(19)国家知识产权局

(12)发明专利申请

(10)申请公布号 CN 119856443 A
(43)申请公布日 2025.04.18

(21)申请号 202380064956.5

(22)申请日 2023.09.05

(30)优先权数据
2213203.9 2022.09.09 GB
2214776.3 2022.10.07 GB
2215419.9 2022.10.18 GB
2218148.1 2022.12.02 GB
2218881.7 2022.12.14 GB
2219677.8 2022.12.23 GB
2302252.8 2023.02.17 GB

(85)PCT国际申请进入国家阶段日
2025.03.10

(86)PCT国际申请的申请数据
PCT/EP2023/074272 2023.09.05

(87)PCT国际申请的公布数据
WO2024/052319 EN 2024.03.14

(71)申请人 区块链许可股份公司
地址 瑞士楚格

(72)发明人 克雷格·史蒂文·赖特

(74)专利代理机构 北京市竞天公诚律师事务所 11770
专利代理师 孙磊 徐民

(51)Int.Cl.
H04L 9/00(2022.01)
H04L 45/16(2022.01)

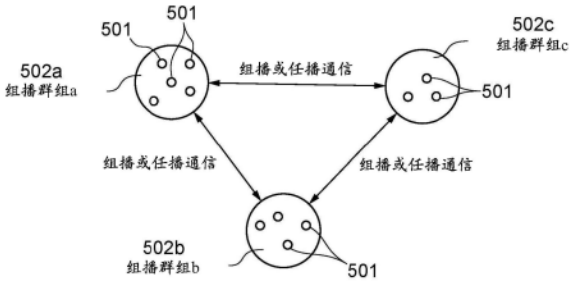
权利要求书2页 说明书61页 附图14页

(54)发明名称

用于改进区块链网络通信的计算机实现的方法和系统

(57)摘要

本发明涉及一种计算机实现的通信方法。所述方法包括一种机制,所述机制用于通过电子网络将警报、通知和更新等区块链相关通信和/或加密货币相关通信尽可能高效、迅速地分发给一个或多个接收者。实施例可以使用IPv6组播来执行此类改进通信。通信可以包括代码、标志或过滤器,所述代码、标志或过滤器使所述通信能够针对特定接收者为目标,并使对通信内容不感兴趣或无权访问通信内容的组播群组成员能够忽略所述通信内容。因此,在处理资源和时间方面都有所改进。在一些示例中,本公开可以有利于实现区块链相关警报密钥或系统,该区块链相关警报密钥或系统可以帮助网络应对紧急情况或威胁,从而提高区块链网络的安全性。



CN 119856443 A

1.一种计算机实现的通信方法,所述方法包括:

由发送资源,将区块链相关通信或加密货币相关通信发送到IPv6组播地址,以便由至少一个接收资源接收;

以及/或者

由至少一个接收资源,接收由发送资源发送到IPv6组播地址的区块链相关通信或加密货币相关通信。

2.根据权利要求1所述的方法,其中:

所述通信是或包括区块链相关警报和/或加密货币相关警报、区块链相关软件更新或加密货币相关软件更新、区块链相关通知或加密货币相关通知、或其他区块链相关通信或加密货币相关通信。

3.根据权利要求1或2所述的方法,其中:

所述IPv6组播地址与和特定区块链网络或加密货币相关的通信相关联。

4.根据前述任一项权利要求所述的方法,其中:

所述至少一个接收资源包括被设置为在区块链网络上运行或与区块链网络一起运行的一个或多个挖掘、验证、钱包和/或服务提供资源。

5.根据前述任一项权利要求所述的方法,所述方法包括以下步骤:

响应于所述区块链相关通信或加密货币相关通信,由所述至少一个接收资源采取至少一个响应动作;可选地,其中:

所述至少一个响应动作包括以下各项中的一项或多项:

i)向一个或多个接收者发送通信;

ii)访问、安装和/或执行数据的一部分,可选地,其中所述数据的所述部分包括一个或多个机器可执行指令;

iii)将至少一个事务输出、事务或事务区块、或加密货币的一部分标记或识别为无效、不可花费、拒绝或予以忽略。

6.根据前述任一项权利要求所述的方法,所述方法包括以下步骤:

由所述至少一个接收资源,将所述通信转发到至少另一接收资源;

可选地,其中:

所述至少另一接收资源包括至少另一IPv6组播地址。

7.根据前述任一项权利要求所述的方法,其中:

i)所述区块链相关通信或加密货币相关通信由被指定为通信合法来源或提供者的生成资源来签名、标记或以其他方式认证;和/或

ii)对所述区块链相关通信或加密货币相关通信进行编码或以其他方式进行保护,使得所述区块链相关通信或加密货币相关通信的内容只能通过使用至少一种解锁机制才能访问、解码、读取、执行或处理,所述至少一种解锁机制诸如密钥、访问码或秘密。

8.根据权利要求7所述的方法,所述方法包括以下步骤:

将所述至少一个密钥、访问码或秘密提供给所述至少一个接收资源或被授权访问、解码、读取、执行或处理所述区块链相关通信或加密货币相关通信的所述内容的另一资源。

9.根据前述任一项权利要求所述的方法,其中所述区块链相关通信或加密货币相关通信包括过滤器代码、标志、标记或其他标识符,优选地,其中:

所述过滤器被设置为作为根据以下项目来使所述区块链相关通信或加密货币相关通信针对/识别所述至少一个接收资源中的一个或多个接收资源的一种手段：

正在发送的区块链相关通信或加密货币相关通信的内容或类型；和/或

预期的、选定的或期望的接收资源集。

10.根据权利要求9所述的方法，其中：

在所述区块链相关通信或加密货币相关通信中，所述过滤器被提供于预先指定的位置和/或被以预定格式提供。

11.根据权利要求9或10所述的方法，其中所述方法包括以下步骤：

由所述至少一个接收资源，根据所述过滤器来处理或忽略所述区块链相关通信或加密货币相关通信。

12.一种计算机设备，所述计算机设备包括：存储器，所述存储器包括一个或多个存储器单元；以及处理装置，所述处理装置包括一个或多个处理单元，其中所述存储器存储被设置在所述处理装置上运行的代码，所述代码被配置为当在所述处理装置上运行时，执行根据前述任一项权利要求所述的方法。

13.一种计算机程序，所述计算机程序包含在计算机可读存储器上并且被配置为当在一个或多个处理器上运行时，执行根据权利要求1至11中任一项所述的方法。

用于改进区块链网络通信的计算机实现的方法和系统

技术领域

[0001] 本文公开的实施例涉及对通过计算机实现的网络传输数据(例如,数据包)的改进。实施例特别适用于但不限于在希望接收、处理、响应和/或存储区块链相关数据/通信的各方之间传输此类数据/通信。具体而言,示例涉及用于向感兴趣的各方、相关联的各方或相关各方发送和接收消息、警报、通知、更新和/或其他内容等电子通信的增强解决方案。

背景技术

[0002] 互联网上的设备被分配唯一的标识符(地址),该唯一的标识符(地址)允许其他设备在网络上识别和定位这些设备。构建初始IP协议时,期望可以从长度为32位的地址区块生成的IP地址的数量足以唯一标识将连接到互联网的所有设备。然而,在设计初始IP协议时,既没有想到互联网会有如此巨大的私人和商业吸引力,也没有想到会有大量各种设备试图连接到互联网。因此,随着个人计算和移动计算技术的发展,随着时间的推移,IPv4所能提供的43亿个地址显然是不够的。

[0003] 虽然IPv4地址耗尽的威胁导致了一些缓解有限集的创造性方法(例如,无类别域间路由(CIPR)、无编号接口和网络地址转换),但是这些措施不足以解决该问题。从短期和长期来看,物联网(IoT)的出现进一步加剧了IPv4的局限性。

[0004] 由于这些挑战,IPv6被提议替代IPv4地址标准。IPv6的核心是使用128位地址,这理论上可以产生3.4×10^{38}个地址。虽然密钥空间的若干范围预先指定用于特定目的,但是剩余地址空间足够大,可以满足连接到具有自己唯一IPv6地址的互联网的每个资源的当前和未来需求。尽管IPv6最显著的优势是拥有更大的地址空间,但是IPv6预计还能提供若干其他优势,其中包括针对组播(multicast)和任播(anycast)的IPv6方法。

[0005] 组播使得能够在单次发送操作中将数据包传输到多个目的地,这是IPv6的基本规范的原生内容。对于IPv6,数据包被发送到组播群组地址;然后,数据包被发送到群组的成员。另一方面,IPv6任播传输使得源资源能够向群组地址发送数据包,但只有群组的一个接收者(拓扑上最接近发送者)会接收到所传输的数据。

[0006] 与单播(unicast)和广播(broadcast)等其他数据包传输/广播方式相比,组播的群组订阅模型及其在IPv6协议中的结合提高了数据包在互联网中的传输效率,减少了网络拥塞。单播是一对一连接,其中数据包从一个IP地址发送到另一IP地址。广播是一对全(one-to-all)传输,其中数据包被发送到网络中的所有地址/节点。因此,在IPv6中使用组播可以为通过互联网传输数据提供更高效且可扩展的方案。

[0007] 除了互联网之外,高效传输数据的需求对于其他网络也至关重要。例如,由于许多分布式账本使用的最大区块大小有限(例如,BTC的1MB区块限制),因此可扩展性对于许多分布式账本来说是一项重大的技术挑战。由于此类协议要求通过网络传播更多、更小的区块,因此网络变得拥塞并且速度变慢。事务需要更长的时间来挖掘和确认。网络性能下降,系统功能受损,导致BTC账本无法与需要快速处理能力的应用一起使用。

[0008] 另一方面,比特币SV协议允许使用更大的区块(目前为4GB,正在向TB区块发展)。

技术挑战在于,如何以快速、安全且高效的方式将这些更大的区块分布在账本的节点网络中的节点上。因此,就区块链相关应用而言,需要提供改进的区块链网络、在时间、处理资源和网络性能方面效率更高的技术方案。

[0009] 另一个挑战在于,以合约方式控制和/或管理网络中的数据包传输,无论是一对一交换还是一对多交换。已知的发布者-订阅者交换效率低下和/或难以扩展。

[0010] 现在已经设计出一种至少可以解决这些和其他技术问题的方案。

[0011] 术语

[0012] 如现有技术已知的,术语“节点”可以指数据结构的基本单元(在计算机科学中),或通信网络(网络/电信)中的连接点,网状网络中的实体,或运行区块链协议实现方式的计算资源,例如比特币网络上的矿工。除此之外,网络中的设备或系统还可以称为“主机”或“对等体”,具体取决于上下文。因此,就本公开而言,由于某些实施例可能涵盖或交叉各种技术领域,因此各个术语之间可能会产生混淆。

[0013] 因此,为了避免混淆并且为了清楚起见,将使用总括术语“网络资源”、“处理资源”、“基于计算机的资源”或简单的“资源”来包括“节点”、“对等体”或“主机”,或网络上的任何设备/系统。这里,更喜欢使用术语“节点”,因为通常意味着(但不一定限于)区块链网络上的节点,例如矿工。

[0014] 此外,为了方便起见,这里可以引用比特币协议/网络/账本,因为它是此类技术中最广为人知的。然而,本公开并不限于与比特币一起使用,并且其他基于账本的协议/网络也属于本公开的范围。例如,包括权益证明机制或利用基于账户而不是基于UTXO的模型的区块链协议、网络和实现方式都属于本公开的范围。还应当注意的是,“比特币”并不限于任何特定的比特币相关协议,任何源自、不同于或偏离原始比特币协议的协议或实现方式都意在属于本公开的范围。公共、私有或许可区块链也属于本公开的范围。

[0015] 本文使用的术语“区块链相关数据”包括但不限于,关于针对或为了实现区块链协议或基于区块链的应用而执行的操作、功能或服务而使用、传输、接收、存储或以其他方式处理的任何数据。

发明内容

[0016] 本公开的实施例提供了用于通过基于计算机的网络传输数据的方案。优选地:

[0017] ●所述方案包括使用IPv6;并且/或者

[0018] ●所述数据是区块链相关数据,但不限于仅用于区块链和区块链相关数据;并且/或者

[0019] ●所述网络是分布式网络,例如账本(区块链)网络或任何点对点(P2P)网络。

[0020] 在本公开的示例性实施例中,基于计算机的资源可以相关联以形成一个或多个组播群组,每个群组具有其自己的相应组播地址。所述组播群组地址是所述群组中资源的逻辑集体标识符,以便它们都可以通过组播通信从发送节点接收数据包。在一些实施例中,所述地址是IPv6组播地址,并且所述数据通过互联网发送和接收。

[0021] 在一个特别有利的示例中,本公开可以用于从发送资源向接收资源组播群组发送数据,并且所述数据涉及区块链区块和/或区块链事务(transaction)的至少一部分。在此类示例中,所述发送资源只需向所有预期接收者发送一次所述数据即可接收副本,而不是

按照单播向每个单个接收者发送多次。

[0022] 在一个或多个实施例中,所述接收资源群组可以形成覆盖网络。所述覆盖网络可以是相对于与给定区块链协议相关联的区块链网络的覆盖层。所述区块链网络可以包括全区块链节点,每个完整区块链节点根据所述协议运行客户端,并且根据所述区块链协议并由所述区块链协议指定来执行以下各项中的至少一项:挖掘、核实、共识和区块链维护功能。在一些实施例中,全节点可以包括用于在事务被写入区块链账本之前存储所述事务的内存池,如下所述并且是本领域已知的。附加地或替代地,所述全区块链节点可以基本上如下所述并参考图1至图4作为区块链节点104。在一个或多个实施例中,所述接收资源中的一个、部分或全部接收资源不是所述区块链网络上的全节点。在本文公开的一个或多个实施例中,所述接收资源中的一个、部分或全部接收资源可以用于执行所述全区块链节点运行的协议指定功能的子集。

[0023] 每个群组中的所述接收资源可以具有各种类型、形式、配置或目的,并且所述发送资源可以是所述群组的成员或在所述群组的外部。本公开无意限制所发送数据的类型或性质,或者发送所述数据的目的。

[0024] 然而,在一个或多个实施例中,群组中的发送节点和/或接收节点中的一个、部分或全部可以是区块链网络上的全节点或覆盖网络上的节点,并且所述数据可以包括与已经被验证但尚未写入区块链账本的未确认事务相关的数据。在此类实施例中,可以提供用于实现内存池的系统和方法,所述内存池在区块链网络或与所述区块链网络交互的覆盖网络中或关联于区块链网络或与所述区块链网络交互的覆盖网络。

[0025] 本公开的有利应用至少可以包括向提供分布式和/或并行化区块链相关功能的计算资源群组发送数据的能力。例如,此类功能可以是挖掘功能、链上搜索功能、核实功能等。本公开的技术目标中的至少一个技术目标可以是增强区块链网络的可扩展性和/或充当(底层)区块链网络顶部的覆盖层的覆盖网络的可扩展性。所述底层区块链网络可以是如本文所述并参考图1至图4的对等(P2P)网络106。根据本公开的实施例,所提供的技术改进中的至少一项或部分技术改进可能不仅涉及在事务通过传统(底层)区块链网络时更快或更有效地传播事务,而且涉及提高事务或区块或其部分的吞吐量。

[0026] 参考图5,示出了三个资源501群组。组播群组“a”502a包含五个资源501,组播群组“b”502b包含四个资源,而组播群组“c”502c包含三个资源。应当理解的是,每个组播群组中的资源501的数量与本发明无关。例如,第一群组可以具有十个资源501,第二群组可以具有一个资源501,第三群组可以具有一百个资源501。如本文所解释的,组播群组502是可通过单个组播地址访问的资源群组。向另一资源发送任何类型的数据的资源501在本文中可以称为发送资源,并且所述数据的接收者可以称为接收资源。

[0027] 图5示出了相互通信的三个资源组播群组中的每个资源组播群组。通信可以包括在传输中发送一个或多个数据包。所述数据可以是区块链相关数据,但不一定如此。所述传输可以包括与对来自一个或多个接收者的数据的请求相关的数据。或者,所述传输可以简单地向所述接收者提供数据,并且可能不包括对响应的请求。本公开不限于所述一个或多个接收者在从所述发送资源接收到所述数据时执行的动作的性质、形式或类型。所述传输可以使用组播和/或任播来执行。

[0028] 当使用组播时,组播群组(例如,群组502a)的资源可以以到与组播群组502a/502b

相对应或关联于的单个组播地址的单次传输的形式向同一群组502a和/或另一组播群组(例如,502b)发送数据。这样,仅发送一次传输,并且只有(但不是全部)作为接收组播群组成员的资源接收所述数据。

[0029] 当使用任播时,组播群组(例如,群组502a)的资源501可以通过以到与组播群组502b相对应或关联于的单个任播地址的单次传输的形式向同一群组502a或另一组播群组(例如,502b)发送数据来传输所述数据。所述一个或多个数据包被路由到组播群组502b的被确定为在拓扑上距离所述发送资源最近的资源501。所述接收资源随后可以将所述数据转发到组播群组“b”的一个或多个其他资源,或者转发到一个或多个其他群组中的任何一个或多个其他资源,或者甚至转发到不属于任何群组的任何其他资源。这样,仅将一次数据传输发送到特定群组内的单个接收者,但随后可以通过组播传输在该群组的其他成员之间传播该数据。这在只有所述组播群组的一个成员或一个成员子集需要接收所述传输以便向整个群组提供所述数据的情况下是有利的。类似地,组播群组的资源可以使用组播或任播来发送或接收数据。

[0030] 当使用组播时,组播群组(例如,群组“b”)的资源可以通过以到与组播群组“a”相对应的单个组播地址的单数据传输的形式向组播群组“a”发送数据(例如,响应于此类请求而请求的数据)来发送所述数据。这样,只需要一个数据传输实例,并且只有组播群组“a”的成员资源接收所述数据。在该实施例中,所述发送资源可以称为“发送资源”,并且组播群组“a”的成员资源可以称为“接收资源”。

[0031] 当使用任播时,组播群组(例如,群组“b”)的资源可以通过以到与组播群组“a”相对应的单个任播地址的单数据传输的形式向组播群组“a”发送数据(例如,响应于所接收请求而请求的数据)来发送所述数据。所述数据被路由到组播群组“a”的资源,该资源被确定为在拓扑上距离发送所述数据最近的资源。所述接收资源随后可以将所述数据转发到组播群组“a”的其他资源。这样,只需一个数据传输实例即可使所述数据到达组播群组“a”,只有组播群组“a”的成员资源接收数据,解决了只有组播群组的子集需要数据的可能性。

[0032] 在一个示例中,发送资源和/或接收资源被配置用于生成、存储、处理、访问和/或维护数据包,所述数据包优选地包括区块链相关数据。根据所述数据包确定分配地址,并且所述数据包通过电子网络至少部分地从所述资源传输到所述分配地址。

[0033] 确定所述分配地址可以包括处理所述数据包以确定密钥,并使用所述密钥从地址集中选择至少一个地址。所述密钥可以通过对所述数据包进行解析来确定。所述发送资源可以持有数据结构,所述数据结构包括与对应密钥集相关联的分配地址集。

[0034] 如本文所教导的,分配可以补充使用IPv6传输数据的高效且可扩展的方案,并且至少一个数据包的传播可以通过在网络内传播数据包的传输来均衡。节点和/或路由器可以被配置为注册或订阅一个或多个分配地址,例如所述多个组播地址的子集,从而使数据包的传输在与所述分配地址相关联的资源之间实现均衡。可以通过在一定范围内的节点和/或路由器之间分布传播的数据包来实现均衡,这些节点和/或路由器会选择性地订阅分配的组播群组和/或从组播地址接收。均衡可以抑制数据包的传输中的瓶颈,特别是当数据包是大区块时,这可能会导致节点或路由器处出现延迟,或者当数据包是事务并且事务量以普遍方式传播而使网络泛洪时。

[0035] 在包括发送数据的实施例中,组播群组的多个资源可以各自发送所述数据的一部

分。在一个实施例中,所述多个资源中的每个资源可以发送所述数据的哈希和/或所述数据的相应部分的哈希。所述哈希可以代替所述数据本身发送或除了所述数据本身之外发送。这种分布有助于减少网络中的拥塞。

[0036] 在实施例中,组播群组中的一个或多个资源可以是:区块链网络中的资源、与金融机构相关联或由金融机构控制的计算资源;商家;和/或数字钱包。

[0037] 在附加或替代实施例中,所述请求可以包括对与区块链相关事件或活动相关的通信或警报的请求。在一个实施例中,所发送的数据包括与区块链相关事件或活动相关的通信或警报。所述通信或所述警报可能涉及所述区块链网络中的双重花费或双重花费尝试。

[0038] 在实施例中,所请求和/或所发送的数据包括:区块链相关数据,例如区块链事务或其一部分;区块链区块的至少一部分;区块链事务脚本的至少一部分;默克尔路径或默克尔证明的至少一部分;和/或与区块链网络的共识机制一起使用或相关联的数据。

[0039] 在一个实施例中,组播群组的资源通过互联网协议(IP)组播地址与一个或多个其他组播群组通信。在一个实施例中,组播群组的资源通过IPv4组播地址与一个或多个其他组播群组通信。在一个实施例中,组播群组的资源通过IPv6组播地址与一个或多个其他组播群组通信。在一个实施例中,资源和/或资源群组可以彼此分离,使得它们通过互联网通信。

[0040] 在一个实施例中,所述组播群组中的每个组播群组包括一个或多个接收资源。在一个实施例中,给定接收资源群组中的每个接收资源用于接收发送到所述给定接收资源群组的所述组播地址的数据。

[0041] 在一个实施例中,资源订阅接收资源群组。在一个实施例中,所述资源通过向网络发送信号来订阅。

[0042] 在一个实施例中,所述资源离开接收资源群组。在一个实施例中,所述资源通过停止向网络发送信号来离开所述群组。

[0043] 在一个实施例中,接收资源群组中的接收资源执行区块链协议指定的功能、与区块链协议中指定的挖掘或共识函数相关的计算或其他操作、简单支付验证(SPV)操作、在区块链事务写入区块链之前或之后对其进行核实、搜索区块链以识别、定位和/或确认区块链中是否存在给定事务或区块、生成区块链事务、将事务写入区块链和/或向区块链网络广播事务。

[0044] 在一个实施例中,可以通过将区块链相关数据的一部分从发送资源发送到一个或多个接收资源群组,对所述一个或多个群组中的每个群组进行轮询以获得目标响应。

[0045] 根据一个或多个实施例,可以提供一种计算机实现的通信方法,所述方法包括一种机制,所述机制用于通过电子网络将诸如警报、通知和更新等区块链相关通信和/或加密货币相关通信尽可能高效、迅速地分发给一个或多个接收者。优选实施例使用IPv6组播来执行此类改进通信。组播通信可以包括代码、标志或过滤器,所述代码、标志或过滤器使所述通信能够针对特定接收者作为目标,并使对通信内容不感兴趣或无权访问通信内容的组播群组成员能够忽略所述通信内容。因此,在处理资源和时间方面都有所改进。在一些示例中,本公开可以有利于实现区块链相关警报密钥或系统,该区块链相关警报密钥或系统可以帮助网络应对紧急情况或威胁,从而提高区块链网络的安全性。

附图说明

[0046] 为了帮助理解本公开的实施例并示出如何实施此类实施例,现将仅通过举例的方式参考附图进行说明,其中:

[0047] 图1是一种用于实现区块链的系统的示意性框图。

[0048] 图2示意性地示出了可记录在区块链中的事务的一些示例。

[0049] 图3A示出了客户端应用程序的示意性框图。

[0050] 图3B示出了可由图3A的客户端应用程序表示的示例性用户界面的示意性模型。

[0051] 图4示出了用于处理事务的一些节点软件的示意性框图。

[0052] 图5示出了本发明的实施例,其中属于组播群组的资源彼此通信以安全、高效且快速地分发电子数据。

[0053] 图6a示出了采用点分十进制表示法的IPv4地址的示例。

[0054] 图6b示出了采用十六进制表示法的IPv6地址的示例。

[0055] 图6c示出了如何保留地址前缀来表示IPv6地址类型。

[0056] 图7示出了数据包从服务器地址到计算机(示出为PC1)的全局单播地址的单播传输。

[0057] 图8示出了组播传输,用于与图7的单播传输进行比较;这里,从服务器发送的数据包通过互联网路由到组播地址以供订阅者检索。

[0058] 图9示出了任播传输,用于与图7和图8进行比较,其中服务器向任播地址发送数据包;该数据包被转发到所订阅资源集的在拓扑上最近的路由器/节点。

[0059] 图10示出了比特币网络中的区块传播。

[0060] 图11示出了本公开的示例性实施例,其中区块链网络中的节点执行一个或多个挖掘区块的组播传输。

[0061] 图12示出了本公开的示例性实施例,其中区块链网络中的节点执行到任播地址的任播传输。

[0062] 图13示出了本公开的示例性实施例,其中出于区块分发目的而组合组播传输和任播传输的使用。

[0063] 图14提供了根据本公开实施例的区块的组播的有利使用的图示,包括考虑地理因素以提高分发速度和效率。

[0064] 图15示出了区块链网络上的节点通过组播传输向网络中的关键节点广播区块。

[0065] 图16示出了区块链网络上的节点B通过组播传输向网络中的多个节点N1至N4进行广播。

[0066] 图17(a)至图17(d)是示出从用于识别和/或确定分配地址的部分数据导出的值的示例的表格。

[0067] 图18示出了区块链网络上的节点B通过组播传输向网络中的节点N1至N8的八个输出中的每个输出向分配地址进行广播。

[0068] 图19示出了区块链网络上的节点B从节点A接收数据并通过组播传输向网络中的多个节点N1至N4表示的分配地址进行广播。

[0069] 图20示出了区块链网络上的节点B,该节点已经订阅从节点C、D和E接收组播广播,并通过到网络中的节点N1至N8的八个输出中的每个输出的组播传输向分配地址进行广播。

[0070] 图21示出了节点B向组播群组、第一订阅者和第二订阅者发送数据包,其中第二订阅者可选地进一步直接或通过第二组播群组向第一用户传输数据包。

[0071] 图22示出了节点B向八个相应组播群组、第一订阅者和第二订阅者传输八个数据包,第一订阅者订阅并访问来自八个组播群组中的两个组播群组的数据包,第二订阅者可选地聚合所述八个数据包并将其传输到第九组播群组,从而为第一订阅者提供对所述八个数据包的替代访问。

[0072] 图23示出了节点B向八个相应组播群组传输八个数据包,以及六个订阅者(名义上为无人机)访问一个或多个数据包。

具体实施方式

[0073] 通过技术背景,并且特别参考图6至图9,提供了对可以与本公开结合使用以提供各个实施例的技术效果和益处的一些传输协议和技术的解释。

[0074] 如现有技术已知的,互联网协议(IP)是通信协议,该通信协议为网络上的计算机提供识别和定位系统并通过互联网路由数据包。互联网上的资源(即,设备/系统)被分配唯一IP地址,用于识别和定位定义。IPv6的设计旨在解决由IPv4引起的IP地址不足问题。

[0075] IPv6地址:

[0076] 图6a示出了采用点分十进制表示法的IPv4地址的示例。该地址由四个8位部分组成,每个部分用点隔开,称为八位位组。

[0077] 为了进行比较,图6b示出了采用十六进制表示法的IPv6地址的示例,其中每个十六进制字符表示一系列4位。该地址由8个16位部分组成,每个部分用逗号隔开。每个16位部分称为十六进制数。该地址可以使用各种规则来简化,包括i)用双冒号替换多个连续全零十六进制数(仅一次),以及ii)移除十六进制数的任何前导零;这会产生:

[0078] 2001:db8::a111:b222:0:abcd

[0079] 鉴于地址格式的差异,与IPv4相比,IPv6允许更多的地址。反过来,这提供了为不同地址类型保留地址子空间的能力。保留地址前缀以表示各种地址类型,如图6c所示,其中全局前缀是IP地址的区块,其由它们的互联网服务提供者(ISP)提供给最终用户(end user)。长度至少为88位,其中子网ID包括16位,并且主机/接口ID包括64位。

[0080] 这些地址类型通常表示网络内投射信息的不同方法,包括下表所示的方法:

[0081]

地址类型	前缀	信息
全局单播	2000::/3	可公开路由
唯一本地	FC00::/7	可在LAN中路由
链路本地	FE80/10	不可路由
组播	FF00::/8	群组地址
任播	2000::/3	共享地址

[0082] 表1

[0083] 组播:

[0084] 组播是一种一对多(one-to-many)网络传输方案,其中发送资源将单个数据包传输到多个目的地。资源仅通过网络发送一个数据副本。在网络中的适用连接点复制数据之后,已经订阅发送者传输的数据源的资源随后将接收数据副本。组播传输在带宽消耗方面

特别高效,因为即使所有群组都接收一份副本,发送资源也只发送一份数据副本。这与单播形成对比,在单播中,发送资源与每个预期接收者建立连接,并向每个接收者发送单独的数据副本。

[0085] 如图6c所示,IPv6地址的子空间可以指定用于不同类型的地址(单播、组播等)。图6c(2001:0db8::a111:b222:0:abcd)所示的地址就是此类地址的示例。对于单播传输,数据包在全局单播地址之间发送。存在不同类型的IPv6单播地址。全局单播地址是可路由的单播地址。(这与公共IPv4地址的用法类似)——例如,请参阅https://www.ciscopress.com/articles/article.asp?p=2803866&seqNum=4。

[0086] 参考图7,数据包从服务器的地址到PC1的全局单播地址的单播传输将导致该数据包通过互联网路由并到达地址为2001:db8::a111:b222:0:abcd的PC1。PC1将是处理数据包的唯一资源。

[0087] 对于组播,与将数据包发送到PC1的地址相反,将数据包发送到组播地址。这将是前缀为FF的IPv6地址。希望从派生方接收数据的资源加入该组播地址的组播群组。这称为他们的“订阅”。

[0088] 当数据包从服务器发送时,该数据包通过互联网路由到组播地址(例如,图8中的“RLocal”,该图示出了从服务器到订阅者PC1和PC2的组播传输)。数据包到达后,订阅者(例如,PC1和PC2)能够检索数据,而非订阅者PC3和PC4将忽略数据包。该组播减少了从服务器向PC1和PC2发送两个单独数据包的需要。只有在到达RLocal时,才会创建数据包的单独副本。

[0089] 为了使组播分组到达PC1,资源PC1必须向RLocal报告其希望加入组播群组FF00:/8。当RLocal看到该报告时,它将打开到PC1的接口,并承诺如果它在网络上看到组播数据包中的任何组播数据包,就会向PC1转发任何组播消息。网络中的路由器(例如,R2)将被选择作为到FF00:/8的组播的集合点(RP)。知道到R2的最佳路径经过R1,RLocal将向R1发送加入报告,要求R1向集合点R2转发对FF00:/8组播事务的请求。R1将向R2发送加入报告。如果集合点要接收组播数据包,它将该数据包转发到R1,R1随后将该数据包传递给RLocal,RLocal随后将该数据包传递给PC1。

[0090] 任播

[0091] IPv6任播包括多个路由器共享公共IPv6任播地址的情况。如上表1所示,任播地址与全局单播地址共享同一前缀。例如:

[0092] 2001:db8::a111:b222:0:abcd

[0093] 也可以用作任播地址。

[0094] 如果数据包由发送资源发送到任播地址,则该数据包被转发到订阅的资源集的最近路由器/节点。虽然地理距离是确定最近资源的一个因素,但在计算中还有其他影响因素:跳数、效率、延迟和成本等。最后,对于任播,预期只有一个资源接收数据包,通常被描述为一对最近(one-to-nearest)传输。

[0095] 参考图9,其示出了从服务器到路由器R3的任播传输,从图中可以看出,数据包被发送到由至少三个路由器(R1、R3、RLocal)共享的任播地址2001:db8:/32。这些路由器中最近的是R3,因此数据包被发送到R3。应当记住的是,“最近”并不一定指地理位置上的接近。

[0096] 说明性实施例

[0097] 现在转到本公开的说明性实施例的讨论,并且参考图5至图15,提供了一种利用这些传输技术在计算网络上快速、安全且可扩展地分发数据的方案。在优选实施例中,数据通过网络(例如,互联网)从一个或多个发送资源传达到一个或多个接收资源。在一些场景中,接收资源被组织成逻辑群组,并且每个群组可以包括一个或多个资源。资源可以包括任何类型的计算资源,由任何一个或多个组织控制或属于任何一个或多个组织,并被设置用于任何合适的目的。每个资源可以包括一个或多个硬件和/或软件组件,并且被设置用于通过电子网络与其他资源通信。在一些情况下,资源可以是区块链网络上的挖掘节点,而在其他情况下,资源可以是数字钱包、加密货币交换所、搜索引擎、文件服务器或服务提供者等。一个或多个资源的类型、形式、目的或配置没有限制。

[0098] 每个群组与相应群组标识符相关联,该群组标识符用作数据可以被发送到的唯一地址。给定群组中的所有资源都与该群组的地址相关联,因此可以接收从发送者发送到该群组地址的数据。地址可以是组播地址,并且在一个优选实施例中,地址是IPv6组播地址。因此,每个接收资源群组都用IP地址来表示。因此,群组地址可以用于实现一对多通信,因为发送资源只需向群组地址发送一次数据包,群组中的每个资源就能接收到该数据包,而不是在一对一通信中向每个资源发送数据包(例如,在单播传输中所执行的)。

[0099] 接收资源可以通过发送组播侦听者发现协议(Multicast Listener Discovery,MLD)消息来订阅(即,加入)群组,该消息表明其参与的意图。有利的是,加入资源可以位于局域网(LAN)或互联网上,因为组播群组不受本地或全局网络地理位置的限制。只要资源发信号通知其是群组的成员,该资源就可以接收发送到该群组地址的组播数据包。因此,资源可以随时动态地加入或退出群组,只需向网络发出加入或停止加入该群组的信号即可。

[0100] 因此,组播群组用于识别接收者群组,每个接收者都对发送到该群组的地址的特定数据传输感兴趣或有需求。虽然只有属于给定群组的资源可以是接收者,但是任何资源都可以向群组发送数据,无论其是否属于该组播群组。一个群组中的资源可以向另一群组发送数据,反之亦然。

[0101] 组播侦听者发现(MLD)和MLD窥探

[0102] 如本领域已知,MLD内置在IPv6协议中。例如,请参见https://en.wikipedia.org/wiki/Multicast_Listener_Discovery。MLD窥探(MLD Snooping)使用MLD来提供多种效率,因为它可以避免在网络中泛洪数据包,从而避免将数据传输到尚未发信号通知有兴趣接收该数据的网络资源。此外,它还提供了更高的网络安全性,因为它可以避免来自未知网络来源的拒绝服务(DOS)攻击。

[0103] 默认情况下,MLD窥探处于禁用状态。因此,当交换机接收到具有组播地址的数据包时,该数据包会被发送到其VLAN中的所有接口端口,但接收到该数据包的端口除外。换句话说,交换机会在VLAN中泛洪数据包。如果资源不是组播群组的成员并且对该信道上的数据不感兴趣,则会忽略数据包。显然,这会导致不必要的网络流量以及能源和处理资源的低效利用。

[0104] 然而,当启用MLD窥探时,交换机仅将组播地址数据包转发到已经发信号通知有兴趣接收发往该地址的数据包的接口端口。换句话说,交换机仅将数据包发送到属于已经订阅该组播群组的成员的端口。因此,MLD窥探允许发送资源选择性地将数据包传输到已经指示有兴趣接收数据包的资源。如果没有网络资源订阅组播群组,则发送资源不会发送任何

数据包。有关更多详细信息,请访问:

[0105] https://techhub.hpe.com/eginfolib/networking/docs/switches/WB/15-18/5998-8170_wb_2920_ipv6_config_guide/content/v33585413.html。

[0106] 区块链相关数据的分发:

[0107] 在一个特别有利的场景中,发送资源和/或接收资源是用于发送、接收、存储和/或处理区块链相关数据的计算资源。在一个示例中,这些资源可以是区块链网络中实现特定区块链协议(例如,比特币SV协议)的节点。可以创建包括区块链网络中的所有节点或节点的子集的组播群组。例如,可以建立组播群组,以在矿工池、PoW计算资源集或任何其他类型的操作之间共享数据。然而,在其他示例中,这些资源中的一个、部分或没有资源可以是区块链网络上的节点,但可以是以某种方式处理数据以用于区块链和/或加密货币相关目的的资源。例如,这些资源可以包括数字钱包提供者、加密货币交换所、银行和金融机构、分布式验证提供者等。

[0108] IPv6的效率被认为对比特币等区块链网络有利,因为1)比特币本身由分布式节点网络维护;并且2)这些节点通过互联网进行点对点通信。

[0109] 对于比特币网络,每个节点预计将存储区块链/账本、内存池(未确认事务的数据集)和UTXO集(所有未发送事务输出的列表)的最新副本。为了维护这些数据集的最新版本,需要在节点之间进行持续通信,其中经过核实的事务和区块在这些节点之间共享。区块包含事务集以及区块头。区块头本身包含用于挖掘区块的随机数,以及表示该区块中事务集的默克尔根。实施例可以在以下方面发挥优势:

[0110] ●事务传播:

[0111] 当钱包向比特币网络提交事务时(例如,用户使用比特币在商店购买商品),接收该事务的全节点104检查该事务是否有效(内容满足该节点的软件的比特币协议版本的所有规则),以及该事务是否不是内存池中已有事务的双重花费。(当两个花费事务试图在区块链上花费给定资金事务的相同输出时,就会发生“双重花费”)。如果满足这两个标准,则比特币节点104更新其个人内存池,并将经过核实的事务发送到它连接到的其他比特币节点集。这些接收节点中的每个接收节点继续执行相同的有效性检查、更新和事务传输步骤。这允许通过比特币网络传播事务。

[0112] ●区块传播:

[0113] 参考图10,其示出了区块链(例如,比特币网络)中节点之间的区块传播。当节点从其内存池中的事务池中挖掘新区块时,该节点会更新其数据存储库(UTXO集、内存池、区块链)并将该新区块转发到其连接的节点。对于比特币协议,节点最多可以有125个连接,其中只有8个连接是传出连接。

[0114] 这些连接的节点依次对区块执行自己的有效性检查、更新其数据存储库并向前中继区块。这允许通过比特币网络传播区块。

[0115] 事务和区块传播的速度尤其重要,因为节点和/或钱包将需要其数据集(UTXO集、内存池、区块链)的最新版本,以便最大限度地降低双重花费的风险。尽早了解最新挖掘的区块也符合全挖掘节点104的最佳利益。这是为了减少这些挖掘节点为内存池生成工作证明(PoW)所花的时间,其中这些事务中的部分或全部事务已经包括在挖掘区块中。

[0116] 对于BTC网络,新挖掘的区块平均需要10秒才能在网络中传播。该传播时间与区块

的大小成正比(对于BTC网络最大为1MB)。另一方面,实现允许大区块大小的比特币SV协议的节点需要创新性方案来减少传播大区块的时间。因此,更快的区块传播对于可扩展性至关重要。

[0117] ●区块头传播

[0118] 鉴于节点从多个来源接收事务,并且这些节点的内存池可能共享事务,因此将整个新挖掘的区块发送到至少8个传出连接可能效率低下,因为接收节点可能已经拥有其内存池中挖掘区块中许多事务的副本。

[0119] 为了解决该问题,发送节点可以发送区块头的副本以及区块中包含的事务ID(事务的哈希)列表,而不是将新挖掘的区块发送到输出点节点。在一些实施例中,这可以是取决于正在使用的区块链协议的有序列表。该(有序)列表以及头部的默克尔根和随机数可以证明挖掘区块的有效性。接收节点可以使用有序列表来确定其内存池中尚未拥有哪些事务(如果有的话)。然后,接收节点可以向发送节点发送对未决事务的副本的请求。接收到该请求后,发送节点将这些副本发送到请求节点。然后,请求节点基于其已经从发送节点接收到的事务和头部信息来编写或编译区块,然后将新区块添加到其区块链的副本中。

[0120] 使用IPv6的组播分发:

[0121] 根据一些实施例,采用数据包的IPv6传输,以有利于通过区块链网络或在区块链网络中进行区块分发。图11示出了从节点5到节点网络的挖掘区块的组播分发的示例。区块链网络(或网络的子集)中希望接收区块更新的节点可以基于特定标准来选择订阅共享组播地址。一个或多个发送(源)节点可以向组播地址发送适用区块。这些区块可以是全区块或部分区块,也可以是挖掘区块或预挖掘区块。

[0122] 在图11的示例中,区块链节点4从PC1、PC2和节点5接收比特币事务,并且能够成功地产生挖掘区块。这旨在尽可能高效地分发到感兴趣节点集。在该示例中,这些感兴趣节点是节点1和节点2。这两个节点均已订阅组播地址2001:db8:/32。节点4向组播地址发送区块的一个副本。到达该地址后,区块被复制,并且副本被发送到订阅者节点1和节点2。

[0123] 如上关于区块头传播所提及的,向接收者发送完整区块可能意味着节点接收其已经拥有的事务的副本。如果所需数据(或其至少一部分)可以在本地访问,而不需要通过网络发送,这可能会导致效率低下。

[0124] 考虑到这一点,可以执行以下过程的变体:

[0125] ●发送节点不会通过组播发送整个区块,而是可以通过IPv6组播仅向组播地址发送区块头和(有序)事务列表;因此,所有订阅节点将通过组播传输接收该信息;

[0126] ●每个接收(即,订阅)节点使用所接收的信息来确定它们需要哪些未决事务(如果有的话)来生成完整区块;

[0127] ●如果接收节点确定其需要至少一个事务来生成区块,则该节点(通过单播传输)向发送节点发送对所需事务(即,缺失事务)的请求;该请求包括其缺失事务的ID;

[0128] ●发送节点从接收节点接收请求;

[0129] 发送节点向接收节点发送包括所请求的缺失事务的传输。优选地,这将是仅到已经发送请求的单个接收节点的单播传输。这是因为相应接收节点的未决节点集可能是唯一的,从而降低了通过IPv6组播向整个订阅群组发送未决事务的价值或好处。

[0130] MLD窥探。如上所提及的,MLD窥探可以为在网络中传输数据提供显著的效率和好

处。对于区块链相关服务或功能,这可以显著地改善区块链实现的应用和服务提供者,以及增强实现底层区块链协议本身的网络。

[0131] 使用IPv6组播,发送资源能够启用MLD窥探。本公开的实施例可以至少包括但不限于以下条款集8中包括的特征。这使得发送者能够选择性地仅向那些指示希望接收数据包的资源传输数据包。这意味着区块链相关或有关数据的传输可以有效地针对特定目的地。这有效地将信息流从推送模式更改为订阅/发布模式;即,接收主机订阅IPv6组播群组,然后数据包从运行MLD窥探(层2)的交换机转发到运行MLD(层3)的路由器,再转发到接收主机。因此,只有必要的流量才通过网络转发。这至少在一定程度上解决了如何在区块链网络中实现可扩展性的公认技术挑战,这需要每秒发送大量事务。因此,结合使用MLD窥探的区块链相关方法和系统促进或使得能够构建改进的区块链网络和区块链实现的应用。

[0132] 例如,考虑由2名成员爱丽丝和鲍勃组成的IPv6组播群组,他们希望参与SPV验证。假设其中一名成员是商家,另一名成员是希望使用比特币从商家购买商品或服务的客户。使用MLD和MLD窥探允许爱丽丝和鲍勃两者接收默克尔路径作为对比特币网络上节点提交的响应,从而显著改善SPV事务。在一些实施例中,区块链网络上的某些节点可以提供该功能作为基于订阅的服务。在其他示例中,应用和服务可以订阅组播群组地址以接收从区块链节点本身上游提交的区块链事务。这是可能的,因为事务是公开的。这种改进的数据流使得区块链事务能够通过默克尔证明使用默克尔路径进行验证,而不是扫描或迭代区块链账本。同样,这为构建需要与区块链相关数据交互、使用或查询区块链相关数据的区块链相关应用提供了更高效的方案。

[0133] 有利地,本公开的一些实施例提供了用于实现区块链网络的内存池或UTXO集的方案。根据此类实施例,网络上的节点可以是区块链节点,并且可以加入本文所述的组播群组。节点可以是全区块链节点104。节点可以通过IPv6组播消息在群组成员之间传输区块链相关数据。区块链相关数据可以是或包括至少一个未确认区块链事务或至少一个未花费事务输出(UTXO)。尽管国际专利申请WO2018/234987公开了使用组播来通过位于区块链网络顶部的专用节点的覆盖网络传播初始事务,但是没有公开使用IPv6组播来与区块链网络本身上的(全)节点一起使用。此外,该国际专利申请没有公开使用组播来传播未确认事务,例如实现内存池所需的事务。事实上,比特币网络仍然没有使用IPv6进行节点间通信,并且WO2018/234987主动公开了使用DHT来代替组播,因为这表明网络缺乏足够的扩展能力来应对组播分发带来的事务输出增加。

[0134] 使用IPv6的任播分发:

[0135] 任播特别适用于对传输速度特别关注的情况。关于区块链网络中的区块传播,节点希望尽快接收新挖掘区块的副本。节点在获得新挖掘区块的副本时,可以选择加入任播地址。这实质上意味着为自己(即,网络接口)分配任播地址。任播地址实质上是共享的单播地址。然后,感兴趣的节点可以向任播地址发送请求传输,表明他们正在寻找新挖掘区块的副本和/或请求获得新挖掘区块的副本。所述请求传输将到达属于任播地址的拓扑上最近的节点。然后,这个最近的节点将直接(使用单播)向提出请求的节点发送所挖掘的区块的副本。

[0136] 图12示出了从节点5到任播地址2001:db8:/32的任播传输的示例。节点1、2和3已经获得新挖掘区块的副本。在接收并核实挖掘区块的副本后,它们各自将自身分配到任播

地址2001:db8:/32。共同理解的是,该任播地址意味着该地址表示接收者拥有新挖掘区块的副本。节点5向任播地址发送对区块的副本的请求;(节点1、2和3中的)在拓扑上最近的节点将是接收该请求的节点。

[0137] 在图12的情况下,最近节点是节点1。然后,如果选择的话,所述节点将通过单播向节点5发送区块的副本。考虑到选择了最近节点,这意味着节点1可能会更快地接收区块的完整副本。

[0138] 然而,应当注意的是,"最近"节点取决于除地理接近性以外的若干因素;延迟和成本被列为其确定的因素。如果到节点1的信道因区块传输和区块请求而变得不堪重负,则"最近"的计算可能会选择另一节点作为新的最近节点。这会在拥有新区块的节点之间分发请求和区块传输。

[0139] 在区块头传输的情况下,该过程仍然可以如上所述地操作。在一个优选实施例中,对新挖掘的区块的区块头的请求将通过任播请求来执行。当确定最近节点时,将从请求节点(节点5)发送单播传输,请求最近节点(节点1)的未决事务。应当记住的是,未决事务是新挖掘的区块中不在请求节点的内存池中的事务。这些未决事务将被发送到请求节点(节点5)。

[0140] 结合使用组播与任播和/或单播进行分发

[0141] 图13提供了结合使用组播与任播进行区块分发的图示。在此类实施例中,将先前描述的组播和任播的使用相结合,以提供从源节点(图13的层0中的N1)向组播订阅节点(层1中的N2…N4)发送区块的方案。其他感兴趣的节点(层2中的N6、N7)通过任播查询传输来确定组播群组(层1)的哪些成员是其最近的对等点。然后,这些层2节点继续从最近的层1节点下载区块。

[0142] 对于图13,节点N1是挖掘区块的第一节点,并将该区块组播到订阅者N2、N3和N4集。N5不是订阅者。这些节点中的每个节点预计还为自己分配任播地址(共享单播地址)。共享该地址的节点预计是具有新挖掘区块的节点。节点N1和N7对该新区块感兴趣,并向N2、N3和N4共享的任播地址发送请求(Q)。该请求被路由到最近的节点。对于N6,最近的节点是N2。N2接收对区块的请求并向N6发送该区块。对于N7的请求,到达N4(最近的节点)。N4通过单点传输向N7发送区块。

[0143] 这可以使用固定的任播地址来实现,如下所述。应当注意的是,这仅用于说明目的,并且可以省略以下步骤中的一些步骤,并且下面提供步骤的顺序并非旨在限制,因为一些步骤可以按照与下面所示的顺序不同的顺序执行;以下步骤列表并非详尽无遗:

[0144] i.关联(例如,关键利益相关者)节点集就其共同义务、责任或目标达成一致(例如,根据特定协议或根据协议条款来分配大区块或区块)。

[0145] ii.这些关联节点订阅共享组播地址。组播地址可以由这些节点中的一个或多个节点确定,也可以由向关联节点发送组播地址的地址确定方确定。订阅地址后,这些节点现在是组播群组成员,即,他们侦听组播地址。

[0146] iii.关联节点向更广泛的网络(例如,比特币网络)或至少向其在网络中的本地或指定社区或协会推广/宣传其服务。

[0147] iv.这些关联节点中的至少一个关联节点或另一方向更广泛的(比特币)网络或至少其各自的本地或指定社区推广其共享组播地址。挖掘新区块的节点需要将其新区块(或

区块头和有序事务列表)发送到该组播地址。

[0148] v.这些关联节点中的至少一个关联节点或另一方向更广泛的比特币网络或至少其各自的本地或指定社区传达唯一任播地址。

[0149] vi.节点(可以是关联节点或非关联节点)挖掘新区块。

[0150] vii.挖掘节点(即,已经挖掘新区块的节点)将新区块(或区块头和事务列表)发送到组播地址。

[0151] viii.区块(或区块头和事务)通过IPv6路由到组播群组的所有成员;换句话说,数据通过组播传输发送到组播地址。

[0152] ix.这些关联节点中的至少一个(但优选地全部)关联节点执行必要的检查,以核实新挖掘区块的合法性。

[0153] x.如果已经发送区块头和事务列表而不是全区块:

[0154] a.则关联节点将有序列表中的事务与其内存池中的事务进行比较。如果无法将列表中的至少一个事务与其内存池中的事务进行匹配,则关联节点会向挖掘节点发送单播请求,请求一个或多个未决事务。

[0155] b.挖掘节点通过单播传输向关键节点发送一个或多个缺失事务。

[0156] 在使用任播的情况下:

[0157] 1.非关联节点可以间歇地向组播群组的任播地址发送请求。请求消息可以包括发送节点的单播地址。

[0158] 2.如果具有任播地址的关联节点(即,接收组播群组成员)接收到对新区块的副本的请求,则关联节点随后通过单播向请求节点发送区块(或区块头和事务列表)的副本(通过任播接收请求意味着群组成员是群组中距离请求发送节点最近的)。

[0159] 3.如果区块头和有序列表发送到非关联节点:

[0160] a.该节点检查其内存池中的有序列表中的事务,即如上所述,该节点检查其内存池并检查列表中的每个事务是否在其内存池中;如果内存池中缺失列表中的任何事务,则该节点向关联节点发送单播请求,以请求一个或多个未决(缺失)事务。

[0161] b.关联节点通过单播传输向该节点发送一个或多个缺失事务。

[0162] 在已经过去一定时间或已经满足标准(例如,区块由关联节点发送到至少25个节点)之后,则关联节点可以将其自身从任播地址取消分配。关联节点专注于侦听组播地址处的新区块。

[0163] 应当注意的是:

[0164] ●节点可以在接收区块请求并传播新区块的同时侦听组播地址处的新区块。

[0165] ●节点可以订阅多个组播地址,即,节点可以在比特币网络上侦听多种不同类型的区块。

[0166] ●节点可以根据其自己的选择将其自身从组播群组或任播地址移除。

[0167] 鉴于比特币网络实现方式中通常存在的对出站节点数量(对于BSV为8)的限制,寻求快速传播其新挖掘区块的节点可能会在仔细考虑其连接到的最多8个节点时发现价值。

[0168] 例如,可以基于8个节点的地理位置来战略性地选择这些节点,因为每个节点都可以是集中在其地理区域内的高容量节点。(“高容量”包括带宽、低延迟、计算能力、存储等因素)。这8个节点加入组播以进行新区块传播,即侦听共享组播地址。挖掘区块的任何节点都

认为适合对该8个中心化节点集执行组播,然后这些中心化节点将该区块传达给各自地理区域内的其他节点。

[0169] 考虑图14,其提供了使用区块相关数据的组播和基于地理位置的任播的区块链相关数据分发的示例。位于加拿大的节点N1挖掘的区块通过组播发送到位于巴西的关键中心节点(N2)、位于德国的关键中心节点(N4)和位于尼日利亚的关键中心节点(N3)。位于澳大利亚的节点(N5)向N2、N3和N4的共享任播地址发送对新区块的请求。该请求到达位于尼日利亚的N3(被确定为最近),N3随后向位于澳大利亚的节点N5发送新区块。

[0170] 应当注意的是,比特币网络内关键节点的集中化可能不会直接映射到地理位置。这些节点可以是"拓扑上集中化的",或者在网络中的新兴集群/社区中具有高度集中性。例如,Tao等人,[Tao,B.、Dai,H.N.、Wu,J.、Ho,I.W.H.、Zheng,Z.和Cheang,C.F.,2021年,比特币事务网络的复杂网络分析,《IEEE电路与系统汇刊第二辑:快速简报》,第69卷第3期,第1009-1013也]显示了比特币核心网络中社区的存在。图15中的网络示出了节点N1通过组播向比特币网络中的关键"中心"节点(N2…N8)广播区块。然后,这些接收节点可以将区块相关数据分发给其社区中的其他节点。

[0171] 均衡

[0172] 如上文结合图5所述,数据包可以传输到至少一个组播地址,其中一个或多个数据包包括在传输中。术语"数据包"可以用于指单个数据包(例如,区块链事务),或数据包集合(例如,包括多个事务的区块链区块)。数据包及其中的数据可以是区块链相关数据,但不一定如此。因此,数据包以本文所述的方式传播。例如,数据包可以包括区块链事务、区块链区块和区块头。

[0173] 与单播和广播等其他数据包传输/广播方式相比,组播及其在IPv6协议中的结合可以提高数据包在互联网中的传输效率,减少网络拥塞。

[0174] 作为对使用IPv6传输数据的高效且可扩展的方案的补充,如本文所教导的,数据包的传播可以得到均衡。数据包的传输可以通过使用分配地址来改进,从而在网络中传播数据包时使用其相关联的资源。

[0175] 分配地址是根据数据包本身确定的。提供多个组播地址来实现所有数据包的传播,并根据要传输的数据包从多个地址中选择一个地址。这可以起到均衡或分散网络中数据包的传输的作用。节点和/或路由器可以被配置为注册或订阅一个或多个分配地址,例如所述多个组播地址的子集,从而使数据包的传输在与所述分配地址相关联的资源之间实现均衡。均衡可以抑制数据包的传输中的瓶颈,特别是当数据包是大区块时,这可能会导致节点或路由器处出现延迟,或者当数据包是事务并且事务量以普遍方式传播而使网络泛洪时。

[0176] 可以通过将传播分配到分配地址来实现负载均衡。发送资源和/或接收资源等资源被配置为发送和/或接收记录等数据包,所述资源适于生成、存储、处理、访问和/或维护数据包记录。数据包可以包括区块链相关数据。资源可以根据数据包确定分配地址。然后,资源可以通过电子网络至少部分地将数据包的传输从发送资源发送到分配地址。附加地或替代地,所述资源可以订阅群组(例如,组播群组),以接收发送到分配地址(例如,分配组播地址)的传输。在发送和/或接收数据包时使用分配地址,可以通过在相应的分配地址及其相关联的资源之间分散数据包的分布来实现负载均衡,其中分配地址的选择根据数据包进

行。这提供了几项重大技术改进,包括提高资源和能源的效率和利用率。

[0177] 图16示出了发送资源B向四个节点(N1至N4)传输数据包。传输中的每个传输都会发送到组播群组。节点N1至N4订阅组播地址。然而,节点N1订阅的是分配地址,即用于接收传输到分配地址的数据包的组播群组,如虚线所示。资源B根据数据包确定分配地址。因此,并非所有数据包都会发送到节点N1,只有发送到分配地址的数据包才会发送到节点N1。通过订阅分配地址,节点N1接收从资源B传输的数据包的子集,其中所述子集是根据数据包本身确定的。这样,节点N1只接收已发送到分配地址的数据包(例如,数据包)子集的传输。

[0178] 在该示例中,节点N2至N4订阅组播群组来接收任何数据包,而不管发送的数据包是什么,而节点N1关注于接收选择的数据包,所述选择是通过为分配地址订阅组播群组来进行的。然而,实际上,节点N1至N4中的每个节点都可以为不同的分配地址订阅组播群组。例如,资源B可以确定数据包被发送到四个分配地址中的一个分配地址,从而可以根据数据包集确定四个数据包子集,并且节点N1至N4中的每个节点都订阅组播群组来接收相应的子集。

[0179] 通过分配和均衡,数据包的传输至少可以提高效率、实现可扩展性、支持网络资源均衡和抑制瓶颈。此外,分配使得与数据包(例如,每个UTXO和/或事务)相关联的信息的处理、存储和核实中的至少一者能够得到更高效的管理,如PCT/EP2022/080084和PCT/EP2022/080081中所描述和教导的,该申请的全部内容以引入方式并入本文。

[0180] 使用数据包来确定所述数据包所发送到的分配地址中的至少一个分配地址使得数据包在网络中的传播能够得到均衡。可以通过在一定范围内的节点和/或路由器之间分布传播的数据包来实现均衡,这些节点和/或路由器会选择性地订阅分配的组播群组和/或从组播地址接收。如本文所教导的使用分配地址来分布数据包的传播可以与数据核实的分布类似并与之互补,因此,以下申请的全部内容以引入方式并入本文:PCT/EP2022/079825;PCT/EP2022/080084;PCT/EP2022/079830;PCT/EP2022/079447;PCT/EP2022/079837;以及PCT/EP2022/080014。

[0181] 因此,分配地址可以是与接收资源群组(例如,图16的节点N1)相关联的组播地址。作为非限制性示例,数据包可以包括事务(Tx)(例如,区块链事务)的至少一部分。尽管本文所教导的分配方法可以应用于任何数据包,但这些方法特别适用和有益于使用区块链相关数据(例如,区块、区块头等)的区块链相关应用。

[0182] 以包括区块链数据的数据包为例,例如数据包包括UTXO数据,举例来说,所述数据包可以分配给一组八个可分配地址中的一个分配地址。作为非限制性示例,图17(a)示出了八个分配地址,每个分配地址与一个二进制值相对应,其中该二进制值可从数据包中导出。例如,数据包中UTXO数据的二进制值以“110”开头,则该数据包将被发送到分配地址“7”。分配地址的范围是可扩展的,例如,分配地址的总数可以是16、256或1024。因此,每个分配地址可以被分配一定范围的数据包来发送和/或接收、存储和/或维护。

[0183] 比特币节点具有125个输入和8个输出,因此,图18表示一种布置,其中资源B是区块链网络上的节点,通过其专用输出中的每个输出向8个分配地址进行传输,例如,具有数据包的数据包可以被发送到8个节点N1至N8中的一个节点。举例来说,这可以通过图17(a)中的表格来实现。资源B的每个输出可以根据要传输的数据包传输到分配地址,例如传输到分配的组播地址/群组。节点N1至N8订阅相应的分配组播地址。通过订阅分配地址,节点N1

接收从资源B传输的数据包的子集,其中所述数据子集(例如,数据包)是根据数据包本身确定的。以图17(a)为例,节点N1订阅接收具有以“000”开头的二进制值的所有数据包。

[0184] 根据数据包确定分配地址可以包括对其中的数据进行解析。再以UTXO为例,可以检索和/或接收和解析未花费事务输出(UTXO)和/或包含UTXO的事务(Tx)的数据的一部分。解析只是对数据包进行处理以确定将数据包传输到哪个分配地址的一个示例。解析可以由发送资源(例如,图16中的节点B或图5中的资源501)执行。解析完成后,数据包被定向传输到分配地址,以便由组播群组接收。

[0185] 在另一示例中,其中数据包是区块,分配地址可以通过对其中的数据包(例如,通过处理区块头)进行处理来确定。以区块头为例,可以对其进行解析,以确定区块传输到哪个分配地址。解析可以由发送资源(例如,图16中的节点B或图5中的资源501)执行。解析完成后,数据包被定向传输到分配地址。因此,区块的传输会根据数据包本身遍布网络和地址(例如,组播地址)。

[0186] 地址的识别和/或分配可以由节点和/或交换机来执行,例如结合图11至图15所示的节点“N”和路由器“R”所描述的。节点、交换机或路由器在网络中充当所述发送资源和/或接收资源。

[0187] 当确定地址分配时,例如根据数据包确定地址分配,其中包括将被持有的具有UTXO/Tx的数据包,发送资源可以选择性地传输数据包。类似地,网络中的数据接收者可以订阅专用于这些分配地址的组播群组。这样,资源的传输和/或订阅就可以专用于其处理的数据包。如本文所述,数据包根据其中的数据确定分配地址,这些数据可以包括以下各项中的至少一项:UTXO标识符;UTXO脚本的哈希;事务标识(TXID)。

[0188] 发送资源可以持有数据结构,例如查找表,该查找表包括与对应密钥集相关联的分配地址集。可以对数据包进行处理,以确定相关联的密钥。发送资源可以使用所确定的密钥来识别要向其传输数据包的分配地址。接收资源可以使用密钥集来识别和订阅接收发送到组播地址的数据的群组,所述组播地址是与对应密钥集相关联的分配地址。确定分配地址可以包括对数据包进行解析以确定密钥,并使用该密钥从地址集中选择至少一个地址。

[0189] 对数据包进行处理(例如,解析),以提供与数据包传输到的分配地址(例如,组播地址)相对应的密钥。从数据包中导出的密钥可以通过使用数据的一部分直接确定,例如密钥确定分配地址,或通过处理间接确定,例如对数据的一部分进行哈希处理,使得所得哈希确定分配地址。数据、密钥和所得哈希中的至少一者可以包括以下各项中的至少一项:由字母和数字组成的数;以及二进制数。所述数用于根据数据结构确定分配地址。

[0190] 作为非限制性示例,数据包包括数据的一部分,该部分包括未花费事务输出(根据用于给定实现的区块链/协议,在一些实施例中可以是UTXO,但在其他实施例中不是)和/或包含(例如)UTXO的事务(Tx)。事务的输入包括:事务ID,该事务ID引用包含所花费的UTXO的事务;输出索引,例如Vout,该输出索引用于标识引用该事务的UTXO;脚本(例如,scriptSig),该脚本满足施加在输出上的条件,用于对其进行解锁;以及序列号。

[0191] 例如,与输出相关联的某个加密货币的潜在接收者可以验证是否存在双重花费。因此,潜在接收者会订阅以组播地址接收数据的群组,例如图16中的节点N1。节点(例如,图16中的节点B)充当发送资源,在无延迟或中断的情况下尽可能快速、高效地广播事务。因此,节点B直接处理事务,或从第三方接收事务,并使用事务的数据包、来自UTXO的数据的一

部分和/或相关联的事务信息来确定分配地址。该确定可以使用UTXO独有的数据的一部分，从而可以确定密钥，该密钥随后确定相关联的信息可以传输到哪个分配地址。

[0192] 图19表示资源A与资源B交互以建立事务的场景。在接收到事务的数据包后，所述数据包对应于该事务，资源B可以将所述数据包传输到网络中由所述数据包定义的分配地址。这样，网络(例如，区块链网络)就会收到数据包(例如，事务)的通知，从而可以识别错误或问题(例如，双重花费)。

[0193] 以事务标识(TxID)为非限制性示例，TxID通常指十六进制形式，也可以表示为二进制数。图17(a)至图17(d)是示出如何使用数据的一部分来确定分配地址的数据结构，例如表格。该数据部分(例如，TxID)可以直接解析或处理，例如进行哈希处理。在图17(a)中，对TxID进行解析，以便选择二进制形式的TxID的前三位数字作为密钥，并将根据二进制值(例如，与TxID相关联的信息，该TxID具有前三位数字为“101”的二进制数)分配的地址分配到分配地址“6”中进行存储/处理。使用二进制的前三位数字能够确定八个地址中的一个地址，而图17(c)示出了如何从二进制形式的TxID中获取前四位数字来支持16个地址之间的分配，例如，将与以前四位数字为“1011”的二进制数开头的TxID相关联的信息分配到分配地址“12”中进行存储/处理。或者，可以使用TxID的十六进制值，如图17(b)所示，其中单个十六进制值映射到地址，例如，“c”映射到“13”，并且在图17(d)中，为一定范围的十六进制值分配地址，例如，将与以“76”开头的TxID相关联的信息分配到地址“8”。

[0194] 或者，可以对数据的一部分进行处理，例如进行哈希处理，以生成十六进制数或二进制数，因此该数据部分以及随后确定用于识别/分配地址的密钥不限于TxID。

[0195] 从事务或其UTXO中选择的数据部分，或所处理的值(例如，哈希值)是伪随机的。因此，对地址的分配是负载均衡的，即用于确定用于分配地址的密钥的数据部分是伪随机的，并在订阅组播地址的所述多个发送资源和/或群组之间分布处理和/或存储。由此可见，与数据包(例如，事务/UTXO)相关联的信息的传播分布在多个地址中。地址之间的分配均衡可以最大限度地降低一些资源处于空闲状态，而其他资源过载，从而导致性能下降甚至故障的风险。因此，网络的弹性、性能和/或效率有所提高。

[0196] 因此，数据包和其中的数据可以用于(i)确定用于传输的分配地址，然后(ii)为识别群组和/或分配地址和/或与资源(例如，数据库)中的数据相关联的信息提供参考。

[0197] 由此可见，数据包和其中的数据部分从区块链导出，并且确定密钥和对应的分配地址和/或资源，该分配地址和/或资源可以接收和存储与所述数据相关联的信息，即与未花费事务输出(UTXO)和/或包含UTXO的事务(Tx)相关联的信息。

[0198] 数据包可以至少部分地包括以下各项中的至少一项：记录所述事务(Tx)的区块的默克尔树；用于记录所述事务(Tx)的区块的默克尔根；默克尔路径，该默克尔路径能够根据所述事务(Tx)的哈希确定用于记录所述事务(Tx)的区块的默克尔根的值；默克尔证明；区块标识符(block_ID)，该区块标识符与区块链区块相关联；事务标识符(TxID)，该事务标识符与区块链区块内多个区块链事务中的事务(Tx)相关联；区块标识符(block_ID)和事务标识符(TxID)的函数；以及区块标识符(block_ID)和事务标识符(TxID)的级联。

[0199] 发送资源可以包括确定数据包(例如，输出/UTXO)中数据的有效性所需的信息和数据包。附加地或替代地，发送资源可以自己或通过核实者生成核实和/或支持输出/UTXO的核实和/或指示是否存在双重花费的数据包。发送资源可以执行以下操作中的至少一项

操作:核实和/或验证所述UTXO;针对所述UTXO执行简单支付验证(SPV)过程的至少一部分;确认给定区块链事务(Tx)是否包含在区块链区块内;生成区块链事务中的至少一个区块链事务的哈希,使用该哈希构建默克尔路径和/或检查该哈希是否与区块链区块的区块头中的事务标识符(TxID)匹配;以及确定用于所述UTXO的默克尔证明。

[0200] 通过提供一种基于数据包(例如,来自UTXO/事务的数据包)识别分配地址的方法,可以实现传输数据包的改进方式,从而提高效率和可扩展性。

[0201] 已经针对单个数据包对发送资源和/或接收资源进行了描述。附加地或替代地,发送资源和/或接收资源通过订阅可以生成、存储、处理、访问和/或维护包括多个数据包的区块,其中该区块中数据包中的每个数据包包括区块链相关数据。发送资源和/或接收资源可以为区块中的每个数据包确定分配地址。发送资源可以通过电子网络至少部分地将区块中的每个数据包的传输从发送资源发送到相应的分配地址。

[0202] 在将数据包发送到其相应的分配地址时,区块可以分割为子区块,并且发送资源通过电子网络将每个子区块传输到对应分配地址。以图18为例,多个数据包可以分割为八个子区块,每个子区块发送到由N1至N8表示的对应分配地址。举例来说,如图17(a)所示,充当发送资源的节点B可以将以二进制值“000”开头的所有数据包分组(group)到节点N1订阅的分配组播地址。

[0203] 图20示出了资源(节点B)可以是发送资源和接收资源。作为发送资源和/或接收资源的示例,节点B订阅至少一个接收资源和/或至少一个组播群组,如本文结合图8和图9以及对应描述所教导的。从节点C、D和E所表示的资源接收数据包。明确地说,发送资源(例如,节点B)附加地或替代地作为接收资源运行。因此,节点B被配置为接收具有数据包的一个数据包和/或多个数据包。然后,节点B可以将数据包(该数据包可以包括区块链相关数据)中继到分配地址,或将包括多个数据包的区块中继到相应的分配地址。

[0204] 节点B可以附加地或替代地运行,以收集和/或合并从节点C、D和/或E接收的一个数据包、多个数据包和数据包区块中的至少一者。然后,节点B可以将数据包或数据包区块中继到对应的分配地址。在收集一个数据包、多个数据包或区块中的至少一者之后,节点B可以对其中的所述数据包或每个数据包进行解析以确定相应的密钥,并使用该密钥将所述数据包或每个数据包中继到地址集中的至少一个地址,例如将所述数据包或每个数据包或区块中继到节点N1至N8所表示的组播地址。

[0205] 发送资源或接收资源(例如,节点B)订阅充当组播地址的组播群组,该组播地址被配置为接收分配给所述组播地址的至少一个数据包。所述分配可以根据至少一个数据包确定。后续处理(例如,对数据包的解析)可以确定向哪个分配地址传输数据包。

[0206] 节点B可以通过向互联网和/或区块链网络等网络发送信号来订阅接收资源群组。节点B可以离开接收资源群组,优选地,其中资源通过停止向网络发送信号而离开该群组。这样,节点B可以“打开(switch-on)”以将自己分配到群组,随后“关闭(switch-off)”,从而从发送地址取消分配发送资源。响应于确定已经满足预定条件(例如,区块链相关数据被发送到预定数量的接收资源,并且/或者已经过去一定时间,或者达到给定日期和时间等)而执行取消分配。

[0207] 数据包可以包括与区块链相关事件或活动相关的通信或警报,例如来自加密货币群组的成员或有兴趣接收此类通知并已加入该群组的任何一方的通知。警报可以包括区块

链网络中双重花费或双重花费尝试的通知,该通知由组播群组中的挖掘节点或服务提供者等接收节点发出。

[0208] 发送资源和/或接收资源被设置为、被配置为和/或用于执行以下操作中的一项或多项:区块链协议指定的功能;与区块链协议中指定的挖掘或共识函数相关的计算或其他操作;简单支付验证(SPV)操作;计算或验证默克尔路径、默克尔路径的证明或根;在区块链事务写入区块链之前或之后对其进行核实;搜索区块链以识别、定位和/或确认区块链中是否存在给定事务或区块;生成区块链事务、将事务写入区块链和/或向区块链网络广播事务。

[0209] 数据包可以包括以下各项中的至少一项:区块链事务的至少一部分;区块链区块的至少一部分;区块链事务脚本的至少一部分;记录所述数据包的区块的默克尔树;记录所述数据包的区块的默克尔根;默克尔路径,所述默克尔路径能够根据所述数据包的哈希来确定用于记录所述数据包的区块的默克尔根的值;默克尔证明;与区块链网络的共识机制一起使用或相关联的数据;权益证明或工作证明操作的结果或相关数据;区块标识符(block_ID),所述区块标识符与区块链区块相关联;事务标识符(TxID),所述事务标识符与区块链区块内多个区块链事务中的事务(Tx)相关联;区块标识符(block_ID)和事务标识符(TxID)的函数;区块标识符(block_ID)和事务标识符(TxID)的级联;数字签名;认证代码;签名消息,所述签名消息用于确定事务状态;协议标志;自主公钥(discretionary public key,DPK);以及自主事务ID(DTxID)。此类实施例可以利用以下申请中的任何一个或多个申请中公开的一个或多个特征,这些申请的全部内容以引入方式并入本文:PCT/IB2019/059807、PCT/IB2019/059808、PCT/IB2019/059809、PCT/IB2019/059793、PCT/IB2019/059795、PCT/IB2019/059791、PCT/IB2019/059803和PCT/IB2019/060226。

[0210] 发送资源和/或接收资源可以包括以下各项中的至少一项:区块链网络中的节点;被设置为提供区块链相关服务的服务提供者;与金融机构相关联或由金融机构控制的计算资源;加密货币交换所或其组成部分;商家资源或其组成部分;数字钱包或其组成部分;软件组件,所述软件组件用于执行或促进简单支付验证(SPV)操作,或处理SPV操作的结果;网络上的MLDv1主机或MLDv2主机、网络交换机或路由器。

[0211] 出于说明而非限制的目的,现在提供一些示例性用例。

[0212] 受控访问

[0213] 附加地或替代地,除了使用如本文所教导的通过管理和/或分配优化资源的传播和/或均衡的节点和/或路由器来传输数据包外,图21至图23示出了使用接收者之间的交换对数据包的受控访问的示例——示例中的接收者名义上是爱丽丝“A”、查理“C”或戴夫“D”,并且发送资源名义上是鲍勃“B”或查理“C”——所述交换使用组播群组“MG”进行,每个群组具有其自己的相应组播地址。如本文所教导的,发送者、接收者和组播群组可以是网络的一部分(例如,区块链网络中的节点)。

[0214] 在图21中,由鲍勃B或查理C表示的发送资源用于执行生成、存储、处理、访问和/或维护数据包中的至少一者。数据包可以包括区块链相关数据。鲍勃或查理通过电子网络至少部分地将数据包的传输发送到组播群组MG1、MG2。鲍勃表示数据包起源的节点。

[0215] 组播群组将数据包提供给最终用户(名义上是爱丽丝A)。爱丽丝可以被描述为数据包的消费者(例如,最终用户)。然而,查理还可以访问和/或订阅组播群组MG1,并将所述

数据包直接或通过另一组播群组MG2提供给最终用户爱丽丝。

[0216] 在一个或多个实施例中,可以通过执行与区块链相关联地执行的智能合约来控制对组播群组的访问(以及因此发送到群组的订阅者的数据)。这可以是以太坊区块、比特币区块链或通过任何其他区块链协议实现的区块链。例如,希望加入群组的用户可能需要满足智能合约中指定的一个或多个条件,并且在成功满足该一个或多个条件后,他们可能会被提供必要的信息,以便能够订阅群组并开始从组播流接收数据包。例如,可以为用户提供使得他们能够加入群组的密钥或令牌(token)或其他资源。这些条件可以包括任何合适的条件,例如支付加入费用,或者提供身份相关数据以验证用户的身份等。同一或其他智能合约可以控制用户对组播群组的持续访问以及向组播群组/通过组播群组传播的数据包。例如,智能合约可能要求用户支付费用、更新其身份验证文档或定期执行一些其他动作。

[0217] 图21中指示了哈希线,以指示鲍勃与爱丽丝之间(即,通过查理)的数据包的可选传输。虽然爱丽丝可以从MG1获得数据包,但是所述数据可以是例如多媒体数据的实时传输(例如,足球比赛)。爱丽丝可能无法观看直播,因此查理C等中间方也订阅从MG1接收并存储数据包,以独立于鲍勃的传输将数据包提供给爱丽丝。查理可以在与原始传输不同的时间直接或通过其他组播群组MG2向爱丽丝传输数据包。

[0218] 在一个示例中,鲍勃作为节点操作并向组播地址(例如,MG1)传输数据包。传输可以至少部分地包括区块头以及一个或多个区块链事务和/或区块链事务标识符(TxID)的列表。组播地址(例如,IPv6组播地址)由多个接收节点(可以包括爱丽丝和查理)订阅。所述节点或每个节点可以是区块链网络上的节点,即发送节点和/或接收节点中的至少一个接收节点。

[0219] 结合中间方查理,发送资源或节点可以附加地充当接收资源或节点,其可以执行以下操作中的至少一项操作:发送、存储、处理、访问和/或维护数据包。

[0220] 数据包直接传输到组播群组MG1并间接传输到组播群组MG2,并且数据包的消费者和/或最终用户可以通过订阅组播群组来获得所述数据包。

[0221] 根据本文的教导和附图,很明显的是,发送资源(例如,节点或路由器)可以传输多个数据包,并且/或者接收资源(例如,节点)可以接收多个数据包。作为非限制性示例,数据包可以是多媒体数据,并且至少部分是数据流,例如多媒体通信信道。

[0222] 多媒体数据可以是例如足球比赛或其子部分。虽然足球比赛可以通过包括视频和音频组合的单个信道传输,但是该足球比赛的镜头可以以多个部分提供,其中一个或多个部分通过不同的信道传输。例如,可以提供多个视频流,每个流由不同的信道支持。例如,这些部分可以包括不同的摄像机角度、球门线摄像机视图、不同语言的音频评论、重播等。这些信道中的每个信道可以在不同的数据包中传输到相应组播群组。

[0223] 使用图22,举例来说,节点B以六个不同流向相应组播群组MGa至MGf传输数据包,所述数据包包括用于现场足球比赛的多媒体数据。群组MGa和MGb接收包括视觉摄像机角度数据在内的数据包,前者跟踪比赛进程,后者显示独家球门线活动。群组MGc和MGd接收数据包,所述数据包包括不同语言的评论,前者采用英语,后者采用德语。群组MGe和MGf接收可选附加内容的数据包,前者提供独家重播动作,后者提供来自裁判安装的随身摄像机的镜头。

[0224] 在比赛期间,爱丽丝通过访问组播群组MGa和MGc来流式传输对抗赛和英语评论。

同时,可选地,节点C处的查理访问并捕获来自所有组播群组MGa至MGf的数据包。所捕获的数据由节点C处的查理收集和/或聚合,并通过组播群组MGm单独且独立地提供,其中MGm将从节点B传输的所有数据包提供给组播群组MGa至MGf,从而按需提供所有匹配信息、语言和摄像机视图。爱丽丝可以访问群组MGm以再次观看一个或多个数据包中包含的对抗赛,也可以访问附加信息。查理等中间方可以操作以合并(例如,池化)来自一个或多个组播群组的数据包,以便随后传输到另一组播群组。

[0225] 发送资源(例如,节点B)可以发送多个数据包。附加地或替代地,数据包可以具有提供多个数据信道的子组件。数据包可以是可分离的,以便根据(i)信道的功能(如上文关于足球比赛的不同方面的示例中所描述的)和/或(ii)基于数据包本身(如条款9和相关联的描述中所描述的)独立地传输到组播群组。

[0226] 本文的教导不限于足球比赛,并且通过其他示例,数据包的传输可以应用于:送货司机,其中控制室发送与送货车辆可以选择性地接收的送货地址、行程、交通信息、天气信息等相关的数据包;无人机的操作和/或协调;仓库及其货物的管理;以及订阅媒体服务,例如Netflix™或Sky™电视。

[0227] 一个或多个数据包和/或组播群组可以通过访问密钥来保护(例如,加密或以其他方式锁定),其中该访问密钥必须在订阅组播群组期间应用和/或在数据包上使用以访问其中的内容。可能需要单独的访问密钥来访问不同的组播群组和/或数据包。例如,可能需要第一访问密钥来访问数据包,而可能需要第二访问密钥来例如通过订阅访问组播群组。

[0228] 发送资源可以通过保护对组播群组的访问和/或保护数据来确定访问数据包是否需要访问密钥。发送资源可以管理对组播群组的访问,例如管理订阅,这需要访问密钥。在示例中,鲍勃B和查理C正在发送资源,并且各自可以分别管理对他们传输的数据包的保护和/或对他们传输到的组播群组的访问。爱丽丝可以通过订阅提供用于加入和接收来自组播群组的数据包的访问密钥的服务来访问数据包。附加地或替代地,爱丽丝可以获得访问密钥或订阅提供访问密钥的服务,从而使得爱丽丝能够解锁受保护的数据包。

[0229] 组播群组的发送资源和/或管理者可以生成以下各方所需的访问密钥:中间方(例如,查理C),其充当聚合者并池化数据包以供最终用户(例如,爱丽丝)随后访问;和/或最终用户(例如,订阅者爱丽丝A)。在一个示例中,访问密钥被提供给查理和爱丽丝。

[0230] 访问密钥可以由中间方或最终用户(例如,传统交换(即,提供访问密钥以换取支付)中的聚合者或最终用户)获得。根据本文的教导,至少使用区块链相关数据和区块链网络上的节点之间的交互以及区块链事务,随后通过支付通道向中间方或最终用户提供至少一个访问密钥,该支付通道可以通过以下链接获知:https://wiki.bitcoinsv.io/index.php/Payment_Channels。

[0231] 使用支付通道,可以使用区块链事务来快速且高效地交换至少一个访问密钥以进行支付。在实践中,中间方或最终用户可以使用和/或建立支付通道来获得一组访问密钥。支付通道以及密钥提供可以由数据的发起者或第三方服务提供者处理。

[0232] 使用访问密钥来高效访问安全数据包得益于使用支付通道,其中使用每个密钥来订阅和/或解锁数据包可以触发对例如发送资源的自动支付,其中发送资源是数据包的来源。访问密钥可以针对以下各项中的至少一项来提供对组播群组和/或数据包的访问:(i)固定时间段;(ii)固定数量的数据;(iii)固定数量的单元;(iv)固定数量的数据包;以及

(v)无限制访问。

[0233] 发送资源(例如,鲍勃或查理)可以向多个组播群组传输数据包。IPv6协议以及区块链应用的范围使得传输的数据包量可能很大,所述数据包被传输到同样大量的组播群组。虽然这可以采用可扩展和粒度的方式来传播数据包,但是可以缓解瓶颈并均衡资源使用。

[0234] 除了本文所教导的传输和/或订阅和/或访问技术之外,发送资源还可以将数据包分配到组播地址,其中所述组播地址是根据以下各项中的至少一项确定的:数据包;以及访问密钥。

[0235] 与枚举条款集9和本文其他地方的特征和实施例相关的分配技术可以应用于补充使用IPv6来传输数据的高效且可扩展的方案,如本文所教导的。均衡可以抑制数据包的传输中的瓶颈,特别是当数据包是大区块时,这可能会导致节点或路由器处出现延迟,或者当数据包是事务并且事务量以普遍方式传播而使网络泛洪时。

[0236] 附加地或替代地,本文的教导适用于接收资源,例如最终用户或聚合者,例如爱丽丝A或查理C,其可以存储、处理、访问和/或维护数据包,所述数据包优选地包括区块链相关数据。接收资源至少部分地通过从电子网络接收数据包的组播群组接收数据包的传输。数据包由最终用户(例如,爱丽丝)和/或聚合者(例如,查理)消费。如上所述,爱丽丝和/或查理可以使用访问密钥来访问安全的数据包,其中数据包和/或对组播群组的访问是安全的并且可使用访问密钥访问。访问密钥可以通过与数据包的发起者、发送资源和组播群组中的至少一者建立的支付通道来获得。

[0237] 图21示出了发送资源(例如,由节点B表示的鲍勃)如何将数据包传输到八个不同的组播群组(名义上是MGa至MGh)的又一示例。鲍勃充当区块链节点,因此存在八个输出。可以基于正在传输的数据包将数据包传输到相应组播群组,所述数据包用于确定分配地址(即,组播群组)。举例来说,可以使用本文条款9的教导和图17(a)的数据表来实现分配的确定。

[0238] 或者,可以使用访问密钥和/或数据包的内容来确定分配。例如,组播群组(名义上是MGa至MGh)可以持有与地理位置相关联的数据,该数据是从来自节点B(发送资源鲍勃)的传输中接收的。每个地理位置可以具有自己的访问密钥,该访问密钥可以通过订阅获得。

[0239] 在一个示例中,发送资源传输数据包(例如,与具有八个区的城市相关联的地图和交通信息)。以类似无人机的方式运行的六辆自动驾驶车辆(例如,出租车)被标记为D1至D6,需要在城市内运输货物或乘客。

[0240] 作为出租车运行的每架无人机(D1至D6)确定其给定行程的起点和终点,以及需要行驶经过的区。然后,无人机从与这些区相关联的组播群组中访问与这些区相关联的对应数据包(例如,通过订阅)。

[0241] 每个区和/或无人机可以获得许可。因此,对于在一个或多个区内运行的无人机,需要获得每个区的许可证,所述许可证提供与关联于许可区的数据包相对应的访问密钥。替代地或附加地,每个无人机可以通过订阅所需的组播群组来获得许可证和对应的访问密钥,从所需的组播群组可以获得所需的许可证、地图和交通数据。可以在需要时进行订阅,并根据需要“开启”或“关闭”。订阅组播群组以获得许可区的数据包可以是基于时间的、基于单元的等。

[0242] 在图23的示例中,无人机D1、D2、D4和D5在同一区内启动和停止,并且开启以分别接收或以其他方式订阅组播群组MGa和MGb。然而,无人机D3穿越三个区并访问与区MGa、MGb和MGc相关的数据包。相比之下,无人机D6穿越六个区并访问与区MGc至MGh相关的数据包。在正常运行期间,无人机D6只能在MGc支持的区运行,并且需要按需前往其他区。因此,无人机D6可以每年订阅组播群组MGc和/或其提供的数据的访问密钥,同时在其他区行驶时根据需要订阅其他组播群组。

[0243] 总体而言,图21至图23以及非限制性示例教导了关于受控传输、传播和/或访问数据包的方法和相关联的系统要求。数据包可以包括多媒体内容、地图数据或类似内容等信息。访问可以通过订阅来实现,这些订阅可以使用例如区块链节点和区块链网络支持的支付通道来支付。示例性应用程序可以是“按次支付”或“按使用支付”服务。实施例可以特别用于其中需要对从来源流式传输到多个潜在数据消费者的数据进行增强控制的应用。

[0244] 因此,本文提供的一些示例涉及使用节点和/或路由器来传输数据包,所述节点和/或所述路由器通过管理和/或分配来优化资源的传播和/或均衡,如条款中概述。具体地,示例涉及对这些数据包的受控传输和/或访问。更具体地,提供了合约访问(例如,对所述数据包的支付)。根据一个可能的方面,本发明可以涉及一种计算机实现的方法,所述方法包括操作用于生成、存储、处理、访问和/或维护数据包的发送资源,所述数据包优选地包括区块链相关数据。所述发送资源可以是所述数据包的发起者(例如,创建者或生产者);或者所述发送资源可以是运营者,例如,整理、聚合或池化数据包以供后续传输(例如,独立于所述数据的原始传输或创建)的分发者。所述发送资源可以(通过电子网络)至少部分地将所述数据包的传输从所述发送资源发送到组播群组。所述组播群组使得所述数据包可供最终用户使用(由其访问)。

[0245] 可以发送和/或接收多个数据包。例如,电影不是以大数据包的形式传输,而是可以分为多个部分,每个部分作为单个数据包发送。所述数据包可以至少部分是数据流,例如多媒体通信信道。所述数据包可以具有用于提供多个数据信道的子组件。

[0246] 所述最终用户通常可以是通过所述组播群组访问所述数据包的消费者,例如,他们是订阅者。组播群组和/或数据包可以是安全的,并且接收者(例如,最终用户)可以进行支付以获得用于访问所述组播群组和/或所述数据包的访问密钥。可以提供多个访问密钥。可能需要第一访问密钥来访问所述数据包。可能需要第二访问密钥来访问所述组播群组。

[0247] 所述发送资源可以生成所述访问密钥。所述发送资源可以将所需要的访问密钥发送到所述数据包的接收者和最终用户中的至少一者以访问所述数据包。所述访问密钥可以在使用支付通道的交换期间提供。附加地或替代地,在一些实施例中,可以结合使用智能合约与区块链,以控制所述用户对所述组播群组的初始和/或持续访问。当与所述区块链相关联地执行时,所述智能合约可能需要所述用户满足一个或多个条件才能订阅所述群组以及/或者继续成为所述群组的成员。

[0248] 所述访问密钥可以被配置为提供对所述数据包的访问,以及/或者同时表示对使用数字锁保护的数字资产或物理资产的许可和/或访问。所述访问密钥可以针对以下各项中的至少一项来提供对所述组播群组和/或所述数据包的访问:(i)固定时间段;(ii)固定数量的数据;(iii)固定数量的单元;(iv)固定数量的数据包;以及(v)无限制访问。

[0249] 在另一示例中,一种计算机实现的方法包括操作用于存储、处理、访问和/或维护

数据包的接收资源,所述数据包优选地包括区块链相关数据。所述方法还包括通过从电子网络接收数据包的组播群组至少部分地接收所述数据包的传输,并作为最终用户消费所述数据包。可以保护所述数据包和/或对所述组播群组的访问。所述接收资源可以使用访问密钥来获得访问权限。所述访问密钥可以通过支付通道获得。

[0250] 所述数据包可以包括以下各项中的至少一项:事务(transaction,Tx)的一部分;输出(例如,UTXO)标识符;脚本(例如,与事务中的输出相关联的脚本)的哈希;事务标识符(TXID);区块链区块;和/或区块头。

[0251] 示例性用例1:双重花费警报和"先见规则"、网络通知等网络通信:

[0252] 众所周知,通过所有类型的电子网络实现的通信都会带来各种重大技术挑战。特别是在区块链相关网络方面,可能还需要尽可能迅速、高效地将信息和数据传播给可能需要根据这些信息/数据采取动作的至少一个目标接收者集或子集。本公开的某些实施例可以使用IPv6组播通信来实现或至少促进向接收资源集分发数据/信息的目标,所述接收资源是本文所教导的组播群组的订阅者。

[0253] 所述组播通信可以是:

[0254] ●警报:例如,某件事情可能发生或可能未发生,或已经识别出对网络/群组的至少一部分有害或以其他方式与之相关的风险或潜在事件的警告;接收者可能需要采取响应动作;响应动作的必要性可以在警报中指明,或以其他某种方式告知接收者;例如,响应动作可以是应用安全修复、软件升级或禁止处理/花费/转移加密货币的一部分;

[0255] ●通知:例如,信息性消息;例如,更新可供下载,事件可能/将要/已经发生;或者可能与接收者相关的任何其他新闻;

[0256] ●指令或触发:例如,消息可以包括可执行代码或数据,该可执行代码或数据使至少一个接收者响应于所述指令/触发采取至少一个动作。这样,所述组播通信可以控制、指导或影响一个或多个接收者的行为。

[0257] 将使用术语"通信"来包括但不限于这些示例,并且包括(但不限于)术语"警报"、"通知"、"指令"、"更新"和/或"触发"。

[0258] 本公开的实施例在通过互联网等电子网络传输通信时可以发挥其优势,以便感兴趣的各方或可能感兴趣的各方可以接收这些通信所包含的数据/信息。根据这些示例性用例,实施例可以包括基本上如本文提供的列举条款(尤其是条款集11)所述的特征。

[0259] 在一些实施例中,可能与通信包括发送资源希望或需要共享的区块链协议级信息/数据的场景有关,组播群组的订阅者可能仅限于某些类型或形式的接收资源。例如,在一些实施例中,所述接收资源可以是全节点,例如区块链网络上的矿工。附加地或替代地,所述接收资源可以包括非挖掘节点。在其他示例中,所述接收资源中的一个或多个接收资源和/或所述发送资源可以是车辆或无人机,所述车辆或无人机可以是自主的、半自主的或由操作人员操作的。以下示例并非旨在具有排他性或详尽无遗,这些示例的特征可以单独使用,或相互结合使用。

[0260] 使用IPv6组播实现加密货币警报密钥

[0261] 在一个示例中,实施例可以使用IPv6组播通信来实现用于向网络上的实体传播关键、紧急或必要通信的警报密钥机制。本公开的实施例呈现了向区块链网络上的节点等相关方传播加密货币相关通信(例如,警报和通知)的优势。根据本公开,可以实现一种区块

链/加密货币警报系统,其中可以通过IPv6组播通信向网络上的全部或部分节点/接收资源广播网络相关数据。所述警报可以包括与例如以下各项中的至少一项相关的数据:安全补丁、与潜在安全漏洞相关的修复或更新、区块链协议的更新版本、软件更新、加密货币双重花费尝试、法律(法院命令)禁令、限制或命令、警报密钥的访问码等。对特定区块链网络/协议感兴趣的各方可以订阅为向此类各方传送相关信息而设立的组播群组。

[0262] 所述警报可以触发或要求所述警报的至少一个接收者做出响应。例如,所述响应可以包括以下各项中的一项或多项:

[0263] ●"冻结"或暂时/永久禁止处理至少一个区块、事务或事务输出;例如,这可以包括禁止花费加密货币或未花费输出的一部分,或核实一个或多个(区块链)事务,或将一个或多个事务包括在区块中,以便可能包括在分布式账本中;冻结/禁止动作可以包括将数据的一部分(例如,事务或区块的至少一部分)标记或识别为无效、不可花费、拒绝或予以忽略;

[0264] ●将警报从所述至少一个接收者转发(即,向前传输)到至少另一接收者;所述至少另一接收资源可以包括至少另一IPv6组播地址;这使得能够将通信从一个组播群组发送到一个或多个其他组播群组,从而为时限更新、通知、警告或安全补丁和解决方案等数据的传播提供快速、高效的机制;

[0265] ●将代码或数据的一部分下载、访问、安装和/或执行到所述接收资源或一个或多个其他资源;例如,所述代码或数据可以与以下各项中的至少一项相关:安全补丁、与潜在安全漏洞相关的修复或更新、区块链协议的更新版本、软件更新、加密货币双重花费尝试、法律(法院命令)禁令、限制或命令。

[0266] 使用代码、标志、标记或其他标识符来过滤传输到网络的IPv6通信

[0267] 在另一示例性实施例中,通信可以包括代码、标志、标记或充当过滤器的其他标识符。

[0268] 所述过滤器可以设置在通信中预先指定的位置和/或以预定格式设置,使得所述接收资源中的至少一个或一些接收资源能够识别、了解所述过滤器和/或根据所述过滤器采取动作。在一些实施例中,所述过滤器可以设置在IPv6数据包(数据包头部)的控制信息中或用户数据的有效载荷中。在一些实施例中,所述过滤器可以是十六进制代码或二进制代码,并且可以与预定信号、状态或意义相关联,或指示预定信号、状态或意义。附加地或替代地,所述过滤器可以与预期接收者的类型相关联,或指示预期接收者的类型。因此,所述过滤器可以作为一种如下手段:根据以下各项来使通信针对特定的接收者或接收者群组/子集:正在发送的通信的内容/类型;和/或预期或期望的接收资源集。

[0269] 例如,假设发送资源向已订阅特定IPv6组播地址的接收资源群组发送通信,其中该IPv6组播地址是为传播与特定区块链网络相关的消息而设置的。一些订阅者可能是区块链网络上的全(挖掘)节点,而其他订阅者可能只是代表第三方使用区块链来执行区块链相关活动(例如,区块核实、SPV和钱包相关服务等)的服务提供者。现在假设所述发送资源已经意识到可能影响整个区块链网络以及使用区块链网络并与之交互的所有各方的恶意活动。所述发送资源希望提醒所有订阅者,因为他们对该区块链感兴趣。因此,所述发送资源可以生成IPv6组播通信并将其发送到群组地址,其中与所述恶意活动相关的信息和/或指令包含在IPv6数据包的有效载荷部分中。所述数据包还可以包含表明该消息是为了引起所

有订阅者注意的标志。因此,每个订阅接口都会检测发送到所述群组地址的数据包,并对其进行处理。可以响应于通信中传达的信息而采取响应动作,例如忽略特定的事务区块或将输出指定为已花费。

[0270] 然而,在另一场景中,所述发送资源可能希望发送仅与订阅资源的子集相关的通信。例如,如果出现协议更新或检测到安全漏洞,挖掘节点可能需要安装软件更新。此类更新可能与不在网络上作为全节点运行的其他订阅者无关,因此对于他们来说,接收和处理他们不需要采取行动的通信是低效的。因此,为了提高网络通信的效率和安全性,所述发送资源可以在通信中加入过滤器,指示该通信只与某些成员相关。成员在看到IPv6数据包时,可以检查过滤器。如果过滤器指示该数据包只与全节点相关,则全节点成员将相应地对此进行解释,对数据包中的数据进行处理,并采取一个或多个适当的动作过程,例如安装更新。然而,非挖掘节点会忽略该数据包,因为过滤器已标记出内容与他们无关。这为群组成员节省了能量、资源和时间。

[0271] 此外,此类标志机制使得能够针对特定的成员子群组进行不同类型的通信,从而为整个区块链相关成员群组提供改进的电子通信解决方案。此外,由于过滤器机制可以为一个或多个组播群组的不同成员提供复杂且结构化的形式,选择性地针对不同类型的通信作为目标,因此能够生成和传输分层的通信和警报。

[0272] 在一个优选实施例中,出于隐私和安全目的,通信中的部分或全部数据可以加密或以其他方式加以保护。因此,敏感信息或仅用于特定接收者的信息可以得到保护。例如,IPv6数据包的有效载荷中的数据可以使用加密密钥进行加密,或进行屏蔽,或使用某种其他安全机制或算法进行编码。可以向授权接收者提供对受保护数据进行解锁(例如,解码)的方法,以便接收者可以在适当情况下读取和使用这些数据。例如,解锁机制可以是密钥、访问码或接收者已知的某种秘密。解锁机制可以由通信生成者/发送者或与之相关联或代表其行事的可信方提供给授权接收者。

[0273] 附加地或替代地,通信的至少一部分可以以某种方式进行标记,使得接收者可以确信该通信是从特定实体或代表特定实体生成和/或发送的。该接收者可能知道该实体是通信和数据的合法或授权来源。在一些示例中,可以通过使用已知属于合法实体的秘密或私钥对通信的至少一部分进行签名来证明通信的真实性。在其他示例中,通信可以包括水印、秘密代码、隐写术或消息,接收者可以使用这些信息来验证通信是从合法来源发送的或代表合法来源发送的。

[0274] “先见规则”和双重花费

[0275] 中本聪白皮书“比特币:一种点对点的电子现金系统”引入了有关比特币网络上事务和区块的“先见规则”的概念。根据该规则,当挖掘节点根据协议评估区块时,它将首先看到的区块视为的第一有效区块,该的第一有效区块被广播到网络并且距离有效链中的创世区块最远。这对于避免“双重花费”场景至关重要。

[0276] 正如比特币SV维基(https://wiki.bitcoinsv.io/index.php/First_seen_rule)所解释的:

[0277] “当两个区块在孤块竞赛中竞争,并且一个节点试图在其中一个区块的基础上进行构建时,如果在竞争对手上发现了新区块,则该节点将停止处理它首先看到的区块并移至最长的链。当接收事务时,应用先见规则来确定哪一个事务在双重花费的情况下是有效

的。当节点检测到双重花费时,该节点总是将其首先接收到的事务视为该硬币的有效花费者。

[0278] 该规则已经进一步扩展,以添加所发现的包括双重花费事务的任何区块,这些区块也应被视为无效,并且该节点应继续对其进行挖掘,除非在该区块顶部发现第二区块,这表明大多数网络已经确定另一事务是首次看到的事务。”

[0279] 因此,尽快将通信传输到网络至关重要。为了在整个网络中完全分发信息,必须在节点之间进行的每“跳hop”都会花费时间,因此网络的安全性会降低。目前,此类通信是使用单播传输在网络中发送的,这意味着每个消息都有一个发送者和一个接收者,当信息在节点之间中继时需要多跳。

[0280] 然而,根据本公开,双重花费(或尝试/可能的双重花费)的通知等通信可以发送到组播群组中的挖掘节点,使得所有相关节点同时尽可能快地接收警报,并且可以采取必要的补救动作。当消息从一个节点中继到另一节点时,没有“跳”。相反,已加入组播群组的每个节点都在侦听订阅流,并将自行接收消息。因此,此类实施例在网络通信和警报的处理、时间和安全性方面都有所改进。

[0281] 在其他示例性应用中,组播群组可以包括不是网络上的矿工或全节点的成员,但需要共享区块链相关信息(例如,事务、区块或区块的各部分)。例如,这些成员中的一个、部分或全部成员可以是希望发送、接收或以其他方式处理区块链事务的商家或其他方。在一些情况下,商家可能希望对事务执行SPV验证,并且需要共享有关默克尔路径和区块头的信息以用于SPV验证。区块发现创建哈希头或区块头。这些被发送到所有SPV节点。使用组播可以以近乎即时的通信方式传递该数据。

[0282] 在另一示例中,发送资源可以是数字货币的来源(例如,中央银行),并且接收者可以是处理该数字货币的银行或其他金融机构。例如,中央银行可以发行中央银行数字货币(CBDC)。就传统现金而言,铸币来源通过车辆运输来将实物纸币和硬币分发到各个银行。就数字现金而言,该分发可以通过组播群组来处理,其中群组的成员是中央银行希望将资金分发到的银行。

[0283] 示例性用例2:分布式区块链功能:

[0284] 实施例可以用于任何类型的数据,并且发送资源和/或接收资源可以被设置为或用于执行任何类型的功能。在一个非限制性示例中,可以将基本上如国际专利申请PCT/EP2023/051529中所描述的与默克尔挑战相关的数据发送到组播群组。在此类场景中,假定资源希望将文件或其他资源的存储委托给多个存储提供者,因此发送资源生成表示该文件的各段的默克尔树,然后将该文件发送给一个或多个存储提供者。随后,当发送资源希望确认存储提供者仍然拥有关于发送资源已经被发送的数据的未更改副本时,发送者以特定方式更改数据,重新计算树的默克尔根,并要求存储提供者对其副本进行相同的更改并发回重新计算的默克尔根。资源可以快速确认存储提供者是否能够提供预期的默克尔根。如果发送回的默克尔根与资源期望的不匹配,则存储提供者的副本一定以某种方式受到损害或更改。当与本公开结合使用时,资源可以将文件的单独部分发送到不同的存储提供者,这些存储提供者中的每个存储提供者都是给定组播群组的成员。当需要确认文件的完整性,或者需要重新组装组成部分时,资源将通过轮询群组来请求该操作。

[0285] 在另一示例性用例中,发送到组播群组的数据是区块链相关数据,因为它构成区

块链事务或事务区块的至少一部分、锁定脚本或解锁脚本的至少一部分,或者包括与默克尔证明/路径相关的数据,或用于实现共识机制的数据(例如,PoW或PoS相关数据)。默克尔证明数据可以包括与区块链事务相关的数据以及用于证明(或核实)事务包含在特定区块中的数据。默克尔证明及其用于验证区块中事务的用途以及简单支付验证(SPV)等相关技术是本领域已知的。区块链相关数据的其他非限制性示例可以包括与区块链网络的共识机制一起使用或相关联的数据。例如,这可以是与工作证明(PoW)计算或某个其他区块链共识机制相关的数据。在一个示例中,这可以是与PoW计算相关的数据,例如英国专利申请号GB2206634.4中所描述的数据。

[0286] 当用于区块链相关目的时,群组中的至少一个接收资源可以被设置为、被配置为和/或用于执行以下操作中的一项或多项操作:

[0287] 区块链协议指定和/或要求/需要的功能;

[0288] 与区块链协议中指定的挖掘或共识函数相关的计算或其他操作;

[0289] 简单支付验证(SPV)操作;

[0290] 在区块链事务写入区块链之前或之后对其进行核实;

[0291] 搜索区块链,以识别、定位和/或确认区块链中是否存在给定事务或区块;

[0292] 生成区块链事务,将事务提交到区块链,以及/或者向区块链网络广播事务。

[0293] 示例性用例3:解决数据包丢失

[0294] 在其他示例中,组播群组的成员可以有利地使用组播、任播和单播传输的组合来确保或实现来自发送资源的数据的不完整接收。考虑这样一种场景,其中发送资源希望向组播群组的所有成员发送数据的一部分,但是群组的接收成员未能接收所有传输的数据。这在网络通信中是一个相当常见的挑战(请参见https://en.wikipedia.org/wiki/Packet_loss)。

[0295] 例如,假设包括10个数据包的组播传输被发送到组播群组,但是特定群组成员(将其称为接收资源)仅接收到所发送的10个数据包中的8个数据包。接收资源丢失数据包2和7。接收资源可以通过使用任播传输向组播群组的最近成员请求丢失的数据包来获得丢失的数据包。由于数据传输被发送到组播群组,因此接收资源知道其他群组成员都已接收到数据传输。

[0296] 该方案可以使用以下方法来执行,该方法包括以下步骤:

[0297] 1.使用组播传输将数据的一部分(例如,包括于多个数据包)从发送资源发送到与组播地址相关联的资源群组;

[0298] 2.在资源群组内的资源处确定该资源尚未接收到数据的完整部分;

[0299] 3.从该资源向组播群组的最近的其他成员发送任播传输,请求该资源尚未接收到的丢失的数据子部分(数据包);以及/或者

[0300] 4.在该资源处从组播群组的最近的其他成员接收丢失的(丢弃的)数据子部分。丢失的数据子部分可以通过任何合适的方法(例如,单播)从最近的其他成员提供给资源。

[0301] 这为如何解决或应对数据包丢失的技术问题提供了方案。结合使用对最近成员的任播请求和提供丢弃的数据的单播响应来恢复丢弃的数据包,通过组播使用初始传输,从而提供一种高效且快速的方法。与其他用例示例和实施例一样,该技术可以与任何类型的数据一起利用,并且可以由任何类型的资源利用,包括但不限于区块链相关数据/资源。

[0302] 示例性用例4:利用分配地址实现高效且具有成本效益的均衡分布。

[0303] 在另一示例中,使用本文的教导,如图16至图20所示,名义上称为“鲍勃”的资源B作为节点(例如,节点B)在网络(例如,结合图5所示和所述的区块链网络)上运行。鲍勃通过网络转发或路由数据、数据包或其他此类数据包。鲍勃可以使用组播、任播和单播传输的任意组合进行通信。鲍勃还可以订阅被配置为从至少一个组播地址接收通信的组播群组。鲍勃或本文中的任何资源还可以使用WO2017/145016(其全部内容均并入本文)的教导以对等方式安全地与网络上的任何其他人进行通信。

[0304] 鲍勃试图确保对区块链网络等网络的稳定性至关重要的信息在网络中高效、无延迟地进行通信。重要信息的示例可以是新事务——在网络上共享事务细节对于抑制双重花费非常重要。由此可见,鲍勃可以与网络共享其生成的任何事务和/或接收的事务,例如从爱丽丝接收的事务。

[0305] 鲍勃不限于共享其生成的或从爱丽丝接收的事务的细节,还可以共享从网络接收的任何数据包或数据区块。在鲍勃是区块链节点的示例中,鲍勃将有125个输入和8个输出。因此,鲍勃可以订阅从多个源(例如,组播地址)接收数据,并向多个地址(例如,组播地址)传输数据。作为非限制性示例,接收和传输的数据可以包括本文条款9.16所列的数据的数据包。然而,一个示例使用事务的传输,并且可选地,使用与事务相关联的数据进行核实(例如,使用默克尔证明的SPV)。

[0306] 通过网络传输数据记录或数据区块等数据包需要时间来传播。通过订阅组播地址或群组向组播地址传输和/或接收数据包可改进传输。然而,为了最大限度地减少传播延迟和/或瓶颈,可以将数据包集(例如,数据包)划分为子集,每个子集分配到不同的地址(例如,组播地址)。举例来说,区块可以根据其中的数据包或区块属性进行传播,该数据包或区块属性决定了分配地址(例如,该区块所传输到的分配组播群组地址)。附加地或替代地,该区块可以划分为几个部分,其中的数据包根据为其中的数据包中的每个数据包确定的“密钥”进行分割和单独传输。

[0307] 通过将数据包子集分配到某个地址,可以通过抑制瓶颈以及整个网络的负载均衡来提高传输效率。分配是根据数据包本身确定的,以从爱丽丝接收的事务为例,鲍勃可以处理爱丽丝的事务并将其传输到分配地址。可以对爱丽丝的事务进行解析和/或哈希处理以生成密钥。该密钥可以从事务数据或哈希的二进制值或十六进制值中导出,并且该密钥可以与分配地址相对应,如结合图17(a)至图17(d)所示和所述。

[0308] 因此,鲍勃充当了通过网络传输的数据包的来源。鲍勃可以是数据包的发起者,或者可以直接从爱丽丝接收事务等数据包。鲍勃不是通过网络随机传输数据包,而是对数据包进行处理以确定将传输发送到哪个分配地址。

[0309] 此外,鲍勃可以合并数据包并分区块传输到分配地址,所述分配地址是根据数据包确定的,所述记录可以根据用于确定分配地址的“密钥”进行分组。

[0310] 虽然鲍勃可以生成事务,或从爱丽丝接收事务,但鲍勃也可以从网络中的其他节点接收数据包。在接收到数据包或数据包区块之后,鲍勃可以执行以下操作中的至少一项操作:

[0311] i.合并发送到分配地址(例如,鲍勃订阅的组播地址)的数据包,并将这些数据包传输到对应的分配地址;

[0312] ii.合并发送到分配地址(例如,鲍勃订阅的组播地址)的数据包,对其中的数据包进行处理(例如,解析),以便为对应数据包中的每个数据包确定分配地址,并将这些数据包单独或分区块传输到相应的分配地址,所述区块持有共享同一分配地址的数据包;以及

[0313] iii.接收发送到分配地址(例如,鲍勃订阅的组播地址)的数据包,对其中的数据包进行处理(例如,解析),以便为对应数据包中的每个数据包确定分配地址,并将这些数据包单独或分区块传输到相应的分配地址,所述区块持有共享同一分配地址的数据包。

[0314] 鲍勃可以通过向网络发送信号或停止向网络发送信号来"打开"和"关闭"对接收资源群组的订阅。这样,鲍勃可以根据以下各项中的至少一项来调节接收和/或传输的数据包量:其容量;时间窗口;合同期;网络容量和传输水平,例如数据包是否在阈值时间段内达到阈值节点数。

[0315] 列举条款

[0316] 现在提供列举条款是为了说明可以根据本公开提供的一些可能的实施例。下面提供的条款集仅用于说明,不应被解释为限制性、排他性或详尽的。一个条款集中叙述的特征可以被利用并合并到其他条款集中的一个或多个条款集中。在以下条款集中的任何一个或多个条款集中,实施例可以提供计算机实现的方法和/或数据分发方法。附加地或替代地,实施例可以提供改进的数据传输或交换方法或改进的电子通信。

[0317] 公开了一种计算机实现的数据分发方法。所述方法可以包括:将(例如,区块链相关)数据的一部分从发送资源发送到一个或多个接收资源群组;所述一个或多个群组中的每个群组可以与相应地址相关联;所述地址可以是组播地址。换句话说,可以形成资源群组,其中,对于每个群组,资源是所述群组的订阅成员,并且所有成员都与标识所述群组的地址相关联。本公开的实施例可以包括生成、创建或提供IPv6组播地址的步骤。

[0318] 所述接收资源中的一部分或全部接收资源可以是区块链网络上的全节点104,也可以是覆盖网络中的节点,所述节点位于所述区块链网络上的一个或多个全节点之上但与所述区块链网络上的所述一个或多个全节点通信。所述发送资源可以是全区块链节点104,也可以是区块链覆盖网络上的节点,该节点位于所述区块链网络上的一个或多个全节点之上但与所述区块链网络上的所述一个或多个全节点通信。这些特征可能适用于下面提供的条款集中的一个或多个条款集。

[0319] 一些实施例可以提供用于实现区块链网络的内存池的方案。

[0320] 一些实施例可以提供用于实现区块链网络的UTXO集的方案。

[0321] 本文还公开了:

[0322] ●一种计算机设备,所述计算机设备包括:存储器,所述存储器包括一个或多个存储器单元;以及处理装置,所述处理装置包括一个或多个处理单元,其中所述存储器存储被设置在所述处理装置上运行的代码,所述代码被配置为当在所述处理装置上运行时,执行根据本文所述或所定义的任何实施例所述的方法;和/或

[0323] ●一种计算机程序,所述计算机程序包含在计算机可读存储器上并且被配置为当在一个或多个处理器上运行时,执行根据本文所述或所定义的任何所述的方法。

[0324] 条款集1:

[0325] 可以提供:

[0326] 条款1.1一种方法,所述方法包括:

[0327] 从至少一个发送资源向至少一个接收资源发送传输;所述发送资源和/或所述接收资源可以是网络上的节点。

[0328] 所述发送资源和/或所述接收资源可以是网络上的MLDv1主机或MLDv2主机、网络交换机或路由器。所述传输可以由所述发送资源根据组播转发表发送。关于条款集8所叙述的特征可以被合并到条款集1或任何其他条款集中。

[0329] 根据替代(而非排他性)措辞,可以提供:一种计算机实现的方法,所述方法包括:

[0330] 通过网络将区块链相关数据的一部分从发送资源发送到与接收资源群组相关联的组播地址。所述接收资源群组可以是多个接收资源中的一个接收资源,所述多个接收资源中的每个群组与相应组播地址相关联。在一些实施例中,所述区块链相关数据可以发送到所述群组中的一个、部分或全部群组。当所述数据被发送到多于一个群组时,所述数据被发送到所述数据被发送到的所述群组的所述相应组播地址中的每个相应组播地址。

[0331] 所述网络可以是对等(P2P)网络和/或分布式网络。所述网络可以是区块链网络,其中所述区块链网络上的节点用于根据所述区块链的协议来执行操作。在其他实施例中,所述网络可以是互联网或LAN或VLAN或电信网络、或包交换网络101。

[0332] 所述发送资源和/或所述至少一个接收资源可以被设置为根据给定区块链的协议来执行操作。附加地或替代地,所述发送资源和/或所述至少一个接收资源可以是区块链网络上的节点、加密货币交换所资源、数字钱包或区块链相关服务提供者。在一些示例性实施例中,至少一个接收节点不是所述区块链网络上的节点;换句话说,它可以在所述区块链网络外部,以及/或者可以不被布置为实现区块链协议或执行共识/协议相关功能。附加地或替代地,在一些示例性实施例中,所述发送资源不是所所述区块链网络上的节点。

[0333] 附加地或替代地,所述发送资源和/或所述至少一个接收资源可以是被设置为和/或用于处理区块链相关数据(例如,与以下各项中的任何一项或多项有关的数据)的资源:

[0334] ●区块链事务

[0335] ●至少一个未确认区块链事务

[0336] ●至少一个未花费事务输出(UTXO)

[0337] ●区块相关数据

[0338] ●用于验证或其他目的的默克尔路径和/或证明

[0339] ●工作证明和/或权益证明操作或任何其他共识操作

[0340] ●区块链挖掘操作

[0341] ●区块链相关警报或信号,所述区块链相关警报或信号与以下各项中的部分或全部相关或者可由以下各项中的部分或全部使用:

[0342] ○区块链网络上的节点;和/或

[0343] ○区块链网络的用户,例如交换所、钱包和区块链相关服务提供者。

[0344] 所述传输可以(至少)包括与以下各项相关的数据:

[0345] ●一个或多个区块链事务;所述数据可以包括至少一个整个事务和/或至少一个事务的一部分;

[0346] ●区块链事务区块;

[0347] ●至少一个默克尔路径和/或默克尔证明;所述默克尔路径/证明数据可以包括与事务区块相关的默克尔树的至少一部分;它可能适合于验证(例如,SPV式验证),或者适合

于确认给定节点或根在给定路径或树中,或者适合于任何一个或多个其他目的;

[0348] ●工作证明和/或权益证明操作,或者由区块链网络上的节点执行的任何其他共识相关操作;

[0349] ●一个或多个区块链挖掘操作,例如由区块链网络上的节点执行的操作;

[0350] ●区块链相关警报或信号,所述区块链相关警报或信号与以下各项中的部分或全部相关或者可由以下各项中的部分或全部使用:

[0351] o区块链网络上的节点;和/或

[0352] o区块链网络的用户,例如交换所、钱包和区块链相关服务提供者;覆盖网络中的一个或多个节点,所述一个或多个节点是相对于所述区块链网络的覆盖层。

[0353] 所述至少一个发送资源可以响应于请求向所述至少一个接收资源发送所述传输。所述请求可以由所述至少一个接收资源或由其他资源发送。所述请求可以由所述至少一个发送资源从所述至少一个接收请求或所述其他资源接收。所述请求可以包括对数据的请求。所述请求可以包括区块链相关数据,例如与一个或多个区块链事务或事务ID(TxID)、一个或多个区块链区块或一个或多个区块头和/或默克尔路径或证明的至少一部分相关的数据。

[0354] 所述数据可以作为/以一个或多个数据的包(“数据包”)的形式通过电子网络传输。优选地,它们是IPv6包。

[0355] 条款1.2根据条款1.1所述的方法,其中所述传输通过互联网等公共网络来执行;优选地,其中:

[0356] 所述传输是IPv6传输、IPv4传输、任播传输或组播传输。

[0357] 条款1.3根据条款1.1或1.2所述的方法,其中所述发送资源和/或所述至少一个接收资源:

[0358] 是任播群组的成员;以及/或者

[0359] 是组播群组的成员。

[0360] 条款集2:

[0361] 附加地或替代地,本公开的一个或多个实施例可以根据以下条款进行定义。条款集2所定义的条款中的任何条款可以与本文提供的任何其他条款集中的一个或多个条款或本文公开的任何其他特征组合。

[0362] 条款2.1一种方法,所述方法包括:

[0363] 接收资源向与网络上的多个发送资源群组中的一个发送资源群组的成员相关联的发送地址发送对区块链相关数据的请求;以及

[0364] 响应于所述请求,从所述群组的至少一个发送资源接收区块链相关数据。

[0365] 所述发送地址可以是发送任播地址或组播地址。所述方法可以是计算机实现的数据分发方法。附加地或替代地,所述方法可以是改进的数据传输或交换方法,也可以是电子通信方法。

[0366] 条款2.2根据条款2.1所述的方法,其中接收所述区块链相关数据包括:通过单播或组播传输从所述至少一个发送资源接收所述区块链相关数据。

[0367] 条款2.3根据条款2.2或2.1所述的方法,其中接收所述区块链相关数据包括:通过任播传输从所述至少一个发送资源接收所述区块链相关数据。

[0368] 条款2.4根据前述任一项条款所述的方法,其中所接收的区块链相关数据包括从所述群组的多个成员接收的区块链相关数据的一个或多个部分。

[0369] 条款2.5根据条款2.4所述的方法,其中区块链相关数据的每个部分包括所述相应部分的哈希。

[0370] 条款2.6根据前述任一项条款所述的方法,所述方法包括:发送任播或组播查询传输;以及响应于所述任播或组播查询传输,(从最近的发送资源)接收以下各项的至少一部分:区块链区块、区块链事务和/或默克尔路径。

[0371] 条款2.7根据前述任一项条款所述的方法,其中所述发送地址与拥有区块链区块的完整副本的发送资源相关联。

[0372] 条款2.8根据条款2.7所述的方法,所述方法包括:从(拓扑上)最近的接收资源接收任播或组播查询传输;以及响应于所述任播或组播查询传输,向所述(拓扑上)最近的接收资源发送以下各项的至少一部分:区块链区块、区块链事务和/或默克尔路径。

[0373] 条款2.9一种方法(例如,计算机实现的数据分发方法),所述方法包括:发送资源向与网络上的多个接收资源群组中的一个接收资源群组的成员相关联的接收地址发送区块链相关数据。所述接收地址可以是任播或组播地址。

[0374] 条款2.10根据前述任一项条款所述的方法,其中所述区块链相关数据包括所述数据的哈希。

[0375] 条款2.11根据条款2.9或2.10所述的方法,所述方法包括:从发送地址取消分配所述发送资源。

[0376] 条款2.12根据条款2.12所述的方法,其中响应于确定已经满足预定条件(例如,所述区块链相关数据被发送到预定数量的接收资源,并且/或者已经过去一定时间,或者达到给定日期和时间等)而执行所述取消分配。

[0377] 条款2.13根据条款2.12所述的方法,其中响应于确定已经过去预选时间段而执行所述取消分配。

[0378] 条款集3:

[0379] 附加地或替代地,本公开的一个或多个实施例可以根据以下条款进行定义。条款集3所定义的条款中的任何条款可以与本文提供的任何其他条款集中的一个或多个条款或本文公开的任何其他特征组合。

[0380] 条款3.1.一种计算机实现的数据分发方法,所述方法包括:

[0381] 将区块链相关数据的一部分从网络上的一个(或至少一个)发送资源发送到某个/所述网络上的一个或多个接收资源群组,其中所述一个或多个群组中的每个群组与相应组播地址相关联。所述网络可以是互联网。在一个优选实施例中,每个群组中的所有接收资源共享对于所述群组唯一的公共组播地址;每个资源群组具有相应组播地址,所述群组的所有成员都订阅所述相应组播地址,以便接收发送到所述群组的共享组播地址的组播传输。

[0382] 所述至少一个发送资源可以通过传输来发送所述数据部分。可以响应于请求或作为请求的一部分将所述数据部分发送到至少一个接收资源群组。所述请求可以包括对数据的请求。所述请求可以包括区块链相关数据,例如与一个或多个区块链事务或事务ID(TxID)、一个或多个区块链区块或一个或多个区块头和/或默克尔路径或证明的至少一部分相关的数据。所述数据可以通过互联网发送。

[0383] 条款3.2.根据条款3.1所述的方法,其中所述发送资源和/或所述一个或多个群组中的至少一个群组中的所述接收资源中的一个、部分或全部接收资源是或包括:

[0384] 网络中的节点;所述网络可以是区块链网络、互联网或电信网络;或者覆盖网络中的节点,所述节点是相对于所述(底层)区块链网络的覆盖层;

[0385] 与金融机构相关联或由金融机构控制的计算资源;

[0386] 商家资源;

[0387] 加密货币交换所;

[0388] 计算资源,所述计算资源被设置为执行或促进SPV验证、或使用SPV验证的结果;

[0389] 区块链相关服务提供者;和/或

[0390] 数字钱包。

[0391] 条款3.3.根据条款3.1或3.2所述的方法,其中所述数据包括:

[0392] 与区块链相关事件或活动相关的通信或警报。

[0393] 条款3.4.根据条款3.3所述的方法,其中所述警报涉及所述区块链网络中的双重花费或双重花费尝试。

[0394] 条款3.5.根据前述任一项条款所述的方法,其中所述区块链相关数据包括以下各项中的一项、部分或全部:

[0395] i)区块链事务的至少一部分;

[0396] ii)区块链区块的至少一部分;

[0397] iii)区块链事务脚本的至少一部分;

[0398] iv)默克尔路径、默克尔树或默克尔证明的至少一部分;

[0399] v)与区块链网络的共识机制一起使用或相关联的数据;

[0400] vi)权益证明或工作证明操作的结果;

[0401] vi)包括区块链区块验证或SPV验证在内的验证操作的结果。

[0402] 条款3.6.根据前述任一项条款所述的方法,其中:

[0403] 所述区块链相关数据由所述发送资源使用组播通信发送到所述一个或多个接收资源群组。

[0404] 条款3.7.根据前述任一项条款所述的方法,其中:

[0405] i)所述组播地址是IP组播地址;并且/或者

[0406] ii)所述组播地址是IPv6组播地址;并且/或者

[0407] iii)所述区块链相关数据通过互联网发送到所述一个或多个接收资源群组。

[0408] 条款3.8.根据前述任一项条款所述的方法,其中:

[0409] 所述一个或多个接收主机群组中的每个接收主机群组包括一个或多个接收资源;并且/或者

[0410] 给定接收资源群组中的每个接收对等体用于接收发送到所述特定接收资源群组的所述组播地址的数据。

[0411] 条款3.9.根据前述任一项条款所述的方法,所述方法包括以下步骤:

[0412] 资源订阅接收资源群组;优选地,其中所述资源通过向某个/所述网络发送信号进行订阅;(所述网络可以是互联网)

[0413] 资源离开接收资源群组;优选地,其中所述资源通过停止向所述网络发送信号而

离开所述群组。

[0414] 条款3.10.根据前述任一项条款所述的方法,其中:

[0415] 所述发送资源和/或所述至少一个或多个接收资源群组中的至少一个接收资源被设置为、被配置为和/或用于执行以下操作中的一项或多项操作:

[0416] 区块链协议指定的功能;

[0417] 与区块链协议中指定的挖掘或共识函数相关的计算或其他操作;

[0418] 简单支付验证(SPV)操作;

[0419] 计算或验证默克尔路径、默克尔路径的证明或根;

[0420] 在区块链事务写入区块链之前或之后对其进行核实;

[0421] 搜索区块链,以识别、定位和/或确认区块链中是否存在给定事务或区块;

[0422] 生成区块链事务,将事务写入区块链,并且/或者向区块链网络广播事务。

[0423] 条款3.11.根据前述任一项权利要求所述的方法,所述方法包括以下步骤:

[0424] 通过将区块链相关数据的所述部分从所述发送资源发送到所述一个或多个接收资源群组,对所述一个或多个群组中的每个群组进行轮询以获得目标响应。

[0425] 条款3.12.一种计算机实现的方法,所述方法包括以下步骤:

[0426] 向区块链网络上的资源群组发送组播通信。

[0427] 条款3.13.根据条款12所述的方法,其中以下各项中的至少一项、部分或全部适用:

[0428] i)所述通信从发送资源发送到所述资源群组;

[0429] ii)所述资源群组是组播群组,并且所述资源群组中的一个或部分资源是所述组播群组的接收资源;

[0430] iii)所述通信涉及所述网络中的双重花费或双重花费尝试;

[0431] iv)所述通信是警报。

[0432] 条款3.14.一种计算机设备,所述计算机设备包括:

[0433] 存储器,所述存储器包括一个或多个存储器单元;以及

[0434] 处理装置,所述处理装置包括一个或多个处理单元,其中所述存储器存储被设置在所述处理装置上运行的代码,所述代码被配置为当在所述处理装置上运行时,执行根据条款3.1至3.13中任一项所述的方法。

[0435] 条款3.15.一种计算机程序,所述计算机程序包含在计算机可读存储器上并且被配置为当在一个或多个处理器上运行时,执行根据条款3.1至3.13中任一项所述的方法。

[0436] 条款集4:

[0437] 附加地或替代地,本公开的一个或多个实施例可以根据以下条款进行定义。条款集4所定义的条款中的任何条款可以与本文提供的任何其他条款集中的一个或多个条款或本文公开的任何其他特征组合。

[0438] 条款4.1.一种方法,所述方法包括以下步骤:

[0439] 从发送资源向至少一个资源群组发送组播通信,其中,优选地:

[0440] i)所述发送资源和/或所述至少一个群组中的至少一个资源是或包括:

[0441] 区块链网络上的节点;和/或

[0442] 数字钱包或数字钱包提供者;和/或

[0443] 加密货币交换所;和/或

[0444] 与一个或多个区块链挖掘节点相关联的资源;和/或

[0445] 被设置为向一个或多个用户提供区块链相关服务的服务提供者。

[0446] 条款4.2.根据条款4.1所述的方法,其中:

[0447] i)所述通信是通过公共网络,优选地是通过互联网发送的;并且/或者

[0448] ii)所述至少一个资源群组是包括成员资源的组播群组,所述成员资源被设置为或用于接收发送到与所述组播群组相关联的(组播)地址的通信;并且/或者

[0449] iii)所述通信涉及所述网络中的双重花费或双重花费尝试;并且/或者

[0450] iv)所述通信是包括区块链相关数据的警报或其他通信。

[0451] 条款集5:

[0452] 附加地或替代地,本公开的一个或多个实施例可以根据以下条款进行定义。条款集5所定义的条款中的任何条款可以与本文提供的任何其他条款集中的一个或多个条款或本文公开的任何其他特征组合。

[0453] 本文公开的实施例可以提供用于网络上的资源之间的改进的电子通信的方法和技术。所述实施例可以被设置为确保或提高各方之间的数据交换或各方之间的传输的可靠性。在一种可能形式的措辞中,此类实施例可以包括一种方法,所述方法包括以下步骤中的一个、部分或全部步骤:

[0454] 通过电子网络从一个或多个发送资源向一个或多个接收资源发送至少一个数据包。所述一个或多个资源可以是组播群组的成员。换句话说,它们可以是公共(共享)组播地址的订阅者;附加地或替代地,所述接收资源中的一个或多个接收资源可以与共享任播地址相关联;在一些情况下,所述一个或多个发送资源还可以与所述共享组播和/或任播地址相关联;所述至少一个数据包可以发送到所述共享组播地址。

[0455] 所述至少一个数据包可以由所述接收资源中的至少一个接收资源接收;

[0456] 所述方法还可以包括以下各项中的一项或多项:

[0457] • 所述至少一个接收资源在接收到所述至少一个数据包后确定所述至少一个接收资源是否应该接收(或需要)至少一个其他数据包;

[0458] • 从所述至少一个接收资源向至少一个其他资源发送对所述至少一个其他数据包的请求;优选地,其中:

[0459] ■所述至少一个其他资源是所述组播群组的成员;并且/或者

[0460] ■所述至少一个其他资源是所述任播群组的成员;并且/或者

[0461] ■所述请求使用组播传输、任播传输或单播传输来发送;

[0462] • 所述至少一个其他资源从所述至少一个接收资源接收对所述至少一个其他数据包的所述请求;

[0463] ■从所述至少一个其他资源向所述至少一个接收资源发送所述至少一个其他数据包;优选地,其中,所述至少一个数据包使用单播传输发送到所述至少一个接收资源。

[0464] 在替代形式的措辞中,此类实施例可以如以下条款中所提供的那样进行描述。前述方法的特征可以包括在以下条款中的任何条款中,反之亦然。

[0465] 条款5.1.一种方法,所述方法包括以下步骤:

[0466] 从作为资源群组的成员的(请求)发送资源向作为所述资源群组的成员的至少一

个其他资源发送请求,其中,优选地:

[0467] i)所述请求包括对一个或多个数据包的请求;并且/或者

[0468] ii)所述请求由于发送到所述发送资源的数据传输的不完整接收而被发送,优选地,其中不完整的数据传输经由或通过发送到所述资源群组的组播传输被发送到所述发送资源和/或所述至少一个其他资源;并且/或者

[0469] iii)所述请求作为任何任播传输发送到所述资源群组中相对于所述发送资源的(拓扑上)最近的资源;并且/或者

[0470] iv)所述请求作为任何组播传输发送到所述资源群组中的(拓扑上)最近的资源;并且/或者

[0471] v)所述请求由于(由数据发送资源)发送到所述(请求)发送资源的数据传输的(由所述发送资源)不完整接收而被发送,优选地,其中所述请求包括对所述(请求)发送资源由于所述数据传输的不完整接收而未能接收的数据的至少一部分(例如,数据包)的请求。

[0472] 条款5.2.根据条款5.1所述的方法,其中所述发送资源和/或所述至少一个其他资源是或包括:

[0473] 区块链网络上的节点;和/或

[0474] 数字钱包或数字钱包提供者;和/或

[0475] 加密货币交换所或其组成部分;和/或

[0476] 与一个或多个区块链挖掘节点相关联或与一个或多个区块链挖掘节点通信的资源;和/或

[0477] 被设置为向一个或多个用户提供区块链相关服务的服务提供者;和/或

[0478] 资源,所述资源被设置为执行、促进或使用SPV验证的结果。所述资源可以包括软件,所述软件用于执行或促进简单支付验证(SPV)操作,或处理SPV操作的结果。

[0479] 条款5.3.根据条款5.1或5.2所述的方法,其中:

[0480] i)所述通信是通过公共网络,优选地是通过互联网发送的;并且/或者

[0481] ii)所述至少一个资源群组是包括成员资源的组播群组,所述成员资源被设置为或用于接收发送到与所述组播群组相关联的(组播)地址的通信;并且/或者

[0482] iii)所述通信涉及所述网络中的双重花费或双重花费尝试;并且/或者

[0483] iv)所述通信是包括区块链相关数据的警报或其他通信;并且/或者

[0484] v)所述通信包括区块链相关数据和/或默克尔路径或默克尔树的至少一部分;并且/或者

[0485] vi)用于执行或促进SPV式验证的数据。

[0486] 条款5.4.根据条款5.1、5.2或5.3所述的方法,所述方法包括以下步骤:

[0487] 从所述其他资源向所述(请求)发送资源提供数据的一个或多个部分。

[0488] 此外,根据一个或多个实施例,可以提供一种方法,所述方法包括:

[0489] 响应于来自(请求)发送资源的请求,向所述(请求)发送资源提供数据的至少一部分;优选地,所述(请求)发送资源是资源群组的成员,并且数据的所述至少一部分由作为所述资源群组的成员的其他资源提供或从所述其他资源提供给所述发送资源;并且其中,优选地:

[0490] i)所述请求包括对一个或多个数据包的请求;并且/或者

[0491] ii)所述请求由于发送到所述发送资源的数据传输的不完整接收而被发送到所述其他资源,优选地,其中不完整的数据传输经由或通过发送到所述资源群组的组播传输被发送到所述(请求)发送资源和/或所述至少一个其他资源;并且/或者

[0492] iii)所述请求作为任何任播传输发送到所述资源群组中相对于所述发送资源的(拓扑上)最近的资源;并且/或者

[0493] iv)所述请求作为任何组播传输发送到所述资源群组中的(拓扑上)最近的资源;并且/或者

[0494] v)所述请求由于(由数据发送资源)发送到所述(请求)发送资源的数据传输的(由所述发送资源)不完整接收而被发送,优选地,其中所述请求包括对所述(请求)发送资源由于所述数据传输的不完整接收而未能接收的数据的至少一部分(例如,数据包)的请求。

[0495] 条款集6:

[0496] 附加地或替代地,本公开的一个或多个实施例可以根据以下条款进行定义。条款集6所定义的条款中的任何条款可以与本文提供的任何其他条款集中的一个或多个条款或本文公开的任何其他特征组合。

[0497] 条款6.1一种方法,所述方法包括以下步骤中的一个或多个步骤:

[0498] 1.形成或提供网络节点群组(集);

[0499] 2.将所述节点群组与组播地址相关联;这些节点现在是所述组播的群组成员,即,它们侦听所述组播地址;在另一形式的措辞中,步骤1和步骤2可以表述为:一个或多个节点加入组播群组;

[0500] 3.推广/宣传/传达可用服务和/或资源,其中所述服务的所述推广/所述宣传/所述传达由所述群组的一个或多个节点/成员向网络上的一个或多个接收者执行;所述网络可以是也可以不是区块链网络;该传达可以是或包括通过所述组播地址向所述群组成员发送数据的邀请;

[0501] 4.所述一个或多个节点/成员向所述网络上的所述一个或多个接收者推广/宣传/传达所述群组的共享组播地址;在一个或多个实施例中,这可以包括邀请或请求所述一个或多个接收者向所述群组组播地址处的所述群组成员发送(例如,区块链相关)数据,例如,邀请或请求区块链挖掘节点向所述群组的共享组播地址发送一个或多个新区块、或事务、默克尔树等或其部分;在一些实施例中,步骤4(即,共享所述组播地址)可以与步骤3(即,向所述网络上的接收者宣传所述服务)组合;

[0502] 5.所述群组的一个或多个节点/成员向所述网络接收者推广/宣传/传达唯一的任播地址;

[0503] 6.区块链挖掘节点挖掘新区块或区块链事务;

[0504] 7.将所述新区块从所述挖掘节点发送到所述群组的共享组播地址;应当注意的是,在其他实施例中,所述一个或多个群组成员请求并且所述网络接收者向所述一个或多个群组成员发送的所述数据可能不包括或与区块链数据相关,例如区块或事务;在一些实施例中,所述数据可以是任何类型的数据,或者可以是区块链相关数据,例如全部或部分区块、全部或部分事务、用于共识相关操作的数据、用于核实事务和/或区块的数据、用于SPV式验证的数据、默克尔树/路径的全部或部分等;

[0505] 8.将所述数据(例如,区块或区块的一部分)路由到所述组播群组的所有成员;这

可以使用IPv6传输通过互联网执行;

[0506] 9.从所述一个或多个节点/成员间歇地向所述组播群组的所述任播地址发送请求;优选地,所述请求包括发送节点的单播地址;

[0507] 10.将节点(成员)与先前推广的任播地址相关联;优选地,其中在接收到新区块或其他类型的数据时执行该操作;

[0508] 11.所述节点/成员通过单播传输向请求节点发送所述数据的副本(例如,区块或区块的一部分);如果具有所述任播地址的节点(组播群组成员)接收到对所述新区块的副本的请求,则可以执行该操作;

[0509] 12.从所述任播地址取消分配所述节点/群组成员;在一些示例中,在确定已经过去预定时间量或已经满足预定标准时执行该操作;

[0510] 13.所述节点/群组成员侦听发送到所述群组的组播地址的新数据传输。

[0511] 上述步骤中的一个或部分步骤可以省略或以与上述顺序不同的顺序执行,或者可以与一个或多个其他步骤合并。

[0512] 条款集7:

[0513] 附加地或替代地,本公开的一个或多个实施例可以根据以下条款进行定义。条款集7所定义的条款中的任何条款可以与本文提供的任何其他条款集中的一个或多个条款或本文公开的任何其他特征组合。

[0514] 根据该实施例的方法可以基本上如本文所述,尤其关于区块头传播。根据一种可能形式的措辞,此类实施例可以包括一种计算机实现的方法,所述方法包括以下步骤:从发送节点发送到多个接收节点发送数据。优选地,所述接收节点中的每个接收节点与IPv6组播地址相关联。所述数据可以包括(用于)区块链区块的区块头的至少一部分;以及所述区块链区块中包括的与所述区块头相关的一个或多个区块链事务的列表。

[0515] 所述方法还可以包括以下步骤:所述接收节点中的至少一个接收节点使用所述数据来识别所述至少一个接收节点需要的至少一个其他区块链事务(即,至少一个“缺失”事务),以便生成所述区块链区块。换句话说,如果所述至少一个接收节点具有a)区块链头部和b)所述区块链区块中包含的所述事务的完整列表,则所述至少一个接收节点将只能生成所述区块的完整、详尽版本或副本。因此,所述至少一个接收节点可以执行检查以识别其需要的任何其他事务,这些事务未包括在所述发送节点发送的所述列表中。识别所述至少一个其他区块链事务可以包括在存储的区块链事务集中搜索所述至少一个其他区块链事务。所述存储的事务集可以由所述至少一个接收节点维护。附加地或替代地,所述存储的事务集可以由所述至少一个接收节点访问或可由所述节点访问。

[0516] 所述方法可以包括以下步骤:从所述存储的区块链事务集中获得所述至少一个其他(缺失)事务;以及使用所述至少一个其他事务和一个或多个区块链事务的所述列表来生成所述区块链区块。

[0517] 然而,如果在所述存储的事务集中没有找到所述至少一个其他事务,则所述方法可以包括以下步骤:从所述至少一个接收节点向以下各项中的一项或多项发送对所述至少一个其他区块链事务的请求:所述发送节点;或者所述IPv6组播地址;或者一个或多个其他节点。所述方法可以包括以下步骤:所述发送节点从所述至少一个接收节点接收所述请求;以及从所述发送节点向所述至少一个接收节点发送传输,所述传输包括所述至少一个其他

区块链事务。所述传输可以是单播传输。

[0518] 附加地或替代地,所述实施例可以在以下条款中进行描述。这些条款中的任何条款中包括的任何特征也可以合并到前述方法步骤中或与前述方法步骤组合,反之亦然。

[0519] 条款7.1一种计算机实现的方法,所述包括以下步骤:

[0520] 从发送节点向组播地址发送区块头(的至少一部分)以及一个或多个区块链事务和/或区块链事务标识符(TxID)的列表;

[0521] 优选地,其中所述(IPv6)组播地址由多个接收(即,订阅)节点订阅。

[0522] 在一些实施例中,所述发送节点和/或所述接收节点中的至少一个接收节点是区块链网络上的节点。优选地,所述组播地址是IPv6组播地址。

[0523] 条款7.2:根据7.1所述的方法,所述方法包括以下步骤:

[0524] 所述接收节点中的至少一个接收节点但优选地全部接收节点使用所接收的信息来识别所述至少一个接收节点需要的任何一个或多个缺失事务,以便生成具有所述区块头的完整区块;

[0525] 优选地,其中如果事务在一个或多个事务的所述列表中但不包括在由所述至少一个接收节点维护和/或可由所述至少一个接收节点访问的事务集(例如,成员池)中,则所述事务是缺失事务。

[0526] 条款7.3:根据7.1或7.2所述的方法,所述方法包括以下步骤:

[0527] 如果所述接收节点识别任何一个或多个缺失事务,则从所述至少一个接收节点向所述发送节点(优选地,通过单播传输)或所述组播群组(优选地,通过组播或任播传输)发送对所述一个或多个缺失事务或所述一个或多个事务标识符的请求;

[0528] 优选地,所述请求包括所请求的一个或多个缺失事务的所述相应一个或多个事务标识符(TxID)。

[0529] 条款7.4:根据7.1、7.2和/或7.3所述的方法,所述方法包括以下步骤:

[0530] 所述发送节点从所述接收节点接收所述请求。

[0531] 条款7.5:根据7.1、7.2、7.3和/或7.4所述的方法,所述方法包括以下步骤:

[0532] 从所述发送节点向所述接收节点发送传输,所述传输包括所请求的一个或多个缺失事务和/或一个或多个事务标识符;优选地,其中所述传输是单播传输;优选地,所述单播传输仅被发送到已经发送所述请求的各个接收节点。

[0533] 所述方法还可以包括:使用一个或多个事务/TxID的所述列表以及至少一个所请求的缺失事务和/或事务标识符来生成包括所述区块头的区块链区块。这可以在所述接收节点接收到所述传输时执行。然后,所述接收节点可以执行一个或多个区块链相关操作(例如,验证或核实操作)。

[0534] 条款集8:

[0535] 附加地或替代地,本公开的一个或多个实施例可以根据以下条款进行定义。条款集8所定义的条款中的任何条款可以与本文提供的任何其他条款集中的一个或多个条款或本文公开的任何其他特征组合。

[0536] 8.1一种方法,所述方法包括以下步骤:

[0537] 通过电子网络从已经启用组播侦听者设备(MLD)窥探的发送资源向组播地址发送传输(通信);并且其中:

[0538] i)所述传输包括区块链相关数据;并且/或者

[0539] ii)所述组播地址与至少一个接收资源相关联,所述接收资源是:

[0540] 网络中的节点;所述网络可以是区块链网络、互联网或电信网络;

[0541] 与金融机构相关联或由金融机构控制的计算资源;

[0542] 商家控制资源;

[0543] 加密货币交换所或其组成部分;

[0544] 计算资源,所述计算资源被设置为执行或促进SPV验证、或使用SPV验证的结果;

[0545] 区块链相关服务提供者;和/或

[0546] 数字钱包或其组成部分;和/或

[0547] 资源,所述资源用于执行或促进简单支付验证(SPV)操作,或处理SPV操作的结果;

[0548] iii)所述传输是或包括与警报相关的数据,优选地,其中所述警报与区块链网络上的一个或多个节点相关、有关或被设置用于由区块链网络上的一个或多个节点利用;并且/或者

[0549] iv)所述传输包括:

[0550] 区块链相关数据和/或默克尔路径或默克尔树的至少一部分;和/或

[0551] 用于执行或促进SPV式验证、或使用SPV验证的结果的数据。

[0552] 一个或多个接收资源可以与所述组播地址相关联。换句话说:至少一个接收资源可以订阅(即,侦听)所述组播地址。所述一个或多个接收资源可以称为组播群组。所述组播地址可以是IPv6地址。所述发送资源和/或所述一个或多个接收资源可以是网络上的设备或系统。所述网络可以是物理网络或逻辑网络。所述网络可以是VLAN。所述发送资源可以是组播路由器。

[0553] 条款8.2根据条款8.1所述的方法,其中所述发送资源用于将所述传输发送到所述电子网络上已经指示或发信号通知接收所述传输的兴趣或意图的一个或多个设备端口的列表。

[0554] 所述列表可以是IPv6组播转发表或数据库。

[0555] 条款8.3根据条款8.1或8.2所述的方法,其中:

[0556] i.所述发送资源被配置为和/或用于监测接收资源和/或组播路由器之间的MLD消息;并且/或者

[0557] ii.所述发送资源可以检查或利用(所监测的)MLD消息来生成IPv6地址和连接到所述一个或多个接收资源的相应网络接口的列表。

[0558] 条款8.4根据条款集8的前述任一项条款所述的方法,其中所述发送资源用于:

[0559] i)仅将所述传输发送到连接到与所述组播地址相关联(订阅/侦听寻址到所述组播地址的网络流量)的相应接收资源的网络接口;以及/或者

[0560] ii)在没有接收资源与所述组播地址相关联的情况下不发送所述传输。

[0561] 条款8.5根据条款集8中的前述任一项条款所述的方法,其中:

[0562] 所述接收资源中的一个或多个接收资源用于发送包括源地址列表的成员资格报告。所述成员资格报告可以以INCLUDE(包括)或EXCLUDE(排除)模式发送。

[0563] 所述发送资源和/或所述接收资源可以用于基本上如本领域所描述的那样实现MLD窥探:

[0564] https://www.juniper.net/documentation/us/en/software/junos/multicast/topics/concept/mld-snooping-overview-l2.html。

[0565] 条款集9:

[0566] 附加地或替代地,本公开的一个或多个实施例可以根据以下条款进行定义。条款集1至8中的任何条款集所定义的条款中的任何条款可以与本文提供的任何其他条款集中的一个或多个条款或本文公开的任何其他特征组合。

[0567] 条款9.1一种计算机实现的方法,所述方法包括:发送和/或接收用于生成、存储、处理、访问和/或维护数据包的资源,所述数据包优选地包括区块链相关数据;根据所述数据包确定分配地址;以及通过电子网络至少部分地将所述数据包的传输从所述发送资源发送到所述分配地址。

[0568] 条款9.2.根据条款9.1所述的方法,其中所述分配地址是与接收资源群组相关联的组播地址。

[0569] 条款9.3.根据前述任一项条款所述的方法,其中所述记录包括以下各项中的至少一项:事务(Tx)的一部分;输出标识符;脚本的哈希;事务标识(TXID);区块链区块;以及区块头。所述输出标识符可以是与所述区块链事务(Tx)中的输出相关联的标识符。例如,所述输出标识符可以是UTXO标识符。脚本的所述哈希可以是与所述事务(Tx)的输出相关联的脚本(例如,UTXO脚本)的哈希。

[0570] 条款9.4.根据前述任一项条款所述的方法,其中确定所述分配地址包括:对所述数据包进行处理以确定密钥;以及使用所述密钥从地址集中选择至少一个地址,所述处理优选地包括对所述数据包进行解析。

[0571] 条款9.5.根据前述任一项条款所述的方法,其中所述发送资源持有、提供或包括数据结构,所述数据结构包括与对应密钥集相关联的分配地址集。

[0572] 条款9.6.根据前述任一项条款所述的方法,其中所述发送资源生成、存储、处理、访问和/或维护包括多个数据包的(零个或更多个区块链事务的)(区块链)区块,其中所述区块中的所述数据包中的每个数据包包括区块链相关数据。

[0573] 所述方法可以包括以下步骤:为所述区块中的每个数据包确定分配地址;以及通过电子网络至少部分地从所述发送资源向所述相应分配地址发送所述区块中的每个数据包的传输。

[0574] 条款9.7.根据条款9.6所述的方法,其中所述区块分割为子区块,并且所述发送资源通过电子网络将每个子区块传输到对应分配地址。

[0575] 条款9.8.根据条款9.6或9.7所述的方法,其中所述多个数据包分割为八个子区块,每个子区块被发送到对应分配地址。

[0576] 条款9.9.根据前述任一项条款所述的方法,其中所述发送资源附加地或替代地用作接收资源,所述方法还包括:接收所述数据包和/或所述多个数据包,以及以下各项中的至少一项:将所述数据包传播到所述分配地址。优选地,传播所述区块包括:向所述相应分配地址传输多个数据包;合并所述区块;以及/或者传输所述多个数据包以传播到对应分配地址。

[0577] 附加地或替代地,所述方法可以包括以下步骤:收集所述数据包、多个数据包或区块中的至少一者,然后对每个数据包进行解析以确定密钥;以及使用所述密钥将每个数据

包传播到地址集中的至少一个地址。

[0578] 条款9.10.根据前述任一项条款所述的方法,其中所述发送资源或所述接收资源订阅至少一个接收资源和/或至少一个组播群组。

[0579] 条款9.11.根据条款9.10所述的方法,其中所述发送资源或所述接收资源订阅被配置为接收分配给所述组播地址的至少一个数据包的组播地址。优选地,所述分配是根据所述至少一个数据包确定的。

[0580] 条款9.12.根据条款9.10或9.11所述的方法,所述方法还包括所述发送资源:通过向网络(例如,互联网和/或区块链网络)发送信号来订阅接收资源群组;以及/或者离开接收资源群组,优选地,其中所述资源通过停止向所述网络发送信号而离开所述群组。根据条款9所述的各方面可以与条款9.2结合。

[0581] 条款9.13.根据前述任一项条款所述的方法,其中所述数据包包括:与区块链相关事件或活动相关的通信、通知、消息或警报。

[0582] 条款9.14.根据前述任一项条款所述的方法,其中所述警报涉及区块链网络中的双重花费或双重花费尝试。

[0583] 条款9.15.根据前述任一项条款所述的方法,其中所述发送资源和/或所述接收资源被设置为、被配置为和/或用于执行以下操作中的一项或多项:

[0584] 区块链协议指定的功能;

[0585] 与区块链协议中指定的挖掘或共识函数相关的计算或其他操作;

[0586] 简单支付验证(SPV)操作;

[0587] 计算或验证默克尔路径、默克尔路径的证明或根;

[0588] 在区块链事务写入区块链之前或之后对其进行核实;

[0589] 搜索区块链,以识别、定位和/或确认区块链中是否存在给定事务或区块;

[0590] 生成区块链事务,将事务写入区块链,并且/或者向区块链网络广播事务。

[0591] 条款9.16.根据前述任一项条款所述的方法,其中所述数据包包括以下各项中的至少一项:

[0592] 区块链事务的至少一部分;

[0593] 区块链区块的至少一部分;

[0594] 区块链事务脚本的至少一部分;

[0595] 记录所述数据包的区块的默克尔树;

[0596] 记录所述数据包的所述区块的默克尔根;

[0597] 默克尔路径,所述默克尔路径能够根据所述数据包的哈希来确定用于记录所述数据包的所述区块的所述默克尔根的值;

[0598] 默克尔证明;

[0599] 与区块链网络的共识机制一起使用或相关联的数据;

[0600] 权益证明或工作证明操作的结果或相关数据;

[0601] 区块标识符(block_ID),所述区块标识符与所述区块链区块相关联;

[0602] 事务标识符(TxID),所述事务标识符与所述区块链区块内多个区块链事务中的事务(Tx)相关联;

[0603] 所述区块标识符(block_ID)和所述事务标识符(TxID)的函数;

[0604] 所述区块标识符(block_ID)和所述事务标识符(TxID)的级联;

[0605] 数字签名;

[0606] 认证代码;

[0607] 签名消息,所述签名消息用于确定事务状态;

[0608] 协议标志;

[0609] 自主公钥(DPK);以及

[0610] 自主事务ID(DTxID)。

[0611] 条款9.17.根据前述任一项条款所述的方法,其中所述发送资源和/或所述接收资源包括:

[0612] 区块链网络中的节点;

[0613] 被设置为提供区块链相关服务的服务提供者;

[0614] 与金融机构相关联或由金融机构控制的计算资源;

[0615] 加密货币交换所或其组成部分;

[0616] 商家资源或其组成部分;

[0617] 数字钱包或其组成部分;

[0618] 软件组件,所述软件组件用于执行或促进简单支付验证(SPV)操作,或处理SPV操作的结果;

[0619] 网络上的MLDv1主机或MLDv2主机、网络交换机或路由器。

[0620] 条款9.18.一种计算机设备,所述计算机设备包括:

[0621] 存储器,所述存储器包括一个或多个存储器单元;以及

[0622] 处理装置,所述处理装置包括一个或多个处理单元,其中所述存储器存储被设置在所述处理装置上运行的代码,所述代码被配置为当在所述处理装置上运行时,执行根据条款9.1至9.17中任一项所述的方法。

[0623] 条款19.一种计算机程序,所述计算机程序包含在计算机可读存储器上并且被配置为当在一个或多个处理器上运行时,执行根据条款9.1至9.17中任一项所述的方法。

[0624] 条款集10:

[0625] 附加地或替代地,本公开的一个或多个实施例可以根据以下条款进行定义。条款集1至9中的任何条款集所定义的条款中的任何条款可以与本文提供的任何其他条款集中的一个或多个条款或本文公开的任何其他特征组合。

[0626] 条款10.1.一种计算机实现的方法,所述方法包括:操作用于生成、存储、处理、访问和/或维护数据包的发送资源,所述数据包优选地包括区块链相关数据;以及,通过电子网络至少部分地将所述数据包的传输从所述发送资源发送到组播群组,其中所述组播群组使得所述数据包可供最终用户使用(make available,也译为所述组播群组将所述数据包提供给最终用户)。可以通过受控访问来使得所述数据包可供使用(也译为,所述数据包可以通过受控访问来提供)。所述受控访问可以(i)通过对所述组播群组的受控访问(例如,通过订阅)和/或(ii)对数据包的受控访问来管理。受控访问可以由所述发送资源配置,例如通过实现对所述组播群组的受控访问和/或通过在传输之前保护所述数据包。

[0627] 条款10.2.根据条款10.1所述的方法,所述方法还包括:用于存储、处理、访问和/或维护所述数据包的接收资源。

[0628] 条款10.3.根据条款10.2所述的方法,其中:所述接收资源订阅(subscribe to)所述组播群组或另一组播群组以接收所述数据包或另一数据包。

[0629] 条款10.4.根据前述任一项条款所述的方法,其中:所述发送资源传输多个数据包;和/或,所述接收资源接收多个数据包。

[0630] 条款10.5.根据前述任一项条款所述的方法,其中所述数据包至少部分是数据流,例如多媒体通信信道。

[0631] 条款10.6.根据前述任一项条款所述的方法,其中所述数据包具有用于提供多个数据信道的子组件。

[0632] 条款10.7.根据前述任一项条款所述的方法,其中所述数据包和/或对所述组播群组的访问是安全的,并且可使用访问密钥和/或智能合约进行访问。

[0633] 条款10.8.根据条款10.7所述的方法,其中,需要第一访问密钥来访问所述数据包;并且,需要第二访问密钥来访问所述组播群组。

[0634] 条款10.9.根据条款10.7或10.8所述的方法,其中,所述发送资源生成所述访问密钥,并且,将所需要的访问密钥发送到所述数据包的接收者和最终用户中的至少一者以访问所述数据包。

[0635] 条款10.10.根据条款10.9所述的方法,其中所述访问密钥是在使用支付通道和/或智能合约的交换期间提供的。

[0636] 条款10.11.根据条款10.7至10.10中任一项所述的方法,其中:所述访问密钥针对以下各项中的至少一项来提供对所述组播群组和/或所述数据包的访问:(i)固定时间段,(ii)固定数量的数据,(iii)固定数量的单元,(iv)固定数量的数据包,(v)无限制访问。

[0637] 条款10.12.根据条款10.4至10.11中任一项所述的方法,其中:所述发送资源将所述多个数据包传输到相应分配地址,其中所述分配地址是根据以下各项来确定的:所述相应数据包,或,所述访问密钥;并且/或者,所述接收资源从至少一个组播群组接收所述多个数据包并聚合所述数据包。

[0638] 条款10.13.根据条款10.12所述的方法,其中所述分配地址是与接收资源群组相关联的组播地址。

[0639] 条款10.14.一种计算机实现的方法,所述方法包括:操作用于存储、处理、访问和/或维护数据包的接收资源,所述数据包优选地包括区块链相关数据;以及,通过从电子网络接收数据包的组播群组至少部分地接收数据包的传输,并作为最终用户消费所述数据包。

[0640] 条款10.15.根据条款10.14所述的方法,其中所述数据包和/或对所述组播群组的访问是安全的,并且可使用访问密钥进行访问,所述访问密钥优选地是通过支付通道获得的。

[0641] 条款10.16.根据前述任一项条款所述的方法,其中所述数据包包括以下各项中的至少一项:事务(Tx)的一部分;输出标识符;脚本的哈希;事务标识(TXID);区块链区块;区块头。例如,所述输出标识符可以是UTXO。所述脚本可以与区块链事务内提供的输出相关联。

[0642] 条款10.17.根据前述任一项条款所述的方法,其中所述数据包包括以下各项中的至少一项:

[0643] 区块链事务的至少一部分;

[0644] 区块链区块的至少一部分;

[0645] 区块链事务脚本的至少一部分;

[0646] 记录所述数据包的区块的默克尔树;

[0647] 记录所述数据包的所述区块的默克尔根;

[0648] 默克尔路径,所述默克尔路径能够根据所述数据包的哈希来确定用于记录所述数据包的所述区块的所述默克尔根的值;

[0649] 默克尔证明;

[0650] 与区块链网络的共识机制一起使用或相关联的数据;

[0651] 权益证明或工作证明操作的结果或相关数据;

[0652] 区块标识符(block_ID),所述区块标识符与所述区块链区块相关联;

[0653] 事务标识符(TxID),所述事务标识符与所述区块链区块内多个区块链事务中的事务(Tx)相关联;

[0654] 所述区块标识符(block_ID)和所述事务标识符(TxID)的函数;

[0655] 所述区块标识符(block_ID)和所述事务标识符(TxID)的级联;

[0656] 数字签名;

[0657] 认证代码;

[0658] 签名消息,所述签名消息用于确定事务状态;

[0659] 协议标志;

[0660] 自主公钥(DPK);

[0661] 自主事务ID(DTxID)。

[0662] 条款10.18.根据前述任一项条款所述的方法,其中发送资源和/或所述接收资源包括:

[0663] 区块链网络中的节点;

[0664] 被设置为提供区块链相关服务的服务提供者;

[0665] 与金融机构相关联或由金融机构控制的计算资源;

[0666] 加密货币交换所或其组成部分;

[0667] 商家资源或其组成部分;

[0668] 数字钱包或其组成部分;

[0669] 软件组件,所述软件组件用于执行或促进简单支付验证(SPV)操作,或处理SPV操作的结果;

[0670] 网络上的MLDv1主机或MLDv2主机、网络交换机或路由器。

[0671] 条款10.19.一种计算机设备,所述计算机设备包括:存储器,所述存储器包括一个或多个存储器单元;以及,处理装置,所述处理装置包括一个或多个处理单元,其中所述存储器存储被设置在所述处理装置上运行的代码,所述代码被配置为当在所述处理装置上运行时,执行根据条款10.1至10.18中任一项所述的方法。

[0672] 条款10.20.一种计算机程序,所述计算机程序包含在计算机可读存储器上并且被配置为当在一个或多个处理器上运行时,执行根据条款10.1至10.18中任一项所述的方法。

[0673] 条款集11:

[0674] 附加地或替代地,本公开的一个或多个实施例可以根据以下条款进行定义。条款

集11所定义的条款中的任何条款可以与本文提供的任何其他条款集中的一个或多个条款或本文公开的任何其他特征组合。

[0675] 所述方法可以被描述为网络安全解决方案和/或(电子)通信或数据传输解决方案。

[0676] 11.1.一种计算机实现的方法,所述方法包括:

[0677] 由发送资源,将区块链相关通信或加密货币相关通信发送到IPv6组播地址,以便由至少一个接收资源接收;

[0678] 以及/或者,

[0679] 由至少一个接收资源,接收由发送资源发送到IPv6组播地址的区块链相关通信或加密货币相关通信。

[0680] 11.2.根据条款11.1所述的方法,其中:

[0681] 所述通信是或包括区块链相关的和/或加密货币相关的警报、区块链相关的或加密货币相关的软件更新、区块链相关的或加密货币相关的通知、或其他区块链相关的或加密货币相关的通信。

[0682] 11.3.根据条款11.1或11.2所述的方法,其中:

[0683] 所述IPv6组播地址与和特定区块链网络或加密货币相关的通信相关联。

[0684] 11.4.根据前述任一项条款所述的方法,其中:

[0685] 所述至少一个接收资源包括被设置为在区块链网络上运行或与区块链网络一起运行的一个或多个挖掘、验证、钱包和/或服务提供资源。

[0686] 11.5.根据前述任一项条款所述的方法,所述方法包括以下步骤:

[0687] 响应于所述区块链相关通信或加密货币相关通信,由所述至少一个接收资源采取至少一个响应动作。所述至少一个响应动作可以包括以下各项中的一项或多项:

[0688] i)向一个或多个接收者发送通信;

[0689] ii)访问、安装和/或执行数据的一部分,可选地,其中所述数据的所述部分包括一个或多个机器可执行指令;

[0690] iii)将至少一个事务输出、事务或事务区块、或加密货币的一部分标记或识别为无效、不可花费、拒绝或予以忽略。

[0691] 11.6.根据前述任一项条款所述的方法,所述方法包括以下步骤:

[0692] 由所述至少一个接收资源,将所述通信转发到至少另一接收资源;

[0693] 可选地,其中:

[0694] 所述至少另一接收资源包括至少另一IPv6组播地址。

[0695] 11.7.根据前述任一项条款所述的方法,其中:

[0696] i)所述区块链相关通信或加密货币相关通信由被指定为通信合法来源或提供者的生成资源来签名、标记或以其他方式认证;和/或,

[0697] ii)对所述区块链相关通信或加密货币相关通信进行编码或以其他方式进行保护,使得所述区块链相关通信或加密货币相关通信的内容只能通过使用至少一种解锁机制才能访问、解码、读取、执行或处理,所述至少一种解锁机制诸如密钥、访问码或秘密。

[0698] 11.8.根据条款11.7所述的方法,所述方法包括以下步骤:

[0699] 将所述至少一个密钥、访问码或秘密提供给所述至少一个接收资源或被授权访

问、解码、读取、执行或处理所述区块链相关通信或加密货币相关通信的所述内容的另一资源。

[0700] 11.9.根据前述任一项条款所述的方法,其中所述区块链相关通信或加密货币相关通信包括过滤器代码、标志(flag)、标记(marker)或其他标识符,优选地,其中:

[0701] 所述过滤器被设置为作为根据以下项目来使所述区块链相关通信或加密货币相关通信针对(target at)/识别所述至少一个接收资源中的一个或多个接收资源的一种手段:

[0702] 正在发送的区块链相关通信或加密货币相关通信的内容或类型;和/或

[0703] 预期的、选定的或期望的接收资源集。

[0704] 11.10.根据条款11.9所述的方法,其中:

[0705] 在所述区块链相关通信或加密货币相关通信中,所述过滤器被提供于预先指定的位置和/或被以预定格式提供。

[0706] 11.11.根据条款11.9或11.10所述的方法,其中所述方法包括以下步骤:

[0707] 由所述至少一个接收资源,根据所述过滤器来处理或忽略所述区块链相关通信或加密货币相关通信。

[0708] 11.12.一种计算机设备,所述计算机设备包括:存储器,所述存储器包括一个或多个存储器单元;以及处理装置,所述处理装置包括一个或多个处理单元,其中所述存储器存储被设置在所述处理装置上运行的代码,所述代码被配置为当在所述处理装置上运行时,执行根据前述任一项条款所述的方法。

[0709] 11.13.一种计算机程序,所述计算机程序包含在计算机可读存储器上并且被配置为当在一个或多个处理器上运行时,执行根据条款11.1至11.11中任一项所述的方法。

[0710] 条款集12

[0711] 附加地或替代地,本公开的一个或多个实施例可以根据以下条款进行定义。条款集12所定义的条款中的任何条款可以与本文提供的任何其他条款集中的一个或多个条款或本文公开的任何其他特征组合。

[0712] 然而,在一个或多个实施例中,群组中的发送节点和/或接收节点中的一个、部分或全部可以是区块链网络上的全节点或覆盖网络上的节点,并且所述数据可以包括已经被验证但尚未写入区块链账本的未确认事务(其相关数据)。在此类实施例中,可以提供用于实现内存池(也称为存储池)的系统和方法,所述内存池形成区块链网络或与所述区块链网络交互的覆盖网络的一部分、在区块链网络或与所述区块链网络交互的覆盖网络中提供或关联于区块链网络或与所述区块链网络交互的覆盖网络。这在本文中可以称为“区块链覆盖网络”。根据https://wiki.bitcoinsv.io/index.php/Mining,已知“内存池是临时事务存储库,并且可以用于持有以不同方式分组的事务,例如下一个区块中要挖掘的事务、要监视的事务或由于nLocktime/nSequence锁而无法挖掘的事务。”在不受限制的情况下,本文使用的术语内存池可以包括该定义。

[0713] 在其他实施例中,可以提供用于实现UTXO集的系统和方法。

[0714] 因此,可以提供:

[0715] 条款12.1一种实现区块链网络的存储池或UTXO集的方法,所述方法包括以下步骤:

[0716] 从发送资源向至少一个接收资源发送传输;或者至少一个接收资源从发送资源接收传输,

[0717] 其中:

[0718] 所述发送资源和/或所述至少一个接收资源是网络上的节点;并且

[0719] 所述传输使用IPv6组播发送,并且包括区块链事务的至少一部分。

[0720] 在一些实施例中,区块链事务的所述至少一部分可以包括整个区块链事务。所述事务可能已经由验证实体核实(验证),所述验证实体用于根据区块链协议来验证所述事务。所述事务可能未经确认,等待成功挖掘到所述区块链账本上与所述区块链协议相关联的区块中。

[0721] 在一些实施例中,区块链事务的所述至少一部分可以包括UTXO。

[0722] 条款12.2根据条款12.1所述的方法,其中:

[0723] i)所述发送资源和/或所述至少一个接收资源是区块链网络上的全或轻节点;或者

[0724] ii)所述发送资源和/或所述至少一个接收资源是区块链覆盖网络上的节点。

[0725] 示例性系统概述

[0726] 仅出于说明目的并且参考图1至图4,现在提供可以在其中实施本公开的一个或多个实施例的计算环境的示例。下面提到的附图标记是指图1至图4。

[0727] 图1示出了一种用于实现区块链150的示例性系统100。系统100可以包括包交换网络(packet-switched network,也译为分组交换网络)101,通常是诸如互联网的广域互联网。包交换网络101包括多个区块链节点104,该多个区块链节点可以被设置成在包交换网络101内形成对等(P2P)网络106。虽然未示出,但是区块链节点104可以被设置为近完全图。因此,每个区块链节点104高度连接到其它区块链节点104。

[0728] 每个区块链节点104包括对等体的计算机设备,不同的节点104属于不同的对等体。每个区块链节点104包括处理装置,该处理装置包括一个或多个处理器,例如一个或多个中央处理单元(CPU)、加速器处理器、专用处理器和/或现场可编程门阵列(FPGA),以及其它设备,例如专用集成电路(ASIC)。每个节点还包括存储器,即采用非暂时性计算机可读介质形式的计算机可读存储器。存储器可包括一个或多个存储器单元,其采用一个或多个存储器介质,例如诸如硬盘等磁介质、诸如固态硬盘(SSD)、闪存或电可擦可编程只读存储器(EEPROM)等电子媒介和/或诸如光盘驱动器等光学介质。

[0729] 区块链150包括一系列数据区块151,其中在分布式或区块链网络106中的多个区块链节点104中的每个节点处维护区块链150的相应副本。如上所述,维护区块链150的副本不一定意味着完全存储区块链150。相反,只要每个区块链节点150存储每个区块151的区块头(下面讨论),区块链150就可以进行数据修剪。区块链中的每个区块151均包括一个或多个事务152,其中该上下文中的事务是指一种数据结构。数据结构的性质将取决于用作事务模型或计划的一部分的事务协议类型。给定的区块链全程使用一个特定的事务协议。在一种常见的事务协议中,每个事务152的数据结构至少包括一个输入和至少一个输出。每个输出指定将数字资产的数量表示为财产的数额,其一个示例是输出被密码锁定到的用户103(需要该用户的签名或其它解进行解锁,从而进行赎回或花费)。每个输入指向先前事务152的输出,从而链接这些事务。

[0730] 每个区块151还包括区块指针155,其指向区块链中先前创建的区块151,以定义区块151的顺序。每个事务152(除coinbase事务之外)包括指向先前事务的指针,以定义事务序列的顺序(注:事务152的序列可进行分支)。区块151的区块链一直追溯到创始区块(Gb)153,该创始区块是区块链中的第一区块。区块链150中早期的一个或多个原始事务152指向创始区块153,而非先前事务。

[0731] 每个区块链节点104被配置为将事务152转发到其它区块链节点104,从而使得事务152在整个网络106中传播。每个区块链节点104被配置为创建区块151,并将相同区块链150的相应副本存储在其相应的存储器中。每个区块链节点104还维护等待并入到区块151中的事务152的有序集(或"池")154。有序池154通常称为"内存池"。在本文中,该术语并不意在限制于任何特定的区块链、协议或模型。该术语是指节点104已接受为有效的有序事务集,并且对于该有序事务集,强制节点104不接受试图花费相同输出的任何其它事务。

[0732] 在给定的当前事务152j中,输入(或每个输入)包括指针,该指针引用事务序列中先前事务152i的输出,指定该输出将在当前事务152j中被赎回或"花费"。通常,先前事务可以是有序集154或任何区块151中的任何事务。尽管为了确保当前事务有效,将需要存在先前事务152i并核实其有效,但是在创建当前事务152j甚至向网络106发送当前事务152j时,不必存在先前事务152i。因此,在本文中,"先前"是指由指针链接的逻辑序列中的前任,而不一定是时间序列中的创建时间或发送时间,因此,不一定排除无序创建或发送事务152i、152j的情况(参见下面关于孤立事务的讨论)。先前事务152i同样可以称为先行事务或前任事务。

[0733] 当前事务152j的输入还包括输入授权,例如先前事务152i的输出被锁定到的用户103a的签名。反过来,当前事务152j的输出可以加密锁定到新用户或实体103b。因此,当前事务152j可将先前事务152i的输入中定义的数额转移到当前事务152j的输出中定义的新用户或实体103b。在某些情况下,事务152可具有多个输出,以在多个用户或实体间分割输入数额(其中一个可以是原始用户或实体103a,以便进行变更)。在某些情况下,事务还可以具有多个输入,将一个或多个先前事务的多个输出中的数额汇总在一起,并重新分配到当前事务的一个或多个输出。

[0734] 根据基于输出的事务协议,例如比特币,当诸如个体用户或组织这类的一方103希望颁布新的事务152j时(由该方采用的自动程序或人为地),该颁布方将该新事务从其计算机终端102发送到接收者。颁布方或接收者将最终向网络106的一个或多个区块链节点104(现在通常是服务器或数据中心,但原则上也可以是其它用户终端)发送该事务。另外还不排除颁布新事务152j的一方103可以将事务直接发送到一个或多个区块链节点104,并且在一些示例中,可以不将事务发送到接收者。接收事务的区块链节点104根据在每个区块链节点104处应用的区块链节点协议来检查事务是否有效。区块链节点协议通常要求区块链节点104检查新事务152j中的加密签名是否与预期签名相匹配,这取决于事务152的有序序列中的先前事务152i。在这种基于输出的事务协议中,这可以包括检查新事务152j的输入中包括的一方103的密码签名或其它授权是否与新事务分配的先前事务152i的输出中定义的条件匹配,其中该条件通常包括至少检查新事务152j的输入中的密码签名或其它授权是否解锁新事务的输入所链接到的先前事务152i的输出。条件可以至少部分地由包括在先前事务152i的输出中的脚本来定义。或者,这可仅由区块链节点协议单独确定,或可通过其组合

确定。无论采用哪种方式,如果新事务152j有效,区块链节点104会将其转发到区块链网络106中的一个或多个其它区块链节点104。这些其它区块链节点104根据相同的区块链节点协议应用相同的测试,并因此将新事务152j转发到一个或多个其它节点104等等。通过这种方式,新事务在区块链节点104的整个网络中进行传播。

[0735] 在基于输出的模型中,给定输出(例如,UTXO)是否分配(例如,花费)的定义是,根据区块链节点协议,其是否通过另一个随后事务152j的输入有效赎回。事务有效的另一个条件是其试图赎回的先前事务152i的输出尚未被另一个事务赎回。同样,如果无效,则事务152j将不会在区块链150中传播(除非被标记为无效并且被传播用于提醒)或记录。这可防止重复花费,即事务处理者对同一个事务的输出分配超过一次。另一方面,基于账户的模型通过保持账户余额防止重复花费。因为同样存在定义的事务顺序,账户余额在任何时候均具有单一定义的状态。

[0736] 除了核实事务有效之外,区块链节点104还争相成为在通常称为挖掘的过程中创建事务区块的第一个节点,而该过程由“工作证明”支持。在区块链节点104处,新事务被添加到尚未出现在记录在区块链150上的区块151中的有效事务的有序池154。然后,区块链节点争相通过尝试解决加密难题以组装有序事务集154中事务152的新有效事务区块151。通常情况下,这包括搜索“随机数”值,从而当随机数与未决事务有序池154的表示并置且进行哈希处理时,哈希值的输出满足预定条件。例如,预定条件可以是哈希值的输出具有某个预定义的前导零数。注意,这仅仅是一种特定类型的工作证明难题,并且不排除其它类型。哈希函数的特性是,相对于其输入,其具有不可预测的输出。因此,该搜索只能通过强力执行,从而在试图解决难题的每个区块链节点104处消耗大量的处理资源。

[0737] 解决难题的第一区块链节点104在网络106上宣布难题解决,提供解决方案作为证明,然后网络中的其它区块链节点104则可以轻松检查该解决方案(一旦给出哈希值的解决方案,就可以直接检查该解决方案是否使哈希值的输出满足条件)。第一区块链节点104将一个区块传播到接受该区块的其它节点达成阈值共识,从而执行协议规则。然后,有序事务集154被每个区块链节点104记录为区块链150中的新区块151。区块指针155还分配给指向该区块链中先前创建的区块151n-1的新区块151n。创建工作证明解所需的大量工作(例如采用哈希的形式)发出信号通知第一节点104的意图以遵循区块链协议。这些规则包括如果它分配与先前核实有效的事务相同的输出,则不接受事务为有效,否则称之为重复花费。一旦创建,区块151就不能修改,因为它在区块链网络106中的每个区块链节点104处进行标识和维护。区块指针155还向区块151施加顺序。由于事务152记录在网络106中每个区块链节点104处的有序区块中,因此提供了事务的不可改变公共分类账。

[0738] 应当注意的是,在任何给定时间争相解决难题的不同区块链节点104可以基于在任何给定时间尚未发布的事务的池154的不同快照来这样做,具体取决于它们何时开始搜索解或接收事务的顺序。解决相应难题的人员首先定义新区块151n中包括的事务152及其顺序,并且更新当前的未发布事务池154。然后,区块链节点104继续争相从新定义的未发布事务有序池154中创建区块,等等。此外,还存在解决可能出现的任何“分叉”的协议,其中两个区块链节点104彼此在很短的时间内解决难题,从而在节点104之间传播区块链的冲突视图。简言之,分叉方向最长的成为最终区块链150。应当注意的是,这不会影响网络的用户或代理,因为同一事务将出现在两个分叉中。

[0739] 根据比特币区块链(和大多数其它区块链),成功构造新区块104的节点被授予在分配附加限定数量数字资产的新特殊类型事务中新分配附加的、接受的数额的数字资产的能力(与代理间或用户间事务相反,该事务将一定数量的数字资产从一个代理或用户转移到另一个代理或用户)。这种特殊类型的事务通常称为“coinbase事务”,但是也可以称为“启动事务”或“产生事务”。它通常形成新区块151n的第一事务。工作证明发出信号通知构造新区块的节点的意图以遵循协议规则,从而允许稍后赎回该特定事务。在可以赎回该特殊事务之前,区块链协议规则可能需要成熟期,例如100个区块。通常,常规(非生成)事务152还将在其输出中的一个输出中指定附加事务费用,以进一步奖励创建其中发布该事务的区块151n的区块链节点104。该费用通常称为“事务费用”,并在下文中讨论。

[0740] 由于事务核实和发布中涉及的资源,通常至少每个区块链节点104采用包括一个或多个物理服务器单元的服务器的形式,或者甚至整个数据中心。但是,原则上来说,任何给定区块链节点104均可采用一个用户终端或联网在一起的一组用户终端的形式。

[0741] 每个区块链节点104的存储器均存储被配置为在区块链节点104的处理装置上运行的软件,以根据区块链节点协议执行其相应的角色并处理事务152。应当理解的是,在本文中归因于区块链节点104的任何动作均可通过在相应计算机设备的处理装置上运行的软件执行。节点软件可以在应用层或诸如操作系统层或协议层的较低层或这些层任意组合的一个或多个应用中实现。

[0742] 扮演消费用户角色的多方103中的每一方的计算机设备102也连接到网络101。这些用户可以与区块链网络106交互,但不参与核实事务或构造区块。其中一些用户或代理103可以充当事务中的发送者和接收者。其它用户可以与区块链150交互,而不必充当发送者或接收者。例如,一些当事方可以充当存储区块链150的副本(例如,已经从区块链节点104获得区块链的副本)的存储实体。

[0743] 各方103中的一些或所有当事方可以作为不同网络的一部分连接,例如覆盖在区块链网络106之上的网络。区块链网络的用户(经常称为“客户端”)可以被称为是包含区块链网络106的系统的一部分;然而,这些用户不是区块链节点104,因为它们不执行区块链节点所需的角色。相反,每一方103可以与区块链网络106交互,从而通过连接到区块链节点106(即,与区块链节点106通信)来利用区块链150。出于说明目的,示出了双方103及其相应的设备102:第一方103a及其相应的计算机设备102a,以及第二方103b及其相应的计算机设备102b。应当理解的是,更多此类当事方103及其相应的计算机设备102可能存在并参与系统100,但为了方便起见,未进行说明。每一方103均可以是个人或组织。仅出于说明目的,在本文中,第一方103a称为爱丽丝,第二方103b称为鲍勃,但应当理解的是,这并不仅限于爱丽丝或鲍勃,且本文对爱丽丝或鲍勃的任何引用均可分别用“第一方”和“第二方”替换。

[0744] 每一方103的计算机设备102包括相应的处理装置,其包括一个或更多个处理器,例如一个或更多个CPU、图形处理单元(GPU)、其他加速器处理器、特定应用程序处理器和/或FPGA。每一方103的计算机设备102还包括存储器,即采用非暂时性计算机可读介质形式的计算机可读存储器。该存储器可包括一个或更多个存储器单元,其采用一个或更多个存储器介质,例如诸如硬盘等磁介质、诸如SSD、闪存或EEPROM等电子媒介和/或诸如光盘驱动器等的光学介质。每一方103的计算机设备102上的存储器存储软件,其包括被设置为在处理装置上运行的至少一个客户端应用程序105的相应实例。应当理解的是,在本文中归因于

给定方103的任何行动均可通过在相应计算机设备102的处理装置上运行的软件执行。每一方103的计算机设备102包括至少一个用户终端,例如台式或笔记本电脑、平板电脑、智能手机或诸如智能手表等的可穿戴设备。给定方103的计算机设备102还可包括一个或更多个其他网络资源,诸如通过用户终端访问的云计算资源。

[0745] 客户端应用程序105最初可通过例如从服务器下载的适当计算机可读存储介质,或通过诸如可移动SSD、闪存密钥、可移动EEPROM、可移动磁盘驱动器、软盘或磁带等的可移动存储设备、诸如CD或DVD ROM等的光盘或可移动光驱等提供至任何给定方103的计算机设备102。

[0746] 客户端应用程序105至少包括“钱包”功能。这有两个主要功能。其中一个功能是使相应方103能够创建、授权(例如签名)事务152并将其发送到一个或多个比特币节点104,然后在区块链节点104的网络中传播,从而包括在区块链150中。另一个功能是向相应方汇报其目前拥有的数字资产数额。在基于输出的系统中,该第二功能包括整理分散在区块链150中属于相关方的各种事务152的输出中定义的数额。

[0747] 注意:虽然各种客户端功能可以描述为集成到给定客户端应用程序105中,但这不一定是限制性的,相反,在本文中所描述的任何客户端功能可以在由两个或更多个不同应用程序组成的套件中实现,例如经由API进行接口连接或一个应用程序作为另一个应用程序的插件。更通俗地说,客户端功能可以在应用层或诸如操作系统的较低层或这些层的任意组合实现。下面将根据客户端应用程序105进行描述,但应当理解的是,这不是限制性的。

[0748] 每个计算机设备102上的客户端应用程序或软件105的实例可操作地耦合到网络106的区块链节点104中的至少一个。这可以启用客户端105的钱包功能,以将事务152发送至网络106。客户端105还可联络区块链节点104,以在区块链150中查询相应方103作为接收者的任何事务(或实际上在区块链150中检查其它方的事务,因为在实施例中,区块链150是在某种程度上通过其公开可见性提供事务信任的公共设施)。每个计算机设备102上的钱包功能被配置为根据事务协议制定和发送事务152。如上所述,每个区块链节点104运行软件,该软件被配置为根据区块链节点协议核实事务152并转发事务152以便在区块链网络106中传播。事务协议和节点协议相互对应,给定事务协议和给定节点协议一起实现给定的事务模型。相同的事务协议用于区块链150中的所有事务152。网络106中的所有节点104使用相同的节点协议。

[0749] 当给定方103(比方说爱丽丝)希望发送拟包含在区块链150中的新事务152j时,她将根据相关事务协议(使用其客户端应用程序105中的钱包功能)制定新事务。然后,她将事务152从客户端应用程序105发送到她所连接的一个或多个区块链节点104。例如,这可能是与爱丽丝的计算机102最佳连接的区块链节点104。当任何给定区块链节点104接收新事务152j时,其将根据区块链节点协议及其相应的角色进行处理。这包括首先检查新接收的事务152j是否满足变为“有效”的特定条件,具体示例稍后将详细讨论。在一些事务协议中,有效条件可通过事务152中包含的脚本在每个事务的基础上进行配置。或者,条件可仅仅是节点协议的内置功能,或通过组合脚本和节点协议进行定义。

[0750] 如果新接收的事务152j通过有效性测试(即:“有效”的条件下),接收事务152j的任何区块链节点104将向在区块链节点104处维护的有序事务集154中添加新的核实有效事务152。进一步地,接收事务152j的任何区块链节点104随后将核实有效事务152传播至网络

106中的一个或多个其它区块链节点104。由于每个区块链节点104应用相同的协议,因此假定事务152j有效,这意味着事务很快将在整个网络106中传播。

[0751] 一旦进入在给定区块链节点104处维护的未决事务有序池154,该区块链节点104将开始争相解决其各自的包含新事务152的池154的最新版本上的工作证明难题(请记住,其它区块链节点104可以尝试基于不同的事务池154来解决难题。但是,首先解决难题的人将定义包括在最新区块151中的事务集合。最终,区块链节点104将解决有序池154的一部分的难题,该有序集154包括爱丽丝的事务152j)。一旦包括新事务152j的池154完成工作证明,其将不可变地成为区块链150中区块151中的一个区块的一部分。每个事务152包括指向早前事务的指针,因此事务的顺序也被不可变地记录下来。

[0752] 不同的区块链节点104可以首先接收给定事务的不同实例,并且因此在一个实例被发布到新区块151中之前具有关于哪个实例"有效"的冲突视图,此时所有区块链节点104同意所发布的实例是唯一的有效实例。如果区块链节点104将一个实例接受为有效实例,然后发现第二实例已记录在区块链150中,则区块链节点104必须接受这一点,并将丢弃(即,视为无效)其最初接受的实例(即,在区块151中尚未公布的实例)。

[0753] 作为基于账户的事务模型的一部分,由一些区块链网络操作的另一种类型的事务协议可称为"基于账户的"协议。在基于账户的情况下,每个事务均不通过参考过去事务序列中先前事务的UTXO来定义转移的数额,而是通过参考绝对账户余额进行定义。所有账户的当前状态由网络的节点单独存储到区块链中,并不断更新。在此类系统中,事务使用账户的运行事务记录(也称为"头寸")进行排序。该值由发送者签名作为其加密签名的一部分,并作为事务引用计算的一部分进行哈希处理。此外,可选的数据字段也可以在事务中签名。例如,如果数据字段中包含先前事务的ID,该数据字段可指向先前事务。

[0754] 基于UTXO的模型

[0755] 图2示出了示例性事务协议。这是基于UTXO的协议的示例。事务152(简称"Tx")是区块链150的基本数据结构(每个区块151包括一个或多个事务152)。下面将通过参考基于输出或基于"UTXO"的协议进行描述。但这并不限于所有可能的实施例。应当注意的是,虽然参考比特币描述了示例性基于UTXO的协议,但是它同样可以在其它示例区块链网络上实现。

[0756] 在基于UTXO的模型中,每个事务("Tx")152包括数据结构,其包括一个或多个输入202和一个或多个输出203。每个输出203可包括未花费事务输出(UTXO),其可用作另一新事务的输入202的来源(如果UTXO尚未赎回)。UTXO包括指定数字资产数额的值。这表示分布式分类账上的一组令牌。UTXO还可包含其来源事务的事务ID以及其它信息。事务数据结构还可包括标头201,其可包括输入字段202和输出字段203的大小指示符。标头201还可包括事务的ID。在实施例中,事务ID是事务数据(不含事务ID本身)的哈希值,且存储在提交至节点104的原始事务152的标头201中。

[0757] 比方说爱丽丝103a希望创建转移相关数字资产数额至鲍勃103b的事务152j。在图2中,爱丽丝的新事务152j标记为"Tx_1"。该新事务获取在序列中先前事务152i的输出203中锁定至爱丽丝的数字资产数额,并至少将此类数额中的一部分转移至鲍勃。在图2中,先前事务152i标记为"Tx_0"。Tx_0和Tx_1只是任意的标记,其不一定意味着Tx_0指区块链151中的第一事务且Tx_1指池154中的后续事务。Tx_1可指向仍具有锁定至爱丽丝的未花费输出203的任

何先前(即先行)事务。

[0758] 当爱丽丝创建其新事务Tx_1时,或至少在她将该新事务发送至网络106时,先前事务Tx_0可能已经有效并包括在区块链150的区块151中。该事务此时可能已包括在区块151中的一个区块中,或者可能仍在有序集154中等待,在这种情况下,该事务将很快包括在新区块151中。或者,Tx_0和Tx_1可以创建并一起发送至网络106;或者,如果节点协议允许缓冲"孤立"事务,Tx_0甚至可以在Tx_1之后发送。本文事务序列上下文中使用的"先前"和"后续"一词是指由事务中指定的事务指针定义的序列中的事务顺序(哪个事务指向哪个其他事务等等)。它们同样可以替换为"前任"和"继任"、"先行"和"后代"或"父项"和"子项"等。这不一定指其创建、发送至网络106或到达任何给定区块链节点104的顺序。然而,指向先前事务(先行事务或"父事务")的后续事务(后代事务或"子事务")不会有效除非父事务有效。在父事务之前到达区块链节点104的子事务被视为孤立事务。根据节点协议和/或节点行为,其可被丢弃或缓冲一段时间,以等待父事务。

[0759] 先前事务Tx_0的一个或更多个输出203中的一个包括特定的UTXO,标记为$UTXO_0$。每个UTXO包括指定UTXO表示的数字资产数额的值以及锁定脚本,该锁定脚本定义后续事务的输入202中的解锁脚本必须满足的条件,以使后续事务有效,从而成功赎回UTXO。通常情况下,锁定脚本将数额锁定至特定方(该数额的事务的受益人)。即,锁定脚本定义解锁条件,该解锁条件通常包括以下条件:后续事务的输入中的解锁脚本包括先前事务被锁定到的一方的加密签名。

[0760] 锁定脚本(亦称scriptPubKey)是节点协议识别的域特定语言中写入的一段代码。此类语言的特定示例称为"脚本(Script)"(S大写),其可由区块链网络所使用。锁定脚本指定花费事务输出203所需的信息,例如爱丽丝签名的要求。解锁脚本出现在事务的输出中。解锁脚本(亦称scriptSig)是提供满足锁定脚本标准所需信息的域特定语言中写入的一段代码。例如,其可包含鲍勃的签名。解锁脚本出现在事务的输入202中。

[0761] 因此在示出的示例中,Tx_0的输出203中的$UTXO_0$包括锁定脚本[Checksig P_A],该锁定脚本需要爱丽丝的签名Sig P_A,以赎回$UTXO_0$(严格来说,是为了使试图赎回$UTXO_0$的后续事务有效)。[Checksig P_A]包含爱丽丝的公私密钥对中的公钥P_A的表示(即哈希)。Tx_1的输入202包括指向Tx_1的指针(例如,通过其事务ID($TxID_0$),其在实施例中是整个事务Tx_0的哈希值)。Tx_1的输入202包括在Tx_0中标识$UTXO_0$的索引,以在Tx_0的任何其他可能输出中对其进行标识。Tx_1的输入202进一步包括解锁脚本<Sig P_A>,该解锁脚本包括爱丽丝的加密签名,该签名由爱丽丝通过将其密钥对中的私钥应用于预定的部分数据(有时在密码学中称为"消息")创建。爱丽丝需要签名以提供有效签名的数据(或"消息")可通过锁定脚本、节点协议或其组合进行定义。

[0762] 当新事务Tx_1到达区块链节点104时,该节点应用节点协议。这包括一起运行锁定脚本和解锁脚本,以检查解锁脚本是否满足锁定脚本中定义的条件(其中该条件可包括一个或更多个标准)。在实施例中,这涉及并置两个脚本:

[0763] <Sig PA><PA>||[Checksig PA]

[0764] 其中"||"表示并置,"<…>"表示将数据放在堆栈上,"[…]"表示由锁定脚本组成的函数(在该示例中指基于堆栈的语言)。同样,脚本可以使用公共堆栈一个接一个地运行,而不是并置脚本。无论采用哪种方式,当一起运行时,脚本使用爱丽丝的公钥P_A(包括在Tx_0

的输出的锁定脚本中),以认证Tx_1的输入中的解锁脚本是否包含爱丽丝签名预期部分的数据时的签名。也需要包括预期的部分数据本身(“消息”),以便执行此认证。在实施例中,签名的数据包括整个Tx_1(因此不需要包括一个单独的元素来明文指定签名的部分数据,因为其本身便已存在)。

[0765] 本领域技术人员将熟悉通过公私密码进行认证的细节。基本上而言,如果爱丽丝已使用其私钥加密签署消息,则给定爱丽丝的公钥和明文中的消息,诸如节点104等其它实体能够认证:消息必须已经由爱丽丝签名。签署通常包括对消息进行哈希,签署哈希值和将此标记到消息作为签名,从而使公钥的任何持有者能够认证签名。因此,应当注意的是,在实施例中,在本文中对签名特定数据片段或事务部分等的任何引用可以意味着对该数据片段或事务部分的哈希值进行签名。

[0766] 如果Tx_1中的解锁脚本满足Tx_0的锁定脚本中指定的一个或多个条件(因此,在所示示例中,如果在Tx_1中提供了爱丽丝的签名并进行认证),则区块链节点104认为Tx_1有效。这意味着区块链节点104会将Tx_1添加到待定事务有序池154。区块链节点104还会将事务Tx_1转发到网络106中的一个或多个其它区块链节点104,以便其会在整个网络106中传播。一旦Tx_1有效并包括在区块链150中,这会将$UTXO_0$从Tx_0定义为已花费。应当注意的是,Tx_1仅在花费未花费事务输出203时才有效。如果其试图花费另一事务152已经花费的输出,则即使满足所有其它条件,Tx_1也将无效。因此,区块链节点104还需要检查先前事务Tx_0中引用的UTXO是否已经花费(即,其是否已经形成另一有效事务的有效输入)。这是为何区块链150对事务152施加定义的顺序很重要的原因之一。在实践中,给定区块链节点104可维护单独的数据库,标记已花费事务152的UTXO 203,但最终定义UTXO是否已花费取决于是否在区块链150中形成了另一有效事务的有效输入。

[0767] 如果给定事务152的所有输出203中指定的总数额大于其所有输入202所指向的总数额,则这是大多数事务模型中的另一失效依据。因此,此类事务不会传播或包括在区块151中。

[0768] 请注意,在基于UTXO的事务模型中,给定UTXO需要作为一个整体使用。不能“留下”UTXO中定义为已花费的一部分数额,而同时又花费另一部分。但UTXO的数额可以在后续事务的多个输出之间分割。例如,Tx_0的$UTXO_0$中定义的数额可以在Tx_1中的多个UTXO之间分割。因此,如果爱丽丝不想将$UTXO_0$中定义的所有数额都给鲍勃,她可以使用剩余部分在Tx_1的第二输出中自己找零,或者支付给另一方。

[0769] 在实践中,爱丽丝通常还需要包括用于比特币节点104的费用,该比特币节点104在区块151中成功包含爱丽丝的事务104。如果爱丽丝未包括此类费用,则Tx_0可能会被区块链节点104拒绝,并且因此尽管在技术上有效,但可能不会传播并且包括在区块链150中(如果区块链节点104不希望接受事务152,节点协议不强迫区块链节点104接受)。在一些协议中,事务费用不需要其自身的单独输出203(即不需要单独的UTXO)。相反,输入202指向的总数额与给定事务152的输出203指定的总数额之间的任何差额都将自动提供给发布事务的区块链节点104。例如,假设指向$UTXO_0$的指针是Tx_1的唯一输入,并且Tx_1仅具有一个输出$UTXO_1$。如果在$UTXO_0$中指定的数字资产数额大于在$UTXO_1$中指定的数额,则可以由赢得工作证明竞赛以创建包含$UTXO_1$的区块的节点104分配该差值。替代地或附加地,这不一定排除可以在其自身事务152的其中一个UTXO 203中明确指定事务费用。

[0770] 爱丽丝和鲍勃的数字资产由区块链150中任何位置的任何事务152中的锁定至他们的UTXO组成。因此,通常情况下,给定方103的资产分散在整个区块链150的各种事务152的UTXO中。区块链150中的任何位置均未存储定义给定方103的总余额的一个数字。客户端应用程序105的钱包功能的作用是将锁定至相应方且在其它随后事务中尚未花费的各种UTXO值整理在一起。为实现这一点,其可以查询存储在任何一个比特币节点104处的区块链150的副本。

[0771] 应当注意的是,脚本代码通常用示意图表示(即使用非精确语言)。例如,可以使用操作码(opcode)来表示特定功能。“OP_...”是指脚本语言的特定操作码。举例来说,OP_RETURN是脚本语言操作码,当在锁定脚本的开始处在操作码前加上OP_FALSE时,操作码创建事务的不可花费输出,该输出可以在事务内存储数据,从而将数据不可改变地记录在区块链150中。例如,数据可包括需存储在区块链中的文件。

[0772] 通常,事务的输入包含对应于公钥PA的数字签名。在实施例中,这基于使用椭圆曲线secp256k1的ECDSA。数字签名对特定的数据段进行签名。在实施例中,对于给定事务,签名将对部分事务输入以及部分或全部事务输出进行签名。对输出的特定部分进行签名取决于SIGHASH标志。SIGHASH标志通常是包含在签名末尾的4字节代码,用于选择签名的输出(并因此在签名时固定)。

[0773] 锁定脚本有时称为“scriptPubKey”,指其通常包括相应事务被锁定到的当事方的公钥。解锁脚本有时称为“scriptSig”,指其通常提供相应的签名。但是更通俗地说,在区块链150的所有应用中,UTXO赎回的条件并不一定包括对签名进行验证。更通俗地说,脚本语言可用于定义任何一个或多个条件。因此,可以优选更为通用的术语“锁定脚本”和“解锁脚本”。

[0774] 侧信道

[0775] 如图1所示,爱丽丝和鲍勃的计算机设备102a、120b中的每个计算机设备上的客户端应用程序都可以包括附加通信功能。此附加功能可使爱丽丝103a建立与鲍勃103b的单独侧信道107(在任何一方或第三方的鼓动下)。侧信道107使得能够脱离区块链网络交换数据。此类通信有时称为“链下off-chain”通信。例如,这可用于在爱丽丝与鲍勃之间交换事务152,而不将该事务(尚未)注册到区块链网络106上或将其发布到链150上,直到其中一方选择将其广播到网络106上。以这种方式共享事务有时称为共享“事务模板transaction template”。事务模板可能缺少形成完整事务所需的一个或多个输入和/或输出。替代地或附加地,侧信道107可用于交换任何其它事务相关数据,例如密钥、议付数额或条款、数据内容等。

[0776] 通过与区块链网络106相同的包交换网络101可建立侧信道107。替代地或附加地,侧信道301可以经由诸如移动蜂窝网络的不同网络或者诸如无线局域网络的局域网建立,甚至经由爱丽丝和鲍勃的设备102a、102b之间的直接有线或无线链路建立。通常,在本文中任何地方所指的侧信道107可以包括经由一项或多项联网技术或通信介质的任何一条或多条链路,这些链路用于“链下”交换数据,即脱离区块链网络106交换数据。在使用多条链路的情况下,链下链路束或集合整体上可以称为侧信道107。因此,应当注意的是,如果说爱丽丝和鲍勃通过侧信道107交换某些信息或数据等,则这不一定意味着所有这些数据都必须通过完全相同的链路或甚至相同类型的网络发送。

[0777] 客户端软件

[0778] 图3A示出了用于实现本公开方案的实施例的客户端应用程序105的示例性实施方式。客户端应用程序105包括事务引擎401和用户界面(UI)层402。根据上文讨论的方案以及稍后将进一步详细讨论的内容,事务引擎401被配置为实现客户端105的基础事务相关功能,诸如制定事务152,通过侧信道301接收和/或发送事务和/或其他数据,和/或发送事务至一个或更多个节点104以通过区块链网络106传播。

[0779] 该UI层402被配置为通过相应用户的计算机设备102的用户输入/输出(I/O)方式呈现用户界面,包括通过设备102的用户输出方式向相应用户103输出信息,和通过设备102的用户输入方式接收来自相应用户103的输入。例如,用户输出方式可包括提供视觉输出的一个或显示多个屏(触摸或非触摸屏)、提供音频输出的一个或更多个扬声器、和/或提供触觉输出的一个或更多个触觉输出设备等。用户输入方式可包括例如一个或更多个触摸屏的输入阵列(可与用于输出方式的那个/那些相同或不同);一个或更多个基于光标的设备,诸如鼠标、轨迹板或轨迹球;一个或更多个麦克风和语音或声音识别算法,用于接收语音或声音输入;一个或更多个基于手势的输入设备,用于接收手动或身体手势形式的输入;或者一个或更多个机械按钮、开关或控制杆等。

[0780] 注:虽然本文中的各种功能可以被描述为集成到同一客户端应用程序105中,但这并不一定构成限制,相反,它们可以在两个或更多个不同应用程序组成的一套程序中实现,例如一个应用程序作为另一个应用程序的插件或经由API(应用程序编程接口)进行接口。比如,事务引擎401的功能可以在单独的应用程序中实现,而不是在UI层402中实现,或者诸如事务引擎401的给定模块的功能可以在多个应用程序之间分割。同时,也不排除部分或全部描述的功能可以在比如操作系统层实现。在本文任何位置引用单个或给定应用程序105或诸如此类的情况下,应当理解的是这只是作为示例,并且更通俗地说,所描述的功能可以在任何形式的软件中实现。

[0781] 图3B给出了用户界面(UI)500的示例的模型,该UI可由客户端应用程序105a的UI层402在爱丽丝的设备102a上呈现。应当理解的是,类似的UI可以由客户端105b在鲍勃的设备102b或任何其他方的设备上呈现。

[0782] 通过图示的方式,图3B从爱丽丝的角度示出了UI 500。该UI 500可包括一个或更多个UI元素501、502、503,该一个或更多个UI元素通过用户输出方式呈现为不同的UI元素。

[0783] 例如,UI元素可包括一个或更多个用户可选择的元素501,这些元素可以是屏幕上的不同按钮、菜单中的不同选项或者诸如此类。用户输入方式被设置成使用户103(在这种情况下为爱丽丝103a)能够选择或以其它方式操作其中一个选项,诸如通过点击或触摸屏幕上的UI元素,或者说出所需选项的名称(注:本文使用的“手动”一词仅用于与自动进行对比,而不一定限于用手执行操作)。

[0784] 替代地或附加地,UI元素可包括一个或更多个数据输入字段502。这些数据输入字段通过用户输出方式呈现,例如屏幕上,并且数据可通过用户输入方式输入到字段中,例如键盘或触摸屏。或者,数据可以例如基于语音识别口头地接收。

[0785] 替代地或附加地,UI元素可包括向用户输出信息的一个或更多个信息元素503。例如,这/这些可以在屏幕上呈现或可听见。

[0786] 应当理解的是,呈现各种UI元素、选择选项和输入数据的特定方式并不重要。这些

UI元素的功能稍后将进行更详细地讨论。还应当理解的是,图3中示出的UI 500只是一个图示模型,在实践中,它可包括一个或更多个进一步的UI元素,为了简洁起见,未对其进行说明。

[0787] 节点软件

[0788] 图4示出了在基于UTXO或基于输出的模型的示例中,在网络106的每个区块链节点104上运行的节点软件450的示例。应当注意的是,另一实体可以运行节点软件450,而不被分类为网络106上的节点104,即,不执行节点104所需的动作。节点软件450可以包含但不限于协议引擎451、脚本引擎452、堆栈453、应用级决策引擎454以及一个或多个区块链相关功能模块455的集合。每个节点104可以运行节点软件,该节点软件包含但不限于以下所有三个:共识模块455C(例如,工作证明)、传播模块455P和存储模块455S(例如,数据库)。协议引擎401通常被配置为识别事务152的不同字段,并根据节点协议处理此类字段。当接收到具有指向另一先前事务152i(Tx_{m-1})的输出(例如,UTXO)的输入的事务152j(Tx_j)时,协议引擎451标识Tx_j中的解锁脚本并将其传递给脚本引擎452。协议引擎451还基于Tx_j的输入中的指针来标识和检索Tx_i。Tx_i可以在区块链150上发布,在这种情况下,协议引擎可以从存储在节点104处的区块链150的区块151的副本中检索Tx_i。或者,Tx_i还可以在区块链150上发布。在这种情况下,协议引擎451可以从节点104维护的未发布有序事务集154中检索Tx_i。无论采用哪种方式,脚本引擎451都会标识Tx_i的引用输出中的锁定脚本,并将其传递给脚本引擎452。

[0789] 因此,脚本引擎452具有Tx_i的锁定脚本和来自Tx_j的相应输入的解锁脚本。例如,在图2中示出了事务标记的Tx_0和Tx_1,但是同样的事务也可以应用于任何事务对。如前所述,脚本引擎452一起运行两个脚本,这将包括根据所使用的基于堆栈的脚本语言(例如脚本)将数据放置到堆栈453上和从堆栈453检索数据。

[0790] 通过同时运行脚本,脚本引擎452确定解锁脚本是否满足锁定脚本中定义的一个或多个标准,即解锁脚本是否对包括锁定脚本的输出进行解锁?脚本引擎452将该确定的结果返回给协议引擎451。如果脚本引擎452确定解锁脚本确实满足在相应的锁定脚本中指定的一个或多个标准,则返回结果“TRUE”。否则,返回结果“FALSE”。

[0791] 在基于输出的模型中,来自脚本引擎452的结果“TRUE”是事务有效性的条件之一。通常,还必须满足由协议引擎451评估的一个或多个进一步协议级条件;例如,Tx_j的输入中所指定的数字资产的总数额不超过其输出中指向的总数额,并且Tx_i的指向输出尚未被另一有效事务花费。协议引擎451评估来自脚本引擎452的结果以及一个或多个协议级条件,并且只有当它们都为TRUE时,协议引擎才核实事务Tx_j有效。协议引擎451将事务是否有效的指示输出到应用级决策引擎454。只有在Tx_j确实有效的条件下,决策引擎454才可以选择同时控制共识模块455C和传播模块455P,以执行其就Tx_j.的相应区块链相关功能。这包括共识模块455C,向节点的相应有序事务集154添加Tx_j,用于并入区块151中;以及传播模块455P,将Tx_j转发到网络106中的另一个区块链节点104。可选地,在实施例中,应用级决策引擎454可以在触发这些函数中的一个或两个函数之前应用一个或多个附加条件。例如,决策引擎可以只选择在事务有效且预留足够事务费用的条件下发布事务。

[0792] 此外,还应当注意的是,在本文中,术语“TRUE”和“FALSE”不一定限于返回仅以单个二进制数(位)形式表示的结果,尽管这确实是一种可能的实现方式。更通俗地说,“TRUE”

可以指指示成功或肯定结果的任何状态,而“FALSE”可以指指示不成功或不肯定结果的任何状态。例如,在基于账户的模型中,可以对签名的隐式协议级核实和智能合约的附加肯定输出的组合来指示结果为“TRUE”(如果两个单独的结果均为TRUE,则认为总体结果为TRUE)。

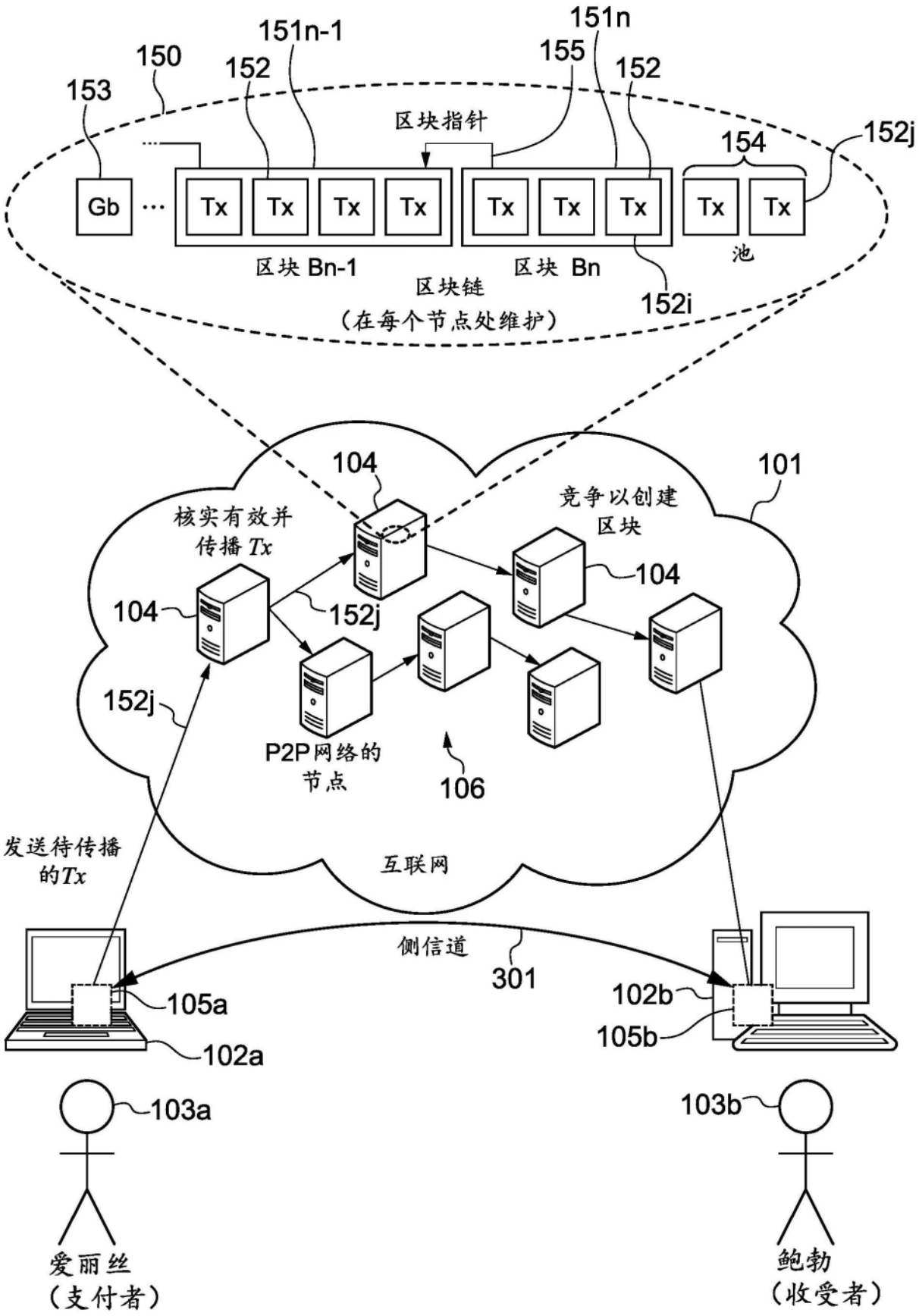

151n-1
151n
150
155
152
152
153
区块指针
154
152j
Gb
Tx
Tx
Tx
Tx
Tx
Tx
Tx
Tx
Tx
池
区块 Bn-1
区块 Bn
区块链
152i
（在每个节点处维护）
104
101
核实有效并
传播 Tx
竞争以创建
区块
104
104
152j
152j
P2P网络的
节点
106
发送待传播
的Tx
互联网
侧信道
301
105a
102b
105b
102a
103a
103b
爱丽丝
（支付者）
鲍勃
（收受者）

图1

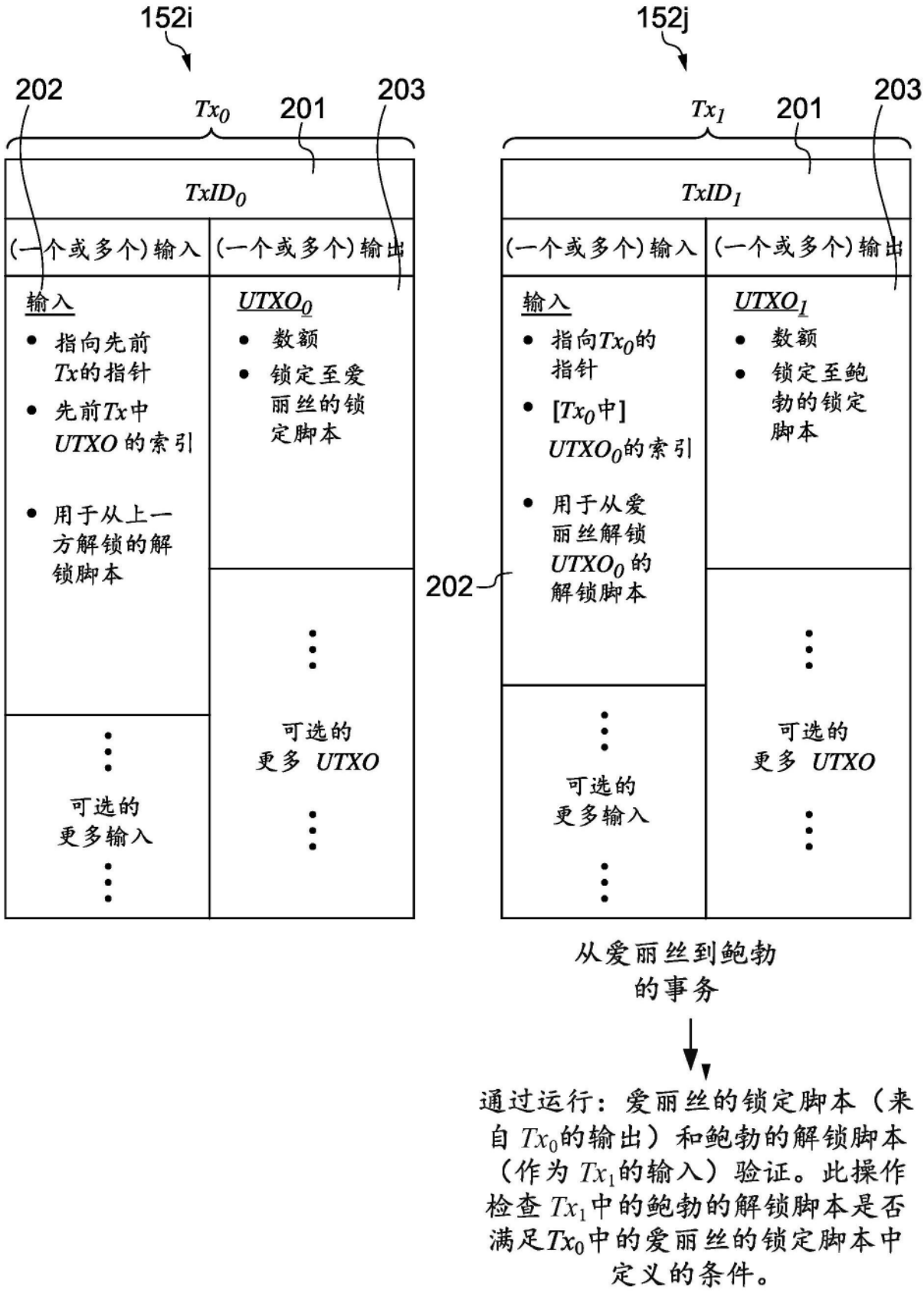

152i
202
Tx_0
201
203
$TxID_0$
(一个或多个)输入
(一个或多个)输出
输入
指向先前Tx的指针
先前Tx中UTXO的索引
用于从上一方解锁的解锁脚本
$UTXO_0$
数额
锁定至爱丽丝的锁定脚本
可选的更多 UTXO
可选的更多输入
152j
Tx_1
201
203
$TxID_1$
(一个或多个)输入
(一个或多个)输出
输入
指向Tx_0的指针
[Tx_0中]$UTXO_0$的索引
用于从爱丽丝解锁$UTXO_0$的解锁脚本
$UTXO_1$
数额
锁定至鲍勃的锁定脚本
可选的更多 UTXO
可选的更多输入
202
从爱丽丝到鲍勃的事务
通过运行：爱丽丝的锁定脚本（来自Tx_0的输出）和鲍勃的解锁脚本（作为Tx_1的输入）验证。此操作检查Tx_1中的鲍勃的解锁脚本是否满足Tx_0中的爱丽丝的锁定脚本中定义的条件。

图2

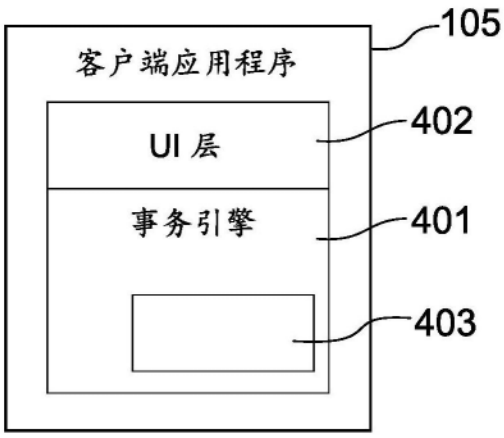


图3A

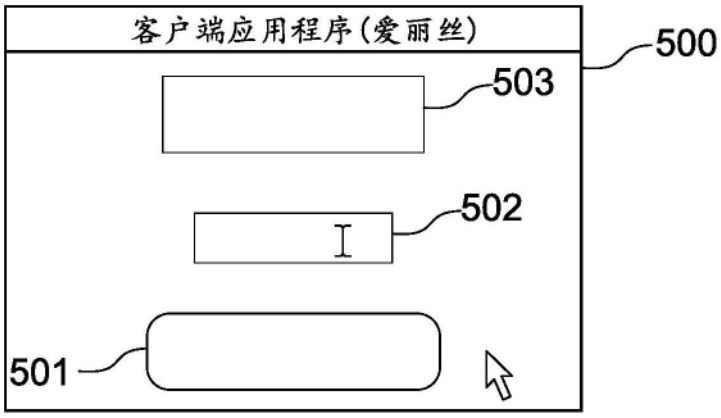


图3B

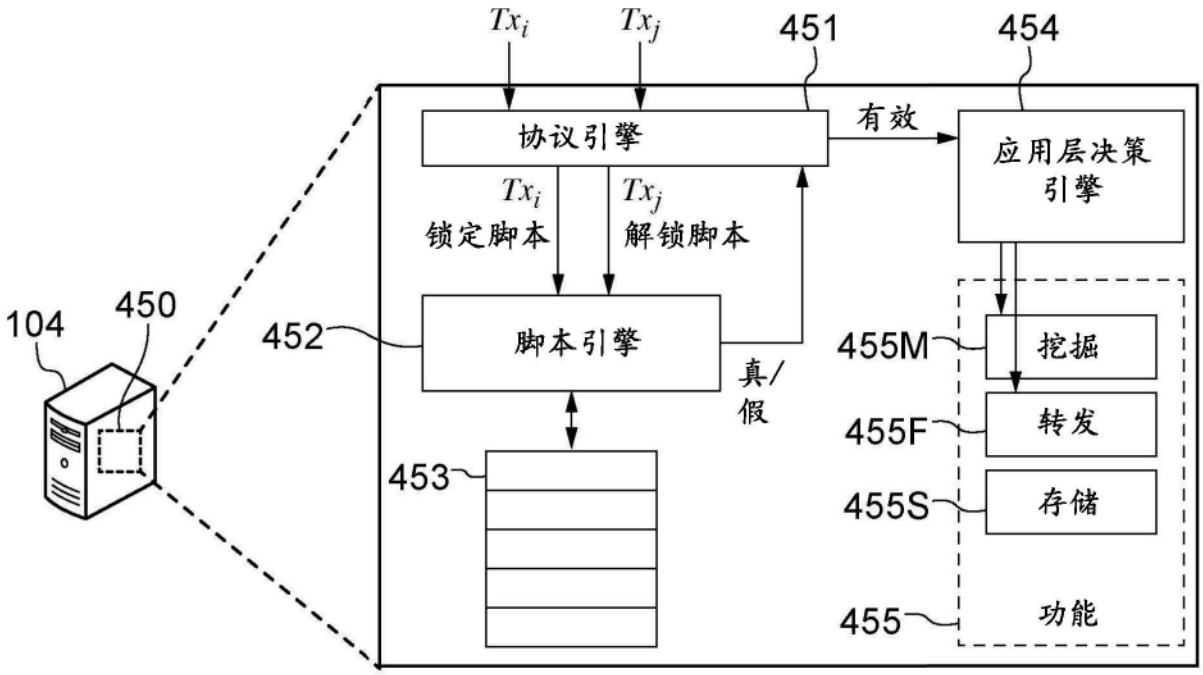

Tx_i
Tx_j
451
454
协议引擎
有效
应用层决策引擎
Tx_i
锁定脚本
Tx_j
解锁脚本
104
450
452
脚本引擎
真/假
455M
挖掘
455F
转发
453
455S
存储
455
功能

图4

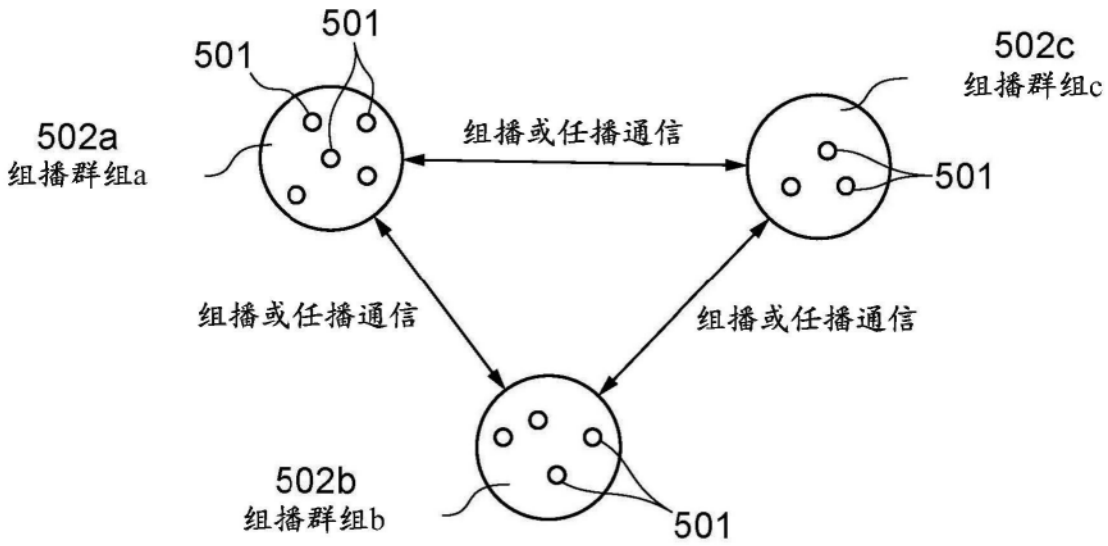

501
501
502c
组播群组c
502a
组播群组a
组播或任播通信
501
组播或任播通信
组播或任播通信
502b
组播群组b
501

图5

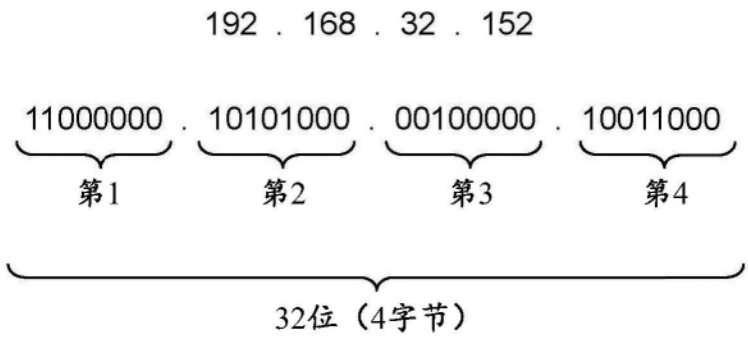

192 . 168 . 32 . 152
11000000 . 10101000 . 00100000 . 10011000
第1
第2
第3
第4
32位（4字节）

图6a

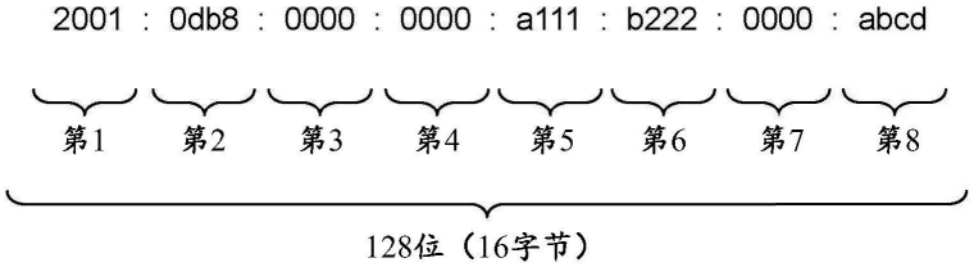

2001 : 0db8 : 0000 : 0000 : a111 : b222 : 0000 : abcd
第1
第2
第3
第4
第5
第6
第7
第8
128位（16字节）

图6b

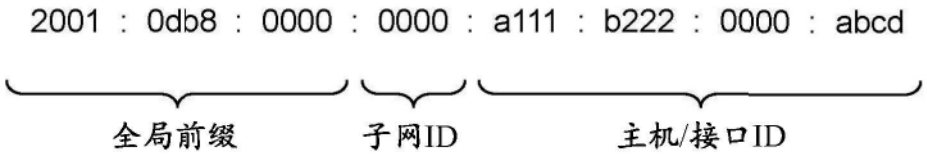

2001 : 0db8 : 0000 : 0000 : a111 : b222 : 0000 : abcd
全局前缀
子网ID
主机/接口ID

图6c

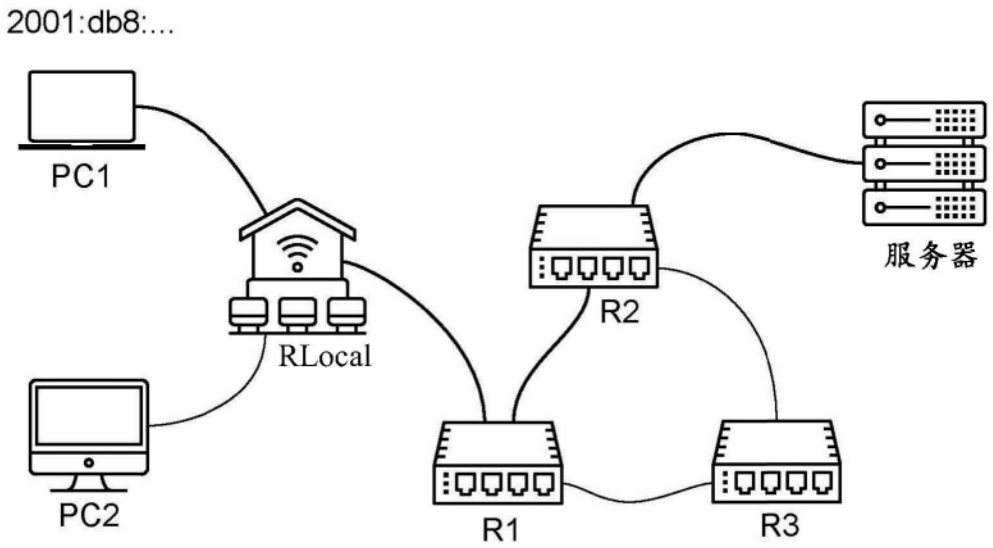

2001:db8:...
PC1
RLocal
PC2
R1
R2
R3
服务器

图7

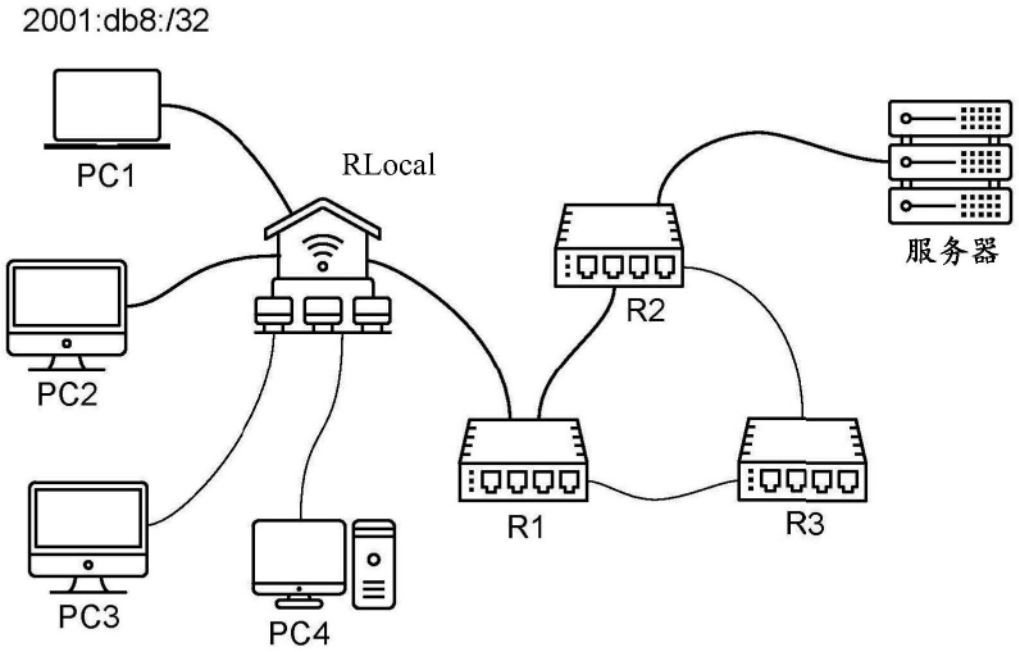

2001:db8:/32
PC1
RLocal
PC2
PC3
PC4
R1
R2
R3
服务器

图8

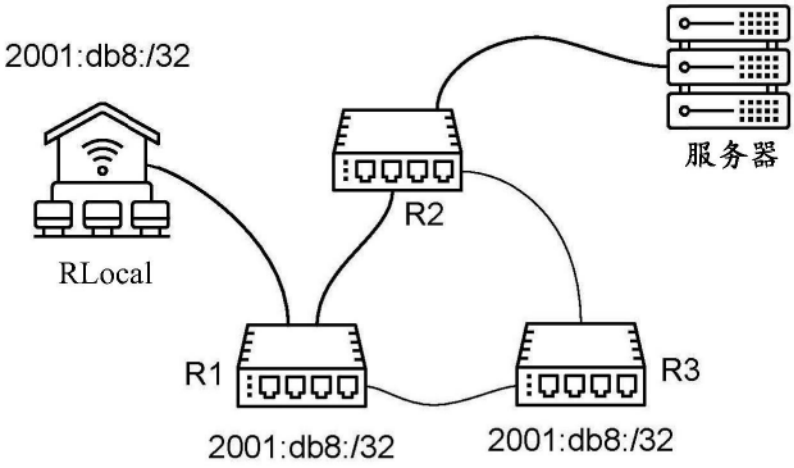

2001:db8:/32
服务器
R2
RLocal
R1
R3
2001:db8:/32
2001:db8:/32

图9

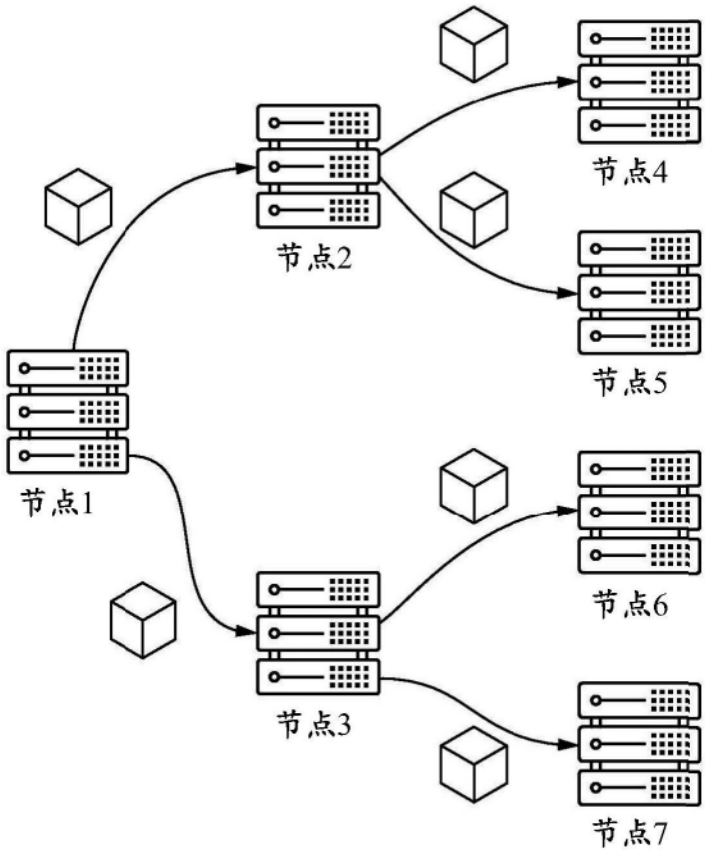

节点4
节点2
节点5
节点1
节点6
节点3
节点7

图10

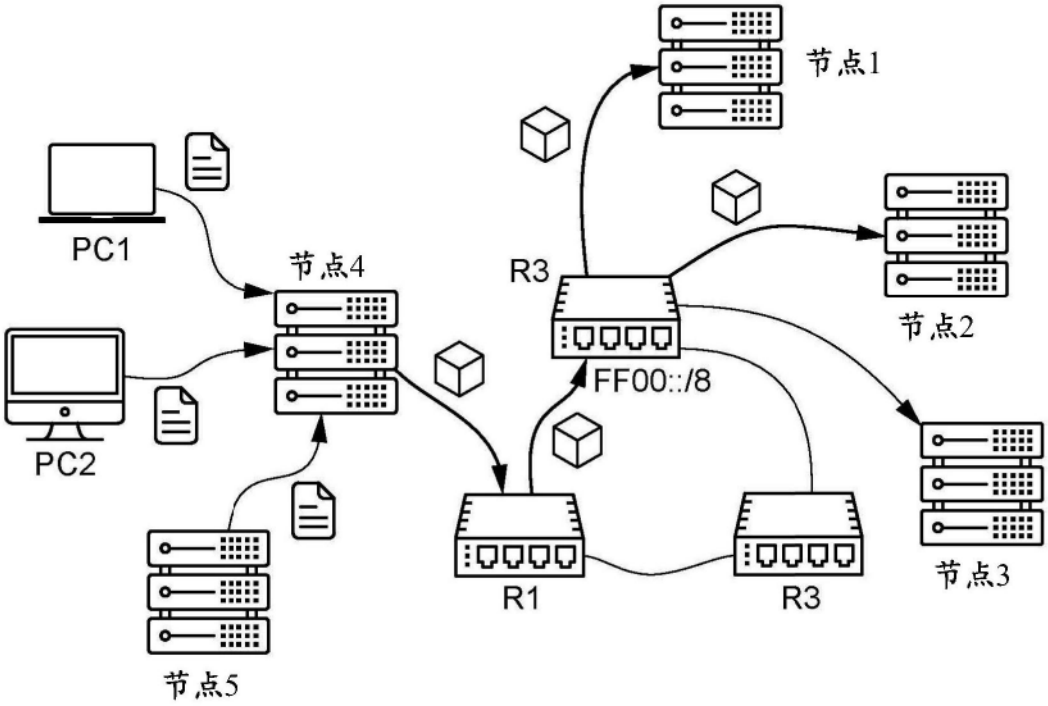

节点1
PC1
节点4
R3
节点2
FF00::/8
PC2
节点3
R1
R3
节点5

图11

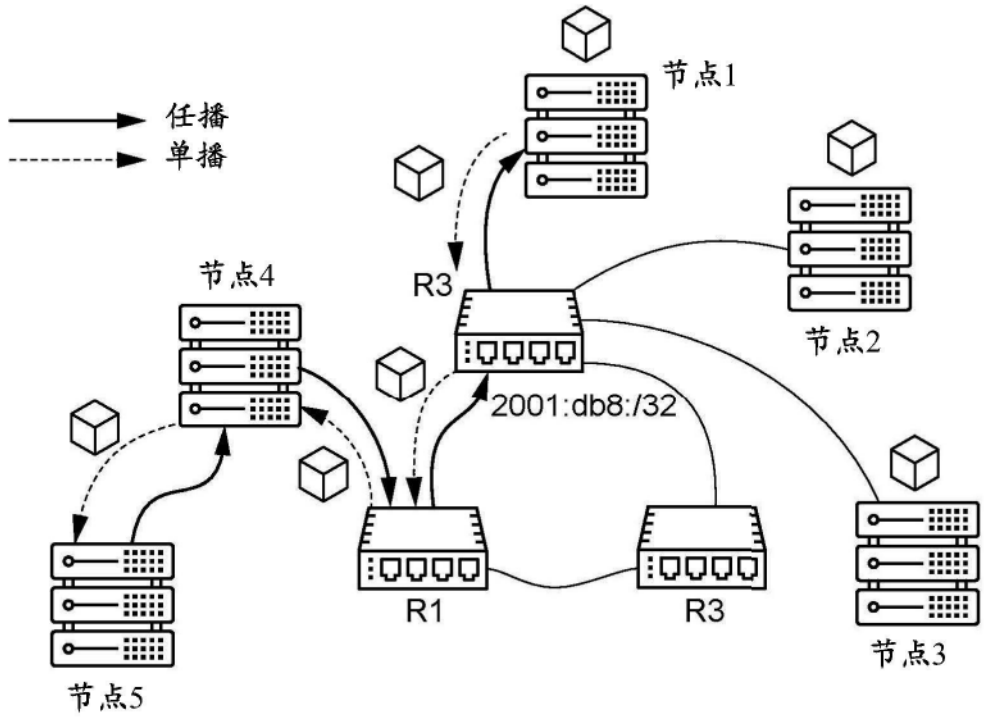

任播
单播
节点1
节点4
R3
节点2
2001:db8:/32
R1
R3
节点3
节点5

图12

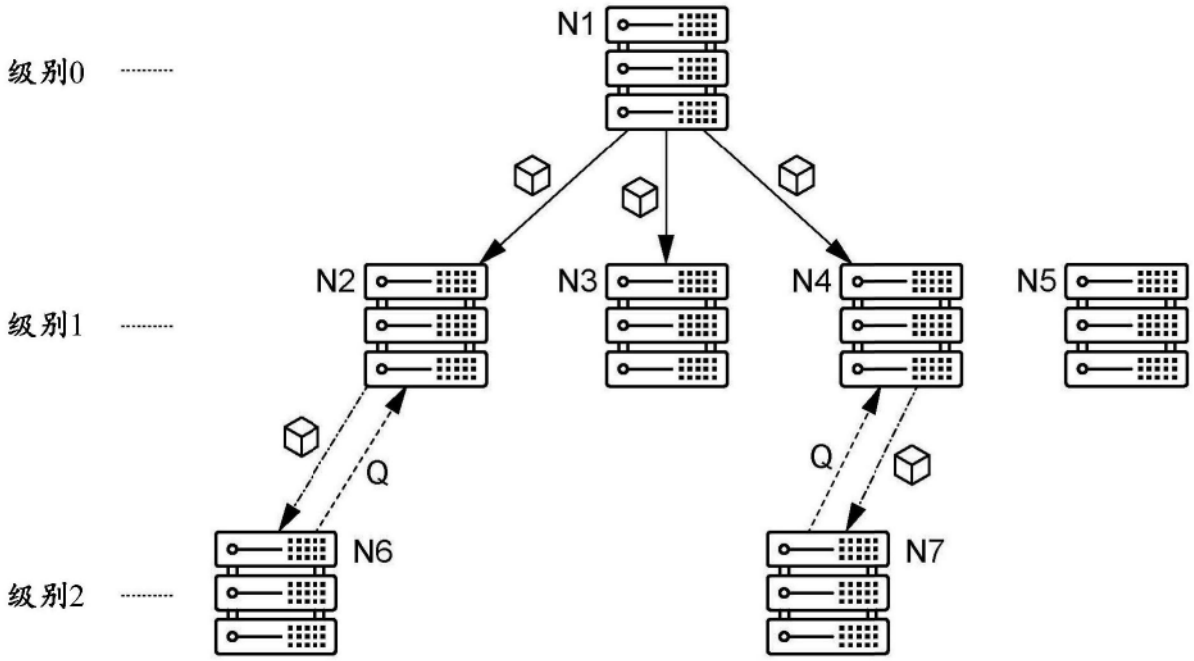


图13

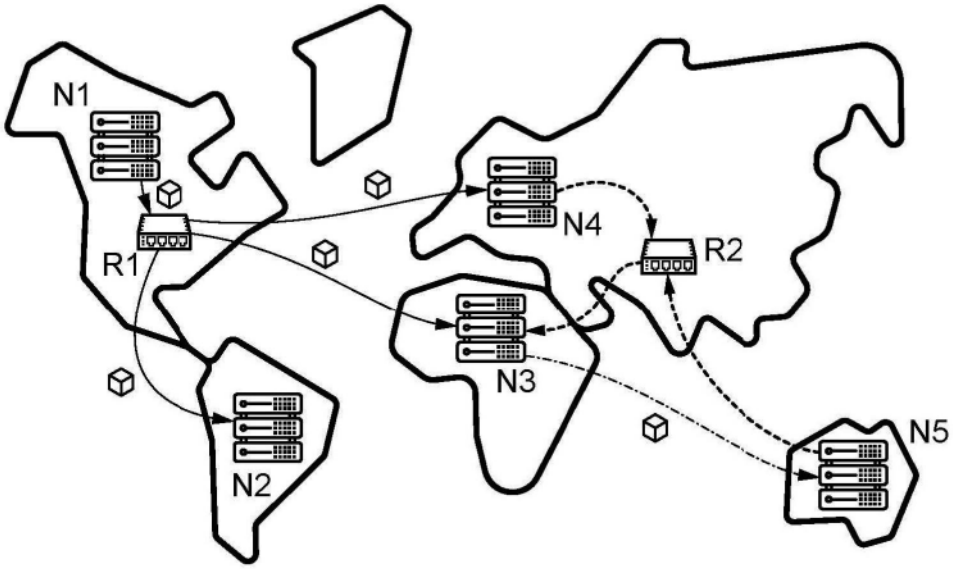


图14

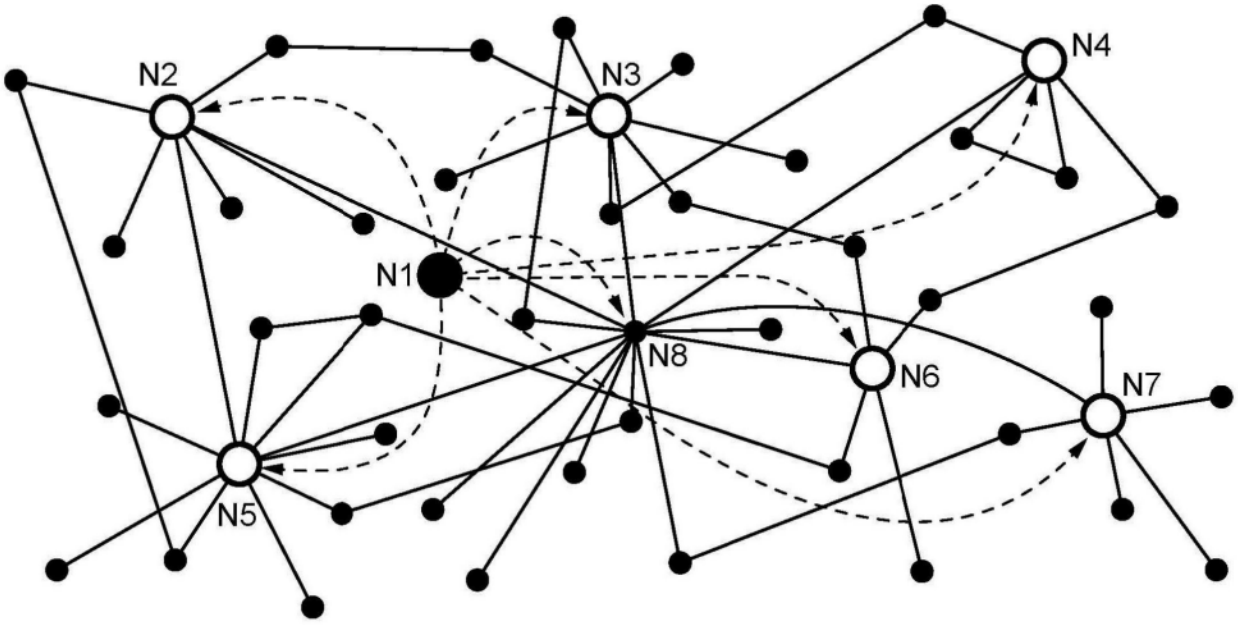


图15

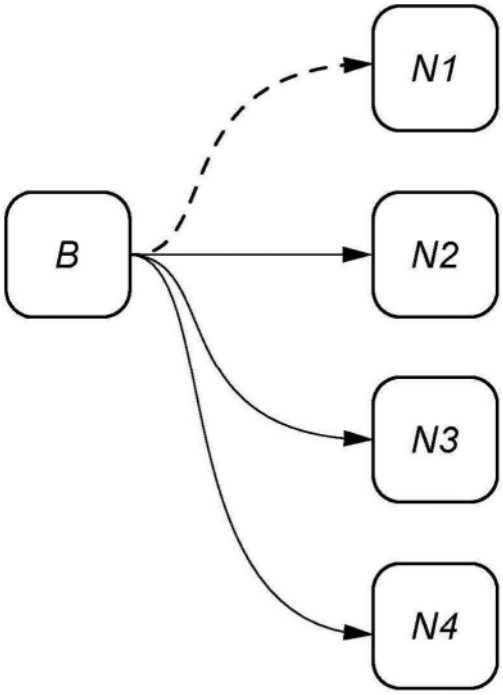


图16

二进制值	分配地址
000	1
001	2
010	3
011	4
100	5
101	6
110	7
111	8

(a)

十六进制值	分配地址
0	1
1	2
2	3
3	4
4	5
5	6
6	7
7	8
8	9
9	10
a	11
b	12
c	13
d	14
e	15
f	16

(b)

二进制值	分配地址
0000	1
0001	2
0010	3
0011	4
0100	5
0101	6
0110	7
0111	8
1000	9
1001	10
1010	11
1011	12
1100	13
1101	14
1110	15
1111	16

(c)

十六进制值范围	分配地址
00-0f	1
10-1f	2
20-2f	3
30-3f	4
40-4f	5
50-5f	6
60-6f	7
70-7f	8
80-8f	9
90-9f	10
a0-af	11
b0-bf	12
c0-cf	13
d0-df	14
e0-ef	15
f0-ff	16

(d)

图17

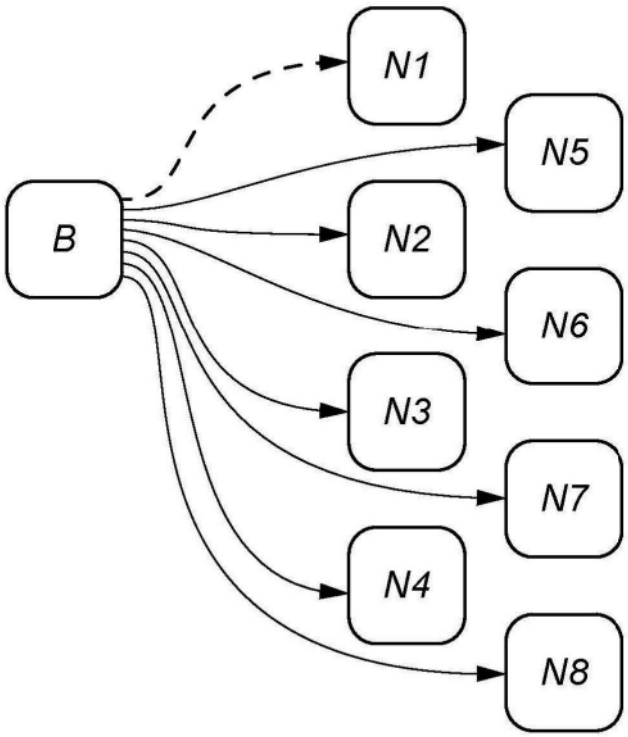


图18

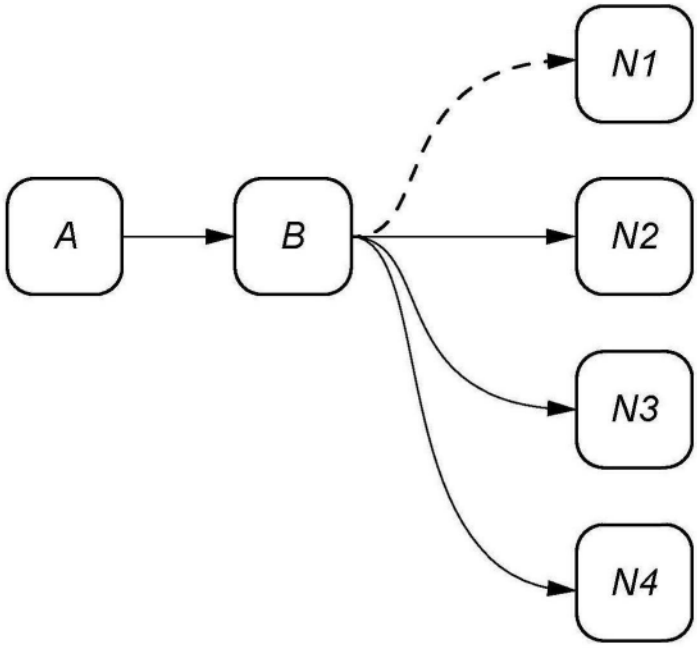


图19

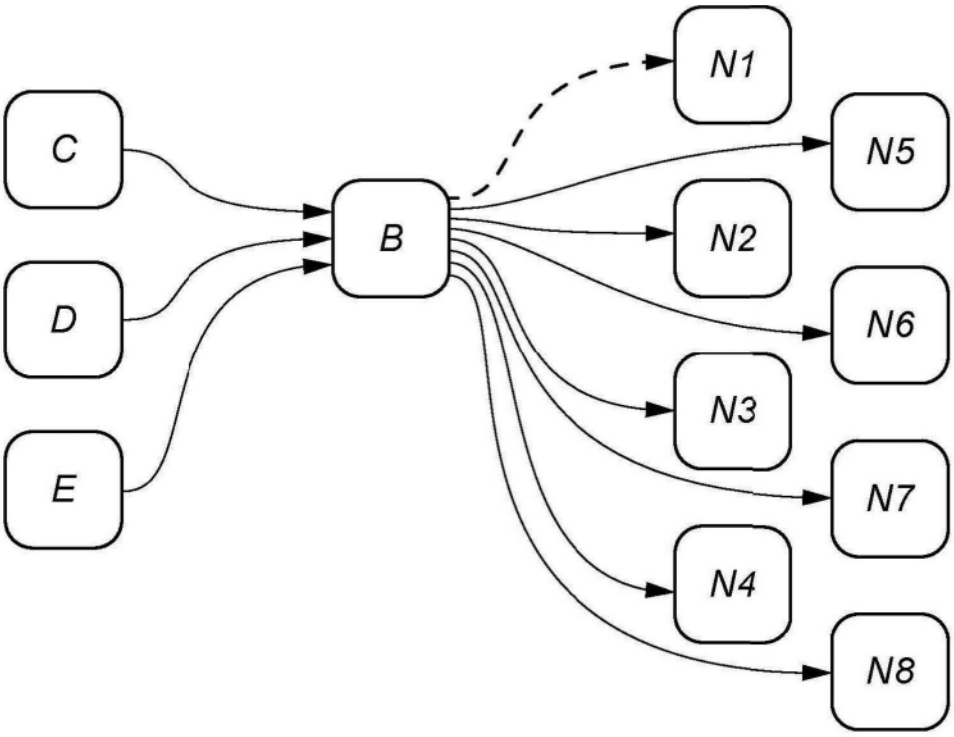


图20

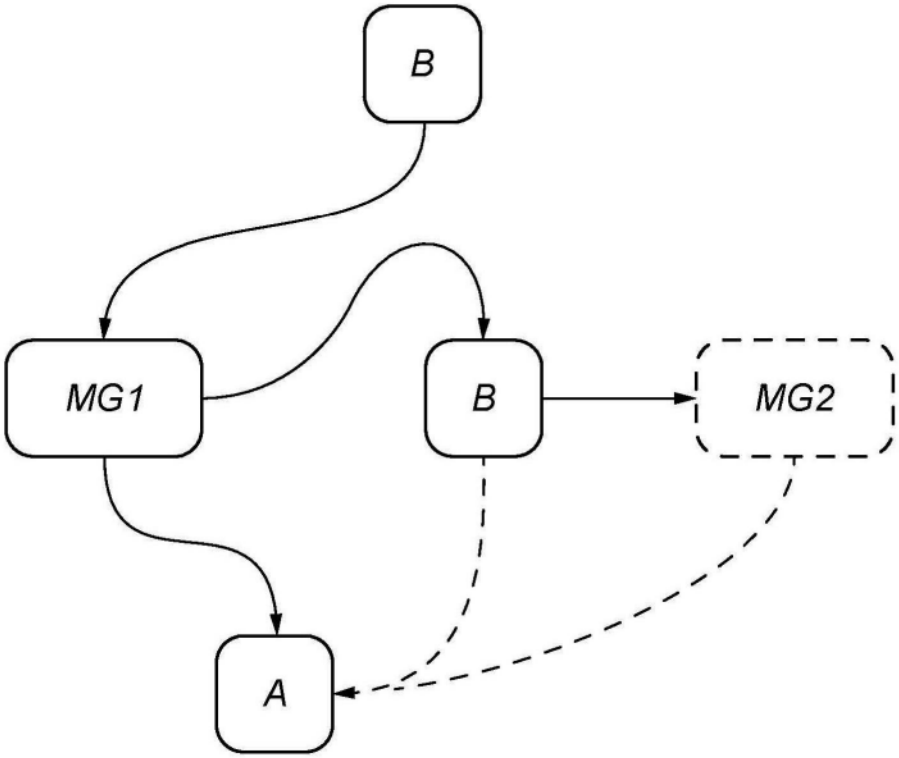


图21

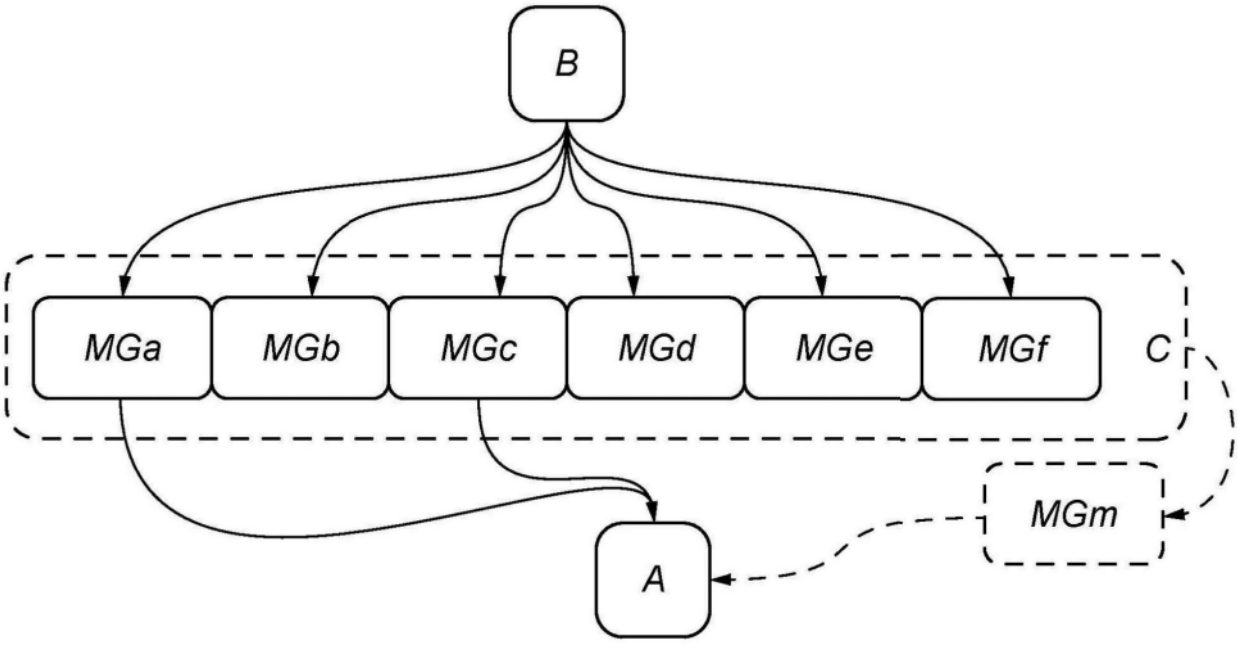


图22

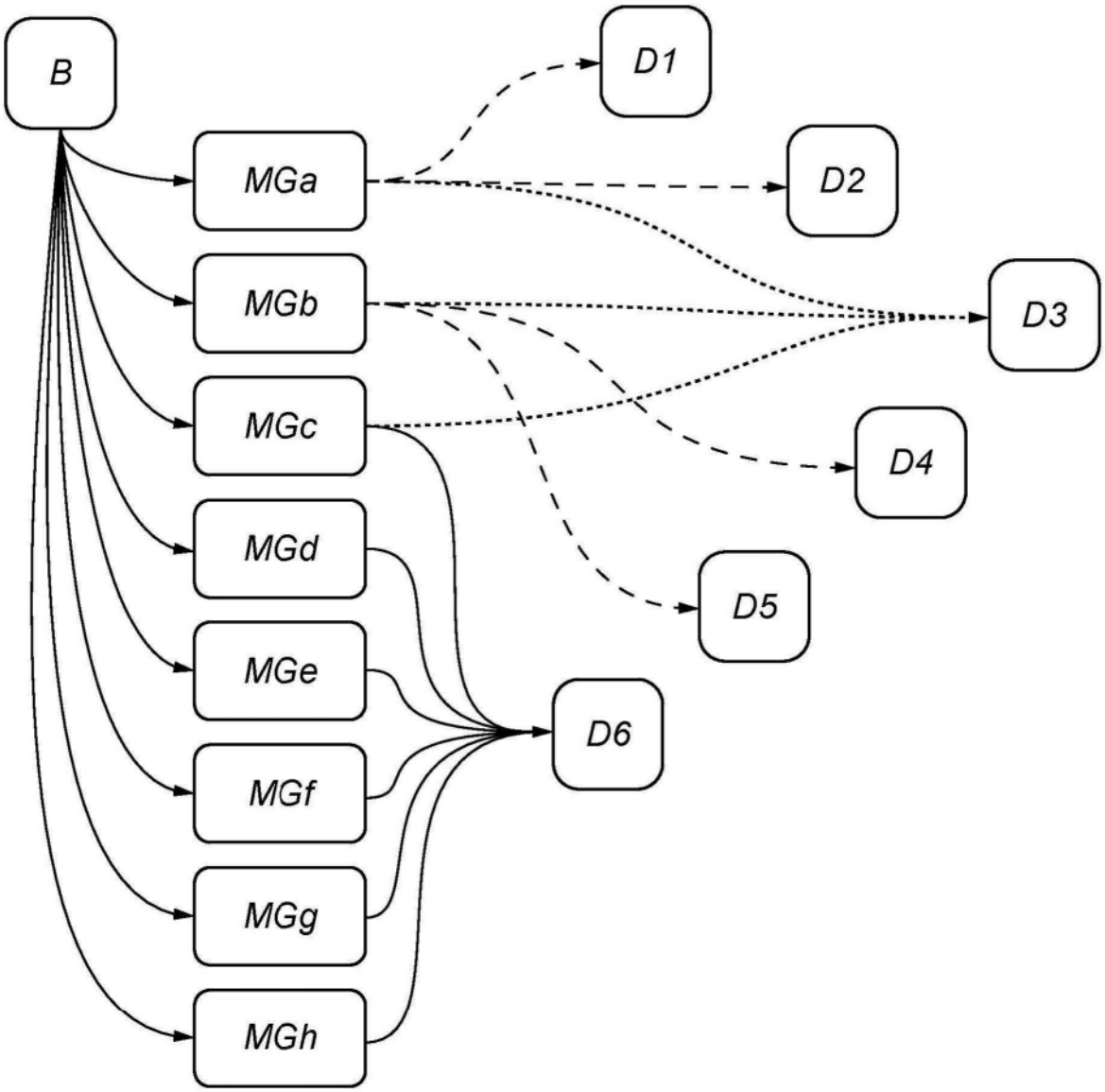


图23