doi:10.14132/j.cnki.1673-5439.2019.05.008

区块链技术安全威胁分析

孙国梓,王纪涛,谷 宇

(南京邮电大学 计算机学院,江苏 南京 210023)

摘要:区块链安全在区块链技术的研究中是很重要的部分,目前区块链安全事件频频发生,对区块链相关的安全威胁需要提高警惕。文中首先对区块链进行了简要说明,然后详细分析了区块链在算法、共识协议、智能合约、用户使用和网络安全中的安全威胁。并说明了公证人机制、哈希时间锁定和侧链/中继链3种跨链技术存在的安全问题以及区块链本身特性对跨链产生的安全问题。进一步又介绍了区块链在安全领域的应用。再分析了区块链隐私保护中的两种隐私威胁。最后,对区块链各个方面的安全威胁提出了相应的应对策略和未来的研究方向。

关键词:区块链;安全威胁;智能合约;跨链技术;隐私保护

中图分类号:TP311.13;TP309 **文献标志码**:A **文章编号**:1673-5439(2019)05-0048-15

Security threat analysis of blockchain technology

SUN Guozi, WANG Jitao, GU Yu

(School of Computer Science, Nanjing University of Posts and Telecommunications, Nanjing 210023, China)

Abstract: The blockchain security plays an important role in the research of a blockchain technology. At present, blockchain security incidents occur frequently, proving that the vigilance to security threats is necessary. Firstly, a brief description of the blockchain is given. Then, the security threats on blockchains in algorithms, consensus mechanisms, smart contracts, user usage, and network security are analyzed, and the security problems of cross-chain technology, including notary mechanism, hash time locking and side chain/relay chain are demonstrated. Afterwards, the security problems caused by the characteristics of blockchain itself are also explained. The application of the blockchain techchnology in the security field is described. Furthermore, two kinds of blockchain privacy threats are proposed. Finally, the corresponding countermeasures and future research directions for security threats in all aspects of blockchains are put forward.

Keywords: blockchain; security threat; smart contract; cross-chain technology; privacy protection

区块链概念的出现主要源于2008年中本聪发表了一篇《比特币:一种点对点的电子现金系统》,他在论文中提出了区块链(Blockchain)这种数据结构。作为计算机时代的先进技术,区块链应用了分布式数据存储、加密算法、共识机制、点对点传输等计算机技术,本质上是一种去中心化基础架构与分布式计算范式。就目前而言,由于区块链技术的快速发展和进步,在不同的行业和不同的场景之下,结合区块链技术的相当一部分应用已经实现落地,而还有一部分在持续发展中。区块链技术的发展可以分为三个阶段,由 Melanie Swan 在其编写的一本书中就将区块链划分成了3种级别。

收稿日期:2019-08-20 **本刊网址**:http://nyzr.njupt.edu.cn

基金项目:国家自然科学基金(61502247)、数学工程与先进计算国家重点实验室开放基金课题(2017A10)和信息网络安全公安部重点实验室开放课题(C17611)资助项目

作者简介:孙国梓,男,博士,教授,sun@njupt.edu.cn

引用本文:孙国梓,王纪涛,谷宇. 区块链技术安全威胁分析[J]. 南京邮电大学学报(自然科学版),2019,39(5):48-62.

区块链 1.0 是基于比特币的诞生而出现,此时的区块链主要用于加密货币。该层次的区块链应用增强了数字货币的具象化形式,形成了一种新型价值的数据表现形式。其通过电子数据的传输与交易完成交易介质、记账单位以及价值存储的功能。比特币就是第一个加密货币的具体实现。

区块链 2.0 主要用于金融服务,这一时代最大的特点就是引入了智能合约的概念,以其最简单的形式来说,是由其创建者编写以执行特定任务的程序。虽然智能合约可以在任何区块链版本上进行编码,但是以太坊是最受欢迎的选项,因为其提供了可扩展的高效处理能力。智能合约的引入使得区块链能做更多复杂的逻辑,而不是简单的点对点转账。

区块链 3.0 指的是其不再只为金融服务,除此之外,更多的场景也用上了区块链技术,包括政府、食品安全、媒体、司法取证等等。这个时代对区块链的认识有了更深的理解,更加认可区块链对于社会发展的价值。Hyperledger(超级账本)项目作为实现了完整权限控制及安全防护的区块链架构,是该阶段的代表技术。

当区块链技术在各行各业兴起之后,大部分专家学者们一直在探索区块链技术如何更好地融入到日常生活中。随着区块链加密货币、交易所、区块链应用等开始慢慢普及,这也让很多黑客攻击者对区块链技术进行了深入研究,为了从区块链中找到技术漏洞作为攻击入口,以便从中获利。

近两年来,区块链在安全方面遇到了很多问题。2019 年 1 月 25 日,全球区块链数据与安全服务商 PeckShield(派盾)联合多家媒体共同发布《2018 年度区块链十大安全事件》,其中有 2018 年 3 月 7 日币安交易所遭黑客攻击,通过程序化交易拉升代币从而获利;2018 年 3 月 20 日以太坊节点持续两年偷渡漏洞,攻击者利用以太坊 RPC API 缺陷盗取节点资产;2018 年 4 月 -5 月 BEN/SMT/EDU 智能合约安全漏洞;2018 年 5 月 29 日 EOS 节点远程代码执行;2018 年 7 月 -8 月 ERC20 等一系列代币假充值漏洞;2018 年 8 月 23 日 FOMO 3D 游戏阻塞攻击决出大奖,破坏游戏平衡;2018 年 9 月 BTC 超发漏洞;2018 年 8 月 -11 月 EOS DApp 等系列漏洞;2018 年 11 月 16 日 BCH 共识破裂硬分叉。这十大安全事件只是区块链中的冰山一角,因此目前区块链的安全问题需要重视起来,减少损失。

1　区块链概述

1.1　区块链定义

最早关于区块链的介绍是在中本聪发表文章《Bitcoin: A Peer-to-Peer Electronic Cash System》,在这篇文章中没有具体提出区块链的定义,但是指出区块链是用来记录交易的一种分布式账本。从此,作为比特币的重要底层技术的区块链逐渐开始被人们重视。

从数据的角度来看,区块链是一种几乎不可能被更改的分布式数据库[1]。这里的“分布式”不仅体现为数据的分布式存储,也体现为数据的分布式记录并且由系统参与者共同维护。

从技术的角度来看,区块链并不是一种单一的技术,而是多种技术整合的结果。这些技术以新的结构组合在一起,形成了一种新的数据记录、存储和表达的方式[2]。

1.2　区块链特性

区块链本身并不是一个单独的技术,而是很多种技术组合形成的。区块链技术发展至今已经形成了一个较完整地技术栈。区块链被广泛地关注和研究主要是因为本身的特性:去中心、透明性和可溯源性、开放性、不可篡改性、匿名性[3]。

(1) 去中心化

与传统的中心化系统不同的是,区块链中并不是由某一个中心来处理数据的记录、存储和更新,每一个节点都是对等的,整个网络的数据维护都是由所有节点共同参与的。在传统的中心化系统中,如果攻击者攻击中心节点就会导致整个网络的不可控,而区块链的去中心化特点提高了整个系统的安全性。

(2) 透明性和可溯源性

在区块链中所有的交易都是公开的,任何节点都可以得到一份区块链上所有的交易记录,除了交易双方的私有信息被加密,区块链上的数据都可以通过公开的接口查询,又因为区块链是以时间序列来记录数据,所以也就保证了用户可以对交易进行溯源[4]。

(3) 不可篡改性

在区块链中所有的信息一旦通过验证共识并且写入区块链之后,这个数据是不可以篡改的,如果想篡改数据就必须挑战 51% 以上的矿工[5],而这样的代价很大并且很难实现。

1.3 区块链体系结构

区块链在经历长时间的演变之后,其体系结构基本已经定型,大多数的区块链底层架构由 6 部分组成,其中有数据层、网络层、共识层、激励层、合约层和应用层,如图 1 所示。

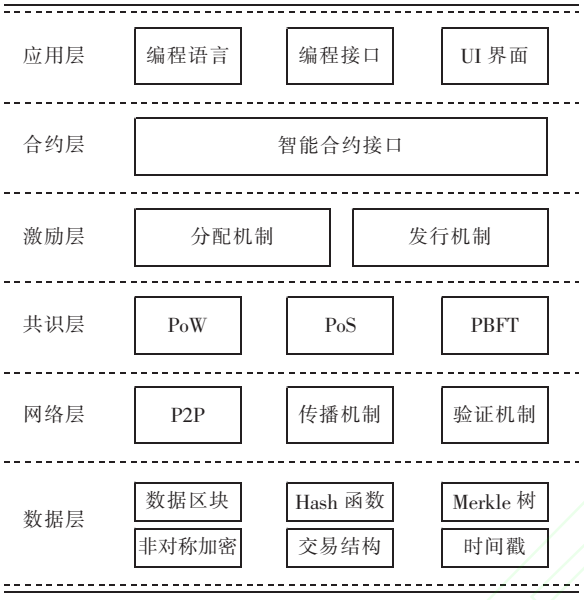

图 1 区块链的底层架构

(1) 数据层

主要包括数据区块、哈希函数、链式结构、Merkle 树、时间戳和非对称加密等[6],在数据层使用时间戳来证明各个交易创建的时间,时间戳服务器对当前交易及其建立的时间和指向之前交易的哈希进行签名,这样就能反映各个交易创建的时间顺序并且这个时间是不可以更改的。在区块链中每一笔交易都是公开的,每一笔交易都显示了交易的来源和交易的去向,但只是显示双方的地址信息并不是个人的真实信息,因此在区块链中的每一个节点都可以对交易进行溯源,数据层使用的各种数据的链式结构和加密算法及时间戳技术保证了数据存储和交易的安全性[7]。

(2) 网络层

主要包括 P2P 网络机制、传播机制和验证机制。区块链基本特性之一就是去中心化,因此任何节点之间都可以进行交易,每一个节点都有广播交易的权利,并通过特殊的验证机制使每个节点都可以对数据进行打包记账,但只有通过大部分节点才能存入区块链[8]。采用 P2P 网络机制使得区块链的节点具有自动组网功能,目前该技术已经是非常成熟和安全的。

(3) 共识层

主要包括各种共识机制的算法:PoW、PoS、DPoS 等。共识机制是区块链的核心技术,它主要决定谁可以记账,会影响整个系统的安全性。去中心化的特性使得区块链需要大多数节点共同参与维护整个系统的运行,遵守同一种协议规则也是必须的,PoW 机制指的是完成一定的工作量才能生成一个新的区块,每个节点根据自己的计算能力进行哈希运算来争取打包区块的权利[9]。该机制可以有效地抵御女巫攻击。

(4) 激励层

主要包括发行机制和分配机制,在区块链系统中,共识节点可以通过打包区块及通过消耗自己的计算资源成功验证和记账来获取相应的奖励。激励机制将经济因素引入区块链体系结构中主要是让节点都愿意遵守区块链的规则,惩罚不遵受规则的节点,实现系统的良性发展。

(5) 合约层

主要包括了脚本代码、算法机制和智能合约。智能合约的概念最早是在 1995 年由 Nick Szabo 提出的,智能合约就是可以运行在以太坊上的程序[10],以太坊就是新一代的区块链系统,其进一步完善了区块链底层中的合约层,而智能合约的出现为区块链提供了可编程的特性。智能合约的执行不需要任何信用方,只要达到智能合约的约束条件就可以自动执行。

(6) 应用层

主要包括各种应用场景和案例等。通过应用层提供用户可编程接口,允许用户自定义、发起和执行合约。例如基于以太坊的各种区块链的 DAPP 都部署在应用层。可编程货币和可编程金融也包括在应用层。

2 区块链主要安全威胁

近年来,区块链以价值安全转移、数据安全存储为用户广泛使用。区块链底层从技术上来说有一系列加密算法和数字签名方式确保交易安全,又依赖于共识机制来产生区块,以组成一种随时间戳排序的链式结构来保证数据的不可篡改。尽管如此,目前区块链依然面临着巨大的安全威胁,基本可分为算法安全威胁、协议安全威胁、智能合约安全威胁、用户使用安全威胁和网络安全威胁 5 种。

2.1 算法安全威胁

区块链底层本身采用了密码学算法的很多机制,例如比特币采用了 SHA256、RIPEMD160 哈希算法和椭圆曲线密码学算法[11],以太坊采用了 Kec-

cak256 哈希算法和椭圆曲线密码学算法[12]。除了比特币和以太坊,其他区块链同样会使用一些其他的哈希函数、加密算法和数字签名方法来保证自身的安全性。就目前而言,这些正在使用的算法都是相对安全的,但在一些特殊情况下或者面对未来发展的背景下,这些算法可能会变得不安全。主要有两个方面的安全挑战:

(1) 哈希函数

哈希函数可能会发生哈希碰撞现象[13],哈希碰撞指的是不同的输入数据通过同一哈希函数计算后生成了相同的哈希值,这种情况的出现取决于哈希值生成的算法。2017 年 7 月麻省理工(MIT)研究者就发现了新型数字加密货币 IOTA 中的加密哈希函数 Curl 中存在着严重的哈希碰撞漏洞,从而导致无法保障 IOTA 的数字签名和工作量证明(PoW)的安全性,次月 IOTA 团队就将 Curl 哈希算法替换成了 SHA3 哈希算法。目前,MD5 和 SHA1 哈希算法都已经被破解,SHA256 依然是安全的,但 SHA256 的安全性也因为 MD5 和 SHA1 的破解而降低,Keccak256 哈希算法就因此诞生,其就是 SHA3 哈希算法的前身。

(2) 量子计算技术

量子计算技术正在飞速发展中,该技术的成熟将会对当今密码学算法造成极大影响。现在密码学算法是安全的主要原因是没有任何方式能短时间计算出复杂的数学难题[14],如果量子计算机成功诞生,其运算速度远远超过现在的计算机系统,那么目前的密码学算法对于量子计算机来说就是一个简单问题。根据对传统密码算法和量子计算技术的研究,量子计算技术对如今密码体制的威胁如表 1 所示。

表 1　量子计算技术对密码体制的威胁

加密算法	类型	作用	理论基础	安全性威胁
AES(高级加密标准)	对称密码体制	加密	字节/字运算	破解难度减半
SHA256	哈希算法	数字指纹	—	破解难度减半
RSA	非对称密码体制	加密、数字签名	大整数分解	失效
DSA(数字签名算法)	非对称密码体制	加密、数字签名	离散对数	失效
ECDH(椭圆曲线迪菲-赫尔曼密钥交换)	非对称密码体制	加密、数字签名	椭圆曲线离散对数	失效
ECDSA(椭圆曲线数字签名算法)	非对称密码体制	数字签名	椭圆曲线离散对数	失效

因此,在量子计算技术完全成熟之前,必须有能够对抗量子计算的新型密码体制出现,否则一切运用现有密码体制的事物都将失去原有的安全性。在未来,尤其是与密码体制紧密相关的区块链技术,更需要具备抗量子计算的密码体制来保证其安全性。

2.2　共识协议安全威胁

共识协议是区块链的重要组成部分,在生成区块时都需要依赖于区块链的共识机制来选择出矿工来打包区块[15]。因此黑客会针对不同的共识机制,采用各种手段来破坏共识原则,以此来控制整个区块链的走向,从而让自己获利。目前主要的共识协议攻击手段有双花攻击、自私挖矿攻击(Selfish Mining)、短程攻击(Short-Range)、长程攻击(Long-Range)、币龄堆积、预计算攻击(Pre-Computation)、女巫攻击(Sybil Attack)等。

(1) 双花攻击

双花攻击主要针对工作量证明(PoW)共识机制,指的是攻击者通过某种方式拥有了区块链全网络上一半以上的算力,并通过其算力来让区块链产生分叉,从而引导主链走向改变的攻击方法[16]。例如,攻击者 A 预先准备好 100 个 BTC,并且其拥有比特币区块链上一半以上的算力,攻击者 100 个 BTC 投放到交易所,然后用其一半以上的算力开始挖矿,等待投放完毕后,攻击者 A 将交易所里的 100 个 BTC 兑现。由于攻击者 A 拥有一半以上的算力,可以控制比特币区块链的走向,让主链变成未包含其投放 100 个 BTC 到交易所行为的分叉链,从而使得投放行为失效,100 个 BTC 返回到攻击者手中,然而此时攻击者已经获得了 100 个 BTC 兑现的资金,这就是攻击者通过双花攻击来无偿兑现的过程。

(2) 自私挖矿

自私挖矿是指攻击者在计算出新区块的哈希值时(即发现有效区块),不将其发现新区块的消息广播给区块链中的其他节点,然后继续挖新区块的下一个区块,直到其他挖矿者挖到有效区块时,攻击者就把先前挖到但未广播给其他节点的所有区块公开,因为攻击者已经成功发现多个连续的区块,所以攻击者所在的链分支比其他分支更长,从而使得区块链主链走向由攻击者控制[17]。尽管有研究者表明这种方式很难实施,但其安全隐患依旧存在。

(3) 短程攻击

短程攻击是指攻击者在区块链中提交一笔交易,在该笔交易打包到新区块时,攻击者依然在该新区块的前一个区块上进行挖矿,一旦另一个分叉的

区块比包含该笔交易的分叉区块更多,那不包含该笔交易的分叉就成为了区块链主链,攻击者就达到了交易回滚的效果[18]。常用的短程攻击是贿赂攻击,即攻击者贿赂其他挖矿者,帮他回滚交易。短程攻击的本质也是双花攻击。

(4) 长程攻击

长程攻击是短程攻击的升级版,攻击者已经拥有一大部分区块链算力资源,采用其拥有的算力资源直接让区块链产生分叉,只要长时间未被其他诚实节点发现,区块链主链走向必定会受到攻击者主导。常见的长程攻击就是 51% 攻击。本质上依然是双花攻击,然而该攻击方式实际上更多出现了权益证明协议(PoS)共识机制,因为 PoS 共识机制不通过算力来选择矿工,相比 PoW 共识机制消耗的资源少。

(5) 币龄堆积

通过币龄堆积的方式来进行攻击主要是针对权益证明协议(PoS)。在 PoS 共识机制是根据币龄来选择打包区块的矿工,所谓币龄就是根据持有货币的量和时间计算出的一个指标数,币龄越高成为矿工的概率就越大[19]。每打包一个区块,对应矿工的币龄都会清空。攻击者在拥有一定数量的货币后,可以通过持续拥有该数量的货币来堆积币龄,币龄足够大时,就能主导区块链区块的生成。攻击者若有足够多的货币,也可以将货币分散到多个节点,通过分布式堆积币龄来共同控制区块链走向。

(6) 预计算攻击

预计算攻击是指攻击者通过随机试错的方式来控制前一个区块的哈希值,从而更容易计算出下一个区块的哈希值。

(7) 女巫攻击

由于区块链节点随时可能加入或者退出,为了维持区块链网络数据稳定,同一份数据通常需要备份到多个分布式节点上,这就是区块链数据冗余机制。在《The Sybil Attack》中叙述了女巫攻击是攻击数据冗余机制的一种有效手段。若区块链网络中存在一个恶意节点,那么同一个恶意节点可以具有多重身份,就像一个细胞可以分裂出多个细胞一样,恶意节点也可以进行分裂[20]。那么原来需要备份到多个节点的数据被欺骗地备份到了同一个恶意节点,因为该恶意节点进行了分裂,伪装了其多重身份,这就是女巫攻击。

2.3 智能合约安全威胁

进入区块链 2.0 时代之后,智能合约成为了区块链中必不可少的一部分。在让区块链能实现更多功能的背景下,由于智能合约的编写依赖于开发人员的主观性,造成智能合约代码出现很多意想不到的漏洞,往往这些漏洞会让用户遭遇巨大损失。在经历各大安全事件和智能合约漏洞挖掘者的助力下,常见的智能合约漏洞主要分为如下几类:

(1) 重入漏洞

智能合约编程具有面向对象的思想,本质上一个智能合约就是一个类,因此在与区块链交互的功能操作非常复杂的情况下,通常需要进行合约调用合约的操作。一旦多个合约相互调用的关系变得复杂,就可能会出现代码重入的问题,所谓代码重入就是在某个时刻调用方法中断以致于执行其他的合约代码,该合约代码又再次调用了该发生中断方法,一直反复进入该方法。攻击者就会利用代码重入问题,让程序反复执行攻击者的恶意代码,以从中获利。在 ERC20 合约中经常出现的 withdraw 函数就可能出现重入问题[21],如下代码所示:

```
function withdraw(uint _amount) public {
    if(balances[msg.sender] >= _amount) {
      if(!msg.sender.call.value(_amount)()) {
        throw;
      }
    }
}
```

该代码首先对余额进行审核,再从 msg.sender 账户地址中转出以太币,最后修改 balances 数组中的余额。当函数执行到 msg.sender.call.value(_amount)() 时,攻击者就能通过 msg.sender 的 fallback 函数重复调用 withdraw 函数,导致 msg.sender 账户的以太币一直在输出,直到余额不足。

(2) 整数溢出漏洞

2018 年,"清华-360 企业安全联合研究中心" ChainTrust 团队对 Etherscan 上的 390 份合约进行了完整分析,发现共有 25 个智能合约具有整数溢出漏洞。整数溢出漏洞的类型繁杂,在这 25 个合约中主要有 underSell(高卖低收)漏洞、ownerUnderflow(下溢增持)漏洞、mintAny(随意铸币)漏洞、overMint(超额铸币)漏洞、allocateAny(超额定向分配)漏洞和 overBuy(超额购币)漏洞。所谓整数溢出是由于计算机中整数具有上限和下限,如果当一个整数超过其上限或者小于其下限,那该整数就可以从一个很大的数变成很小的数或者从一个很小的数变成很大的数,这种现象在合约进行转账的过程中很容易被黑客攻击者作为攻击点,以此实现无偿获取货币

的目的[22]。

(3) tx. origin 和 msg. sender 混淆漏洞

在以太坊的 solidity 智能合约语言里,语言开发者为用户提供了 tx. origin 和 msg. sender 变量来获取账户地址[23]。然而,很多合约开发者经常将这两个变量混淆,它们的本质含义截然不同。假设当前有合约 A 调用合约 B,合约 B 调用合约 C,那么在合约 C 中的 tx. origin 是合约 A 的地址,msg. sender 是合约 B 的地址。也就是说,tx. origin 变量获取的是发送交易的最初调用方地址,msg. sender 变量获取的是直接调用方的地址。若合约开发人员在开发过程将这两个变量混淆,将会发送意想不到的错误结果。

(4) 拒绝服务漏洞

拒绝服务漏洞就是攻击者通过某种手段让某些代码逻辑执行失败,以这种方式持续消耗调用合约需要的 gas。例如,攻击者可能会将合约中的某些数组或者映射的大小设置成巨大,当合约对这些数据或者映射进行循环遍历时,就可能由于消耗的 gas 过多而执行失败;还可能某些合约在执行前,调用者必须通过一些验证,如果调用者由于某些原因无法进行验证,则无法正常调用合约;攻击者可以设定一个持续拒绝调用的合约,来阻止其他人对合约进行调用。

(5) 关键字过时

目前,solidity 语言更新迭代的速度非常快,以致于很多智能合约开发者无法很快熟悉最新版本[24]。由于最新版本可能与旧版本并不兼容,智能合约开发者可能会使用某些在新版本中过时的关键字来实现想要的效果,此时智能合约开发者可能并不知道这些关键字过时了,最终导致整个智能合约执行的效果与预期不符,甚至由于没有关键字的限制发生一些严重的错误。

(6) 未检查返回值漏洞

solidity 语言提供了几种外部调用的函数方法 call( ), callcode( ), delegatecall( ) 和 send( )。这些函数方法具有 bool 返回值,然而在计算错误方面的行为与其他 Solidity 函数方法完全不同,这些函数产生的结果并不会广播给所有人,并且不会导致当前执行中止[25]。这些函数会返回一个布尔值为 false 之后,继续执行接下来的代码。如果开发者并没有发现这种问题的存在,那当不满足条件返回 false 时,程序还会继续进行,最终得到一个无法想象的结果。

(7) 短地址/参数漏洞

2017 年 4 月,Golem 项目在一篇博文中提及发现了一个影响交易的安全漏洞。根据该帖子,当某些交易所处理 ERC20 令牌的交易时,没有对账户地址长度进行输入验证。这导致传送给智能合约转账函数的参数异常,以及传输金额的一系列错误问题。短地址攻击是 EVM 本身接受不正确填充参数的副作用。利用这一点攻击者可以通过使用专门制作的地址来进行攻击。例如某交易所具有交易功能,可以接收收件人地址和金额。然后,函数接口 transfer (address to, uint256 amount) 使用填充参数与智能合约函数进行交互,将 12 位零字节的地址(预期的 20 字节长度)预先设置为 32 字节长,Bob 要求 Alice 转让他 20 个代币。但 Bob 恶意地将 Alice 的地址截断以消除尾随的零,Alice 使用交换接口和 Bob 较短的 19 字节地址进行交互,该接口用 12 个零字节填充地址,使其成为 31 个字节而不是 32 个字节。有效地窃取以下 amount 参数中的一个字节。最终,执行智能合约代码的 EVM 将会注意到数据未被正确填充,并会在 amount 参数末尾添加丢失的字节。有效地传输 256 倍以上的令牌。

(8) 交易顺序依赖

在区块链中发起的交易需要经过矿工的打包才能最终记录到链上,在打包过程中,这些交易的打包顺序是具有优先级的,矿工通常会选择那些具有更高 gas 费用的交易优先打包[26]。由于存在这种机制,攻击者完全可以通过支付较高的 gas 费用来阻碍其他低费用的交易,导致某些交易无法正常执行。

(9) 合约构造函数与合约名不一致

智能合约开发人员,可能会由于不够细心等原因,将构造函数名写得与合约名不同,这样会导致该函数不再是构造函数,能被其他人调用。这种情况的风险在于构造函数的目的通常是初始化某些合约变量,如果能被其他人调用,那合约的数据就会发生异常,即在不应该重置的时刻发生了数据重置。

(10) 时间操作/伪随机

在智能合约中,很多地方需要用到某些数据上链的时间,由于区块链并不是发起交易即上链的形式,需要经过矿工挖矿之后才能真正上链,因此数据上链时间很大一部分取决于矿工[27]。在 solidity 语言中通过 block. timestamp 或者 now 来获取时间戳,可能缺乏时间的真实性。还有许多开发者,会利用 block. timestamp 或者 now 来生成随机数,这样的行为是不妥当的,若矿工是恶意节点,那该时间戳可能会受到恶意矿工控制。

2.4 用户使用安全威胁

区块链的安全性不仅仅在其本身,也有可能出现在区块链用户上。区块链用户可以分为开发者用户和普通用户,不同的用户类型会执行区块链系统中不同的功能操作。攻击者会根据用户身份进行针对性攻击,主要分为节点暴露 API 接口和钱包私钥窃取两种情况。

(1) 节点暴露 API 接口

由于目前大多数区块链平台对于开发者来说,并没有一些比较友好的区块链应用集成开发平台(IDE)供开发者进行开发[28]。但前不久,美国硅谷技术团队黑曜石实验室(Obsidian Labs)发布了 EOS Studio,该平台就是为 EOS 区块链量身定做的集成开发平台。如果这样的集成开发平台被普及,那节点暴露 API 的问题可能会更少地出现,就如今来说作为开发者的区块链用户,依然需要通过各种区块链提供的 API 来进行开发,通常开发者用户会频繁调用这些 API 来减轻开发负担。攻击者就可能会针对这些开发者节点进行攻击,通过开发者节点来控制这些 API 来获取区块链中一些重要信息。

(2) 钱包私钥窃取

相对于开发者用户来说,普通用户的比例更大。普通用户最频繁的操作就是登录区块链钱包进行货币交易,通常普通用户的安全意识也比较匮乏。在普通用户用其区块链钱包进行交易时,必须是以“热钱包”形式存在,也就是必须要连接到区块链中,此时该节点用户就是在线的。黑客攻击者就可能在这种时候入侵该节点用户,从而窃取该用户的钱包私钥,进一步盗取用户钱包中的货币资金[29]。然而离线的钱包(“冷钱包”)依然有可能被黑客攻击,黑客能通过社会工程学或一些物理攻击手段来窃取用户钱包的私钥,以达到盗取货币的目的。所以普通用户需要加强安全意识,最好的方式就是将私钥记忆在脑中或者锁进保险箱内。

2.5 网络安全威胁

凡是网络都会存在病毒类的恶意程序威胁,区块链系统也是一种新型网络架构。攻击者会直接对区块链网络进行持续攻击来盗取货币资金,或者采用间接方式来敲诈拥有区块链货币的用户。主要的威胁形式有 BGP 路由广播劫持、伪造数字签名和勒索病毒。

(1) BGP 路由广播劫持

BGP 是自治系统间的路由协议[30]。BGP 交换的网络可达性信息提供了足够的信息来检测路由回路并根据性能优先和策略约束对路由进行决策。攻击者利用 BGP 路由的重定向能利用其他矿工节点为自己挖矿。基本劫持流程:当某一矿工 A 连接到有效合法的矿池请求和接收任务,劫持者就开始进行攻击,在矿工 A 尝试连接矿池过程中,劫持者会通过一个新的 BGP 将矿工 A 的路径定向到一个恶意矿池,并维持这种定向。将第一次被劫持过的矿工连接到第二个劫持者的恶意矿池,避免重复劫持。此时攻击者就能停止攻击,矿工 A 就会免费作为攻击者的挖矿劳动力。

(2) 伪造数字签名

攻击者通过伪造企业的数字签名来躲避验证,并且诱导普通用户将其货币资金转给自己,从而无偿地骗取用户,让自己获利。一般分为以不可忽略的概率推算出系统的私钥和有效的通用性攻击算法两种伪造攻击方式。例如对于多重签名来说,攻击者根据身份的不同可以分为 3 类:签名发起者和收集者、内部的其他签名者和外部攻击者。不同身份对于搜集攻击所必备的数据信息的难易程度也是不同的,通常签名发起者最容易搜集到攻击所需数据,内部其他签名者次之,外部攻击者最为困难。假设攻击所需的必要数据就是各个签名者的数据 D,通过该数据 D 能窃取到签名者的私钥。如果攻击者是签名发起者和收集者,那么他可以合法地接收到其他签名者的数据 D;内部其他签名者通过在在内部网络中偷听或截取数据 D;外部攻击者要首先入侵内部网络然后再实施网上偷听或截取。另外,对于多重签名来说,能成功窃取签名者私钥的完全攻击还分为两类:一类是仅能伪造单个签名者的签名,另一类是既能伪造单个签名,又能伪造多重签名。后者相对于前者而言,攻击更完全。

(3) 勒索病毒

2017 年 5 月,全球近 100 个国家的微软系统计算机同时遭到名为 WannaCry(想哭吗)[31] 或 Wanna Decryptor(想解锁吗)的电脑病毒袭击。如果想要被感染病毒的计算机解除锁定,只能向对方支付所要求的比特币,否则硬盘将被彻底清空。这一场比特币勒索事件更是波及到了国内多个高校,导致高校产生巨大损失。尽管这种攻击方式并没有直接攻击区块链系统,但攻击者利用比特币的匿名性让被感染用户进行匿名转账。勒索方式不仅限于加密计算机文件,还可以通过其他侵害计算机用户个人利益的手段。本质上就是结合区块链技术的传统网络威胁。

3　区块链跨链安全

随着区块链技术不断发展,各种企业级区块链平台也应运而生,导致区块链底层架构也变得类型不一,区块链跨链的需求也在持续上涨。为了实现不同的区块链之间进行跨链数据交互,各区块链专家和高级区块链技术人员们一直在研究如何能更好地进行跨链操作,目前主流的跨链技术有公证人机制、哈希时间锁定和侧链/中继链 3 种,但这 3 种跨链技术都存在自身的缺陷,同时也无法避免在跨链交互过程中具有共性的问题。本文罗列了 10 种跨链安全问题,其中前 3 种是基于 3 种主流跨链技术的安全问题,后 7 种是跨链过程普遍存在的共性问题。

3.1　公证人机制安全问题

公证人机制是在不同区块链之间设置一个完全可信的中间人,当需要进行跨链操作时,不同区块链将需要进行跨链的数据信息提交给该中间人,由中间人完成不同区块链之间的跨链数据交互。尽管公证人机制的优势是不需要考虑不同区块链的底层架构设计,但这种方式破坏了区块链的去中心化特性,因为存在于区块链之间的公证人是完全中心化的。如果公证人以一种伪装可信状态存在,那会对区块链信息的安全性造成极大影响,在一个多链系统中数据信息就不再安全了,只有公证人真实可信才能确保区块链进行安全交互。

3.2　哈希时间锁定安全问题

哈希时间锁定是一种通过哈希锁与时间锁相结合来实现资产原子交换的方式,其技术安全性主要依赖于资金锁定和时间锁定。目前,比特币的闪电网络就是基于哈希时间锁实现资金的跨链交换的,然而在闪电网络中就预见了这种方式会面临的安全问题。

(1) 恶意节点建立多笔超时交易

在基于哈希时间锁的闪电网络中,由于每进行一笔资金交换,都需要进行时间锁定来限制交易必须在某个时间段内完成,若有某些恶意节点短时间内建立大量资金交易,同时故意让交易发送超时,那么将会给整个网络造成很多超时交易信息,从而让网络发送阻塞,影响整个网络正常运作。

(2) 资金锁定需维持“热钱包”状态

通过哈希时间锁来进行资金交换,必须在一定时间内对交易资金进行锁定,这段时间交易双方必须是以“热钱包”的状态存在,即用户钱包必须是联网状态,因为双方需要及时对交易的反馈做出反应,例如转移资金时的数字签名验证。然而,“热钱包”很容易被黑客盯上,黑客能通过各种手段来窃取“热钱包”的私钥,进而偷取用户钱包内的资金[32]。这就增加了区块链跨链安全交易的风险。

3.3　侧链/中继链安全问题

侧链是完全拥有某一条链功能的另一条区块链,可读取和验证主链上的信息,并且侧链对主链来说是隐藏的。而中继链能够访问和验证进行交互操作的多方区块链,并对多方区块链数据信息进行转移,本质上是一种去中心化的公证人机制。尽管相对于公证人机制来说,通过这类方法提升了跨链过程的安全性,但由于侧链/中继链机制在执行过程中主要是依据区块链头信息进行验证,并不能获取主链网络上完整的交易数据信息。因此侧链/中继链并不能做到对主链数据的追溯,或是识别一些常见的区块链攻击现象[33]。又因为侧链/中继链也需要矿工来生成区块链,但通常并不是由主链上的所有节点来进行维护,所以侧链/中继链的矿工也需要有完全可信度,否则将会导致参与跨链交互的区块链发送异常,甚至导致系统紊乱奔溃。

3.4　孤块问题

孤块主要出现在使用工作量证明(PoW)共识机制的区块链中,在各节点通过计算机算力来计算满足区块链难度值的区块哈希的过程中,可能会有多个节点在短时间段内都计算出了满足难度的区块哈希,即生成了有效区块,但由于验证区块是否有效的过程并不是瞬间完成的,因此区块链会选择在这个短时间段内最早生成的有效区块作为当前区块链的下一个区块,那么剩余的未被选中的区块将被废弃,转变为孤块。若进行跨链交互的区块链中具有采用工作量证明(PoW)的区块链[34],那么在进行跨链交易的时候,很可能会计算出包含该跨链交易数据信息的区块,但由于短时间内有比该区块更早的区块生成,此时包含跨链交易数据信息的区块会从有效区块转变为孤块,从而让交易信息丢失在区块链网络中,最终交互链中的跨链交易信息不再具有完整性。

3.5　长程攻击问题

长距离攻击主要针对的是采用权益证明协议(PoS)的区块链,由于权益证明协议具有弱主观性,区块链网络中的新节点和长期离线节点会受到弱主观性的影响。在这类区块链中,恶意节点可以预先生成大量的区块,并在某一时刻将这些区块公开,这

些瞬间增多的区块会因为区块链最长链原则导致区块链主链改变。如果跨链交易数据信息已经打包在旧主链的区块上,由于主链改变会使得这些跨链交易数据信息被丢失[35]。这种现象很可能会导致跨链交易时智能合约操作被打断,更可能产生双花现象。

3.6 多链数据同步超时问题

在一个需要进行跨链操作的多链系统中,多链数据同步至关重要。在数据同步的过程中,必须要保证不同链都已经满足某些同步条件后才能完成数据同步。在这样的原则下,必定会有某些链迟迟未满足同步条件的情况,当这种情况发生时,多链系统可能会认定本次数据同步超时,那么这次同步的操作数据信息就会被当做无效数据丢给系统进行处理以及垃圾回收[36]。若在较短时间内有过多的同步超时现象一定会影响其他正常执行的同步操作,甚至会让整个系统网络发生阻塞,如果阻塞过于严重则会导致整个多链系统瘫痪。由于多链系统是由多条区块链组成,只要某两条区块链间具有严重阻塞现象,那就会进一步影响这两条链与其他链的跨链交互。此时的区块链就不再安全。

3.7 区块膨胀问题

区块链具有永久存储的特性,所以区块链的区块数据文件会随着时间推移而持续增加。就目前而言,比特币和以太坊全节点数据都已经达到了几百个 GB,未来依然会持续增长。当跨链技术成熟以后,区块链的操作不单单仅限于自身操作,还要处理各种复杂的跨链操作,这样无疑会大大增加区块存储数据量[37]。并且,区块链存储数据量会随着参与区块链的数量增加而成指数级增长趋势。那么必定会面临区块链数据过多的情况,即区块膨胀问题。

3.8 故障扩散问题

众所周知,当一个系统由多个相关部件组成时,一个部件就能影响整个系统,就像多链数据同步超时问题一样。在一个复杂的多链系统中,每一条区块链都是整个多链系统运作的重要组成部分。由于区块链本身也会被黑客通过各种手段进行攻击,如果一些攻击者针对多链系统中某一区块链进行频繁攻击,并且攻击成功导致该链发送严重故障,那该故障就会导致整个多链系统发送更大的系统故障,即故障扩散问题。黑客对一个多链系统进行攻击,其攻击成功的概率与多链系统中区块链的数量息息相关,这是因为每多一条区块链,就为黑客多提供一个攻击对象,那黑客攻击成功的可能性就会增加,使得多链系统的安全性下降。

3.9 跨链重放攻击问题

跨链重放攻击主要涉及跨链过程中的智能合约。这类攻击的发生主要会在对区块链进行硬分叉之后,在发生硬分叉后,区块链就会变为两条链,一条为旧链,一条为新链。攻击者能在旧链或新链中找到一个有效的交易,并且将该交易转移到另一条链上。因为这两条链其实对于整个区块链来说都是合法的,并且对于某个有效交易来说并没有标识其属于新链还是旧链[38]。那么此时这笔交易能被旧链和新链都认可,相当于一笔交易进行了两次。在区块链技术还未成熟的当下,各区块链都可能面临系统升级或重大故障而需要进行硬分叉,跨链重放攻击会让用户的资产严重损失。因此在对跨链技术进行研究的过程中,需要考虑这样的攻击问题。

3.10 升级兼容性问题

在跨链技术的研究中,必须要考虑区块链版本升级后的兼容性问题。一个多链系统中,每一条区块链都是相关的,一旦不同区块链存在跨链交互关系,那某一区块链版本升级后必须能让其相关的另外区块链识别或认可,否则发生一些操作功能无法兼容的问题,会影响跨链交互,更可能由于兼容性问题引发一些严重的安全性问题。升级兼容性问题也具有扩散性,多链系统中的某一区块链若想进行版本升级,必须要让新版本能被与其相关的所有区块链都适应,这对于一个多链系统来说,区块链的版本升级就变得极其困难,一旦升级所需考虑的问题增多,那升级后会产生问题的概率和数量也会一定程度增多。

4 区块链安全领域应用

由于以太坊创始人 Vitalik Buterin 将智能合约应用到了区块链上,让区块链领域发生了巨大变革。通过智能合约,区块链能实现更多的复杂逻辑操作,而不仅仅是货币交易[39]。区块链的不可篡改性、可溯源性、永久存储性等特性适用于各行各业,所以很多领域都与区块链技术相融合。可结合的最主要价值就是能依靠区块链来保证各领域某些环节的安全性,区块链应用可分为应用区块链进行数据管理、区块链应用于物联网以及域名系统应用区块链。

4.1 应用区块链进行数据管理

应用区块链进行数据管理是区块链最广泛的应用,最初的区块链应用系统就是利用区块链保证数据的安全性。到目前为止,有很多企业开展的基于

区块链存储的应用项目都已经落地,主要涉及领域有法律、医疗、食品、金融等。

(1) 基于区块链的电子存证系统

采用区块链来存储电子证据指纹,以确保电子证据的完整性和真实性,能有效验证电子证据在获取到上庭审判期间是否被篡改[40]。在 2018 年,浙江杭州一项侵害作品信息网络传播权纠纷案就结合区块链技术用于数据存储的技术原理,以电子证据审查的法律标准为基础,首次对区块链电子存证的效力审查标准进行了探索。

(2) 基于区块链与智能合约的医疗信息管理体系 MedRec

麻省理工学院研究人员 Azaria A 的团队开发了一个名为 MedRec 的系统,用于有效管理存储基于以太坊区块链的医疗记录。该团队针对医疗数据管理领域的监管缺陷,以及后端系统等问题,采用以太坊中的智能合约,创建了分散的医疗保健数据管理系统。该系统编写了挂号员合约(RC)、医患关系合约(PPR)和总结合约(SC)3 个智能合约,在医疗领域建立了一条共有区块链,给患者提供了长期可靠的信息记录与跨院数据共享功能,实现了数据的共享性与不可篡改性[41-42]。

(3) 基于区块链的无密钥签名架构

该架构将基于哈希树的数据签名扩展到服务器辅助的个人数字签名方案。新的签名方案不使用 trapdoor 函数,仅基于密码散列函数,因此能够抵抗量子计算攻击。在无密钥签名架构中,将区块链中的哈希树数据签名(时间戳)解决方案与哈希序列认证机制相结合,保障了签名的时效性与抗抵赖性[43-44]。

4.2　区块链应用于物联网

物联网近年来发展迅速,很多物联网设施已经在多种场合普及,但在物联网设备的安全管理、信用建立、设备智能化上依然存在许多问题。如今,各企业、高校已经开始将区块链技术融入到物联网中,以此来解决一些物联网无法解决的安全问题。

(1) 基于区块链的物联网可伸缩管理

为了解决大规模物联网(IoT)设备集中式管理的安全性和可伸缩性问题,合肥工业大学徐晓冰提出一种基于区块链技术的轻量级物联网设备可伸缩管理框架[45]。该框架采用区块链网络,在网络中部署智能合约为设备管理提供操作接口,利用设备管理器将轻量级物联网设备独立于区块链网络之外,并改进了区块链中拜占庭容错算法(PBFT)的一致性协议,增加了动态选举机制。

(2) 基于区块链的边缘计算 IIOT 架构

在智能制造系统中,工业物联网通过先进的管理技术将制造设备互联,实现了信息的实时传输、设备的范化感知和数据的快速分析处理。但是由于制造设备的异构性、物联网网关数据分析能力的有限性、制造设备的存储力低下,设备和数据的低安全性等缺陷严重阻碍了智能制造的发展。BEIIOT 架构从制造企业的实际生产过程与应用角度出发,将区块链技术与边缘计算相结合,通过对服务器进行 P2P 组网以实现对设备去中心化管理。

(3) 物联网 + 区块链助力食品质量安全保障

农业供给侧改革背景下,需要加强果蔬农产品质量安全体系的建设。近年来,物联网技术在农业方面的应用得到快速发展,使得传统农业迎来了新的变革,同时区块链技术的出现又弥补了农业物联网的不足,为农业物联网数据的存证和溯源提供了依据。通过物联网 + 区块链技术不但解决了生产者和消费者信息不对称问题,也为安全可靠的可追溯性提供了保障[46]。

4.3　域名系统应用区块链

Mirai 僵尸网络[47]证明了网络罪犯可以很容易地破坏关键因特网基础设施。攻击者只需攻破大型网站的域名系统(DNS)服务提供商,就可以切断其他服务的网络访问。而如果用区块链来存储 DNS 记录,能让攻击者从单一目标变成多目标,以此来增强 DNS 的安全性。

Nebulis 是一个探索分布式 DNS 概念的新项目[48],Nebulis 使用以太坊区块链和星际文件系统(IPFS),还有 HTTP 的分布式替代协议,来注册并解析域名。通过使用区块链方法的可信 DNS 基础设施,将能大幅增强该互联网核心信任基础设施。除了 Nebulis,还有 Blockstack、NNS 等都是基于区块链的分布式域名解析系统。

5　区块链隐私保护威胁

尽管区块链网络中每个用户都是匿名的,但由于区块链本身的交易透明性,区块链依然存在隐私保护的威胁。尤其是在大数据技术已经相当成熟的当下,匿名也许并不能真正的隐藏用户身份。目前,区块链隐私保护威胁主要有大数据推测用户身份和暴露用户交易金额。

5.1　大数据推测用户身份

在大数据时代下,很多隐藏信息能够通过大量

的数据样本结合机器学习分析出很多有价值的重要信息。在区块链网络中所有的交易信息是公开透明的,任何人都可以获取到区块链上的所有交易信息,如果有人对这些交易信息通过大数据技术进行分析,就能够得出账户地址和账户地址之间的关系、交易和交易之间的关系以及账户地址和交易之间的关系[49]。分析者可以从两种角度出发来分析数据,以此来推测出用户身份。

(1) 账户地址为出发点

分析者也许通过某种方式知道一些账户地址背后的用户真实身份,假设分析者知道账户地址 A 的真实身份,然后利用现有的区块链浏览器搜索这个账户地址的活动或者读取区块数据库文件通过编程方式筛选出与 A 账户相关的活动。再根据发生事件的时间范围与 A 账户活动的时间进行比较,将一些有效信息都过滤出来,最后通过大数据分析这些有效信息,以已知真实身份的账户地址为基准,推测与其相关的其他账户地址的真实身份。

(2) 交易为出发点

分析者首先清楚某些交易的实际意义,通过这些交易入手,对交易双方的用户地址进行连锁式筛选,将与这些交易或者与这些交易的账户地址相关的有效信息过滤出来,最后通过大数据分析这些有效信息,以已知实际意义的交易为基准,推测与其相关的账户地址的真实身份。

因此一些恶意用户能通过大数据手段从区块链网络中获取区块链用户的私人信息,未来可能需要采用同态加密或者零知识证明等方式来让区块链数据信息更加具有隐私性。

5.2 暴露用户交易金额

因为区块链的交易数据全网可见,所以用户交易的货币数量也能被全网看到。然而,尽管一些区块链具有匿名性,但很多用户并不希望这些交易金额数据被其他人看见,一些敏感信息用户也希望能达到一定程度的隐私性。因此,区块链在隐私保护上依然需要进行大量的研究。将来,在确保区块链隐私保护时,必然不能打破区块链本身的一些优质特性,因此区块链隐私保护还面临着巨大挑战。

6 区块链安全研究方向及对策建议

区块链技术从各个角度暴露了不同的安全威胁类型,但针对这些安全威胁依然能够通过相应的方法进行预防和解决,因此本文提出了目前区块链安全研究方向以及相应的对策建议。

6.1 算法安全策略

区块链底层的算法安全主要基于密码学的应用。对于比特币采用的 SHA256、RIPEMD160 哈希算法和椭圆曲线密码学算法,以及以太坊采用的 Keccak256 哈希算法和椭圆曲线密码学算法,虽然目前能够较为稳定地保持区块链底层的安全,但是随着计算机算力的不断提升,其安全性也将不断受到挑战。所以安全研究人员一方面可以加强对于哈希函数本身复杂度与抗攻击性的设计,另一方面可以研究能够抵御量子攻击的密码学算法。

6.2 共识机制安全策略

目前共识机制种类繁杂,若需要完全解决共识机制存在的安全威胁是非常困难的,但在不同场景下依然需要使用特定的共识机制来满足需求。因此,区块链安全研究人员可以从两个方面来进行研究和解决,一是深入分析不同共识机制的缺陷,针对这些缺陷采用合适的弥补方式来逐步完善共识机制的安全性;二是融合不同共识机制的优点进行互补或是设计更安全的新共识机制。

6.3 智能合约安全策略

智能合约的安全威胁主要发生在开发者代码编写过程中,因此编写完的智能合约代码必须经过严格审计,目前在市面上已经具有类似于智能合约漏洞代码自动检测的系统工具,开发者可以通过这类工具对自己编写的智能合约代码进行审计。对于智能合约编写,白帽汇安全研究院有如下几点安全建议和注意事项提示:

(1) 尽量避免外部调用;

(2) 仔细权衡再发生重要操作时的代码逻辑,避免逻辑陷阱;

(3) 处理外部调用错误;

(4) 开发者必须对外部调用的控制流程有详细的了解;

(5) 标记不受信任的业务内容;

(6) 正确的使用断言;

(7) 小心整数除法的四舍五入;

(8) 不要假设业务创建时余额为零;

(9) 记住链上的数据是公开的;

(10) 在双方或多方参与的业务应用中,参与者可能会“脱机离线”后不再返回;

(11) 明确标明函数和状态变量的可见性;

(12) 将程序锁定到特定的编译器版本;

(13) 小心分母为零;

(14) 区分函数和事件;

(15) 避免死循环;

(16) 升级有问题的业务层代码。

6.4 用户使用安全策略

普通区块链用户最关键的就是自己的私钥,黑客会通过各种手段来窃取用户的私钥,从而转移用户的数字资产。通常,用户很可能会将私钥存储在自己的电子设备上,因此电子设备的安全漏洞很容易成为黑客的攻击目标,进而入侵到用户的电子设备中窃取私钥。为了确保用户使用的安全性,最好的方式就是将私钥记忆在脑中或者记录在纸上锁进自己的保险箱中来抵御黑客的窃取。

6.5 网络安全策略

区块链底层主要是通过 P2P 网络来进行通讯,所以针对网络层的安全策略主要包含 P2P 网络安全和网络验证机制两个方面。可以从下面 3 点来进行预防:

(1)在网络的传输过程中,使用可靠的加密算法进行传输,防止恶意攻击者对节点网络进行流量窃取或劫持。如开启 Jsonrpc 的节点强制使用 https 传输,而不是 HTTP 协议进行传输。

(2)加强网络数据中传输的有效性、合理性、安全性进行验证,防止出现整型溢出等情况导致的数据错误。

(3)对于重要操作和信息,客户端节点需要进行必要的验证。

6.6 跨链安全策略

区块链跨链过程的安全性主要取决于不同区块链之间数据信息交互的原子性、同步性和网络通道的安全性。假设某双链系统具有区块链 A 和区块链 B,那么区块链 A 的改变应该能够导致区块链 B 的状态发生瞬变,并且通信过程是不可篡改的,同时整个双链系统依然具备区块链本身的去中心化特性。目前而言,区块链跨链技术依然无法实现真正的跨链。然而,量子物理学中的量子纠缠现象非常适用于跨链数据的交互,因此将来区块链跨链领域的发展必然离不开量子物理在通信领域的突破。

6.7 应用安全策略

目前,基于区块链的数据存储与管理是区块链最广泛的应用。同时,在物联网及域名系统领域,区块链也具有良好的表现。针对金融、法律、医疗、食品等诸多行业,区块链的落地应用需做到以下基本原则:

(1)应保证用户的敏感信息不被入侵。

(2)针对区块链业务系统,应做好权限管理,防止越权操作、资源滥用等行为。

(3)在区块链接口调用层面,应注意接口设计的规范、防止接口被 DDoS 攻击。

(4)虽然区块链本质上是去中心化、去信任的数据库,但其生命周期仍免不了人为参与,在区块链应用中,应避免钓鱼攻击、社会工程学攻击等人为安全威胁。

6.8 区块链取证策略

区块链犯罪威胁的有效应对是确保社会安全的重要部分。在对区块链技术下的犯罪侦查过程中,由于区块链假名性或匿名性导致区块链取证极其困难,所以计算机取证人员在对区块链数据进行取证时,可以从区块链隐私保护威胁入手。通常计算机取证人员在进行区块链相关犯罪的工作时,为了知晓这些嫌疑账户地址背后的真实身份,都需要对区块链中一些具有嫌疑的区块链账户地址进行详细分析。因此,区块链中利用大数据技术推测用户身份的隐私保护威胁在区块链取证领域就是一种有效的方法。

从取证出发点来看,可分为以嫌疑账户地址为出发点和以嫌疑交易为出发点,取证过程与区块链隐私保护威胁中的大数据推测用户身份的过程相同。

从取证交易数据类型来看,可分为外部交易取证和内部交易取证[50]。外部交易指的是区块链用户调用智能合约发生的交易;内部交易指的是区块链中某一智能合约调用另一智能合约发生的交易。对于外部交易取证而言,取证人员可以利用区块链浏览器来追溯交易与交易的联系以及交易与账户地址的联系,也可以通过编程的方式直接对区块链的数据文件进行逆向还原区块数据信息,从而分析外部交易。对于内部交易而言,取证人员无法直接通过区块链浏览器获取,只能通过对区块链源码中控制内部交易的部分进行代码插装,即根据取证需求自己编写代码穿插到区块链源码中,然后在区块链运行过程中通过插装的程序代码获取内部交易数据,再进一步对这些内部交易数据分析,最终形成取证归档报告。

7 结束语

在区块链技术的发展下,区块链安全问题更需要被重视。在未来,区块链底层技术架构研究过程中,必须将安全问题放在重要的位置,增强区块链系统的抗攻击性。同时,对于智能合约,更应该对其进

行严格审计,保证智能合约的安全使用,避免各类合约漏洞引起重大损失。就跨链而言,必定是区块链的发展趋势,跨链技术的安全性研究道路还很长,针对目前的跨链技术安全问题,希望将来能有合理有效的方式解决。因此,区块链安全的发展应该与区块链技术发展同步进行,为区块链技术发展起到辅助作用,加快区块链产业安全落地。

参考文献:

[1] 金鑫. 基于区块链技术的网络信息安全研究[J]. 信息系统工程,2018(12):79,82.

[2] 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.
YUAN Yong, WANG Feiyue. Blockchain: the state of the art and future trends[J]. Acta Automatica Sinica, 2016, 42(4): 481 -494. (in Chinese)

[3] 王锡亮,刘学枫,赵淦森,等. 区块链综述:技术与挑战[J]. 无线电通信技术,2018,44(6):531 -537.
WANG Xiliang, LIU Xuefeng, ZHAO Gansen, et al. Overview of blockchain: technology and challenges[J]. Radio Communications Technology, 2018, 44(6):531 -537. (in Chinese)

[4] 邵奇峰,金澈清,张召,等. 区块链技术: 架构及进展[J]. 计算机学报,2018,41(5):969 -988.
SHAO Qifeng, JIN Cheqing, ZHANG Zhao, et al. Blockchain: architecture and research progress[J]. Chinese Journal of Computers, 2018, 41(5):969 -988. (in Chinese)

[5] 汪垚. 区块链技术在互联网安全中的应用探究[J]. 企业科技与发展. 2019(2):133 -134.

[6] ALI M, NELSON J, SHEA R, et al. Blockstack: a global naming and storage system secured by blockchains[C]// Annual Technical Conference. 2016: 181 -194.

[7] 孙国梓,冒小乐,陈鼎洁,等. 基于区块链技术的电子数据存证系统[J]. 西安邮电大学学报,2018,23(4):82 -87.
SUN Guozi, MAO Xiaole, CHEN Dingjie, et al. Electronic data storage and certificate system based on blockchain [J]. Journal of Xi'an University of Posts and Telecommunications, 2018, 23(4):82 -87. (in Chinese)

[8] 张俊,高文忠,张应晨,等. 运行于区块链上的智能分布式电力能源系统:需求、概念、方法以及展望[J]. 自动化学报,2017,43 (9):1544 -1554.
ZHANG Jun, GAO Wenzhong, ZHANG Yingchen, et al. Blockchain based intelligent distributed electrical energy systems: needs, concepts, approaches and vision[J]. Acta Automatica Sinica, 2017, 43(9): 1544 -1554. (in Chinese)

[9] LI Z, BARENJI A V, HUANG G Q. Toward a blockchain cloud manufacturing system as a peer to peer distributed network platform[J]. Robotics and Computer-Integrated Manufacturing, 2018, 54: 133 -144.

[10] RIZK A, BISBAL J, BERGSTRÄBER S, et al. Brokerless inter-domain virtual network embedding: a blockchain-based approach[J]. IT-Information Technology, 2018, 60 (5/6): 293 -306.

[11] CHAKRAVORTY A, RONG C. Ushare: user controlled social media based on blockchain[C]// Proceedings of the 11th International Conference on Ubiquitous Information Management and Communication. 2017: 99.

[12] SAMANIEGO M, DETERS R. Blockchain as a service for IoT[C]// IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData). 2016: 433 -436.

[13] 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.
SI Xueming, XU Mixue, YUAN Chao. Survey on security of blockchain[J]. Journal of Cryptologic Research, 2018, 5(5):458 -469. (in Chinese)

[14] WÜST K, GERVAIS A. Ethereum eclipse attacks[R]. Zurich: ETH Zurich, 2016.

[15] 邓栊涛,毛向杰. 后量子密码技术在区块链系统中的应用[J]. 信息通信,2018,31(12):54 -56.
DENG Longtao, MAO Xiangjie. The application of post-quantum cryptography in blockchain system[J]. Information & Communications, 2018, 31(12):54 -56. (in Chinese)

[16] 邸剑,吝伟华. 区块链中矿池选择策略的研究与分析[J/OL]. 计算机应用研究,2019,37(6):1 -6[2019-08-10]. https://doi.org/10.19734/j.issn.1001-3695.2018.12.0875.
DI Jian, LIN Weihua. Research and analysis of mining pool selection strategy in blockchain[J/OL]. Application Research of Computers, 2019, 37(6): 1 -6[2019-08-10]. https://doi.org/10.19734/j.issn.1001-3695.2018.12.0875. (in Chinese)

[17] 李康,孙毅,张珺,等. 零知识证明应用到区块链中的技术挑战[J]. 大数据,2018,4(1):57 -65.
LI Kang, SUN Yi, ZHANG Jun, et al. Technical challenges in applying zero-knowledge proof to blockchain[J]. Big Data Research, 2018, 4(1): 57 -65. (in Chinese)

[18] 韩健,邹静,蒋瀚,等. 比特币挖矿攻击研究[J]. 密码学报,2018,5(5):470 -483.
HAN Jian, ZOU Jing, JIANG Han, et al. Research on mining attacks in bitcoin[J]. Journal of Cryptologic Research, 2018, 5(5): 470 -483. (in Chinese)

[19] PORRU S, PINNA A, MARCHESI M, et al. Blockchain-oriented software engineering: challenges and new directions[C]// IEEE/ACM 39th International Conference on

Software Engineering Companion (ICSE-C). IEEE,2017: 169 - 171.

[20] VUKOLIĆ M. Rethinking permissioned blockchains[C]// Proceedings of the ACM Workshop on Blockchain, Cryptocurrencies and Contracts. ACM,2017: 3 - 7.

[21] 钱卫宁,邵奇峰,朱燕超,等. 区块链与可信数据管理:问题与方法[J]. 软件学报, 2018,29(1):150 - 159.
QIAN Weining, SHAO Qifeng, ZHU Yanchao, et al. Research problems and methods in blockchain and trusted data management[J]. Journal of Software, 2018, 29(1): 150 - 159. (in Chinese)

[22] ATZEI N, BARTOLETTI M, CIMOLI T. A survey of attacks on ethereum smart contracts (SoK)[C]// Principles of Security and Trust. 2017:164 - 186.

[23] CHRISTIDIS K, DEVETSIKIOTIS M. Blockchains and smart contracts for the Internet of Things[J]. IEEE Access,2016,4: 2292 - 2303.

[24] FAOUR N. Transparent voting platform based on permissioned blockchain[EB/OL]. [2019-06-10]. arXiv Preprint arXiv1802. 10134. https: // arxiv. org/abs/ 1802. 10134.

[25] KOSBA A, MILLER A, SHI E, et al. Hawk: the blockchain model of cryptography and privacy-preserving smart contracts[C]// IEEE Symposium on Security and Privacy (SP). IEEE,2016.

[26] WATANABE H, SHIGERU F, ATSUSHI N, et al. Blockchain contract securing a blockchain applied to smart contracts[C]// IEEE International Conference on Consumer Electronics (ICCE). IEEE,2016.

[27] NUGENT T, UPTON D, CIMPOESU M. Improving data transparency in clinical trials using blockchain smart contracts[J/OL]. F1000Research,2016,5: 2541[2019-07-20]. https://doi. org/10. 12688/f1000research. 9756. 1.

[28] RAMACHANDRAN A, KANTARCIOGLU M. Using blockchain and smart contracts for secure data provenance management[EB/OL]. 2017[2019-07-25]. arXiv Preprint arXiv1709. 10000. https://arxiv. org/abs/1709. 10000.

[29] WEBER I, XU X, RIVERET R, et al. Untrusted business process monitoring and execution using blockchain[C]// International Conference on Business Process Management. 2016.

[30] 刘敖迪,杜学绘,王娜,等. 区块链技术及其在信息安全领域的研究进展[J]. 软件学报,2018,29(7):2092 - 2115.
LIU Aodi, DU Xuehui, WANG Na, et al. Research progress of blockchain technology and its application in information security[J]. Journal of Software, 2018, 29(7): 2092 - 2115. (in Chinese)

[31] SMITH B R, GARCIA-LUNA-ACEVES J J. Securing the border gateway routing protocol[C]// IEEE Global Telecommunications Conference. 1996.

[32] MOHURLE S, PATIL M. A brief study of wannacry threat: Ransomware attack 2017[J]. International Journal of Advanced Research in Computer Science,2017,8(5): 454 - 460.

[33] 李芳,李卓然,赵赫. 区块链跨链技术进展研究[J]. 软件学报,2019,30(6):1649 - 1660.
LI Fang, LI Zhuoran, ZHAO He. Research on the progress in cross-chain technology of blockchains[J]. Journal of Software,2019,30(6):1649 - 1660. (in Chinese)

[34] 曾帅,袁勇,倪晓春,等. 面向比特币的区块链扩容:关键技术,制约因素与衍生问题[J]. 自动化学报,2019,45(6):1015 - 1030.
ZENG Shuai, YUAN Yong, NI Xiaochun, et al. Scaling blockchain towards bitcoin: key technologies, constraints and related issues[J]. Acta Automatica Sinica,2019,45(6):1015 - 1030. (in Chinese)

[35] GREEN M, MIERS I. Bolt: anonymous payment channels for decentralized currencies[C]// Proceedings of the ACM SIGSAC Conference on Computer and Communications Security. ACM,2017: 473 - 489.

[36] KSHETRI N. Blockchain's roles in strengthening cybersecurity and protecting privacy[J]. Telecommunications Policy,2017,41(10): 1027 - 1038.

[37] AHMED S, BROEK N. Food supply: blockchain could boost food security[J]. Nature,2017,550(7674): 43.

[38] 吴振铨,梁宇辉,康嘉文,等. 基于联盟区块链的智能电网数据安全存储与共享系统[J]. 计算机应用,2017,37(10):2742 - 2747.
WU Zhenquan, LIANG Yuhui, KANG Jiawen, et al. Secure data storage and sharing system based on consortium blockchain in smart grid[J]. Journal of Computer Applications,2017,37(10):2742 - 2747. (in Chinese)

[39] 张诗童,秦波,郑海彬. 基于哈希锁定的多方跨链协议研究[J]. 网络空间安全,2018,9(11):57 - 62,67.
ZHANG Shitong, QIN Bo, ZHENG Haibin. Research on the protocol of multiple cross-chains based on the hash lock[J]. Cyberspace Security,2018,9(11):57 - 62,67. (in Chinese)

[40] WOHRER M, ZDUN U. Smart contracts: security patterns in the ethereum ecosystem and solidity[C]// International Workshop on Blockchain Oriented Software Engineering (IWBOSE). IEEE,2018.

[41] AZARIA A, EKBLAW A, VIEIRA T, et al. MedRec: using blockchain for medical data access and permission management[C]// IEEE International Conference on Open and Big Data. 2016: 25 - 30.

[42] BULDAS A, LAANOJA R, TRUU A. Keyless signature infrastructure and PKI: hash-tree signatures in pre-and post-quantum world[J]. International Journal of Services Technology & Management,2017,23(1/2): 117.

[43] BULDAS A, LAANOJA R, TRUU A. Efficient quantum-

immune keyless signatures with identity[J]. IACR Cryptology ePrint Archive,2014: 321.

[44] ANDREAS B, MATHIEU C, MEEUW A. A decentralised sharing app running a smart contract on the ethereum blockchain[C]// Proceedings of the 6th International Conference on the Internet of Things. ACM,2016.

[45] 徐晓冰,戚枭宏,王建平,等. 基于区块链的物联网可伸缩管理机制[J/OL]. 计算机应用研究,2019,37(7): 1-5[2019-08-20]. https://doi.org/10.19734/j.issn.1001-3695.2019.01.0022.
XU Xiaobing, QI Xiaohong, WANG Jianping, et al. IoT scalable management mechanism based on blockchain[J/OL]. Application Research of Computers,2019,37(7):1-5[2019-08-20]. https://doi.org/10.19734/j.issn.1001-3695.2019.01.0022. (in Chinese)

[46] KHAN M A, SALAH K. IoT security: review, blockchain solutions, and open challenges[J]. Future Generation Computer Systems,2018,82: 395-411.

[47] ANTONAKAKIS M, APRIL T, BAILEY M, et al. Understanding the mirai botnet[C]//26th Security Symposium (Security 17). 2017: 1093-1110.

[48] HU Weihong, AO Meng, SHI Lin, et al. Review of blockchain-based DNS alternatives[J]. Chinese Journal of Network and Information Security,2017,3(3): 71-77.

[49] ZYSKIND G, NATHAN O. Decentralizing privacy: using blockchain to protect personal data[C]// IEEE Security and Privacy Workshops. 2015: 180-184.

[50] 孙国梓,王纪涛. 浅析区块链取证与存证[J]. 中国信息安全,2019(5):61-64.