文章编号:1008-5564(2020)03-0037-11

区块链安全综述

张　杰
(安徽财经大学 管理科学与工程学院,安徽 蚌埠 233030)

摘　要:以区块链安全相关文献为研究对象,依据区块链的基础架构,从协议层、扩展层、应用层三个层面讨论了加密机制、共识机制、网络通信、智能合约与隐私等五个方面所存在的安全问题,分析了相关攻击的原理和过程以及应对这些安全问题的相关措施.通过对文献的梳理和分析,并结合时代背景与目前存在的不足,提出区块链技术的研究趋势.

关键词:区块链安全;共识机制;智能合约;隐私保护
中图分类号:TP393　　文献标志码:A

Overview of Blockchain Security

ZHANG Jie
(School of Management Science and Engineering, Anhui University of Finance and Economics, Bengbu 233030, China)

Abstract: In this paper, taking the blockchain security related literature as the research object, according to the blockchain infrastructure, from the three levels of protocol layer, extension layer and application layer, five aspects of the existing security problems such as encryption mechanism, consensus mechanism, network communication, smart contract and privacy and so on are discussed, and the principle and process of related attacks and the relevant measures to deal with these security problems are analyzed. Based on the literature review and analysis, combined with the background of the times and the existing shortcomings, the research trend of blockchain technology is proposed.

Key words: blockchain security; consensus mechanism; smart contract; privacy protection

比特币自 2009 年诞生以来,便吸引着各界人士的目光,并引发了投资浪潮.作为它背后的技术基础——区块链技术,由于其开放性、去中心化、数据防篡改等特点和优势,展现出了广泛的应用前景,从加密货币到安全合同、电子健康档案、金融业和供应链管理等[1].据一些媒体报道称,全球至少有 75 家银行正计划实施区块链解决方案,Facebook 正在秘密开发一种大规模定制的基于区块链技术的加密货币系统[2],在国内,中国银联与光大银行开发了基于区块链的可信电子凭证系统等.

随着区块链技术的快速发展和广泛应用,一些不法分子趁机利用区块链技术的安全漏洞和管理不

收稿日期:2020-03-12
基金项目:安徽高校自然科学研究项目(KJ2020A0013;KJ2019A0657);安徽财经大学校级项目(ACKYB19012;ACKYB18010)
作者简介:张　杰(1996—),男,安徽六安人,安徽财经大学管理科学与工程学院硕士研究生,主要从事智能商务与数据挖掘研究.

够完善等问题对用户进行攻击,使得区块链技术面临着许多安全威胁和挑战.2014年3月,不法分子利用DDoS(Distributed Denial of Service,分布式拒绝服务)攻击比特币交易平台Mt.Gox,致使该交易平台被盗85万枚比特币,损失超过4.5亿美元[3].2016年6月,当时区块链业界最大的众筹项目The DAO遭受攻击,损失约6 000万美元[4].2017年5月,勒索软件WannaCry利用Windows系统漏洞加密用户文件以索取比特币赎金,两天内在150个国家感染了大约23万名受害者[5].

本文将介绍区块链技术的相关原理和发展现状;将依据区块链的基础架构,从协议层、扩展层和应用层分别介绍区块链的安全问题;结合区块链相关安全问题提出了相应的应对措施;总结目前存在的不足并提出未来研究趋势.

1 区块链技术概论

1.1 区块链的基础技术

1.1.1 区块链技术的定义

区块链技术起源于中本聪2008年发表的论文《比特币:一种点对点的电子现金系统》[6],是比特币等新型数字货币的底层实现关键.区块链技术本质上是自带信任化和不可篡改的系统上各节点共同维护的分布式记录系统.每个节点都可以通过特定的哈希函数将接收到的交易信息以Merkle树的形式存储,并打包到一个带有时间戳的数据区块中,通过去中心化共识机制,链接到系统中,形成新的区块[7].所有的区块以链状结构相互连接,故称为区块链.

1.1.2 区块链技术的基础架构

区块链的基础架构可以简单分为三层:协议层、扩展层和应用层,其中协议层又可分为存储层和网络层,它们相互独立却又互相联系,具体如图1所示.

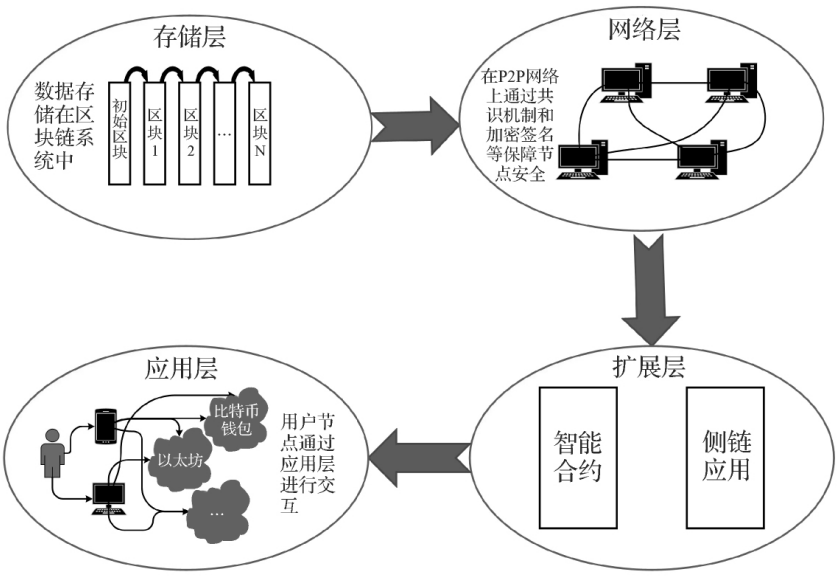

图1 区块链技术的基础架构

存储层:交易信息及数据存储在区块中,并以链状结构连接在一起,形成区块链,该阶段主要涉及到数据区块、哈希函数、Merkle树和时间戳等技术要素.

网络层:主要包括了区块链节点之间的通信网络、非对称加密技术和共识机制.在区块链系统中,节点之间采用P2P网络(peer-to-peer,对等网络),所有节点地位相同且不存在任何第三方的权威机构.非对称加密技术通常在加密和解密的过程中采用两个非对称的密码,即公钥和私钥,以满足区块链系统中的安全性要求和所有权验证的需求.作为一个去中心化的系统,为了保证交易和数据的可靠性和一致性,区块链系统采用去中心化的共识机制,现有的区块链系统主要应用四大共识机制:PoW(工作量证明机制)、PoS(权益证明机制)、DPoS(委托权益证明机制)和PBFT(实用拜占庭容错协议)[8].PoW机制利用解决一个计算困难但容易验证的数学难题来证明数据的可信性,PoS以权益证明替代工作量证明,权益即节点拥有数字货币的数量,衡量权益基于币龄,类似于现实生活中的股东机制,区块链系统中拥有股份最多即权益最高的节点进行区块的生成.DPoS机制中节点以其所拥有的股份权重享有相应的投票权利并根据投票选出一定数量的委托节点对系统进行维护[9].PBFT共识机制允许在系统上恶意节点不高于总数1/3的情况下确保数据的安全性和可信性[10].

扩展层: 以“智能合约”为代表的基于区块链技术的扩展实现.智能合约实质上是部署在区块链系统上的去中心化、可信任的共享代码[11],合约双方就合约细节、违约情况等内容签署合同,并将内容以脚本的形式部署在区块链系统中,在满足合约的情况下实现自动化执行合约.

应用层: 基于区块链技术的各种应用场景,各类数字货币的轻钱包(客户端)便是应用层最典型的应用,用户可通过应用软件客户端,与区块链系统进行交互.随着区块链技术的发展,其应用场景也将更为广泛.

1.1.3　区块链技术的运行过程

中本聪在白皮书中详细地介绍了区块链系统的运行过程[6],在新的交易信息向全网广播之后,系统中的分布式节点将接收到的交易信息打包到区块中并进行计算,率先得到工作量证明解的节点向全网广播,其余节点接收到广播后对该区块进行验证,通过验证的区块的哈希值作为下一个区块的父哈希值,表示其余节点认可了该区块为有效区块.

1.2　区块链技术发展现状

自比特币诞生以来,区块链一共经历了三个阶段: 以数字货币为主的区块链 1.0,以数字金融为核心的区块链 2.0,面向数字社会的区块链 3.0[12].区块链 1.0 阶段是以比特币等加密货币为代表的区块链技术.在区块链 2.0 阶段,引入了智能合约,以太坊是该阶段的代表,在以太坊中,开发人员可以使用图灵完备的编程语言来开发智能合约,实现丰富的功能.区块链 3.0 阶段,开发人员基于可用的智能合约,开发功能更为丰富的 DApps(Decentralized Application,去中心化应用),DApps 中后端代码运行在去中心化的点对点网络上,数据交互由部署在区块链系统上的智能合约完成,与传统 APP 一样,DApps 允许使用任何语言编写前端代码和用户界面,以便对其后端进行调用.

2　区块链技术的相关安全问题

按照区块链技术的基础架构,从协议层安全、扩展层安全、应用层安全三个方面对区块链技术的安全问题进行分析.

2.1　协议层安全问题

区块链技术所面临的主要的协议层安全问题有加密机制安全问题、共识机制安全问题和网络通信安全问题等.

2.1.1　加密机制安全问题

(1) 私钥安全问题: 在区块链系统中,私钥是用户身份凭证.Mayer 在 ECDSA(椭圆曲线数字签名算法)方案中发现了一个漏洞,比特币和以太坊运行在一条特定的曲线——secp256k1 上,而且仅生成私钥和公钥,即意味着所有的参数是公开的,有可能会泄露信息,攻击者可利用该漏洞复刻用户的私钥,一旦用户的私钥被盗,很难恢复[13].Schmidt 等人发现攻击者可利用临时私钥攻击用户,盗取用户的签名私钥[14].Courtois 等人提出了一类具有不良随机数的 ECDSA 攻击,如果在 ECDSA 方案中,两个用户签名使用了相同的随机数,则其中的每个签名者都可以计算另一个签名者的私钥[15].

(2) 加密算法安全问题: 区块链系统中主要采用的加密算法是哈希函数,目前这类加密算法理论上是非常安全的,但仍然存在着安全隐患.Horalek 团队分析了利用彩虹表破解哈希函数,攻击者利用生成的彩虹表与哈希函数进行碰撞,从而获得密码[16].哈希长度扩展攻击也是攻击者用来破解哈希函数的一类方法,长度扩展攻击是在消息与密钥的长度已知的情形下,针对某些允许包含额外信息的加密散列函数的攻击手段[17].

2.1.2　共识机制安全问题

作为去中心化的系统,区块链技术依靠共识机制保障数据的可信性,当前区块链系统中主要应用的共识机制包括 PoW、PoS、PBFT、DBFT 等,攻击者可能利用共识机制的漏洞对区块链系统进行攻击,针对共识机制攻击的主要类型如表 1 所示.

表1 共识机制攻击主要类型

攻击类型	双花攻击	51%攻击	自私挖矿	币龄攻击	远程攻击
共识机制	PoW	PoW	PoW	PoS	PoS

在基于PoW共识机制的区块链系统中,双花攻击和51%攻击是系统面临的主要安全问题,双花攻击是攻击者利用区块链网络交易的延时性,使用相同的数字货币进行两笔交易的攻击模式.由于交易的发起和验证具有时间差,攻击者发起两笔交易,在第二笔交易被验证为无效之前,攻击者已经获得了第一笔交易的输出,从而导致了双花攻击,Karame等人分析了双花攻击并提出了一种不支付任何数字货币仍获得交易输出的攻击模型[18].当基于PoW机制的系统中某个节点掌握了51%的算力,便有可能发动51%攻击[19],这是由于在PoW区块链中,允许出现分叉的现象,而最长的链被认为是主链,当某个节点掌握了51%的算力时,相较于其他"诚实的节点"更容易找出最长的链,从而原本真实的主链会被替代,数据信息将可能会被随意篡改.自私挖矿攻击是攻击者利用区块链系统分叉出一条私链,并将挖到的区块链接到私链中,使私链长度大于公链,并且不对其他节点进行广播.当公链长度快要赶上私链时,攻击者将私链公布到区块链系统中,由于最长的链被认为是主链,"诚实的节点"在不知情的情况下认可了该私链的合法性,并选择在该私链上继续挖矿,可能会导致"诚实的节点"没有回报.Nayak等人在研究自私挖矿攻击的基础上提出了顽固挖矿攻击,可使得攻击者获得更为高额的利益[20].

PoS共识机制是为了解决PoW机制过于消耗算力而提出的,可以利用权益证明替代工作量证明.在基于PoS共识机制的区块链系统中,币龄攻击和远程攻击是两种常见的安全问题.由于币龄是衡量权益的标准,攻击者可能节省出最高的币龄成为区块链系统中权益最高的节点,从而使区块链分叉并进行双花攻击,但由于从币龄攻击中获得的利益较低,远程攻击是更为常见的一种攻击.攻击者通过回溯到初始区块对区块链进行分叉,创建一条长于主链的链,并篡改信息,替代原先的主链[21].

2.1.3 网络通信安全问题

区块链采用去中心化的P2P网络技术,攻击者可能会恶意造成网络的延迟或者隔离对区块链系统进行攻击,主要包括日蚀攻击[22]、可伸缩度量攻击[23]、BGP劫持攻击[24]和余额攻击[25]等,相关攻击如表2所示.

表2 网络通信安全问题

攻击类型	日蚀攻击	可伸缩度量攻击	BGP劫持攻击	余额攻击
原因	攻击者垄断受害者的交易连接,使受害者与系统中其他节点隔离	利用比特币的可伸缩度量性延迟交易信息的传递	通过拦截区块链的网络流量延迟网络信息有效传递或区块同步的速度	低算力攻击者短暂扰乱相同算力的子群之间的通讯

2.2 扩展层安全问题

扩展层是以"智能合约"为代表的基于区块链技术的扩展实现.智能合约实质上是部署在区块链系统上的去中心化、可信任的共享代码,由于当前智能合约可能存在一些安全漏洞和防范措施不够完善等问题,攻击者可利用这些安全问题对区块链进行攻击.

2.2.1 智能合约漏洞安全问题

Luu等人将智能合约的漏洞分为交易顺序依赖漏洞、时间戳依赖漏洞、处理异常漏洞和可重入缺陷漏洞[26],依赖性漏洞是由于智能合约的执行正确与否与以太坊的状态有关,而有效的交易可能会影响以太坊的状态.当一个新的区块含有两笔交易时,交易的先后顺序可能会引起以太坊的最终状态不同,而交易的顺序取决于矿工,从而导致智能合约的执行依赖于矿工的操作.时间戳依赖漏洞是由于某些智能合约是根据区块中的时间戳所执行的,而时间戳是由矿工根据自身的时间所设置的,若攻击者修改时间,可能会导致风险.在不同的智能合约相互调用时可能出现处理异常漏洞,若被调用的合约产生错误返回值却没有被正确验证时,可能会遭受到攻击.可重入缺陷漏洞是指攻击者可以利用调用了智能合约而状态未改变的中间状态对合约进行反复的调用.

Nikolic等人根据智能合约漏洞将智能合约漏洞分为浪子合约、自杀合约、贪婪合约和遗嘱合约[27],

如表 3 所示.

表 3　漏洞合约的类型及定义

类型	浪子合约	自杀合约	贪婪合约	遗嘱合约
定义	合约在触发后,交易资金能通过漏洞经过交易转移到特定地址,该合约为浪子合约	智能合约的拥有者可以在以太坊发生故障时选择退回,但是当退出指令也可以被其他节点执行时,该合约为自杀合约	智能合约所涉及的商品以及加密货币锁定在以太坊中,交易双方均无法得到,也不能取消的合约	若已经完成或关闭且代码和全局变量被清除的智能合约仍能继续收到交易,这类合约称为遗嘱合约

2.2.2　智能合约运行安全问题

智能合约在运行部署过程中,依然存在安全问题.在以太坊中,部署智能合约需要消耗 gas(以太坊费用),攻击者可能会利用这一特性对区块链系统进行攻击,使用户浪费大量的 gas.Chen T 等人分析了存在待优化问题的智能合约,该类合约主要存在无用代码和循环相关问题[28],Teutsch 等人分析出两种可能的恶意脚本攻击,资源枯竭攻击和不正确交易攻击[29].在以太坊中,攻击者可能向系统提供一个需要耗费许多资源的验证交易,系统上其他的节点必须花费大量的精力和时间去完成验证,即使以太坊引入了 gas 系统,由于交易费用仅需区块创始者支付,攻击者仍然可以零费用地造成其余节点大量算力的浪费.由于某些节点可能出于“理性”会跳过需要耗费大量资源的交易,当需求验证的节点向其他节点提供验证交易时,恶意验证节点可能会提供错误的验证方案,由于“理性”的节点验证这个错误方案时可能会耗费大量资源,故这些节点会跳过验证,并认可错误的验证方案是可行的,此时,得到的共识方案是不可信的.在智能合约运行过程中,存在的另一个安全问题是 DDoS(分布式拒绝服务)攻击,攻击者利用大量的网络节点同时对系统发起请求,以造成系统拥挤,无法提供正常的服务.智能合约的部署会消耗 gas 值,而某一些操作需要消耗的 gas 值可能设置的过低,攻击者可以大量执行该操作来消耗网络资源以造成系统拥堵.攻击者曾利用大量执行 extcodesize 操作攻击区块链系统,执行 extcodesize 操作时需消耗 gas 值很低,攻击者可以在一次交易中执行 5 万次该操作,导致区块同步的速率大大降低[30].

2.2.3　犯罪智能合约问题

犯罪智能合约是犯罪分子利用其进行各种违法行为,可能会造成机密信息的泄露和密钥丢失等问题的一类智能合约.Juels 等人分析了一例利用犯罪智能合约窃取密钥的安全事故[31],攻击者利用 PwdTheft 这一犯罪智能合约,与 SGX(软件保护拓展)、HTTPS(超文本传输协议安全)等可信的硬件技术相结合,窃取了用户的密钥.

2.3　应用层安全问题

应用层是基于区块链技术的各类应用场景,用户在与区块链系统交互时,可能会发生隐私安全问题.攻击者可能通过利用数据挖掘手段获取用户的物理身份或其他附加信息,导致用户的隐私泄露,本小节主要从身份隐私和交易隐私两个方面分析了区块链技术应用时的安全问题[32].

2.3.1　身份隐私安全问题

尽管区块链技术被认为是具有匿名性的技术,但想要做到完全的匿名是十分困难的,多数区块链系统都存在着匿名性不足的安全问题.区块链中每个节点通过 P2P 网络相互连接,Koshy 等人确定了 P2P 网络中三种异常的中继模式,攻击者可以利用比特币地址找到所对应的用户 IP 地址[33].用户的交易行为也有可能泄露个人信息,Androulaki 等人总结了六种可能会泄露个人信息的交易行为,并通过将比特币作为交易货币在大学中进行了实验,发现通过对交易行为进行聚类分析,可近似得到 40%的用户的个人资料[34].攻击者也可能通过女巫攻击[35](利用单个节点伪造多重身份从而对系统进行攻击,破坏系统的冗余机制)破坏或阻止分散的匿名协议,造成用户真实身份的泄露的风险[36].

2.3.2　交易隐私安全问题

除却用户身份隐私可能会被泄露之外,攻击者也可能会通过对用户攻击窃取用户的交易隐私.Fleder 等人提出攻击者可能将外部信息资源与信息流分析等技术相结合,对典型的用户行为、支出和查询习惯、同一用户多个账户间的比特币流水等相关统计量进行分析,窃取用户的交易隐私[37].

3 区块链技术安全问题的应对措施

本节将分别从协议层、扩展层以及应用层的安全问题论述相关的应对措施.

3.1 协议层安全问题应对措施

针对私钥安全问题,Gennaro 提出了一种基于 ECDSA 的门限签名算法来保护比特币钱包[38],门限钱包技术即将密钥进行分割,只有超过门限阈值才能获得签名授权.具体而言,将密钥分为 n 份,每份由一个节点保管,当门限阈值为 t 时,只有当不少于 t 个节点参与交易时,才可以获得密钥信息.Gennaro 在基于比特币系统采用的 ECDSA 密钥算法上,提出了优化的阈值 DSA 算法,在保证私钥安全性的前提下,提高了签名的速率.

针对共识机制相关安全问题,Pérez-Solà 等人提出了一种利用特殊的比特币脚本 FR-P2PK 来预防双花攻击的交易机制[39],在该交易机制中,交易的发起者选择一个随机数 k 和一个公钥 PKα,并根据该脚本产出 FR-P2PK 输出,同时该发起者存储一部分资金在该输出中并向网络中广播等待交易确认,在一笔交易中,交易的确认同时包括公钥 PKα 所对应私钥 SKα 的有效签名和随机数 k 所产生的有效签名,若交易的发起者想进行双花攻击,该随机数 k 会产生两个不同的有效签名,此时根据 ECDSA 漏洞,网络中的观察节点便可根据 k 产生的不同的有效签名获得进行交易的签名私钥,使攻击发起者可能会面临账户资金丢失的风险,从而预防双花交易,但此种机制可能会导致交易接收方面临着钱财两空的风险.Heilman 等人提出了一种利用时间戳惩罚隐藏区块的矿工的方案以减少自私挖矿的收益[40],当公链与私链长度相同时,自私挖矿攻击获利的阈值为 $\alpha>25\%$[41],在该方案中,可将攻击获利的阈值提高为 $\alpha>32\%$,以降低自私挖矿收益的概率,但此方案引入的第三方违背了区块链去中心化的思想.AlMallohi 等人提出了一种多变量检查点的方式以缓解权益证明机制中的远程攻击[42],检查点是被区块链节点一致验证的某一时刻的系统状态,AlMallohi 等人以区块、活跃用户和权益作为多变量来确定检查点的位置,但该方案仅可以在一定程度上缓解远程攻击.

针对区块链网络通信相关问题,Walck 等人提出了三种策略来应对日蚀攻击[43]:(1)部分随机选择 HB(High-Bandwidth,高带宽)邻居节点.在区块传输协议中,系统上的每个节点 V 可以选择 3 个 HB 邻居节点,当新区块进行广播时,HB 邻居节点接收到该广播信息后并不会广播新区块的信息而是向节点 V 发送一个未经请求的新的区块,部分随机选择 HB 邻居节点即 3 个 HB 邻居节点总有 1 个是随机选择的,可防止攻击节点完全控制 HB 邻居节点,从而保证总有一个邻居节点是非攻击节点.(2)在传出连接中选择 HB 邻居节点.因为攻击节点通常选择在启动时连接其余节点,当在传出连接中选择的 HB 邻居节点通常不会被选择作为攻击节点.(3)减少区块超时下载.降低延时 1 分钟,可以将攻击效率减少约 9.6%.面对 BGP 劫持攻击,Apostolaki[24] 等人认为短期内可以增加节点连接的多样性,监视往返时间,监视其他的统计信息比如连接的分布、请求与响应的时间间隔以及其他较低级别的连接异常等,长期范围可以加密比特币通信,使用独特的控制和数据通道等.

3.2 扩展层安全问题应对措施

本小节主要介绍几种增强智能合约安全性的相关措施.

3.2.1 Oyente

Oyente 是 Luu L 等人提出的一种智能合约漏洞分析器[26],利用符号执行技术,分析智能合约编译的字节码,并通过运行在以太坊虚拟机中的模型来检测部署的智能合约.Oyente 中的核心模块主要有控制流程图构造器、探测器、核心分析器、验证器和可视化器.首先,Oyente 基于以太坊字节码构造智能合约静态控制流程图,探测器通过以太坊状态和控制流程图信息模拟智能合约的运行,此时控制流程图得到进一步的丰富和改进,核心分析器模块可以利用相关分析方法检测四种不同的漏洞,验证器模块则可以验证已经被检测出的漏洞以及可能被攻击的路径,已验证的漏洞和控制流程图通过可视化器模块提供给用户,供用户用以调节和分析.然而 Oyente 漏洞分析器仅能分析四种漏洞,对于智能合约中的整数溢出漏洞以及公平性漏洞,Oyente 并不能很好地应对.

3.2.2　Town Crier

Town Crier(TC) 是 Zhang F 等人提出的可进行链下数据交互的已认证数据输入系统[44].由于部署在区块链上的智能合约无法直接访问网络,无法通过 https 直接获取数据,TC 可以充当 https 数据源与智能合约链接的桥梁.TC 合约在用户合约和 TC 服务器之间充当 API(应用程序编程接口) ,并作为 TC 系统的前端,TC 系统中的核心程序在 Intel SGX 上运行,主要功能是从用户合约中得到数据请求,并从启用 https 的网站中得到数据,最后以含数字签名的区块链信息形式打包给用户.TC 系统中还包括中继模块,中继模块是智能合约、SGX 环境以及数据源网站之间的网络通信中心,通过中继模块可以实现核心程序与网络通信间的隔离,即使中继模块受到攻击或者网络通信数据包受到篡改,也不会改变 TC 的正常功能,在 TC 系统下可以安全地实现智能合约的链下数据交互.

3.2.3　内存池优化

内存池优化是一种应对 DDoS 攻击的方案[45],在加密货币中,内存池充当 UTXO(未确认交易) 的缓存,攻击者可以通过大量未经确认的交易堵塞内存池,使用户支付高额的费用,对内存池的优化可分为基于费用的内存池优化和基于年龄的内存池优化.在基于费用的内存池优化方案中,设立一个初始阈值,当交易缓存数量超过这个阈值时,内存池开始过滤垃圾信息,检查每个交易是否缴纳中继费并更新内存池状态,当内存池缓存到达基线阈值时,每个传入的交易不仅需要缴纳中继费还需要缴纳挖掘费,交易才会被认可,在过滤了垃圾交易信息之后,内存池得到优化,若缓存小于基线阈值时,仅需缴纳中继费,若优化后的内存池大于基线阈值,仍需缴纳挖掘费.在基于年龄的内存池优化方案中,当内存池缓存达到基线阈值,并且内存池只接受支付中继费和挖矿费的交易,对每个传入的交易,通过父交易的年龄总和除以父交易的总数来计算交易的平均年龄,并在内存池上应用“最低年龄限制”过滤器,只有当交易年龄满足标准时,交易才会被许可.通过内存池优化的方案,攻击者进行 DDoS 攻击的成本大大提高,这将缓解 DDoS 攻击,然而这两种方案都有一些局限性,在基于费用的内存池优化方案中,当对某一笔交易进行挖掘时,往往需要挖掘出其父交易的信息,若父交易被挖掘出的优先级因子较低,可能会导致挖掘子交易的费用提高,在基于年龄的内存池优化方案中,用户进行一些快速交易时,可能无法等待这些交易被验证,导致其无法被内存池认可.

3.3　应用层安全问题应对措施

在区块链应用过程中,由于区块链的公开性,可能导致用户的隐私安全受到威胁,本小节将介绍 4 种针对区块链隐私的保护技术: 点对点混合协议、环签名、非交互式零知识证明以及 Hawk 框架技术.

3.3.1　点对点混合协议

用户通过点对点混合协议,可以混淆自己的交易轨迹,在混合协议中,用户在进行交易时,会同时广播自己的交易信息,在没有任何可信第三方的条件下,通过混合协议,与不相关的匿名客户的资金相混合,完成合成后的交易,由于客户之间是相互匿名的,攻击者很难通过交易结果得到用户的隐私[46],表 4 介绍一些不同的混合协议.由于在混合过程中,攻击者可能会盗窃加密货币且易遭受到单点攻击,点对点混合协议很难在现实中应用.

表 4　相关 P2P 混合协议

协议	类型	特征和属性	优点	缺点
CoinJoin[47]	P2P	使用多重签名交易加强隐私	防止盗窃、降低交易费用	匿名程度取决于参与者的人数,容易受到 DoS 攻击和女巫攻击
CoinShufflfle[48]	P2P	通过密码混合协议来协调 CoinJoin 的去中心化协议	内部不可链接性、有效防止 DoS 攻击和良好的防盗性	较低的匿名性和可否认性
Xim[49]	P2P	匿名合作和多轮混合	分布式配对,内部不可链接性、有效阻止女巫攻击和 DoS 攻击	混合时间较长

续表4 表4 相关P2P混合协议

协议	类型	特征和属性	优点	缺点
Dice Mix [50]	P2P	基于CoinJoin优化的P2P混合解决方案,提高加密货币的匿名性	低混合时间、确保交易者的匿名性	容易受到DoS攻击和女巫攻击,不支持机密交易
Value Shuffle [51]	P2P	基于CoinShufflfle协议,采用机密交易混合方法实现综合交易隐私	具有不可链接性、机密交易兼容性、防盗性以及一次支付交易性	容易受到DoS攻击和女巫攻击

3.3.2 环签名

环签名作为一种数字签名,可从一组可能的签名者中生成匿名有效的签名,且不需要告知实际的签名生成者[52]. 用户A选择一组包含自己的参与者组,并形成环,每个参与者都有一个公钥,用户A用他的私钥和环中成员的所有公钥签署消息,验证者可以知道其中一个参与者组已经对消息进行了签名,但是不知道实际的签名者是谁,因此环签名为签名者提供了完全匿名性.环签名的修改版本之一是可跟踪环签名,这种类型的环签名可以检测两个签名是否由同一个用户产生,每个可跟踪的环签名都有一个标记T,包含每个成员的公钥和特定选项标签,用户A用自己的私钥和标记T进行签名,验证者也用T来验证生成的签名,而不仅仅是公钥.

3.3.3 非交互式零知识证明

零知识证明是一种加密方法,其目的是在不泄露任何额外信息的情况下证明给定的命题,非交互式零知识证明是零知识证明的一种拓展,求证者和证明者之间不需要交互.Sasson等人提出一种应用非交互式零知识证明的数字货币Zerocoin[53],可以同时实现匿名交易和交易隐私安全,Zerocash利用零知识简洁非交互式知识论证(zk-SNARKs)和一个承诺方案隐藏交易的原始地址,并让货币价值赋予在承诺方案和零知识证明中,使货币价值具有可公开验证性.交易的发送方使用接收方的公钥对交易金额和其他元数据进行加密,并在交易中附加密文,使交易金额和目标地址得到保密.虽然Zerocash具有高度的安全性,但在实现匿名交易和交易隐私安全的同时,会消耗极大的算力作为代价.

3.3.4 Hawk

Hawk框架是Kosba等人提出的用于保护智能合约隐私的框架结构[54].Hawk共包含私有部分和公有部分,开发者可以将私人数据和财务信息等以代码的形式写入私有部分,不涉及隐私的信息以代码的形式写入公有部分.Hawk框架程序可以分为三个部分:(1)在虚拟机中执行的部分;(2)仅有用户执行的部分;(3)可信任第三方管理员执行的部分.管理员可以看到Hawk合约中的私有部分但不可以公开,若管理员违背Hawk协议,会自动受到经济处罚,用户将会得到补偿.虽然Hawk在一定程度上可以保护智能合约用户的隐私,但它引入第三方机构,与区块链去中心化的思想有悖.

4 区块链安全研究的不足与趋势

4.1 区块链安全研究的不足

近些年区块链技术的迅速发展,与金融、物联网、供应链、医疗等和我们生活息息相关的各行各业不断融合,使区块链技术愈发成为我们可靠的工具,而区块链安全问题是影响区块链技术发展的核心问题,近几年学者的不断研究,使区块链安全研究取得一系列的突破,但仍然存在着一些不足.

(1)区块链安全技术的实用性仍需提高

尽管一些安全措施的提出在一定程度上缓解了攻击问题,但在实际应用中仍具有一定难度.用来解决双花攻击的FR-P2PK脚本方案虽然在一定程度上可以预防双花攻击,但是同时可能会在交易过程中造成交易资源的浪费,智能合约漏洞检测器Oyente在面对智能合约中一些复杂的漏洞时并不能很好地应对,Hawk框架引入了第三方机构,这与区块链去中心化的思想相悖.诸如此类,如何协调好区块链的去中心化、安全性以及实用性仍是一个亟待解决的难题.

(2)定量研究方法较少

虽然众多学者对区块链安全进行了广泛的研究,但目前部分对区块链安全问题的研究仍停留在理论模型阶段,相关措施可能仅从定义和公式进行推导归纳总结,缺乏相关的实验数据和模拟作为模型的支撑,若进行相关的仿真实验,区块链安全问题的研究将更具有说服力.

4.2　区块链安全研究的趋势

通过对相关研究的梳理与分析,并结合区块链发展背景,本小节提出三种未来区块链安全研究的趋势.

(1) 搭建良好的区块链环境

搭建良好的区块链环境主要包括区块链的网络环境与应用环境.区块链系统搭载在 P2P 网络上,而在网络通信的过程中可能会发生 BGP 劫持等一些安全攻击.同时,区块链应用平台,尤其是以太坊等智能合约平台,由于其丰富的可拓展性,其安全性也应该得到我们足够高的重视.因此,搭建良好的区块链环境,是未来区块链技术应用的基础保障,也是应当重点研究的方向之一.

(2) 建立节能高效的共识算法

共识机制是区块链验证机制的根本,比特币中的 PoW 机制消耗大量的算力且效率低下,PoS 机制虽然在一定程度上节约了算力,但可能由于某些节点权益较高造成不公平的现象甚至危害到区块链系统.如何利用技术的发展,建立一个更为节能高效的共识算法值得探究.

(3) 完善监管机制与审查机制

由于区块链技术是新近发展的技术,相关监管与审查机制并不到位,有些不法份子利用区块链进行违法行为,造成用户的隐私或者财产受到威胁.可想而知,加强对区块链技术的监管与审查,建立完善的机制,是区块链技术应用的重要保障.

5　总结

本文从区块链安全问题分析的角度出发,首先介绍了区块链技术的基本原理和发展现状,然后根据区块链的基础架构,从协议层、扩展层与应用层分别对区块链加密机制安全、共识机制安全、网络通信安全、智能合约安全以及隐私安全五个方面介绍相关的安全问题,并重点介绍相关攻击的原理和后果; 其次,介绍了一些应对措施,并对这些安全措施进行分析与总结,目前而言,针对协议层与扩展层的安全问题,尤其是共识机制与智能合约的相关攻击是影响区块链安全的主要因素; 最后,提出一些区块链技术的研究方向,以期为区块链技术的研究和发展带来一些启发.

参 考 文 献

[1] BECK R, AVITAL M, ROSSI M, et al. Blockchain technology in business and information systems research [J]. Business & Information Systems Engineering, 2017,59(6): 381 - 384.

[2] HUGHES L, DWIVEDI Y K, MISRA S K, et al. Blockchain research, practice and policy: Applications, benefits, limitations, emerging research themes and research agenda [J]. International Journal of Information Management, 2019, 49: 114-129.

[3] JAKE A. Behind the biggest bitcoin heist in history: Inside the implosion of mt.gox [EB/OL]. (2017-4-13) [2020-1-12]. https://www.thedailybeast.com/behind-the-biggest-bitcoin-heist-in-history-inside-the-implosion-of-mt-gox

[4] VITALIK B. Critical update re: Dao vulnerability [EB/OL]. (2016-6-17) [2020-1-12]. https://blog.ethereum.org/2016/06/17/critical-update-re-dao-vulnerability/.

[5] DHVANESH A. Wannacry ransomware attack [EB/OL]. (2017-6-19) [2020-1-12].https://www.igeeksblog.com/wannacry-ransomware-attack/.

[6] NAKAMOTO S. Bitcoin: A peer-to-peer electronic cash system [EB/OL]. (2008-11-1) [2020-1-12].https://bitcoin.org/bitcoin.pdf/

[7] 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.

[8] ZHENG Z, XIE S, DAI H N, et al. Blockchain challenges and opportunities: A survey [J]. International Journal of Web and Grid Services, 2018, 14(4): 352-375.

[9] BACH L M, MIHALJEVIC B, ZAGAR M. Comparative analysis of blockchain consensus algorithms [C] //2018 41st In-

ternational Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO). IEEE, 2018: 1545-1550.

[10] CASTRO M, LISKOV B. Practical Byzantine fault tolerance and proactive recovery [J]. ACM Transactions on Computer Systems (TOCS), 2002, 20(4): 398-461.

[11] WANG S, YUAN Y, WANG X, et al. An overview of smart contract: architecture, applications, and future trends [C] // 2018 IEEE Intelligent Vehicles Symposium (IV). IEEE, 2018: 108-113.

[12] ZHAO J L, FAN S, YAN J. Overview of business innovations and research opportunities in blockchain and introduction to the special issue [J]. Financial Innovation, 2016, 2(1): 28.

[13] MAYER H. ECDSA security in bitcoin and ethereum: a research survey [J]. CoinFaabrik, 2016, 28: 126.

[14] SCHMIDT J M, MEDWED M. A fault attack on ECDSA [C] //2009 Workshop on Fault Diagnosis and Tolerance in Cryptography (FDTC). IEEE, 2009: 93-99.

[15] COURTOIS N T, VALSORDA F, EMIRDAG P. Private key recovery combination attacks: On extreme fragility of popular bitcoin key management, wallet and cold storage solutions in presence of poor RNG events [R]. Cryptology ePrint Archive: Report 2014: 848.

[16] HORALEK J, HOLIk F, HORAK O, et al. Analysis of the use of Rainbow Tables to breakhash [J]. Journal of Intelligent & Fuzzy Systems, 2017, 32(2): 1523-1534.

[17] CORON J S, DODIS Y, MALINAUD C, et al. Merkle-Damgård revisited: How to construct a hash function [C] //Annual International Cryptology Conference. Springer, Berlin, Heidelberg, 2005: 430-448.

[18] KARAME G O, ANDROULAKI E, CAPKUN S. Double-spending fast payments in bitcoin [C] //Proceedings of the 2012 ACM conference on Computer and communications security. ACM, 2012: 906-917.

[19] BASTIAAN M. Preventing the 51%-attack: a stochastic analysis of two phase proof of work in bitcoin [C] //22nd Twente Student Conference on IT. (2015-1-23) [2020-1-18]. http://referaat.cs.utwente.nl/conference/22/paper/7473/preventingthe-51-attack-a-stochasticanalysis-oftwo-phase-proof-of-work-in-bitcoin.pdf. 2015.

[20] NAYAK K, KUMAR S, MILLER A, et al. Stubborn mining: Generalizing selfish mining and combining with an eclipse attack [C] //2016 IEEE European Symposium on Security and Privacy (EuroS&P). IEEE, 2016: 305-320.

[21] VASIN P. Blackcoin's proof-of-stake protocol v2 [EB/OL]. (2014-7-1) [2020-1-18]. https://blackcoin.co/blackcoin-pos-protocol-v2-whitepaper.Pdf.

[22] HEILMAN E, KENDLER A, ZOHAR A, et al. Eclipse attacks on bitcoin's peer-to-peer network [C] //24th {USENIX} Security Symposium ({USENIX} Security 15). 2015: 129-144.

[23] GERVAIS A, RITZDORF H, KARAME G O, et al. Tampering with the delivery of blocks and transactions in bitcoin [C] //Proceedings of the 22nd ACM SIGSAC Conference on Computer and Communications Security. ACM, 2015: 692-705.

[24] APOSTOLAKI M, ZOHAR A, VANBEVER L. Hijacking bitcoin: Routing attacks on cryptocurrencies [C] //2017 IEEE Symposium on Security and Privacy (SP). IEEE, 2017: 375-392.

[25] NATOLI C, GRAMOLI V. The balance attack or why forkable blockchains are ill-suitedfor consortium [C] //2017 47th Annual IEEE/IFIP International Conference on DependableSystems and Networks (DSN). IEEE, 2017: 579-590.

[26] LUU L, CHU D H, OLICKEL H, et al. Making smart contracts smarter [C] //Proceedings of the 2016 ACM SIGSAC conference on computer and communications security. ACM, 2016: 254-269.

[27] NIKOLI C I, KOLLURI A, SERGEY I, et al. Finding the greedy, prodigal, and suicidal contracts at scale [C] //Proceedings of the 34th Annual Computer Security Applications Conference. ACM, 2018: 653-663.

[28] CHEN T, LI X, LUO X, et al. Under-optimized smart contracts devour your money [C] //2017 IEEE 24th International Conference on Software Analysis, Evolution and Reengineering (SANER). IEEE, 2017: 442-446.

[29] LUU L, TEUTSCH J, KULKARNI R, et al. Demystifying incentives in the consensus computer [C] //Proceedings of the 22nd ACM SIGSAC Conference on Computer and Communications Security. ACM, 2015: 706-719.

[30] JEFFREY WILCKE. The Ethereum network is currently undergoing a DoS attack [EB/OL]. (2016-9-22) [2020-1-18]. https://blog.ethereum.org/2016/09/22/ethereum-network-currently-undergoing-dos-attack/

[31] JUELS A, KOSBA A, SHI E. The ring of gyges: Investigating the future of criminal smart contracts [C] //Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security. ACM, 2016: 283-295.

[32] FENG Q, HE D, ZEADALLY S, et al. A survey on privacy protection in blockchain system [J]. Journal of Network and

Computer Applications, 2019, 126: 45-58.
[33] KOSHY P, KOSHY D, MCDANIEL P. An analysis of anonymity in bitcoin using P2P network traffic [C] //International Conference on Financial Cryptography and Data Security. Springer, Berlin, Heidelberg, 2014: 469-485.
[34] ANDROULAKI E, KARAME G O, ROESCHLIN M, et al. Evaluating user privacy in bitcoin [C] //International Conference on Financial Cryptography and Data Security. Berlin, Heidelberg: Springer, 2013: 34-51.
[35] DOUCEUR J R. The sybil attack [C] //International workshop on peer-to-peer systems. Berlin, Heidelberg: Springer, 2002: 251-260.
[36] BISSIAS G, OZISIK A P, LEVINE B N, et al. Sybil-resistant mixing for bitcoin [C] //Proceedings of the 13th Workshop on Privacy in the Electronic Society. 2014: 149-158.
[37] FLEDER M, KESTER M S, PILLAI S. Bitcoin transaction graph analysis [J]. arXiv preprint arXiv, 2015: 1502.01657.
[38] GENNARO R, GOLDFEDER S, NARAYANAN A. Threshold-optimal DSA/ECDSA signatures and an application to Bitcoin wallet security [C] //International Conference on Applied Cryptography and Network Security. Springer, Cham, 2016: 156-174.
[39] PéREZ-SOLà C, DELGADO-SEGURA S, NAVARRO-ARRIBAS G, et al. Double-spending prevention for bitcoin zero-confirmation transactions [J]. International Journal of Information Security, 2019, 18(4): 451-463.
[40] HEILMAN E. One weird trick to stop selfish miners: Fresh bitcoins, a solution for the honest miner [C] //International Conference on Financial Cryptography and Data Security, Berlin, Heidelberg: Springer, 2014: 161-162.
[41] EYAL I, SIRER E G. Majority is not enough: Bitcoin mining is vulnerable [C] //International conference on financial cryptography and data security, Berlin, Heidelberg, Springer, 2014: 436-454.
[42] ALMALLOHI I A I, ALOTAIBI A S M, ALGHAFEES R, et al. Multivariable based checkpoints to mitigate the long range attack in proof-of-stake based blockchains [C] //Proceedings of the 3rd International Conference on High Performance Compilation, Computing and Communications, 2019: 118-122.
[43] WALCK M, WANG K, KIM H S. Tendril Staller: Block delay attack in bitcoin [C] //2019 IEEE International Conference on Blockchain (Blockchain). IEEE, 2019: 1-9.
[44] ZHANG F, CECCHETTI E, CROMAN K, et al. Town crier: An authenticated data feed for smart contracts [C] //Proceedings of the 2016 aCM sIGSAC conference on computer and communications security, 2016: 270-282.
[45] SAAD M, NJILLA L, KAMHOUA C, et al. Mempool optimization for defending against DDoS attacks in poW-based blockchain systems [C] //2019 IEEE International Conference on Blockchain and Cryptocurrency (ICBC). IEEE, 2019: 285-292.
[46] CONTI M, KUMAR E S, LAL C, et al. A survey on security and privacy issues of bitcoin [J]. IEEE Communications Surveys & Tutorials, 2018, 20(4): 3416-3452.
[47] MAXWELL G. CoinJoin: Bitcoin privacy for the real world [C] //Post on Bitcoin forum. 2013.
[48] RUFFING T, MORENO-SANCHEZ P, KATE A. Coinshuffle: Practical decentralized coin mixing for bitcoin [C] //European Symposium on Research in Computer Security. 2014: 345-364.
[49] BISSIAS G, OZISIK A P, LEVINE B N, et al. Sybil-resistant mixing for bitcoin [C] //Proceedings of the 13th Workshop on Privacy in the Electronic Society, 2014: 149-158.
[50] RUFFING T, MORENO-SANCHEZ P, KATE A. P2P mixing and unlinkable bitcoin transactions [C] //Network & Distributed System Security Symposium, 2017.
[51] RUFFING T, MORENO-SANCHEZ P. Valueshuffle: Mixing confidential transactions for comprehensive transaction privacy in bitcoin [C] //International Conference on Financial Cryptography and Data Security. Cham, 2017: 133-154.
[52] RIVEST R L, SHAMIR A, TAUMAN Y. How to leak a secret [C] //International Conference on the Theory and Application of Cryptology and Information Security, Berlin, Heidelberg: Springer, 2001: 552-565.
[53] SASSON E B, CHIESA A, GARMAN C, et al. Zerocash: Decentralized anonymous payments from bitcoin [C] //2014 IEEE Symposium on Security and Privacy. IEEE, 2014: 459-474.
[54] KOSBA A, MILLER A, SHI E, et al. Hawk: The blockchain model of cryptography and privacy-preserving smart contracts [C] //2016 IEEE symposium on security and privacy (SP). IEEE, 2016: 839-858.

[责任编辑 马云彤]