(19)中华人民共和国国家知识产权局

(12)发明专利

(10)授权公告号 CN 108965259 B
(45)授权公告日 2021.03.26

(21)申请号 201810643035.5
(22)申请日 2018.06.21
(65)同一申请的已公布的文献号
申请公布号 CN 108965259 A
(43)申请公布日 2018.12.07
(73)专利权人 佛山科学技术学院
地址 528000 广东省佛山市南海区狮山镇仙溪水库西路佛山科学技术学院
(72)发明人 朱珍 谢建勤 霍颖瑜
(74)专利代理机构 广州嘉权专利商标事务所有限公司 44205
代理人 王国标
(51)Int.Cl.
H04L 29/06(2006.01)
H04L 9/06(2006.01)

审查员 曾建琼

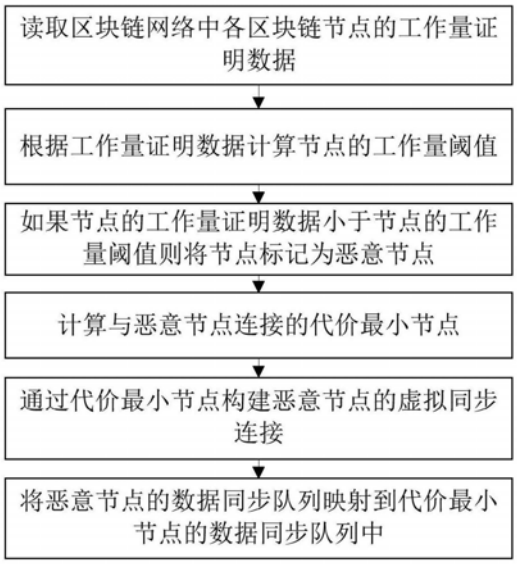
权利要求书2页 说明书5页 附图1页

(54)发明名称

一种区块链恶意节点发现与隔离方法及装置

(57)摘要

本发明公开了一种区块链恶意节点发现与隔离方法及装置,为每一个区块链网络中的区块的节点计算工作量,如果发现工作量超过了区块的阈值,则将该区块的节点标识为恶意节点,并执行恶意节点隔离程序,大大提高了整个区块链的可靠性,在不影响区块链节点的服务下,隔离了恶意的区块链节点,提升了区块链系统的容错能力,保证了在区块链系统中某些区块出现恶意节点的情况下,仍然能保证区块链系统正常运行。



CN 108965259 B

1.一种区块链恶意节点发现与隔离方法,其特征在于,所述方法包括以下步骤:

步骤1,读取区块链网络中各区块链节点的工作量证明数据,所述工作量证明数据为区块链节点的数据同步总时间的十进制形式经过SHA256哈希运算的递增值字符串,SHA256哈希运算的方法为:将十进制数X看作十三进制,再按照十三进制数以转换基数转换成十进制数,提取转换后的十进制数的其中若干位作为X的哈希值,所述转换基数为大于原来基数的数,并且两个基数应该是互素的;

步骤2,根据工作量证明数据计算节点的工作量阈值;工作量阈值为计算节点工作量证明数据与相邻节点工作量证明数据总和的加权几何平均数;

步骤3,如果节点的工作量证明数据小于节点的工作量阈值则将节点标记为恶意节点;

步骤4,计算与恶意节点连接的代价最小节点;

步骤5,通过代价最小节点构建恶意节点的虚拟同步连接,具体为:将恶意节点断开连接,将与恶意节点断开的连接重新连接至代价最小节点;

步骤6,将恶意节点的数据同步队列映射到代价最小节点的数据同步队列中,具体为:将恶意节点的数据同步队列中的数据同步请求按照原队列的顺序依次添加到代价最小节点的数据同步队列中,同时清空恶意节点的数据同步队列;

在步骤4中,所述计算与恶意节点连接的代价最小节点的方法包括以下子步骤:

步骤4.1,恶意节点发送同步数据包请求给区块链中所有的节点;

步骤4.2,各区块链节点接收到同步数据包请求后返回应答数据包到恶意节点;

步骤4.3,恶意节点接收应答数据包,应答响应时间最短的节点为代价最小节点;

所述应答数据包至少包括应答节点ID编号、应答响应时间。

2.根据权利要求1所述的一种区块链恶意节点发现与隔离方法,其特征在于,在步骤1中,所述区块链网络为多个区块链节点构成的网状拓扑结构,每个区块链节点都有唯一的节点ID编号、数据同步队列,所述数据同步队列用于按照同步发生时间的顺序将数据同步请求排队依次进行数据同步,同步序列队列中的元素为数据同步请求,每个区块链节点至少有一个相邻的节点,所述各区块链节点通过有线网络、无线网络任意一种互相连接并进行通信。

3.一种区块链恶意节点发现与隔离装置,其特征在于,所述装置包括:存储器、处理器以及存储在所述存储器中并可在所述处理器上运行的计算机程序,所述处理器执行所述计算机程序运行在以下装置的单元中:

工作量读取单元,用于读取区块链网络中各区块链节点的工作量证明数据;所述工作量证明数据为区块链节点的数据同步总时间的十进制形式经过SHA256哈希运算的递增值字符串,SHA256哈希运算的方法为:将十进制数X看作十三进制,再按照十三进制数以转换基数转换成十进制数,提取转换后的十进制数的其中若干位作为X的哈希值,所述转换基数为大于原来基数的数,并且两个基数应该是互素的;

阈值计算单元,用于根据工作量证明数据计算节点的工作量阈值;工作量阈值为计算节点工作量证明数据与相邻节点工作量证明数据总和的加权几何平均数;

恶意标记单元,用于在如果节点的工作量证明数据小于节点的工作量阈值时将节点标记为恶意节点;

代价计算单元,用于计算与恶意节点连接的代价最小节点;

虚拟连接单元，用于通过代价最小节点构建恶意节点的虚拟同步连接，具体为：将恶意节点断开连接，将与恶意节点断开的连接重新连接至代价最小节点；

队列映射单元，用于将恶意节点的数据同步队列映射到代价最小节点的数据同步队列中，具体为：将恶意节点的数据同步队列中的数据同步请求按照原队列的顺序依次添加到代价最小节点的数据同步队列中，同时清空恶意节点的数据同步队列；

所述代价计算单元用于计算与恶意节点连接的代价最小节点包括：

恶意节点发送同步数据包请求给区块链中所有的节点；

各区块链节点接收到同步数据包请求后返回应答数据包到恶意节点；

恶意节点接收应答数据包，应答响应时间最短的节点为代价最小节点；

所述应答数据包至少包括应答节点ID编号、应答响应时间。

一种区块链恶意节点发现与隔离方法及装置

技术领域

[0001] 本公开涉及区块链技术领域,具体涉及一种区块链恶意节点发现与隔离方法及装置。

背景技术

[0002] 区块链网络是一种开放的、不受限制的网络,各区块链节点对整个网络的了解是十分有限的,每个区块链节点只需维护邻居节点的信息,并进行实时更新,就可以保证整个网络正常运行。也正因为如此,区块链网络的安全问题也特别突出:恶意节点通过伪装自己,可自由加入或离开区块链网络,并可利用区块链节点的局限性来发动攻击或破坏网络的完整性。

[0003] 目前,针对区块链网络的Sybil攻击、日蚀攻击(Eclipse Attack)、DDoS(Distributed Denial of Service,分布式拒绝服务)攻击等的相关研究在国际国内获得了广泛关注。Sybil攻击通过向区块链网络中引入多个恶意构造的节点来达到控制整个层叠网络的目的,它可以被用于监控发布和搜索流量、隔离特定共享内容等;日蚀攻击的目的是将若干个目标节点从区块链网络中隔离出去,劫持其通信信息,控制其网络行为。DDoS攻击的目标是单个区块链网络节点,占用甚至耗尽其资源(如CPU、带宽等),使其不能正常提供服务。目前暂无相关的同类技术以防止该类问题的发生。

发明内容

[0004] 本公开提供一种区块链恶意节点发现与隔离方法及装置,本发明为每一个区块链网络中的区块的节点计算工作量,如果发现工作量超过了区块的阈值,,如果发现错误计数器的错误数量超过了阈值,则将该区块的节点标识为恶意节点,并执行恶意节点隔离程序。

[0005] 为了实现上述目的,根据本公开的一方面,提供一种区块链恶意节点发现与隔离方法,所述方法包括以下步骤:

[0006] 步骤1,读取区块链网络中各区块链节点的工作量证明数据;

[0007] 步骤2,根据工作量证明数据计算节点的工作量阈值;

[0008] 步骤3,如果节点的工作量证明数据小于节点的工作量阈值则将节点标记为恶意节点;

[0009] 步骤4,计算与恶意节点连接的代价最小节点;

[0010] 步骤5,通过代价最小节点构建恶意节点的虚拟同步连接;

[0011] 步骤6,将恶意节点的数据同步队列映射到代价最小节点的数据同步队列中。

[0012] 进一步地,在步骤1中,所述区块链网络为多个区块链节点构成的网状拓扑结构,每个区块链节点都有唯一的节点ID编号、数据同步队列,所述数据同步队列用于按照同步发生时间的顺序将数据同步请求排队依次进行数据同步,同步序列队列中的元素为数据同步请求,每个区块链节点至少有一个相邻的节点,所述各区块链节点通过有线网络、无线网络任意一种互相连接并进行通信。

[0013] 进一步地，在步骤1中，所述工作量证明数据包括区块链节点的数据同步总时间的十进制形式经过SHA256哈希运算的递增值字符串，SHA256哈希运算的方法为：将十进制数X看作十三进制，再按照十三进制数以转换基数转换成十进制数，提取其中若干为作为X的哈希值，所述转换基数为大于原来基数的数，并且两个基数应该是互素的，所述数据同步总时间的十进制形式，例如数据同步总时间为80127429秒，则十进制形式为$(80127429)_{10}$。

[0014] 例如：

[0015] $Hash(80127429)=(80127429)_{13}=8*137+0*136+1*135+2*134+7*133+4*132+2*131+9=(502432641)_{10}$，如果取中间三位作为哈希值，得Hash(80127429)＝432。

[0016] 进一步地，在步骤2中，所述根据工作量证明数据计算节点的工作量阈值的方法为：工作量阈值为计算节点工作量证明数据与相邻节点工作量证明数据总和的加权几何平均数。

[0017] 进一步地，在步骤4中，所述计算与恶意节点连接的代价最小节点的方法包括以下子步骤：

[0018] 步骤4.1，恶意节点发送同步数据包请求给区块链中所有的节点；

[0019] 步骤4.2，各区块链节点接收到同步数据包请求后返回应答数据包到恶意节点；

[0020] 步骤4.3，恶意节点接收应答数据包，应答响应时间最短的节点为代价最小节点；

[0021] 所述应答数据包至少包括应答节点ID编号、应答响应时间。

[0022] 进一步地，在步骤5中，通过代价最小节点构建恶意节点的虚拟同步连接的方法为：将恶意节点断开连接，将与恶意节点断开的连接重新连接至代价最小节点。

[0023] 进一步地，在步骤6中，所述将恶意节点的数据同步队列映射到代价最小节点的数据同步队列中的方法为：将恶意节点的数据同步队列中的数据同步请求按照原队列的顺序依次添加到代价最小节点的数据同步队列中，同时清空恶意节点的数据同步队列。

[0024] 本发明还提供了一种区块链恶意节点发现与隔离装置，所述装置包括：存储器、处理器以及存储在所述存储器中并可在所述处理器上运行的计算机程序，所述处理器执行所述计算机程序运行在以下装置的单元中：

[0025] 工作量读取单元，用于读取区块链网络中各区块链节点的工作量证明数据；

[0026] 阈值计算单元，用于根据工作量证明数据计算节点的工作量阈值；

[0027] 恶意标记单元，用于在如果节点的工作量证明数据小于节点的工作量阈值时将节点标记为恶意节点；

[0028] 代价计算单元，用于计算与恶意节点连接的代价最小节点；

[0029] 虚拟连接单元，用于通过代价最小节点构建恶意节点的虚拟同步连接；

[0030] 队列映射单元，用于将恶意节点的数据同步队列映射到代价最小节点的数据同步队列中。

[0031] 本公开的有益效果为：本发明提供一种区块链恶意节点发现与隔离方法及装置，大大提高了整个区块链的可靠性，在不影响区块链节点的服务下，进一步发挥了区块链系统的聚合特性，提升了区块链系统的容错能力，保证了在区块链系统中某些区块出现恶意节点的情况下隔离恶意节点后，仍然能保证区块链系统正常运行，不影响区块链的同步效率。

附图说明

[0032] 通过对结合附图所示出的实施方式进行详细说明，本公开的上述以及其他特征将更加明显，本公开附图中相同的参考标号表示相同或相似的元素，显而易见地，下面描述中的附图仅仅是本公开的一些实施例，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获得其他的附图，在附图中：

[0033] 图1所示为一种区块链恶意节点发现与隔离方法的流程图；

[0034] 图2所示为一种区块链恶意节点发现与隔离装置图。

具体实施方式

[0035] 以下将结合实施例和附图对本公开的构思、具体结构及产生的技术效果进行清楚、完整的描述，以充分地理解本公开的目的、方案和效果。需要说明的是，在不冲突的情况下，本申请中的实施例及实施例中的特征可以相互组合。

[0036] 如图1所示为根据本公开的一种区块链恶意节点发现与隔离方法的流程图，下面结合图1来阐述根据本公开的实施方式的一种区块链恶意节点发现与隔离方法。

[0037] 本公开提出一种区块链恶意节点发现与隔离方法，具体包括以下步骤：

[0038] 步骤1，读取区块链网络中各区块链节点的工作量证明数据；

[0039] 步骤2，根据工作量证明数据计算节点的工作量阈值；

[0040] 步骤3，如果节点的工作量证明数据小于节点的工作量阈值则将节点标记为恶意节点；

[0041] 步骤4，计算与恶意节点连接的代价最小节点；

[0042] 步骤5，通过代价最小节点构建恶意节点的虚拟同步连接；

[0043] 步骤6，将恶意节点的数据同步队列映射到代价最小节点的数据同步队列中。

[0044] 进一步地，在步骤1中，所述区块链网络为多个区块链节点构成的网状拓扑结构，每个区块链节点都有唯一的节点ID编号、数据同步队列，所述数据同步队列用于按照同步发生时间的顺序将数据同步请求排队依次进行数据同步，同步序列队列中的元素为数据同步请求，每个区块链节点至少有一个相邻的节点，所述各区块链节点通过有线网络、无线网络任意一种互相连接并进行通信。

[0045] 进一步地，在步骤1中，所述工作量证明数据包括区块链节点的数据同步总时间的十进制形式经过SHA256哈希运算的递增值字符串，SHA256哈希运算的方法为：将十进制数X看作十三进制，再按照十三进制数以转换基数转换成十进制数，提取其中若干为作为X的哈希值，所述转换基数为大于原来基数的数，并且两个基数应该是互素的，所述数据同步总时间的十进制形式，例如数据同步总时间为80127429秒，则十进制形式为$(80127429)_{10}$。

[0046] 例如：

[0047] Hash(80127429)＝$(80127429)_{13}$＝8*137+0*136+1*135+2*134+7*133+4*132+2*131+9＝$(502432641)_{10}$，如果取中间三位作为哈希值，得Hash(80127429)＝432。

[0048] 进一步地，在步骤2中，所述根据工作量证明数据计算节点的工作量阈值的方法为：工作量阈值为计算节点工作量证明数据与相邻节点工作量证明数据总和的加权几何平均数。

[0049] 进一步地，在步骤4中，所述计算与恶意节点连接的代价最小节点的方法包括以下

子步骤：

[0050] 步骤4.1，恶意节点发送同步数据包请求给区块链中所有的节点；

[0051] 步骤4.2，各区块链节点接收到同步数据包请求后返回应答数据包到恶意节点；

[0052] 步骤4.3，恶意节点接收应答数据包，应答响应时间最短的节点为代价最小节点；

[0053] 所述应答数据包至少包括应答节点ID编号、应答响应时间。

[0054] 进一步地，在步骤5中，通过代价最小节点构建恶意节点的虚拟同步连接的方法为:将恶意节点断开连接，将与恶意节点断开的连接重新连接至代价最小节点。

[0055] 进一步地，在步骤6中，所述将恶意节点的数据同步队列映射到代价最小节点的数据同步队列中的方法为:将恶意节点的数据同步队列中的数据同步请求按照原队列的顺序依次添加到代价最小节点的数据同步队列中，同时清空恶意节点的数据同步队列。

[0056] 本公开的实施例提供的一种区块链恶意节点发现与隔离装置，如图2所示为本公开的一种区块链恶意节点发现与隔离装置图，该实施例的一种区块链恶意节点发现与隔离装置包括:处理器、存储器以及存储在所述存储器中并可在所述处理器上运行的计算机程序，所述处理器执行所述计算机程序时实现上述一种区块链恶意节点发现与隔离装置实施例中的步骤。

[0057] 所述装置包括:存储器、处理器以及存储在所述存储器中并可在所述处理器上运行的计算机程序，所述处理器执行所述计算机程序运行在以下装置的单元中：

[0058] 工作量读取单元，用于读取区块链网络中各区块链节点的工作量证明数据；

[0059] 阈值计算单元，用于根据工作量证明数据计算节点的工作量阈值；

[0060] 恶意标记单元，用于在如果节点的工作量证明数据小于节点的工作量阈值时将节点标记为恶意节点；

[0061] 代价计算单元，用于计算与恶意节点连接的代价最小节点；

[0062] 虚拟连接单元，用于通过代价最小节点构建恶意节点的虚拟同步连接；

[0063] 队列映射单元，用于将恶意节点的数据同步队列映射到代价最小节点的数据同步队列中。

[0064] 所述一种区块链恶意节点发现与隔离装置可以运行于桌上型计算机、笔记本、掌上电脑及云端服务器等计算设备中。所述一种区块链恶意节点发现与隔离装置，可运行的装置可包括，但不仅限于，处理器、存储器。本领域技术人员可以理解，所述例子仅仅是一种区块链恶意节点发现与隔离装置的示例，并不构成对一种区块链恶意节点发现与隔离装置的限定，可以包括比例子更多或更少的部件，或者组合某些部件，或者不同的部件，例如所述一种区块链恶意节点发现与隔离装置还可以包括输入输出设备、网络接入设备、总线等。

[0065] 所称处理器可以是中央处理单元(Central Processing Unit,CPU)，还可以是其他通用处理器、数字信号处理器(Digital Signal Processor,DSP)、专用集成电路(Application Specific Integrated Circuit,ASIC)、现成可编程门阵列(Field-Programmable Gate Array,FPGA)或者其他可编程逻辑器件、分立门或者晶体管逻辑器件、分立硬件组件等。通用处理器可以是微处理器或者该处理器也可以是任何常规的处理器等，所述处理器是所述一种区块链恶意节点发现与隔离装置运行装置的控制中心，利用各种接口和线路连接整个一种区块链恶意节点发现与隔离装置可运行装置的各个部分。

[0066] 所述存储器可用于存储所述计算机程序和/或模块，所述处理器通过运行或执行

存储在所述存储器内的计算机程序和/或模块，以及调用存储在存储器内的数据，实现所述一种区块链恶意节点发现与隔离装置的各种功能。所述存储器可主要包括存储程序区和存储数据区，其中，存储程序区可存储操作系统、至少一个功能所需的应用程序(比如声音播放功能、图像播放功能等)等；存储数据区可存储根据手机的使用所创建的数据(比如音频数据、电话本等)等。此外，存储器可以包括高速随机存取存储器，还可以包括非易失性存储器，例如硬盘、内存、插接式硬盘，智能存储卡(Smart Media Card,SMC)，安全数字(Secure Digital,SD)卡，闪存卡(Flash Card)、至少一个磁盘存储器件、闪存器件、或其他易失性固态存储器件。

[0067] 尽管本公开的描述已经相当详尽且特别对几个所述实施例进行了描述，但其并非旨在局限于任何这些细节或实施例或任何特殊实施例，而是应当将其视作是通过参考所附权利要求考虑到现有技术为这些权利要求提供广义的可能性解释，从而有效地涵盖本公开的预定范围。此外，上文以发明人可预见的实施例对本公开进行描述，其目的是为了提供有用的描述，而那些目前尚未预见的对本公开的非实质性改动仍可代表本公开的等效改动。

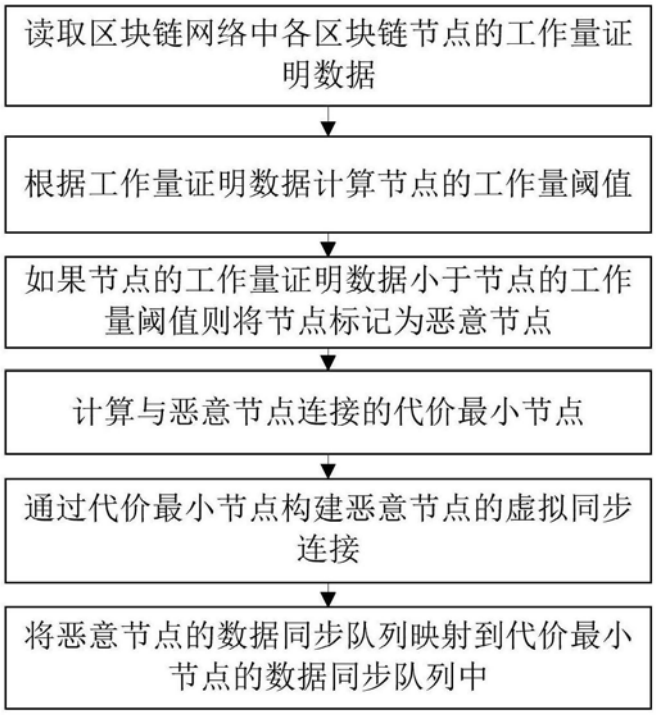

读取区块链网络中各区块链节点的工作量证明数据
根据工作量证明数据计算节点的工作量阈值
如果节点的工作量证明数据小于节点的工作量阈值则将节点标记为恶意节点
计算与恶意节点连接的代价最小节点
通过代价最小节点构建恶意节点的虚拟同步连接
将恶意节点的数据同步队列映射到代价最小节点的数据同步队列中

图1

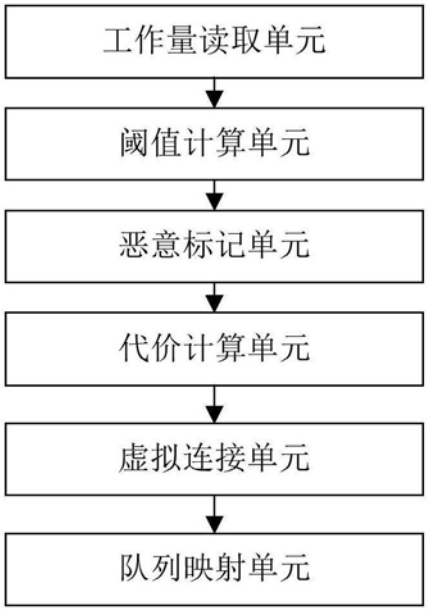

工作量读取单元
阈值计算单元
恶意标记单元
代价计算单元
虚拟连接单元
队列映射单元

图2