DOI:10.13878/j.cnki.jnuist.2019.05.002

刘九良[1]　付章杰[1]　孙星明[1]

区块链安全综述

摘要

区块链技术提供了一种在开放环境中存储数据、执行交易和处理业务的新方法,具有去中心化、防篡改等优势.从以比特币为代表的1.0时代,到以以太坊为代表的2.0时代,区块链技术已经对金融、物联网、供应链等行业产生了革命性的影响.然而由于技术和管理等方面的问题,目前区块链技术仍面临着很多安全挑战.首先,本文从信息安全、系统安全和隐私安全3个角度讨论了恶意信息攻击、51%攻击、智能合约攻击、拒绝服务攻击等8种区块链技术面临的攻击,分析了这些攻击的原理、执行过程和破坏性.接着,从以上3个角度详细讨论了智能矿池、Securify分析工具、混合技术、零知识证明等12种区块链安全保障技术,分析了这些安全保障技术的原理、执行过程、优点和局限性.最后,对区块链技术的未来研究方向进行了展望.

关键词

区块链;安全保障;隐私保护;智能合约

中图分类号 TP309.2

文献标志码 A

收稿日期 2019-07-28

资助项目 国家自然科学基金(U1836110,U1836208)

作者简介

刘九良,男,硕士生,主要研究方向为区块链信息隐藏.20171211482@nuist.edu.cn

付章杰(通信作者),男,博士,教授,主要研究方向为网络与信息安全.wwwfzj@126.com

1 南京信息工程大学 计算机与软件学院,南京,210044

0 引言

近年来,凭借去中心化、公开性和防篡改等优势,区块链技术引起了学术界和工业界的广泛关注.比特币是第一个以区块链为底层技术的应用,在2015、2016年被评为“最佳表现货币”[1].2016年5月,比特币网络中每天的确认交易总数已经超过了30万[2].进入区块链2.0时代后,以以太坊为代表的智能合约系统已经在物联网[3]、供应链[4]和市场预测[5]等领域被广泛使用.目前,被称为区块链3.0的EOS(Enterprise Operation System,商用分布式设计区块链操作系统)每秒可以处理上千级别的交易量,拥有更加广泛的应用场景.

由于新技术不够成熟、管理不够完善,区块链技术一直面临着很多安全挑战.Matzutt等[6]的研究表明比特币区块链中1.4%的交易包含非金融类信息,甚至包含一些非法和色情信息.一旦这类恶意信息被存储到区块链中,就无法被删除.因此,恶意信息攻击会对区块链的使用者造成永久性的伤害.2014年3月,昔日最大的比特币交易平台Mt.Gox在DDoS(Distributed Denial of Service,分布式拒绝服务)攻击下损失了价值超过4亿美元的比特币.此次事件不仅造成了很多比特币持有者的经济损失,还导致了Mt.Gox公司破产倒闭.智能合约系统同样面临着巨大的安全挑战.2016年6月,犯罪分子利用智能合约中的可重入性漏洞成功攻击了以太坊的DAO项目[7].DAO项目因此损失了6 000万美元.另外,由于区块链的公开性,隐私泄露问题[8]也让很多用户对区块链应用望而生畏.

本文将从信息安全、系统安全和隐私安全3个角度分析区块链技术面临的安全问题,并从以上3个角度分析一些区块链安全保障技术.本文的第1节简要介绍了区块链技术的原理和发展情况;第2节从3个层面详细分析了区块链技术面临的安全问题;第3节对一些区块链安全保护技术进行了分析和讨论.最后,我们展望了区块链技术的未来研究方向,并对全文进行了总结.

1 区块链技术概述

区块链是比特币的底层技术,首次出现在由中本聪在2008年发表的《比特币:一种点对点的电子现金系统》[9]中.文中详细描述了如何建立一套全新的、去中心化的、不需要信任基础的点对点交易体系,其可行性已经被自2009年运行至今的比特币所证明.

1.1 区块链技术的基本原理

区块链本质上是一个不可篡改的、数据不断增长的分布式交易账本.分布式体现在区块链系统中没有一个明确的中心机构.系统中所有的完整客户端节点都是对等的,都保存一份相同的账本.账本中包含区块链系统中所有被确认过的交易.这些交易通常以 Merkle 树的形式存储,并被打包到每个区块中.每个区块都指向上一个区块的头哈希值.这样,所有的区块连接成一条长长的链.这条区块连接成的链被称为区块链.

区块链技术通过去中心化共识机制保证整个网络承认同一条链.区块链中的新交易会被 P2P 网络广播到其他节点.接收到交易的节点需要根据一定的标准对交易进行独立验证.一旦验证不通过,这笔交易就会被验证节点丢弃.为了保证所有节点对交易账本达成去中心化共识,区块链网络中的工作量证明(Proof of Work)算法通过竞争的方式挑选出"记账员".这名"记账员"也就是挖矿成功的矿工.挖矿过程其实是努力求解数学难题的过程.最先求解成功的矿工拥有一次记账权,即将打包的区块连接到链上的权利.作为奖励,"记账员"会获得奖金和交易费."记账员"计算出的难题答案会被放到新区块中,作为矿工的工作量证明.在这种工作量证明机制下,每个节点都会独立地选择累计工作量最大的链,最终整个区块链网络达成一种去中心化的共识.

由于每个区块都指向上一个区块的头哈希值,要想篡改一个区块的交易记录,必须重新计算该块之后的所有区块.根据比特币网络的算力以及现有的计算设备,一般一个区块后有 6 个区块就很难被篡改了.

1.2 区块链技术的发展

以比特币为首的加密数字货币时代被称为是区块链 1.0 时代.为了增加区块链应用的灵活性,区块链 2.0 向用户提供了可编程的脚本.其中,图灵完备的分布式智能合约系统以太坊是这个时代的代表.智能合约是部署在区块链上的去中心化、可信息共享的程序代码.签署合约的各参与方就合约内容达成一致,将内容以脚本的形式部署在区块链上,即可不依赖任何中心机构自动化地代表各签署方执行合约.然而,由于延迟和数据吞吐量的难题,以太坊每秒只能处理 30~40 笔交易.因此以太坊很难成为主流的交易场景.为了实现分布式应用的性能拓展,EOS 通过并行链和 DPOS(Delegated Proof Of Stake,委托权益证明)解决了这两个难题.EOS 每秒可以处理上千笔交易,被认为是区块链 3.0 时代的代表.

2 区块链面临的安全问题

本节将从信息安全,系统安全和隐私安全 3 个角度分析区块链技术面临的安全问题.本节分析的一些攻击方式曾成功地攻破区块链系统,例如 51% 攻击、智能合约漏洞和拒绝服务攻击.有些攻击方式仍未攻破区块链系统,如一些加密算法攻击.然而主动防御才是解决区块链安全问题的最有效途径.

2.1 信息安全问题

信息安全问题是指区块链的信息传递功能可能被一些恶意节点利用.区块链本质上是一个分布式的数据库.在公有链中这个数据库对所有人开放,在许可链中这个数据库向部分人开放.因此,一旦有恶意节点传输恶意信息到区块链上,区块链网络中的其他节点都会成为受害者.Matzutt 等[6]的研究显示,比特币区块链中包含 1.4%的非金融数据.其中包括一些恶意内容,例如指向色情内容的链接.由于区块链系统中缺乏中心机构,人们很难管控被发布到区块链上的内容.图 1 展示了一位用户在以太坊中发布的信息.这位用户表示人们应该小心区块链中的垃圾信息.

表 1 展示了部分 Matzutt 等[6]总结的嵌入信息到区块链中的方法.这些嵌入方法的隐蔽性较低,容易被其他用户发现.表中的开销表示嵌入每个字节需要消耗的美元数(根据当时的比特币价格计算).OP_RETURN 脚本允许用户在一笔比特币交易中输入 80 B 的注释信息.Coinbase 交易是指区块中的第

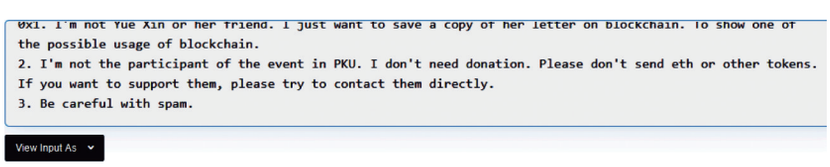


图 1 以太坊中的任意信息

Fig. 1 Arbitrary information in Ethereum

一笔交易,由挖矿成功的矿工执行.Coinbase 交易允许矿工嵌入 96 B 的任意信息.表 1 中的后 3 种方案通过比特币交易脚本嵌入任意信息.例如,比特币地址“15gHNr4TCKmhHDEG31L2XFNvpnEcnPSQvd”在区块链中以 16 进制形式存储:334E656C736F6E2D4D616E64656C612E6A70673F.这个 16 进制码可以转换为 Unicode 字符串:‘3Nelson-Mandela.jpg?’.用户可以根据要上传的信息选择比特币的输出地址构建一笔包含任意信息的交易.

表 1 简单的数据嵌入方法

Table 1 Low-level data insertion methods

嵌入方法	最大嵌入量/B	开销/美元	效率
OP_RETURN	80	3.18~173.55	低
Coinbase	96	无	低
P2PK	85 345	1.24~207.79	高
P2MS	92 625	1.11~234.33	高
P2SH Out.	62 400	1.03~225.61	高

Alsalami 等[10]指出人们可以使用一些传统的信息隐藏方法在区块链中隐蔽地传输秘密信息.例如,一个区块链节点可以申请多个交易地址.发送方 Alice 可以选择任意地址进行一笔交易.如果发送方 Alice 和接收方 Bob 事先约定了一种规则,如地址 A1 代表 0,地址 A2 代表 1,他们之间就可以进行隐蔽通信.Partala[11]证明了这种在区块链中隐蔽通信的方法是安全的,即通信双方可以确保信息被对方接受.一旦这种方法被人恶意使用,区块链很可能成为不法分子传输信息的秘密通道.

2.2 系统安全问题

系统安全问题是指区块链系统漏洞引起的安全问题.攻击者可以利用这些漏洞盗取数字货币,甚至单纯地破坏区块链系统.系统安全是区块链安全的根本,主要包括共识算法安全、加密算法安全、智能合约安全和系统资源安全.针对这 4 个方面,本节分析了 4 种类型的攻击:51%攻击、加密算法攻击、智能合约攻击和分布式拒绝服务攻击.

2.2.1 51%攻击

对于工作量证明算法(Proof of Work),51%攻击是指某个拥有全网 50%以上算力的矿工可以攻击整个区块链系统.由于这个矿工可以生成绝大多数的块,他就可以通过故意制造分叉来实现“双重支付”,或者通过拒绝服务的方式来阻止特定的交易或攻击特定的钱包地址.虽然个体很难获得 50%以上的算力,但某些大型矿池可能做到.2014 年 1 月,ghash.io 矿池的算力已经达到了比特币网络的 42%.为了防止 ghash.io 的算力超过全网的 50%,很多矿工自愿退出了矿池[12].2018 年,Blockchain.com 网站曾经报道,5 大矿池的总算力已经超过了全网算力的 70%.如果这些矿池之间进行合作,51%攻击很容易被实现.对于权益证明算法(Proof of Stake),如果某个矿工的拥有币的总量超过全网的 50%,也可以发动 51%攻击.一旦 51%攻击发生了,攻击者之外的其他节点不会承认攻击者生成的链条,整个网络中的币可能变的一文不值.所以,从攻击者利益的角度来看,51%攻击很难在现实中发生.

2.2.2 加密算法攻击

区块链的安全性依赖于密码学加密算法的强度.多数区块链操作都会使用密码学中的哈希算法.例如,区块之间通过区块头哈希值进行连接;交易地址通常由哈希操作产生.SHA-256(Secure Hash Algorithm-256,哈希 256 算法)是多数区块链使用的哈希算法.一些区块链也使用 Ripemd160(RACE Integrity Primitives Evaluation Message Digest 160,RACE 原始完整性校验消息摘要 160)算法和 sCrypt 算法.然而,这些哈希算法都可能遭受 Hash 碰撞攻击.目前,SHA-256 算法被认为是不可攻破的,但仍可能受到长度扩展攻击.攻击者可以利用长度扩展攻击在原始数据的后面附加一些自定义数据,进而改变消息的哈希值.Ferguson 等[13]指出,双重 SHA-256 可以用于防止长度扩展攻击.

非对称加密算法对区块链的安全也至关重要.例如,区块链交易的公钥和私钥一般由 ECDSA(Elliptic Curve Digital Signature Algorithm,椭圆曲线数字签名算法)产生.一些区块链,如比特币和以太坊,使用了特定的 ECDSA 算法——secp256k1 椭圆曲线算法.这种椭圆曲线采用了特殊的构造方式,允许高效计算.然而,Bernstein 等[14]的研究表示,secp256k1 中存在一些可能导致弱点的缺陷.因此 secp256k1 被评估为不安全的加密算法.斯坦福大学[15]的一个研究表明,椭圆加密算法中的加法和倍增操作在时间和性能开销上差异很大.因此人们可以对椭圆加密算法进行侧信道攻击.椭圆加密算法还依赖于安全的随机数生成器.Ducklin[16]的研究表明一些安卓比特币钱包被盗和基于 java 的伪随机数生成器存在漏洞有关.此外,量子计算一直威胁着传统密码学的安全.

未来,量子计算很可能成功破解 ECDSA、DSA(Digital Signature Algorithm,数字签名算法)等非对称加密算法,并导致 SHA-256 算法和 AES(Advanced Encryption Standard,高级加密标准)算法的加密强度减半.

2.2.3 智能合约漏洞

智能合约本质上是运行在区块链上的程序,由开发人员编写.由于目前以太坊等区块链系统的智能合约漏洞防范措施不够完善,安全意识一般的合约开发者很可能开发出包含致命漏洞的智能合约.黄凯峰等[17]对智能合约安全问题进行了分析和总结.付梦琳等[18]对智能合约漏洞分析工具进行了研究.Luu 等[19]提出的合约分析器 Oyente 发现了 4 种潜在的智能合约安全漏洞.他们分析了 19 366 份以太坊智能合约,发现 8 833 份合约是易受攻击的.4 种漏洞的详情如下:

1) 交易顺序依赖漏洞:在区块链中,每个区块中都包含很多交易.一个区块中交易的顺序是由矿工决定的.例如,一个区块中存在交易 t1 和 t2,并且这 2 个交易都由同一个合约产生.这时候矿工可以选择先执行 t1 或先执行 t2.然而有些合约对交易的执行顺序是有依赖性的,错误的执行顺序可能对合约造成负面影响.

2) 时间戳依赖漏洞:在区块链中,每个区块的时间戳用于记录区块的诞生时间.然而时间戳是完全由矿工决定的.如果某个合约将时间戳作为代码的触发条件,就很容易出现业务逻辑混乱的现象.

3) 未处理异常漏洞:这种漏洞通常在合约相互调用时发生.例如,当合约 A 调用合约 B 时,合约 B 发生了异常,并停止执行,返回 false.在某些情况下,合约 A 需要显式地检查调用是否被正确执行.如果合约 A 没有正确地检查异常信息,未处理异常漏洞就发生了.

4) 可重入性漏洞:当外部地址或其他合约向一个合约地址发送以太币时,该合约的 fallback 函数就会被执行.攻击者可以利用 fallback 函数调用 withdraw 函数实现递归调用合约.这种攻击可以盗取用户的以太币.

表 2 总结了一些智能合约漏洞引发的攻击案例.2016 年的 The DAO 事件是第一起智能合约攻击事件.黑客利用可重入性漏洞盗取了 DAO 项目的所有资金.此后,智能合约攻击事件频繁发生.2017 年 7 月,由于 Parity 多重签名钱包的 initWallet 函数是公开函数,攻击者通过调用 initWallet 函数直接改变了钱包的所有者.因此 Parity 损失了价值 3 000 万美元的以太币.同年 11 月,一位用户名为“devops199”的开发人员意外调用了 kill 函数,导致 Parity 钱包中所有智能合约失效,钱包中的加密数字货币再也无法找回.2018 年 4 月,Beauty Chain 因为整数溢出漏洞被盗取了大量 BEC 代币,损失了上百亿美元.被称为区块链 3.0 的 EOS 也频频发生智能合约攻击事件.2018 年 9 月,黑客通过利用 EOSBet 合约在校验收款方时存在的漏洞伪造了转账通知.黑客利用自己的两个账号相互转账,以零成本获取平台的巨额奖励.这次攻击导致 EOS 损失了 80 万美元.EOS 从诞生至今已经遭受了 10 次以上的智能合约攻击,损失超过千万美元.

表 2 智能合约攻击案例

Table 2 Attack cases of smart contracts

案例	发生时间	攻击类型	造成损失
The DAO	2016-06	可重入性漏洞	6 000 万美元
Parity 钱包	2017-07	权限控制问题	3 000 万美元
Devops199	2017-11	意外 kill	2.8 亿美元
Beauty Chain	2018-04	整数溢出	100 亿美元
EOSBet	2018-09	伪造转账	80 万美元

2.2.4 分布式拒绝服务攻击

拒绝服务攻击旨在破坏对特定目标的网络或资源的访问.由多个位置的攻击者同时发动的拒绝服务攻击被称为分布式拒绝服务攻击.一旦分布式拒绝服务攻击发生在区块链中,整个区块链网络可能面临瘫痪.在以太坊中发送交易需要消耗一定量的 gas(交易费).这种机制可以在一定程度上抵制 DoS 攻击.然而由于以太坊的 EXTCODESIZE 操作码的 gas 消耗定价过低,攻击者曾成功地对以太坊发动了 DoS 攻击[20].EXTCODESIZE 操作码是用来读取智能合约代码大小的.EXTCODESIZE 被调用时,节点需要读取磁盘的状态信息.由于 EXTCODESIZE 只消耗 20 gas,攻击者可以在一笔交易中执行 5 万次 EXTCODESIZE 操作.这种攻击可以消耗区块链网络大量的计算资源和网络资源,导致区块链网络拥堵甚至瘫痪.

一些攻击者还使用了 SUICIDE 操作码发动 DoS 攻击[21].攻击者们使用 SUICIDE 操作产生了 1 900 万个空账户.由于空账户需要被存储在状态树中,大量的空账户浪费了磁盘资源.在这种攻击模式下,区块链网络的节点同步速度和交易处理速度都有较大

的下降.智能合约代币所有者的权限过大也可能导致拒绝服务攻击.如果代币合约所有者一直冻结合约,合约中的其他用户将无法进行交易.

2.3 隐私安全问题

虽然一些用户认为区块链是匿名的,但是多数区块链都没有达到匿名的程度.虽然区块链交易地址没有和用户的真实身份绑定在一起,但是根据区块链上公开的交易记录,人们仍可以推测出某个账户地址对应的使用者真实身份.事实上,区块链用户只是使用"假名"进行交易.Chainalysis 公司[22]和 Elliptic 公司已经可以提供识别区块链钱包使用者真实身份的服务.美国国税局已经批准通过 Chainalysis 公司查找偷税漏税者.通过分析区块链的 p2p 网络,攻击者可以找到交易地址对应的 IP 地址.例如,Koshy 等[23]从 p2p 网络角度分析了交易的转发模式,进而得出一些比特币交易对应的 IP 地址.Bissias 等[24]指出女巫攻击可以破坏区块链的分布式匿名协议,增加发现用户真实身份的可能性.

除了个人身份信息,业务信息也可能是用户需要保护的重要隐私.本文将业务隐私分为交易隐私和合约隐私.交易隐私是指区块链交易包含的交易金额、交易时间等隐私.如果攻击者可以将某个用户的交易链接起来,用户的账户余额、生活习惯等信息很可能被攻击者获取.交易图分析可以通过机器学习等手段获取交易吞吐量、交易模式等信息.Ron 等[25]利用这种方式发现了比特币网络中的 4 种典型的交易模式.利用这些交易模式信息和去匿名化技术,攻击者可以获取一个人的财政历史.合约隐私是指智能合约中包含的业务隐私.智能合约在医疗、物联网、供应链等领域有广泛的应用.这些领域往往对隐私保护的要求较高.例如,与医疗相关的智能合约很可能包含用户的健康隐私信息;与物联网相关的智能合约可能包含传感器获取的用户隐私.

3 区块链安全保障技术

本节将分析一些区块链安全保障技术.虽然这些技术可以提高区块链的安全性,但是可能会对区块链的去中心化、可扩展性产生一定的负面影响.在实际使用中,我们应该根据业务需求选择合适的安全保障技术.

3.1 信息安全

Matzutt 等[26]提出了 3 种阻止恶意信息被上传到区块链上的方法.这些方法提高了攻击者上传恶意信息的门槛.3 种方法如下:

1)内容过滤器:内容过滤器可以检测交易中的可读字符串,并拒绝包含恶意字符串的交易被执行.

2)强制最低交易费:该措施可以使在大型交易中插入恶意信息在经济上不可行,但也造成了无辜用户的经济损失.

3)地址自校验:该方法可以阻止用户使用任意交易地址传递信息.

以上 3 种方法的结合使用可以在一定程度上限制用户上传恶意信息.然而这些措施也会影响无辜用户的体验:强制最低交易费可能会增加无辜用户的交易费用;内容过滤器和地址自校验会增加无辜用户的交易时间.

μchain[27]可以根据共识机制修改区块中的内容.因此如果检测到 μchain 中包含恶意信息,人们可以将这些信息永久删除.虽然利用隐写术可以在区块链中隐蔽通信,但相应的隐写分析技术[28]也可以检测区块链中的隐蔽信息.利用 μchain 和隐写分析术,人们可以检测并删除被上传到区块链上的恶意信息.然而 μchain 的可修改机制也会在一定程度上降低区块链的安全性.

区块链的信息安全不仅需要技术的支持,更需要道德的约束和法律的保障.2019 年 1 月 10 日,中国国家互联网信息办公室发布了《区块链信息服务管理规定》.同年 5 月 23 日,《区块链信息服务管理规定》发布了明确管理责任,提供法律依据.规定明确指出,对于违反法律、行政法规和服务协议的区块链信息服务使用者,应当依法采取处理措施;构成犯罪的,依法追究刑事责任.

3.2 系统安全

本节将分析 3 种区块链安全保障技术:SmartPool、智能合约分析器和定量框架.SmartPool 用于解决区块链矿池引起的 51%攻击问题;智能合约分析器可以检测合约中的漏洞;定量框架可以在区块链安全和性能之间做出正确权衡.

3.2.1 SmartPool

2.2.1 节中提到,曾有矿池的算力超过了全网算力的 40%,这与区块链的去中心化思想相违背.Luu 等[29]提出的 SmartPool 是一种基于以太坊智能合约的矿池,旨在提供高效的,分布式的挖矿服务.SmartPool 的执行过程如图 2 所示.图 2 的左侧表示矿工,右侧表示 SmartPool 矿池.首先,矿工挖矿前需要构造区块模版,即将矿池合约的地址作为

Coinbase 地址.接着,矿工开始挖掘份额.挖掘到足够的份额后,矿工开始构建增广梅克尔树(用于安全高效地证明),并提交份额到矿池.矿池收到份额后,矿工开始提交 ShareProof 证明.最后,矿池根据 ShareProof 证明的验证情况发放奖励.矿池合约中的 claimList 用于存储用户提交的份额,verClaimList 用于存储证明的验证情况.矿池的验证机制可以高效地检测出无效份额或被夸大的份额.验证失败的矿工无法获得任何收益.

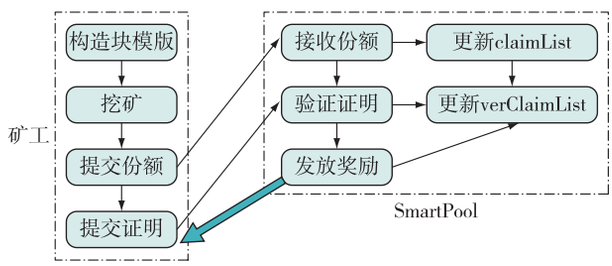


图 2　SmartPool 的执行过程

Fig. 2　Overview of SmartPool's execution process

与传统的 P2P 矿池相比,SmartPool 有如下优势:

1)去中心化:SmartPool 的核心功能是通过部署在区块链上的智能合约实现的.矿工挖矿需要通过矿池客户端连接到以太坊.矿池依赖以太坊的共识机制运行,而不是依赖某个矿池拥有者.

2)高效:矿工只需要发送部分份额给 SmartPool 验证,因此 SmartPool 比 P2P 矿池更高效.增广梅克尔树也可以提高验证的效率.

3)安全:SmartPool 的智能合约可以识别出不诚实的矿工,只有诚实的矿工能够按贡献比例获得奖励.

SmartPool 本质上是基于以太坊智能合约的矿池.显然智能合约并不是绝对安全的.如果 SmartPool 智能合约存在漏洞,攻击者可能利用这些漏洞欺骗矿池,进而盗取大量的挖矿收益.此外,由于以太坊智能合约的可扩展性不够强(每秒处理的交易数量较少),SmartPool 并没有被广泛使用.

3.2.2　智能合约漏洞分析器

Luu 等[19]提出了可以检测智能合约漏洞的合约分析器——Oyente.Oyente 利用符号执行技术分析智能合约编译生成的字节码,并跟踪字节码在以太坊虚拟机中的执行过程.由于以太坊将字节码存储在自己的区块链中,Oyente 可以用于检测已经部署完毕的合约.Oyente 将以太坊字节码和全局状态作为输入,核心模块包括 4 个部分:控制流图构建器、探测器、核心分析器和验证器.首先,Oyente 根据字节码静态地构建智能合约的控制流图.然后,探测器根据以太坊状态、控制流图信息和静态符号执行模拟合约的运行.核心分析器会利用相关的分析算法检测各种漏洞.验证器验证漏洞后,可视化模块将漏洞分析情况展示给用户.

Tsankov 等[30]提出了一种可扩展的、自动化的智能合约漏洞分析工具——Securify.Securify 可以明确地指出合约是否是安全的.首先,Securify 通过分析合约的依赖图提取代码的精确语义信息.然后,Securify 根据语义信息检查遵从模式和违反模式.最后,Securify 根据检查的结果对合约的安全性进行分类.Mueller 等[31]开发了 Mythril 分析器.Mythril 是一个以太坊字节码漏洞分析工具.它使用符号执行,SMT(Satisfiability Modulo Theories,可满足性模理论)solver 和污点分析检测合约漏洞.

表 3 对 3 种工具进行了横向对比.代码覆盖率是指源代码被测试的比例.Oyente 分析工具的代码覆盖率相对较高,但不能检测整数溢出漏洞和一些公平性漏洞.Securify 自动化程度较高,可以减少大量的人力.跟其他两种方法相比,Securify 各个方面都有一定的优势.Mythril 可以和其他分析工具结合使用,有较好的可扩展性,但在正确率和效率方面表现较差.然而由于智能合约分析工具的起步较晚,目前已有的智能合约分析工具仍然难以保障智能合约安全.这些工具都存在代码覆盖率低,误报率高的缺点,而且多数合约分析工具自动化程度较低.

表 3　智能合约分析工具对比

Table 3　Comparison of smart contract analysis tools

分析工具	优点	缺点	花费时间/s
Oyente	代码覆盖率高	漏洞类型少	30
Securify	自动化程度高	—	20
Mythril	可扩展性高	误报率高,效率低	60

3.2.3　定量框架

区块链的可扩展性、去中心化和安全性不可能同时提高,必须有所取舍.这就是以太坊创始人 Vitalik 提出的区块链技术的“三元悖论”.为了在可扩展性和安全性之间做出正确权衡,Kosba 等[32]提出了定量框架.定量框架主要用于分析基于 PoW 的区块链的执行性能和安全措施.这个框架主要包含 2 个部分:区块链模拟器和安全模型.区块链模拟器用于模仿区块链的行为,输入为共识协议和区块链网

络参数.模拟器通过分析可以获得区块的传播次数、块大小、网络延时、陈腐块率和吞吐量等信息.陈腐块是指一些已经被挖出但没有被写到链上的区块.吞吐量表示区块链每秒可以处理的交易数量.收到这些统计信息后,安全模型根据马尔科夫决策过程生成最优的对抗策略.定量框架可以在一定程度上提高区块链的安全性.

3.3 隐私安全

本节将分析3种区块链隐私保护技术:混合技术,零知识证明和Hawk框架.混合技术是一种相对简单的隐私保护技术,可以用于保护用户的身份隐私;零知识证明通过复杂的密码学技术保护隐私,可以用于保护用户的身份隐私和业务隐私;Hawk框架利用零知识证明等技术保护智能合约隐私.

3.3.1 混合技术

混合服务主要用于保护用户的身份隐私,防止交易被链接.Bonneau等[33]提出的Mixcoin可以实现比特币的匿名支付.Mixcoin是一种中心化的混合服务,负责将多笔不相关的交易混合成若干笔交易.不诚实的Mixcoin中心机构可能盗取用户的比特币.为了防止这个问题,Mixcoin增加了一个基于签名的问责机制.这种机制可以曝光混合者的盗窃行为,让作弊机构的信誉受到损失.然而问责机制并不能从技术上完全阻止中心机构的不诚实行为.2013年出现的CoinJoin[34]是一种分布式的混合服务.多个需要交易的用户可以在没有中心机构的情况下进行合作,将多笔交易合并成一笔交易.合作者之间可能互不相识.因此攻击者很难通过合成的交易分析出交易者的身份.然而CoinJoin服务在没有中心服务器的情况下仍然难以实行.CoinJoin的不正确实现降低了协议的隐私保护性.Kristov开发了一个名为“CoinJoin Sudoku”的工具.这个工具能够识别SharedCoin(一个实现CoinJoin的混合服务中心机构)交易,并且可以发现特定的付款人和收款人之间的关系.为了解决这个问题,Tim等[35]使用Dissent技术扩展了CoinJoin的概念,提出了CoinShuffle.CoinShuffle可以在没有可信第三方的情况下实现混合服务,是完全分布式的混合服务协议,并且可以防止偷盗.

混合服务可以在很大程度上增加攻击者获取用户隐私的难度.然而,集中混合服务容易遭受单点攻击;分布式混合服务在现实中难以完美地实现.另外,混合服务很难保护用户的业务隐私,即无法保护交易金额、交易数据和合约内容等信息.

3.3.2 非交互式零知识证明

零知识证明是密码学中的一个概念,目标是证明一个给定的命题而不泄露任何附加信息.非交互式零知识证明是零知识证明的一个变种,无需证明者和验证者之间相互交互.Zerocoin采用了非交互式零知识证明保护用户的交易隐私,被挖出的Zerocoin币可以进行赎回操作,被赎回的Zerocoin币会进入一个收集器,当用户花销时,Zerocoin只显示用户在收集器中拥有币而不显示拥有哪个币[36].然而Zerocoin没有隐藏交易金额的功能,并且容易遭受侧信道攻击.Zerocash进一步解决了这两个问题,提高了隐私保护的级别[37].Zerocash采用简洁性非交互式零知识证明(zk-SNARKs)和一个承诺方案隐藏交易的地址.Zerocash的发送方会利用接收方的公钥对交易金额和交易元数据进行加密.密文被添加在交易之后.根据公钥加密的安全性,这种交易不会泄露交易金额和目标地址.Zerocash虽然获得了极高的匿名性并且保护了交易隐私,但是需要花费较高的计算资源.另外,Zerocoin和Zerocash的可扩展性较弱,它们都没有智能合约功能.

3.3.3 Hawk

为了保护智能合约的交易隐私,Ahmed等[38]提出了Hawk框架.使用Hawk的合约开发者无需了解密码学和隐私保护的知识,编写私有智能合约就能有效地保护隐私.Hawk包含私有智能合约和公开智能合约两个部分.开发者可以将隐私数据和交易金额等信息写入私有合约,将可以公开的部分写入公开合约.Hawk的编译过程包括3个部分:1)以太坊虚拟机执行程序;2)智能合约用户执行程序;3)管理员执行程序.管理员可以是一个值得信任的第三方,也可以是Intel SGX(可以防止隐私泄露).

图3展示了一个在Hawk中实现的密封拍卖案例.在Hawk中,密封拍卖的投标者通过私有合约进行投标.私有合约通过zk-SNARKs保护用户的投标金额隐私,并且可以计算出投标胜利者.管理员根据最终的结果返回资金并发放奖励.为了防止作弊,管理员需要事先在公共合约中存储一定的金额.如果管理员出现操作超时等行为,这些资金会转移给所有投标者.当然,如果采用可信计算设备作为管理员,Hawk系统将更加安全.虽然Hawk在提供智能合约的情况下保护了用户隐私,但Hawk的可扩展性不是很强,而且不是完全的去中心化.

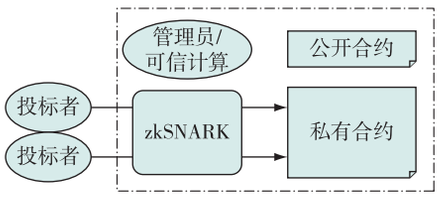


图 3　Hawk 中的密封拍卖案例

Fig. 3　An example of sealed auction in Hawk

4　未来方向

本节将列举 3 个未来可能的研究方向:

1)区块链的三元悖论表明区块链技术很难在去中心化、可扩展性和安全性 3 个方面同时提高.例如,以太坊的可扩展性高于比特币,但安全性却低于比特币;零币的安全性高于以太坊,但可扩展性低于以太坊.如何根据实际的应用场景在 3 种属性之间做出权衡是区块链应用的关键.因此,如何定量衡量 3 种属性之间的关系并根据需求动态调整 3 种属性是未来的一个研究方向.

2)共识机制是区块链安全的根本,但工作量证明机制导致浪费了大量的算力.而深度学习的训练过程也需要消耗大量算力.如果可以将深度学习的训练过程同时作为区块链的挖矿过程,矿工们可以节省大量的硬件资源和电力资源.因此如何利用深度学习技术创造新的区块链共识机制是未来的一个研究方向.

3)区块链隐私保护技术固然可以为普通人的隐私安全提供保障,但不法分子也可能利用这些技术逃避法律的惩罚.目前,区块链技术还没有完善的监管机制和审计机制.如何在提供隐私保护的情况下监管区块链中的不法交易仍是未来需要解决的难题.

5　总结

本文首先介绍了区块链的基本原理,然后从信息安全、系统安全和隐私安全 3 个角度分析了区块链技术面临的安全问题.接着,本文分析了一些区块链安全保护技术,并对这些技术的优缺点进行了总结.虽然信息安全目前受到的关注较少,但区块链中恶意信息的危害已经初步展现出来了.区块链上的隐藏的信息也有可能对社会安全造成危害.系统安全是区块链安全的根本,目前多数攻击针对的是区块链的系统安全.与此同时,区块链系统也在被攻击的过程中不断更新技术,修复漏洞.区块链作为公开性的交易账本,隐私保护是用户关心的重大问题.目前很多区块链应用已经可以较好地保护用户的隐私.我们相信,随着技术的发展和管理规范水平的提高,未来区块链技术会在解决这 3 大安全问题的道路上持续进步.

参考文献

References

[1] Desjardins J. It's official: bitcoin was the top performing currency of 2015, 2016[EB/OL]. [2019-06-05]. http://money. visualcapitalist. com/its-official-bitcoin-was-the-top-performing-currency-of-2015/

[2] Confirmed transactions per day, 2017[EB/OL]. [2019-06-05]. https://blockchain. info/charts/n-transactions?timespan=all/#

[3] Zhang Y, Wen J T. The IoT electric business model: using blockchain technology for the Internet of Things[J]. Peer-to-Peer Networking and Applications, 2017, 10(4): 983-994

[4] Skuchain [EB/OL]. [2019-06-05]. http://www.skuchain.com/

[5] Augur[EB/OL]. [2019-06-05]. http://www.augur.net/

[6] Matzutt R, Hiller J, Henze M, et al. A quantitative analysis of the impact of arbitrary blockchain content on bitcoin[C]//Proceedings of the 22nd International Conference on Financial Cryptography and Data Security (FC), Springer, 2018

[7] Buterin V. Critical update RE: Dao vulnerability, 2016[EB/OL]. [2019-06-05]. https://blog. ethereum. org/2016/06/17/critical-update-re-dao-vulnerability/

[8] Miller A, Möser M, Lee K, et al. An empirical analysis of linkability in the monero blockchain[J/OL]. arXiv e-print, 2017. https://arxiv.org/abs/1704. 04299

[9] Nakamoto S. Bitcoin: a peer-to-peer electronic cash system[EB/OL]. [2019-06-05]. http://bitcoin.org/bitcoin.pdf

[10] Alsalami N, Zhang B. Uncontrolled randomness in blockchains: covert bulletin board for illicit activities[EB/OL]. [2019-06-05]. https://eprint. iacr. org/eprint-bin/getfile. pl? entry = 2018/1184&version = 20181210: 211536&file = 1184. pdf

[11] Partala J. Provably secure covert communication on blockchain[J]. Cryptography, 2018, 2(3): 18

[12] Hajdarbegovic N. Bitcoin miners ditch ghash.io pool over fears of 51% attack, 2014[EB/OL]. [2019-06-05]. http://www. coindesk. com/bitcoin-miners-ditch-ghash-iopool-51-attack/

[13] Ferguson N, Schneier B. Practical cryptography[M]. New York: Wiley, 2003

[14] Bernstein D J, Lange T. Safecurves: choosing safe curves for elliptic-curve cryptography[EB/OL]. [2019-06-05]. http://safecurves.cr.yp.to/

[15] University Stanford. Pertinent side channel attacks on elliptic curve cryptographic systems[R]. Stanford: Stanford

University,2011
[16] Ducklin P. Android random number flaw implicated in bitcoin thefts[EB/OL].[2019-06-05].https://nakedsecurity.sophos.com/2013/08/12/android-random-number-flaw-implicated-in-bitcoin-thefts/
[17] 黄凯峰,张胜利,金石.区块链智能合约安全研究[J].信息安全研究,2019,5(3):192-206
HUANG Kaifeng,ZHANG Shengli,JIN Shi.The security research of blockchain smart contract[J].Journal of Information Security Research,2019,5(3):192-206
[18] 付梦琳,吴礼发,洪征,等.智能合约安全漏洞挖掘技术研究[J].计算机应用,2019,39(7):1959-1966
FU Menglin,WU Lifa,HONG Zheng,et al.Research on smart contracts vulnerability mining technique[J].Journal of Computer Applications,2019,39(7):1959-1966
[19] Luu L,Chu D,Olickel H,et al.Making smart contracts smarter[C]//Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security-CCS'16,Vienna,Austria.New York,USA:ACM Press,2016
[20] Gautham.Ethereum network comes across yet another DoS attack[EB/OL].[2019-06-05].http://www.newsbtc.com/2016/09/23/ethereum-dao-attack-attack-platforms-credibility/
[21] Rivlin B. Vitalik buterin on empty accounts and the ethereum state[EB/OL].[2019-06-05].https://www.ethnews.com/vitalik-buterin-on-empty-accounts-and-theethereum-state
[22] Chainalysis[EB/OL].[2019-06-28].https://www.chainalysis.com/
[23] Koshy P,Koshy D,McDaniel P.An analysis of anonymity in bitcoin using P2P network traffic[M]//Financial Cryptography and Data Security.Berlin,Heidelberg:Springer Berlin Heidelberg,2014:469-485.DOI:10.1007/978-3-662-45472-5_30
[24] 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-WPES'14,Scottsdale,Arizona,USA.New York,USA:ACM Press,2014
[25] Ron D,Shamir A.Quantitative analysis of the full bitcoin transaction graph[M]//Financial Cryptography and Data Security.Berlin,Heidelberg:Springer Berlin Heidelberg,2013:6-24.DOI:10.1007/978-3-642-39884-1_2
[26] Matzutt R,Henze M,Ziegeldorf J H,et al.Thwarting unwanted blockchain content insertion[C]//2018 IEEE International Conference on Cloud Engineering(IC2E),Orlando,FL.New York,USA:IEEE,2018
[27] Puddu I,Dmitrienko A,Capkun S.μchain:how to forget without hard forks[J].IACR Cryptology ePrint Archive,2017:106
[28] Wang H Q,Wang S Z.Cyber warfare[J].Communications of the ACM,2004,47(10):76-82
[29] Luu L,Velner Y,Teutsch J,et al.Smartpool:practical decentralized pooled mining[C]//Proceedings of the 26th USENIX Security Symposium August 16-18,2017,Vancouver,BC,Canada,2017
[30] Tsankov P,Dan A,Drachsler-Cohen D,et al.Securify:practical security analysis of smart contracts[C]//Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security-CCS'18,Toronto,Canada.New York,USA:ACM Press,2018
[31] Mueller B,Honig J,Parasaram N,et al.ConsenSys/mythril[EB/OL].[2019-06-25].https://github.com/ConsenSys/mythril
[32] Gervais A,Karame G O,Wüst K,et al.On the security and performance of proof of work blockchains[C]//Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security-CCS'16,Vienna,Austria.New York,USA:ACM Press,2016
[33] Bonneau J,Narayanan A,Miller A,et al.Mixcoin:anonymity for bitcoin with accountable mixes[M]//Financial Cryptography and Data Security.Berlin,Heidelberg:Springer Berlin Heidelberg,2014:486-504.DOI:10.1007/978-3-662-45472-5_31
[34] Maxwell G.CoinJoin:bitcoin privacy for the real world[C].Bitcoin forum.(2013-08-22)[2019-06-05].https://bitcointalk.org/index.php?topic=279249
[35] Ruffing T,Moreno-Sanchez P,Kate A.CoinShuffle:practical decentralized coin mixing for bitcoin[M]//Computer Security-ESORICS 2014.Cham:Springer International Publishing,2014:345-364.DOI:10.1007/978-3-319-11212-1_20
[36] Miers I,Garman C,Green M,et al.Zerocoin:anonymous distributed E-cash from bitcoin[C]//2013 IEEE Symposium on Security and Privacy,Berkeley,CA.New York,USA:IEEE,2013
[37] Sasson E B,Chiesa A,Garman C,et al.Zerocash:decentralized anonymous payments from bitcoin[C]//2014 IEEE Symposium on Security and Privacy,San Jose,CA.New York,USA:IEEE,2014
[38] 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),San Jose,CA.New York,USA:IEEE,2016

A survey on the security of blockchain

LIU Jiuliang[1] FU Zhangjie[1] SUN Xingming[1]
1 School of Computer and Software,Nanjing University of Information Science and Technology,Nanjing 210044

Abstract Blockchain technology,which has the advantages of decentralization and tamper-proofing,provides a new

way to store information, execute transactions and handle business logic in an open environment. From the 1.0 era represented by Bitcoin to the 2.0 era represented by Ethereum, blockchain technology has revolutionized the finance, Internet of Things, supply chains and other industries. However, blockchain technology still faces many security challenges due to technical and management issues. Firstly, we discuss eight kinds of blockchain attacks in terms of information security, system security and privacy security, such as malicious information attacks, 51% attacks, smart contract attacks, denial of service attacks, etc., and analyze the principles, implementation processes and destructiveness of these attacks. Secondly, we discuss twelve blockchain security technologies from the above three perspectives, such as SmartPool, Securify analysis tool, mixing service and zero-knowledge proof, and analyze the principles, implementation processes, advantages and limitations of these technologies. Finally, we look forward into the future research directions of blockchain technology.

Key words blockchain; security; privacy preserving; smart contracts