区块链资产窃取攻击与防御技术综述

余北缘，任珊瑶，刘建伟
（北京航空航天大学网络空间安全学院，北京 海淀 100191）

摘 要：自中本聪提出比特币以来，区块链技术得到了跨越式发展，特别是在数字资产转移及电子货币支付方面。以太坊引入智能合约代码，使其具备了同步及保存智能合约程序执行状态，自动执行交易条件并消除对中介机构需求，Web3.0 开发者可利用以太坊提供的通用可编程区块链平台构建更加强大的去中心化应用。公链系统具备的特点，如无须中央节点控制、通过智能合约保障交互数据公开透明、用户数据由用户个人控制等，使得它在区块链技术发展的过程中吸引了更多的用户关注。然而，随着区块链技术的普及和应用，越来越多的用户将自己的数字资产存储在区块链上。由于缺少权威机构的监管及治理，以太坊等公链系统正逐步成为黑客窃取数字资产的媒介。黑客利用区块链实施诈骗及钓鱼攻击，盗取用户所持有的数字资产来获取利益。帮助读者建立区块链资产安全的概念，从源头防范利用区块链实施的资产窃取攻击。通过整理总结黑客利用区块链环境实施的资产窃取攻击方案，抽象并归纳威胁模型的研究方法，有效研究了各类攻击的特征及实施场景。通过深入分析典型攻击方法，比较不同攻击的优缺点，回答了攻击能够成功实施的根本原因。在防御技术方面，针对性结合攻击案例及攻击实施场景介绍了钓鱼检测、代币授权检测、代币锁定、去中心化代币所属权仲裁、智能合约漏洞检测、资产隔离、供应链攻击检测、签名数据合法性检测等防御方案。对于每一类防御方案，给出其实施的基本流程及方案，明确了各防护方案能够在哪类攻击场景下为用户资产安全提供防护。

关键词：区块链；钓鱼攻击；诈骗攻击；智能合约安全
中图分类号：TP393
文献标志码：A
DOI: 10.11959/j.issn.2096−109x.2023001

Overview of blockchain assets theft attacks and defense technology

YU Beiyuan, REN Shanyao, LIU Jianwei
School of Cyber Science and Technology, Beihang University, Beijing 100191, China

Abstract: Since Satoshi Nakamoto’s introduction of Bitcoin as a peer-to-peer electronic cash system, blockchain technology has been developing rapidly especially in the fields of digital assets transferring and electronic currency payments. Ethereum introduced smart contract code, giving it the ability to synchronize and preserve the execution status of smart contract programs, automatically execute transaction conditions and eliminate the need for intermediaries. Web3.0 developers can use Ethereum’s general-purpose programmable blockchain platform to build

收稿日期：2022−07−10；**修回日期**：2022−12−24
通信作者：刘建伟，liujianwei@buaa.edu.cn
基金项目：国家自然科学基金（61972018，61932014）
Foundation Item: The National Natural Science Foundation of China (61972018, 61932014)

引用格式：余北缘, 任珊瑶, 刘建伟. 区块链窃取攻击与防御技术综述[J]. 网络与信息安全学报，2023, 9(1): 1-17.
Citation Format: YU B Y, REN S Y, LIU J W. Overview of blockchain theft attacks and defense technology[J]. Chinese Journal of Network and Information Security, 2023, 9(1): 1-17.

more powerful decentralized applications. Ethereum's characteristics, such as central-less control, public and transparent interaction data guaranteed by smart contracts, and user-controlled data, have attracted more attentions. With the popularization and application of blockchain technology, more and more users are storing their digital assets on the blockchain. Due to the lack of regulatory and governance authority, public chain systems such as Ethereum are gradually becoming a medium for hackers to steal digital assets. Generally, fraud and phishing attacks are committed using blockchain to steal digital assets held by blockchain users. This article aims to help readers develop the concept of blockchain asset security and prevent asset theft attacks implemented using blockchain at the source. The characteristics and implementation scenarios of various attacks were effectively studied by summarizing the asset theft attack schemes that hackers use in the blockchain environment and abstracting research methods for threat models. Through an in-depth analysis of typical attack methods, the advantages and disadvantages of different attacks were compared, and the fundamental reasons why attackers can successfully implement attacks were analyzed. In terms of defense technology, defense schemes were introduced such as targeted phishing detection, token authorization detection, token locking, decentralized token ownership arbitration, smart contract vulnerability detection, asset isolation, supply chain attack detection, and signature data legitimacy detection, which combine attack cases and implementation scenarios. The primary process and plans for implementation of each type of defense plan were also given. And then it is clear which protective measures can protect user assets in different attack scenarios.

Keywords: blockchain, phishing attack, fraud attack, smart contract security

0 引言

2013 年 12 月，Vitalik 分享了以太坊网络的白皮书[1]，详细描述了以太坊的愿景与构建目标：搭建一个满足图灵完备特性的区块链网络。通过引入智能合约，使开发者能够在无须搭建点对点网络、区块链 RPC、共识算法等基础设施的前提下，使用契约型编程语言快速开发去中心化应用，为开发者提供一套能够稳定运行去中心化应用的“世界计算机”系统。

以太坊的出现有效解决了比特币网络中构建去中心化应用所面临的数据容量及交易类型限制等问题。为了激励去中心化节点参与共识共同搭建“世界计算机”，防范攻击者向区块链网络发动拒绝服务攻击，以太坊引入了一种效用货币 ETH，在使用以太坊转账、部署智能合约、调用智能合约时，用户需要支付 ETH 以确保交易能够被节点打包和执行。随着基于以太坊网络开发的 DeFi 生态[2]的发展及 NFT[3]这类去中心化应用开始火爆，ETH 及使用 ETH 作为结算的衍生品价格逐渐上涨，为实现利益的最大化，部分黑客尝试使用网络攻击技术获取用户通过区块链网络持有的数字资产，危害用户的资产安全。

本文主要研究了以下内容。

1) 对区块链环境中针对数字资产窃取攻击的研究方向进行了总结，介绍研究背景、研究采用的技术、研究成果并对其优劣进行了详细分析。

2) 对区块链环境下的数字资产防盗技术这一研究进行了总结，介绍研究背景、研究采用的技术、研究成果并对相关研究的优劣进行了细致分析。

3) 详细介绍了与区块链资产窃取技术相关的专有名词，并给出了定义。

4) 分类介绍了区块链资产窃取攻击的实施方法及威胁模型：通过介绍敌手实施攻击的过程及其为了使攻击成功所采用的技术及策略，帮助读者建立对资产窃取攻击的认识。

5) 在区块链资产窃取方面：将威胁模型划分为仿冒钓鱼、代币恶意授权、智能合约漏洞、供应链、私钥泄露、远程控制、盲签名威胁 7 类。通过分析攻击特点、攻击实施流程、攻击成功关键因素并绘制威胁模型的方式，帮助读者更好地理解各威胁对用户资产带来的危害。

6) 分类研究各类保护区块链资产的防护方案，阐述并分析了各类防护方案的原理、关键技术和优缺点。

1　主要内容

1.1　区块链技术概述

区块链主要具有以下特点[4]：① 去中心化，区块链网络中没有任何可信第三方存在，这与有政府、银行或金融机构做背书的传统中心化金融系统存在差异；② 零信任化，所有区块链节点彼此之间无须信任，只需要按照共识算法执行即可对区块链账本条目达成一致；③ 公开性[5]，任何节点可以结合使用需求随时加入或退出区块链网络，通过区块链存储的账本数据可公开查询；④ 不易篡改性，区块中已记录的交易数据随着区块高度的增长，不易被篡改；⑤ 匿名性[6]，尽管通过统计学方法及区块链浏览器能够分析特定地址的历史交易行为及关联地址信息，但无法将区块链地址与真实的用户身份进行关联。

1.2　区块链资产窃取攻击概述

作为一种使用密码学技术为网络交易数据安全提供保护[7]的零信任环境，区块链及其衍生环境中存在大量威胁用户资产安全的漏洞和缺陷。随着区块链网络、去中心化应用的普及，区块链匿名特性逐渐显露其弊端：被盗资产无法找回，攻击者身份难以追踪及确认。随着利用区块链发行的加密货币影响力逐步增加，缺乏监管的特性使其逐步成为网络犯罪分子使用的理想工具。使用加密货币实施网络洗钱、网络钓鱼、资产窃取、网络欺诈的案例逐步增多[8]。

在数字资产窃取攻击这一细分领域，学术界及产业界主要开展了以下研究。

（1）犯罪案例及犯罪心理学研究[9]

通过对现有利用区块链为媒介实施资产窃取攻击的案例进行研究。这类研究的主要贡献有：① 阐明了区块链因监管缺失逐步成为黑客攻击媒介的背景，通过案例分析解释了黑客利用区块链窃取“数字货币”的优势及劣势；② 结合案例学习，阐述了黑客利用区块链及“数字货币”为媒介实施攻击的犯罪心理；③ 对攻击方案与区块链在攻击实施中起到的作用进行了关联分析，阐明了区块链及加密货币如何在技术演进中成为促进网络犯罪实施的工具；④ 阐述了利用区块链实施的违法犯罪行为，如网络洗钱、网络诈骗、金融犯罪等其他犯罪案例，为研究人员、监管及立法机构提供了充实的研究对象和依据。同时，这类研究存在以下不足：① 没有对资产窃取攻击及其防御技术进行深入研究及阐述；② 研究中介绍资产窃取相关的案例已无法满足用户在当前网络环境下对区块链资产安全的需求。

（2）全节点攻击向量抓取及行为识别[10]

为了抓取敌手实施资产窃取攻击时向区块链网络发送的交易数据及攻击向量，部分研究人员通过改造以太坊全节点代码并引入蜜罐的技术手段对数据收集及研究：抓取敌手通过 HTTP RPC 向含蜜罐功能的以太坊全节点发送的探测数据及攻击向量。这一研究主要具备以下优点：① 通过引入蜜罐技术以识别部分针对区块链全节点及对应区块链账户的资产窃取攻击向量的行为；② 能够识别攻击者通过 RPC 调用发送至全节点的用于窃取 ETH 及 ERC20 标准代币的交易攻击向量行为；③ 通过对蜜罐日志分析发现攻击者为了隐藏其 IP 地址会选择使用 Tor 网络[11]发送攻击向量，为以太坊全节点运营商在系统安全建设方面提供了样本和参考；④ 使用污点分析的方法对攻击者发起攻击的地址及资金流向进行了详细的跟踪，揭示了攻击者在通过攻击获利后需要通过中心化交易所对资金进行变现的现象。这类研究也存在一定不足：① 对研究人员的技术储备要求较高；② 通过研究所识别的攻击的主要实施目标为以太坊全节点运营商，对普通区块链用户资产安全影响有限；③ 缺少保障区块链用户资产安全的分析与研究；④ 缺少对窃取符合 ERC721[12]及 ERC1155[13]标准代币的数据及攻击案例。

（3）钓鱼攻击场景识别及技术研究[14]

有研究人员通过对发生在区块链环境下的资产窃取攻击案例进行分析：有效地归纳攻击场景和实施攻击需要使用的技术。这类研究主要具备以下优点：① 利用区块链实施资产窃取攻击的类型主要为钓鱼攻击；② 用数据证明钓鱼攻击的影响力，即无须攻破区块链基础设施，仅通过精心设计构造的钓鱼场景就可误导用户主动转账、披露敏感信息、主动运行恶意可执行程序等；③ 钓鱼攻击成功率高，即用户轻信其通过零信任环境接收的信息且疏于对信息的含义及合法性进行检

查；④ 社会工程学攻击[15]主要利用受害人在受骗后的独立错误行为获得成功[16]。这类研究同时存在以下不足：① 仅阐述了利用钓鱼攻击窃取用户数字资产的攻击场景，缺少对私钥扫描、盲签名、供应链攻击等新兴攻击技术的研究与分析，缺乏对资产窃取攻击全貌的总结及分析；② 虽然详细整理了利用钓鱼实施的资产窃取的攻击类型，但缺少对攻击实施流程及威胁模型的总结。

（4）智能合约漏洞及攻击分析[17]

研究人员通过对以太坊及其智能合约框架进行系统分析，系统整理了以太坊及智能合约编程语言中存在的安全漏洞及对应的攻击方案。这类研究主要具备以下优点：① 系统阐述了以太坊及其智能合约编程语言存在的安全漏洞；② 结合攻击案例，为智能合约开发者进行安全开发提供了参考；③ 直击要害，通过对存在漏洞的智能合约代码进行简化，帮助研究人员、开发者更好地理解及掌握漏洞产生原因及危害；④ 促进了智能合约形式化分析及验证技术[18]的发展。这类研究主要存在以下不足：① 对研究人员的技术储备要求较高；② 缺少从区块链用户角度规避存在智能合约漏洞项目的建议及注意事项。

（5）私钥窃取技术研究

部分研究人员将研究重点聚焦在如何通过技术手段直接从区块链钱包中获取私钥，进而控制对应钱包内的数字资产。相关工作[19]通过对硬件钱包进行安全性分析，主要做出了以下贡献：① 通过利用电磁信号、签名运算时间等侧信道数据，攻击者有机会获取硬件钱包私钥信息；② 通过对存在安全漏洞的硬件钱包进行渗透，攻击者有一定概率能够窃取硬件钱包私钥。这类研究向产业界证明了将私钥脱网存储的硬件钱包并不完全安全。相关研究存在以下的弊端：① 威胁模型较为理想，与实际环境差异较大；② 缺少对完整攻击方案及攻击利用方法的整理；③ 随着硬件钱包的更新迭代，安全性得到显著提升，研究所提出的攻击方案在实践中难以复现；④ 针对硬件钱包安全这一研究领域，缺少对硬件钱包供应链攻击、硬件钱包地址隐蔽替换[20]等新兴攻击方案的分析与介绍。此外，有部分研究人员重点对安卓操作系统上使用的区块链钱包应用进行了详细分析[21]，通过屏幕截图及敏感信息识别、USB调试截获用户键盘输入两类攻击方法，敌手能够直接盗取用户的钱包私钥及钱包解锁口令，对用户资产安全造成严重的威胁，该研究证明在实验环境下敌手有能力抓取用户的钱包私钥。

通过对现有研究分析能够发现：针对区块链资产窃取攻击这一主题，国内外研究人员主要从犯罪及立法、区块链节点安全运营、钓鱼场景识别、代码漏洞审计与识别、私钥窃取技术等角度开展研究。随着网络攻防技术的发展，各类攻击技术也在演进与迭代。本文对以区块链为媒介实施资产窃取的攻击样本及攻击特征进行了总结整理，有助于帮助学术界及产业界更好地认识相关攻击的危害，有助于针对相关攻击提出防御方案，切实保护用户的资产安全。

1.3 区块链资产防盗技术概述

通过区块链购买及持有的数字资产、“数字货币”通常对应着链上治理和代币价值权益，一旦数字资产被窃取，则权益将跟随资产全部转移至敌手处使用户蒙受损失。通过研究安全机制防止用户持有的代币被黑客窃取，是保护用户权益的基础和核心。在实践中，为了解决数字资产易被黑客盗取的问题，学术界及产业界主要开展了以下研究。

（1）钓鱼行为识别

有研究人员通过将钓鱼检测任务转换为分类问题开展研究：根据区块链地址的历史交易记录、交易金额等特征结合随机游走[22]、图神经网络[23]等模型提取目标区块链地址的行为及身份特征。这类研究主要具备以下优势：① 在检测存在钓鱼行为的区块链地址方面取得了较优的准确率；② 部分研究人员将交易收发地址作图节点，交易金额作有向边的方法将各图节点之间发生的多条交易合并为单条交易最终形成节点的小规模交易模式图[24]。该方法有效降低了训练模型的复杂度，提高了训练效率。这类研究在实践中也存在的一定的劣势：① 对于无任何历史交易的新区块链地址，检测能力较弱；② 部分研究缺少对交易数据的处理，计算复杂度较高；③ 无法对社交网络身份仿冒、站点仿冒等复杂环境中实施的钓鱼攻击进行识别。

（2）智能合约漏洞检测

部分研究人员采用语义分析法对智能合约进行安全分析[25]：通过分析智能合约引用及依赖，提取代码语义并进行合规性检查的方式检测智能合约中存在的安全漏洞、违背安全开发要求的代码用例。部分研究人员利用深度神经网络[26]扫描智能合约中存在的漏洞；还有部分研究人员采用模糊测试技术与机器学习技术相结合的方式实现了代码审计及检测工具[27]，有效检测智能合约中存在的安全隐患。这类工作为安全开发智能合约提供了解决方案，但无法在用户端保护区块链资产安全。

（3）智能合约敏感方法调用检测

研究人员通过对以太坊中主流的代币合约、NFT 交易平台合约所提供的方法进行分析及归类，识别存在资产窃取风险的智能合约方法，并在用户调用敏感方法时发出告警。这类防护技术主要具备以下优势：① 守护程序以浏览器插件形式常驻内存，用户友好度较高；② 对于代币授权这类符合 ERC20、ERC721 及 ERC1155 标准的敏感调用方法检测准确度高；③ 对在 NFT 交易平台免费售卖 NFT 这一可能使用户资产受损的操作检测准确度高；④ 适用于所有兼容以太坊虚拟机的区块链系统。这类研究存在以下缺陷：① 缺少对部分不常用但危险的智能合约方法的检测，攻击者可利用相关调用绕过检测，窃取用户资产；② 对不按照 ERC20、ERC721 及 ERC1155 代币标准开发的智能合约方法检测效果较差，需重点提高扩展性；③ 无法对未开源代码的智能合约敏感调用进行检测。

代币授权机制能够将用户的代币消费权限委托给去中心化应用，使其可以代表用户将代币传输给任意接收者：去中心化应用通常采用无限授权方案，以提高可用性。为了对去中心化应用存在的代币数量无限授权现象及其危害进行系统分析，研究人员对所有与 ERC20 代币标准关联的授权交易进行了详细分析[28]。经分析发现，超过 60% 的去中心化应用存在代币无限授权行为。通过对以太坊上知名的 31 个去中心化应用进行分析发现：这些应用存在无限授权风险，其中只有 3 款应用会通过前端界面向用户揭示代币无限授权的风险，5 款应用允许用户修改授权的代币数量。这一研究证明了代币授权操作对用户资产安全存在的潜在危害。针对未开源的合约代币无法解析的问题，研究人员通过符号执行技术[29]，对代码未开源的 ERC20 代币进行了详细的分析：经审查发现超过 400 个未开源的代币合约在进行代币授权操作时存在恶意行为，给用户资产安全带来了严重的威胁。

针对智能合约敏感调用检测，研究人员主要从实时检测及数据安全分析两个角度进行了研究：证明了代币无限授权、通过恶意去中心化应用授权代币对用户资产安全造成的危害。

（4）代币防盗技术

针对代币易通过授权操作被敌手窃取的缺陷，部分研究人员提出通过在以太坊代币标准中增加安全逻辑的方式提升代币安全性（代币锁定[30]、去中心化的代币所属权仲裁[31]是目前常见的解决方案）。通过为代币加锁，帮助用户有效规避因代币无限授权、盲签名等敏感操作所导致的代币被盗现象。上述研究充分证明了防范不安全的代币授权操作是避免资产被盗的重要手段，但也有部分批评者认为这类防护方案违背了去中心化精神。

（5）安全教育及培训

通过安全教育及培训，帮助用户理解区块链资产窃取攻击的危害、潜在威胁、攻击实施流程、攻击者能够成功窃取用户资产的主要原因。通过安全教育，使用户掌握能够帮助保护其资产安全的技术，如钓鱼信息识别、密钥安全管理[32]、程序沙箱[33]、供应链攻击检测[34]等技术，使用户具备主动识别潜在的安全风险的能力，保护资产安全。

2　专有名词定义

本节给出了与区块链领域相关的专有名词及其定义。

定义 1　（智能合约）智能合约[35]是指一套数字形式定义的承诺，使协议能够在不需要可信第三方介入的情况下按照合约条款自动执行。在以太坊中，智能合约是通过数字形式对达成的协议进行监督执行，其本质是一段能够被以太坊虚拟机（EVM）执行的代码。智能合约一旦被部署，将不易篡改。

定义 2　（智能合约漏洞）智能合约漏洞[36]是指开发智能合约代码时，因代码特性或疏忽而引入的安全缺陷。一旦智能合约中存在的漏洞被黑客利用，将可能导致用户存储在智能合约中的资产被黑客盗取，使用户资产受损。

定义 3　（区块链账户）在以太坊中主要支持两种类型的区块链账户[37]。① 智能合约账户：无私钥，由智能合约代码控制，可以被外部账户调用并按照智能合约代码定义的方法执行交易。② 外部账户：由用户持有的私钥控制。外部账户可以根据使用需求发送交易，如转移 ETH、调用智能合约方法或部署智能合约。

定义 4　（区块链钱包）区块链钱包是一种应用，主要提供了钱包私钥管理、外部账户管理、账户余额查询、交易签名及交易发送等功能。利用区块链钱包能够帮助用户方便地使用去中心化应用、调用智能合约方法。Metamask[38]是一款常用的软件钱包：通过与以太坊节点服务商 Infura 合作，使用户无须搭建以太坊全节点即可接入以太坊网络[39]。Ledger 是一款常用的硬件钱包[40]，使用离线存储技术避免私钥泄露，保证用户资产安全。

定义 5　（钱包密钥）钱包密钥这一概念来自于公钥密码学技术。在区块链环境下需使用公钥密码学技术生成公私钥对[41]。在区块链环境中公钥主要用于生成钱包地址，私钥则用于对交易数据进行签名。区块链钱包会使用哈希函数生成交易摘要，由用户授权钱包使用外部账户对应的私钥对交易摘要进行签名以使用区块链进行转账、调用智能合约等操作。为了保护私钥，区块链钱包通常采用 KDF 算法[42]对私钥进行加密处理，也有部分区块链钱包会生成已经过 KDF 加密处理的 Keystore 文件[43]以保护私钥安全。

定义 6　（钱包地址）钱包地址是区块链账户地址的简称，是一串能够被区块链节点识别的唯一标识符，用户可以使用区块链钱包向指定的钱包地址[44]转移数字资产。

定义 7　（去中心化应用）去中心化应用[45]通常指使用智能合约开发语言构建，运行在区块链网络上的应用程序。常见的去中心化应用会为用户提供一组前端界面，以方便用户通过浏览器和前端接口与智能合约进行交互。去中心化应用通常具备代码开源、支持加密货币支付、无中间节点、基于区块链开发等特点。

定义 8　（节点）参与维护区块链数据的计算设备即节点[46]：通过贡献运算能力维护区块链网络安全而获得奖励。处在运行状态的节点需要完成以下任务：① 接收并同步链上交易数据；② 同步区块高度至最新状态；③ 验证区块及区块内包含交易的正确性；④ 处理交易并打包；⑤ 参与共识协议就区块数据与其他分布式节点达成一致。

定义 9　（交易费）运行区块链共识协议的节点为区块链网络运行提供了计算资源，按照共识协议要求将获得交易费作为报酬。在使用区块链网络进行转账、与智能合约进行交互时区块链外部账户内需要包含足够支付交易费[47]的效用货币。通过交易费这一设计，能够在一定程度上防范黑客实施拒绝服务攻击对区块链服务可用性的影响。

定义 10　（数字资产）数字资产是区块链链上资产的统称，在以太坊中常见的数字资产主要包括 ETH 这类效用货币和符合 ERC20、ERC721 和 ERC1155 标准的链上代币。

3　威胁模型及攻击方案分析

本节对常见的资产窃取攻击技术进行介绍，通过将攻击抽象为威胁模型的方法帮助读者更好地认识资产窃取攻击。通过对不同威胁模型中有代表的攻击技术、攻击实施方案及策略进行总结，引出该类威胁所对应的攻击能够成功实施的主要原因。最后对各类威胁模型及危害用户资产安全的攻击技术进行分析。

3.1　典型威胁模型及攻击方案介绍

威胁模型 1（仿冒钓鱼威胁）仿冒钓鱼威胁（模型如图 1 所示）主要源自敌手通过社交身份仿冒、站点仿冒、邮件仿冒等钓鱼攻击手法窃取用户持有的区块链数字资产。

在社交身份仿冒方面，敌手通常会利用社交网络创建虚假社交账号，冒充知名区块链项目和用户身份。通过获取用户信任、投放钓鱼信息的方式诱导用户完成对敌手实施资产窃取攻击有利的行动，如主动提供社交账号密码、区块链私钥等敏感信息或执行向敌手钱包地址转账、访问敌手提供的恶意站点等不安全操作。

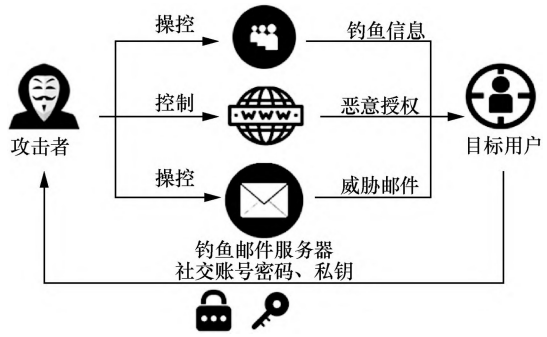

图 1　仿冒钓鱼威胁模型

Figure 1　Counterfeit-phishing threat model

在站点仿冒方面，敌手主要通过复制网站副本、申请相近域名，向潜在受害者投放包含虚假资源链接的信息，在仿冒站点中添加窃取用户区块链资产的恶意授权或转移逻辑的方式实施资产窃取攻击。为了创建不易于被用户识别的仿冒站点和页面，敌手通常会使用 Punycode[48]编码域名的方式误导用户：通过肉眼检查无法区分经 Punycode 编码的域名与正常域名之间存在的差异[49]。此外，部分敌手会采用注册.xyz 后缀的同名域名的方法以误导用户。创建虚假社交账号并对虚假账号进行运营，待获得关注及用户信任后向目标用户投放仿冒站点链接，是仿冒威胁中敌手通常采用的攻击策略。

在邮件仿冒方面，敌手通常会使用技术手段[50]篡改发件地址并冒充官方口吻向用户投放钓鱼邮件。通过威胁或设置任务倒计时的策略误导用户：“您必须按照邮件所述的要求执行特定操作，否则您的区块链账户将被冻结”。一旦用户选择相信并按照要求执行任务，其数字资产安全将受到严重威胁。

仿冒钓鱼威胁具有影响范围广、受害用户多、攻击实施成本低等特点。相关攻击技术能够成功实施的原因在于其巧妙地利用了用户对与其建立联系的陌生人存在的潜在信任：通过仿造的社交账号、域名和网站使用户误认为其正在访问或使用官方服务，最终完全信任并完成对敌手有利的行为[51]：主动提供钱包私钥或助记词、将代币使用权授予敌手控制的区块链地址、主动向敌手控制的区块链地址转账代币等。

威胁模型 2（代币恶意授权威胁）代币恶意授权威胁（模型如图 2 所示）主要源自敌手滥用 ERC20、ERC721、ERC1155 这类以太坊标准代币合约中提供的代币授权方法恶意转移用户授权其使用的代币类攻击。

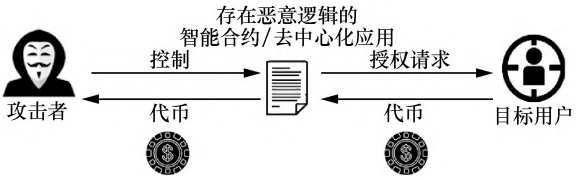

图 2　代币恶意授权威胁模型

Figure 2　Malicious token approval threat model

敌手利用存在恶意逻辑的智能合约或去中心化应用向用户发起代币授权请求，申请由敌手控制的区块链地址转移用户持有的代币，在获得用户授权后敌手通过发起代币转账交易的方式将代币转移，最终成功窃取用户持有的数字资产。

表 1 列出了以太坊 ERC20、ERC721 及 ERC1155 标准代币中提供的代币授权方法及作用，通过调用相关方法[52]能够将用户的代币使用权限委托至去中心化应用。

表 1　ERC 标准代币授权方法及作用

Table 1　ERC standard approve method and effects

ERC 标准	方法名	方法作用	EVM 编码
ERC20	approve	授权第三方账户使用指定额度的代币	0x095ea7b3
ERC721	approve	授权第三方账户使用指定编号的代币	0x095ea7b3
ERC721	setApprovalForAll	授权第三方账户使用持有的所有合约代币	0xa22cb465
ERC1155	setApprovalForAll	授权第三方账户使用持有的所有合约代币	0xa22cb465

代币恶意授权威胁相关的攻击技术能够成功实施的原因在于：授权是满足以太坊标准的合法智能合约方法，用户通常会相信向其发送代币授权请求的去中心化应用是安全且能够妥善使用的数字资产。

代币恶意授权是窃取用户区块链资产的主要方法，实际研究表明[29]，敌手能够在无须用户干预的情况下直接转移用户授权其使用的任意数字资产，对用户的区块链资产安全造成严重的危害。对敏感授权行为进行检测并向用户发布告警是防范这类攻击的主要思路。

威胁模型 3（智能合约漏洞威胁）智能合约漏洞威胁（模型如图3所示）主要源自开发者在开发智能合约时因疏忽或开发语言局限而在代码中引入的缺陷，使敌手能够在未授权的情况下控制智能合约，触发对敌手有利的智能合约逻辑或方法。

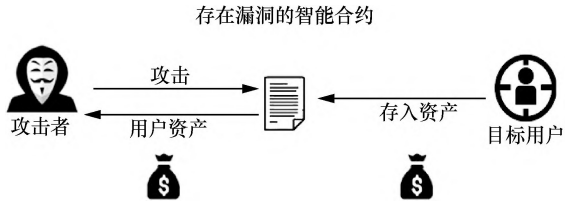

图3　智能合约漏洞威胁模型
Figure 3　Smart contract vulnerability threat model

2016年，通过攻击以太坊上最大的众筹项目——The DAO[53]智能合约，黑客获得了超过1亿美元的灰色收入。利用The DAO智能合约中存在的重入漏洞，敌手配合智能合约的fallback函数以递归调用的形式持续从The DAO智能合约中提取资产直至合约内资产完全枯竭。该攻击影响深远，最终导致以太坊团队被迫通过区块链硬分叉升级恢复The DAO合约内存储的资产，这一举动引发了以太坊社区关于是否需要通过中心化手段分叉区块链以干涉敌手作恶的讨论。

2022年，通过攻击BSC链的TokenHub跨链桥合约[54]，黑客获得了超过7亿美元的灰色收入。利用TokenHub智能合约中存在的IAVL树校验漏洞，黑客从跨链桥凭空生成了超过200万个BNB代币，最终通过技术手段获利离场。该攻击直接导致币安官方宣布BSC链停链以排查漏洞并查封黑客通过攻击获得的资产。这一攻击还为BSC链的借贷协议Venus带来了超过1亿美元的坏账。

智能合约漏洞造成的资产损失数额巨大，仅2022年上半年发生在区块链领域的安全事件就造成了超过19亿美元的损失。由于区块链具有强匿名特性，大量黑客能够在攻击智能合约漏洞获得巨额收入的同时逍遥法外。智能合约漏洞还具备影响范围广的特点：合约内存放的资产大多来自用户持有的“数字货币”，一旦资产被黑客窃取，用户将面临取证困难、数字资产不受相关法律保护、敌手身份难以追查核实等问题。

攻击智能合约中存在的缺陷，使智能合约能够执行开发人员预期外的行为是敌手能够成功从智能合约中窃取数字资产的主要原因。通过逻辑形式化验证[55]、代码审计[56]等方式修复智能合约存在的逻辑漏洞是防范相关攻击的主要思路。

威胁模型 4（供应链威胁）供应链威胁（模型如图4所示）是一种面向软件开发者及应用分发商的新兴威胁[57]。敌手可通过入侵区块链钱包供应链、区块链开源框架供应链等投放恶意逻辑抓取钱包私钥的方式窃取数字资产。

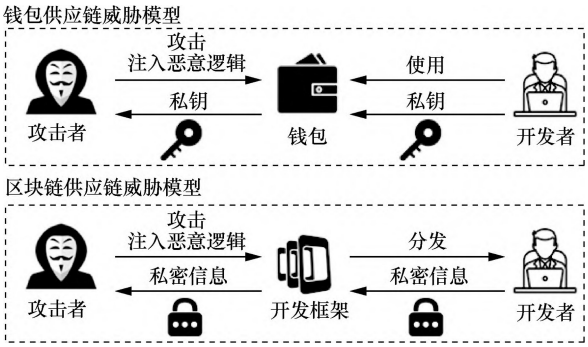

图4　供应链威胁模型
Figure 4　Supply chain threat model

在区块链钱包供应链方面主要面临两类威胁。① 软件钱包[58]供应链威胁：通过复制软件钱包开源代码，注入恶意逻辑并通过应用商店或社交网络分发的方式实施供应链攻击。② 硬件钱包[59]供应链威胁：通过快递截取、硬件固件破解及刷机、假冒钱包替换等方式实施供应链攻击。

在区块链开发框架供应链方面，敌手主要通过在开放框架内注入恶意逻辑并分发至去中心化开发者的方式实施供应链攻击，有部分敌手利用软件源在托管开发框架时缺少对代码合法性、软件包名合法性的验证逻辑，成功将存在恶意逻辑的开发框架发布[60]在pypi、npm、maven等知名软件源中，以针对区块链开发者实施供应链攻击。

供应链攻击主要具备攻击噪声低的特点，直至发现数字资产被恶意窃取时，用户仍难以排查钱包私钥丢失的原因。供应链威胁及其相关的攻击技术能够成功实施的原因在于：用户通常会信任其通过应用商店、知名软件源所下载软件的可靠性；信任其购买的硬件钱包在生产及分发各环节是完全安全且未被篡改的。当用户按照正常的信任及运行权限使用存在供应链攻击的区块链钱包及开发工具时，敌手能够窃取私钥信息进而威胁用户的资产安全。

威胁模型 5（私钥泄露威胁）私钥泄露威胁（模型如图 5 所示）主要源自用户未妥善管理区块链钱包密钥，使敌手能够通过技术手段获取用户钱包私钥，进而窃取区块链资产。

图 5　私钥泄露威胁模型

Figure 5　Private key leakage threat model

部分开发者在开发去中心化应用时，未妥善管理钱包私钥，直接在程序代码段内以明文形式引用钱包私钥并将应用代码开源至 Github 等开源应用分发平台，而敌手可通过敏感信息匹配的方式抓取用户本无意公开的私钥[61]，进而实施资产窃取攻击。

私钥泄露是资产窃取攻击中危害最严重的威胁，因为一旦掌握用户泄露的钱包私钥，敌手即可完全控制、访问、转移钱包内的所有数字资产。

用户未按照密钥管理要求管理钱包私钥是私钥泄露的主要原因。妥善管理钱包私钥[62]，不向任何人透露与钱包私钥相关的信息是防范这类攻击的主要思路。

威胁模型 6（远程控制威胁）远程控制威胁（模型如图 6 所示）主要源自用户在未对其通过 Web3 环境接收的可执行程序进行安全检测的情况下即执行并导致主机被敌手控制：敌手通常使用其控制的主机执行对敌手有利的命令，进而窃取用户持有的数字资产。

在获得主机控制权后敌手通常会采用以下策略实施攻击：① 检查主机内安装的区块链钱包应用；② 部署键盘记录器[63]；③ 执行口令本地破解攻击[64]；④ 查询用户常用的区块链交易地址；⑤ 通过技术手段误导用户执行对敌手有利的行为；⑥ 远程控制用户区块链钱包，转移数字资产。

部署键盘记录器能够帮助敌手抓取用户通过键盘键入的任意数据，敌手可利用该方法获取区块链钱包的解锁口令，进而实现资产窃取攻击。口令本地破解攻击通常采用统计学方法[65]对用户设置的口令进行分析，以提升破解速度，若本地破解成功，则敌手能够在用户不知情的情况下解锁区块链钱包，直接窃取钱包内数字资产。

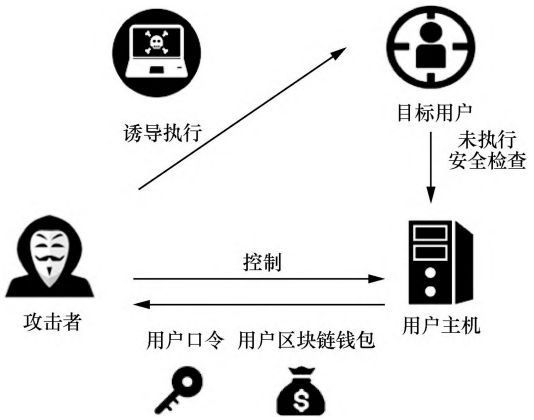

图 6　远程控制威胁模型

Figure 6　Remote control threat model

通过区块链浏览器查询用户区块链钱包的联系人或近期交易地址数据，敌手可以获取用户在使用区块链时经常进行交易操作的地址信息（如交易所充值地址），利用这类信息敌手可利用外包计算[20]生成近似的区块链地址。在用户复制转账地址时，通过剪贴板替换攻击[66]将用户复制的地址替换为敌手生成的近似地址，利用用户在转账时对目的地址校验不够仔细的疏忽实现资产窃取攻击。

远程控制威胁主要具有收益−成本比率[67]较高的特性，使用 APT[68]工具可以零成本且自动生成远程控制脚本。一旦远控脚本被成功执行，敌手即可控制目标主机并尝试窃取用户持有的数字资产。

对可执行程序安全性完全信任，在包含区块链钱包的主机内以最高权限运行可执行程序，是远程控制威胁危害用户资产安全的主要原因。利用虚拟机、沙箱、杀毒软件等工具对可执行程序进行安全性验证是防范相关攻击的主要思路。

威胁模型 7（盲签名威胁）盲签名[69]威胁（模型如图 7 所示）主要源自敌手通过去中心化应用向用户发起恶意签名请求时，用户在未对待签名数据所对应的区块链交易行为进行合法验证的前提下直接授权使用私钥签名数据所导致的资产窃取攻击。

敌手可按照区块链交易格式，构造转移用户全部数字资产这类对其有利的交易数据，通过计算交易数据对应 Hash 值并通过恶意去中心化应用诱导用户使用钱包私钥对 Hash 值签名的方式

获得能够帮助区块链节点验证交易数据合法性的签名数据。随后，敌手可利用其控制的区块链 RPC 节点广播交易数据及签名数据，达到窃取用户资产的目的。

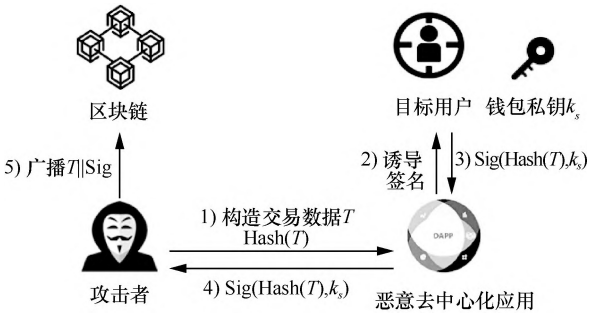

图 7 盲签名威胁模型

Figure 7 Blind signature threat model

尽管钱包私钥没有泄露，但敌手可通过生成聚合交易 Hash 并以用户签名的方式窃取用户钱包内持有的所有数字资产，严重危害用户数字资产安全。在盲签名威胁中，待签名数据是一串肉眼无法识别其含义的十六进制数据，这一特征导致用户无法验证 Hash 内容及对应交易行为的合法性。避免盲签名威胁的主要思路是检测或验证发起签名请求的去中心化应用是否存在恶意的资产窃取行为。

3.2 分析

区块链资产窃取攻击威胁种类繁多且难以禁止的原因如下。

1) 区块链交易不可逆：逆转一笔区块链交易在理论上是复杂的，一旦数字资产被盗，用户将难以追回被盗资产。

2) 数字资产容易变现：通过攻击零成本获得的数字资产具有易于变现的特点，代币可通过去中心化交易所卖出，NFT 则可通过交易平台售卖，为敌手实施攻击提供了动机。

3) 安全教育缺失：在区块链环境中实施的安全攻击种类众多，普通用户缺少保护其资产的安全教育，这为敌手实施攻击提供了重要的前提。

4) 受众范围广：区块链应用受众范围广，参与用户量大，随着“数字货币”市值上涨，实施资产攻击的收益产出比逐渐提高。

3.3 威胁攻击实例实施流程

3.3.1 仿冒钓鱼威胁

仿冒钓鱼威胁攻击实施流程如图 8 所示。

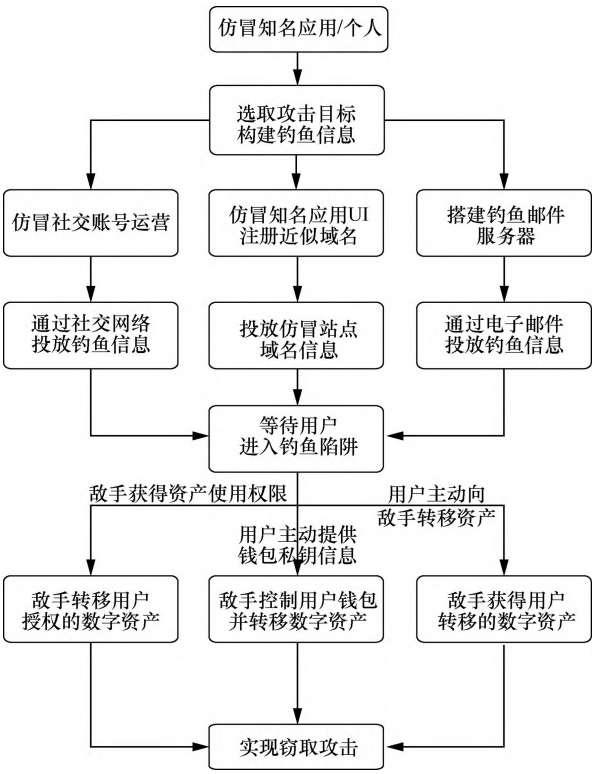

图 8 仿冒钓鱼威胁攻击实施流程

Figure 8 Counterfeit-phishing threat attack procedure

3.3.2 代币恶意授权威胁

代币恶意授权威胁攻击实施流程如图 9 所示。

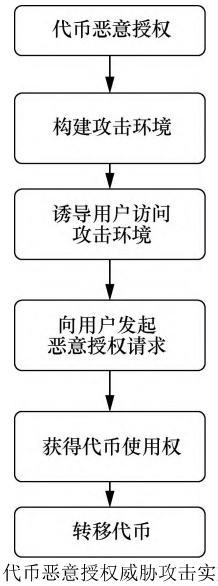

图 9 代币恶意授权威胁攻击实施流程

Figure 9 Malicious token approval threat attack procedure

3.3.3 供应链威胁

软件钱包供应链攻击实施流程如图 10 所示。硬件钱包供应链攻击实施流程如图 11 所示。

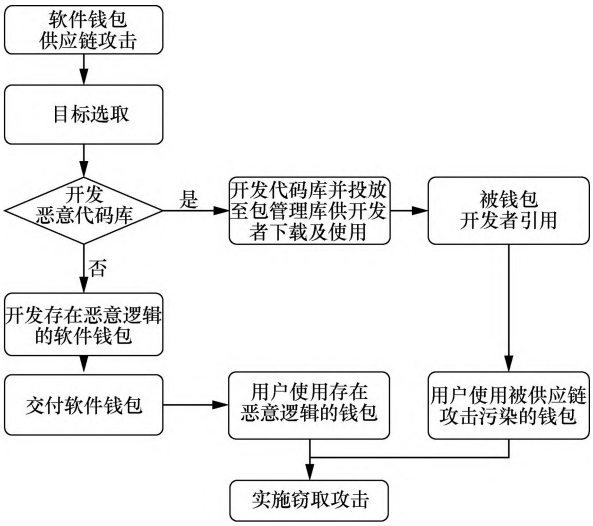

图 10　软件钱包供应链攻击实施流程

Figure 10　Software wallet supply chain attack implementation procedure

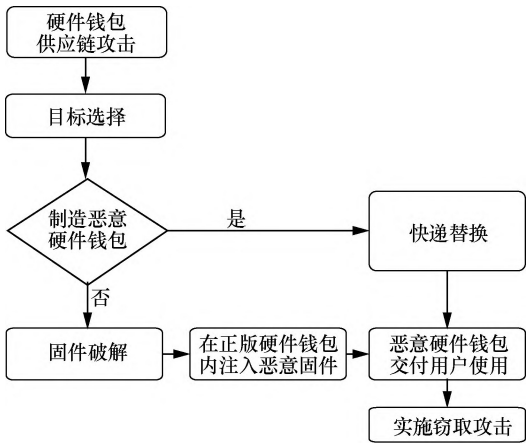

图 11　硬件钱包供应链攻击实施流程

Figure 11　Hardware wallet supply chain attack implementation procedure

3.3.4　私钥泄露威胁

私钥泄露威胁攻击实施流程如图 12 所示。

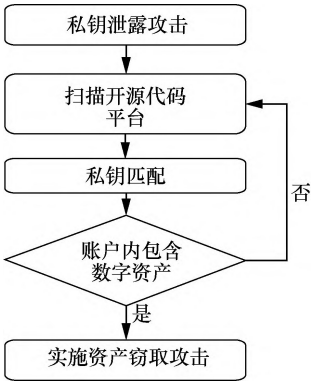

图 12　私钥泄露威胁攻击实施流程

Figure 12　Private key leakage threat attack implementation procedure

3.3.5　远程控制威胁

远程控制威胁攻击实施流程如图 13 所示。

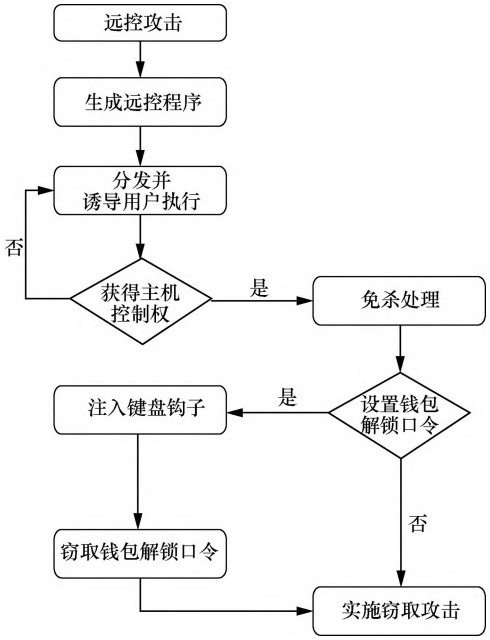

图 13　远程控制威胁攻击实施流程

Figure 13　Remote control threat attack implementation procedure

3.3.6　盲签名威胁

盲签名威胁攻击实施流程如图 14 所示。

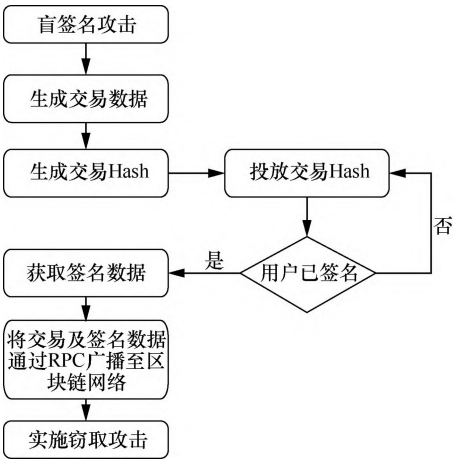

图 14　盲签名威胁攻击实施流程

Figure 14　Blind signature threat attack implementation procedure

表 2 给出了各类威胁在隐蔽性、成功率收益成本比率及攻击实施难度的评级。通过分析与研究掌握各攻击特点发现：降低攻击者收益成本比率，提高攻击实施难度，对高隐蔽的攻击方法进行检测是防范攻击的重要手段。

表 2 威胁分析评级
Table 2 Threat analysis ratings

安全威胁	隐蔽性	成功率	收益成本比率	实施难度
仿冒钓鱼	低	低	低	低
代币恶意授权	中	中	中	中
智能合约漏洞	高	高	高	高
供应链	高	高	高	高
私钥泄露	高	中	中	低
远程控制	中	中	中	中
盲签名	高	中	高	低

3.4 威胁评级

攻击隐蔽性、成功率、收益成本比率及攻击实施的难易程度是对不同类型区块链资产窃取威胁进行评判，设计针对性防御手段的重要指标。

通过对大量利用区块链网络实施的资产窃取攻击案例分析发现：① 攻击隐蔽性越强，攻击实施成功率越高；② 在同等条件下，具备高收益成本比率的攻击方法将优先被敌手所使用；③ 敌手实施攻击所需要的步骤越烦琐复杂，通过攻击所获得收益成本比率越高且攻击手法越隐蔽；④ 私钥窃取类攻击的隐蔽性较高，且用户在资产被盗后难以通过链上交易排查及分析私钥丢失的原因；⑤ 盲签名攻击的实施难度较低，但在隐蔽性及收益成本比率方面具有一定的优势。

4 防御方案

4.1 防御方案设计

本节重点总结学术界针对各类区块链资产窃取威胁所设计的防御方案及所需技术。

4.1.1 仿冒钓鱼威胁防御方案

（1）基于机器学习的钓鱼站点检测方案

利用机器学习算法检测钓鱼站点是帮助用户防范威胁模型 1 所述攻击的主要解决方案：利用机器学习算法，将钓鱼站点检测问题转换为机器学习中的二分类问题[70]，训练模型并对数据进行检测。按照数据收集–模型训练–模型评估–模型测试–数据预测的顺序开展研究。图 15 给出了钓鱼站点检测方案：利用机器学习技术训练识别钓鱼站点，及时向用户发起告警提示。

在数据收集方面，研究人员需要收集钓鱼站点和正常站点数据并做标签。为了使模型更加精确，研究人员通常会选择收集站点域名、站点 DNS 注册信息、站点前端代码、站点 Logo、站点层叠样式表单[71]等，能够帮助模型区分仿冒与合法站点类别的信息。此外，为降低数据复杂度提升运算效率，还需要使用特征提取算法对数据进行预处理。

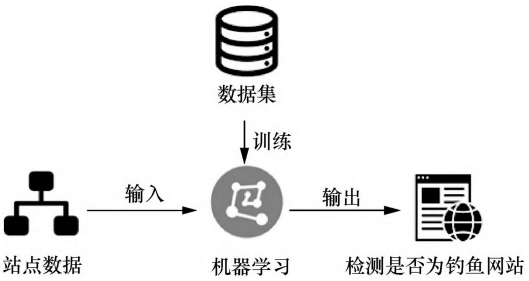

图 15 钓鱼站点检测方案
Figure 15 Phishing site detection scheme

在模型训练方面，研究人员通常会选取多种分类模型对数据进行训练。利用测试数据集对不同模型的检测准确率和精度进行评价。常用的钓鱼站点检测模型主要包括 SVM、KNN、XGB 等，利用上述模型，有研究人员在钓鱼站点检测方面实现了超过 99%的检测准确率[72]，基本满足用户的使用需求。

4.1.2 代币恶意授权威胁防御方案

（1）基于区块链交易数据的代币授权行为检测技术

交易数据检测是区块链钱包在防范代币威胁模型 2 所述攻击的主要解决方案。研究人员通过对以太坊中常用的 ERC20、ERC721 及 ERC1155 代币合约进行解析，提取去中心化应用向用户申请代币授权操作时发起的交易数据特征[73]（如表 1 中 EVM 编码列所示）。在去中心化应用向用户发起符合特征的交易时，向用户发出告警提示：“一旦该授权交易发出并被区块链确认，将会允许被授权地址使用及转移用户持有的数字资产”。

（2）基于访问控制的代币防盗标准

在智能合约代码层面添加访问控制状态信息，在去中心化应用不具备访问控制权限时，禁止调用代币授权方法是从智能合约代码层面防范威胁模型 2 的主要解决方案。

研究人员在对相关标准进行研究后发现，

ERC721 代币在实现时并未考虑资产窃取等安全攻击实例，通过对现有 ERC721 标准合约代码进行修订，如添加锁定、转移两类访问控制权限状态，以帮助代币持有者防范资产恶意授权攻击。研究人员将修订的代币标准更名为 ERC721-G 标准。

当 ERC721-G 标准[30]的数字资产处于“锁定”状态时：去中心化应用无法向用户发起针对 ERC721G 代币的授权请求，代币完全锁定在区块链钱包内。当 ERC721-G 标准的数字资产处于“转移”状态时：允许去中心化应用向用户发起代币授权请求，用户也可将代币转移至任意区块链地址。

（3）基于去中心化仲裁的可追回代币标准

在代币标准合约中添加去中心化仲裁及代币追回逻辑是防范威胁模型 2 所述攻击的解决方案。

研究人员在 ERC20 及 ERC721 标准合约的基础上改进并提出了 ERC20-R 及 ERC721-R 标准[31]：通过引入去中心化第三方仲裁技术帮助用户明确争议资产归属。存在所属权争议的资产将按照仲裁结果发还至经仲裁确认的所有者处。在代币因恶意授权丢失后，用户可利用该标准申请去中心化仲裁，尝试追回被盗资产。图 16 给出了去中心化代币防护方案：利用去中心化代码实现的代币锁定及仲裁逻辑，避免攻击者利用存在所有权争议的资产进行变现。

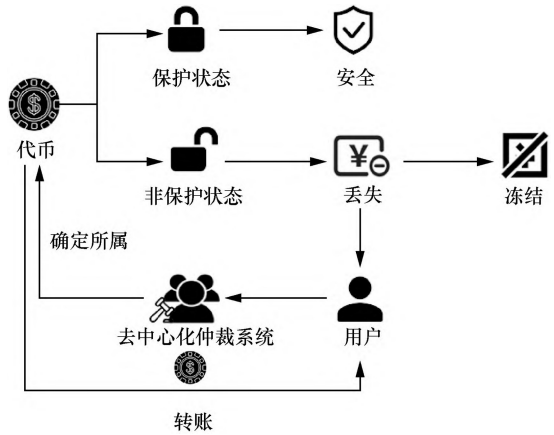

图 16　去中心化代币防护方案

Figure 16　Decentralized token protection scheme

这类防护方案在实践中也存在一些问题，如在技术上无法解决仲裁陪审团成员与敌手合谋对仲裁结果造成的影响。此外，通过逆转区块链交易追回资产的业务逻辑也引发了部分去中心化拥趸对该方案的批评和讨论。

4.1.3　智能合约漏洞威胁防御方案

（1）基于图神经网络的智能合约漏洞检测技术

利用图神经网络检测智能合约存在的漏洞是帮助开发者防范威胁模型 3 所描述攻击的主要解决方案：按照合约代码图生成−正则化处理−使用基于消息传播的神经网络训练检测的顺序开展研究[26]。图 17 给出了智能合约漏洞识别方案：利用深度神经网络对智能合约代码片段抽象形成的智能合约图进行检测，根据结果提醒需要开发者额外检查的智能合约代码片段。

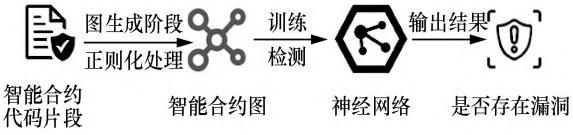

图 17　智能合约漏洞识别方案

Figure 17　Smart contract vulnerability detection scheme

在图生成阶段，通过智能合约数据流和控制流之间的依赖关系，对合约方法调用及变量使用情况进行建模，将智能合约源代码片段转换为智能合约图：点集代表函数名及变量名，边集代表函数执行路径。

在正则化处理阶段，研究人员针对消息传播导致的重要图节点被逐步忽略的问题，通过将节点属性聚合的方式消除部分边缘节点，以提高神经网络运算效率。

在训练阶段，研究人员引入了一种能够对图进行半监督学习的卷积神经网络[74]，配合消息传播算法按序遍历智能合约图的边集，最终生成合约是否包含漏洞的运算结果。

通过使用自动化检测技术对智能合约进行检测，修复相关漏洞能够有效减少因智能合约漏洞所造成的潜在资产损失。

4.1.4　供应链威胁防御方案

（1）基于挑战−应答的供应链攻击防御技术

在硬件钱包初始化时，利用挑战−应答认证技术[75]验证硬件钱包固件完整性是防范威胁模型 4 所述攻击的解决方案。该方案成功避免了用户使用被供应链攻击污染的硬件钱包，并保护了用户资产。图 18 给出了硬件钱包挑战应答方案：利用公钥加解密技术配合挑战方案对钱包固件合法性进行检测。

注入安全验证密钥：在生产硬件钱包时，在

硬件钱包安全芯片内注入仅用于进行固件完整性验证的密钥对。

接收挑战值：在用户激活钱包时，用户需要与 HSM 验证节点建立连接，接收 HSM[76]验证节点使用私钥签名的挑战值，HSM 验证节点使用固件完整性验证公钥加密的一次性随机数。

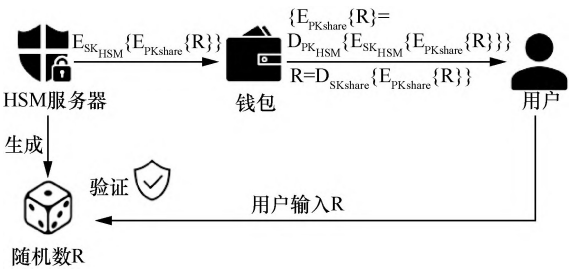

图 18 硬件钱包挑战应答认证方案

Figure 18 Hardware wallet challenge-response authentication scheme

挑战值合法性认证：使用硬件钱包及 HSM 节点公钥对 HSM 签名的挑战值数据合法性进行验证，验证 HSM 节点合法性。

应答值运算：使用硬件钱包的固件完整性验证私钥解密接收的挑战值，得到 HSM 生成的一次性随机数。

应答值一致性比较：将解密后的数据安全传输至 HSM 节点，通过对比一次性随机数与用户发回的返回值以验证节点固件完整性。若认证失败，则意味着用户持有的硬件钱包固件已被篡改。

（2）基于开源仓库及包管理平台数据对比的供应链攻击检测技术

有研究人员在对开源应用分析时发现，开源代码库中的代码与通过包管理工具中分发的代码存在差异时，通常代表程序可能遭受了供应链攻击，需要开发者进行甄别以防范威胁模型 4 所涉及的攻击[77]。

源代码库识别：通过挖掘应用主页中的元数据属性来识别源代码库。

存储库复制及运算：复制存储库并提取主分支中的所有提交数据、代码变更情况。对于向存储库提交的变更，检查变更所涉及的文件，计算文件哈希，并收集文件内容。

利用包管理工具下载分发版本的包：对于包内包含的所有文件，计算哈希值并收集文件内容。

一致性比较：对比存储库及分发版本包内的文件哈希值和内容，检测代码差异，识别潜在的供应链攻击。

4.1.5 密钥泄露威胁防御方案

（1）基于资产隔离的代币防盗技术

基于资产隔离的防盗技术通过帮助用户妥善管理区块链资产，使攻击者通过私钥窃取攻击只能盗用无实际变现价值的测试网资产。

这一方案要求开发者申请专门用于开发去中心化应用的区块链钱包且只允许用户在开发钱包内存储测试网代币。即使私钥因为疏忽被上传至公共代码库，通过私钥也只能盗取不具有任何价值的测试网代币。

通过采用将开发钱包与资产钱包完全隔离的策略，保护用户数字资产安全，图 19 给出了钱包资产隔离防护方案：利用测试钱包进行应用开发，利用资产钱包存储数字资产，以避免私钥因滥用所导致的泄露。

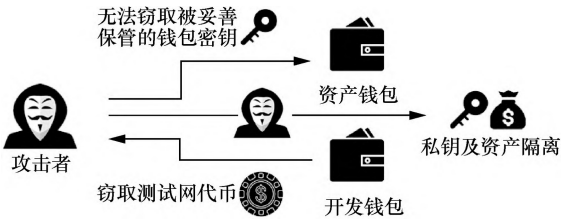

图 19 钱包资产隔离防护方案

Figure 19 Wallet assets isolation protection scheme

4.1.6 远程控制威胁防御方案

（1）基于沙箱的可执行程序行为分析技术

使用沙箱技术对来源不明的可执行程序行为进行分析，是排查异常程序、防范威胁模型 6 所述攻击的主要防护方案。

该方案要求用户优先使用沙箱运行其通过互联网获取的可执行程序，沙箱程序能够记录可执行程序的恶意行为并上报用户。在验证可执行程序不存在任何异常行为的前提下，用户可根据实际需求选择主机中运行可执行程序。

（2）基于反病毒技术的恶意程序识别技术

利用防病毒工具查杀带有恶意特征的可执行程序，而在系统妥善配置防火墙则能够帮助用户主机建立防范恶意流量入侵的防护屏障，增加敌手实施远控攻击的难度。

4.1.7 盲签名威胁防御方案

（1）签名数据合法性检测技术

签名数据检测是区块链钱包软件在防范威

胁模型 7 所述攻击的主要解决方案。研究人员通过对以太坊中常用的签名标准及待签名数据进行解析。在去中心化应用向用户发起符合盲签名特征的请求时，强制向用户发出告警：“签署该消息将威胁资产安全，请谨慎签署”。

（2）基于签名处理函数分析的签名行为识别技术

针对部分智能合约存在对签名数据进行处理的逻辑，有研究人员采用了另一种检测方案：对智能合约的 ABI 及签名处理函数进行解析，在用户执行签名操作前向用户展示签名触发后的资产流向，帮助用户理解签名后其账户内的资产产生的变化，如资产以极低的价格卖出或资产被转移等，进而提醒用户签名数据所导致的潜在风险。图 20 给出了签名合法性及行为检测方案：通过对待签名数据进行解析，判定签名操作是否安全，并向用户发出告警。

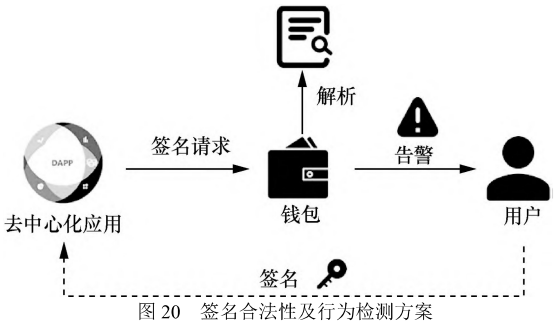

图 20　签名合法性及行为检测方案

Figure 20　Signature legitimacy and behavior detection scheme

4.2　安全教育

通过研究发现，部分保护区块链资产安全的检测技术仍然处于实验阶段，尚不具备大规模使用的能力。这一现象突出了通过安全教育等手段帮助用户建立维护其数字资产安全的认识和技巧的重要性。

在安全教育方面，大多数基于 DAO 治理的教育组织在尝试通过授课、安全教育等方式帮助用户建立防范资产窃取攻击的技巧。

1) 软件定期更新：用户使用的区块链钱包通常为浏览器插件钱包，其安全性依赖于操作系统和浏览器，定期更新操作系统、浏览器、区块链钱包使其保持最新状态是保护数字资产安全的重要技巧，是避免攻击者利用低版本软件漏洞实施攻击的重要手段。

2) 拒绝相信任何通过 Web3 接收的私信消息及数据：在去中心化网络中，用户通常不通过私信这类直接信息交互的方式建立联系，而是通过群聊、论坛等方式建立联系。通过教育使用户拒绝一切通过 Web3 发起的私聊，是防范仿冒钓鱼、远控威胁的重要方法。

5　结束语

近年来，随着区块链技术的发展，国内外涌现出大量公链系统，为用户便捷地访问 Web3 服务，利用公链购买符合个人审美的数字资产、实现价值转移提供了极大的便利。区块链资产具有高流动、易变现等特性，区块链网络具备匿名等特性，为攻击者实施资产窃取攻击提供了极大便利。本文通过对利用区块链网络实施资产窃取的威胁进行分类总结，分析了各类攻击的原理及实施流程，给出了各威胁的评价指标，最终总结了针对各类区块链资产窃取的威胁所设计的防御方案。

参考文献：

[1] VITALIK B. A next-generation smart contract and decentralized application platform[R]. 2014.

[2] ZETZSCHE D A, ARNER D W, BUCKLEY R P. Decentralized finance[J]. Journal of Financial Regulation, 2020, 6(2): 172-203.

[3] WANG Q, LI R, WANG Q, et al, Non-fungible token (NFT): Overview, evaluation, opportunities and challenges[J]. arXiv preprint arXiv:2105.07447. 2021.

[4] BONNEAU J, MILLER A, CLARK J, et al. SoK: research perspectives and challenges for bitcoin and cryptocurrencies[C]//Proceedings of 2015 IEEE Symposium on Security and Privacy. 2015: 104-121.

[5] REBECCA, YANG, . Public and private blockchain in construction business process and information integration[J]. Automation in Construction, 2020, 118: 103276.

[6] ANDOLA N, RAGHAV, YADAV V K, et al. Anonymity on blockchain based e-cash protocols—A survey[J]. Computer Science Review, 2021, 40: 100394.

[7] MUKHOPADHYAY U, SKJELLUM A, HAMBOLU O, et al. A brief survey of cryptocurrency systems[C]//Proceedings of 2016 14th Annual Conference on Privacy, Security and Trust (PST). 2017: 745-752.

[8] HIGBEE A. The role of crypto-currency in cybercrime[J]. Computer Fraud & Security, 2018(7):13-15.

[9] REDDY E, MINNAAR A. Cryptocurrency: a tool and target for cybercrime[J]. Acta Criminologica: African Journal of Criminology & Victimology,2018, 31(3):71-92.

[10] CHENG Z, HOU X, LI R, et al. Towards a first step to understand the cryptocurrency stealing attack on Ethereum[C]//22nd International Symposium on Research in Attacks, Intrusions and Defenses (RAID 2019). 2019: 47-60.

[11] DINGLEDINE R, MATHEWSON N, SYVERSON P. Tor: the second-generation onion router[R]. Naval Research Lab.2004.

[12] ENTRIKEN W, SHIRLEY D, EVANS, et al. Eip-721: Erc-721

non-fungible token standard[S]. Ethereum Improvement Proposals, 2018.
[13] RADOMSKI W, COOKE A, CASTONGUAY P, et al. Eip 1155: Erc-1155 multi token standard[S]. Ethereum, 2018.
[14] ANDRYUKHIN A A. Phishing attacks and preventions in blockchain based projects[C]//Proceedings of 2019 International Conference on Engineering Technologies and Computer Science (EnT). 2019: 15-19.
[15] SALAHDINE F, KAABOUCH N. Social engineering attacks: A survey[J]. Future Internet, 2019, 11(4): 89.
[16] ANDRYUKHIN A A. Methods of protecting decentralized autonomous organizations from crashes and attacks[J]. Proceedings of the Institute for System Programming of the RAS, 2018, 30(3): 149-164.
[17] ATZEI N, BARTOLETTI M, CIMOLI T. A survey of attacks on ethereum smart contracts SoK[C]//Proceedings of the 6th International Conference on Principles of Security and Trust - Volume 10204. 2017: 164-186.
[18] BHARGAVAN K, DELIGNAT-LAVAUD A, FOURNET C, et al. Formal verification of smart contracts: Short paper[C]//Proceedings of the 2016 ACM Workshop on Programming Languages and Analysis for Security. 2016: 91-96.
[19] GURI M. BeatCoin: leaking private keys from air-gapped cryptocurrency wallets[C]//Proceedings of 2018 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). 2019: 1308-1316.
[20] IVANOV N, YAN Q B. EthClipper: a clipboard meddling attack on hardware wallets with address verification evasion[C]//Proceedings of 2021 IEEE Conference on Communications and Network Security (CNS). 2022: 191-199.
[21] HE D J, LI S H, LI C, et al. Security analysis of cryptocurrency wallets in android-based applications[J]. IEEE Network, 2020, 34(6): 114-119.
[22] LIN D, WU J J, YUAN Q, et al. T-EDGE: Temporal weighted MultiDiGraph embedding for ethereum transaction network analysis[J]. Frontiers in Physics, 2020, 8: 204.
[23] CHEN W, GUO X, CHEN Z, et al. Phishing scam detection on ethereum: towards financial security for blockchain ecosystem[C]//IJCAI. 2020:4506-4512.
[24] ZHANG D J, CHEN J Y, LU X S. Blockchain phishing scam detection via multi-channel graph classification[C]//International Conference on Blockchain and Trustworthy Systems. 2021: 241-256.
[25] 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. 2018: 67-82.
[26] ZHUANG Y, LIU Z G, QIAN P, et al. Smart contract vulnerability detection using graph neural network[C]//IJCAI. 2020:3283-3290.
[27] LIAO J W, TSAI T T, HE C K, et al. SoliAudit: smart contract vulnerability assessment based on machine learning and fuzz testing[C]//Proceedings of 2019 Sixth International Conference on Internet of Things: Systems, Management and Security (IOTSMS). 2019: 458-465.
[28] WANG D B, FENG H, WU S W, et al. Penny wise and pound foolish: quantifying the risk of unlimited approval of ERC20 tokens on ethereum[C]//Proceedings of 25th International Symposium on Research in Attacks, Intrusions and Defenses. 2022:99-114.
[29] HE Z Y, LIAO Z, LUO F, et al. TokenCat: detect flaw of authentication on ERC20 tokens[C]//Proceedings of ICC 2022 - IEEE International Conference on Communications. 2022: 4999-5004.
[30] CAO Z, ZHEN Y, FAN G, et al. TokenPatronus: a decentralized NFT anti-theft mechanism[J]. arXiv preprint arXiv:2208.05168.
[31] WANG K L, WANG Q C, BONEH D. ERC-20R and ERC-721R: reversible transactions on ethereum[J]. arXiv preprint arXiv: 2208.00543.
[32] GUAN L, LIN J Q, LUO B, et al. Protecting private keys against memory disclosure attacks using hardware transactional memory[C]//Proceedings of 2015 IEEE Symposium on Security and Privacy. 2015: 3-19.
[33] MALAN D J. CS50 sandbox: Secure execution of untrusted code[C]//Proceedings of SIGCSE '13: Proceeding of the 44th ACM Technical symposium on Computer science education. 2013: 141-146.
[34] OHM M, SYKOSCH A, MEIER M. Towards detection of software supply chain attacks by forensic artifacts[C]//Proceedings of the 15th International Conference on Availability, Reliability and Security. 2020: 1-6.
[35] ZIBIN, ZHENG, . An overview on smart contracts: Challenges, advances and platforms[J]. Future Generation Computer Systems, 2020, 105: 475-491.
[36] PEREZ D, LIVSHITS B. Smart contract vulnerabilities: Does anyone care[J]. arXiv preprint arXiv:1902.06710.
[37] VUJIČIĆ D, JAGODIĆ D, RANĐIĆ S. Blockchain technology, bitcoin, and Ethereum: a brief overview[C]//Proceedings of 2018 17th International Symposium INFOTEH-JAHORINA (INFOTEH). 2018: 1-6.
[38] LEE W M. Using the MetaMask chrome extension[M]// Beginning Ethereum Smart Contracts Programming. Berkeley, CA: Apress, 2019: 93-126.
[39] PANDA S K, SATAPATHY S C. An investigation into smart contract deployment on ethereum platform using Web3.js and solidity using blockchain[C]// Data Engineering and Intelligent Computing. 2021: 549-561.
[40] KHAN A G, ZAHID A H, HUSSAIN M, et al. Security of cryptocurrency using hardware wallet and QR code[C]//Proceedings of 2019 International Conference on Innovative Computing (ICIC). 2020: 1-10.
[41] KOBLITZ N, MENEZES A, VANSTONE S. The state of elliptic curve cryptography[J]. Designs, Codes and Cryptography, 2000, 19(2/3): 173-193.
[42] PERCIVAL C, JOSEFSSON S. The scrypt password-based key derivation function (RFC7914) [S].2016.
[43] PRAITHEESHAN P, XIN Y W, PAN L, et al. Attainable hacks on keystore files in ethereum wallets—A systematic analysis[C]// International Conference on Future Network Systems and Security. 2019: 99-117.
[44] DASGUPTA D, SHREIN J M, GUPTA K D. A survey of blockchain from security perspective[J]. Journal of Banking and Financial Technology, 2019, 3(1): 1-17.
[45] CAI W, WANG Z H, ERNST J B, et al. Decentralized applications: the blockchain-empowered software system[J]. IEEE Access, 2018, 6: 53019-53033.
[46] KIM S K, MA Z E, MURALI S, et al. Measuring ethereum network peers[C]//Proceedings of the Internet Measurement Conference 2018. 2018: 91-104.
[47] PIERRO G A, ROCHA H. The influence factors on ethereum transaction fees[C]//Proceedings of 2019 IEEE/ACM 2nd International Workshop on Emerging Trends in Software Engineering for Blockchain (WETSEB). 2019: 24-31.
[48] ATHULYA A A, PRAVEEN K. Towards the detection of phishing attacks[C]// Proceedings of 2020 4th International Conference on

Trends in Electronics and Informatics (ICOEI)(48184). 2020: 337-343.
[49] GABRILOVICH E, GONTMAKHER A. The homograph attack[J]. Communications of the ACM, 2002, 45(2): 128.
[50] YU B Y, LI P, LIU J W, et al. Advanced analysis of email sender spoofing attack and related security problems[C]//Proceedings of 2022 IEEE 9th International Conference on Cyber Security and Cloud Computing (CSCloud)/2022 IEEE 8th International Conference on Edge Computing and Scalable Cloud (EdgeCom). 2022: 80-85.
[51] SALAHDINE F, KAABOUCH N. Social engineering attacks: A survey[J]. Future Internet, 2019, 11(4): 89.
[52] LI A, LONG F. Detecting standard violation errors in smart contracts[J]. arXiv preprint arXiv:1812.07702.2018
[53] MEHAR M I, SHIER C L, GIAMBATTISTA A, et al. Understanding a revolutionary and flawed grand experiment in blockchain[J]. Journal of Cases on Information Technology, 2019, 21(1): 19-32.
[54] Oxford Analytica. Binance breach underlines risks for crypto ecosystem[R]. Emerald Expert Briefings, 2022.
[55] ABDELLATIF T, BROUSMICHE K L. Formal verification of smart contracts based on users and blockchain behaviors models[C]//Proceedings of 2018 9th IFIP International Conference on New Technologies, Mobility and Security (NTMS). 2018: 1-5.
[56] ROZARIO A M, THOMAS C. Reengineering the audit with blockchain and smart contracts[J]. Journal of Emerging Technologies in Accounting, 2019, 16(1): 21-35.
[57] OHM M, PLATE H, SYKOSCH A, et al. Backstabber's knife collection: A review of open source software supply chain attacks[C]//International Conference on Detection of Intrusions and Malware, and Vulnerability Assessment. 2020: 23-43.
[58] ROBINSON A, CORCORAN C, WALDO J. New risks in ransomware: supply chain attacks and cryptocurrency[J]. Science, Technology, and Public Policy Program Reports.2022.
[59] ARAPINIS M, GKANIATSOU A, KARAKOSTAS D, et al. A formal treatment of hardware wallets[C]//International Conference on Financial Cryptography and Data Security. 2019: 426-445.
[60] ZAHAN N, ZIMMERMANN T, GODEFROID P, et al. What are weak links in the npm supply chain[C]//Proceedings of 2022 IEEE/ACM 44th International Conference on Software Engineering: Software Engineering in Practice (ICSE-SEIP). 2022: 331-340.
[61] MELI M, MCNIECE M R, REAVES B. How bad can it git? characterizing secret leakage in public github repositories[C]//NDSS.
[62] GUTOSKI G, STEBILA D. Hierarchical deterministic bitcoin wallets that tolerate key leakage[C]//International Conference on Financial Cryptography and Data Security. 2015: 497-504.
[63] RAHIM R, NURDIYANTO H, SALEH A A, et al. Keylogger application to monitoring users activity with exact string matching algorithm[J]. Journal of Physics: Conference Series, 2018, 954: 012008.
[64] BLOCKI J, HARSHA B, ZHOU S. On the economics of offline password cracking[C]//Proceedings of 2018 IEEE Symposium on Security and Privacy (SP). 2018: 853-871.
[65] WANG D, CHENG H B, WANG P, et al. Zipf's law in passwords[J]. IEEE Transactions on Information Forensics and Security, 2017, 12(11): 2776-2791.
[66] ZHANG X, DU W L. Attacks on Android clipboard[C]//International Conference on Detection of Intrusions and Malware, and Vulnerability Assessment. 2014: 72-91.
[67] LI Y J, LI H W, LV Z Z, et al. Deterrence of intelligent DDoS via multi-hop traffic divergence[C]//Proceedings of the 2021 ACM SIGSAC Conference on Computer and Communications Security. 2021: 923-939.
[68] DO XUAN C, DAO M H. A novel approach for APT attack detection based on combined deep learning model[J]. Neural Computing and Applications, 2021, 33(20): 13251-13264.
[69] POINTCHEVAL D, STERN J. Provably secure blind signature schemes[M]//Lecture Notes in Computer Science. 1996: 252-265.
[70] BASIT A, ZAFAR M, LIU X, et al. A comprehensive survey of AI-enabled phishing attacks detection techniques[J]. Telecommunication Systems, 2021, 76(1): 139-154.
[71] MAO J, BIAN J D, TIAN W Q, et al. Phishing page detection via learning classifiers from page layout feature[J]. EURASIP Journal on Wireless Communications and Networking, 2019(1): 43.
[72] CHEN Y H, CHEN J L. AI@ntiPhish—Machine learning mechanisms for cyber-phishing attack[J]. IEICE Transactions on Information and Systems, 2019, E102.D(5): 878-887.
[73] ANSARI K H, KULKARNI U. Implementation of ethereum request for comment (ERC20) Token[C]//Proceedings of the 3rd International Conference on Advances in Science & Technology (ICAST).2020.
[74] KIPF T N, WELLING M. Semi-supervised classification with graph convolutional networks[J]. arXiv preprint arXiv:1609.02907.2016.
[75] GILAD Y, HERZBERG A, SHULMAN H. Off-path hacking: The illusion of challenge-response authentication[C]//Proceedings of IEEE Security & Privacy. 2013: 68-77.
[76] SEOL J, JIN S, LEE D, et al. A trusted IaaS environment with hardware security module[J]. IEEE Transactions on Services Computing, 2016, 9(3): 343-356.
[77] VU D L, PASHCHENKO I, MASSACCI F, et al. Towards using source code repositories to identify software supply chain attacks[C]//Proceedings of the 2020 ACM SIGSAC Conference on Computer and Communications Security. 2020: 2093-2095.

[作者简介]

余北缘（1996– ），男，北京人，北京航空航天大学博士生，主要研究方向为网络应用安全。

任珊瑶（1999– ），女，河南周口人，北京航空航天大学博士生，主要研究方向为空天信息网络安全。

刘建伟（1964– ），男，山东莱州人，博士，北京航空航天大学教授、博士生导师，主要研究方向为密码学与网络安全。