

区块链矿池网络及典型攻击方式综述

倪雪莉^{1,2,3}, 马卓^{1,2}, 王群^{1,2}

(1.江苏警官学院计算机信息与网络安全系,江苏 南京 210031; 2.江苏省电子数据取证分析工程研究中心,江苏 南京 210031;
3.南京信息工程大学计算机学院、网络空间安全学院,江苏 南京 210044)

摘要: 区块链网络是构建在TCP/IP体系之上的一类覆盖网络,在不依赖可信中心服务节点和可信信道的前提下,为分布式环境中互不信任的节点之间就账本数据达成一致性提供通信保障。随着区块链挖矿技术的发展,尤其是基于ASIC、GPU等硬件的工作量证明共识挖矿技术在比特币(BTC)、以太坊(ETH)、莱特币等主流加密货币中的应用,支撑矿池挖矿方式的矿池网络引起了研究者的广泛关注,因此归纳并总结区块链矿池网络及其安全方面的研究成果对于追踪区块链技术研究进展和拓展区块链应用范围具有重要价值。首先,结合传统对等(P2P)网络组网模式,针对BTC、ETH和超级账本等典型应用场景,梳理区块链P2P网络运行机制和特点。然后,介绍矿池、矿场以及矿池网络概念,分析矿池网络的组成要素以及GetWork、GetBlockTemplate和Stratum典型矿池网络协议的工作原理。接着,重点讨论针对矿池网络的自私挖矿、跳池、扣块、空块等典型攻击方式的实现过程,并提出相应的防范方法。最后,对矿池网络的未来发展方向进行展望。

关键词: 区块链; 对等网络; 矿池网络; 共识机制; 网络攻击

中图分类号: TP309

文献标志码: A

DOI:10.19678/j.issn.1000-3428.0068203

Overview of Blockchain Mining Pool Networks and Typical Attack Modes

NI Xueli^{1,2,3}, MA Zhuo^{1,2}, WANG Qun^{1,2}

(1.Department of Computer Information and Cybersecurity, Jiangsu Police Institute, Nanjing 210031, Jiangsu, China;
2.Jiangsu Electronic Data Forensics and Analysis Engineering Research Center, Nanjing 210031, Jiangsu, China;
3.School of Computer Science, Nanjing University of Information Science and Technology, Nanjing 210044, Jiangsu, China)

[Abstract] The blockchain network is a type of overlay network constructed on a Transmission Control Protocol/Internet Protocol(TCP/IP) system. It provides communication support to ensure the consistency of ledger data between mutual distrust nodes in a distributed environment without relying on trusted central-service nodes and trusted channels. Owing to the development of blockchain mining technology, particularly the application of Proof of Work (PoW) consensus mining technology based on Application-Specific Integrated Circuit (ASIC), Graphics Processing Unit (GPU), and other hardware used in mainstream cryptocurrencies such as Bitcoin(BTC), Ethereum(ETH), and Litecoin (LTC), researchers have extensively investigated the mining pool network, which supports the mining pool mode. However, results pertaining to the mining pool network and its security are scarce. Therefore, the abovementioned results must be summarized and synthesized to monitor the progress of blockchain technology research and expand blockchain application research. First, based on the networking mode of the classical Peer-to-Peer(P2P) network, this study reviews the operating mechanism and characteristics of the blockchain P2P network based on typical application scenarios such as BTC, ETH, and Hyperledger. Second, this study introduces the concept of mining pool, mining field, and mining pool network, as well as analyzes the components of the mining pool network and the operating principle of typical mining pool network protocols such as GetWork, GetBlockTemplate, and Stratum. Subsequently, the implementation process of typical attack modes such as selfish mining, pool hopping, block withholding, and empty block attacks against the mining pool network is discussed, and the corresponding prevention methods are proposed. Finally, future developments for the mining pool network are recommended.

[Key words] blockchain; Peer-to-Peer(P2P) network; mining pool network; consensus mechanism; network attack

0 引言

区块链技术因比特币(BTC)在全球的持续升温而引起广泛关注,因其具有的去中心化、自治性、开放性、匿名性、防篡改等特征^[1],不但成为构建各类

加密数字货币的基石,而且应用已向着金融、物联网、数字版权保护、医疗、政务等众多领域快速拓展,并正在对传统行业产生冲击和变革。

比特币创造了去中心化加密数字货币的神话,区块链技术确保了比特币在发行、应用、管理等各个

收稿日期:2023-08-10 修回日期:2023-10-12

基金项目:国家自然科学基金(62272203);江苏省市场监督管理局科技计划项目(KJ21125027)。

通信作者 E-mail:nixueli@jspi.edu.cn

环节的安全性。共识机制^[2-3]保证了区块链系统中数据的一致性和不可篡改性,比特币系统利用基于哈希函数求解问题的工作量证明(PoW)^[4]共识算法实现了交易的安全性。在基于PoW共识的区块链系统中,矿工(挖矿节点)以消耗算力解决特定哈希函数的求解问题来生成新区块,此过程称为挖矿。当某一矿工挖到一个新区块时,为了获取系统的奖励(当前为6.25 BTC)和手续费(打包进该区块的所有交易交纳的手续费),需要将该区块尽快广播给其他矿工,当其他正在挖矿的矿工接收到一个新区块时,立即对其合法性进行验证,验证通过后将其链接到正在挖矿的区块后面,并在该区块基础上继续挖下一个区块。采用PoW共识算法的挖矿机制,其挖矿难度随网络中算力的增加不断上升,独立矿工受算力限制挖矿成功的概率急剧下降^[5]。在此情况下,为了获得稳定的挖矿收益,原来独立的矿工在相应协议的支持下有机组织起来,形成了共同参与挖矿的矿池。

矿池的出现打破了区块链已有的完全去中心化机制,出现了物理上的局部中心化网络或逻辑上的中心化扩展网络。虽然代表矿池的中心化网络对外仍然以单一节点(矿池节点)呈现,但矿池网络内部不同节点之间需要在矿池网络协议的协调下有序工作。远远超出单一矿工节点算力的矿池的出现破坏了传统PoW算法的公平性,进而影响了区块链的安全性^[6],攻击者借助于区块链固有运行机制对矿池环境的不适应性以及区块链网络存在的安全风险,攻击矿池网络甚至威胁整个区块链系统的安全。

近年来,随着区块链技术的发展和应用领域的不断拓展,学术界和工业界加快了区块链关键技术的研究步伐和应用创新进程,但系统分析区块链网络尤其是矿池网络的研究成果较少且不聚焦。在国外研究方面:文献[7]提出一个用于分析矿池中奖励共享的概念框架,该框架以矿池中报告的有效工作量证明(share)为中心,通过提出的绝对再分配和相对再分配两个新的标准优化了矿池矿工的奖励共享机制;文献[8]针对PoW矿池挖矿可能存在的运营成本超出挖矿回报的风险,利用破产理论和保险风险分担方法对矿池风险进行研究,并提出几个明确的风险计算公式;文献[9]针对矿池对区块链去中心化机制产生的负面影响,提出一个优化分析模型和可降低风险的计算工具。在国内研究方面:文献[10]在对矿池结构进行分析的基础上,提出一种衡量矿工计算效率的数值模型(MENM)以及基于该模型实现对矿池中单个矿工难度的性能优化机制(DDCT),以提高矿池效率;文献[11]针对矿池算力和奖励机制对矿工的影响,提出一个基于风险决策准则的矿池选择算法;文献[12]通过对基于PoW共识机制矿池挖矿困境的博弈均衡分析,提出利用零行列式(ZD)来优化挖矿策略的具体算法,并通过仿

真方法验证了算法的有效性。通过对以上成果的梳理分析可以看出,随着加密数字货币的迅猛发展,针对矿池挖矿的研究成为当前及未来的研究热点和重点。现有研究主要基于矿池的经济激励机制,就挖矿中的收益分配提出更加优化的算法和策略,而系统分析矿池网络体系结构和协议的成果较少。

矿池网络是在区块链对等(P2P)网络基础上通过矿池协议构建的一个实现众多矿工联合挖矿的分布式网络,矿池网络同时面临传统P2P网络和专门针对矿池网络的安全威胁。本文的工作主要集中在:1)对区块链P2P网络进行系统分析,这是区块链网络的核心;2)详细讨论了矿池网络的组成及主要协议,这是分析矿池挖矿的关键;3)对矿池网络中存在的典型安全攻击方式进行探讨,这是有效保障和系统掌握矿池挖矿技术的基础。在此基础上,对矿池网络的未来发展进行展望。

1 区块链 P2P 网络

图1给出了矿池网络的研究架构,本节重点对区块链P2P网络进行分析。在区块链系统中,P2P网络是实现不同节点之间通信的基础设施,也是构建矿池网络的基础平台。P2P网络是构建在TCP/IP体系之上的覆盖网络^[13],而矿池网络是构建在P2P网络之上的扩展网络,P2P网络是矿池网络的基础。

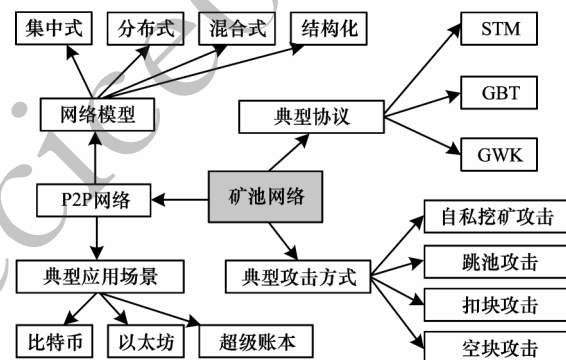


图1 矿池网络的研究架构

Fig.1 Research architecture of mining pool network

1.1 P2P 网络模型

在P2P网络中,根据通信需要每一个节点的身份可在客户端与服务器之间进行动态转换。结合P2P网络技术和应用发展,考虑到P2P网络中节点频繁加入和退出这一特征,本节重点从网络服务过程中的路由选择策略设计出发,主要针对新节点加入后邻居节点的发现机制,将P2P网络模型分为集中式、分布式、混合式、结构化4种类型进行比较研究。

集中式模型是为了适应互联网多媒体应用而较早出现的P2P网络模型,是一种中心化的网络服务模式。集中式P2P网络模型如图2(a)所示,信息索引服务器中保存着资源节点的索引信息(主要包括

节点 IP 地址、资源访问端口、资源名称等),用户通过信息索引服务器查询到所要访问的资源地址后,再点对点传输资源内容。如图 2(b)所示,分布式模型是一种节点之间按需动态连接的随机 P2P 网络模型,新节点加入后的邻居发现是分布式模型需要重点解决的问题,以比特币系统为例,新节点的发现主要采取 3 种方式:1)采用 DNS 查询(由比特币社区成员维护 DNS 种子,如 dnsseed.bluematt.me、seed.bitcoinstats.com 等);2)采用硬编码方式将一些稳定节点作为种子提供给新节点;3)采用消息泛洪方式将要查询的内容发送到整个网络,直至找到所需的内容为止,其中可采用生存时间(TTL)来限制消息在网络中的传播范围。如图 2(c)所示,混合式模型是集中式和分布式模型的混合体,网络中的节点由超级节点(SN)和普通节点组成,其中超级节点为新节点加入提供服务,新节点选择一个能够提供优质服务的超级节点作为其父节点。结构化模型也是一

种分布式模型,但如图 2(b)所示的分布式模型中的节点组织具有随机性,代表的是一种随机网络,而结构化模型中的所有节点是按照特定结构(如树状结构、环状结构等)进行有序管理。分布式哈希表(DHT)^[14]是分布式计算系统中的一种类型,主要用于创建各种点对点通信服务。DHT 作为一种分布式数据库,用 Key/Value 对来存储数据,例如用 Key 存放文件名,用 Value 存放保存该文件的节点 IP 地址,节点可以利用 Key 在数据库中查找对应的 Value 值。DHT 的具体实现有多种方式,如图 2(d)所示的是基于环形 DHT 的结构化模型,其中每个节点只知道与其相连的前后节点的信息。

为了便于对比分析,表 1 对 4 类模型分别从中心化程度、优缺点、典型应用等方面进行比较。需要说明的是:表 1 中的中心化程度主要针对节点之间的路由发现过程,而 P2P 网络中的数据传输仍然使用分布式环境中的去中心化机制。

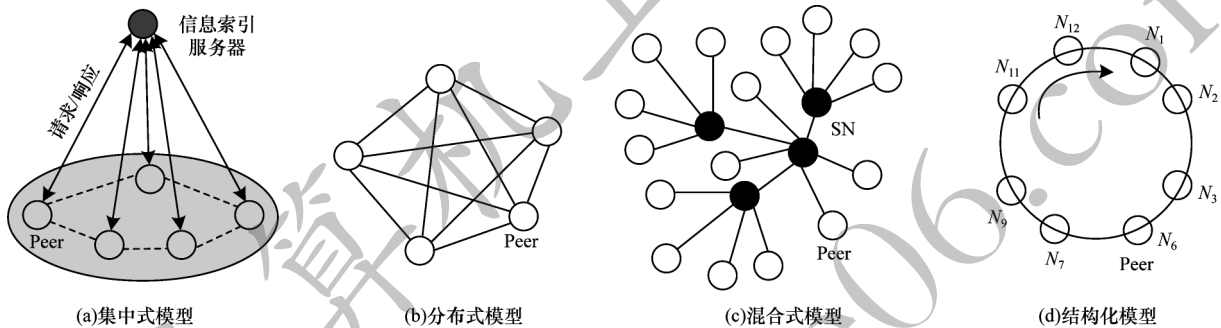


图 2 P2P 网络的 4 类典型模型
Fig.2 Four typical models of P2P networks

表 1 不同 P2P 网络模型的主要性能比较

Table 1 Comparison of the main performance of different P2P network models

类型	中心化程度	优点	缺点	典型应用
集中式	中心化	结构简单,实现容易	容易存在性能瓶颈和单点故障	Napster ^[15]
分布式	去中心化	具有较好的可扩展性,不存在结构上的性能瓶颈和单点故障	消息传递的可控性差,容易形成泛洪循环及响应消息风暴	比特币 ^[16] 、Gnutella ^[17]
混合式	中心化与去中心化结合	可避免大规模泛洪,组网灵活且服务高效,实现难度小	超级节点容易成为网络攻击的目标	Gossip ^[18] 、KaZaA ^[19] 、超级账本 ^[20]
结构化	去中心化	具有良好的可扩展性,资源定位快速,查询便捷	网络容纳的节点数量受所使用的哈希函数限制,节点信息列表的维护占用资源多	Chord ^[21] 、CAN ^[22] 、Kademlia ^[23] 、以太坊 ^[24]

1.2 区块链系统中的 P2P 网络

目前,区块链的主流应用主要集中在公有链中的比特币和以太坊以及联盟链中的超级账本,本节主要针对以上 3 种典型应用场景,重点从节点发现、节点功能、信息交互等方面分析 P2P 网络的特征。

1.2.1 比特币系统中的 P2P 网络

比特币系统中的 P2P 网络构建在 TCP 协议上,信息在节点之间采用明文方式传输。在新节点加入后,主要通过 DNS 种子、硬编码种子节点和消息泛洪 3 种方式发现邻居节点,一个全新的节点可以通过启用 DNS 种子查询机制从 DNS 服务器处获得特定节点的信息,也可以在节点启动时自动加载硬编

码种子节点信息。当节点接入后会将发现的邻居节点地址信息以 LevelDB 格式保存在本地 peers.dat 数据库中,当节点启动时由 address manager 命令载入。另外,当新节点加入网络后,可以通过 Net.AdvertiseLocal()命令以“推”的方式将自己的地址信息推送给其他节点,也可以通过 Net.GetAddresses()命令以“拉”的方式从邻居节点获取地址以扩充自己的地址库。

目前,出于 IP 地址匮乏和安全需要,大部分机构的内部网络使用私有 IP 地址,在网络出口处通过网络地址转换(NAT)服务实现私有 IP 地址与公用 IP 地址之间的映射。比特币系统使用了通用即插即用

(UPnP)协议实现内外网节点之间的通信。

在区块链系统中,每个P2P网络节点分别是承担不同功能的一类特殊计算机,是实现区块链分布式账本技术、去中心化机制和保证区块链系统安全性与可靠性的基础。比特币系统中的节点提供了钱包、矿工、完整区块链、网络路由4类典型功能,其中所有P2P网络节点都具有网络路由功能,另外,将同时拥有4类功能的节点称为比特币核心。全节点拥有完整的区块链账本数据,能够独立校验区块链上的所有交易并实时更新数据。轻量级节点或简易支付验证(SPV)^[25]节点只存储了区块链头数据。比特币核心钱包是全节点,其他大部分钱包都是轻量级节点。独立矿工是存储了完整区块链数据的矿工。

1.2.2 以太坊系统中的P2P网络

以太坊的许多开发思想和实现思路来源于比特币,其中以太坊系统中的P2P网络也是在借鉴了比特币网络基础上的进一步优化和改进。出于安全考虑,以太坊系统中的P2P网络采用了安全加密方式。

以太坊是基于DHT技术的结构化P2P网络,通过Kademlia(简称为Kad)协议来维护每个节点列表。具体而言,Kad网络使用DHT来定位资源,通过共同维护的路由表实现在分布式环境中快速准确地定位目标节点。当使用UDP协议定位到目标节点后,再通过TCP协议传输数据,而且数据在传输过程中经过了加密处理。新节点使用类似于比特币系统中的硬编码种子方式接入P2P网络,在节点接入网络后,会将发现的节点以LevelDB格式保存在本地的地址数据库中^[26],在节点启动时使用LoadSeedNodes()方式连同种子节点一并载入,形成较为完整的路由信息表^[27]。但是,与比特币系统不同的是,Kad网络的每个节点都拥有全网唯一的节点ID,所以以太坊中不存在节点之间用于广播地址信息的泛洪机制。

根据2023年7月Ethernodes网站统计,国内以太坊节点数仅有8个,仅占全球的0.1%,如此少的节点增加了国内以太坊用户区块同步的时间。为了解决这一问题,以太坊中文技术社区EthFans曾发起“星火节点计划”,希望国内对以太坊项目感兴趣的组织和个人能够运行超级节点。EthFans会将所有加入该计划的超级节点列表信息生成一个static-nodes.json格式的静态节点文件,用户节点只需要将该静态节点文件加入个人钱包就可以连接到超级节点,加快区块的同步速度。

与比特币系统一样,以太坊节点主要负责交易和区块的接收与验证、交易处理、挖矿、共识、路由等功能,主要分为全节点、轻节点和归档节点3种类型。全节点拥有完整的区块链账本信息,具备对交易的有效性进行独立验证的能力。矿工必须是全节点。轻节点只需要存储区块头数据,以最少的状态信息来发送和传递交易数据。归档节点在全节点的基础上,还存储了每个区块的高度值等状态信息,以便于快速定位到某个指定的区块。

1.2.3 超级账本中的P2P网络

比特币和以太坊是加密数字货币的典型代表,超级账本的出现使区块链技术开始应用于更广泛的领域,尤其为各类企业级应用提供了新的解决方案。本节以Hyperledger Fabric为例进行分析。Fabric是一个支持准入机制的分布式账本方案开发平台,通过基于模块化架构的共识算法、加密机制、智能合约、身份认证等可扩展组件,为不同复杂场景中的企业级应用提供了一个通用的底层基础服务框架。

Fabric使用Gossip协议^[28-29]实现P2P网络节点之间的通信,该P2P网络构建在HTTP/2之上。Gossip协议的设计灵感来自传染病感染和社会谣言传播机制,即在复杂的环境中通过消息的随机传播实现最终的一致性。Gossip协议的主要特征为:在一个网络域内,其中一个节点在接收到一条信息后,会将该信息发送给随机选择的 k 个节点,持续此过程,直至所有节点中的信息达成最终一致。此过程虽然显得混乱,而且会产生大量冗余信息,但可以确保网络域内各节点对某一时间点之前的信息在一定时间内达成最终的一致。在Fabric中,Gossip协议负责发现新节点、更新节点列表、去除离线节点等操作。由于Fabric主要提供企业级服务,而企业级网络中一般拥有一套较为规范的用户管理系统,因此Gossip协议为每个节点提供了一个配置文件来配置节点启动后可联系的其他节点信息,而没有使用比特币和以太坊中的种子节点和泛洪机制。

在Fabric 1.0中,根据实现功能的不同,可以将节点主要分为排序(Orderer)、背书(Endorser)和记账(Committer)节点,不同节点之间的操作流程示意图如图3所示(彩色效果见《计算机工程》官网HTML版,下同),为描述方便,同类节点在图中仅标出1个。

1)背书请求。客户端(Client)产生交易,并用自己的私钥对交易进行签名,然后将交易和对应的签名信息按规定格式打包后发送给背书节点。

2)背书验证。背书节点对交易信息的身份合法性和交易内容的正确性进行验证,通过验证后,背书节点用自己的私钥对背书结果进行背书签名,然后按照规定格式打包后返还给客户端。

3)交易提交。客户端在收到背书结果后验证其正确性,验证通过后对交易和背书结果进行签名,然后打包发送给排序节点。

4)交易打包。排序节点验证客户端签名的合法性,验证通过后对交易进行排序(在交易量较大的Fabric系统中,可采用Kafka^[30]集群对交易进行排序),当满足出块策略(如达到出块时间、交易数量达到了出块要求等)时,则将交易打包进区块,并对区块进行签名后发送给记账节点。

5)节点记账。记账节点在接收到区块数据后,对区块以及区块中的交易进行验证,其中交易验证主要验证交易是否满足背书策略以及交易的读写集版本是否正确等。在验证通过后,执行交易内容,然后将区块链接到本地区块链。

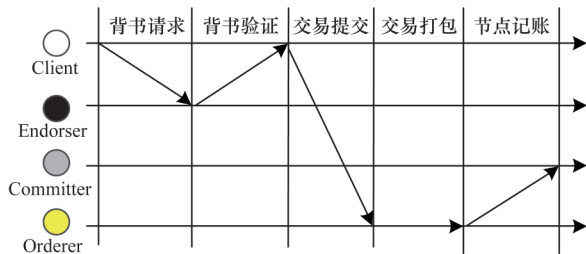


图 3 Fabric 中节点之间的信息交互流程
Fig.3 Procedure of information interaction between nodes in a Fabric

在以上操作过程中,Gossip 协议负责除客户端

之外的其他节点之间的通信,实现从单一源节点到多个目标节点之间数据的高效分发,同时在后台实现不同节点之间的数据同步,而且可以处理网络中的拜占庭问题和网络分区,并能够适应节点频繁加入和退出网络的需要。

在 P2P 网络中,衡量网络性能的主要指标体现在通信协议(TCP 或 UDP)、是否采用加密机制、节点发现机制、节点之间的组网方式以及节点加入系统时的准入机制(是否需要进行身份验证)等方面。为便于系统掌握 P2P 网络的运行机理及特点,表 2 对 3 种典型应用场景中 P2P 网络的主要性能进行综合比较。

表 2 3 种典型应用场景中的 P2P 网络主要性能比较

Table 2 Comparison of the main P2P network performance in three typical application scenarios

主要性能指标	比特币	以太坊	超级账本
通信协议	TCP	TCP/UDP	TCP/UDP
是否加密	非加密网络	加密网络	加密网络
节点发现机制	DNS 种子、硬编码种子、泛洪	DNS 种子、硬编码种子	配置文件
组网方式	随机网络	Kad 网络	混合网络
节点准入机制	无准入机制	无准入机制	有准入机制

2 矿池网络

2.1 矿池、矿场与矿池网络

矿池是一个由多个独立矿工(或矿机)组成的专用网络,目的是通过联合单个矿工的算力共同参与挖矿过程^[31-32]。为了进一步降低挖矿成本,提高挖矿效率,可以将一定数量的矿机集中在一起(如一个设备机房)进行管理,从而形成矿场。矿池是一个逻辑上的集合,组成矿池的矿机可以分布在不同的地理位置甚至是不同地区或国家,矿工只需要经申请注册后就可以加入矿池,并在矿池网络协议的协调下进行挖矿。矿场是一个物理上的集合,组成矿场的矿机需要集中在一个相对固定的地方进行统一管理。

随着 BTC、以太坊(ETH)、莱特币(LTC)、泰达币(USDT)等加密数字货币的全球影响力不断增强,全网的算力也在快速提升,单一矿工在算法竞争中胜出的可能性逐渐减小。在此情况下,独立矿工倾向于加入矿池,将众多节点的算力进行合并运行,从而形成矿工联盟,以抱团挖矿的形式减少收入差距并获得相对稳定的挖矿收益。在此机制中,不论单个节点的算力大小,只要能够加入矿池参与共同挖矿,都可以根据对矿池资源的整体贡献度来获得收益。以比特币系统为例,目前主要的矿池有 BTC.com、Poolin、AntPool、F2Pool 等。

区块链系统中的挖矿是指节点根据共识算法生成区块的过程,凡是参与挖矿的节点都称为矿工。在基于算力竞争的区块链系统中,超强的全网算力

竞争有限的区块记账权,致使单个设备或有限的算力在竞争中获得记账奖励的机会微乎其微。以比特币系统为例,系统每 10 min 生成 1 个区块,成功挖出该区块的矿工将获得一定数额的比特币(当前为 6.25 BTC)奖励,矿工获得奖励的概率与设备算力的大小成正比。在此情况下,当算力相差不大的众多矿工竞争数量极其有限的区块记账权时,成功概率几乎接近于 0。在众多矿工联合形成矿池后,会在矿池中确定一位矿池管理员(矿池管理员会收取一定比例的手续费),在挖到区块后,首先将出块奖励保存于代表矿池拥有者的比特币钱包,然后由该矿池管理员负责对所获得的奖励根据贡献度进行再次分配。在此过程中,每个矿工无论是否挖出了有效区块,都会得到相应的奖励,实现挖矿过程的利益均沾。在矿池挖矿过程中,矿池管理员会向每个参与挖矿的矿池矿工下发一个难度值低于全网难度值的工作量,矿工在求得该 share 后提交给矿池管理员,再由矿池管理员验证该 share 是否满足全网难度值证明,因为满足低难度值的 share 有可能满足全网难度值证明。在此过程中,当矿工提交的低难度值证明 share 不符合全网难度值证明要求时,其结果对矿池挖矿是没有意义的,只能作为矿池管理员评估其工作量的依据。

矿池网络是利用相关协议和管理方式构建在区块链上的分布式系统,基于功能实现,矿池网络主要由位于中心节点的矿池服务器和分布在矿池服务器周边的众多矿池矿工组成。矿池服务器是整个矿池

网络的核心,一方面负责与矿池矿工联系进行联合挖矿,另一方面负责与矿池网络之外的其他区块链节点进行通信,共享挖矿信息,参与挖矿竞争。例如,当矿池挖出一个区块后,需要通过矿池服务器尽快向矿池网络之外的全网其他节点进行广播,以便获得区块的记账权进而获得系统的奖励。在矿池网络中,矿池矿工和矿池服务器之间的通信并没有使用区块链系统(如比特币、以太坊等)中的 P2P 网络协议,而是使用专门开发的矿池网络协议。但是,作为全节点的矿池服务器在与区块链系统中的其他节点(如独立矿工、其他矿池服务器等)进行通信时使用通用的区块链 P2P 网络协议或专门用于加快区块在不同矿工或矿池服务器之间传播的比特币中继网络^[33]。矿池网络示意图如图 4 所示。

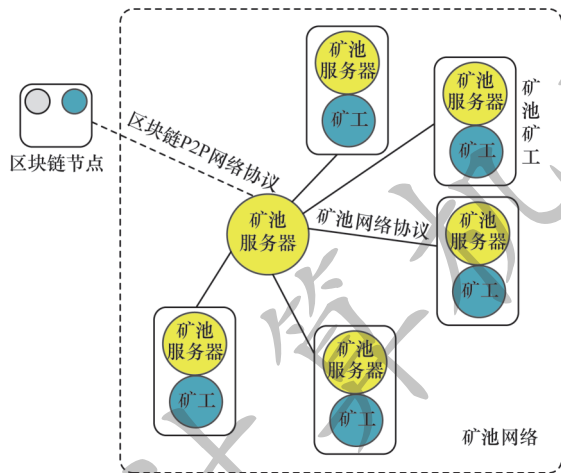


图 4 区块链矿池网络示意图

Fig.4 Schematic diagram of blockchain mining pool network

2.2 矿池网络协议

矿池通过专有的矿池网络协议来协调矿工之间的操作,动态调用并分配各矿工提供的资源,矿工在建立矿池账号后将利用该账号将矿机连接到矿池服务器。当矿机在线运行挖矿程序时,需要实时保持与矿池服务器之间的连接以及与其他矿工之间操作上的同步。常用的矿池协议包括 GetWork(简称为 GWK)协议、GetBlockTemplate(简称为 GBT)协议和 Stratum(简称为 STM)协议。

2.2.1 GetWork 协议

挖矿是一个算法运算过程,对于 PoW 共识算法来说是反复执行哈希函数并检测执行结果的过程。区块链系统中的每一个区块由区块头和区块体两部分组成,其中区块体中打包着一笔笔交易,再将由按序排列的交易最后生成的哈希 MerkleRoot 保存到区块头指定的字段,比特币系统的区块头除 MerleRoot 外,还包括 Version、PrevBlock、Time、Bits、Nonce 共 6 个字段,每个字段的具体定义如表 3 所示。

表 3 比特币系统的区块头组成

Table 3 Block header composition of the Bitcoin system		
字段名	大小/Byte	说明
MerkleRoot	32	由打包进本区块的所有交易构造的 Merkle 树根
Version	4	版本号,反映系统的共识机制
PrevBlock	32	父区块头的哈希值,用于建立与父区块的连接
Time	4	以 s 为单位的 Unix 时间戳
Bits	4	本区块难度,每 2 016 个区块调整 1 次
Nonce	4	介于 0~2 ³² 的随机数

在比特币区块头的 6 个字段中,Version、PrevBlcok 和 Bits 字段相对固定,矿工可以自由调整的 3 个字段分别是 MerkleRoot、Time 和 Nonce,每一次挖矿的实质就是对区块头的 80 Byte 连接进行 2 次 Hash 256 运算,其值如果小于难度对应的目标值,将挖出新区块。

CPU 挖矿利用客户端远程过程调用(RPC)接口 Setgenerate 控制挖矿。矿工首先初始化区块头的各字段值,然后计算 Hash 值并验证结果,如不符合条件则 Nonce 自增,接着再计算和验证,如此重复。在进行 CPU 挖矿时,Nonce 提供的 4 Byte 搜索空间完全能够满足遍历要求。在 GPU 运算 SHA 256 双哈希时,仅调整 Nonce 值无法满足 PoW 算法的出块时间要求,因此需要对 Time 和 Nonce 值进行交替调整。

GPU 挖矿使用 GetWork 协议^[34],通过该协议实现了挖矿程序与客户端的分离,即数据与计算之间相互分开。GetWork 协议的核心思想是:由节点构造区块,然后将区块头数据交给挖矿程序,由挖矿程序遍历 Nonce 进行挖矿,在找到符合难度要求的 Nonce 值后交给节点进行验证,节点提取 Nonce 和 Time 值对区块进行验证,验证通过后立即向全网广播,尽快获得该区块的记账权,进而获得系统奖励。在一次遍历结束后,调用 GetWork 协议,节点重新构造新区块,并重复上述过程。可以看出,在使用 GetWork 协议组成的矿池中,矿工只拥有新构造区块的 80 Byte 的头信息,而没有完整的区块链账本数据和待确认的交易数据,所以 Version、PrevBlock、Bits、MerkleRoot 这 4 个字段必须由客户端节点提供,挖矿程序主要是递增遍历 Nonce,需要时再调整 Time 值。

由于矿机需要频繁调整 RPC 接口,与当前矿机快速提升的挖矿速度之间产生较大反差,因此比特币、莱特币等系统节点已经用更高效的 GetBlockTemplate 协议来替代 GetWork 协议。

2.2.2 GetBlockTemplate 协议

GetBlockTemplate^[35]是由比特币社区于 2012 年开发的用于取代 GetWork 协议的去中心化挖矿协议。最大特点是让矿工自己构造区块,因为在将交易打包进区块时,矿工可以构建 Coinbase 交易(矿工的挖矿收入,包括系统奖励和区块中所有交易支付的交易费,都存放在该交易中),2~100 Byte 的

Coinbase 字段提供了充足的随机数扩展空间,克服了 4 Byte Nonce 空间在随机数遍历时存在的空间限制。

与 GetWork 协议相比,GBT 协议主要从以下 4 个方面进行了优化:1)将区块构造操作转移给了矿工,同时矿工可以调整 Coinbase 交易来修改打包进区块的交易,这使得区块生成实现了去中心化,从而提高了比特币网络的安全性;2)矿池可以根据需要制定挖矿规则,提高了系统的可扩展性;3)极大减少了区块创建过程中产生的网络流量负载,同时也减轻了矿池服务器的工作压力;4)掌握着区块链上与挖矿有关的所有信息,矿工可以独立选择需要打包进区块的交易,提高了整个系统运行过程的透明性。GBT 协议虽然提供了能够满足算法需求的搜索空间,但正常的一次协议调用需要把已打包进区块的所有交易数据都交给矿工,在每一次操作过程中节点都会返回约 1.5 MB 的数据,因此带来了过大的数据负载。

2.2.3 Stratum 协议

为了解决 GBT 协议在应用中暴露出的矿工与矿池之间信息交互过于频繁且数据量大、矿机内存消耗过大、矿工无法获取到区块链系统最新的区块变化等问题,提出了 Stratum 协议^[36]。

Stratum 协议综合了区块链技术的发展和矿池网络的优势,形成了目前基于区块链的加密数字货币系统使用的事实上的挖矿协议,使矿工能够可靠、高效地从矿池服务器获取任务^[37]。利用 Stratum 协议可以实现矿工与矿池之间任务的动态分配,对于矿池来说,可以将新任务以强制方式分配给矿工并使矿工无条件执行,矿工也可以主动向矿池申请新任务。提供可按需扩展的充足搜索空间是矿池挖矿需要解决的核心问题。GetWork 协议利用 8 Byte 的 Nonce 和 Time 字段提供搜索空间,但该空间早已不能满足新型矿池挖矿的要求。GBT 协议为矿工自由构造 Coinbase 交易提供了巨大的搜索空间,但需要将形成区块的所有交易数据全部交给矿工,在增加了矿工节点存储空间的同时,也对矿池网络带宽提出了更高要求。Stratum 协议通过改进 Coinbase 交易的构造策略,在给矿工提供足够搜索空间的同时,还能大幅度减少矿工与矿池之间交互时所需要传输的信息量,解决了 GetWork 和 GBT 协议存在的不足。

不同的 Coinbase 交易形成不同的 MerkleRoot 哈希值,进而提供更大的算法遍历空间。在 Stratum 协议中,矿工在构造 Coinbase 交易时,其中 ScriptSig 字段中的一些信息可以让矿工自己填充,而且由 Coinbase 交易生成 MerkleRoot 时无需提供全部交易数据。如图 5 所示,假设区块中包含 15 笔用户交易以及相应的 Coinbase 交易,矿池首先根据区块构建机制对每一笔交易进行处理,然后只需要将其中的 4 个运算得到的 Hash 值(图中虚线框中的 4 个节点)以及构造 Coinbase 交易需要的信息交给矿工。在此基础上,矿工就可以根据 Merkle 树的生成规则自行生成 MerkleRoot 值^[38]。基于此方法,当区块中包含

N 笔交易时,矿池只需要将 1b N 个 Hash 值发送给矿工,大幅降低了矿工与矿池之间的数据交互量。

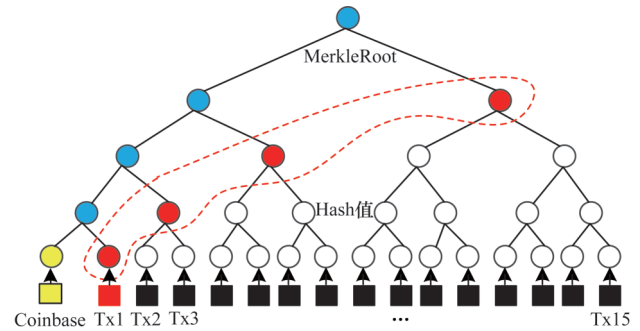


图5 Merkle树及MerkleRoot的生成过程

Fig.5 Generation process of Merkle tree and MerkleRoot

Stratum 协议严格定义了矿工与矿池之间通信的接口规范、数据结构和交互逻辑,在以太坊矿池网络中,有时矿池软件与钱包安装在一起合称为矿池,矿工与矿池软件之间的通信也采用 Stratum 协议。Stratum 协议采用轻量级的 JSON 数据格式,以提高数据处理效率。以太坊矿池挖矿的基本操作流程(如图 6 所示)具体如下:

1) 身份注册。启动挖矿程序,使用 mining.subscribe 方法连接到矿池;矿池使用 mining.notify 消息返回订阅号 ID、指定的初始难度、Extranonce(用于增加搜索空间)等信息,矿工将这些信息保存在本地,在整个挖矿过程中都要用到这些数据。需要说明的是:矿池允许利用同一个注册账号添加多个不同名字的矿工进行同时挖矿。

2) 身份认证与授权。矿工使用 mining.authorize 方法向矿池进行身份认证和授权,只有通过认证的合法矿工,矿池才会对其指配挖矿任务。

3) 任务指配。矿池通过 mining.notify 方法向矿工指配任务,其中主要包括任务号 ID(每一次任务都拥有唯一的标识符)、交易列表的压缩表示方式(图 5 中虚线框中 4 个节点代表的 Hash 值)、Version、Time 和 Bits 等。

4) 挖矿。矿工在接收到矿池下发的挖矿任务后,开始构造 Coinbase 交易、生成 MerkleRoot 和构建区块头,开始挖矿过程。

5) 提交和确认结果。矿工在寻找到小于目标值(由矿池下发的难度值产生)的 share 时,以 mining.submit 方法将其上交给矿池,其中主要包括矿工名字、任务号 ID、Extranonce、Time 和 Nonce。当矿池接收到以上 5 个字段的信息后,首先根据任务号 ID 找到之前指配的任务,然后重构区块,再验证 share 难度,之后进一步检测该 share 是否符合全网难度。当检测通过后,矿池通过 server.result 方法返回 true,说明 share 提交成功。

6) 调整难度。矿池会记录每个矿工提交的 share,并根据每次成功提交的 share 重新调整下一次挖矿时使用的难度,并随时通过 mining.set_difficulty 方法通知给矿工。

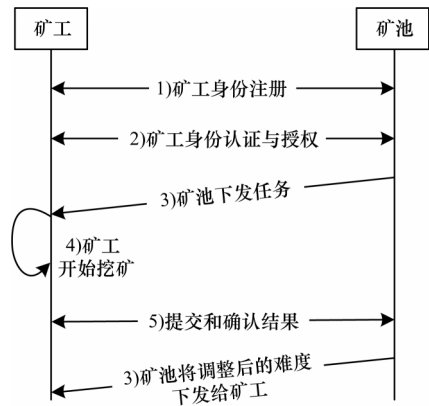


图 6 以太坊矿池挖矿的基本操作流程
Fig.6 Basic operation process of Ethereum mining pool mining

表 4 3 种典型矿池协议的性能比较

Table 4 Performance comparison of three typical mining pool protocols

协议	算法实现所需字段	遍历空间大小/Byte	区块生成特点	主要应用场景	功能特征	安全性	网络负载
GWK	Nonce+Time	8	中心化	CPU/GPU 挖矿	数据与挖矿分离	低	较小
GBT	Nonce+Coinbase	4~104	去中心化	大型矿池和矿场	矿工自己构造区块	较高	大
STM	Nonce+Coinbase	4~104	去中心化	大型矿池和矿场、大算力矿机	矿工与矿池间任务的动态分配	高	小

3 针对矿池网络的典型攻击方式

目前,矿池已经成为 PoW 共识挖矿算力的主要来源,如果矿池网络自身存在安全风险或攻击者利用矿池作恶,将会对区块链系统的安全产生严重威胁^[40-41]。本节重点对矿池网络中的典型攻击方式进行分析,并提出必要的防范方法。

3.1 自私挖矿攻击

分叉技术是软件开发过程中从已有项目的基础上快速产生另一项目的常见方法,在区块链系统中指主链从某一区块开始产生了 2 条或 2 条以上支链的过程。以比特币系统为例,将分叉分为自然分叉和人为分叉两种类型^[42]。自然分叉是临时产生的分叉,系统最终只会保留算力最大的一条链作为主链。人为分叉是在已有区块链的基础上产生另一条同源区块链的过程,两条分叉链之间即可以相互兼容(称为“软分叉”),也可以互不兼容(称为“硬分叉”)。

自私挖矿攻击^[6,43-44]是指在不影响区块链网络正常运行的前提下,利用区块链分叉原理,攻击者通过蓄意制造分叉并恶意设置挖矿策略,从而在区块链网络中发起不公平竞争的一种挖矿行为。在比特币系统中,诚实矿工在挖到一个区块后会尽快将其广播出去以得到网络中其他矿工的确认。同时,所有矿工坚持最长链原则,即在区块链出现分叉时会将最长的一条链作为主链,而且存在相同高度的分叉链时,诚实矿工会将最先形成的一条链作为主链。基于以上挖矿规则,自私挖矿中的攻击者在成功挖到一个区块后并不一定会立即广播出去,而是有策略地选择后续的操作,以获得高出正常挖矿的收益。

除前文介绍的 3 种典型矿池网络协议外,随着近年来全球矿池挖矿方式的不断升温,还出现了一些新的协议、技术和模式,如混合挖矿^[38]。域名币^[39]较早使用混合挖矿形式,通过挂靠方式将比特币作为父链,域名币作为辅链,使用 AuxPoW^[38]协议进行挖矿。矿工在挖得比特币的同时可以挖到域名币。

表 4 针对协议的算法实现及功能特点,分别从所涉及的字段、遍历空间大小、区块生成过程的特点、协议的主要功能特征、协议的主要应用场景、协议的网络安全性、协议实现过程的网络负载大小等方面对 3 类典型矿池协议进行对比分析。

自私挖矿存在多种策略,其中典型的策略是当攻击者挖出一个区块时并不立即广播,而是继续在该区块的基础上挖下一个区块,当攻击者监测到本地区块高度大于诚实矿工的区块高度时,立即将自己的多个连续区块广播出去,从而在诚实矿工节点上产生分叉,根据最长链原则,攻击者在挖矿竞争中抢先获得记账权,从而获得系统奖励。从长远来看,随着 PoW 挖矿难度的不断增大,矿池会借助算力上的绝对优势实施自私挖矿攻击,以破坏挖矿的公平性,同时迫使一些原本诚实的矿工在利益驱动下转向恶意矿池^[45],对区块链网络安全带来威胁。

自私挖矿策略是自私挖矿攻击的核心。在自私挖矿策略^[6]的基础上,SAPIRSHEIN 等^[46]拓展了自私挖矿的底层模型,并优化了攻击者策略,但部分策略的安全性较弱。NAYAK 等^[44]通过有效扩展挖掘策略空间为矿工赚取更多的收益,同时还将自私挖矿攻击与网络层的日食攻击^[47]相结合来进一步扩大收益,该方法虽然实现较为灵活,但难度较大、效率较低。阮娜等^[48]在对单一攻击者的自私挖矿策略进一步优化的基础上,提出包含单一攻击者与多攻击者的两阶段自私挖矿攻击模型,该方法主要集中于对内部攻击者的研究。LEE 等^[49]在分析了矿池网络运行机制的基础上,提出通过在矿池与矿工之间共享挖矿信息来应对自私挖矿的策略,该方法在单一矿池中的应用效果较好,但在多矿池联合挖矿环境中不太理想。

针对区块链自私挖矿攻击,最有效的防范方法是通过改变 PoW 机制的挖矿策略来增大矿池自私挖矿的成本,降低自私挖矿的收益。一种方法是当

诚实矿工收到一个具有相同高度的分叉链时,不是像 PoW 机制中默认的那样将最先生成的链作为主链,而是随机选取其中一条链作为主链,并继续在该主链上挖矿;另一种方法是诚实矿工(尤其是长期在线的诚实矿工)每次只接收单一区块,而拒绝同时接收分叉链中的多个区块。另外,近年来快速发展的人工智能技术也开始被应用到防御自私挖矿中^[50]。

3.2 跳池攻击

在矿池挖矿中,矿池的功能是通过矿池管理员给矿池矿工分配一定难度的计算任务,并根据矿工提交的符合计算要求的解来统计每个矿工的工作量并分配奖励。在此过程中,如何有效设置经济激励机制对吸引矿工加入矿池挖矿非常重要,与此同时,也为作恶者借助策略对存在的漏洞发起攻击提供了条件。跳池攻击^[51]是指攻击者为了追求高额收益,不是一直留在一个矿池中进行挖矿,而是根据不同矿池的当前收益切换到具有更高收益的矿池进行挖矿的一种攻击现象。跳池攻击直接利用了矿池挖矿激励机制存在的漏洞,尤其是借助不同矿池奖励分

配模式的特点,追求最大的收益,而忽视矿池运行的稳定性。对于任何一个矿池,出于安全性要求,需要加入矿池的矿工是忠诚的,即希望该矿工一直留在矿池中挖矿,而跳池攻击损害了忠诚矿工的利益,破坏了矿池运行的稳定性。

目前,主要的矿池挖矿奖励分配模式包括 Proportional、PPS、PPLNS、Slush、Geometric、Triple mining、P2Pool、Luke-Jr 等类型^[52],表 5 描述了不同奖励分配模式的特点和主要特征。以 Proportional 模式为例,如果矿池长时间没有挖到区块,那么矿池中矿工提交的 share 将逐渐贬值,即算力越来越不值钱。这时,一些矿工将会暂时离开当前矿池,选择加入一个刚刚挖出区块的矿池进行挖矿,如果一段时间后没有拿到奖励,矿工则可能会返回原有矿池继续挖矿。攻击者会给每个矿池的挖矿时间设置一个阈值,当矿工在一个矿池中的挖矿时间达到阈值时将跳到另一个刚刚挖出区块而且挖矿周期短的矿池进行挖矿^[53]。可以看出,攻击者为了追求更高的收益,特别会选择在 Proportional 和 Slush 模式下实施跳池攻击。

表 5 主要矿池挖矿奖励分配模式比较

Table 5 Comparison of the main distribution modes of mining pool mining rewards

分配模式	功能描述	主要特征
Proportional	矿池在每一轮(两个相邻区块间的时间间隔)挖到区块后,按矿工提交的 share 比例分配奖励	矿工收益不稳定,每一轮的挖矿时间不确定,每个 share 的收益不同,容易存在跳池攻击
PPS	解决了 Proportional 模式中收益不稳定问题;由矿池管理员根据总算力预测每天可生成的区块数和 share 数量以及每个 share 对应的奖励;当矿工提交 share 时,立即获得对应的奖励	矿工收益稳定,在提交 share 后可立即拿到预期的奖励,矿工的风险转移到矿池管理员
PPLNS	是对 Proportional 和 PPS 模式中矿工奖励分配方式的改进,只会将奖励分配给区块发现前最后 N 个提交 share 的矿工	矿工能否获得收益与出块时间有关,可有效防范跳池攻击
Slush	是对 Proportional 模式的改进,对每个 share 按照提交时间计算积分,越靠近出块时间积分越高,获得的奖励也越高	出块时间越短,share 获得的奖励越高;存在跳池攻击的可能
Geometric	是对 Slush 模式的改进,将奖励分为固定奖励和可变奖励,固定奖励由生成的区块确定,可变奖励由矿池管理员在每一轮挖矿开始时设定	每一轮挖矿时间越短,可变奖励越高;可避免跳池攻击
Triple mining	用于由多个矿池组成的联合矿池挖矿环境,在挖到一个区块后将奖励的 1% 按每个矿池算力大小进行分配	适用于多矿池联合挖矿,可有效激励中小型矿池挖矿
P2Pool	将挖矿奖励按比例分为 3 个部分:99% 平均分配给所有矿工,0.5% 分配给挖出区块的矿工,0.5% 为矿池管理员手续费	可防止比特币系统中因算力过于集中出现的 51% 攻击威胁;不存在中心节点,可防范 DDoS 攻击
Luke-Jr	每个矿工的 share 同时用于当前区块和下一个区块的生成;如果生成当前区块时矿工的总金额不足 1 BTC,奖励将累加到下一个区块,直至达到 1 BTC 时才支付;如果矿工在一周内未提交 share,则将当前金额支付给矿工	有效促使矿工留在矿池持续进行挖矿,可防止跳池攻击

跳池攻击不仅出现在矿池挖矿中,而且出现在跨链操作中。同一矿工在不同的时间和不同的区块链上挖矿会存在不同的收益,因此为了获得更大的收益,部分矿工会选择暂时离开原有的矿池,而加入收益率高的分叉链上的矿池进行挖矿。例如,当比特币系统分叉为比特币和比特币现金(BCC)后,形成了两个奖励分配模式和代币发行机制不同的同源区块链,曾经一段时间部分矿工开始从 BTC 迁移到 BCC 挖矿,后来由于 BCC 中算力的大量涌入,导致在下一个难度调整时会提高难度值,因此矿工又纷

纷迁回 BTC 矿池。

针对跳池攻击,目前有效的防范方法主要有:1)选择更优的奖励分配模式,例如,可选择 PPLNS、Geometric、Luke-Jr 等模式,防止攻击者为了追求收益的最大化实施跳池攻击;2)优化矿池奖励分配模式,例如,文献^[54]针对 PPS 和 PPLNS 模式对矿池带来的安全风险,设计一种新的基于零行列式(ZD)理论的矿池挖矿策略,该策略具有免费、适用性广和公平等特性,需要结合矿池挖矿技术的发展,对相关算法进行有针对性的研究;3)选择符合矿工预期的矿

池,为了使矿工在加入矿池时能够对预期收益进行评估,防止出现类似跳池攻击的现象,目前已出现了类似 Multipool^[55-56]的矿池,该类型矿池会将矿工推荐到当前收益最大的矿池进行挖矿。

3.3 扣块攻击

在矿池挖矿过程中的扣块(BWH)攻击^[57-58]是指攻击者在挖到 share 时,如果该 share 符合出块要求则将其保留,否则提交给矿池管理员,以此降低矿池和矿池中诚实矿工的收益,但当矿池中的诚实矿工挖到区块时,攻击者仍会根据自己提交的 share(无价值的 share)来分得奖励。由此可以看出,扣块攻击在未做出任何贡献的情况下分摊了诚实矿工应获得的收益,并使得矿池利益严重受损。

另外,扣块攻击经常被恶意攻击者用于实现不同矿池之间的恶意竞争。作恶矿池将自身的部分算力(矿工)注入被攻击对手矿池进行扣块攻击,以降低对手算力的价值,并从对手矿池中分得本应属于矿池和矿工的一定数量的收益。不过,矿池之间的扣块攻击也为攻击者所在的矿池带来了一定的损失和风险,被注入到对手矿池的算力削弱了本矿池的算力,也损失了由这部分算力带来的直接收益。因此,攻击者会科学计算被注入对手矿池的算力比例,在尽可能维护自身利益的前提下,有效降低对手的收益,并迫使对手矿池中的矿工转入其他矿池进行挖矿。

防范扣块攻击的方法主要是改变收益的分配模式(如采用 PPLNS 模式)。另外,针对扣块攻击,文献[59]在研究了比特币中扣块攻击的基础上,分析了比特币中防范针对主要奖励分配模式的扣块攻击方法,但该方法仅适用于比特币系统。文献[60]认为检测扣块攻击具有挑战性,只有通过诚实矿工寻求利益的一致性才是最佳选择,并证明了双重收益方案的可行性,但该方法的有效性尚待在不同类型的矿池网络中进行验证。文献[61]在分析扣块攻击收益特点的基础上,提出一种称为“特殊奖励”的机制,旨在给予实际挖出区块的矿工额外的奖励,而对于从未向矿池提供有效区块的矿工降低奖励分配,以此来防御扣块攻击行为。该方法需要结合具体的矿池奖励分配模式,在具体实现过程中进行有针对性的策略设计。

3.4 空块攻击

区块是由合法交易打包生成的数据单位,一笔交易只有打包进区块后才能被最后确认。在区块中的第一笔交易(Coinbase 交易)用于存放挖出该区块后系统给予的奖励以及打包进区块的其他有效交易交纳的所有手续费。空块攻击^[62]是指攻击者通过构造只包含 Coinbase 交易的空区块,拒绝对有效交易打包,导致大量交易由于未能打包进区块而无法得到确认的攻击方式。区块链系统的设计目标是实现对交易的打包确认,交易是区块链系统的最小数据单位,也是实现价值生成与转移以及信息交换的核

心,然而如果一个区块链系统中的矿工只挖空块而不打包用户交易,区块链系统也将失去其应用价值。当区块链系统中存在大量空块时,相当于对系统实施 DDoS 攻击。

由于挖空块相对容易,因此在矿池中作恶者很容易实施空块攻击。首先,从区块生成算法来看,空块属于合法区块;其次,空块具有快速传播优势。一个区块一般由 80 Byte 的区块头和以 MB 为单位的区块体组成,由于空块大小主要由区块头决定,在空块确认时不存在对用户交易进行验证的过程,因此空块的传输速度很快,在传播时间上具有竞争优势;最后,空块避免了因存在重复交易而被作为非法区块的现象发生。正常的区块只有经矿工验证通过后才能链接到主链上,区块合法的前提是该区块中包含的交易合法,而且本区块中的交易不能出现在前面的区块中,否则存在重复交易的区块为非法区块。由于空块中不存在用户交易,因此不存在交易重复问题。

针对空块攻击的主要防范方法是限制空块的生成,对于频繁生成空块的节点限制其挖矿或进行必要的经济惩罚。另外,建立矿工收益与打包进区块的交易数量之间的关联关系,单个区块包含的交易越多,矿工获得的收益也越大。从矿工的角度来看,避免挖空块的前提是尽快或提前得到当前区块中包含的交易。目前,在 BTC 和 BCH 矿池中,多采用紧凑型区块^[63]或瘦区块^[64]技术,在矿池中提前保存有需要进行验证的区块中的交易,避免在需要对交易进行验证时从其他节点下载完整的区块数据,提高了交易验证效率。然而,该方法的实现对矿机中用户交易的存储和管理也提出了更高的要求,在一定程度上影响了矿池的效率。

为了便于理解,表 6 从攻击的实现原理、主要攻击目标、攻击难度等方面对 4 类典型的针对矿池网络的攻击方式进行对比分析。

表 6 典型的矿池网络攻击方式对比分析
Table 6 Comparative analysis of typical mining pool network attack modes

攻击方式	实现原理	主要攻击目标	攻击难度
自私挖矿攻击	区块链分叉	PoW 挖矿策略	高
跳池攻击	共识机制	矿池奖励分配模式	中
扣块攻击	共识机制	share	低
空块攻击	区块生成	矿池中诚实的矿工	低

4 挑战与展望

区块链在继承了传统 P2P 网络的基础上,结合自身要求进行了功能扩宽,其中矿池网络就是区块链挖矿发展的产物。

1) 区块链 P2P 网络研究是基础。P2P 网络是建立在 TCP/IP 基础上的一种具有特定应用功能的覆盖网络,矿池网络是基于区块链 P2P 网络的扩展网

络,区块链 P2P 网络是研究矿池网络的基础。对于区块链 P2P 网络的研究主要集中于 2 个方面:

(1) P2P 网络自身技术,重点对网络信任模型、覆盖网络的拓扑一致性与效率、资源定位与搜索、网络抖动、网络容错性等方面进行研究。

(2) P2P 网络与区块链技术的结合,重点从比特币、以太坊、超级账本等典型的区块链应用场景出发,对涉及的核心技术进行针对性的研究,例如:针对比特币网络中的交易模式分析,可充分利用图神经网络、图论等理论加强对比特币系统交易网络的可视化模型研究;针对以太坊中的结构化网络特点,重点加强 DHT 及相关技术在地址管理和路由算法中的应用研究;针对超级账本技术,重点对超级节点选择策略、用户身份认证技术(尤其是可控匿名认证)、隐私保护等方面进行深入研究。

2) 矿池网络技术研究是关键。矿池网络是在区块链技术挖矿过程中矿工为了追求更大收益而形成的一个逻辑上的网络,有关矿池网络的研究重点集中在以下 3 个方面:

(1) 矿池网络协议。网络功能的实现依赖于协议,协议的研究仍然是矿池网络研究的重点,一方面需要结合矿池挖矿技术和管理的需要,对应用中的矿池网络协议进行进一步优化,同时加强对协议漏洞,尤其是安全漏洞的挖掘、分析和修复,防止攻击者利用漏洞实施对矿池网络的攻击,另一方面根据新的挖矿模式的出现开发新的矿池网络协议。

(2) 对矿池网络与区块链 P2P 网络之间的运行机制进行进一步优化,矿池网络具有相对的独立性,从整个挖矿过程来看每一个矿池相当于一个挖矿节点,需要与外界频繁交换挖矿信息,这就涉及矿池网络与区块链 P2P 网络之间的协调,需要进一步优化网络边界性能,提升信息交换效率。

(3) 优化矿池利益分配方式,开发符合新型挖矿要求的矿池利益分配策略,矿池挖矿是一种典型的趋利行为,矿池矿工为了追求更大的收益,矿池管理员力求收取更多的挖矿手续费。为此,矿池中不同利益方如何建立有效的利益分配关系不仅关系到矿工参与矿池挖矿的积极性,更关系到矿池的发展,主要涉及矿池挖矿奖励分配策略的设计与优化,需要针对具体矿池,在 Proportional、PPS、PPLNS 等分配模式的基础上,综合矿池发展定位、对应虚拟货币币种的影响力、共识机制等方面的因素,科学开发和运用矿池挖矿收益分配策略。

3) 矿池网络安全研究是保障。目前,大部分矿池都属于开放矿池,用户只需要接入互联网就可以通过注册加入矿池,并通过贡献有效工作量证明来获得相应的收益。矿池网络的开放性不仅容易遭受传统网络中的 DDoS、协议分析、端口扫描等攻击,而且还会受到自私挖矿、扣块、跳池、空块等专门针对矿池网络的安全威胁,针对矿池网络的安全研究变

得更加复杂。为此,针对矿池网络安全的研究,仍然需要在借鉴互联网安全技术的基础上,结合区块链技术特点和矿池网络运行机制进行创新。例如,针对扣块攻击难以定位具体攻击者这一问题,可以采用博弈理论来分析和设定挖矿规则,使攻击者难以获得预期的作恶收益。

从技术实现角度看,基于区块链技术的各类虚拟货币之间的交易实质是通过技术手段(如不同虚拟货币之间的跨链交易)来改变虚拟货币的控制权。由于虚拟货币继承了区块链技术的去中心化、匿名性等特征,为其流通与应用监管带来了挑战,已成为犯罪分子逃避监管及实施各类犯罪活动的工具。另外,虚拟货币挖矿行为占用了大量网络带宽,浪费了大量社会资源,亟待对其进行有效监管。例如,通过监测发现,2021 年仅江苏省进行虚拟货币挖矿的矿池出口流量就达到 1.377 Gb/s,参与挖矿的互联网主机 IP 地址数量达到了 4 502 个,消耗算力超过 10 PH/s,每天耗能达到 2.6×10^5 kWh。在此情况下,加强对矿池挖矿行为的监管和整治势在必行,除出台相关的法律法规外,加强技术监管仍然是根本。下一步需要立足矿池网络实现原理,通过流量监测和协议分析等技术,识别互联网中的矿池流量,进而实现对挖矿流量及矿工主机的溯源与监管,如何将目前发展中的零信任网络、深度学习等技术应用到矿池网络监管是一个重要的研究方向。

综上,针对矿池网络技术的演进和安全防范的研究,主要集中于以下 4 个方面:1) 矿池性能的优化以及矿池运行的稳定性;2) 矿场的科学部署和矿池网络的科学设计;3) 随着矿机技术和工艺的不断提升,如何更加有效地提升和管理矿池的算力并降低功耗;4) 重点从安全漏洞研究入手,加强矿池网络协议和运行机制的安全研究等。

5 结束语

随着因虚拟货币兴起所带来的矿池挖矿产业的快速发展,无论是从技术发展还是应用监管角度,都有必要对矿池网络进行较系统的研究。本文在介绍传统 P2P 网络工作原理和组网特点的基础上,结合具体应用场景分析区块链 P2P 的运行特点,在此基础上,重点从协议实现出发讨论矿池网络的工作机制,并对典型的针对矿池网络的攻击行为和防范方法进行阐述。矿池网络及其安全仍然是未来区块链技术研究的重点和热点,下一步将从矿池网络协议实现、矿池收益分配策略、针对矿池挖矿的安全性等方面进行针对性的深入研究。

参考文献

- [1] 张亮,刘百祥,张如意,等. 区块链技术综述[J]. 计算机工程, 2019, 45(5): 1-12.
ZHANG L, LIU B X, ZHANG R Y, et al. Overview of blockchain technology[J]. Computer Engineering, 2019,

- 45(5):1-12. (in Chinese)
- [2] 王群,李馥娟,倪雪莉,等. 区块链共识算法及应用研究[J]. 计算机科学与探索,2022,16(6):1214-1242.
WANG Q, LI F J, NI X L, et al. Survey on blockchain consensus algorithms and application [J]. Journal of Frontiers of Computer Science and Technology, 2022, 16(6):1214-1242. (in Chinese)
- [3] 谭敏生,杨杰,丁琳,等. 区块链共识机制综述[J]. 计算机工程,2020,46(12):1-11.
TAN M S, YANG J, DING L, et al. Review of consensus mechanism of blockchain[J]. Computer Engineering, 2020, 46(12):1-11. (in Chinese)
- [4] DWORK C, NAOR M. Pricing via processing or combatting junk mail [M]. Berlin, Germany: Springer, 2007.
- [5] LASZKA A, JOHNSON B, GROSSKLAGS J. When bitcoin mining pools run dry [M]. Berlin, Germany: Springer, 2015.
- [6] EYAL I, SIRER E G. Majority is not enough: bitcoin mining is vulnerable [M]. Berlin, Germany: Springer, 2014.
- [7] CAN B, HOUGAARD J L, POURPOUNE M. On reward sharing in blockchain mining pools [EB/OL]. [2023-06-27]. <https://arxiv.org/abs/2107.05302>. pdf.
- [8] ALBRECHER H, FINGER D, GOFFARD P O. Blockchain mining in pools: analyzing the trade-off between profitability and ruin [EB/OL]. [2023-06-27]. <https://arxiv.org/abs/2109.03085>. pdf.
- [9] CHATZIGIANNIS P, BALDIMTSI F, GRIVA I, et al. Diversification across mining pools: optimal mining strategies under PoW [J]. Journal of Cybersecurity, 2022, 8(1):1-15.
- [10] LI X P, LI Z. A performance measurement and optimization mechanism for blockchain mining pool system [C]// Proceedings of the 3rd International Conference on Blockchain Technology and Applications. New York, USA: ACM Press, 2020:27-33.
- [11] 邸剑,齐伟华. 区块链中矿池选择策略的研究与分析[J]. 计算机应用研究,2020,37(6):1804-1807.
DI J, LIN W H. Research and analysis of mining pool selection strategy in blockchain [J]. Application Research of Computers, 2020, 37(6):1804-1807. (in Chinese)
- [12] 唐长兵,杨珍,郑忠龙,等. PoW 共识算法中的博弈困境分析与优化[J]. 自动化学报,2017,43(9):1520-1531.
TANG C B, YANG Z, ZHENG Z L, et al. Game dilemma analysis and optimization of PoW consensus algorithm [J]. Acta Automatica Sinica, 2017, 43(9):1520-1531. (in Chinese)
- [13] BERNIS A. Network scaffolding for efficient stabilization of the Chord overlay network [EB/OL]. [2023-06-27]. <https://arxiv.org/abs/2109.14126>. pdf.
- [14] DHT: distributed hash table [EB/OL]. [2023-06-27]. <https://courses.cs.duke.edu/fall15/cps214/Day20.pdf>.
- [15] Napster [EB/OL]. [2023-06-27]. <https://www.britannica.com/topic/Napster>.
- [16] NAKAMOTO S. Bitcoin: a peer-to-peer electronic cash system [EB/OL]. [2023-06-27]. <https://bitcoin.org/bitcoin.pdf>.
- [17] BORDIGNON F R A, TOLOSA G. Gnutella: distributed system for information storage and searching model description [EB/OL]. [2023-06-27]. https://www.researchgate.net/publication/228546808_Gnutella_Distributed_System_for_Information_Storage_and_Searching_Model_Description.
- [18] GIAKKOUPIS G, KERMARREC A M, WOELFEL P. Gossip protocols for renaming and sorting [C]// Proceedings of the 27th International Symposium. Berlin, Germany: Springer, 2013:194-208.
- [19] LIANG J, KUMAR R, ROSS K W. The KaZaA overlay: a measurement study [EB/OL]. [2023-06-27]. <https://cse.engineering.nyu.edu/~ross/papers/KazaaOverlay.pdf>.
- [20] ANDROULAKI E, BARGER A, BORTNIKOV V, et al. Hyperledger Fabric: a distributed operating system for permissioned blockchains [EB/OL]. [2023-06-27]. <https://arxiv.org/abs/1801.10228>. pdf.
- [21] KUSHWAHA R, KULKARNI S, SINGH Y N. Generalized distance metric for different DHT routing algorithms in peer-to-peer networks [EB/OL]. [2023-06-27]. <https://arxiv.org/abs/2303.13965>. pdf.
- [22] RATNASAMY S, FRANCIS P, HANDLEY M, et al. A scalable content-addressable network [J]. ACM SIGCOMM Computer Communication Review, 2001, 31(4):161-172.
- [23] MAYMOUNKOV P, MAZIÈRES D. Kademia: a peer-to-peer information system based on the XOR metric [M]. Berlin, Germany: Springer, 2002.
- [24] Ethereum whitepaper [EB/OL]. [2023-06-27]. <https://ethereum.org/en/whitepaper/>.
- [25] KLONOWSKI M, PIOTROWSKA A M. Light-weight and secure aggregation protocols based on Bloom filters [J]. Computers & Security, 2018, 72:107-121.
- [26] JEZEK K. Ethereum data structures [EB/OL]. [2023-06-27]. <https://arxiv.org/abs/2108.05513>. pdf.
- [27] 武岳,李军祥. 区块链P2P网络协议演进过程 [J]. 计算机应用研究,2019,36(10):2881-2886,2929.
WU Y, LI J X. Evolution process of blockchain P2P network protocol [J]. Application Research of Computers, 2019, 36(10):2881-2886,2929. (in Chinese)
- [28] DEMERS A, GREENE D, HOUSER C, et al. Epidemic algorithms for replicated database maintenance [J]. ACM SIGOPS Operating Systems Review, 1988, 22(1):8-32.
- [29] BERENDEA N, MERCIER H, ONICA E, et al. Fair and efficient gossip in Hyperledger Fabric [C]// Proceedings of the 40th International Conference on Distributed Computing Systems. Washington D. C., USA: IEEE Press, 2020:190-200.
- [30] GORENFLO C, LEE S, GOLAB L, et al. FastFabric: scaling Hyperledger Fabric to 20,000 transactions per second [EB/OL]. [2023-06-27]. <https://arxiv.org/abs/1901.00910>. pdf.
- [31] EYAL I. The miner's dilemma [EB/OL]. [2023-06-27]. <https://arxiv.org/abs/1411.7099>. pdf.
- [32] LUU L, VELNER Y, TEUTSCH J, et al. Smartpool: practical decentralized pooled mining [C]// Proceedings of the 26th USENIX Security Symposium. Berkeley, USA: USENIX Association, 2017:1409-1426.
- [33] Saylor Academy. Bitcoin relay networks [EB/OL]. [2023-06-27]. <https://learn.saylor.org/mod/book/view.php?id=36307&chapterid=18898>.
- [34] Wiki. Getwork [EB/OL]. [2023-06-27]. <https://en.bitcoin.it/wiki/Getwork>.
- [35] Wiki. Getblock template [EB/OL]. [2023-06-27]. <https://en.bitcoin.it/wiki/Getblocktemplate>.

- [36] Wiki. Stratum mining protocol[EB/OL]. [2023-06-27]. https://en.bitcoin.it/wiki/Stratum_mining_protocol.
- [37] RECAPARREN R, CARBUNAR B. Hardening stratum, the bitcoin pool mining protocol[EB/OL]. [2023-06-27]. <https://arxiv.org/abs/1703.06545>. pdf.
- [38] Bitcoin Wiki. Merged mining specification[EB/OL]. [2023-06-27]. https://en.bitcoin.it/wiki/Merged_mining_specification.
- [39] Namecoin. Namecoin[EB/OL]. [2023-06-27]. <https://www.namecoin.org/>.
- [40] LI S N, CAMPAJOLA C, TESSONE C J. Twisted by the pools: detection of selfish anomalies in proof-of-work mining[EB/OL]. [2023-06-27]. <https://arxiv.org/abs/2208.05748>. pdf.
- [41] 魏松杰, 吕伟龙, 李莎莎. 区块链公链应用的典型安全问题综述[J]. 软件学报, 2022, 33(1): 324-355.
WEI S J, LÜ W L, LI S S. Overview on typical security problems in public blockchain applications[J]. Journal of Software, 2022, 33(1): 324-355. (in Chinese)
- [42] YIU N C K. An overview of Forks and coordination in blockchain development[EB/OL]. [2023-06-27]. <https://arxiv.org/abs/2102.10006>. pdf.
- [43] 王贺立, 闫巧. 基于交易记录特征的自私挖矿检测方案[J]. 网络与信息安全学报, 2023, 9(2): 104-114.
WANG H L, YAN Q. Selfish mining detection scheme based on the characters of transactions[J]. Chinese Journal of Network and Information Security, 2023, 9(2): 104-114. (in Chinese)
- [44] NAYAK K, KUMAR S, MILLER A, et al. Stubborn mining: generalizing selfish mining and combining with an eclipse attack[C]//Proceedings of 2016 IEEE European Symposium on Security and Privacy. Washington D. C., USA: IEEE Press, 2016: 305-320.
- [45] SAAD M, NJILLA L, KAMHOUA C, et al. Countering selfish mining in blockchains[EB/OL]. [2023-06-27]. <https://arxiv.org/abs/1811.09943>. pdf.
- [46] SAPIRSHTAIN A, SOMPOLINSKY Y, ZOHAR A. Optimal selfish mining strategies in bitcoin[M]. Berlin, Germany: Springer, 2017.
- [47] HEILMAN E, KENDLER A, ZOHAR A. Eclipse attacks on Bitcoin's peer-to-peer network[C]//Proceedings of the 24th USENIX Conference on Security Symposium. Washington D. C., USA: IEEE Press, 2015: 129-144.
- [48] 阮娜, 刘汉卿, 斯雪明. 采用工作量证明共识机制的区块链中挖矿攻击者间的“鲶鱼效应”[J]. 计算机学报, 2021, 44(1): 177-192.
RUAN N, LIU H Q, SI X M. Catfish effect between selfish miners in proof-of-work based blockchain[J]. Chinese Journal of Computers, 2021, 44(1): 177-192. (in Chinese)
- [49] LEE S, KIM S. Rethinking selfish mining under pooled mining[J]. ICT Express, 2023, 9(3): 356-361.
- [50] NIKHALAT-JAHROMI A, SAGHIRI A M, MEYBODI M R. Nik defense: an artificial intelligence based defense mechanism against selfish mining in bitcoin[EB/OL]. [2023-06-27]. <https://arxiv.org/abs/2301.11463>. pdf.
- [51] SINGH S, SALIM M, CHO M, et al. Smart contract-based pool hopping attack prevention for blockchain networks[J]. Symmetry, 2019, 11(7): 941.
- [52] ROSENFELD M. Analysis of bitcoin pooled mining reward systems[EB/OL]. [2023-06-27]. <https://arxiv.org/abs/1112.4980>. pdf.
- [53] LIU K Y, OHSAWA Y. Auction based rewards distribution method in pool mining[C]//Proceedings of the 1st International Electronics Communication Conference. New York, USA: ACM Press, 2019: 103-110.
- [54] SHI H, WANG S, HU Q, et al. Hopping-proof and fee-free pooled mining in blockchain[EB/OL]. [2023-06-27]. <https://arxiv.org/abs/1912.11575>. pdf.
- [55] Multipool[EB/OL]. [2023-06-27]. <https://en.bitcoin.it/wiki/Multipool>.
- [56] Multipool. org[EB/OL]. [2023-06-27]. <http://www.multipool.org/>.
- [57] COURTOIS N T, BAHACK L. On subversive miner strategies and block withholding attack in bitcoin digital currency[EB/OL]. [2023-06-27]. <https://arxiv.org/abs/1402.1718>. pdf.
- [58] Bitcoin. What is a block withholding attack?[EB/OL]. [2023-06-27]. <https://bitcoin.stackexchange.com/questions/4943/what-is-a-block-withholding-attack>.
- [59] BAG S, RUJ S, SAKURAI K. Bitcoin block withholding attack: analysis and mitigation[J]. IEEE Transactions on Information Forensics and Security, 2017, 12(8): 1967-1978.
- [60] LEE S, LEE D, KIM S. Block double-submission attack: block withholding can be self-destructive[EB/OL]. [2023-06-27]. <https://arxiv.org/abs/2208.05425>. pdf.
- [61] BAG S, SAKURAI K. Yet another note on block withholding attack on bitcoin mining pools[M]. Berlin, Germany: Springer, 2016.
- [62] 田国华, 胡云瀚, 陈晓峰. 区块链系统攻击与防御技术研究进展[J]. 软件学报, 2021, 32(5): 1495-1525.
TIAN G H, HU Y H, CHEN X F. Research progress on attack and defense techniques in block-chain system[J]. Journal of Software, 2021, 32(5): 1495-1525. (in Chinese)
- [63] Bitcoin/Bips. Compact block relay[EB/OL]. [2023-06-27]. <https://github.com/bitcoin/bips/blob/master/bip-0152.mediawiki>.
- [64] DING D, JIANG X, WANG J, et al. Txilm: lossy block compression with salted short hashing[EB/OL]. [2023-06-27]. <https://arxiv.org/abs/1906.06500>. pdf.

编辑 陆燕菲