并进行详细说明, 重点指出了区块链技术与其他技术相比在安全方面的优势与劣势. 之后, 对区块链安全问题进行了深入分析, 理清区块链安全问题的发现、弥补、再出现新问题的演进脉络. 总体来说, 对区块链安全影响最严重的是多种攻击手段结合的系统攻击, 为此针对某项安全问题出现后的弥补措施都属于被动防御, 而改变区块链体系结构的主动防御才是应对安全问题的最有效途径, 所以最后介绍了区块链安全问题的直接解决措施和根本应对机制. 在根本应对方式中提出对区块链进行异构化, 明确现有区块链为同构系统的原因和各层同构的输入输出情况, 引进随机异构的区块链系统改进方式. 最后从信息安全角度提出安全的异构区块链的未来研究方向, 可以认识到随机异构的区块链系统是解决区块链安全问题的有效途径.

References

[1] NAKAMOTO S. Bitcoin: A peer-to-peer electronic cash system[EB/OL]. https://bitcoin.org /bitcoin.pdf. 2008.
[2] WOOD G. Ethereum: A secure decentralised generalised transaction ledger[EB/OL]. http://gavwood.com/Paper.pdf. 2014.
[3] EOS.IO technical white paper, v2[EB/OL]. https://steemit.com/eos/@eosio/eos-io-technical-white-paper. 2018.
[4] VAN SABERHAGEN N. CryptoNote v 2.0[EB/OL]. https://cryptonote.org/whitepaper.pdf. 2018.
[5] SASSON E B, CHIESA A, GARMAN C, et al. Zerocash: Decentralized anonymous payments from Bitcoin[C]. In: 2014 IEEE Symposium on Security and Privacy (SP). IEEE, 2014: 459–474. [DOI: 10.1109/SP.2014.36]
[6] DUFFIELD E, DIAZ D. Dash: A privacy-centric crypto-currency[EB/OL]. https://www.whitepapertracker.com/wp/Dash/Dash_whitepaper.pdf.
[7] The ZILLIQ: A technical whitepaper[EB/OL]. https://docs.zilliqa.com/whitepaper.pdf. 2017.
[8] POPOV S. The tangle[EB/OL]. https://iota.org/IOTA_Whitepaper.pdf. 2018.
[9] CHURYUMOV A. Byteball: A decentralized system for storage and transfer of value[EB/OL]. https://byteball.org/Byteball.pdf. 2017.
[10] LUO J H. Overview on peer-to-peer[EB/OL]. http://www.intsci.ac.cn/users/luojw/P2P/.
[11] CASTRO M, LISKOV B. Practical Byzantine fault tolerance and proactive recovery[J]. ACM Transactions on Computer Systems, 2002, 20(4): 398–461. [DOI: 10.1145/571637.571640]
[12] OKI B M, LISKOV B H. Viewstamped replication: A new primary copy method to support highly-available distributed systems[C]. In: ACM Symposium on Principles of Distributed Computing. ACM, 1988: 8–17. [DOI: 10.1145/62546.62549]
[13] ONGARO D, OUSTERHOUT J. In search of an understandable consensus algorithm[EB/OL]. https://raft.github.io/raft.pdf. 2014.
[14] KARP R, SCHINDELHAUER C, SHENKER S, et al. Randomized rumor spreading[C]. In: Proceedings of 41st Annual Symposium on Foundations of Computer Science. IEEE, 2000: 565–574. [DOI: 10.1109/SFCS.2000.892324]
[15] MAYMOUNKOV P, MAZIÈRES D. Kademlia: A peer-to-peer information system based on the XOR metric[C]. In: Peer-to-Peer Systems—IPTPS 2002. Springer Berlin Heidelberg, 2002: 53–65. [DOI: 10.1007/3-540-45748-8_5]
[16] AXON L M, GOLDSMITH M. PB-PKI: A privacy-aware blockchain-based PKI[C]. In: International Conference on Security and Cryptography. Madrid, Spain. 2017: 311–318. [DOI: 10.5220/0006419203110318]
[17] ZYSKIND G, NATHAN O, PENTLAND A. Decentralizing privacy: Using blockchain to protect personal data[C]. In: IEEE Security and Privacy Workshops. IEEE Computer Society, 2015: 180–184. [DOI: 10.1109/SPW.2015.27]
[18] WANG X, YU H. How to break MD5 and other Hash functions[C]. In: Advances in Cryptology—EUROCRYPT

2005. Springer Berlin Heidelberg, 2005: 19–35. [DOI: 10.1007/11426639_2]
[19] CORON J S , DODIS Y. MALINAUD C, et al. Merkle-damgard revisited: How to construct a Hash function[C]. In: Advances in Cryptology—CRYPTO 2005. Springer Berlin Heidelberg, 2005: 430–448. [DOI: 10.1007/11535218_26]
[20] HEILMAN E, KENDLER A, ZOHAR A, et al. Eclipse attacks on Bitcoin's peer-to-peer network[C]. In: USENIX Conference on Security Symposium. USENIX Association, 2015: 129–144.
[21] WÜST K, GERVAIS A. Ethereum eclipse attacks[EB/OL]. https://www.research-collection.ethz.ch/bitstream/handle/20.500.11850/121310/eth-49728-01.pdf.
[22] APOSTOLAKI M, ZOHAR A, VANBEVER L. Hijacking Bitcoin: Routing attacks on cryptocurrencies[C]. In: 2017 IEEE Symposium on Security and Privacy (SP). IEEE, 2017: 375–392. [DOI: 10.1109/SP.2017.29]
[23] EYAL I, SIRER E G. Majority is not enough: Bitcoin mining is vulnerable[C]. In: Financial Cryptography and Data Security—FC 2014. Springer Berlin Heidelberg, 2014: 436–454. [DOI: 10.1007/978-3-662-45472-5_28]
[24] NAYAK K, KUMAR S, MILLER A, et al. Stubborn mining: Generalizing selfish mining and combining with an eclipse attack[C]. In: IEEE European Symposium on Security and Privacy. IEEE, 2016: 305–320. [DOI: 10.1109/EuroSP.2016.32]
[25] BUTERIN V, GRIFFITH V. Casper the friendly finality gadget[EB/OL]. https://github.com/ethereum/research/blob/ master/papers/casper-basics. 2017.
[26] KWON J. TenderMint: Consensus without mining[EB/OL]. https://tendermint.com/static/docs/tendermint.pdf. 2014.
[27] CHJANGO U. Consensus compare Casper vs Tendermin[EB/OL]. https://blog.cosmos.network/consensus-compare-casper-vs-tendermint-6df154ad56ae.
[28] NIKOLIC I, KOLLURI A, SERGEY I, et al. Finding the greedy, prodigal, and suicidal contracts at scale[EB/OL]. http://ilyasergey.net/papers/maian-draft.pdf. 2018.
[29] KANTER I, AVIAD Y, REIDLER I, et al. An optical ultrafast random bit generator[J]. Nature Photonics, 2009, 4(1): 58–61. [DOI: 10.1038/nphoton.2009.235]
[30] FIORENTINO M, SANTORI C, SPILLANE S M, et al. Secure self-calibrating quantum random-bit generator[J]. Physical Review A, 2007, 75(3): 723–727. [DOI: 10.1103/PhysRevA.75.032334]

作者信息

斯雪明 (1966–), 福建诸暨人, 教授, 研究员. 主要研究领域为密码学、区块链、高性能计算体系结构、网络安全、数据科学.
sxm@fudan.edu.cn

苑超 (1992–), 山东烟台人, 副研究员. 主要研究领域为区块链安全与隐私保护、网络密码.
yc_jszx@163.com

徐蜜雪 (1993–), 山东烟台人, 硕士. 主要研究领域为对称密码算法的安全性分析、基于区块链的加密货币.
mixue_xu@163.com