(19)国家知识产权局

(12)发明专利

(10)授权公告号 CN 115208767 B
(45)授权公告日 2023.10.27

(21)申请号 202210512262.0

(22)申请日 2022.05.12

(65)同一申请的已公布的文献号
申请公布号 CN 115208767 A

(43)申请公布日 2022.10.18

(73)专利权人 哈尔滨工业大学(深圳)
地址 518055 广东省深圳市南山区桃源街道深圳大学城哈尔滨工业大学校区

(72)发明人 刘洋 张玉玺 林致远 王轩 张伟哲 蒋琳 刘川意 吴宇琳

(74)专利代理机构 广州市华学知识产权代理有限公司 44245
专利代理师 戴晓琴 李斌

(51)Int.Cl.
*H04L 41/12*(2022.01)
*H04L 41/14*(2022.01)
*H04L 43/04*(2022.01)
*H04L 9/40*(2022.01)

(56)对比文件
CN 111082995 A,2020.04.28
CN 114285640 A,2022.04.05
US 2002156920 A1,2002.10.24
US 5185860 A,1993.02.09
CN 112751697 A,2021.05.04
CN 103765835 A,2014.04.30
杨磊;秦志光;钟婷.基于聚类推荐的P2P信任模型.计算机应用研究.2010,(第04期),全文.
廖海亮;胡光岷;钱峰;杨志豪.网络拓扑识别:基于traceroute的层析成像方法.计算机应用研究.2009,(01),全文.

审查员 莫海兰

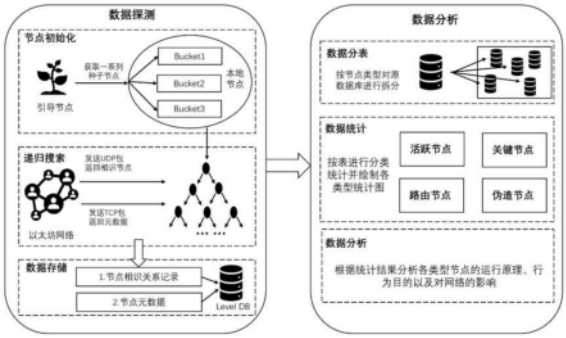
权利要求书2页 说明书9页 附图2页

(54)发明名称

基于仿真技术的以太坊网络探测方法、装置、设备及介质

(57)摘要

本发明公开了一种基于仿真技术的以太坊网络探测方法、装置、计算机设备和存储介质,所述方法包括:采集数据,所述数据包括节点间相识关系和节点元数据;创建启动节点后,通过利用节点发现协议的特点,对对等节点进行反复查询并聚合去重,节点数据库得到此前未被分析的节点相识关系;根据所述节点间相识关系和节点元数据,对以太坊网络中节点的行为进行分析。本发明通过利用节点发现协议的特点,对对等节点进行反复查询并聚合去重,节点数据库得到此前未被分析的节点相识关系,进而根据节点相识关系和节点元数据对以太坊网络中节点的行为进行分析,发现的活跃节点数量比现有其他方法都多,表明本方法可以更加完整的展现以太坊网络性质。




CN 115208767 B

1.一种基于仿真技术的以太坊网络探测方法,其特征在于,所述方法包括:

采集数据,所述数据包括节点相识关系和节点元数据;创建启动节点后,通过利用节点发现协议的特点,对对等节点进行反复查询并聚合去重,节点数据库得到此前未被分析的节点相识关系;

根据所述节点相识关系和节点元数据,对以太坊网络中节点的行为进行分析,包括:

将所有节点相识关系和节点元数据保存在本地数据库中,对本地数据库中的数据进行分表;

将表中的节点划分为活跃节点、关键节点、路由节点以及恶意节点四种类别;

统计表中各类别节点的数量;

根据统计结果,对以太坊网络中节点的行为进行分析;

其中,所述活跃节点为当前存在于网络中正常运行区块链协议的节点,是区块链运行不可或缺的因素;

所述关键节点为活跃节点,并具体满足以下所有条件:a)能运行最新版本客户端;b)对等节点数量超过第一设定阈值;c)相识节点个数超过第二设定阈值;

所述路由节点为一类特殊的节点,不运行任何应用层协议,只进行节点记录的转发;

所述恶意节点不运行任何区块链协议,也没有与其他节点的相识关系,却广播伪造的节点记录或伪造节点身份让活跃节点与其进行连接的特殊节点。

2.根据权利要求1所述的以太坊网络探测方法,其特征在于,分得的表包括活跃节点表和相识关系表;

所述根据统计结果,对以太坊网络中节点的行为进行分析,包括:

根据统计结果计算活跃节点在网络中所占的比重;

遍历相识关系表,找出全部活跃节点,采用PageRank算法分析活跃节点表中的关键节点及其影响因子;针对恶意节点进行分析,对伪造行为的原理以及对网络的影响进行分析。

3.根据权利要求1所述的以太坊网络探测方法,其特征在于,所述节点元数据包括节点记录序号、客户端版本及开发语言、操作系统类型以及支持的应用层协议,其中:

获取节点记录序号数据包括:

启动节点向远程节点模拟发送ENR Request Packet,从接收到的ENR Response Packet中解析出节点记录序号数据;

获取其余元数据包括:

启动节点与远程节点完成RLPx协议的ECIES握手后,双方再进行协议握手,在协议握手阶段从对方的握手包中获取客户端版本及开发语言、操作系统类型以及支持的应用层协议;根据对以太坊客户端源码的分析,当远程节点返回错误信息“too many peers”时将此节点视为连接超过50个节点,作为活跃节点。

4.根据权利要求1~3任一项所述的以太坊网络探测方法,其特征在于,所述采集数据,通过探测器采集数据,包括仿真节点初始化和递归查询,其中:

所述仿真节点初始化包括:

在初始状态下,基于仿真技术创建启动节点,并为启动节点指定一系列种子节点,启动节点对种子节点进行递归搜索直到没有新节点出现,即完成对整个以太坊网络的搜索;

所述递归查询为针对每个节点的查询过程,包括:

发送UDP数据包在节点发现协议上获取节点相识的所有节点，再与其建立TCP连接并且通过模拟RLPx协议的握手过程来获取节点相应的元数据，从而获得需要采集的数据。

5.一种基于仿真技术的以太坊网络探测装置，其特征在于，所述装置包括：

数据采集模块，用于采集数据，所述数据包括节点相识关系和节点元数据；创建启动节点后，通过利用节点发现协议的特点，对对等节点进行反复查询并聚合去重，节点数据库得到此前未被分析的节点相识关系；

行为分析模块，用于根据所述节点相识关系和节点元数据，对以太坊网络中节点的行为进行分析，包括：

将所有节点相识关系和节点元数据保存在本地数据库中，对本地数据库中的数据进行分表；

将表中的节点划分为活跃节点、关键节点、路由节点以及恶意节点四种类别；

统计表中各类别节点的数量；

根据统计结果，对以太坊网络中节点的行为进行分析；

其中，所述活跃节点为当前存在于网络中正常运行区块链协议的节点，是区块链运行不可或缺的因素；

所述关键节点为活跃节点，并具体满足以下所有条件：a)能运行最新版本客户端；b)对等节点数量超过第一设定阈值；c)相识节点个数超过第二设定阈值；

所述路由节点为一类特殊的节点，不运行任何应用层协议，只进行节点记录的转发；

所述恶意节点不运行任何区块链协议，也没有与其他节点的相识关系，却广播伪造的节点记录或伪造节点身份让活跃节点与其进行连接的特殊节点。

6.一种计算机设备，包括处理器以及用于存储处理器可执行程序的存储器，其特征在于，所述处理器执行存储器存储的程序时，实现权利要求1-4任一项所述的以太坊网络探测方法。

7.一种存储介质，存储有程序，其特征在于，所述程序被处理器执行时，实现权利要求1-4任一项所述的以太坊网络探测方法。

# 基于仿真技术的以太坊网络探测方法、装置、设备及介质

## 技术领域

[0001] 发明属于计算机网络安全技术领域，特别是涉及一种基于仿真技术的以太坊网络探测方法、装置、计算机设备及存储介质。

## 背景技术

[0002] 目前以太坊是区块链应用最广泛的智能合约平台。尽管针对以太坊共识算法和合约代码安全性分析的研究越来越多，但是针对以太坊的点对点网络特性的研究还没有得到充分的重视。有研究表明，使用工作量证明机制的区块链系统其安全性依赖于点对点网络的可靠性。

[0003] 以太坊使用点对点网络来交流其区块链的状态，以太坊的网络旨在模拟基于Kademlia DHT的结构化图。由于以上不同，需要对以太坊点对点网络进行完整、全面的探测分析，找出其中可能存在的风险和隐患。

[0004] 以太坊的点对点网络上主要运行了两个协议，分别是基于UDP的节点发现协议和基于TCP的RLPx协议。

[0005] 节点发现协议中，节点之间通过相互探测来发现网络中的其他节点。为了加入以太坊网络并开始进行区块同步，以太坊客户端会指定一组种子节点来发现其他的活跃节点并将它们的信息保存到对应的桶中。为了能够在节点间尽快地沟通节点记录，以太坊的Node Discovery Protocol使用UDP作为传输层协议。在该协议的v4版本中包括六种消息类型:Ping、Pong、FindNode、Neighbors、ENRRequest、ENRResponse，其中每两个之间互相作为应答数据包。Ping和Pong包用于判断远程节点是否存活，Neighbors包每次返回16个同FindNode包中节点距离最近的记录。运行节点发现协议并添加节点记录到节点数据库的过程，第一个RTT时间内本地发送FindNode包并接收远程节点返回的Neighbors包，将其中保存的16条节点记录保存至节点数据库;第二个RTT时间本地将向远程节点发送Ping包尝试激活远程节点，收到返回Pong包说明对方存活，此后对剩余节点循环往复不断执行上述操作。

[0006] 以太坊网络中的所有节点都有各自独立的节点记录，每个节点记录通过节点ID进行标识。节点ID是一个使用16进制表示的512位的ECDSA公钥。目前有enode和enr两种形式的节点记录，enode为明文表示，enr是使用节点私钥签名并分别进行RLP编码和base64编码后的结果。两个节点之间的距离被称为对数距离。以太坊使用的计算函数是对Kademlia算法的修改，本地节点得知的所有节点记录会按照对数距离进行排序。计算对数距离的过程如下:(1)使用keccak256算法计算两个节点ID哈希值。(2)对两个哈希值取异或，然后对异或结果取对数。

[0007] 节点发现完成后的下一个步骤就是同新发现的节点交换数据，RLPx协议就是用来在两个节点之间建立一个可以进行安全通讯的TCP连接。建立连接的过程可以被划分为两个步骤:加密握手和子协议握手。加密握手基于ECIES构造接下来通信使用的对称加密密钥，子协议握手为通信双方沟通子协议名称和版本，选择合适的协议进行数据传输。通讯双

方首先向对方发送一条HELLO消息,其中包含了自身节点ID、DEVp2p协议版本、客户端名称、支持的应用层协议以及本地监听的端口号(默认30303)。

[0008] 节点发现协议的规范指明每一次返回的相邻数据包将包括16条节点记录,这些节点记录在数据库中与发现节点发送的记录距离最近。此前的探测方法并没有考虑节点数据库中存储的历史节点记录,对每个节点的探测只有一次发现节点和相邻数据包往返,因此仅能获取相当有限的节点记录条目。

## 发明内容

[0009] 为了解决上述现有技术的不足,本发明提供了一种基于仿真技术的以太坊网络探测方法、装置、计算机设备和存储介质,该方法基于仿真技术创建启动节点后,利用原有节点发现协议的特点,通过利用节点发现协议的特点,对对等节点进行反复查询并聚合去重,节点数据库得到此前未被分析的节点相识关系,进而利用采集到的节点相识关系以及节点元数据对以太坊网络中节点的行为进行分析,发现的活跃节点数量比现有其他方法都多,表明本方法可以更加完整地展现以太坊网络的性质。

[0010] 本发明的第一个目的在于提供一种基于仿真技术的以太坊网络探测方法。

[0011] 本发明的第二个目的在于提供一种基于仿真技术的以太坊网络探测装置。

[0012] 本发明的第三个目的在于提供一种计算机设备。

[0013] 本发明的第四个目的在于提供一种存储介质。

[0014] 本发明的第一个目的可以通过采取如下技术方案达到:

[0015] 一种基于仿真技术的以太坊网络探测方法,所述方法包括:

[0016] 采集数据,所述数据包括节点相识关系和节点元数据;创建启动节点后,通过利用节点发现协议的特点,对对等节点进行反复查询并聚合去重,节点数据库得到此前未被分析的节点相识关系;

[0017] 根据所述节点相识关系和节点元数据,对以太坊网络中节点的行为进行分析。

[0018] 进一步的,所述根据所述节点相识关系和节点元数据,对以太坊网络中节点的行为进行分析,包括:

[0019] 将所有节点相识关系和节点元数据保存在本地数据库中,对本地数据库中的数据进行分表;

[0020] 将表中的节点划分为活跃节点、关键节点、路由节点以及恶意节点;

[0021] 统计各表中节点的类别;

[0022] 根据统计结果,对以太坊网络中节点的行为进行分析。

[0023] 进一步的,所述对本地数据库中的数据进行分表,即按照节点类型对本地数据库中的数据进行分表,包括活跃节点表、相识关系表以及关键节点表。

[0024] 进一步的,所述根据统计结果,对以太坊网络中节点的行为进行分析,包括:

[0025] 根据统计结果计算各类活跃节点在网络中所占的比重;

[0026] 遍历相识关系表,找出全部活跃节点,采用PageRank算法分析表中的关键节点及其影响因子;针对恶意节点进行分析,对伪造行为的原理以及对网络的影响进行分析。

[0027] 进一步的,所述活跃节点为当前存在于网络中正常运行区块链协议的节点,是区块链运行不可或缺的因素;

[0028] 所述关键节点为活跃节点，并拥有优秀的网络条件和硬件资源，对新区块的出块和广播有着很大影响力；

[0029] 所述路由节点为一类特殊的节点，不运行任何应用层协议，只进行节点记录的转发，对新节点快速加入区块链网络具有重要意义；

[0030] 所述恶意节点不运行任何区块链协议，也没有与其他节点的相识关系，却大量广播伪造的节点记录或伪造节点身份让活跃节点与其进行连接的特殊节点。

[0031] 进一步的，所述节点元数据包括节点记录序号、客户端版本及开发语言、操作系统类型以及支持的应用层协议，其中：

[0032] 获取节点记录序号数据包括：

[0033] 启动节点向远程节点模拟发送ENR Request Packet，从接收到的ENR Response Packet中解析出节点记录序号数据；

[0034] 获取其余元数据包括：

[0035] 启动节点与远程节点完成RLPx协议的ECIES握手后，双方再进行协议握手，在协议握手阶段从对方的握手包中获取客户端版本及开发语言、操作系统类型以及支持的应用层协议；根据对以太坊客户端源码的分析，当远程节点返回错误信息“too many peers”时将此节点视为连接超过50个节点，作为活跃节点。

[0036] 进一步的，所述采集数据，通过探测器采集数据，包括仿真节点初始化和递归搜索，其中：

[0037] 所述仿真节点初始化包括：

[0038] 在初始状态下，基于仿真技术创建启动节点，并为启动节点指定一系列种子节点，启动节点对种子节点进行递归搜索直到没有新节点出现，即完成对整个以太坊网络的搜索；

[0039] 所述递归搜索包括：

[0040] 针对每个节点的查询过程包括：发送UDP数据包在节点发现协议上获取节点相识的所有节点，再与其建立TCP连接并且通过模拟RLPx协议的握手过程来获取节点相应的元数据，从而获得需要采集的数据。

[0041] 本发明的第二个目的可以通过采取如下技术方案达到：

[0042] 一种基于仿真技术的以太坊网络探测装置，所述装置包括：

[0043] 数据采集模块，用于采集数据，所述数据包括节点相识关系和节点元数据；创建启动节点后，通过利用节点发现协议的特点，对对等节点进行反复查询并聚合去重，节点数据库得到此前未被分析的节点相识关系；

[0044] 行为分析模块，用于根据所述节点相识关系和节点元数据，对以太坊网络中节点的行为进行分析。

[0045] 本发明的第三个目的可以通过采取如下技术方案达到：

[0046] 一种计算机设备，包括处理器以及用于存储处理器可执行程序的存储器，所述处理器执行存储器存储的程序时，实现上述的以太坊网络探测方法。

[0047] 本发明的第四个目的可以通过采取如下技术方案达到：

[0048] 一种存储介质，存储有程序，所述程序被处理器执行时，实现上述的以太坊网络探测方法。

[0049] 本发明相对于现有技术具有如下的有益效果：

[0050] 1、本发明通过利用节点发现协议的特点，对对等节点进行反复查询并聚合去重，节点数据库中得到此前未被分析的节点相识关系；进而根据节点相识关系以及节点元数据对节点的行为进行分析，发现的活跃节点数量比现有其他方法都多，说明本方法可以更加完整的展现以太坊网络性质，即本方法在以太坊网络中具有更强的适用性。

[0051] 2、本发明通过对路由节点的定义，对提高网络拓扑的建立效率具有举足轻重的作用，进而通过对关键节点行为的分析，发现底层点对点网络有着向中心化发展的趋势。

[0052] 3、通过采用本发明提供的方法，发现了大量的节点记录伪造行为，有益于今后对以太坊网络的通信效率和网络安全问题工作进行定量分析。

## 附图说明

[0053] 为了更清楚地说明本发明实施例或现有技术中的技术方案，下面将对实施例或现有技术描述中所需要使用的附图作简单地介绍，显而易见地，下面描述中的附图仅仅是本发明的一些实施例，对于本领域普通技术人员来讲，在不付出创造性劳动的前提下，还可以根据这些附图示出的结构获得其他的附图。

[0054] 图1为本发明实施例1的基于仿真技术的以太坊网络探测方法的原理图。

[0055] 图2为本发明实施例1的基于仿真技术的以太坊网络探测方法的流程图。

[0056] 图3为本发明实施例1的仿真节点在网络中运行的示意图。

[0057] 图4为本发明实施例2的基于仿真技术的以太坊网络探测装置的结构框图。

[0058] 图5为本发明实施例3的计算机设备的结构框图。

## 具体实施方式

[0059] 为使本发明实施例的目的、技术方案和优点更加清楚，下面将结合本发明实施例中的附图，对本发明实施例中的技术方案进行清楚、完整地描述，显然，所描述的实施例是本发明的一部分实施例，而不是全部的实施例，基于本发明中的实施例，本领域普通技术人员在没有作出创造性劳动前提下所获得的所有其他实施例，都属于本发明保护的范围。应当理解，描述的具体实施例仅仅用以解释本申请，并不用于限定本申请。

[0060] 实施例1：

[0061] 如图1、2所示，本实施例提供一种基于仿真技术的以太坊网络探测方法，该方法通过利用节点发现协议的特点，对对等节点进行反复查询并聚合去重，可以从节点数据库中得到此前未被分析的节点相识关系，进而利用采集到的节点相识关系以及节点元数据，可以对以太坊网络中节点的行为进行分析总结。

[0062] S101、通过探测器采集的数据包括节点相识关系和节点元数据。

[0063] 本实施例通过探测器采集的数据包括两种主要数据：节点相识关系和节点元数据，其中：

[0064] (1)节点相识关系。

[0065] 将每个节点本地数据库中存储的节点记录视作此节点的相识节点。节点发现协议的规范指明每一次返回的邻居数据包包括16条节点记录，这些节点记录在数据库中与发现节点发送的记录距离最近。此前的探测方法中没有考虑节点数据库中存储的历史节点记

录,对每个节点的探测只有一次发现节点和邻居数据包往返,因此仅能获取相当有限的节点记录条目。本发明采用反复查询,聚合后去重的方法获取对等节点保存的所有节点记录,将这种节点保存了另一个节点的节点记录的非对称关系称为节点相识关系,得到了此前未被分析的节点相识关系。

[0066] (2)节点元数据。

[0067] 节点元数据包括节点记录序号、客户端版本及开发语言、操作系统类型以及支持的应用层协议。节点记录序号被称作seq,其数值可以从节点发现协议中获取。由于Geth和Parity客户端针对Ethereum Node Records标准的实现不同,Geth客户端的seq从0开始自增,而Patiry客户端选择使用随机数作为初始值,因此可以将Geth客户端的seq数值高低作为节点活跃度的衡量指标之一。RLPx协议完成加密握手过程后,需要继续执行协议握手,这一过程双方之间需要交换客户端名称以及支持的子协议,其余的数据可以在协议握手中获取。

[0068] 获取节点元数据的过程包括以下步骤:

[0069] (2-1)获取节点记录序号。

[0070] 启动节点向远程节点模拟发送ENR Request Packet,从接收到的ENR Response Packet中解析出节点记录序号(seq)数据。

[0071] (2-2)获取其余元数据。

[0072] 启动节点与远程节点首先完成RLPx协议的ECIES握手,下一步双方将进行协议握手,在这一阶段可以从对方的握手包中获取客户端版本、应用层协议等其他信息。根据对以太坊客户端源码的分析,当远程节点返回错误信息“too many peers”时将此节点视为连接超过50个节点,属于相当活跃的节点。

[0073] (3)通过探测器采集数据。

[0074] 本实施例通过探测器采集的数据包括节点相识关系和节点元数据,具体过程如下:

[0075] 如图3所示,仿真节点在网络中的运行包括初始化和递归搜索两个步骤。探测器使用go语言在1.17版本下编译运行。为了提高数据存取效率,所有节点记录和相识关系保存在LevelDB中,并通过前缀编码的方式模拟表结构来进行管理。探测器还提供了RPC接口来实时监控数据采集进度和当前发现的网络状态,其中:

[0076] (3-1)仿真节点初始化。

[0077] 在初始状态下需要创建启动节点,该启动节点基于仿真技术虚拟化得出;此后为启动节点指定一系列种子节点,启动节点将对种子节点进行递归搜索直到没有新节点出现,即完成对整个以太坊网络的搜索。

[0078] (3-2)递归搜索。

[0079] 针对每个节点的查询过程也分成两步,首先发送UDP数据包在节点发现协议上获取此节点相识的所有节点,之后与其建立TCP连接并且通过模拟RLPx协议的握手过程来获取此节点相应的元数据。经过以上两个步骤就可以得到最终的实验数据集,即节点相识关系和节点元数据。

[0080] S102、根据节点相识关系和节点元数据,对以太坊节点的行为进行分析。

[0081] 进一步的,步骤S102具体包括:

[0082] (1)数据分表。

[0083] 在查询过程中为了提高数据存取效率,所有节点记录和相识关系保存在LevelDB本地数据库中,并通过前缀编码的方式模拟表结构来进行管理。

[0084] 在对整个以太坊网络数据进行抓取结束后,使用Python对数据库中的数据按照行为类型进行分表,包括活跃节点表、相识关系表以及关键节点表等。

[0085] 本实施例提供的一个案例是从2021年12月2日到2022年3月2日,对以太坊网络进行了持续一个季度的监测,共采集33G共计2亿余条原始数据。探测器布置在服务器上(Intel(R) Xeon(R) Gold 5220 CPU @ 2.20GHz *72 CPU, 128G RAM,2TB SSD),操作系统为Linux 18.04。数据分析程序基于python3.9版本,使用levelDB作为本地数据库对数据进行分类存储。

[0086] (2)节点定义。

[0087] 为了便于分析和描述,依照网络中的典型行为将节点划分为四类:活跃节点、关键节点、路由节点以及恶意节点,其中:

[0088] (2-1)活跃节点。

[0089] 活跃节点指当前存在于网络中可以正常运行区块链协议的节点,是区块链运行不可或缺的因素。若节点满足以下任意一个条件,则称之为活跃节点:

[0090] (a)该节点在RLPx协议握手阶段返回非错误元数据;

[0091] (b)可通过Node Discovery Protocol v5获得非空ENR记录;

[0092] (c)至少连接过其他节点一次(认识的节点超过一个)。

[0093] 活跃节点代表以太坊网络中正常运行的节点,是所有点对点网络运行的根基,通过研究活跃节点可以得出以太坊网络的拓扑结构,从而了解以太坊自身能否安全稳定运行。

[0094] (2-2)关键节点。

[0095] 关键节点首先必须是活跃节点,并且拥有优秀的网络的条件和硬件资源,对新区块的出块和广播有着很大的影响力。通过对采集到的网络拓扑数据进行分析发现,底层网络有着向关键节点中心化发展的趋势。若节点满足以下所有条件,则称之为关键节点:

[0096] (a)运行最新版本客户端,表明此节点被积极维护;

[0097] (b)对等节点数量超过50,表明此节点对外活跃度很高;

[0098] (c)相识节点个数超过50000,表明此节点长期稳定运行。相识节点指本地节点在节点发现协议中发现的所有节点,保存在节点数据库中。

[0099] 关键节点被精心维护,在区块链网络中占据核心地位。从出块情况看,它们占据了绝大多数算力,属于高价值节点,最容易成为攻击的目标。

[0100] (2-3)路由节点。

[0101] 路由节点是一类特殊的节点,它们不运行任何应用层协议,只进行节点记录的转发,它们对新节点快速加入区块链网络具有重要意义。

[0102] (2-4)恶意节点。

[0103] 恶意节点指不运行任何区块链协议,也没有与其他节点的相识关系,却大量广播伪造的节点记录或伪造节点身份让活跃节点与其进行连接的特殊节点。恶意节点会造成以太坊网络效率降低,并对特定节点的安全性造成重大影响。恶意节点的典型行为是伪造节

点记录,这一主动进行的恶意行为进一步加剧了底层网络的混乱。恶意伪造节点记录是指攻击者生成大量随机公钥封装成节点记录后向外广播。

[0104] 本实施例提供的一个案例是经过一个季度的探测后,最终得到2578458条节点记录、124972682条相识关系。根据节点的典型行为将其划分成活跃节点、关键节点、路由节点、恶意节点四类。从数量上看,最终得到64559个活跃节点,其中包括关键节点和2039个路由节点。活跃节点数量相比两年前翻了一番,说明以太坊网络规模在近两年快速扩张。同时通过采用本发明提供的方法,发现的活跃节点数量也比当前其余方法都多,说明本方法可以更加完整的展现以太坊网络性质。从节点性质上看,路由节点对提高网络拓扑的建立效率具有举足轻重的作用,关键节点对新区块出块和上链有主导作用,底层点对点网络有着向中心化发展的趋势。

[0105] 恶意节点的典型行为是伪造节点记录,这一主动进行的恶意行为进一步加剧了底层网络的混乱。恶意伪造节点记录是指攻击者生成大量随机公钥封装成节点记录后向外广播。Kademlia算法是造成恶意伪造节点记录行为的根本原因,攻击者只需要伪造大量不同公钥的节点记录并向外广播,就总会有距离相近的节点主动传递虚假记录到整个网络中。这一行为将迅速污染网络中大部分节点的节点数据库。攻击者还可以使用这种方法对任意节点发起日食攻击,因此所有关键节点都应该配置预防措施避免受到日食攻击。此外,不仅有恶意伪造的节点记录,还有许多关键节点为了提高网络权重,刻意生成不同的节点记录,诱导其余节点主动建立连接。这一行为明显不利于节点间的公平竞争,增强了网络的中心化。

[0106] 针对当前以太坊网络中存在着普遍的节点记录伪造行为,目前全部记录中有近半数记录为随机伪造。导致这种伪造行为的根源在于以太坊节点发现协议使用的路由算法,区块链网络中各方为了自身利益,基于种种原因都有重复伪造记录的动机,这些动机将会产生的现象也与实际发现的数据相符。

[0107] (3)数据统计。

[0108] 统计各表节点的所携带元数据并绘制统计图、IP地图以及热力图等,便于直观的观察分析。

[0109] (4)数据分析。

[0110] 总结各类活跃节点在网络中所占的比重;遍历关系表,找出全部活跃节点,采用PageRank算法分析节点表中的关键节点及其影响因子;针对恶意节点进行分析,揭示出以太坊网络中普遍存在的伪造节点记录行为,并对伪造行为的原理、目的以及对网络的影响进行分析,最后提出普通节点的应对方案。

[0111] 本领域技术人员可以理解,实现上述实施例的方法中的全部或部分步骤可以通过程序来指令相关的硬件来完成,相应的程序可以存储于计算机可读存储介质中。

[0112] 应当注意,尽管在附图中以特定顺序描述了上述实施例的方法操作,但是这并非要求或者暗示必须按照该特定顺序来执行这些操作,或是必须执行全部所示的操作才能实现期望的结果。相反,描绘的步骤可以改变执行顺序。附加地或备选地,可以省略某些步骤,将多个步骤合并为一个步骤执行,和/或将一个步骤分解为多个步骤执行。

[0113] 实施例2:

[0114] 如图4所示,本实施例提供了一种基于仿真技术的以太坊网络探测装置,该装置包

括数据采集模块401和行为分析模块402,其中:

[0115] 数据采集模块401,用于采集数据,所述数据包括节点相识关系和节点元数据;创建启动节点后,通过利用节点发现协议的特点,对对等节点进行反复查询并聚合去重,节点数据库得到此前未被分析的节点相识关系;

[0116] 行为分析模块402,用于根据所述节点相识关系和节点元数据,对以太坊网络中节点的行为进行分析。

[0117] 本实施例中各个模块的具体实现可以参见上述实施例1,在此不再一一赘述;需要说明的是,本实施例提供的装置仅以上述各功能模块的划分进行举例说明,在实际应用中,可以根据需要而将上述功能分配由不同的功能模块完成,即将内部结构划分成不同的功能模块,以完成以上描述的全部或者部分功能。

[0118] 实施例3:

[0119] 本实施例提供了一种计算机设备,该计算机设备可以为计算机,如图5所示,其通过系统总线501连接的处理器502、存储器、输入装置503、显示器504和网络接口505,该处理器用于提供计算和控制能力,该存储器包括非易失性存储介质506和内存储器507,该非易失性存储介质506存储有操作系统、计算机程序和数据库,该内存储器507为非易失性存储介质中的操作系统和计算机程序的运行提供环境,处理器502执行存储器存储的计算机程序时,实现上述实施例1的以太坊网络探测方法,如下:

[0120] 采集数据,所述数据包括节点相识关系和节点元数据;创建启动节点后,通过利用节点发现协议的特点,对对等节点进行反复查询并聚合去重,节点数据库得到此前未被分析的节点相识关系;

[0121] 根据所述节点相识关系和节点元数据,对以太坊网络中节点的行为进行分析。

[0122] 实施例4:

[0123] 本实施例提供了一种存储介质,该存储介质为计算机可读存储介质,其存储有计算机程序,所述计算机程序被处理器执行时,实现上述实施例1的以太坊网络探测方法,如下:

[0124] 采采集数据,所述数据包括节点相识关系和节点元数据;创建启动节点后,通过利用节点发现协议的特点,对对等节点进行反复查询并聚合去重,节点数据库得到此前未被分析的节点相识关系;

[0125] 根据所述节点相识关系和节点元数据,对以太坊网络中节点的行为进行分析。

[0126] 需要说明的是,本实施例的计算机可读存储介质可以是计算机可读信号介质或者计算机可读存储介质或者是上述两者的任意组合。计算机可读存储介质例如可以是但不限于电、磁、光、电磁、红外线、或半导体的系统、装置或器件,或者任意以上的组合。计算机可读存储介质的更具体的例子可以包括但不限于:具有一个或多个导线的电连接、便携式计算机磁盘、硬盘、随机访问存储器(RAM)、只读存储器(ROM)、可擦式可编程只读存储器(EPROM或闪存)、光纤、便携式紧凑磁盘只读存储器(CD-ROM)、光存储器件、磁存储器件、或者上述的任意合适的组合。

[0127] 综上所述,本发明通过采集全网节点本地数据库中存储的所有节点记录,获取更加完整全面的数据来对网络状态进行分析,并对发现的节点进行分类总结,将节点划分为活跃节点、关键节点、路由节点以及恶意节点,同时分析它们对网络的影响,并对伪造节点

的恶意行为模式进行分析。

[0128] 以上所述，仅为本发明专利较佳的实施例，但本发明专利的保护范围并不局限于此，任何熟悉本技术领域的技术人员在本发明专利所公开的范围内，根据本发明专利的技术方案及其发明构思加以等同替换或改变，都属于本发明专利的保护范围。

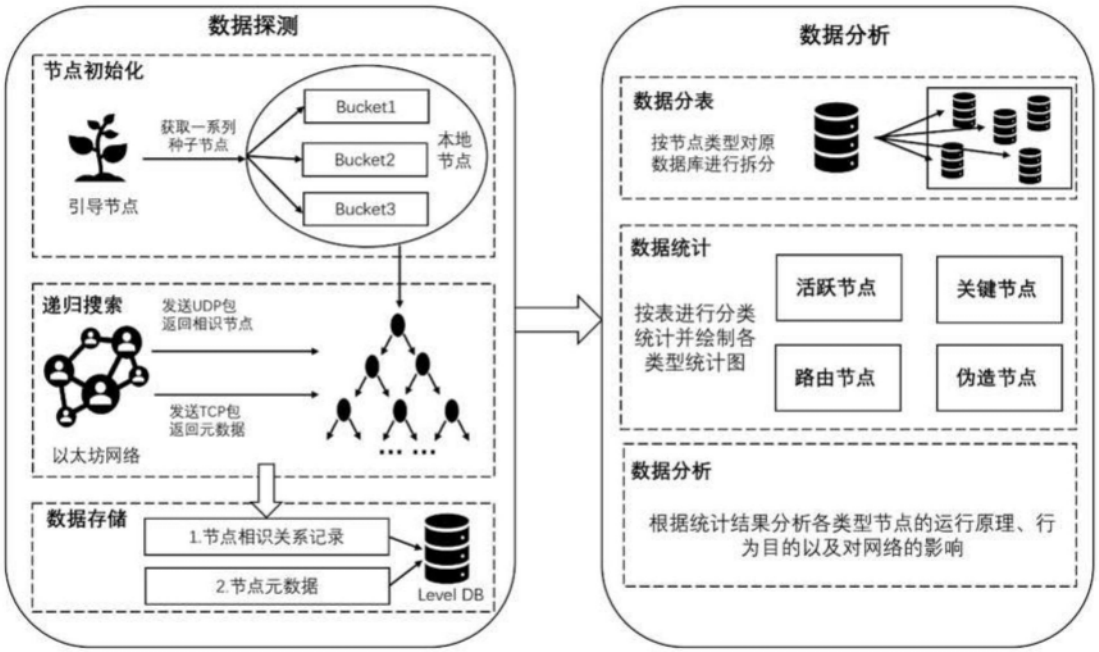

数据探测
节点初始化
获取一系列
种子节点
Bucket1
Bucket2
Bucket3
本地
节点
引导节点
递归搜索
发送UDP包
返回相识节点
发送TCP包
返回元数据
以太坊网络
数据存储
1.节点相识关系记录
2.节点元数据
Level DB
数据分析
数据分表
按节点类型对原
数据库进行拆分
数据统计
按表进行分类
统计并绘制各
类型统计图
活跃节点
关键节点
路由节点
伪造节点
数据分析
根据统计结果分析各类型节点的运行原理、行
为目的以及对网络的影响

图1

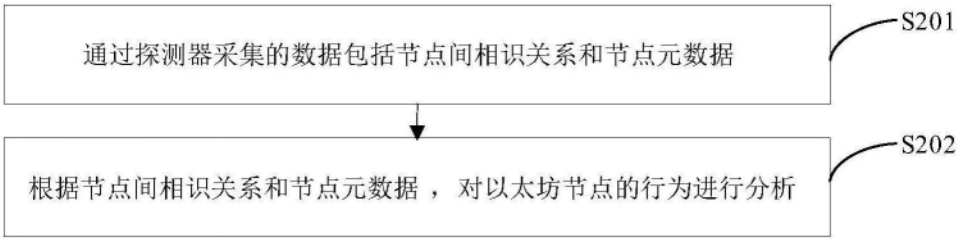

通过探测器采集的数据包括节点间相识关系和节点元数据
S201
根据节点间相识关系和节点元数据 ， 对以太坊节点的行为进行分析
S202

图2

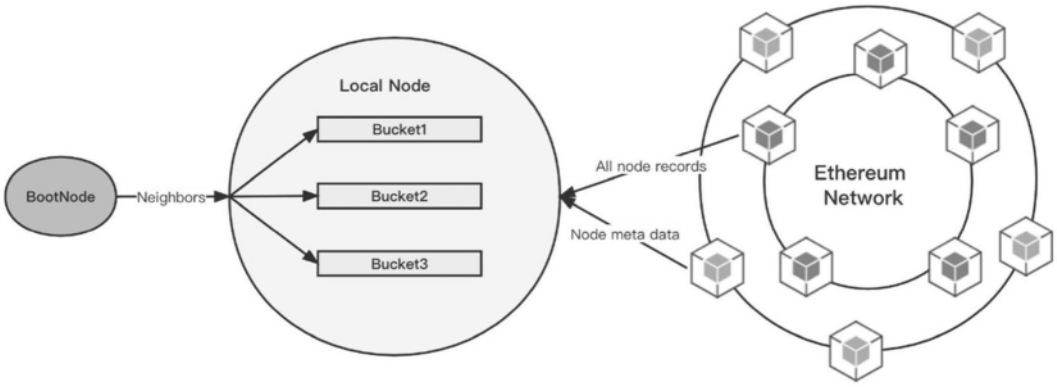

Local Node
Bucket1
Bucket2
Bucket3
BootNode
Neighbors
All node records
Node meta data
Ethereum
Network

图3

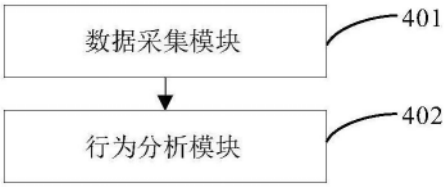

数据采集模块
401
行为分析模块
402

图4

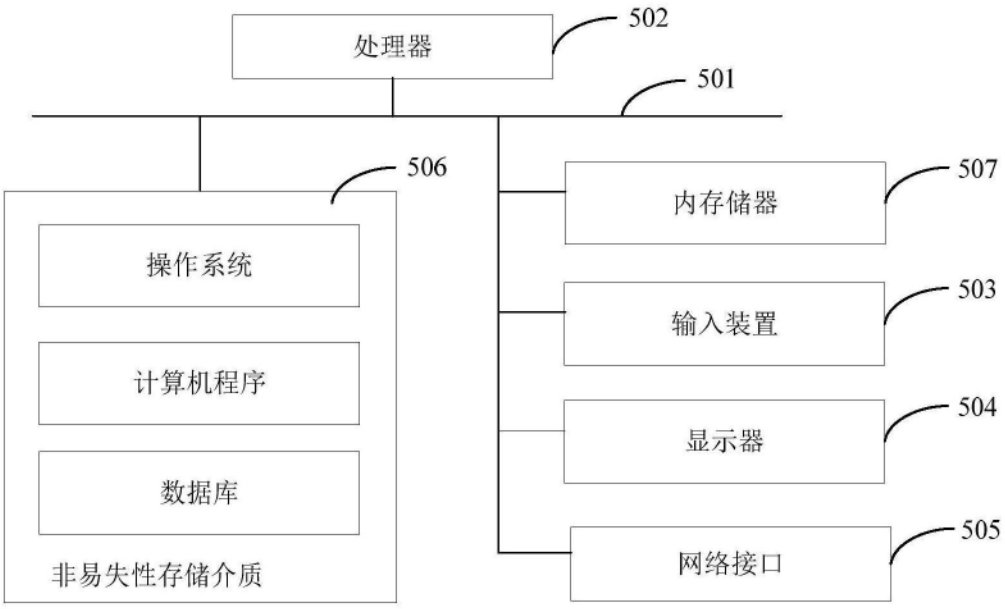

处理器
502
501
506
操作系统
计算机程序
数据库
非易失性存储介质
内存储器
507
输入装置
503
显示器
504
网络接口
505

图5