(19)国家知识产权局

(12)发明专利申请

(10)申请公布号 CN 115392912 A
(43)申请公布日 2022.11.25

(21)申请号 202211314715.5

(22)申请日 2022.10.26

(71)申请人 南方科技大学
地址 518055 广东省深圳市南山区桃源街道学苑大道1088号

(72)发明人 张锋巍 宁振宇 廖京辉 汪湛博

(74)专利代理机构 广州嘉权专利商标事务所有限公司 44205
专利代理师 张英凤

(51)Int.Cl.
G06Q 20/38(2012.01)
H04L 9/32(2006.01)

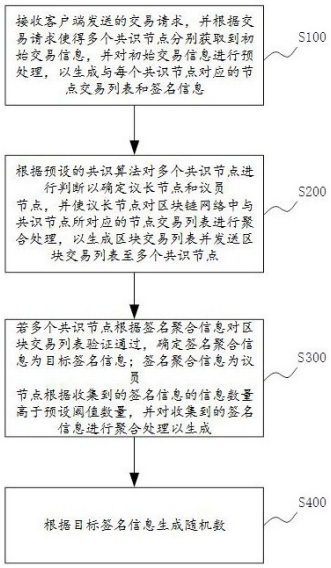
权利要求书3页 说明书12页 附图5页

(54)发明名称

随机数生成方法、系统、设备及存储介质

(57)摘要

本发明公开了一种随机数生成方法、系统、设备及存储介质，涉及计算机技术领域。该方法包括：接收客户端发送的交易请求，并根据交易请求使得多个共识节点分别获取到初始交易信息，并对初始交易信息进行预处理，以生成与每个共识节点对应的节点交易列表和签名信息；根据预设的共识算法对多个共识节点进行判断以确定议长节点和议员节点，并使议长节点对区块链网络中与共识节点所对应的节点交易列表进行聚合处理，以生成区块交易列表并发送区块交易列表至多个共识节点；若多个共识节点根据签名聚合信息对区块交易列表验证通过，确定签名聚合信息为目标签名信息；根据目标签名信息生成随机数。通过本公开实施例能够安全地生成随机数。



CN 115392912 A

1.一种随机数生成方法,其特征在于,包括:

接收客户端发送的交易请求,并根据所述交易请求使得多个共识节点分别获取到初始交易信息,并对所述初始交易信息进行预处理,以生成与每个所述共识节点对应的节点交易列表和签名信息;

根据预设的共识算法对多个所述共识节点进行判断以确定议长节点和议员节点,并使所述议长节点对区块链网络中与所有所述共识节点所对应的所述节点交易列表进行聚合处理,以生成区块交易列表并发送所述区块交易列表至多个所述共识节点;

若多个所述共识节点根据签名聚合信息对所述区块交易列表验证通过,确定所述签名聚合信息为目标签名信息;所述签名聚合信息为所述议员节点根据收集到的所述签名信息的信息数量高于预设阈值数量,并对收集到的所述签名信息进行聚合处理以生成;

根据所述目标签名信息生成随机数。

2.根据权利要求1所述的随机数生成方法,其特征在于,所述对所述初始交易信息进行预处理,以生成与每个所述共识节点对应的节点交易列表和签名信息,包括:

多个所述共识节点根据预设的签名算法对所述初始交易信息进行验证,并筛选出具有有效签名的所述初始交易信息,将所述具有有效签名的所述初始交易信息确定为有效交易信息;

多个所述共识节点将所述有效交易信息按照先入先出顺序分别推入至对应的交易缓存池中以生成对应的所述节点交易列表和所述签名信息。

3.根据权利要求2所述的随机数生成方法,其特征在于,所述多个所述共识节点根据预设的签名算法对所述初始交易信息进行验证,并筛选出具有有效签名的所述初始交易信息将所述具有有效签名的所述初始交易信息确定为有效交易信息,包括:

多个所述共识节点筛选出在满足预设数量初始节点交易列表条件下的所有初始交易信息;

多个所述共识节点计算每个初始交易信息的时间戳值,在所述初始交易信息中根据所述时间戳值筛除符合预设筛除条件的异常交易信息,以得到所述有效交易信息。

4.根据权利要求2所述的随机数生成方法,其特征在于,所述多个所述共识节点将所述有效交易信息按照先入先出顺序分别推入至对应的交易缓存池中以生成对应的所述节点交易列表和所述签名信息,包括:

多个所述共识节点根据每个所述有效交易信息对应的时间戳值,计算出所有所述有效交易信息分别对应的平均时间戳值;

多个所述共识节点根据所述平均时间戳值对所有所述有效交易信息进行排序,以得到与所述有效交易信息对应的交易顺序;

多个所述共识节点根据所述交易顺序和所述先入先出顺序,将与多个所述共识节点对应的所述有效交易信息分别推入至对应的交易缓存池中以生成对应的所述节点交易列表和所述签名信息。

5.根据权利要求1所述的随机数生成方法,其特征在于,在所述接收客户端发送的交易请求,并根据所述交易请求使得多个共识节点分别获取到初始交易信息,并对所述初始交易信息进行预处理,以生成与每个所述共识节点对应的节点交易列表和签名信息之后,所述方法还包括:

根据所述交易请求使多个所述共识节点从预设数量的所述节点交易列表中获取到相同交易信息的所有下标信息；

多个所述共识节点计算每一所述节点交易列表中的所述相同交易信息的每一下标信息与其他下标信息之间的距离值；

多个所述共识节点比较所有节点交易列表中所述相同交易信息的所述距离值，将所述距离值的误差范围超过预设范围的初始交易信息确定为恶意交易信息，并筛除所述恶意交易信息和与所述恶意交易信息所对应的节点交易列表。

6.根据权利要求1至5任一项所述的随机数生成方法，其特征在于，所述根据预设的共识算法对多个所述共识节点进行判断以确定议长节点和议员节点，包括：

获取多个所述共识节点对应的随机计时信息，每个所述共识节点向其他多个所述共识节点发送投票请求信息，并接收到其他多个所述共识节点根据所述投票请求信息反馈的投票信息；

每个所述共识节点统计根据在所述随机计时信息对应的计时期内接收到的所述投票信息的投票数量，并根据每个所述共识节点对应的所述投票数量确定出所述议长节点和所述议员节点。

7.根据权利要求1至5任一项所述的随机数生成方法，其特征在于，所述方法还包括：

若多个所述共识节点根据所述签名聚合信息对所述区块交易列表验证失败，发送重新共识指令至多个所述共识节点，以使多个所述共识节点重新生成节点交易列表。

8.一种随机数生成系统，其特征在于，包括：

预处理模块，用于接收客户端发送的交易请求，并根据所述交易请求使得多个共识节点分别获取到初始交易信息，并对所述初始交易信息进行预处理，以生成与每个所述共识节点对应的节点交易列表和签名信息；

聚合交易列表模块，用于根据预设的共识算法对多个所述共识节点进行判断以确定议长节点和议员节点，并使所述议长节点对区块链网络中与所有所述共识节点所对应的所述节点交易列表进行聚合处理，以生成区块交易列表并发送所述区块交易列表至多个所述共识节点；

聚合签名信息模块，用于若多个所述共识节点根据签名聚合信息对所述区块交易列表验证通过，确定所述签名聚合信息为目标签名信息；所述签名聚合信息为所述议员节点根据收集到的所述签名信息的信息数量高于预设阈值数量，并对收集到的所述签名信息进行聚合处理以生成；

生成随机数模块，用于根据所述目标签名信息生成随机数。

9.一种电子设备，其特征在于，包括：

至少一个存储器；

至少一个处理器；

至少一个计算机程序；

所述计算机程序被存储在存储器中，处理器执行所述至少一个计算机程序以实现：

如权利要求1至7任一项所述的随机数生成方法。

10.一种存储介质，其特征在于，所述存储介质存储有可执行指令，可执行指令能被计算机执行，使所述计算机执行：

如权利要求1至7任一项所述的随机数生成方法。

随机数生成方法、系统、设备及存储介质

技术领域

[0001] 本发明涉及计算机技术领域，尤其是涉及一种随机数生成方法、系统、设备及存储介质。

背景技术

[0002] 相关技术中，目前在使用的区块链系统包括两种：去中心化账本和去中心化计算机。其中，去中心化账本为第一代技术，其只用于记录多方之间传递的交易信息，一般不带有自动执行交易的能力。而第二代技术去中心化计算机可以支持复杂的系统逻辑，而不是简单的账本。这些执行逻辑是由区块链参与者组织的智能合约来实现的，整个区块链网络会为智能合约的代码提供执行环境。智能合约提供的运算能力和属性又与传统计算机有所不同，因为它的代码是高度透明的，参与者可以轻松的预测执行结果，这为计算机生成伪随机数造成一定困难。而随机数在各种现实场景有着广泛的应用，这些都对区块链网络的应用造成了限制。

[0003] 其中，相关技术中赖于以下几个模型生成随机数，并有如下缺点：

1.选举特殊节点来中心化生成随机数。这种方式对特殊节点的要求较高，因为随机性难以在单次情况下被验证，并不适用于某些区块链场景。

[0004] 2.使用外部的随机数。这种情况下，区块链需要完全信任对外部的随机数生成器，外部系统将作为代理生成随机数并返回给区块链系统。除随机数本身外，外部系统通常还会将随机数生成相关的密码学证明打包一同交给系统验证。这种方案不仅可以提供随机性，还可以提供一定的验证能力。然而这种外部系统的使用导致区块链会严重依赖外部实现，直接的数据强耦合可能会影响数据的质量和系统的可用性。

[0005] 3.基于可验证延迟函数的随机数。这类方案的缺陷在于，随着计算机算力的不断增强和新的数学方法的进步，许多密码学方案被攻击的可能性变大。针对这类方案依赖使用的延迟函数密码学方案，攻击者有许多潜在手段可能影响系统，从而给系统带来潜在的威胁。

发明内容

[0006] 本发明旨在至少解决现有技术中存在的技术问题之一。为此，本发明提出一种随机数生成方法、系统、设备及存储介质，能够安全的生成随机数并具有实用性。

[0007] 为实现上述目的，本公开实施例的第一方面提出了一种随机数生成方法，包括：

接收客户端发送的交易请求，并根据交易请求使得多个共识节点分别获取到初始交易信息，并对初始交易信息进行预处理，以生成与每个共识节点对应的节点交易列表和签名信息；

根据预设的共识算法对多个共识节点进行判断以确定议长节点和议员节点，并使议长节点对区块链网络中与共识节点所对应的节点交易列表进行聚合处理，以生成区块交易列表并发送区块交易列表至多个共识节点；

若多个共识节点根据签名聚合信息对区块交易列表验证通过，确定签名聚合信息为目标签名信息；签名聚合信息为议员节点根据收集到的签名信息的信息数量高于预设阈值数量，并对收集到的签名信息进行聚合处理以生成；

根据目标签名信息生成随机数。

[0008] 在一些实施例中，对初始交易信息进行预处理，以生成与每个共识节点对应的节点交易列表和签名信息，包括：

多个共识节点根据预设的签名算法对初始交易信息进行验证，并筛选出具有有效签名的初始交易信息将具有有效签名的初始交易信息确定为有效交易信息；

多个共识节点将有效交易信息按照先入先出的顺序分别推入至对应的交易缓存池中以生成对应的节点交易列表和签名信息。

[0009] 在一些实施例中，多个共识节点根据预设的签名算法对初始交易信息进行验证，并筛选出具有有效签名的初始交易信息将具有有效签名的初始交易信息确定为有效交易信息，包括：

多个共识节点筛选出在满足预设数量初始节点交易列表条件下的所有初始交易信息；

多个共识节点计算每个初始交易信息的时间戳值，在初始交易信息中根据时间戳值筛除符合预设筛除条件的异常交易信息，以得到有效交易信息。

[0010] 在一些实施例中，多个共识节点将有效交易信息按照先入先出的顺序分别推入至对应的交易缓存池中以生成对应的节点交易列表和签名信息，包括：

多个共识节点根据每个有效交易信息对应的时间戳值，计算出所有有效交易信息分别对应的平均时间戳值；

多个共识节点根据平均时间戳值对所有有效交易信息进行排序，以得到与有效交易信息对应的交易顺序；

多个共识节点根据交易顺序和先入先出的顺序，将与多个共识节点对应的有效交易信息分别推入至对应的交易缓存池中以生成对应的节点交易列表和签名信息。

[0011] 在一些实施例中，在接收客户端发送的交易请求，并根据交易请求使得多个共识节点分别获取到初始交易信息，并对初始交易信息进行预处理，以生成与每个共识节点对应的节点交易列表和签名信息之后，随机数生成方法还包括：

根据交易请求使共识节点从预设数量的节点交易列表中获取到相同交易信息的所有下标信息；

多个共识节点计算每一节点交易列表中的相同交易信息的每一下标信息与其他下标信息之间的距离值；

多个共识节点比较所有节点交易列表中相同交易信息的距离值，将距离值的误差范围超过预设范围的初始交易信息确定为恶意交易信息，并筛除恶意交易信息和与恶意交易信息所对应的节点交易列表。

[0012] 在一些实施例中，根据预设的共识算法对多个共识节点进行判断以确定议长节点和议员节点，包括：

获取多个共识节点对应的随机计时信息，每个共识节点向其他多个共识节点发送投票请求信息，并接收到其他多个共识节点根据投票请求信息反馈的投票信息；

每个共识节点统计根据在随机计时信息对应的计时期内接收到的投票信息的投票数量，并根据每个共识节点对应的投票数量确定出议长节点和议员节点。

[0013] 在一些实施例中，随机数生成方法还包括：

若多个共识节点根据签名聚合信息对区块交易列表验证失败，发送重新共识指令至多个共识节点，以使多个共识节点重新生成节点交易列表。

[0014] 为实现上述目的，本公开实施例的第二方面提出了一种随机数生成系统，包括：

预处理模块，用于接收客户端发送的交易请求，并根据交易请求使得多个共识节点分别获取到初始交易信息，并对初始交易信息进行预处理，以生成与每个共识节点对应的节点交易列表和签名信息；

聚合交易列表模块，用于根据预设的共识算法对多个共识节点进行判断以确定议长节点和议员节点，并使议长节点对区块链网络中与所有共识节点所对应的节点交易列表进行聚合处理，以生成区块交易列表并发送区块交易列表至多个共识节点；

聚合签名信息模块，用于若多个共识节点根据签名聚合信息对区块交易列表验证通过，确定签名聚合信息为目标签名信息；签名聚合信息为议员节点根据收集到的签名信息的信息数量高于预设阈值数量，并对收集到的签名信息进行聚合处理以生成；

生成随机数模块，用于根据目标签名信息生成随机数。

[0015] 为实现上述目的，本公开实施例的第三方面提出了一种电子设备，包括：

至少一个存储器；

至少一个处理器；

至少一个程序；

所述程序被存储在存储器中，处理器执行所述至少一个程序以实现：

如上述第一方面所述的一种随机数生成方法。

[0016] 为实现上述目的，本公开实施例的第四方面提出了一种存储介质，该存储介质是计算机可读存储介质，所述计算机可读存储介质存储有计算机可执行指令，所述计算机可执行指令用于使计算机执行：

如上述第一方面所述的一种随机数生成方法。

[0017] 根据本发明实施例提供的随机数生成方法、系统、设备及存储介质，至少具有如下有益效果：首先接收客户端发送的交易请求，并根据交易请求使得多个共识节点分别获取到初始交易信息，并对初始交易信息进行预处理，以生成与每个共识节点对应的节点交易列表和签名信息；根据预设的共识算法对多个共识节点进行判断以确定议长节点和议员节点，并使议长节点对区块链网络中与共识节点所对应的节点交易列表进行聚合处理，以生成区块交易列表并发送区块交易列表至多个共识节点；若多个共识节点根据签名聚合信息对区块交易列表验证通过，确定签名聚合信息为目标签名信息；签名聚合信息为议员节点根据收集到的签名信息的信息数量高于预设阈值数量，并对收集到的签名信息进行聚合处理以生成；根据目标签名信息生成随机数。通过本公开实施例能够安全的生成随机数并对随机数进行验证使得随机数生成系统能够适用更多区块链应用场景，且更具有实用性。

[0018] 本发明的附加方面和优点将在下面的描述中部分给出，部分将从下面的描述中变得明显，或通过本发明的实践了解到。

附图说明

[0019] 下面结合附图和实施例对本发明做进一步的说明,其中:

图1为本发明提供的一种随机数生成方法的第一具体流程示意图;

图2为图1中步骤S100的一具体流程示意图;

图3为图2中步骤S110的一具体流程示意图;

图4为图2中步骤S120的一具体流程示意图;

图5为本发明提供的对图1中一种随机数生成方法补充的第二具体流程示意图;

图6为图1中步骤S200的一具体流程示意图;

图7为本发明提供的一种随机数生成方法的随机数调用的燃料能耗示意图;

图8为本发明提供的一种随机数生成方法的参考实现的链上开销示意图;

图9为本发明提供的一种随机数生成方法的BLS签名聚合的时间示意图;

图10为本发明提供的一种随机数生成方法的BLS初始设置的时间示意图。

具体实施方式

[0020] 下面详细描述本发明的实施例,所述实施例的示例在附图中示出,其中自始至终相同或类似的标号表示相同或类似的元件或具有相同或类似功能的元件。下面通过参考附图描述的实施例是示例性的,仅用于解释本发明,而不能理解为对本发明的限制。

[0021] 在本发明的描述中,需要理解的是,涉及到方位描述,例如上、下、前、后、左、右等指示的方位或位置关系为基于附图所示的方位或位置关系,仅是为了便于描述本发明和简化描述,而不是指示或暗示所指的装置或元件必须具有特定的方位、以特定的方位构造和操作,因此不能理解为对本发明的限制。

[0022] 在本发明的描述中,若干的含义是一个以上,多个的含义是两个以上,大于、小于、超过等理解为不包括本数,以上、以下、以内等理解为包括本数。如果有描述到第一、第二只是用于区分技术特征为目的,而不能理解为指示或暗示相对重要性或者隐含指明所指示的技术特征的数量或者隐含指明所指示的技术特征的先后关系。

[0023] 本发明的描述中,除非另有明确的限定,设置、安装、连接等词语应做广义理解,所属技术领域技术人员可以结合技术方案的具体内容合理确定上述词语在本发明中的具体含义。

[0024] 本发明的描述中,参考术语“一个实施例”、“一些实施例”、“示意性实施例”、“示例”、“具体示例”、或“一些示例”等的描述意指结合该实施例或示例描述的具体特征、结构、材料或者特点包含于本发明的至少一个实施例或示例中。在本说明书中,对上述术语的示意性表述不一定指的是相同的实施例或示例。而且,描述的具体特征、结构、材料或者特点可以在任何的一个或多个实施例或示例中以合适的方式结合。

[0025] 首先,对本申请中涉及的若干名词进行解析:

最大可获取价值(MEV,Maximal Extractable Value):指区块链中实际负责生成区块链的节点通过组织交易顺序、临时增加剔除交易而可获得的价值。

[0026] 博内-琳恩-沙克姆签名(音译)(BLS Signature,Boneh-Lynn-Shacham Signature):一种数字签名的方法,允许使用者验证签名者的真实性。

[0027] 先入先出算法(FIFO,First-In-First-Out):一种组织数据结构的算法,通常最早

进入的条目最先得到处理。

[0028] 软件防护扩展(SGX,Software Guard Extensions):英特尔公司®提供的一种硬件可信执行环境技术。

[0029] 实用拜占庭容错(PBFT,Practical Byzantine Fault Tolerant):PBFT是一种基于投票的共识算法,即:拜占庭容错:即使某些节点出现故障或恶意,只要连接了最小百分比的节点,正常工作并且行为诚实,网络的活性和安全性也可以得到保证。

[0030] 相关技术中赖于以下几个模型生成随机数,并有如下缺点:

1.选举特殊节点来中心化生成随机数。这种方式对特殊节点的要求较高,因为随机性难以在单次情况下被验证,并不适用于某些区块链场景。

[0031] 2.使用外部的随机数。这种情况下,区块链需要完全信任对外部的随机数生成器,外部系统将作为代理来生成随机数并返回给区块链系统。除随机数本身外,外部系统通常还会将随机数生成相关的密码学证明打包一同交给系统验证。这种方案不仅可以提供随机性,还可以提供一定的验证能力。然而这种外部系统的使用导致区块链会严重依赖外部实现,直接的数据强耦合可能会影响数据的质量和系统的可用性。

[0032] 3.基于可验证延迟函数的随机数。可验证延迟函数是一种密码学特殊构造的函数,其正向计算函数的值需要一定时间,且这种计算过程无法被显著加速;在正向计算结束后,验证结果的正确性的操作通常非常容易,时间消耗显著低于正向计算,使得所有人都可以轻松验证结果。这类方案的缺陷在于,随着计算机算力的不断增强和新的数学方法的进步,许多密码学方案被攻击的可能性在变大。针对该类方案依赖使用的延迟函数密码学方案,攻击者有许多潜在手段可能影响系统,如通过设计专用硬件来加速延迟函数的执行,进而提前预测相关伪随机数的值。

[0033] 基于此,本公开实施例提出的一种随机数生成方法、系统、设备及存储介质,能够通过具有更好稳定性和鲁棒性的阈值签名算法实现安全的生成随机数。

[0034] 其具体通过如下实施例进行说明,首先描述本公开实施例中的随机数生成方法。

[0035] 如图1所示,其为本申请实施例提供的一种随机数生成方法的实施流程示意图,随机数生成方法可以包括但不限于步骤S100至S400。

[0036] S100,接收客户端发送的交易请求,并根据交易请求使得多个共识节点分别获取到初始交易信息,并对初始交易信息进行预处理,以生成与每个共识节点对应的节点交易列表和签名信息;

S200,根据预设的共识算法对多个共识节点进行判断以确定议长节点和议员节点,并使议长节点对区块链网络中与共识节点所对应的节点交易列表进行聚合处理,以生成区块交易列表并发送区块交易列表至多个共识节点;

S300,若多个共识节点根据签名聚合信息对区块交易列表验证通过,确定签名聚合信息为目标签名信息;签名聚合信息为议员节点根据收集到的签名信息的信息数量高于预设阈值数量,并对收集到的签名信息进行聚合处理以生成;

S400,根据目标签名信息生成随机数。

[0037] 在一些实施例的步骤S100中,接收客户端发送的交易请求,并根据交易请求使得多个共识节点分别获取到初始交易信息,并对初始交易信息进行预处理,以生成与每个共识节点对应的节点交易列表和签名信息。可以理解的是,客户端向计算机程序发送交易请

求，随机数生成设备根据接收到的交易请求使得多个共识节点分别获取到初始交易信息，也即每个共识节点从BFT共识网络中收集交易，以得到初始交易信息，每个共识节点再分别对初始交易信息进行预处理，从而生成与每个共识节点所对应的节点交易列表和签名信息，签名信息可以为每个共识节点对生成的节点交易列表根据本地BLS私钥进行签名而得到的。

[0038] 需要说明的是，预处理为多个共识节点根据预设的签名算法对初始交易信息进行验证，并筛选出具有有效签名的初始交易信息，将具有有效签名的初始交易信息确定为有效交易信息；多个共识节点再将有效交易信息按照先入先出的顺序分别推入至对应的交易缓存池中以生成对应的节点交易列表和签名信息。

[0039] 在一些实施例的步骤S200中，根据预设的共识算法对多个共识节点进行判断以确定议长节点和议员节点，并使议长节点对区块链网络中与共识节点所对应的节点交易列表进行聚合处理，以生成区块交易列表并发送区块交易列表至多个共识节点。可以理解的是，计算机程序根据预设的共识算法对多个共识节点进行判断，根据该判断确定出议长节点和议员节点。在确定出议长节点之后，议长节点再对区块链网络中与多个共识节点分别对应的节点交易列表进行聚合处理，从而生成区块交易列表，再将区块交易列表广播至区块链网络，以便于区块链网络中的多个共识节点进行收集，以使多个共识节点能够收集到与区块交易列表对应的交易信息。

[0040] 需要说明的是，区块交易列表即对区块链网络中多个共识节点对应的节点交易列表进行聚合而得到的一个节点交易列表集合。

[0041] 在一些实施例的步骤S300中，若多个共识节点根据签名聚合信息对区块交易列表验证通过，确定签名聚合信息为目标签名信息；签名聚合信息为议员节点根据收集到的签名信息的信息数量高于预设阈值数量，并对收集到的签名信息进行聚合处理以生成。可以理解的是，根据步骤S200判断得到的议员节点收集到的签名信息的信息数量高于预设阈值数量，该预设阈值数量可以为2/3，则对收集到的签名信息进行聚合处理以生成签名聚合信息，在根据签名聚合信息对步骤S200中得到的区块交易列表进行验证处理，如果多个共识节点根据签名聚合信息对区块交易列表验证通过，则确定签名聚合信息即为目标签名信息。

[0042] 在一些实施例的步骤S400中，根据目标签名信息生成随机数。可以理解的是，根据步骤S300中得到的目标签名信息生成随机数。即将目标签名信息作为生成随机数的生成随机数种子，再根据预设的生成算法对随机数种子进行处理，以生成随机数。

[0043] 需要说明的是，当一个共识节点从区块链网络接收到足够多的BLS签名时，它会调用BLS聚合算法将这些BLS签名聚合成一个最终的签名，即目标签名信息，并且目标签名信息被用作随机数，因为所有共识节点运行相同的BLS算法，因此所有共识节点生成的随机数是相同的。整个区块链网络是基于拜占庭容错共识算法实现的，将BLS签名聚合的阈值设为超过所有共识节点数量的1/3。举例说明，当区块链网络中有七个共识节点的时候，那么只需要收集到三个共识节点的签名信息，就可以聚合成最终的签名，即目标签名信息，也就是随机数种子。之所以考虑到设置节点数量为超过1/3，是因为如果把阈值设为小于共识节点的1/3，那么恶意节点将会可以联合起来，构造虚假的随机数种子，以影响随机数生成的正确性。

[0044] 在一些实施例中，参考图2所示，步骤S100还可以包括但不限于步骤S110至S120。

[0045] S110，多个共识节点根据预设的签名算法对初始交易信息进行验证，并筛选出具有有效签名的初始交易信息将具有有效签名的初始交易信息确定为有效交易信息；

S120，多个共识节点将有效交易信息按照先入先出的顺序分别推入至对应的交易缓存池中以生成对应的节点交易列表和签名信息。

[0046] 在一些实施例的步骤S110中，多个共识节点根据预设的签名算法对初始交易信息进行验证，并筛选出具有有效签名的初始交易信息，并将具有有效签名的初始交易信息确定为有效交易信息。可以理解的是，多个共识节点根据本地预设的签名算法对初始交易信息进行验证处理，签名算法可以为BLS私钥加密、公钥解密算法，并筛选出具有有效签名的初始交易信息，以防止一些初始交易信息无签名或者篡改签名，因此要筛选出具有有效签名的初始交易信息，并将该具有有效签名的初始交易信息作为有效交易信息。

[0047] 需要说明的是，获取到有效交易信息还可以通过以下步骤：多个共识节点筛选出在满足预设数量初始节点交易列表条件下的所有初始交易信息；多个共识节点计算每个初始交易信息的时间戳值，在初始交易信息中根据时间戳值筛除符合预设筛除条件的异常交易信息，从而得到有效交易信息。

[0048] 在一些实施例的步骤S120中，多个共识节点将有效交易信息按照先入先出顺序分别推入至对应的交易缓存池中以生成对应的节点交易列表和签名信息。可以理解的是，多个共识节点将通过步骤S120得到的有效交易信息按照先入先出顺序分别推入至每个共识节点所对应的交易缓存池中，从而生成每个共识节点所对应的节点交易列表和与节点交易列表对应的签名信息。

[0049] 需要说明的是，交易缓存池为FIFO交易缓存池，其是一个先进先出的交易缓存池，存在于每个共识节点中。交易缓存池本质上是一个交易队列，共识节点将从区块链网络中获取到的交易从交易队列的尾部推送入交易缓存池，然后从交易队列前端弹出交易，从而实现每笔交易都能按照先入先出的排序逻辑进行排序。此外，再把交易信息对应的交易推入交易缓存池之前，共识节点会验证每笔交易的数字签名以及共识节点本身的账户余额。只有那些通过了签名验证并且有足够的余额支付手续费的交易，才会被推入缓存池中。而那些验证失败的交易，将会直接被丢弃。在每轮共识开始的时候，共识节点会从交易缓存池中获取一定数量的交易信息对应的交易并将这些交易信息对应的交易打包成节点交易列表。这些节点交易列表将会被广播到区块链网络中。议长节点将会监听网络中的这些包含了节点交易列表的信息。

[0050] 在一些实施例中，参考图3所示，步骤S110还可以包括但不限于步骤S111至S112。

[0051] S111，多个共识节点筛选出在满足预设数量初始节点交易列表条件下的所有初始交易信息；

S112，多个共识节点计算每个初始交易信息的时间戳值，在初始交易信息中根据时间戳值筛除符合预设筛除条件的异常交易信息，以得到有效交易信息。

[0052] 在一些实施例的步骤S111中，多个共识节点筛选出在满足预设数量初始节点交易列表条件下的所有初始交易信息。可以理解的是，多个共识节点先筛选满足预设数量的初始节点交易列表，预设数量可以为区块链共识网络中超过2/3的初始节点交易列表，以保证能够符合拜占庭算法，在获取这些至少2/3的初始节点交易列表对应的所有初始交易信息，

以得到有效交易信息。

[0053] 在一些实施例的步骤S112中，多个共识节点计算每个初始交易信息的时间戳值，在初始交易信息中根据时间戳值筛除符合预设筛除条件的异常交易信息，以得到有效交易信息。可以理解的是，多个共识节点分别计算每个共识节点对应的每个初始交易信息的时间戳值，再根据每个初始交易信息对应的时间戳值筛除符合预设筛除条件的异常交易信息，即对每个初始交易信息对应的每笔交易筛除掉时间戳值处于边缘的1/3部分交易，以保证交易排序算法中没有人可以决定每笔交易的排序，只能由交易排序算法决定，以此保证避免别人临时构造交易，并把交易插入区块交易列表中：在随机数被使用前，交易列表已经被聚合完成，临时再生成需要超过2/3节点重新生成，超出原假设要求；没有人可以从区块交易列表中删除有效交易：聚合交易列表中的已有交易如果被删除，需要更改超过2/3的交易列表，超出原假设要求；区块交易列表的公平性对共识节点是可验证的：所有正常共识节点交易列表均为FIFO广播，任何人都可以聚合。

[0054] 在一些实施例中，参考图4所示，步骤S120还可以包括但不限于步骤S121至S123。

[0055] S121，多个共识节点根据每个有效交易信息对应的时间戳值，计算出所有有效交易信息分别对应的平均时间戳值；

S122，多个共识节点根据平均时间戳值对所有有效交易信息进行排序，以得到与有效交易信息对应的交易顺序；

S123，多个共识节点根据交易顺序和先入先出的顺序，将与多个共识节点对应的有效交易信息分别推入至对应的交易缓存池中以生成对应的节点交易列表和签名信息。

[0056] 在一些实施例的步骤S121中，多个共识节点根据每个有效交易信息对应的时间戳值，计算出所有有效交易信息分别对应的平均时间戳值。可以理解的是，多个共识节点分别计算每个有效交易信息对应的每笔交易的时间戳值，每个共识节点再根据每笔交易的时间戳值计算出所有有效交易信息分别对应的平均时间戳值，以根据该平均时间戳值对每笔交易对应的每个有效交易信息进行排序。

[0057] 在一些实施例的步骤S122中，多个共识节点根据平均时间戳值对所有有效交易信息进行排序，以得到与有效交易信息对应的交易顺序。可以理解的是，多个共识节点根据步骤S121中计算得到的平均时间戳值对步骤S112得到的有序交易信息进行排序，要说明的是，排序可以为按照交易金额或者剩余余额从大到小的顺序进行排序，从而得到与有效交易信息对应的每笔交易的交易顺序。

[0058] 在一些实施例的步骤S123中，多个共识节点根据交易顺序和先入先出顺序，将与多个共识节点对应的有效交易信息分别推入至对应的交易缓存池中以生成对应的节点交易列表和签名信息。可以理解的是，每个共识节点根据步骤S122得到的交易顺序和步骤S120中的先入先出顺序，将每个共识节点的有序交易信息对应的交易分别推入至每个共识节点的交易缓存池中，从而生成每个共识节点对应的节点交易列表，且每笔交易中都有对应的签名，因此，交易的顺序确定了，签名的顺序也随之确定，得到节点交易列表从而也得到签名列表，而签名信息中则包含此签名列表。

[0059] 在一些实施例中，参考图5所示，一种随机数生成方法还可以包括但不限于步骤S130至S150。

[0060] S130，根据交易请求使共识节点从预设数量的节点交易列表中获取到相同交易信

息的所有下标信息；

S140，多个共识节点计算每一节点交易列表中的相同交易信息的每一下标信息与其他下标信息之间的距离值；

S150，多个共识节点比较所有节点交易列表中相同交易信息的距离值，将距离值的误差范围超过预设范围的初始交易信息确定为恶意交易信息，并筛除恶意交易信息和与恶意交易信息所对应的节点交易列表。

[0061] 在一些实施例的步骤S130中，根据交易请求使共识节点从预设数量的节点交易列表中获取到相同交易信息的所有下标信息。可以理解的是，每个共识节点从预设数量的节点交易列表中获取到相同交易信息的所有下标信息，要说明的是，预设数量即为超过2/3个节点交易列表，相同交易信息即为每个交易信息对应的同一笔交易，然后计算机程序根据交易请求获取到同一笔交易的所有下标信息。

[0062] 在一些实施例的步骤S140中，多个共识节点计算每一节点交易列表中的相同交易信息的每一下标信息与其他下标信息之间的距离值。可以理解的是，每个共识节点分别计算每一个节点交易列表中同一笔交易信息的每一个下标信息和其它下标信息之间的距离值，用于确定其是否为恶意交易信息。

[0063] 在一些实施例的步骤S150中，多个共识节点比较所有节点交易列表中相同交易信息的距离值，将距离值的误差范围超过预设范围的初始交易信息确定为恶意交易信息，并筛除恶意交易信息和与恶意交易信息所对应的节点交易列表。可以理解的是，每个共识节点比较步骤S140中得到的同一笔交易的下标信息之间的距离值，将距离值的误差范围超过预设范围的初始交易信息认作为恶意交易信息，再筛选出恶意交易信息对应的交易，从而剔除恶意交易信息以及剔除与恶意交易信息对应的节点交易列表。

[0064] 需要说明的是，假设一共有七个共识节点，在聚合交易列表时，只需要获取五个节点交易列表，而在计算聚合结果即区块交易列表时，还需要从这五个节点交易列表中，计算出不超过1/3个恶意节点的数量，也就是说两个离群值，因此在最终聚合的时候，将会是有三个节点交易列表参与聚合得到最终的区块交易列表。而最终的区块交易列表将会和由生成它的节点交易列表一起被广播到整个网络中，其他的共识节点在收到这个信息的时候，也可以根据相同的逻辑自己去生成区块交易列表来验证来自于议长节点的区块交易列表是否为真。由此可使得本申请方法具有可验证性，并且聚合结果来自于整个区块链网络(共识网络)。

[0065] 在一些实施例中，参考图6所示，步骤S200还可以包括但不限于步骤S210至S220。

[0066] S210，获取多个共识节点对应的随机计时信息，每个共识节点向其他多个共识节点发送投票请求信息，并接收到其他多个共识节点根据投票请求信息反馈的投票信息；

S220，每个共识节点统计根据在随机计时信息对应的计时期内接收到的投票信息的投票数量，并根据每个共识节点对应的投票数量确定出议长节点和议员节点。

[0067] 在一些实施例的步骤S210中，获取多个共识节点对应的随机计时信息，每个共识节点向其他多个共识节点发送投票请求信息，并接收到其他多个共识节点根据投票请求信息反馈的投票信息。可以理解的是，多个共识节点获取到对应的随机计时器并产生随机计时信息，每个共识节点向其他共识节点发送请求投自己为议长节点一票的投票请求信息，每个共识节点仅能投一票并根据接收到投票请求信息的接收顺序反馈发出投票请求的共

识节点一票的投票信息。

[0068] 在一些实施例的步骤S220中，每个共识节点统计根据在随机计时信息对应的计时期内接收到的投票信息的投票数量，并根据每个共识节点对应的投票数量确定出议长节点和议员节点。可以理解的是，每个共识节点统计在随机计时信息对应的计时期内收到的投票信息的投票数量，并对每个共识节点对应的投票数量进行比较排序处理，确定投票数量最多的共识节点为议长节点，其余共识节点即为议员节点。

[0069] 需要说明的是，对应上述根据共识算法从多个共识节点中确定议长节点和议员节点的例子如下：比如说现在一共有3个将军A，B，C，每个将军都有一个随机时间的倒计时，倒计时一结束，这个将军就会把自己当成大将军候选人，然后派信使去问其他几个将军，能不能选我为总将军，假设现在将军A倒计时结束了，他派信使传递选举投票的信息给将军B和C，如果将军B和C还没把自己当成候选人(倒计时还没有结束)，并且没有把选举票投给其他，他们把票投给将军A，信使在回到将军A时，将军A知道自己收到了足够的票数，成为了大将军。在这之后，是否要进攻就由大将军决定，然后派信使去通知另外两个将军，如果在一段时间后还没有收到回复(可能信使被暗杀)，那就再重派一个信使，直到收到回复。

[0070] 在一些实施例的步骤中，随机数生成方法还包括：

若多个共识节点根据签名聚合信息对区块交易列表验证失败，发送重新共识指令至多个共识节点，以使多个共识节点重新生成节点交易列表。

[0071] 可以理解的是，如果多个共识节点根据步骤S300得到的签名聚合信息对区块交易列表验证失败，其中签名聚合信息为议员节点根据收集到的签名信息的信息数量高于预设阈值数量，并对收集到的签名信息进行聚合处理生成的，则发送重新共识指令至多个共识节点，以使多个共识节点重新生成节点交易列表，以执行随机数生成方法。

[0072] 通过本公开实施例上述的一种随机数生成方法通过具有更好稳定性和鲁棒性的阈值签名算法实现安全的生成随机数。

[0073] 请参照图7至图10，图7为随机数调用的燃料能耗示意图，图8为参考实现的链上开销示意图，图9为BLS签名聚合的时间示意图，图10为BLS初始设置的时间示意图。通过图7可知，GAS Cost Ratio为随机数消耗的燃料，GAS Cost为交易的燃料消耗，本实施例提供的随机数生成方法，随着合约中随机数调用次数的增加，平均燃料消耗呈下降趋势，因此，可以有效降低智能合约运行时的随机数相关开销。通过图8可知，BaseLine为基线，本实施例提供的随机数生成方法，且基线为回调机制下的链上数据开销，参考实现链上开销的节省比例在随机数占比上均是高于回调机制，因此节省了随机数相关开销。通过图9可知，图9的左轴为BLS算法聚合签名的时间，右纵轴为标准差，通过图9可知采用BLS算法进行聚合签名，随着随机数调用次数的增加，平均花费的时间降低。通过图10，且图10为7个节点完成分布式密钥生成的时间，则整体时间在0-6000ms之间波动，大部分均落在3000ms以为，则50％可以在1000ms内完成，由此可知，本实施例所采用BLS算法进行签名进行初始化所耗费的时间较少，使得随机数生成效率提高。

[0074] 另外，本公开实施例还提供一种随机数生成系统，可以实现上述一种随机数生成方法，该系统包括：

预处理模块，用于接收客户端发送的交易请求，并根据交易请求使得多个共识节点分别获取到初始交易信息，并对初始交易信息进行预处理，以生成与每个共识节点对应

的节点交易列表和签名信息；

聚合交易列表模块，用于根据预设的共识算法对多个共识节点进行判断以确定议长节点和议员节点，并使议长节点对区块链网络中与所有共识节点所对应的节点交易列表进行聚合处理，以生成区块交易列表并发送区块交易列表至多个共识节点；

聚合签名信息模块，用于若多个共识节点根据签名聚合信息对区块交易列表验证通过，确定签名聚合信息为目标签名信息；签名聚合信息为议员节点根据收集到的签名信息的信息数量高于预设阈值数量，并对收集到的签名信息进行聚合处理以生成；

生成随机数模块，用于根据目标签名信息生成随机数。

[0075] 通过本公开实施例提供的一种随机数生成系统，能够安全的生成随机数并使得随机数生成系统具有实用性。

[0076] 其中，一种随机数生成系统的具体操作过程参照上述的一种随机数生成方法，此处不再赘述。

[0077] 另外，本公开实施例还提供一种电子设备，该设备包括：

至少一个存储器；

至少一个处理器；

至少一个程序；

所述程序被存储在存储器中，处理器执行所述至少一个程序以实现：

如本公开实施例第一方面提供的一种随机数生成方法。

[0078] 另外，本公开实施例还提供一种存储介质存储有可执行指令，可执行指令能被计算机执行，使计算机执行如本公开实施例第一方面提供的一种随机数生成方法。

[0079] 存储器作为一种非暂态存储介质，可用于存储非暂态软件程序以及非暂态性计算机可执行程序。此外，存储器可以包括高速随机存取存储器，还可以包括非暂态存储器，例如至少一个磁盘存储器件、闪存器件、或其他非暂态固态存储器件。在一些实施方式中，存储器可选包括相对于处理器远程设置的存储器，这些远程存储器可以通过网络连接至该处理器。上述网络的实例包括但不限于互联网、企业内部网、局域网、移动通信网及其组合。

[0080] 本公开实施例描述的实施例是为了更加清楚的说明本公开实施例的技术方案，并不构成对于本公开实施例提供的技术方案的限定，本领域技术人员可知，随着技术的演变和新应用场景的出现，本公开实施例提供的技术方案对于类似的技术问题，同样适用。

[0081] 在本申请所提供的几个实施例中，应该理解到，所揭露的装置和方法，可以通过其它的方式实现。例如，以上所描述的装置实施例仅仅是示意性的，例如，所述单元的划分，仅仅为一种逻辑功能划分，实际实现时可以有另外的划分方式，例如多个单元或组件可以结合或者可以集成到另一个系统，或一些特征可以忽略，或不执行。另一点，所显示或讨论的相互之间的耦合或直接耦合或通信连接可以是通过一些接口，装置或单元的间接耦合或通信连接，可以是电性，机械或其它的形式。

[0082] 所述作为分离部件说明的单元可以是或者也可以不是物理上分开的，作为单元显示的部件可以是或者也可以不是物理单元，即可以位于一个地方，或者也可以分布到多个网络单元上。可以根据实际的需要选择其中的部分或者全部单元来实现本实施例方案的目的。

[0083] 另外，在本申请各个实施例中的各功能单元可以集成在一个处理单元中，也可以

是各个单元单独物理存在,也可以两个或两个以上单元集成在一个单元中。上述集成的单元既可以采用硬件的形式实现,也可以采用软件功能单元的形式实现。

[0084] 所述集成的单元如果以软件功能单元的形式实现并作为独立的产品销售或使用时,可以存储在一个计算机可读取存储介质中。基于这样的理解,本申请的技术方案本质上或者说对现有技术做出贡献的部分或者该技术方案的全部或部分可以以软件产品的形式体现出来,该计算机软件产品存储在一个存储介质中,包括多指令用以使得一台计算机设备(可以是个人计算机,服务器,或者网络设备等)执行本申请各个实施例所述方法的全部或部分步骤。而前述的存储介质包括:U盘、移动硬盘、只读存储器(Read-Only Memory,简称ROM)、随机存取存储器(Random Access Memory,简称RAM)、磁碟或者光盘等各种可以存储程序的介质。

[0085] 以上参照附图说明了本公开实施例的优选实施例,并非因此局限本公开实施例的权利范围。本领域技术人员不脱离本公开实施例的范围和实质内所作的任何修改、等同替换和改进,均应在本公开实施例的权利范围之内。

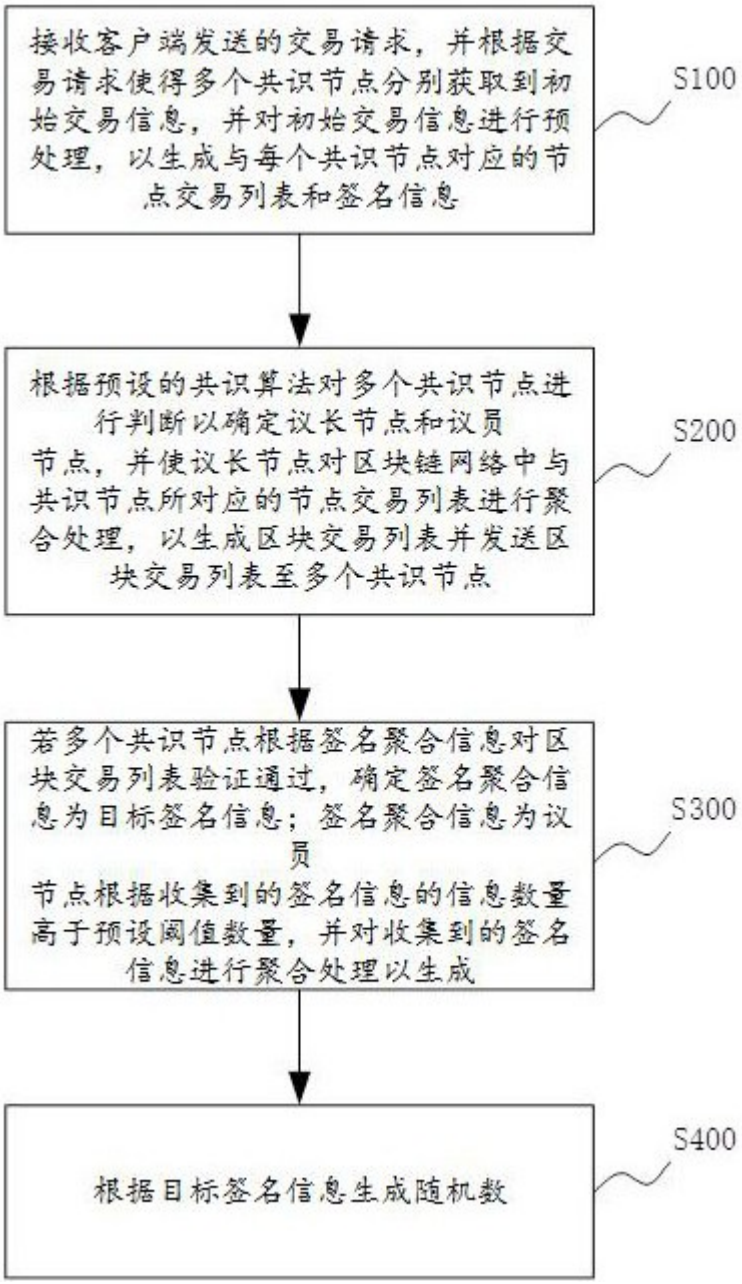

接收客户端发送的交易请求，并根据交易请求使得多个共识节点分别获取到初始交易信息，并对初始交易信息进行预处理，以生成与每个共识节点对应的节点交易列表和签名信息
S100
根据预设的共识算法对多个共识节点进行判断以确定议长节点和议员节点，并使议长节点对区块链网络中与共识节点所对应的节点交易列表进行聚合处理，以生成区块交易列表并发送区块交易列表至多个共识节点
S200
若多个共识节点根据签名聚合信息对区块交易列表验证通过，确定签名聚合信息为目标签名信息；签名聚合信息为议员节点根据收集到的签名信息的信息数量高于预设阈值数量，并对收集到的签名信息进行聚合处理以生成
S300
根据目标签名信息生成随机数
S400

图1

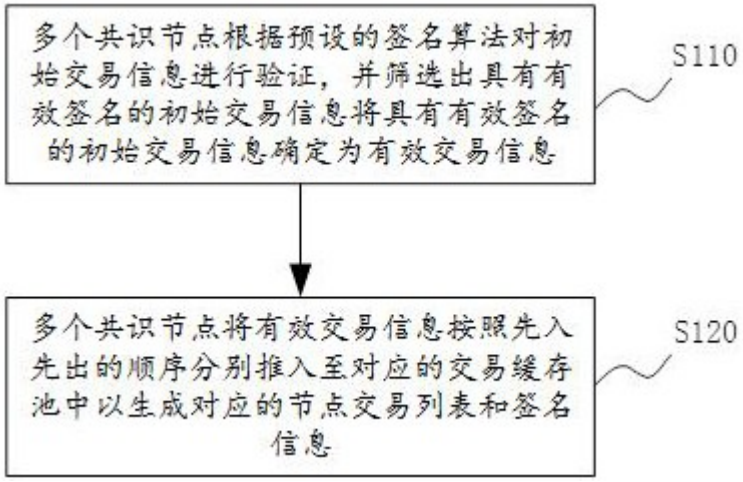

多个共识节点根据预设的签名算法对初始交易信息进行验证，并筛选出具有有效签名的初始交易信息将具有有效签名的初始交易信息确定为有效交易信息
S110
多个共识节点将有效交易信息按照先入先出的顺序分别推入至对应的交易缓存池中以生成对应的节点交易列表和签名信息
S120

图2

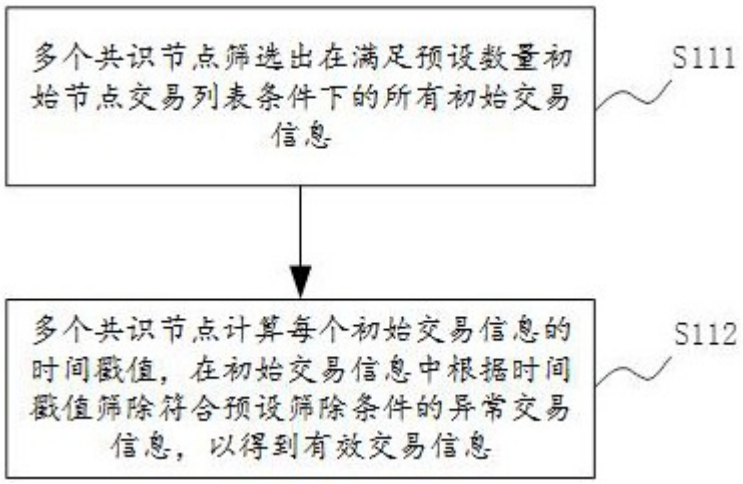

多个共识节点筛选出在满足预设数量初始节点交易列表条件下的所有初始交易信息
S111
多个共识节点计算每个初始交易信息的时间戳值，在初始交易信息中根据时间戳值筛除符合预设筛除条件的异常交易信息，以得到有效交易信息
S112

图3

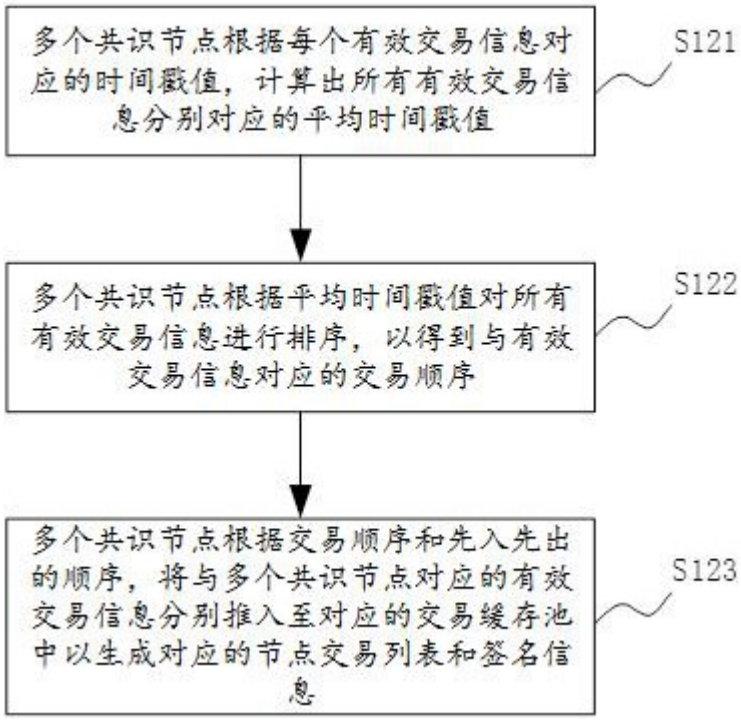

多个共识节点根据每个有效交易信息对应的时间戳值，计算出所有有效交易信息分别对应的平均时间戳值
S121
多个共识节点根据平均时间戳值对所有有效交易信息进行排序，以得到与有效交易信息对应的交易顺序
S122
多个共识节点根据交易顺序和先入先出的顺序，将与多个共识节点对应的有效交易信息分别推入至对应的交易缓存池中以生成对应的节点交易列表和签名信息
S123

图4

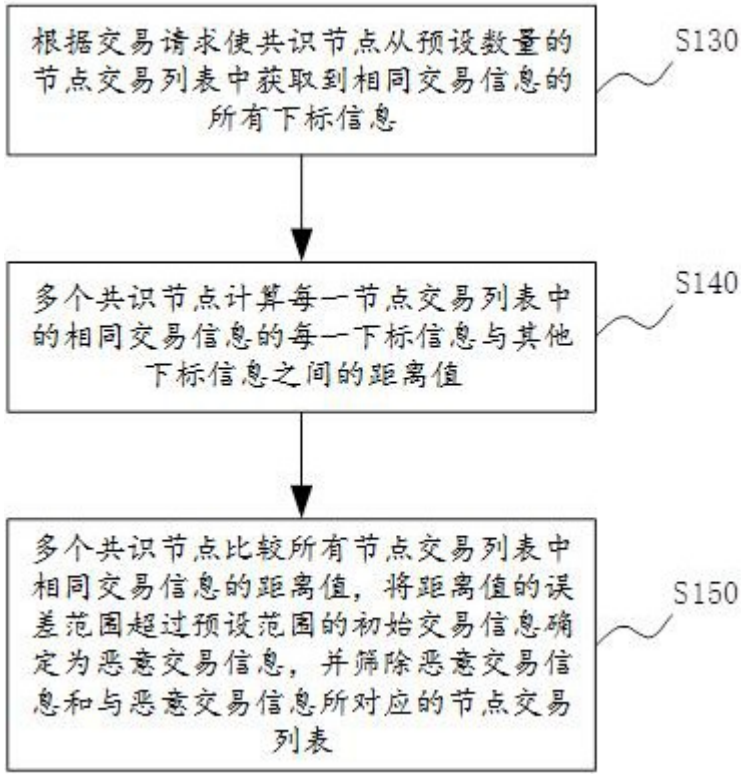

根据交易请求使共识节点从预设数量的节点交易列表中获取到相同交易信息的所有下标信息
S130
多个共识节点计算每一节点交易列表中的相同交易信息的每一下标信息与其他下标信息之间的距离值
S140
多个共识节点比较所有节点交易列表中相同交易信息的距离值，将距离值的误差范围超过预设范围的初始交易信息确定为恶意交易信息，并筛除恶意交易信息和与恶意交易信息所对应的节点交易列表
S150

图5

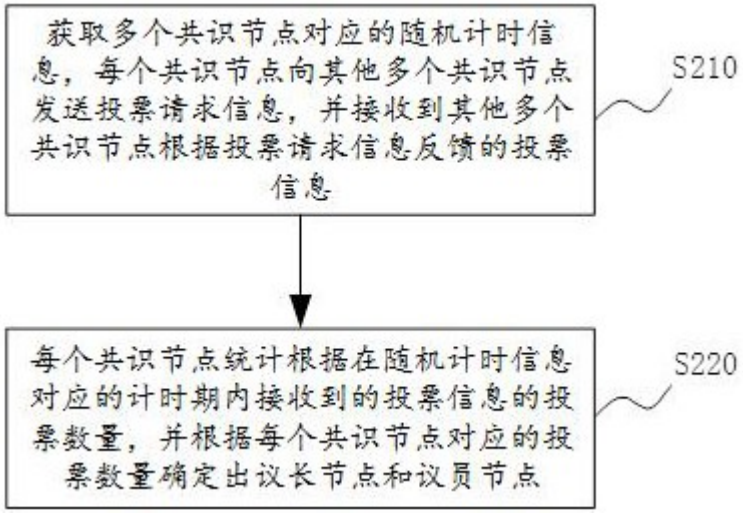

获取多个共识节点对应的随机计时信息，每个共识节点向其他多个共识节点发送投票请求信息，并接收到其他多个共识节点根据投票请求信息反馈的投票信息
S210
每个共识节点统计根据在随机计时信息对应的计时期内接收到的投票信息的投票数量，并根据每个共识节点对应的投票数量确定出议长节点和议员节点
S220

图6

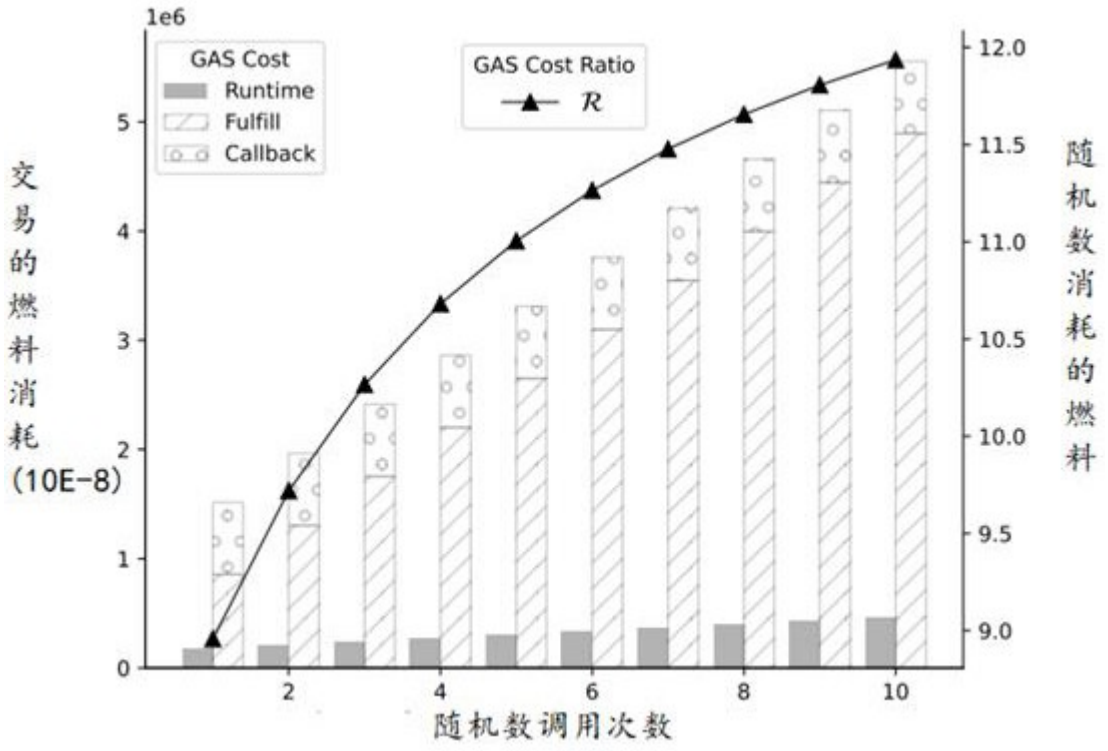

1e6
GAS Cost
Runtime
Fulfill
Callback
GAS Cost Ratio
R
交易的燃料消耗(10E-8)
随机数消耗的燃料
随机数调用次数
0
1
2
3
4
5
9.0
9.5
10.0
10.5
11.0
11.5
12.0
2
4
6
8
10

图7

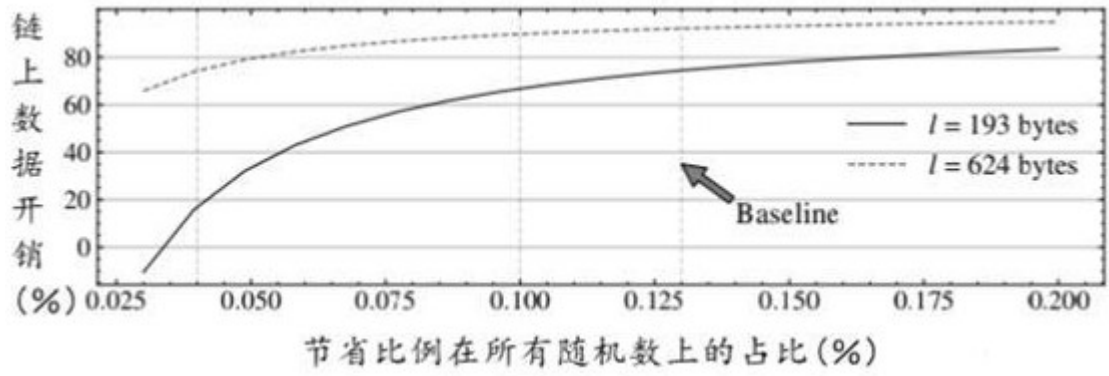

链上数据开销(%)
80
60
40
20
0
0.025
0.050
0.075
0.100
0.125
0.150
0.175
0.200
l = 193 bytes
l = 624 bytes
Baseline
节省比例在所有随机数上的占比(%)

图8

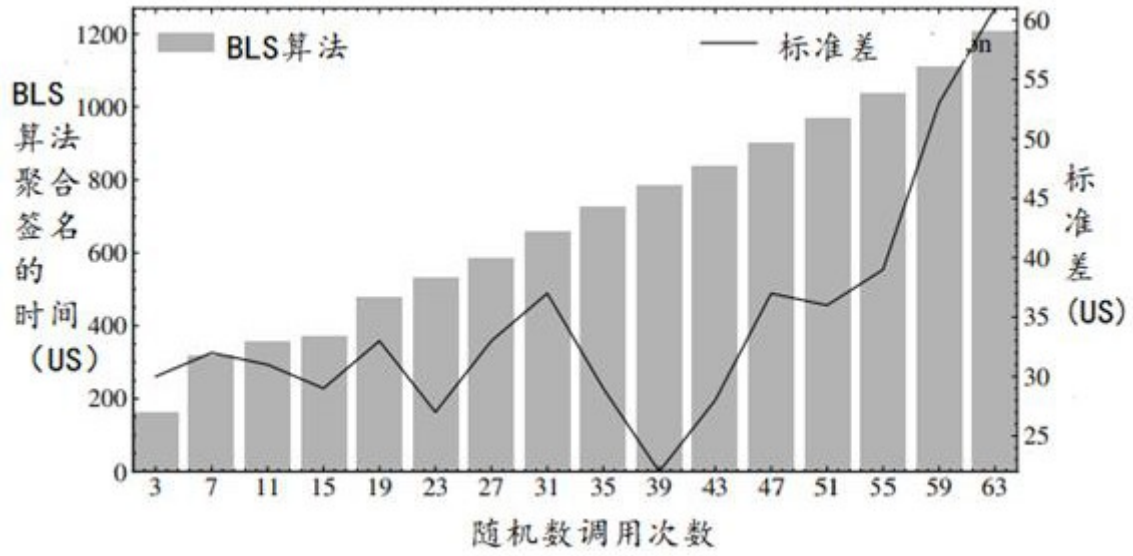

BLS算法聚合签名的时间(US)
BLS算法
标准差
标准差(US)
1200
1000
800
600
400
200
0
60
55
50
45
40
35
30
25
3
7
11
15
19
23
27
31
35
39
43
47
51
55
59
63
随机数调用次数

图9

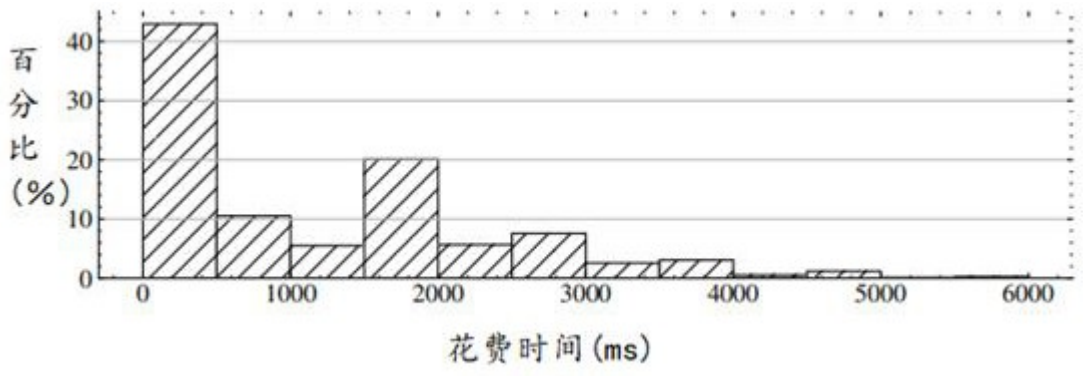

百分比(%)
40
30
20
10
0
0
1000
2000
3000
4000
5000
6000
花费时间(ms)

图10