区块链中攻击方式的研究

刘汉卿 阮 娜

(上海交通大学电子信息与电气工程学院 上海 200240)

摘 要 随着以数字加密货币为代表的区块链 1.0 技术和以以太坊为代表的区块链 2.0 技术的发展,区块链技术的安全性成为了研究热点问题.区块链系统的数据层、网络层、共识层、激励层、合约层与应用层均存在可被攻击者利用的漏洞.本文通过分析比特币、以太坊等平台中常见的攻击方式,提出了全新的区块链中攻击方式的分类方法.本文提出的攻击分类方法体现出不同攻击方式间的差异性与关联性,并从多个角度归纳了各类攻击的特点.最后,本文根据各类攻击特点总结了区块链中攻击方式的预防措施和检测方法,并指出了区块链中攻击问题的未来研究方向.

关键词 区块链;比特币;以太坊;共识机制;智能合约

中图法分类号 TP311 **DOI 号** 10.11897/SP.J.1016.2021.00786

A Survey on Attacking Strategies in Blockchain

LIU Han-Qing RUAN Na

(*School of Electronic Information and Electrical Engineering, Shanghai Jiao Tong University, Shanghai* 200240)

Abstract The blockchain technology is the basis of digital cryptocurrencies like Bitcoin and Ethereum. With the development of blockchain technology, the security of the blockchain technology has been seen as the top priority and been widely concerned by the public. Generally speaking, a blockchain consists of six layers: the data layer, the network layer, the consensus layer, the incentive layer, the contract layer, and the application layer. In recent years, researchers have proposed many attacking strategies in all six layers of the blockchain. The data layer is threatened by exposure of nodes' identity and disclosure of private data. The network layer, the consensus layer, and the incentive layer face many well-known attacking strategies, including eclipse attack, routing attack, selfish mining, stubborn mining, and block withholding attack. The smart contract layer is threatened by the code vulnerability in smart contracts and is vulnerable to attacks like 'The Dao' attack. The application layer faces the problems brought by the vulnerability in decentralized applications. There are both correlations and differences among those attacks in the blockchain. For example, selfish mining and block withholding attack relate to the same layers of the blockchain, but there are some significant differences between them. Meanwhile, an effective way to optimize an attack in the blockchain is to combine it with another attack. For instance, selfish mining attack can be combined with block withholding attack, and the combination of selfish mining attack and block withholding attack is named as fork after withholding attack. Analyzing the attacks independently cannot help to reveal the correlations and differences among attacks in the blockchain. In our work, we analyze well-known attacks in the blockchain and

收稿日期:2019-05-23;在线发布日期:2020-02-13.本课题得到国家自然科学基金青年基金(61702330)资助.**刘汉卿**,硕士研究生,主要研究方向为区块链安全性与区块链中的数据隐私.E-mail:hqliu233@sjtu.edu.cn.**阮 娜**(通信作者),博士,副教授,中国计算机学会(CCF)专业会员,主要研究方向为安全与隐私、区块链与大数据.E-mail:naruan@cs.sjtu.edu.cn.

propose a novel method to classify attacks in the blockchain. Our attack classification method preserves the correlations and reveals the differences between different attacks in the blockchain. Our attack classification method first classifies attacks into four types: attacks in the data layer, attacks in the network layer, the consensus layer and the incentive layer, attacks in the contract layer, and attacks in the application layer. Attacks in each type can be further classified according to some principles. For example, attacks in the data layer can be further classified according to the attackers' aim. The attack classification method proposed by our work helps to summarize the characteristics of the attacks. With these characteristics, the preventive measures and detecting measures of each attack can be concluded. For example, some attacks in the network layer, the consensus layer and the incentive layer including selfish mining and block withholding attack can be prevented by designing reasonable parameters of the blockchain. These attacks can also be detected via monitoring the valid computational power in the blockchain system. Some attacks in the contract layer can be prevented by some smart contract security analysis tools such as OYENTE and can be detected via graph analysis of the blockchain network. Our work also points out that optimizing attacking strategies in the blockchain, developing efficient smart contract security analysis tools, and regulating the blockchain through anonymization are three promising fields in blockchain research.

Keywords　blockchain; Bitcoin; Ethereum; consensus mechanism; smart contract

1　引　言

随着互联网时代的到来，交易双方几乎完全依赖于第三方金融机构处理电子支付并实现线上交易.但是，第三方机构带来了隐私泄露问题，这也引发了公众对第三方机构中数据安全的担忧.当缺乏可信任的第三方机构时，交易双方需要一个全新的机制进行交易[1].区块链技术可以解决缺乏可信第三方机构的问题.

2008 年，有学者化名为“中本聪”提出区块链的概念[2].区块链技术基于密码学原理的分布式共识账本技术.区块链以链式区块结构存储数据，具有去中心、开放、交易透明、交易双方匿名与不可篡改等特征.区块链技术出现之后，许多大型机构将其视作改变业务运作方式的突破性技术.中国工业和信息化部在《中国区块链技术和发展应用白皮书》中将当前的区块链技术分为区块链 1.0 阶段技术与区块链 2.0 阶段技术，并对区块链 3.0 阶段技术做了展望[3].

在区块链 1.0 阶段，区块链技术主要被应用于以比特币、莱特币[4]和比特币现金为代表的数字加密货币.区块链 2.0 阶段的代表是以太坊[5].在区块链 2.0 阶段还出现了微软以太坊区块链即服务、IBM 超级账本 Hyperledger Fabric[6]、亚马逊 AWS 区块链模板、百度区块链开放平台、腾讯云区块链即服务等区块链即服务(BaaS)技术平台.

尽管随着区块链即服务技术平台的出现，区块链技术正由区块链 1.0 阶段向区块链 2.0 阶段过渡，但数字加密货币仍然是区块链技术最主要的应用.表 1 中列举了迄今为止(2019.10)市值最庞大的六种数字加密货币.在这些数字加密货币中，比特币、当前阶段的以太币、比特币现金与莱特币采用了工作量证明共识机制.工作量证明共识机制在比特币等数字加密货币中的成功应用以及比特币的先发优势是工作量证明共识机制被广泛采用的直接原因[7].

表 1　主要数字加密货币市值与其共识机制

数字加密货币名称	市值	共识机制
比特币(Bitcoin)	$147,535,421,488	工作量证明
以太币(Ether)	$19,813,404,611	工作量证明/权益证明
瑞波币(XRP)	$12,120,271,587	瑞波共识
比特币现金(Bitcoin Cash)	$4,192,486,587	工作量证明
莱特币(Litecoin)	$3,677,545,736	工作量证明
EOS 币(EOS)	$2,958,673,545	委任权益证明

以比特币为代表的基于区块链的数字加密货币拥有着庞大的市值，这不可避免地导致了针对这些数字加密货币的攻击的出现.2010 年 8 月，未知黑

客利用比特币大整数溢出的漏洞，创造了超过 1800 亿枚比特币，比特币因此被迫进行了历史上第一次硬分叉.这次攻击被普遍认为是针对工作量证明数字加密货币的第一起攻击，攻击者利用了比特币的代码漏洞.在此之后，随着比特币等数字加密货币的不断完善，攻击者逐渐将目标转移至区块链机制本身以及区块链生态.2012 年 3 月，比特币交易所 Bitcoinica 被黑客盗取客户的比特币密钥.2016 年，由于以太坊智能合约中的重大漏洞，黑客得以使用单一币种多次提现并使 The DAO 项目[8]遭受攻击.该次攻击导致了以太坊区块链硬分叉.2018 年 4 月，比特币黄金(Bitcoin gold)遭遇了 51%攻击，损失超过 1800 万美元.2018 年 4 月，攻击者利用美币(Beauty chain)智能合约中的漏洞，盗取 579 亿枚美币.2018 年 5 月，萌奈币(Monacoin)遭受自私挖矿(Selfish mining)攻击，损失超过 9 万美元.上述针对数字加密货币的攻击中，攻击者利用区块链本身机制问题以及区块链生态中的漏洞实施攻击.

在学术界，研究者们倾向于研究涉及区块链机制的攻击问题.2008 年中本聪在提出区块链技术的同时提出了 51%攻击[2]，并说明比特币在攻击者拥有大多数算力时是不可靠的.Miller 等研究者[9]在此后发现比特币中的算力有着集中的趋势，这提升了比特币遭受 51%攻击的风险.Karame 等研究者[10]在 2012 年的研究展现了双花攻击(double spending)在比特币快速支付场景中的应用.此后，Rosenfeld[11]、Karame[12]、Gervais[7]与 Möser[13]等研究者分别从不同角度分析了数字加密货币中的双花攻击问题.2014 年 Eyal 等研究者[14]提出自私挖矿攻击，攻击者通过隐藏区块的方式实现自私挖矿攻击.Göbel 等研究者[15]与 Heilman 等研究者[16]分别分析了自私挖矿攻击的可行性与阻止自私挖矿攻击的措施.Nayak[17]、Sapirshtein[18]与 Kwon[19]等研究者随后分别提出了对自私挖矿攻击的优化.Carlsten 等研究者[20]分析了比特币中自私挖矿攻击的发展趋势.Eyal 等研究者[21]提出了区块截留攻击(Block Withhoulding Attack)，并指出矿池(Mining pool)在区块截留攻击中面临囚徒困境问题.Courtois 等研究者[22]进一步优化了区块截留攻击中攻击者的策略.Laszka 等研究者[23]通过博弈论指出了区块截留攻击为区块链系统带来的影响.在上述研究中，研究者们提出的攻击主要针对区块链的共识机制与激励机制.研究者们也意识到区块链系统中的组网方式、消息传播机制与智能合约同样可以被攻击者针对.2015 年 Biryukov 等研究者[24]提出了针对比特币的女巫攻击(Sybil attack)，Heilman 等研究者[25]提出了日蚀攻击(Eclipse attack).在 Heilman 工作的基础上，Nayak 等研究者[17]研究了日蚀攻击对自私挖矿攻击的影响.2016 年之后，Juels[26]、Luu[27]与 Tsankov[28]等研究者将区块链中的攻击拓展到了区块链的合约层.

随着区块链技术的不断发展，目前国内外已有多篇关于区块链技术的综述类研究成果.Bonneau 等研究者[29]讨论了比特币的稳定性与匿名性，并分析了比特币等数字加密货币的发展现状与发展前景.Tschorsch 等研究者[30]从比特币的协议、安全、隐私与网络架构方面介绍了区块链技术的发展现状以及区块链技术在数字加密货币中的应用现状.袁勇等研究者[31]总结了区块链的基础模型与关键技术，并对区块链技术的发展做了展望.何蒲等研究者[32]讨论了区块链的基础技术与应用前瞻.邵奇峰等研究者[33]介绍了区块链的系统架构.Atzei 等研究者[34]总结了针对以太坊中智能合约的攻击.Lin 等研究者[35]介绍了区块链中的一些攻击方式以及区块链在可扩展性方面面临的安全性威胁.Li 等研究者[36]介绍了区块链中的攻击方式与区块链合约层中的攻击实例.韩璇等研究者[37]总结了区块链中安全问题的研究现状.在上述综述中，Atzei[34]、Lin[35]、Li[36]与韩璇[37]等研究者的综述工作涉及了区块链的安全问题.

现有关于区块链安全问题的综述侧重于独立分析每一个攻击策略，且没有对区块链中的攻击做出分类[34-35]或仅依据攻击所在的区块链层次将攻击简单分类[36-37].独立地分析两个所在层次相同的攻击(例如自私挖矿攻击与区块截留攻击)不利于通过对比得出这两个同层次攻击间的差异性.同时，在现实中也存在着“跨层次”的攻击(例如自私挖矿攻击涉及区块链共识层与激励层)与“跨层次组合”的攻击(例如共识层与激励层的固执挖矿攻击可以与网络层的日蚀攻击组合).对攻击不做分类或仅依靠攻击所在层次分类割裂了不同层次间攻击的关联.因此，现有的攻击分类方法难以体现同层次攻击间的差异性与不同层次攻击间的关联性.

与上述工作不同，本文通过分析区块链中各攻击方式之间的关联性与差异性，提出了全新的攻击分类方法.本文提出的攻击分类方法在保留不同层次攻击间的关联性的同时，还体现出了同层次攻击间的差异性.区块链中的攻击方式可以首先根据攻击所在的区块链层次分为四大类：区块链数据层中的攻击、区块链网络层、共识层、激励层中的攻击、区

块链合约层中的攻击与区块链应用层中的攻击.每一大类攻击可以依据一定的分类标准进一步细分以体现同一大类不同攻击间的差异性.区块链数据层中的攻击可以依据攻击者的目的进一步分类;区块链网络层、共识层、激励层中的攻击可以依据攻击者的行为、攻击者的目的、受攻击对象进一步分类;区块链合约层中的攻击可以依据攻击者利用的漏洞类型进一步分类;区块链应用层中的攻击可以依据导致攻击发生的因素进一步分类.当区块链中出现攻击时,本文提供的攻击分类方法可以准确地将攻击分类并从多个角度总结出该攻击的特点.此外,本文还根据各类攻击的特点提出了各类攻击的预防检测措施.

本文第 2 节介绍区块链的层次架构以及区块链各层面临的安全性问题;第 3 节提出区块链中攻击的分类方法;第 4 节提出对各类区块链中攻击方式的预防与检测措施;第 5 节指出区块链攻击问题的未来研究方向;第 6 节总结全文.

2　区块链的架构及各层的安全性问题

本节通过介绍区块链系统的层次与架构,说明区块链系统各层面临的安全性问题.

2.1　区块链架构

中本聪[2]将区块链系统划分为数据层、网络层、共识层与激励层.中国工业和信息化部[3]将区块链 2.0 阶段的区块链架构划分为数据层、网络层、共识层、激励层与智能合约层.袁勇等研究者[31]将区块链划分为数据层、网络层、共识层、激励层、合约层与应用层.本文采用如图 1 所示的区块链六层架构模型.

图 1　区块链六层架构

区块链数据层涉及了时间戳[38-40]、梅克尔树(Merkle tree)[41-43]和哈希函数[44-45]等关键技术.通常来说,每一个区块包含区块头(Block header)与区块体(Block body).以比特币为例,比特币的区块头中存储了当前协议版本、前一个区块的哈希值、梅克尔根、当前系统中生成区块的难度、记录该区块产生时间的时间戳和一个随机数[2].区块体中包含了当前区块记录的交易信息.区块以链式结构存储保证了区块链中数据的不可篡改性.

区块链网络层封装了区块链系统的组网方式、消息传播协议和数据验证机制等要素[31].区块链系统大多使用对等式(P2P)网络,节点以扁平拓扑结构相联通.比特币与以太坊基于 TCP 实现 P2P 协议,每个节点承担着路由、验证区块数据、广播区块、广播交易信息和选择节点的功能.

区块链共识层的核心技术是共识机制.主流的区块链共识机制有:工作量证明(Proof of Work,POW)[2]、权益证明(Proof of Stake,POS)[46]、实用拜占庭容错(Practical Byzantine Fault Tolerance,PBFT)[47]、委任权益证明(Delegated Proof of Stake,DPOS)[48]与瑞波共识(Ripple)[49]等.基于区块链的数字加密货币大多采用工作量证明共识机制.

区块链的激励层保障了去中心化系统的有效运行.区块链的激励机制包含了发行机制与分配机制.以比特币为例,节点生成新区块后可以获得一定数额的区块奖励.除区块奖励外,新区块中包含的交易手续费也将奖励给发现新区块的节点.比特币的分配机制决定了仅有发现新区块的节点可以获得奖励.为了能够更稳定地获取“挖矿”收益,拥有较小算力的矿工自发组织了矿池.目前主流的矿池分配机制是 PPS 模式(Pay Per Share)与 PPLN 模式(Pay Per Last N Shares)[50].

区块链合约层包含由各类脚本代码、算法生成的智能合约.智能合约的概念由 Sazbo 等研究者① 提出.比特币等数字加密货币采用简单的脚本代码控制交易过程,这些脚本代码是非图灵完备的.以太坊率先应用图灵完备的智能合约脚本语言.智能合约为互不信任的实体提供了在没有可信第三方的条件下进行交易的方法.

区块链应用层封装了区块链的应用场景和应用案例.在区块链 1.0 阶段,区块链的应用层主要支持

① First Monday. https://doi.org/10.5210/fm.v2i9.548

数字加密货币交易;在区块链 2.0 阶段,区块链的应用层除了支持数字加密货币交易外,还支持去中心化应用.

2.2 区块链各层的安全性问题

区块链数据层面临着密钥被泄露、节点关联性被暴露等安全性问题.在短期内,区块链数据层涉及到的哈希函数、数字签名与零知识证明等技术难以受到计算技术的威胁.但是未来计算技术的发展可能导致上述密码算法的失效.基于区块链的数字加密货币通过数字假名实现匿名性.然而,区块链中记录的交易信息保留了用户节点之间的关联性.节点间关联性被暴露威胁了基于区块链的数字加密货币的匿名性.

区块链网络层的组网方式、消息传播机制为攻击者提供了一定的便利.攻击者通过获取受害节点路由信息、控制受害节点的相邻节点、误导受害节点的相邻节点等方式实施路由攻击、日蚀攻击等攻击.攻击者可以将受害节点与区块链网络完全隔离,从而分裂区块链网络.

区块链共识层的共识机制可以被攻击者利用.目前基于区块链的数字加密货币主要采用工作量证明共识机制.工作量证明机制的安全性依赖于"区块链中大多数节点都是诚实的"这一假设.然而该假设并非可靠,矿池的出现增加了攻击者拥有区块链系统中大多数算力的可能性.

区块链激励层的安全性依赖于"矿工节点获得区块奖励的数量与节点拥有的资源(例如工作量证明共识机制下节点的算力)成正比"这一假设.然而,一些恶意节点可能期望获得高于自己应有份额的区块奖励.

区块链合约层中的智能合约代码对于所有节点是公开可见的.智能合约被发布后,其代码便不可更改.攻击者可以通过分析智能合约代码中的数据结构漏洞或逻辑漏洞发起攻击.

区块链应用层的开发通常依赖于区块链服务供应商.第三方机构在开发应用层的过程中产生的代码漏洞威胁了区块链应用的安全性.同时,基于区块链的应用也为这些第三方机构带来了监管问题.

3 区块链中攻击的分类

在当前的研究中,研究者们倾向于根据区块链中攻击所在层次对区块链中的攻击进行分类.在该分类方法下,区块链中的攻击分为数据层攻击、网络层攻击、共识层攻击、激励层攻击、合约层攻击和应用层攻击.依据区块链中攻击所在层次分类可以大致地将区块链中的攻击方式做区分,但是仅仅依靠区块链中攻击所在层次分类存在三大问题:

(1)该分类方式不能体现同层次攻击之间的差异性:例如 The Dao 攻击与对 Fomo3D 游戏的攻击都属于区块链合约层中的攻击.但是两个攻击中,攻击者的目的与攻击者实施攻击的方式有很大的差异.

(2)存在着大量"跨层次"的攻击:例如自私挖矿攻击与区块截留攻击既涉及了区块链共识层的共识机制,也涉及了区块链激励层的激励机制与分配机制.

(3)存在着攻击"跨层次组合"问题:例如日蚀攻击属于网络层攻击,但是日蚀攻击可以与涉及共识层与激励层的自私挖矿攻击或固执挖矿攻击结合,形成新的攻击策略.

"跨层次"攻击与"跨层次组合"攻击问题基本上集中于区块链的网络层、共识层与激励层.因此,发生在区块链网络层、共识层与激励层的攻击间存在着较高的关联性.为了避免割裂不同层次间攻击的关联,本章首先将区块链中的攻击分为四大类:数据层攻击、网络层、共识层、激励层攻击、合约层攻击与应用层攻击.

区块链应用层中的攻击多数由区块链用户疏忽或区块链生态漏洞导致,与区块链技术本身的关联性较小.因此本章将着重介绍区块链数据层中攻击、区块链网络层、共识层、激励层中攻击与区块链合约层中攻击的分类,并总结各类攻击的特点.

3.1 数据层中攻击分类

数据层中的攻击可以依据攻击者目的分为三类:(1)目的是获取节点身份信息;(2)目的是窃取链上隐私数据;(3)目的是篡改链上数据.

(1)目的是获取节点身份信息.基于区块链的数字加密货币的匿名性由数字假名保证,一个用户可以同时拥有多个数字假名.尽管参与交易的双方通过这种方式实现匿名,然而在多数数字加密货币中,交易双方的关联性仍被记录在区块链上.两个区块链节点间的关联性可以通过这两个节点间的交易记录推测[51].启发式聚类等方法[52]可以进一步聚类区块链节点,并展现各簇节点间的关联性.攻击者可以利用区块链节点间的关联性推测节点的真实身

份.这类攻击的特点是:攻击者依赖于节点间的关联性.

攻击者依赖于节点间的关联性:该类攻击的攻击者主要通过区块链图分析[53-56]与对区块链节点聚类[52,57]实施攻击.这两种方式的最终目的都是获取区块链网络所有节点之间的关联性,从而推断特定节点的真实身份.

(2)目的是窃取链上隐私数据.区块链技术也被应用于数据共享与数据管理等领域[58-59].基于区块链的隐私数据共享需要确保上链数据的正确性、上链数据的隐私性与上链数据的可共享性.在医疗数据共享[60]以及个人信息共享[61]等场景中,若直接将数据上链,攻击者可以轻易地获取大量用户的隐私数据.这类攻击的特点是:攻击者可以获取权限以外的隐私数据.

攻击者可以获取权限以外的隐私数据:公链中的隐私数据共享一般通过链上(信息共享)-链下(隐私数据计算)的模式实现[58].在该模式下,链上部分仅保留计算最终结果等信息,参与链下计算部分的节点可以获得需要计算的隐私数据.攻击者可以伪装成可信任节点执行链下计算并获取权限外的隐私数据.

(3)目的是篡改链上数据.保证上链数据的不可篡改性是区块链技术的特点之一.区块链每个区块的区块头中存储着上一个区块区块头哈希值,这保证了被篡改数据的区块会立即被其余节点识别出.攻击者可以通过变色龙哈希函数[62](chameleon hash functions)在区块链中重写特定区块或重写特定区块中的特定交易[63-64].该类攻击的特点是:攻击者新生成的区块需要被多数节点接受.

攻击者新生成的区块需要被多数节点接受:显而易见的是,攻击者无论是重写区块链中的某一区块,还是重写特定区块中的特定交易,都需要生成新的区块并将其传播到区块链网络中,该新生成的区块需要得到多数节点的共识.

3.2　网络层、共识层、激励层中攻击分类

区块链网络层、共识层、激励层中的攻击被广泛研究,因为它们是所有攻击中与区块链机制关系最密切的.攻击者根据区块链机制提出相应的攻击策略.此类攻击涉及到大量攻击方式,难以通过单一的标准对这些攻击实现精确的分类.因此,本章中将提出三个分类标准对区块链网络层、共识层、激励层中的攻击进行分类.

3.2.1　依据攻击者行为分类

在此分类标准下,区块链网络层、共识层、激励层中的攻击可以分作四类:(1)攻击者选择时机发布新区块;(2)攻击者藏匿或丢弃区块;(3)攻击者部署伪节点;(4)攻击者直接制造分叉.

(1)攻击者选择时机发布新区块.攻击者常通过自行选择发布区块时机的方式获取额外的收益.这类攻击以自私挖矿攻击为代表[14-15],除了自私挖矿攻击以外,这类攻击还包括固执挖矿攻击[17]、优化自私挖矿攻击[18]和多人自私挖矿攻击[65-66]等.这类攻击具有以下特点:攻击者行为取决于攻击者状态与状态转移概率;攻击者的行为在区块链中制造分叉;攻击者的攻击行为存在着失败的概率.

攻击者行为取决于攻击者状态与状态转移概率:以自私挖矿攻击为例,自私挖矿攻击的核心思想在于攻击者根据自身状态决定下一步的行为,并通过选择性地发布自己发现的区块浪费区块链网络中其余矿工的算力.在自私挖矿攻击模型中,攻击者的状态表示攻击者未发布的私有链领先主链的区块个数,被记作 S.攻击者的行为依据如图 2 所示的状态机,该状态机规定了攻击者发布区块的时机以及发布区块的数量.图中参数 β 表示攻击者的算力在全网占比,参数 γ 表示攻击者在诚实矿工中的影响力.

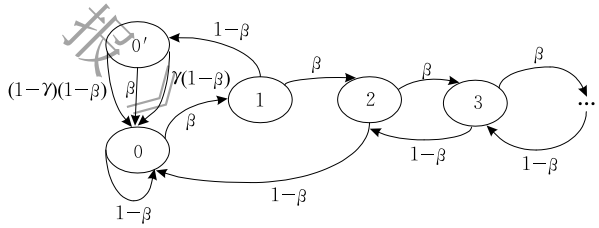

图 2　自私挖矿状态机

固执挖矿攻击在自私挖矿攻击的基础上,扩展了攻击者的状态.与自私挖矿攻击相同,攻击者的行为取决于状态机.

优化自私挖矿策略与固执挖矿策略有着相似的效果.但是优化自私挖矿策略不再取决于状态机,而是依赖状态转移概率通过马尔科夫决策过程寻找最优策略.优化自私挖矿策略未能考虑到网络传播时延参数,在引入网络传播时延参数后,优化自私挖矿策略无法再取得超越自私挖矿攻击的表现.

攻击者的行为在区块链中制造分叉:该类攻击主要针对采用工作量证明共识机制的区块链.工作量证明区块链中,矿工普遍需要遵守一定的协议,如比特币协议.遵守协议的矿工被称为诚实矿工.诚实

矿工承认区块链网络内最长链中的区块，并在最长链尾部“挖矿”.当诚实矿工发现新的区块时，会立即向区块链网络广播.这些协议避免了区块链网络中出现长时间分叉，但是却无法阻止攻击者主动地制造分叉.

在自私挖矿攻击、固执挖矿攻击与优化自私挖矿攻击中，攻击者的行为中都包含了“匹配(Match)”操作以及“覆盖(Override)”操作.通过“匹配”操作，攻击者在区块链中制造与当前主链高度相同的分叉链；通过“覆盖”操作，攻击者在区块链网络中制造高度高于当前主链的分叉链.

攻击者的攻击行为存在着失败的概率：这类攻击中，攻击者蓄意制造区块链分叉的行为存在着失败概率.当攻击者实施“覆盖”操作时，由于攻击者发布的分叉链长度长于主链，诚实矿工将承认该分叉链并在分叉链尾部继续“挖矿”.但是，当攻击者实施“匹配”操作时，攻击者无法保证攻击者发布的链被区块链网络中的诚实节点承认.

攻击者算力越高，单次攻击行为失败的概率越低.因此，仅有计算力高于一定阈值的攻击者才可以提高自己挖出的区块在全网中所占的份额.在自私挖矿中该阈值为 1/3，即计算力超过全网算力 1/3 的攻击者能获得更高相对收益[14].固执挖矿和优化自私挖矿策略可以将该阈值最多降低至 23%[17].当攻击者算力达不到一定阈值时，攻击者无法通过攻击获得额外收益.

(2)攻击者丢弃区块.藏匿并丢弃已发现的区块同样可以成为攻击者的攻击方式.不同于攻击者选择发布区块时机类攻击，这类攻击的攻击者在藏匿区块后，丢弃部分或全部区块而不是选择时机发布这些区块.这类攻击以区块截留攻击与区块截留并分叉攻击为代表.该类攻击具有如下特点：攻击者加入矿池后实施攻击；攻击者攻击行为不存在失败的概率.

攻击者加入矿池后实施攻击：这类攻击主要针对采用工作量证明共识机制的区块链，且属于矿池间的攻击策略.图 3 展示了该类攻击的攻击场景.当工作量证明区块链系统中存在两个矿池时，将这两个矿池记作矿池 A 与矿池 B.在矿池中，矿工需要向矿池的管理员提交轻量级部分工作量证明(Partial Proof of Work)，管理员需要在矿工提交的轻量级的部分工作量证明中寻找符合区块链系统当前难度的完整工作量证明(Full Proof of Work).矿池依据矿工提交的轻量级工作量证明给予矿工奖励.在区块截留攻击中，矿池 A 向矿池 B 派遣拥有算力 $x_{A,B}$ 的攻击者，该攻击者向 B 矿池提交部分工作量证明以向矿池证明自身的工作量，同时丢弃自己找到的完整工作量证明.

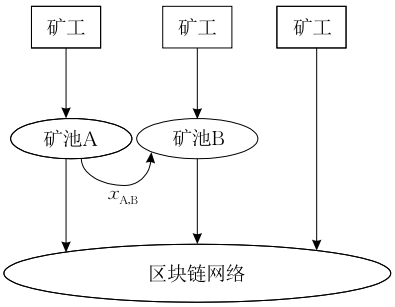

图 3 区块截留攻击场景

在区块截留攻击中，攻击者向矿池提交部分工作量证明并丢弃完整工作量证明[21-23].区块截留并分叉攻击[19]拓展了此类攻击中攻击者的行为.攻击者根据不同的场景选择性地丢弃区块，未被丢弃的区块可以被用于在区块链网络中制造分叉.该策略使攻击者与矿池 A 获得更高的收益.

攻击者攻击行为不存在失败的概率：在区块截留攻击与区块截留后分叉(Fork after withholding)攻击中，攻击者单次丢弃区块并获利的行为不存在失败的概率.在矿池 A 与矿池 A 派遣的攻击者内部存在着利益分配的问题.矿池 A 的收益来源于向区块链网络提交完整工作量证明后获得的区块奖励，攻击者的收益来源于向矿池 B 提交部分工作量证明后获得奖励.矿池 A 与矿池 A 派遣出的攻击者内部的利益分配的方式决定了他们各自获得的收益数量.但是，若将矿池 A 与该攻击者视作一个整体，该整体获得的收益较发动攻击前并没有减少，而矿池 B 获得的区块奖励则因攻击者丢弃完整工作量证明的行为有所下降.

(3)攻击者部署伪节点.区块链系统中，攻击者的行为不局限于选择时机发布区块或者丢弃区块.攻击者可以通过部署大量伪节点的方式对区块链系统网络层发起攻击.传统点对点网络中的女巫攻击同样可以作用于区块链网络中，此外，日蚀攻击和路由攻击同样是区块链系统中典型的攻击方式.该类攻击具有如下特点：单个攻击者可以部署大量恶意节点从而干扰其余节点甚至分裂区块链网络；攻击者部署伪节点的行为通常还伴随着其他攻击行为.

单个攻击者可以部署大量恶意节点从而干扰其

余节点甚至分裂区块链网络：攻击者部署伪节点类攻击首先出现于传统的点对点网络，并可以移用到区块链中. 例如在比特币中，比特币中的客户端节点与服务器节点维持与网络中其他 8 个节点的传出连接. 如果某个节点与 8 个传出连接节点中的任何一个节点失去连接，该节点会尝试用新节点替换. 默认情况下，比特币服务器节点最多可以接受 117 个传入连接.

采用女巫攻击的攻击者可以部署大量伪节点，并向诚实的节点提供虚假的信息以干扰诚实的节点. 日蚀攻击针对了比特币的网络传播机制，采用日蚀攻击的攻击者通过独占受害者的所有传入连接和传出连接的方式，将受害者与区块链网络中的其余节点隔离.

攻击者部署伪节点的行为通常还伴随着其他攻击行为：通过部署伪节点的方式干扰其他节点并非该类攻击的最终目标. 为了获得攻击收益攻击者还需要实施其他的攻击行为. 在日蚀攻击中，由于攻击者将受害者与区块链网络中的其余节点隔离开，因此攻击者可以轻易地对受害者实施零区块确认双重支付攻击(适用于快速支付)或 N 区块确认双重支付攻击[10,25]. 同时，攻击者可以选择不传播受害者发现的区块，从而提升攻击者在区块链网络中的相对收益. 此外，当攻击者与受害者拥有足够多的计算力时，攻击者可以迫使受害者参与攻击者在区块链网络中发起的自私挖矿攻击或 51%攻击[17].

(4) 攻击者直接制造分叉. 在区块链系统中，当攻击者拥有足够算力后，攻击者可以无需考虑攻击策略直接在区块链的任意位置创建分叉. 该类攻击需要攻击者拥有超过全网 50%的算力，攻击策略以 51%攻击与贿赂攻击为代表. 该类攻击具有的特点是：攻击者拥有优势算力.

攻击者拥有优势算力：仅当攻击者拥有优势算力时，才可以直接在区块链的任意位置制造分叉. 若攻击者的算力超过全网 50%的算力，攻击者可以直接发起 51%攻击；若攻击者的算力不足全网 50%时，攻击者可以发起贿赂攻击. 一种简单的贿赂攻击策略是在分叉链上加入贿赂其余算力的交易，仅当分叉链成为主链后，该交易才被确认.

3.2.2　依据攻击者目的分类

本节介绍依据攻击者目的的攻击分类标准. 在此分类标准下，区块链网络层、共识层、激励层中的攻击可以分为两类：(1) 攻击者目的为区块奖励；(2) 攻击者目的为双重支付.

(1) 目的为区块奖励. 在采用工作量证明共识机制的区块链中，发现新区块的矿工会获得一定数额的区块奖励. 目的为区块奖励的攻击通常发生于数字加密货币中，比特币等数字加密货币价值的提升刺激矿工们通过一定的策略获得更多的区块奖励. 该类攻击最典型的代表为自私挖矿攻击与区块截留攻击. 除此之外，这类攻击还包括固执挖矿攻击、优化自私挖矿攻击与区块截留并分叉攻击等. 这类攻击具有如下特点：① 攻击者短时期内提高自己的相对收益；② 攻击者需要通过长时间的攻击提升自己的绝对收益；③ 攻击者造成系统内有效算力的下降.

攻击者短时期内提高自己的相对收益：该类攻击的攻击者在短时期内是“非理性”的[7]. 攻击者的“非理性”体现在：通过该类攻击，攻击者在短期内的绝对收益不会提升. 自私挖矿攻击与区块截留攻击可以很好地解释“非理性”的含义.

采用自私挖矿攻击策略的攻击者通过选择性发布区块在区块链系统中制造分叉. 若攻击者制造的分叉链在与诚实矿工支持的主链的竞争中失败，那么攻击者最新发布的区块将被区块链系统视作孤块(Orphan block). 发现孤块的矿工耗费了大量计算力资源却无法获得区块奖励或仅获得较少的区块奖励. 在攻击者计算力不变的前提下，由于攻击者发布的区块有着最终成为孤块的几率，攻击者在短时期内的绝对收益将会下降. 通过蒙特卡洛算法进行数值仿真可以对采用自私挖矿策略的攻击者短期内的绝对收益做定量分析[7]. 仿真结果表明，攻击者在短期内的绝对收益将降低超过 30%. 但是，采用自私挖矿策略的攻击者在计算力超过一定阈值的情况下可以获得更高的相对收益[14]. 一些在自私挖矿攻击的基础上做出优化的攻击，例如固执挖矿攻击与优化自私挖矿攻击，短时间内同样致力于提升攻击者的相对收益.

区块截留攻击的攻击者每次攻击行为不存在失败的概率，因此不会产生孤块. 从绝对收益的角度来考虑，在短时期内区块截留攻击的攻击者的绝对收益不会下降. 从相对收益的角度考虑，在区块链系统中存在两个矿池的场景下，将两个矿池分别记作矿池 A 与矿池 B. 令 m_a，m_b 分别表示矿池 A 与矿池 B 计算力，m 表示区块链系统中的总计算力，$x_{a,b}$ 表示矿池 A 向矿池 B 派遣的攻击者的算力，则矿池 A 的

相对收益为 $r_a=\frac{m_a(m_b+x_{a,b})-x_{a,b}^2}{m_a(m-x_{a,b})(m_b+x_{a,b})}>\frac{m_a}{m}$[21]. 一些在区块截留攻击的基础上做出改进的攻击,例如区块截留后分叉攻击,短时间内同样致力于提升攻击者的相对收益 r_a.

攻击者需要通过长时间的攻击提升自己的绝对收益:目的为区块奖励的攻击者不会仅满足于提升自己的相对收益.以比特币为代表的数字加密货币拥有挖矿难度调整机制,这保证了攻击者可以通过长时间的攻击,将相对收益的提升转化为绝对收益的提升.

以比特币为例,每产生 2016 个有效区块后,区块链系统中的所有节点都会自动调整挖矿难度.产生 2016 个有效区块的期望时长为 20160 分钟(14 天).所有节点根据产生 2016 个有效区块的实际时长与期望时长的比值调整难度.当实际时长小于期望时长时,挖矿难度增加;反之,挖矿难度降低.以太坊与莱特币等采用工作量证明共识机制的数字加密货币难度调整机制与比特币类似.

对目的为区块奖励类攻击的攻击者来说,在短期内,攻击者绝对收益下降,相对收益上升;长期来看,区块链系统中挖矿难度将降低,攻击者的绝对收益将上升.

攻击者造成系统内有效算力的下降:该类攻击制造分叉链、藏匿区块的行为会导致工作量证明区块链系统内有效算力的下降.系统内有效算力的下降体现为区块链主链增长速度的下降.以自私挖矿攻击与区块截留攻击为例.

在自私挖矿攻击模型中,令 α 表示攻击者计算力在区块链网络中的占比.攻击者将导致区块链系统内有效算力下降 $\alpha-\frac{\alpha(\alpha-2\alpha^2)(2-\alpha)}{2\alpha^3-4\alpha^2+1}$;在区块截留攻击模型中,令 m 表示区块链系统中的总计算力,$x_{a,b}$ 表示矿池 A 向矿池 B 派遣的攻击者的算力.区块链系统内的有效算力将下降 $\frac{x_{a,b}}{m}$.

若在攻击中存在多个攻击者,那么攻击者们将会面临"囚徒困境"问题.因此,多个采用区块截留攻击策略的攻击者间存在博弈问题[21-23];多个自私挖矿攻击者间同样存在博弈[65-66].多个攻击者的存在将进一步削弱区块链系统中的有效算力.

(2)目的为双重支付.从数字加密货币诞生起,双重支付就是数字加密货币面临的最大威胁.尽管基于区块链的数字加密货币已采用一定机制以阻止双重支付行为,例如 N 区块确认机制,但是攻击者仍然可以通过一定方法实现双重支付.双重支付在基于工作量证明共识机制的区块链中相对容易实现,因为攻击者可以利用发起交易至交易被确认之间的时间间隔发起攻击.在快速支付场景中,由于交易被比特币系统确认需要一定的时间,因此受害者(卖家)通常在交易被确认之前就将一定价值的物品发送给攻击者.这导致攻击者可以轻易地实现双花攻击[10].目的为双重支付的攻击具有的最大特点是:攻击者可以通过不同手段实现双重支付.这些方法包括 51%攻击、贿赂攻击与日蚀攻击等.

攻击者可以通过不同手段实现双重支付:在交易被确认前尝试双重支付是该类攻击的攻击途径之一,但是该方式仅适用于快速支付场景.在快速支付场景中的双重支付攻击也被称为零确认双重支付攻击.

51%攻击也是实现双重支付的方法.在采用工作量证明共识机制的区块链中,攻击者可以在拥有超过全网 50%的算力后发起 51%攻击.目的为双重支付的攻击者可以在交易 T 被高度为 H 的区块确认后,在高度 $H-1$ 的区块后制造分叉链,并记录与交易 T 冲突的交易 T'.由于攻击者自身的计算力优势,包含交易 T 的区块将最终成为孤块,攻击者因此得以实现双重支付.

攻击者也可以通过贿赂攻击实现双重支付.贿赂攻击通过贿赂费引诱其它算力帮助攻击者实现双重支付[67-68].在贿赂攻击中,攻击者通过贿赂部分算力实体,使自身掌握的算力提升至超过全网算力 50%,从而以类似于 51%攻击的手段实施双重支付.

攻击者还可以通过日蚀攻击实现双重支付.攻击者成功将部分节点从区块链网络中分裂出去后,攻击者与被分裂网络中的节点做交易 T,并仅向被分裂的网络广播.同时,攻击者使用同一笔货币与未被分裂的网络中的节点做交易 T',并向未被分裂的网络广播这笔交易 T'.由于攻击者分裂了区块链网络,被分裂网络中的节点误以为交易 T 已被区块链网络确认;未被分裂网络中的节点由于没有接收到交易 T 的信息,从而认定交易 T' 合法.因此,这两笔交易都会被视作有效交易并最终被确认.

3.2.3 依据受攻击对象分类

本节介绍依据受攻击对象的攻击分类标准.在此分类标准下,区块链网络层、共识层、激励层中的攻击可以分为两类:(1)受攻击对象为全网所有节

点；(2)受攻击对象为部分节点.

(1)受攻击对象为全网所有节点. 当攻击者的行为令区块链网络的所有节点遭受损失时，受攻击的对象可以被认为是全网所有节点. 该类攻击包含：51%攻击、贿赂攻击、自私挖矿攻击与区块截留后分叉攻击等. 该类攻击的特点是：攻击者的收益与决策受区块链系统共识层与网络层参数影响.

攻击者的收益与决策受区块链系统共识层与网络层参数影响：区块链系统参数分为区块链共识层参数与区块链网络层参数. 区块链共识层参数包含：区块生成时间间隔，各矿工算力与各矿池算力等；区块链网络层参数包含：区块大小、节点位置、节点的传入节点数量、节点的传出节点数量与节点间信息传输机制等. 区块链网络层参数与区块链共识层参数共同决定了区块链系统中区块链分叉的概率. 记区块链系统中产生孤块的概率为 τ，每一个区块平均网络传播时延为 t_{BP}. 在比特币中，$\tau=0.41\%$，$t_{BP}=8.7$ s；在以太坊中，$\tau=6.8\%$，$t_{BP}=0.5-0.75$ s[7]. 自私挖矿攻击、贿赂攻击、51%攻击与区块截留后分叉攻击等攻击方式受到了参数 τ 和 t_{BP} 的影响.

自私挖矿攻击受到参数 τ 和 t_{BP} 的影响最大. 参数 τ 和 t_{BP} 直接决定了自私挖矿模型中攻击者对诚实矿工的影响率 γ，自私挖矿模型中攻击者的最低计算力阈值随 γ 的变化在 0 至 1/3 之间波动[14]. 对于自私挖矿攻击的优化方向之一是依据参数 τ 和 t_{BP} 调整攻击者的行为与决策. 优化自私挖矿攻击与固执挖矿攻击都是基于这一优化方向对自私挖矿攻击做改进. 区块截留后分叉攻击由于采纳了自私挖矿攻击的策略，也可以基于该优化方向做出改进.

当 51%攻击被攻击者用于实现双重支付时，区块链参数 τ 和 t_{BP} 也决定了攻击者在制造分叉链时获得的来自诚实矿工的支持. 攻击者获得的支持越多，实现双重支付这一目的所花费的时间越短.

当贿赂攻击被攻击者用于实现双重支付时，区块链参数 τ 和 t_{BP} 决定了攻击者实现双重支付所花费的时间. 攻击者还可以通过参数 τ 和 t_{BP} 调整贿赂金额与受贿计算力的大小.

(2)受攻击对象为部分节点. 当攻击者的行为仅令区块链网络中的部分节点遭受损失时，受攻击的对象可以被认为是部分节点. 该类攻击包含日蚀攻击、女巫攻击、路由攻击与区块截留攻击等. 该类攻击的特点是：攻击者的收益与决策不受区块链系统共识层参数的影响.

攻击者的收益与决策不受区块链系统共识层参数的影响：日蚀攻击、女巫攻击、路由攻击与区块截留攻击拥有着截然不同的攻击者行为与攻击者目的. 但是这些攻击均不受区块链共识层参数影响.

女巫攻击中伪节点的部署受网络层参数的影响. 但是由于伪节点不参与共识，因此区块链系统共识层的参数无法影响女巫攻击攻击者的决策与行为.

路由攻击通过 BGP(Border Gateway Protocol)劫持等方式，割裂部分区块链节点与区块链网络的联系. 路由攻击无需参与共识，因此不受区块链共识层参数影响.

日蚀攻击涉及到将区块链系统中部分节点与区块链网络分裂，因此采用日蚀攻击的攻击者在部署节点时需要考虑区块链系统网络层参数，例如节点位置分布、节点传入节点数量分布、节点传出节点数量分布与节点间信息传输机制等.

在区块截留攻击中，攻击者无需在区块链系统中制造分叉. 因此攻击者既不需要考虑区块链系统共识层参数，也不需要考虑区块链系统网络层参数. 值得一提的是，区块截留后分叉攻击作为区块截留攻击的优化，并不属于该类攻击.

3.3　合约层中攻击分类

区块链合约层中的攻击与区块链的机制有较密切的关系. 与区块链共识层、网络层、激励层中的攻击不同，区块链合约层中攻击的攻击者并非设计一定的攻击策略，而是利用区块链各层中机制的漏洞. 通过对现有合约层攻击案例的分析，可以将能够被合约层攻击利用的漏洞总结为以下几个类型：调用未知函数漏洞(Call to the unknown)、不包含 gas 发送漏洞(Gasless send)、无法获取异常漏洞(Exception disorders)、重入漏洞(Reentrancy)、合约不可更改漏洞(Immutable bugs)、调用栈深度溢出漏洞(Stack size limit)、交易依赖漏洞(Unpredictable state)以及破坏随机性漏洞(Generating randomness).

调用未知函数漏洞：智能合约代码中的错误有几率导致调用未知函数漏洞. 每个智能合约的函数通过函数名和参数类型来保证唯一性. 当合约因代码错误未能成功调用到函数时，将默认调用 fallback()函数.

不包含 gas 发送漏洞：当使用 send()函数发送

以太币到一个合约时，有可能会引发 out-of-gas 异常.若没有特别指定 gas 消耗的上限，调用 send()函数所消耗的 gas 默认上限是(2,300).若 send()函数未指定签名且 fallback()函数存在，send()函数将会调用 fallback()函数，从而引发 out-of-gas 异常.

无法获取异常漏洞：在以太坊中，智能合约执行到 out-of-gas、调用堆栈溢出与 throw 语句会导致异常抛出.当被调用的合约在执行时有异常抛出，该合约终止的同时返回 false.但是以太坊中智能合约使用的 solidity 语言没有一个统一的方法去处理异常.因此可能无法获取被调用的合约中的异常信息，这将最终导致无法获取异常漏洞.

重入漏洞：如果一个函数能够在先前的调用执行完成之前再次被调用，则该函数是可重入的，在智能合约中函数的重入会导致意外的执行结果[69].Solidity 语言不支持智能合约的并发执行，也没有提供任何可以暂停函数执行的中断，这导致了重入漏洞的产生.在智能合约中，如果某个外部可调用函数无法正确管理全局状态，则它容易受到重入攻击.尽管交易费和栈深度会限制递归调用的次数，但是这种违背开发者本意的重入调用依然会造成意外的执行结果.

合约不可更改漏洞：在智能合约的开发者创建一个智能合约之后，该智能合约便无法更改.智能合约在开发过程中，不可避免地存在着开发者未考虑到的语法漏洞或数据结构漏洞.这些不可避免的漏洞有可能被合约的使用者发现并加以利用.

调用栈深度溢出漏洞：当一个智能合约调用自己或调用其他智能合约时，交易的调用堆栈深度将增加 1.当调用堆栈达到上限 1024，合约再次调用自己或其他合约的行为将导致异常抛出.攻击者可以首先创造一个即将达到上限的调用堆栈，并调用受害者的智能合约从而导致异常的抛出.若受害者的智能合约无法正确地处理该异常，那么攻击者将得以利用调用栈深度溢出漏洞实施攻击.

交易依赖漏洞：智能合约状态的更新依赖于交易的执行顺序，当用户调用合约进行交易的时候，同时间其他用户的交易也可能会改变智能合约的状态.这有可能导致交易依赖漏洞.因为在区块链系统中，矿工可以任意选择被区块收录的交易并决定区块内的交易排列顺序，所以用户不能确定交易真正执行时合约的状态就是发起调用请求时合约的状态.攻击者可以利用智能合约中对交易顺序依赖的漏洞发起攻击[70-71].

破坏随机性漏洞：部分智能合约有时需要产生伪随机数，例如实现彩票功能的智能合约.一般来说，智能合约选定区块链中未来某个区块的时间戳或哈希值作为随机数的产生种子.攻击者可以基于随机数的产生原理进行攻击.拥有足够计算资源的攻击者可以操纵下一个区块，产生对自己有利的区块时间戳或哈希值[72].

上述漏洞中，调用未知函数漏洞、不包含 gas 发送漏洞、无法获取异常漏洞、重入漏洞、合约不可更改漏洞与调用栈深度溢出漏洞属于区块链合约层的智能合约数据结构漏洞与智能合约逻辑漏洞.交易依赖漏洞与破坏随机性漏洞属于非合约层漏洞.

区块链合约层中著名的攻击包括 The Dao 攻击、对 King of the Ether Throne 游戏的攻击、对 Fomo3D 游戏的攻击、对 Rubixi 智能合约的攻击和对 GovernMental 智能合约的攻击等.根据这些攻击利用的漏洞类型可以对它们进行分类并总结它们的特点.本章中提出合约层中攻击分类标准：依据攻击者利用的漏洞类型分类.

区块链合约层中的攻击可以根据攻击利用的漏洞类型分为两类：(1)攻击者仅利用合约层漏洞；(2)攻击者同时利用合约层漏洞与非合约层漏洞.

(1)攻击者利用合约层漏洞.该类攻击仅利用调用未知函数漏洞、不包含 gas 发送漏洞、无法获取异常漏洞、无法获取异常漏洞、合约不可更改漏洞与调用栈深度溢出漏洞等合约层漏洞.攻击的实施不涉及区块链的共识过程与区块的传播过程.这类攻击以 The Dao 攻击、对 King of the Ether Throne 游戏的攻击以及对 Rubici 合约的攻击为代表.这类攻击有以下特点：攻击者无需“挖矿”.

攻击者无需“挖矿”：攻击者仅通过合约层漏洞实现攻击，无需依赖于涉及到共识层、网络层与激励层的行为.通过三个例子可以很好地展现该特点.

2016 年 6 月的 The Dao 攻击造成了约 6000 万美元的损失.在该合约中的余额返还函数中，开发者选择先进行转账操作，再更新用户在此合约中的账户余额.由于没有正确管理全局状态，攻击者可以在余额状态更新前多次重入余额返还函数提取余额.The Dao 攻击利用了调用未知函数漏洞与重入漏洞.

King of the Ether Throne 是基于以太坊的游戏.其规则是玩家与当前的优胜者将一定数量的以

太币发送到某一智能合约中，智能合约将通过某一特定规则决定胜利者. 攻击者可以利用不包含 gas 发送漏洞确保自己总是优胜的一方.

Rubici 是以太坊中的智能合约. 合约的创建者试图通过该合约实现一个庞氏骗局. 合约的开发者曾将原名为 DynamicPyramid 的智能合约更名为 Rubici. 但是合约的开发者无意间保留了 DynamicPyramid() 构造函数. 合约拥有者在函数调用权限设定上的疏漏导致攻击者可以任意调用该构造函数并获取一定数额的以太币. 在该案例中，攻击者利用合约不可更改漏洞攻击 Rubici 合约.

从上述三个例子可以看出，在这类攻击中，攻击者仅需要寻找智能合约代码中的逻辑漏洞或数据结构漏洞. 攻击者无需参与到“挖矿”这一过程中，无需参与到认证区块合法性等一系列共识层、激励层与网络层行为中.

(2) 攻击者同时利用合约层漏洞与非合约层漏洞. 该类攻击除了利用合约层漏洞外还利用了交易依赖漏洞与破坏随机性漏洞等涉及共识层、网络层与激励层的漏洞. 这类攻击以对 Fomo3D 游戏的攻击与对 GovernMental 智能合约的攻击为代表. 这类攻击有以下特点：攻击者需要“挖矿”.

攻击者需要“挖矿”：这类攻击的攻击者除了需要利用合约层漏洞外，还需要参与区块链的共识过程与区块的传播过程. 通过两个例子可以阐明该特征.

攻击者对智能合约 Governmental 的攻击是该类攻击代表之一. 攻击者既可以利用合约层漏洞也可以利用非合约层漏洞对 Governmental 合约实施攻击. 当攻击者拥有一定算力并成功挖到新区块时，攻击者可以确保对 Governmental 合约实施的攻击不存在失败的概率. 作为矿工，攻击者可以任意选择收入区块的交易、任意排列区块内的交易顺序. 因此攻击者既可以在自己新挖到的区块中拒绝收录其余玩家在 Governmental 最终获胜的交易，也可以通过对交易的排序，使自己始终成为 Governmental 游戏的最终获胜者. 此时，攻击者利用了交易依赖漏洞. 此外，由于 Governmental 合约没有对抛出的异常做正确的处理，攻击者也可以利用合约层无法获取异常漏洞与调用栈深度溢出漏洞对该合约实施攻击.

攻击者对 Fomo3D 游戏的攻击是该类攻击的另一个代表. 攻击者同时利用合约层漏洞与非合约层漏洞对 Fomo3D 游戏实施攻击. Fomo3D 游戏发放奖励的操作由其合约中的 airdrop() 函数控制. airdrop() 函数中的“随机数”种子由该交易所在区块的区块信息和交易发起者地址计算得来. 当攻击者挖到下一区块时，可以轻易地预测 Fomo3D 游戏中的随机数并获取一定数量的奖励. 在攻击者对 Fomo3D 游戏的攻击中，攻击者同时利用了合约层合约不可更改漏洞与非合约层破坏随机性漏洞.

从上述两个例子可以看出，该类攻击的攻击者实施攻击时既需要利用合约层漏洞，也需要利用非合约层漏洞. 攻击者利用非合约层漏洞时需要参与到区块链共识层、激励层与网络层行为中，即攻击者需要“挖矿”.

3.4　应用层中攻击分类

区块链应用层中的攻击与区块链本身机制相关性较弱. 根据导致应用层攻击发生的因素可以将应用层中的攻击分为两类：(1) 密钥被泄露或被破解导致的攻击；(2) 区块链应用依赖的第三方机构导致的攻击.

(1) 密钥被泄露或被破解导致的攻击. 一旦数字加密货币用户掌握的密钥被泄露，该用户将遭受损失. 密钥被泄露可能由用户的疏忽或者攻击者采用的字典攻击(Dictionary Attack)[73] 导致. 同时，随着量子计算等计算技术的发展，区块链技术当前普遍采用的密码算法以及用户的密钥有被攻破的风险. 该类攻击可以出现于大多数涉及区块链技术的场景中，因此无明显特征.

(2) 区块链应用依赖的第三方机构导致的攻击. 在大多数情况下，用户依赖于第三方机构提供的区块链服务使用区块链应用. 这使得攻击者可以利用第三方机构开发应用层时留下的代码漏洞实施攻击. 以比特币为例，攻击者利用比特币交易所 Bitcoinica 的应用漏洞，盗取该交易所客户的比特币密钥. 该类攻击涉及到开发区块链应用的第三方机构，可以出现于大多数涉及区块链技术的场景中，因此同样无明显特征.

4　区块链中攻击的预防与检测

依据区块链中每类攻击的特征可以有针对性地提出每一类攻击的预防与检测措施. 表 2 总结了区块链中攻击的分类方法以及各类攻击的特征.

表 2 区块链中攻击分类方法以及各类攻击特征

攻击所在层次	攻击分类依据	攻击分类	现有的攻击方式	攻击特征
数据层	依据攻击者目的分类	目的是获取节点身份信息	利用区块链去匿名化技术实施的攻击	攻击者依赖于节点间的关联性
		目的是窃取链上隐私数据	利用隐私数据上链机制实施的攻击	攻击者可以获取权限以外的隐私数据
		目的是篡改链上数据	利用变色龙哈希函数实施的攻击	攻击者新生成的区块需要被多数节点接受
网络层、共识层与激励层	依据攻击者行为分类	选择时机发布区块	自私挖矿攻击、固执挖矿攻击与优化自私挖矿攻击等	行为依赖于特定状态机 在区块链中制造分叉 存在失败的概率
		丢弃区块	区块截留攻击与区块截留并分叉攻击等	加入矿池后实施攻击 不存在失败的概率
		部署伪节点	女巫攻击、日蚀攻击与路由攻击	分裂区块链网络 伴随其他攻击行为
		直接制造分叉	51%攻击与贿赂攻击	攻击者拥有优势算力
	依据攻击者目的分类	目的为区块奖励	自私挖矿攻击、区块截留攻击、固执挖矿攻击、优化自私挖矿攻击与区块截留并分叉攻击等	攻击者短时期内相对收益提升 攻击者短时期内绝对收益下降 造成区块链系统内有效算力的下降
		目的为双重支付	51%攻击、贿赂攻击与日蚀攻击等	可以通过不同方式实现双重支付
	依据受攻击对象分类	受攻击对象为全网所有节点	51%攻击、贿赂攻击、自私挖矿攻击与区块截留后分叉攻击等	攻击者受区块链系统共识层、网络层参数影响
		受攻击对象为部分节点	日蚀攻击、女巫攻击、路由攻击与区块截留攻击等	攻击者不受区块链系统共识层参数影响
合约层	依据攻击者利用的漏洞类型分类	仅利用合约层漏洞	The Dao 攻击、对 King of the Ether Throne 游戏的攻击与对 Rubici 合约的攻击等	攻击者无需参与区块链“挖矿”过程 攻击频率高
		同时利用合约层与非合约层漏洞	对 Fomo3D 游戏的攻击与对 GovernMental 智能合约的攻击等	攻击者需要参与区块链“挖矿”过程 攻击频率低
应用层	依据导致攻击发生的因素分类	密钥被泄露或被破解	字典攻击等	无明显特征
		第三方机构带来的漏洞	利用数字加密货币交易所漏洞的实施攻击等	无明显特征

4.1 数据层中攻击的预防与检测

数据层中的攻击可以依据攻击者的目的，分为目的是获取节点身份信息的攻击、目的是窃取链上隐私数据的攻击和目的是篡改链上数据的攻击. 表 3 总结了区块链数据层中攻击的预防与检测措施.

表 3 区块链数据层中攻击的预防与检测措施

攻击分类依据	攻击分类	预防检测措施
依据攻击者目的分类	目的是获取节点身份信息	利用环签名技术、零知识证明技术与混币技术等技术预防攻击
	目的是窃取链上隐私数据	通过规定节点权限、设计支持安全多方计算的智能合约等方式预防攻击
	目的是篡改链上数据	诚实节点通过比较被修改区块的高度与当前区块链的高度检测攻击

攻击者目的是获取节点身份信息：该类攻击的特征是：依赖于区块链节点间的关联性. 通过隐藏区块链节点与交易间的关联性可以预防该类攻击. 目前已有部分基于区块链的数字加密货币利用零知识证明与环签名等技术隐藏节点间的关联性. 门罗币环签名技术将交易双方的真实身份隐藏. 零币(Zerocoin)利用零知识证明技术隐藏了用户真实身份以及用户节点间的关联性. 大零币(Zerocash) 在零币的基础上，进一步隐藏了交易双方的交易金额，更好地保护了用户节点间的关联性. 混币技术[74]将多笔交易凑成一笔交易执行，同样可以隐藏用户节点与用户节点、用户节点与交易之间的关联性. 达世币(Dashcoin)应用了混币技术. 环签名技术、零知识证明技术与混币技术增加了验证交易或执行交易的计算开销，隐藏了区块链节点与节点间、节点与交易间的关联性.

攻击者目的是窃取链上隐私数据：该类攻击的特征是：攻击者可以获取权限以外的隐私数据. 通过设定区块链各节点的权限以及取消链下计算部分可以预防该类攻击. 以基于公链的链上-链下隐私数据

共享模式[58]为例，公链未规定各节点的权限导致攻击者得以伪装成诚实节点在链下计算部分获取隐私数据.基于公链开发支持链上安全计算、保护隐私数据的智能合约可以预防该类攻击[75].采用联盟链也可以作为该类攻击的预防措施，联盟链可以更好地规定各节点的权限，并保证被授权节点是可信的.联盟链也可以将链下安全多方计算[76]部分集成至智能合约中[77].基于公链开发支持链上安全计算的智能合约适用于大部分应用场景，但是也存在着计算开销较大的问题[78-79].基于联盟链开发支持链上安全计算的智能合约可以更好地规定节点权限且参与多方安全计算的组织数量较小，但是联盟链无法适用于所有的应用场景.

攻击者目的是篡改链上数据：该类攻击的特点是：攻击者新生成的区块需要被多数节点接受.通过校验被修改区块的高度可以检测该类攻击.利用变色龙哈希函数修改区块的方法可以轻易生成被篡改的区块，却难以使该区块被多数节点接受(即使该区块拥有合法的区块头信息).区块链网络中的诚实节点可以通过比较被修改区块的高度与当前区块链最长链的高度检测该类攻击.通过校验被修改区块的区块高度预防该类攻击具有检测开销小、检测方便的优点.

4.2　网络层、共识层、激励层中攻击的预防与检测

区块链网络层、共识层、激励层中的攻击可以依据多个分类标准实现分类.多个分类标准可以从多个角度展现攻击的特点，并根据攻击的特点提出针对攻击的预防、检测措施.表 4 总结了区块链网络层、共识层、激励层中攻击的预防与检测措施.

表 4　区块网络层、共识层、激励层中攻击的预防与检测措施

攻击分类依据	攻击分类	预防检测措施
依据攻击者行为分类	选择时机发布区块	通过分析区块链的分叉率检测攻击
	丢弃区块	通过改良矿池内部分配机制预防攻击
	部署伪节点	通过部署可靠的中继节点以及引入白名单机制预防攻击
	直接制造分叉	通过阻止矿池吸纳过多算力的方式预防攻击
依据攻击者目的分类	目的为区块奖励	通过监控区块链系统内的有效算力检测攻击
	目的为双重支付	通过 N 区块后确认等方式预防攻击
依据受攻击对象分类	受攻击对象为全网所有节点	通过采用合理的共识层、网络层参数预防攻击
	受攻击对象为部分节点	通过增加节点间的连接度、完善节点间信息传输机制、优化全节点位置分布预防攻击

4.2.1　依据攻击者行为分类

网络层、共识层、激励层中的攻击可以依据攻击者行为，分为攻击者选择时机发布区块、攻击者丢弃区块、攻击者部署伪节点以及攻击者直接制造分叉四类.

攻击者选择时机发布区块：该类攻击特征是：攻击者行为取决于攻击者状态、攻击者制造分叉、攻击存在失败概率.通过统计区块链网络一段时间内的分叉率可以检测该类攻击.受网络传播时延的影响，区块链网络中存在着自然产生的分叉.产生自然分叉的概率可以通过蒙特卡洛方法从数值上预测[80].在实际中比特币产生自然分叉的概率为 0.41%，以太坊产生自然分叉的概率是 6.8%[7].比特币与以太坊采用的区块参数的不同导致了他们产生了不同的自然分叉概率.当区块链中各参数已知时，区块链诚实节点可以根据当前参数预测区块链产生自然分叉的概率.在该类攻击中，攻击者频繁地在区块链网络中制造分叉，这导致区块链网络的分叉率显著高于诚实节点预测值.诚实节点因此可以检测到攻击的发生.通过检测区块链网络的分叉率检测该类攻击的优点是：检测开销小、任何节点都可以进行检测.

攻击者丢弃区块：该类攻击特征是：攻击者加入矿池后丢弃区块、攻击不存在失败概率.通过改变矿池内部分配机制等措施可以预防该类攻击.改进矿池内部分配机制可以有效地阻止攻击者加入矿池后丢弃区块的行为[81-82].在不改变矿池内部分配机制的前提下，矿池向区块链网络做出承诺方案(Commitment scheme)同样可以阻止攻击者丢弃区块的行为[83].通过改进矿池内部分配机制预防该类攻击具有实现简单的优点，但是该方法无法从根源上杜绝该类攻击.引入承诺方案的方法可以彻底防止攻击者故意丢弃区块的行为，但是引入承诺方案需要改变矿工挖矿的机制，其实现较为复杂.

攻击者部署伪节点：该类攻击特征是：分裂区块链网络并伴随其他攻击行为.部署一定数量的可靠的中继节点可以预防该类攻击.部署可靠的中继节点可以有效地阻止攻击者通过部署伪节点的方式干扰区块链网络[84-85].引入白名单机制并仅信任特定的节点是预防该类攻击的另一种措施[25].部署可靠的中继节点与引入白名单机制可以降低区块链网络

的网络传播时延并预防该类攻击，但是上述两种方法可能导致区块链系统的中心化.

攻击者直接制造分叉：该类攻击特征是：攻击者拥有优势算力.通过一定的机制阻止攻击者控制过多算力可以预防该类攻击.Eyal 等研究者在当前工作量证明共识机制的基础上，提出了两阶段工作量证明以阻止矿池吸纳过多算力.两阶段工作量证明共识机制可以有效地预防该类攻击，但是实现两阶段工作量证明需要改变区块链网络的挖矿方式.

4.2.2 依据攻击者目的分类

网络层、共识层、激励层中的攻击可以依据攻击者目的分为目的是区块奖励、目的是双重支付两类.

目的是区块奖励：该类攻击的特征是：攻击者短时期内相对收益提升、攻击者短时期内绝对收益下降、造成区块链系统内有效算力的下降.通过监测区块链网络内的有效算力可以检测该类攻击.该类攻击以自私挖矿攻击[14]和区块截留攻击[21]为代表.在自私挖矿攻击中，攻击者制造的分叉与孤块[7]导致区块链系统内有效算力的下降；在区块截留攻击中，攻击者丢弃的区块导致区块链系统内有效算力的下降.对区块链系统内有效算力的监测可以检测攻击，比特币等数字加密货币的有效算力可以通过挖矿难度与主链增长速度计算得出.监测区块链系统内的有效算力的优点是检测开销小、任何节点都可以进行检测.但是该方法仅对该类攻击提供了检测措施，却无法制止攻击者的攻击行为.

目的是双重支付：该类攻击的特征是：实现方法多.该特征导致区块链系统中单个诚实节点很难通过特定的策略阻止该类攻击.因此，区块链系统中的所有节点都需要遵守一定的协议以预防该类攻击.例如，比特币用户通过 N 区块后确认交易的方法预防该类攻击.比特币 N 区块后确认交易的机制显著降低了目的为双重支付的攻击出现的概率，但是也导致交易确认时间长等一系列问题.

4.2.3 依据受攻击对象分类

网络层、共识层、激励层中的攻击可以依据受攻击对象分为受攻击对象为全网所有节点与受攻击对象为部分节点两类.

受攻击对象为全网所有节点：该类攻击的特征是：攻击者受区块链系统共识层、网络层参数影响.设定合理的共识层、网络层参数可以预防该类攻击.这些参数包括区块大小、生成区块的时间间隔、节点间的连接度等.合理的共识层、网络层参数可以有效预防自私挖矿攻击、固执挖矿攻击与双花攻击[7].以自私挖矿攻击为例，减小区块大小并增加节点间的连接度可以降低受攻击者影响的诚实矿工的比例，从而增加自私挖矿攻击者单次攻击行为失败的概率.减小区块大小等方法可以预防该类攻击，但同时也导致区块链吞吐率的下降.

受攻击对象为部分节点：该类攻击的特征是：攻击者仅受网络层参数影响.根据该特征，可以通过增加节点间的连接度、完善节点间信息传输机制、优化全节点位置分布等措施预防该类攻击.举例来说，通过部署可靠中继节点预防路由攻击[84-85]的措施，涉及了合理地部署全节点和增加用户节点与全节点间的连接度；通过引入白名单机制预防日蚀攻击[25]的措施，涉及了完善节点间信息传输机制.增加节点间的连接度、完善节点间信息传输机制、优化全节点位置分布等方法可以有效地阻止攻击者分裂区块链网络，但是实现上述方法的开销较大.

4.3 合约层中攻击的预防与检测

合约层中的攻击可以依据攻击者利用的漏洞类型，分为仅利用合约层漏洞的攻击与同时利用合约层漏洞和非合约层漏洞的攻击.表 5 总结了区块链合约层中攻击的预防与检测措施.

表 5 区块链合约层中攻击的预防与检测措施

攻击分类依据	攻击分类	预防检测措施
依据攻击者利用的漏洞类型	仅利用合约层漏洞的攻击	通过智能合约形式化验证的工具预防攻击 通过合理地使用区块链去匿名化工具检测攻击
	同时利用合约层漏洞和非合约层漏洞的攻击	通过智能合约形式化验证的工具预防攻击 通过合理地使用区块链去匿名化工具检测攻击

在同时利用合约层漏洞和非合约层漏洞的攻击中，虽然攻击者利用了非合约层漏洞，但是攻击者在共识层中挖到的区块是合法的区块.区块链诚实节点难以通过共识层中的措施预防或检测该类攻击.因此，无论是利用合约层漏洞的攻击还是同时利用合约层漏洞和非合约层漏洞的攻击，其预防与检测措施都是基于合约层的.

智能合约的开发者可以通过一定的方式避免合约层漏洞的出现.例如，智能合约中的 transfer() 函数相较于 send() 函数增加了异常抛出，因此使用

transfer()函数可以一定程度上避免合约层不包含gas发送漏洞.开发者们还可以通过判断输入数据是否在一定区间内的方式避免智能合约中的语法漏洞与数据结构漏洞.

除此之外,智能合约的开发者与使用者还可以总结智能合约中已知的漏洞并开发智能合约形式化验证工具以预防该类攻击.Pierrot等研究者[72]提出了智能合约的形式验证框架,该框架使用一种针对程序验证的函数式语言F*,将使用Solidity语言编写的合约编译成为F*的程序,或者将以太坊虚拟机字节码程序(EVM Bytecode)反编译成为F*的程序.Luu等研究者[27]提出了名为OYENTE的符号执行工具以检测智能合约的漏洞.OYENTE检测了19366个现有智能合约并在8833条智能合约中发现潜在的漏洞,其中包含著名的The DAO漏洞[8].Wohrer等研究者与Grossman等研究者[86-87]构建了针对特定领域的自动验证器并建立了专用于识别重入问题的智能合约检测工具.Tsankov等研究者[28]提出了名为SECURIFY的轻量级、可扩展的以太坊智能合约检测器.Park等研究者[88]提出的以太坊虚拟机检测器以及Bartoletti等研究者[89]提出的BitML都能起到检测或预防智能合约漏洞的功能.目前,智能合约安全性分析工具Oyente、VaaS、Securify与Smartdec都已经投入使用.

合理地使用区块链去匿名化工具有助于检测攻击者.Chen等研究者[90]构建了以太坊以太币流通图、智能合约创建图与智能合约调用图.构建以太坊网络的图分析可以检测创建与调用恶意智能合约的节点.

智能合约形式化验证工具可以高效地检测出智能合约中特定类型的漏洞或已出现过的漏洞,却难以检测出未知的漏洞.区块链去匿名化工具可以挖掘出攻击者之间的潜在联系,但是该方法可能威胁到区块链系统中诚实节点的隐私性.

4.4　应用层中攻击的预防与检测

应用层中的攻击可以依据导致攻击发生的因素分为密钥被泄露或被破解导致的攻击与第三方机构漏洞导致的攻击.表6总结了区块链应用层中攻击的预防与检测措施.

表6　区块链应用层中攻击的预防与检测措施

攻击分类依据	攻击分类	预防检测措施
依据导致攻击发生的因素	密钥被泄露或被破解导致的攻击	通过托管密钥、采用门限签名技术预防攻击
	第三方机构漏洞导致的攻击	通过增强应用层软件保护预防攻击

密钥被泄露或被破解导致的攻击:区块链的用户可以利用第三方机构的服务器托管密钥以保证其密钥的安全性.但是该措施一定程度上牺牲了区块链的去中心化特性.门限签名技术也能够对密钥提供一定的保护.

第三方机构漏洞导致的攻击:第三方机构开发区块链应用带来的漏洞难以被完全消除.第三方开发者在开发应用层的过程中应增强应用层软件保护.

5　区块链攻击问题的未来研究重点

5.1　对攻击策略的研究

2008年比特币诞生之后,研究者们提出大量区块链中攻击方式.这其中51%攻击、自私挖矿攻击已经出现在现实的案例中.对日蚀攻击的研究也促使以太坊开发者发布Geth v1.8.1补丁修复网络.由此可见,对区块链中攻击的研究是具有重大意义的.在后续的研究中,研究者既可以尝试改进及组合现有的攻击以形成新的攻击策略,也可以根据新出现的区块链机制提出全新攻击方式.

5.2　对智能合约安全性分析工具的研究

以太坊智能合约使用的Solidity语言尚未完全成熟,其中的安全性漏洞可以直接被攻击者利用从而威胁到智能合约的安全性.目前,已有一些针对智能合约形式化验证的工具出现,例如Oyente、VaaS、Securify与Smartdec等.但是现有的形式化验证和程序分析工具多是针对已知漏洞的检测和验证.对智能合约安全性分析工具的后续研究也应着眼于在智能合约代码中寻找潜在的、未知的漏洞.

5.3　对区块链去匿名化的研究

对区块链去匿名化的研究可被视作一把双刃剑.在一方面,利用区块链去匿名化的研究成果,攻击者可以通过挖掘区块链用户节点间的关联性实施攻击;在另一方面,区块链去匿名化的研究可以找出区块链中部署或调用恶意智能合约的节点.在对区块链去匿名化的后续研究中,如何权衡区块链中的监管问题与区块链用户隐私问题是值得研究的.未来,区块链去匿名化研究既应做到检测区块链网络中的恶意节点,也应保证不侵犯诚实节点的隐私.

6 总 结

区块链中的攻击方式之间既存在着差异性,也存在着一定的关联性.独立地讨论每一种攻击方式不仅不利于挖掘攻击之间的关联性,也不利于通过对比得出攻击之间的差异性.本文提出了全新的区块链攻击分类方法.本文提出的分类方法在保留区块链中不同攻击方式间关联性的同时,也展现了攻击方式之间的差异性.本文首先将区块链中的攻击划分为四大类:数据层中的攻击、网络层、共识层、激励层中的攻击、合约层中的攻击与应用层中的攻击.数据层中的攻击可以依据攻击者的目的进一步分类;网络层、共识层、激励层中的攻击可以依据攻击者的行为、攻击者的目的与受攻击对象进一步分类;合约层中攻击可以依据攻击者利用的漏洞类型进一步分类;应用层中的攻击可以依据导致攻击发生的因素进一步分类.本文在提出攻击分类方法的同时,还详细总结了各类型攻击的特征.根据各类型攻击的特征,本文提出了对各类型攻击的预防措施与检测措施.对区块链中攻击方式及其预防检测措施的研究既有助于完善区块链底层技术,也能够促进基于区块链技术的应用的发展.

说 明:本文作者阮娜于 2018 年 CCF 区块链大会做邀请主题报告,本文基于该邀请主题报告整理.

参 考 文 献

[1] Kim D J, Ferrin D L, Rao H R. A trust-based consumer decision-making model in electronic commerce: The role of trust, perceived risk, and their antecedents. Decision Support Systems, 2008, 44(2): 544-564

[2] Nakamoto S. Bitcoin: A peer-to-peer electronic cash system. 2008

[3] Ministry of Industry and Information Technology. China Blockchain Technology and Application Development White Paper, 2016(in Chinese)
(工信部. 中国区块链技术和应用发展白皮书, 2016)

[4] Lee C. Litecoin-open source P2P digital currency. White Paper, 2011

[5] Buterin V. A next-generation smart contract and decentralized application platform. White Paper, 2014

[6] Cachin C. Architecture of the hyperledger blockchain fabric//Proceedings of the Workshop on Distributed Cryptocurrencies and Consensus Ledgers. Chicago, USA, 2016: 310: 4

[7] Gervais A, Karame G O, Wüst K, et al. On the security and performance of proof of work blockchains//Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security. Vienna, Austria, 2016: 3-16

[8] Mehar M I, Shier C L, Giambattista A, et al. Understanding a revolutionary and flawed grand experiment in blockchain: The DAO attack. Journal of Cases on Information Technology, 2019, 21(1): 19-32

[9] Miller A, Kosba A, Katz J, et al. Nonoutsourceable scratch-off puzzles to discourage Bitcoin mining coalitions//Proceedings of the 2015 ACM SIGSAC Conference on Computer and Communications Security. Denver, USA, 2015: 680-691

[10] Karame G O, Androulaki E, Capkun S. Double-spending fast payments in Bitcoin//Proceedings of the 2012 ACM Conference on Computer and Communications Security. Raleigh, USA, 2012: 906-917

[11] Rosenfeld M. Analysis of hashrate-based double spending. arXiv preprint arXiv:1402.2009, 2014

[12] Karame G O, Androulaki E, Roeschlin M, et al. Misbehavior in Bitcoin: A study of double-spending and accountability. ACM Transactions on Information and System Security, 2015, 18(1): 1-32

[13] Möser M, Böhme R, Breuker D. Towards risk scoring of Bitcoin transactions//Proceedings of the International Conference on Financial Cryptography and Data Security. Christ Church, Barbados, 2014: 16-32

[14] Eyal I, Sirer E G. Majority is not enough: Bitcoin mining is vulnerable. Communications of the ACM, 2018, 61(7): 95-102

[15] Göbel J, Keeler H P, Krzesinski A E, et al. Bitcoin blockchain dynamics: The selfish-mine strategy in the presence of propagation delay. Performance Evaluation, 2016, 104: 23-41

[16] Heilman E. One weird trick to stop selfish miners: Fresh Bitcoins, a solution for the honest miner//Proceedings of the International Conference on Financial Cryptography and Data Security. Christ Church, Barbados, 2014: 161-162

[17] Nayak K, Kumar S, Miller A, et al. Stubborn mining: Generalizing selfish mining and combining with an eclipse attack//Proceedings of the 2016 IEEE European Symposium on Security and Privacy. Saarbrücken, Genmany, 2016: 305-320

[18] Sapirshtein A, Sompolinsky Y, Zohar A. Optimal selfish mining strategies in Bitcoin//Proceedings of the International Conference on Financial Cryptography and Data Security. Christ Church, Barbados, 2016: 515-532

[19] Kwon Y, Kim D, Son Y, et al. Be selfish and avoid dilemmas: Fork after withholding (faw) attacks on Bitcoin//Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security. Dallas, USA, 2017: 195-209

[20] Carlsten M, Kalodner H, Weinberg S M, et al. On the instability of Bitcoin without the block reward//Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security. Vienna, Austria, 2016: 154-167

[21] Eyal I. The miner's dilemma//Proceedings of the 2015 IEEE Symposium on Security and Privacy. San Jose, USA, 2015: 89-103

[22] Courtois N T, Bahack L. On subversive miner strategies and block withholding attack in Bitcoin digital currency. arXiv preprint arXiv:1402.1718, 2014

[23] Laszka A, Johnson B, Grossklags J. When Bitcoin mining pools run dry//Proceedings of the International Conference on Financial Cryptoy and Data Security. San Juan, Puerto Rico, 2015: 63-77

[24] Biryukov A, Pustogarov I. Bitcoin over Tor isn't a good idea//Proceedings of the 2015 IEEE Symposium on Security and Privacy. San Jose, USA, 2015: 122-134

[25] Heilman E, Kendler A, Zohar A, et al. Eclipse attacks on Bitcoin's peer-to-peer network//Proceedings of the 24th USENIX Security Symposium. Washington, USA, 2015: 129-144

[26] Juels A, Kosba A, Shi E. The ring of gyges: Investigating the future of criminal smart contracts//Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security. Vienna, Austria, 2016: 283-295

[27] Luu L, Chu D H, Olickel H, et al. Making smart contracts smarter//Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security. Vienna, Austria, 2016: 254-269

[28] Tsankov P, Dan A, Drachsler-Cohen D, et al. Securify: Practical security analysis of smart contracts//Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security. Toronto, Canada, 2018: 67-82

[29] Bonneau J, Miller A, Clark J, et al. SoK: Research perspectives and challenges for Bitcoin and cryptocurrencies//Proceedings of the 2015 IEEE Symposium on Security and Privacy. San Jose, USA, 2015: 104-121

[30] Tschorsch F, Scheuermann B. Bitcoin and beyond: A technical survey on decentralized digital currencies. IEEE Communications Surveys and Tutorials, 2016, 18(3): 2084-2123

[31] Yuan Yong, Wang Fei-Yue. Blockchain: The state of the art and future trends of blockchain. Acta Automatica Sinica, 2016, 42(4): 481-494(in Chinese)
(袁勇，王飞跃. 区块链技术发展现状与展望. 自动化学报, 2016, 42(4): 481-494)

[32] He Pu, Yu Ge, Zhang Yan-Feng, et al. Survey on blockchain technology and its application prospect. Computer Science, 2017, 44(4): 1-7(in Chinese)
(何蒲，于戈，张岩峰等. 区块链技术与应用前瞻综述. 计算机科学, 2017, 44(4): 1-7)

[33] Shao Qi-Feng, Jin Che-Qing, Zhang Zhao, et al. Blockchain: The structure and progress. Chinese Journal of Computers, 2018, 41(5): 969-988(in Chinese)
(邵奇峰，金澈清，张召等. 区块链技术：架构及进展. 计算机学报, 2018, 41(5): 969-988)

[34] Atzei N, Bartoletti M, Cimoli T. A survey of attacks on Ethereum smart contracts (SoK)//Proceedings of the International Conference on Principles of Security and Trust. Uppsala, Sweden, 2017: 164-186

[35] Lin I C, Liao T C. A survey of Blockchain security issues and challenges. International Journal of Network Security, 2017, 19(5): 653-659

[36] Li X, Jiang P, Chen T, et al. A survey on the security of blockchain systems. Future Generation Computer Systems, 2017, http://dx.doi.org/10.1016/j.future.2017.08.020

[37] Han Xuan, Yuan Yong, Wang Fei-Yue. The research status and future trends of blockchain security issues. Acta Automatica Sinica, 2019, 45(1): 206-225(in Chinese)
(韩璇，袁勇，王飞跃. 区块链安全问题：研究现状与展望. 自动化学报, 2019, 45(1): 206-225)

[38] Haber S, Stornetta W S. How to time-stamp a digital document//Proceedings of the Conference on the Theory and Application of Cryptography. Santa Barbara, USA, 1990: 437-455

[39] Bayer D, Haber S, Stornetta W S. Improving the efficiency and reliability of digital time-stamping//Proceedings of the Sequences II. New York, USA, 1993: 329-334

[40] Massias H, Avila X S, Quisquater J J. Design of a secure timestamping service with minimal trust requirement//Proceedings of the 20th Symposium on Information Theory in the Benelux. Haasrode, Belgium, 1999

[41] Merkle R C. A digital signature based on a conventional encryption function//Proceedings of the Conference on the Theory and Application of Cryptographic Techniques. Berlin, Heidelberg, 1987: 369-378

[42] Merkle R C. Protocols for public key cryptosystems//Proceedings of the 1980 IEEE Symposium on Security and Privacy. Oakland, USA, 1980: 122-122

[43] Jakobsson M, Leighton T, Micali S, et al. Fractal Merkle tree representation and traversal//Proceedings of the Cryptographers' Track at the RSA Conference. San Francisco, USA, 2003: 314-326

[44] Carter J L, Wegman M N. Universal classes of hash functions. Journal of Computer and System Sciences, 1979, 18(2): 143-154

[45] Damgård I B. A design principle for hash functions//Proceedings of the Conference on the Theory and Application of Cryptology. New York, USA, 1989: 416-427

[46] King S, Nadal S. PPCoin: Peer-to-peer crypto-currency with proof-of-stake. White Paper, 2012

[47] Castro M, Liskov B. Practical Byzantine fault tolerance//Proceedings of the 3rd USENIX Symposium on Operating Systems Design and Implementation, New Orleans, USA, 1999, 99: 173-186

[48] Kiayias A, Russell A, David B, et al. Ouroboros: A provably secure proof-of-stake blockchain protocol//Proceedings of the Annual International Cryptology Conference. Santa Barbara, USA, 2017: 357-388

[49] Schwartz D, Youngs N, Britto A. The ripple protocol consensus algorithm. Ripple Labs Inc White Paper, 2014

[50] Rosenfeld M. Analysis of Bitcoin pooled mining reward systems. arXiv preprint arXiv:1112.4980, 2011

[51] Reid F, Harrigan M. An analysis of anonymity in the Bitcoin system//Yaniv A, Yuval E Armin C, Nadav A, Alex P eds. Security and Privacy in Social Networks. New York: Springer-Verlag, 2013: 197-223

[52] Meiklejohn S, Pomarole M, Jordan G, et al. A fistful of Bitcoins: Characterizing payments among men with no names //Proceedings of the 2013 Conference on Internet Measurement Conference. Barcelona, Spain, 2013: 127-140

[53] Ron D, Shamir A. Quantitative analysis of the full Bitcoin transaction graph//Proceedings of the International Conference on Financial Cryptography and Data Security. Berlin, Heidelberg, 2013: 6-24

[54] Maesa D D F, Marino A, Ricci L. Uncovering the Bitcoin blockchain: An analysis of the full users graph//Proceedings of the 2016 IEEE International Conference on Data Science and Advanced Analytics. Montreal, Canada, 2016: 537-546

[55] Lee S, Yoon C, Kang H, et al. Cybercriminal Minds: An investigative study of cryptocurrency abuses in the Dark Web// Proceedings of the Network and Distributed Systems Security Symposium 2019. San Diego, USA, 2019

[56] Moser M, Soska K, Heilman E, et al. An empirical analysis of traceability in the monero blockchain//Proceedings of the Privacy Enhancing Technologies Symposium. Barcelona, Spain, 2018: 143-163

[57] Fanti G, Viswanath P. Deanonymization in the Bitcoin P2P network//Proceedings of the Advances in Neural Information Processing Systems. Los Angeles, USA, 2017: 1364-1373

[58] Kang J, Yu R, Huang X, et al. Blockchain for secure and efficient data sharing in vehicular edge computing and networks. IEEE Internet of Things Journal, 2018, 6(3): 4660-4670

[59] Alvarado C, Devadoss N, Rivens R, et al. It's your data: A Blockchain solution to Facebook's data stewardship problem. SMU Data Science Review, 2018, 1(4): 2

[60] Azaria A, Ekblaw A, Vieira T, et al. MedRec: Using blockchain for medical data access and permission management //Proceedings of the 2nd International Conference on Open and Big Data. Vienna, Austria, 2016: 25-30

[61] Zyskind G, Nathan O. Decentralizing privacy: Using blockchain to protect personal data//Proceedings of the 2015 IEEE Security and Privacy Workshops. San Jose, USA, 2015: 180-184

[62] Krawczyk H, Rabin T. Chameleon signatures//Proceedings of the Network and Distributed System Security Symposium. San Diego, USA, 2000:143-154

[63] Derler D, Samelin K, Slamanig D, et al. Fine-grained and controlled rewriting in blockchains: Chameleon-hashing gone attribute-based. IACR Cryptology ePrint Archive, 2019, 2019: 406

[64] Ateniese G, Magri B, Venturi D, et al. Redactable blockchain—or—rewriting history in Bitcoin and friends// Proceedings of the 2017 IEEE European Symposium on Security and Privacy. Paris, France, 2017: 111-126

[65] Liu H, Ruan N, Du R, et al. On the strategy and behavior of Bitcoin mining with N-attackers//Proceedings of the 2018 on Asia Conference on Computer and Communications Security. Incheon, South Korea, 2018: 357-368

[66] Bai Q, Zhou X, Wang X, et al. A deep dive into blockchain selfish mining//Proceedings of the 2019 IEEE International Conference on Communications. Shanghai, China, 2019: 1-6

[67] Bonneau J. Why buy when you can rent//Proceedings of the International Conference on Financial Cryptography and Data Security. Christ Church, Barbados, 2016: 19-26

[68] Liao K, Katz J. Incentivizing blockchain forks via whale transactions//Proceedings of the International Conference on Financial Cryptography and Data Security. Sliema, Malta, 2017: 264-279

[69] Liu C, Liu H, Cao Z, et al. ReGuard: Finding reentrancy bugs in smart contracts//Proceedings of the 40th International Conference on Software Engineering: Companion. Hawaii, USA, 2018: 65-68

[70] Decker C, Wattenhofer R. Bitcoin transaction malleability and MtGox//Proceedings of the European Symposium on Research in Computer Security. Wroclaw, Poland, 2014: 313-326

[71] Kosba A, Miller A, Shi E, et al. Hawk: The blockchain model of cryptography and privacy-preserving smart contracts //Proceedings of the 2016 IEEE Symposium on Security and Privacy. San Jose, USA, 2016: 839-858

[72] Pierrot C, Wesolowski B. Malleability of the blockchain's entropy. Cryptography and Communications, 2018, 10(1): 211-233

[73] Jablon D P. Extended password key exchange protocols immune to dictionary attack//Proceedings of the IEEE 6th Workshop on Enabling Technologies: Infrastructure for Collaborative Enterprises. Massachusetts, USA, 1997: 248-255

[74] Ruffing T, Moreno-Sanchez P, Kate A. CoinShuffle: Practical decentralized coin mixing for Bitcoin//Proceedings of the European Symposium on Research in Computer Security. Wroclaw, Poland, 2014: 345-364

[75] Steffen S, Bichsel B, Gersbach M, et al. zkay: Specifying and enforcing data privacy in smart contracts//Proceedings of the 2019 ACM SIGSAC Conference on Computer and Communications Security. London, UK, 2019: 1759-1776

[76] Yao A C. Protocols for secure computation//Proceedings of the 23rd Annual Symposium on Foundations of Computer Science. Washington, USA, 1982: 160-164

[77] Benhamouda F, Halevi S, Halevi T T. Supporting private data on Hyperledger Fabric with secure multiparty computation. IBM Journal of Research and Development, 2019, 63(2/3): 1-8

[78] Wang X, Ranellucci S, Katz J. Global-scale secure multiparty computation//Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security. Dallas, USA, 2017: 39-56

[79] Barak A, Hirt M, Koskas L, et al. An end-to-end system for large scale P2P MPC-as-a-service and low-bandwidth MPC for weak participants//Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security. Toronto, Canada, 2018: 695-712

[80] Decker C, Wattenhofer R. Information propagation in the Bitcoin network//Proceedings of the 2013 IEEE P2P. Trento, Italy, 2013: 1-10

[81] Bag S, Sakurai K. Yet another note on block withholding attack on Bitcoin mining pools//Proceedings of the International Conference on Information Security. Honolulu, USA, 2016: 167-180

[82] Schrijvers O, Bonneau J, Boneh D, et al. Incentive compatibility of Bitcoin mining pool reward functions//Proceedings of the International Conference on Financial Cryptography and Data Security. Christ Church, Barbados, 2016: 477-498

[83] Bag S, Ruj S, Sakurai K. Bitcoin block withholding attack: Analysis and mitigation. IEEE Transactions on Information Forensics and Security, 2016, 12(8): 1967-1978

[84] Apostolaki M, Marti G, Müller J, et al. SABRE: Protecting Bitcoin against routing attacks//Proceedings of the 26th Annual Network and Distributed System Security Symposium. San Diego, USA, 2019: 02A1

[85] Apostolaki M, Zohar A, Vanbever L. Hijacking Bitcoin: Routing attacks on cryptocurrenciess//Proceedings of the 2017 IEEE Symposium on Security and Privacy. San Jose, USA, 2017: 375-392

[86] Wohrer M, Zdun U. Smart contracts: Security patterns in the Ethereum ecosystem and solidity//Proceedings of the 2018 International Workshop on Blockchain Oriented Software Engineering. Campobasso, Italy, 2018: 2-8

[87] Grossman S, Abraham I, Golan-Gueta G, et al. Online detection of effectively callback free objects with applications to smart contracts//Proceedings of the ACM on Programming Languages, Paris, France, 2017: 48

[88] Park D, Zhang Y, Saxena M, et al. A formal verification tool for Ethereum VM Bytecode//Proceedings of the 2018 26th ACM Joint Meeting on European Software Engineering Conference and Symposium on the Foundations of Software Engineering. Florida, USA, 2018: 912-915

[89] Bartoletti M, Zunino R. BitML: A calculus for Bitcoin smart contracts//Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security. Toronto, Canada, 2018: 83-100

[90] Chen T, Zhu Y, Li Z, et al. Understanding Ethereum via graph analysis//Proceedings of the IEEE INFOCOM 2018-IEEE Conference on Computer Communications. Honolulu, USA, 2018: 1484-1492

LIU Han-Qing, M. S. candidate. His research interests include security of the blockchain and data privacy in the blockchain.

RUAN Na, Ph. D., associate professor. Her research interests include security & privacy, blockchain and big data.

Background

Most traditional payments on the Internet are based on the trusted third parties. The trust-based payment model has some inevitable shortcomings which arouse the public's concern. In the past decade, the public's interest has focused on decentralized cryptocurrencies based on blockchain technology. Some digital cryptocurrencies such as Bitcoin apply blockchain technology. To ensure the performance of a blockchain, trade-off in the design of blockchain must be made. Some mechanisms in the data layer, the network layer, the consensus layer, the incentive layer, the contract layer, and the application layer of the blockchain will inevitably result in attacks. Researchers have proposed various attacking strategies in all six layers of the blockchain. The relationship and differences among these attacks need to be studied.

This work summarizes well-known attacks in the blockchain and provides a novel way to taxonomies them. The attack classification method presented by this work reveals the relationship and differences among attacks in the blockchain and summarizes the features of them. This work also presents methods to detect or prevent these attacks based on their features.

Before this work, Professor Ruan and her team has worked on the topic of blockchain for more than three years. One of our work named '*On the strategy and behavior of Bitcoin mining with N attackers*' was accepted by Asia CCS 2018. Moreover, Professor Ruan was invited to give a talk on blockchain security on 2018 CCF Chinese Blockchain Conference (CCF CBC2018, CCF-18-TC35-01N). This work is partly summarized from that report.

This work is supported by the National Natural Science Foundation of China under Grant No. 61702330.