

联盟链的可信度验证方法、系统、装置及设备

技术领域

[01]本说明书实施例涉及信息技术领域，尤其涉及联盟链的可信度验证方法、系统、装置及设备。

5 背景技术

[02]在联盟链中，常常存在功能差异很大的多个节点，例如，在一条著作权存证的联盟链上，可能包括作品发布节点、版权登记节点、版权转让节点以及公证节点等等。而基于用户的不同需求，和用户对接的往往只是其中的一个节点，该节点可以认为是该用户的对接节点。例如，用户通过某节点所发布的应用程序 APP 发布了一项交易，并通过该对接节点将该交易进行了联盟链存证，以后再进行验证时也往往是通过该对接节点进行。

[03]在这个过程中，用户本身难以感知整个联盟链的其它节点，通常也对于其它节点并无多大兴趣。在用户体验中，交易的完成和验证仿佛是对接节点为中心的，进而，用户就会对该对接节点以及联盟链的可信度产生疑虑。

15 [04]基于此，需要一种可以让用户对联盟链的可信度进行验证的方案。

发明内容

[05]针对现有技术中用户在对于联盟链的可信验证中，体验不佳的问题，为提高用户体验，本说明书实施例提供一种可以让用户对联盟链的可信度进行验证的方案，该方案的第一方面，包括一种联盟链的可信度验证方法，在客户端生成交易，并通过对接节点将所述交易上链存证后，包括：

[06]客户端获取联盟链中的多个节点地址；

[07]根据所述多个节点地址，发送简单支付验证 SPV 请求至所述多个节点，其中，所述 SPV 请求中包含所述交易的摘要哈希；

25 [08]任一节点接收所述 SPV 请求，基于所述摘要哈希执行 SPV 验证，验证所述交易是是否存在于所述联盟链中，并返回验证结果至客户端；

[09]客户端基于所述多个节点分别返回的验证结果的一致程度，确定所述联盟链的可信

度。

[10]第二方面,本说明书实施例还提供一种联盟链的可信度验证方法,在用户生成交易,并通过对接节点将所述交易上链存证后,包括:

[11]获取联盟链中的多个节点地址;

- 5 [12]根据所述多个节点地址,发送简单支付验证 SPV 请求至所述多个节点,其中,所述 SPV 请求中包含所述交易的摘要哈希;

[13]根据所述多个节点分别返回的验证结果的一致程度,确定所述联盟链的可信度。

[14]第三方面,本说明书实施例还提供一种联盟链中的请求处理方法,在节点为联盟链中的节点时,包括:

- 10 [15]所述节点确定自身节点用户的用户标识,并从确定出由用户标识组成的白名单,其中,所述用户标识用于标识用户身份,以及,用于标识和该用户对接的节点;

[16]发送白名单至联盟链中的其它节点,以便其它节点根据所述白名单确定是否执行非自身节点用户所发送的请求,所述请求包括交易位置查询请求或者简单支付验证 SPV 请求,所述请求中包含目标交易的摘要哈希。

- 15 [17]与第一方面对应的,本说明书实施例还一种联盟链的可信度验证系统,包括客户端和联盟链网络,所述联盟链网络包括多个节点;在客户端生成交易,并通过对接节点将所述交易上链存证后,

[18]客户端获取联盟链中的多个节点地址;

- 20 [19]根据所述多个节点地址,发送简单支付验证 SPV 请求至所述多个节点,其中,所述 SPV 请求中包含所述交易的摘要哈希;

[20]联盟链网络中的任一节点接收所述 SPV 请求,基于所述摘要哈希执行 SPV 验证,验证所述交易是否存在于所述联盟链中,并返回验证结果至客户端;

[21]客户端基于所述多个节点分别返回的验证结果的一致程度,确定所述联盟链的可信度。

- 25 [22]与第二方面对应的,本说明书实施例还提供一种联盟链的可信度验证装置,在用户生成交易,并通过对接节点将所述交易上链存证后,所述装置包括:

[23]获取模块,获取联盟链中的多个节点地址;

[24]发送模块,根据所述多个节点地址,发送简单支付验证 SPV 请求至所述多个节点,其中,所述 SPV 请求中包含所述交易的摘要哈希;

[25]接收模块,接收所述多个节点分别返回的验证结果;

[26]验证模块,根据所述多个节点分别返回的验证结果的一致程度,确定所述联盟链的可信度。

5

[27]与第三方面对应的,本说明书实施例还提供一种联盟链中的请求处理装置,位于所述联盟链中的节点上,包括:

[28]确定模块,所述节点确定自身节点用户的用户标识,并从确定出由用户标识组成的白名单,其中,所述用户标识用于标识用户身份,以及,用于标识和该用户对接的节点;

10 [29]发送模块,发送白名单至联盟链中的其它节点,以便其它节点根据所述白名单确定是否执行非自身节点用户所发送的请求,所述请求包括交易位置查询请求或者简单支付验证 SPV 请求,所述请求中包含目标交易的摘要哈希。

[30]本说明书实施例所提供的方案中,在客户端通过对接节点完成交易上链存证之后,针对该交易,客户端针向联盟链中的多个节点发起 SPV 请求,验证所述交易是否在联盟链上,从而可以得到多个节点对于该交易的各自的验证结果。进而,可以基于多个节点的 SPV 验证结果的一致程度去验证该联盟链的可信度,提高用户体验。

15

[31]应当理解的是,以上的一般描述和后文的细节描述仅是示例性和解释性的,并不能限制本说明书实施例。

[32]此外,本说明书实施例中的任一实施例并不需要达到上述的全部效果。

20 附图说明

[33]为了更清楚地说明本说明书实施例或现有技术中的技术方案,下面将对实施例或现有技术描述中所需要使用的附图作简单地介绍,显而易见地,下面描述中的附图仅仅是本说明书实施例中记载的一些实施例,对于本领域普通技术人员来讲,还可以根据这些附图获得其他的附图。

25 [34]图 1 为当前联盟链中所涉及的一种架构示意图;

[35]图 2 是本说明书实施例提供的系统方面的一种联盟链的可信度验证方法的流程示意图;

[36]图 3 为本说明书是实施例所提供的客户端方面的一种联盟链的可信度验证方法的流程示意图;

[37]图 4 为本说明书是实施例所提供的一种联盟链的请求处理方法的流程示意图;

[38]图 5 为本说明书实施例所提供的一种可信度验证装置的结构示意图;

5 [39]图 6 为本说明书实施例所提供的一种请求处理装置的结构示意图;

[40]图 7 是用于配置本说明书实施例方法的一种设备的结构示意图。

具体实施方式

[41]为了使本领域技术人员更好地理解本说明书实施例中的技术方案,下面将结合本说明书实施例中的附图,对本说明书实施例中的技术方案进行详细地描述,显然,所描述
10 的实施例仅仅是本说明书的一部分实施例,而不是全部的实施例。基于本说明书中的实施例,本领域普通技术人员所获得的所有其他实施例,都应当属于保护的范围。

[42]在联盟链中通常包含了多个不同的功能节点,在当前,联盟链常采用的一种架构为,各功能节点分别面向各自的用户,用户通过他们感兴趣的功能节点接入联盟链。

[43]在本说明书实施例所涉及的联盟链中的节点,可以认为每个节点都参与联盟链网络
15 的路由功能,同时也可以包含其他功能,例如,每个节点都可以参与验证并传播交易及区块信息,发现并维持与对等节点的连接,以及还可以在本地存储有完整的联盟链,和一些与联盟链相关的数据。

[44]如图 1 所示,图 1 为当前联盟链中所涉及的一种架构示意图。在图 1 中,联盟链网络中的节点可能都包含有不同的功能,以及,各节点由于提供不同的功能,面向的目标
20 用户也常常并不相同,在同一联盟链中,各功能节点还经常分别开发自己的应用程序 APP 让自身节点用户进行注册并接入。而用户则通常从中选取一个节点对接联盟链,进行交易发布以及验证。

[45]以下结合附图,详细说明本说明书各实施例提供的技术方案。本说明书实施例的方案的第一方面,如图 2 所示,图 2 是本说明书实施例提供的系统方面的一种联盟链的可
25 信度验证方法的流程示意图,在客户端生成交易,并通过对接节点将所述交易上链存证后,该流程具体包括如下步骤:

[46]S201, 客户端获取联盟链中的多个节点地址。

- [47]对客户端而言，已知的是对接节点的地址，联盟链中的其它节点地址可以向对接节点请求获得。也可以通过其它方式获取，例如，联盟链中的所有节点定时将自己的地址发布至某公开云端，客户端本地保存一张地址列表，并且客户端定期从该公开云端获取所有节点的地址对该地址列表进行更新，从而，可以从该地址列表中随时选取若干节点地址。通过该方式，可以绕开客户端的对接节点，提高用户对于整个联盟链的信任程度。
- [48]S203，根据所述多个节点地址，发送简单支付验证 SPV 请求至所述多个节点，其中，所述 SPV 请求中包含所述交易的摘要哈希。
- [49]由于在用户完成交易并通过对接节点上链存证之后，就会收到一个关于该存证交易的通知消息，通常其中就包括摘要哈希，并保存于客户端本地。因此，客户端总是可以从本地中获取该摘要哈希，并将其加入 SPV 请求请求中。
- [50]在客户端方面，可以是在收到该通知消息后，根据用户的指令发起 SPV 请求；也可以是，接收到该通知消息即触发 SPV 请求。
- [51]S205，任一节点接收所述 SPV 请求，基于所述摘要哈希执行 SPV 验证，验证所述交易是否存在于所述联盟链中，并返回验证结果至客户端。
- [52]在区块链的每个区块中，包含了记录于该区块的所有交易，并且可以默克尔 Merkle 树表示。区块中所有的交易将数据哈希化，然后将哈希值存储至相应的叶子节点中。树中的每个叶子节点表征了一个交易。树中的一个叶子节点表征区块中存在一笔对应的交易。为了证明区块中存在某个特定的目标交易，一个节点只需要计算 $\log_2 N$ 个哈希值，形成一条从目标交易到树根的 Merkle 路径即可。
- [53]节点在进行简单支付验证（Simplified Payment Verification, SPV）时，不必保存所有交易也不必下载整个区块。节点可以仅仅保存区块头，并通过目标交易的哈希和 Merkle 路径来验证目标交易是否存在于该区块中。换言之，各节点的 SPV 验证结果是一个二值结果，要么为“是”，要么为“否”。
- [54]此外，需要说明的是，任一节点接收到的请求可以是直接来自于客户端，也可以是接收联盟链中其它节点所转发的客户端请求。
- [55]S207，客户端基于所述多个节点分别返回的验证结果的一致程度，确定所述联盟链的可信度。
- [56]由于一个交易在联盟链中要么存在，要么不存在，理论上，当联盟链没有问题时，各节点所返回的 SPV 验证结果应该完全相同。因此，一个较为严格的可信度确认方式

为，若所有 SPV 验证结果均一致为“是”，则确认该联盟链是可信的，否则是不可信的。当然，由于各种网络原因、设备原因等等，可以容许一定的偏差。例如，设定一个阈值，若 SPV 验证结果的一致为“是”的程度超过该阈值，则确认该联盟链是可信的。

- [57]进一步地，当确认该联盟链不可信时，还可以发出警报。具体的，警报消息中可以
- 5 指出各节点的验证结果不一致的程度是多少（即“是”和“否”的结果分别是多少），以及，具体的给出与多数结果不一致的节点和该类节点的验证结果。以及，还可以根据返回的所有结果的不一致的程度计算一个可信度数值作为参考。例如，若返回的结果中不存在占比超过 95% 的相同验证结果，则认为联盟度可信度为 0，否则，将所述相同验证结果的占比作为该联盟链的可信度。
- 10 [58]本说明书实施例所提供的方案中，在用户通过对接节点完成交易上链存证之后，针对该交易，用户针向联盟链中的多个节点发起 SPV 请求，从而可以得到多个节点对于该交易的各自的 SPV 验证结果。进而，可以基于多个节点的 SPV 验证结果的一致程度去验证该联盟链的可信度，提高用户体验。

[59]在一种具体的实施方式下，客户端获取联盟链中的多个节点地址，可以是

- 15 [60]客户端随机获取联盟链中的多个节点地址，随机获取节点地址验证一方面可以使得验证结果更加公正，另一方面，也可以使得用户的请求平均的流向向各节点，避免某些用户多的节点负荷太重。又或者，客户端获取联盟链中包含所述对接节点地址的多个节点地址，在这种方式下，用户可以首先选取一批节点地址，然后再将对接节点的地址加入即可。加入对接节点进行验证时，在返回的结果中也包含对接节点的验证结果，可以
- 20 使得验证更具有针对性，提高用户体验。

- [61]在一种具体的实施方式下，客户端还可以根据所述多个节点地址，发送交易位置查询请求至所述多个节点，其中，所述交易位置查询请求中包含所述交易的摘要哈希；任一节点接收所述位置查询请求，基于所述摘要哈希各自查询所述摘要哈希所对应的交易在所述联盟链中的位置信息，并返回所述位置查询结果至客户端；客户端基于所述多个
- 25 节点分别返回的位置查询结果的一致程度，验证包含所述交易信息的联盟链的可信度。

[62]一个区块链由多个区块组成，同时，一个区块中通常包含多个交易。因此，在本说明书实施例中，所述的位置信息具体指的是该交易被存证时，处于区块链中的哪个区块上，以及，在该区块中的什么位置。

[63]在区块链中，可以有多种方式用来标识不同的区块，例如，区块头哈希值或者区块

高度 (block height)。区块头哈希值即为区块头进行哈希计算而得到的哈希值, 可以用于唯一、明确地标识一个区块。在区块链中, 通常第一个区块其区块高度为 0, 以后每增加一个区块, 区块高度加 1。一个区块通常有一个明确的区块高度。因此, 区块头哈希值或者区块高度可以作为区块元数据的一部分, 被存储在节点中一个独立的数据库表中, 以便于索引和更快地检索到该区块。

[64]同时, 在一个区块中, 由于通常包含了多个交易, 因此, 还可以用各交易在该区块中的地址偏移量来分别标识区块中的交易。显而易见, 在同一个区块中, 各交易的地址偏移量并不相同。

[65]进而, 可以在交易所处的区块上链存证以后, 各节点中可以通过维护一张形如 (交易摘要哈希, 区块头哈希值, 地址偏移量), 或者, (交易摘要哈希, 区块高度, 地址偏移量) 的数据表, 就可以通过交易的摘要哈希查询得到对应的区块标识以及交易在区块中的地址。换言之, 节点可以通过交易的摘要哈希确定该交易在联盟链中的位置。

[66]当然, 由于区块链的具体格式是可以自定义的, 在不同的区块格式下, 位置信息的内容也会有所不同, 这并不构成对本方案的限定。

[67]由于一个交易在联盟链中只会有一个确定的位置, 因此, 联盟链的可信度可以基于查询结果的一致程度而定。理论上, 各节点所返回的位置信息应该完全相同。一个较为严格的验证方式即为, 若所有位置查询结果均一致, 则该联盟链为可信的。当然, 由于各种网络原因、设备原因等等, 可以容许一定的偏差。例如, 根据返回的所有结果的对一致程度进行计算, 若返回的结果中不存在占比超过 95% 的相同查询结果, 则认为联盟度可信度为 0, 否则, 将所述相同结果的占比作为该联盟链的可信度。

[68]进一步地, 当确定联盟链不可信时, 还可以发出警报。具体的, 警报消息中可以指出各节点的查询结果不一致的程度是多少 (即有多少个或者多少比例与多数结果不一致), 以及, 具体的给出与多数结果不一致的节点和该类节点的查询结果。

[69]需要说明的是, 上述基于位置查询结果的一致性进行验证的方案, 和基于 SPV 验证的结果的一致性进行验证的方案, 属于可以同时分开进行的方案。在实际操作中, 二者的验证结果是分别独立的。换言之, 在同时执行两种验证方案时, 需要二种验证方案的结果同时满足一致性条件, 才认为联盟链是可信的。以及, 在验证的过程中, 两种方案的执行不分先后。

[70]由于在联盟链中, 各功能节点通常会有自己的对接客户端以及对应的对接用户。在

本说明书实施例的方案中，各节点经常需要处理来自于非自身节点用户的请求。

- [71]在一种实施方式下，节点可以对于任意连接自己的客户端所发送的查询请求或者 SPV 请求进行处理。在另一种实施方式下，基于联盟共享的原则，各节点还可以提供查询服务或者 SPV 服务给白名单用户，如果发送请求的客户端在白名单上，则进行处理，
- 5 否则，不进行处理。白名单用于确认所述客户端的用户类型为非法用户或者合法用户，所述合法用户包括自身节点用户或者其它节点用户。换言之，节点可以根据白名单确认发送请求的客户端是非法用户、自身节点合法用户或者非自身节点合法用户。

- [72]确定白名单用户的具体方式包括：联盟链中的任一节点确定自身的白名单，并广播白名单至联盟链中的其它节点，以便其它节点根据所述白名单确定是否执行 SPV 验证
- 10 处理。一种常见的处理方式即为，联盟链中的任一节点将自身的注册用户确认为白名单用户并进行广播。而其它节点则可以根据请求所包含的客户端标识是否是白名单用户，来决定是否进行进一步的处理。此处的白名单可以以节点为最小单元，也可以以用户为最小单元，各节点所保存的白名单用户可以相同，也可以不同。节点接收到白名单用户所发送的请求时才进行处理。

- 15 [73]例如，假设联盟链中存在 A、B、C、D 四个节点，在上述方案中，可以 B、C、D 节点将 A 节点的对接用户确认为白名单用户，四个节点共同维护；也可以在 B 节点
- 白名单用户中包括 A 节点的用户，但是 C、D 节点的白名单用户中不包括 A 节点的用户。具体的情形可以基于业务情形自行确定。

- [74]在较为一般的情形中，政府机构（例如公证处）或者公益机构（例如慈善机构）节
- 20 点的对接用户可以是所有联盟链中其它节点的白名单用户，一个节点的业务伙伴节点的节点用户也可以是该节点的白名单用户。进一步，在各节点中还可以根据用户的来源或者历史行为数据以及其它因素（例如，第三方信用评估分），对白名单用户进行权限分级，例如，最低权限的白名单用户只有查询权限，更高权限的白名单用户可能还可以拥有进一步的其它权限等等。

- 25 [75]在实际应用中，一个联盟链中各节点的用户数量情形并不相同，有的节点的对接用户多，有的节点的对接用户少。通常而言，那些直接面对市场的节点的对接用户的数量总是多余一些后方节点的数量。例如，在一个用于保护著作权的联盟链中，面对创作者的作品发布平台的注册用户，总是远多于公证处的注册用户。

[76]那么在这种情形下，本说明书实施例的方案中，联盟中的各节点在对于请求处理上

并不是“公平”的。换言之，注册用户少的节点总是会接收到超出本身本应负责处理的请求数量，这对于注册用户少的节点并不是很有利。

[77]此时，一种可实施的方式为，任一节点在接收到请求并决定处理时，首先做一个判断，确定该节点确定自身对于其它节点用户所发起的位置查询请求的第一处理次数，以及，确认其它节点对于该节点用户所发起的位置查询请求的第二处理次数；根据所述第一处理次数和第二处理次数，判断是否延迟处理所述位置查询请求。

[78]第一处理次数和第二处理次数可以以一段时间为周期，例如，每天或者每月，定期进行清零，也可以是全部历史数据的数量统计。判断是否延迟处理的条件，可以是根据第一处理次数 X 和第二处理次数 Y 计算获得一个贡献比例值 Z 与预设阈值进行比较，例如， $Z=(X-Y)/Y$ ，或者， $Z=X/Y$ 等等。贡献比例值表征了一个节点在处理请求时的“自身贡献”和“请求他人”的比例，一旦贡献比例值超过了一定阈值，则表示该节点已经做出了较多贡献，则该节点可以延迟处理接收到的其它节点用户所发送的请求，延迟处理请求可以有效降低弱节点（即注册用户少的节点，一般对于大流量的处理能力相对弱）的负荷。由于在本说明书实施例的方案中，客户端并不需要即时得到验证结果，因此各节点对于请求的处理可以是异步的，延迟处理并不会影响本说明书实施例的方案的效果。

[79]在一种实施方式下，客户端在选取多个节点时，有可能连续多次选到同一个节点，在这种方式下，客户端可以判断对该节点的交易位置查询请求的发送次数是否到达阈值，若是，对该节点延迟发送交易位置查询请求。发送次数的统计可以统计一段时间内的次数，也可以统计所有的历史次数。通过上述方式，在客户端方面即可以避免连续的请求另一节点，降低对另一节点的负荷的影响。

[80]本说明书实施例的方案的第二方面，如图 3 所示，图 3 为本说明书是实施例所提供的客户端方面的一种联盟链的可信度验证方法的流程示意图，在用户生成交易，并通过对接节点将所述交易上链存证后，包括：

[81]S301，获取联盟链中的多个节点地址；具体的方式包括，随机获取联盟链中的多个节点地址；或者，获取联盟链中包含所述对接节点地址的多个节点地址。

[82]S303，根据所述多个节点地址，发送简单支付验证 SPV 请求至所述多个节点，其中，所述 SPV 请求中包含所述交易的摘要哈希；

[83]S305，根据所述多个节点分别返回的验证结果的一致程度，确定所述联盟链的可信度。

[84]进一步地，上述方法还包括，根据所述多个节点地址，发送交易位置查询请求至所述多个节点，其中，所述交易位置查询请求中包含所述交易的摘要哈希；基于所述多个节点分别返回的位置查询结果的一致程度，验证包含所述交易信息的联盟链的可信度。

[85]进一步，所述 S303 中的发送简单支付验证 SPV 请求至所述多个节点，包括，针对
5 所述多个节点中的任一节点，判断对该节点的 SPV 请求的发送次数是否到达阈值，若是，对该节点延迟发送 SPV 请求。

[86]本说明书实施例的方案的第二方面，如图 4 所示，图 4 为本说明书是实施例所提供的一种联盟链的请求处理方法的流程示意图，在用户生成交易，并通过对接节点将所述交易上链存证后，包括：

10 [87]S401，所述节点确定自身节点用户的用户标识，并从确定出由用户标识组成的白名单，其中，所述用户标识用于标识用户身份，以及，用于标识和该用户对接的节点；联盟链中可以通过事先协商好的格式，在用户标识中包含有对接节点的信息，例如，在用户标识开头加上不同的序号用以标识该用户的对接节点。

[88]S403，发送白名单至联盟链中的其它节点，以便其它节点根据所述白名单确定是否
15 执行非自身节点用户所发送的请求，所述请求包括交易位置查询请求或者简单支付验证 SPV 请求，所述请求中包含目标交易的摘要哈希。

[89]进一步地，所述方法还包括，节点接收任一用户所发送的请求，所述请求中还包括用户标识；判断所述用户标识是否处于白名单中，若否，不对请求执行处理。

[90]进一步的，上述方法还包括，接收任一用户所发送的请求，所述请求中还包括用户
20 标识，当所述用户标识所对应的用户非自身节点用户时：

[91]确定该节点对于其它节点用户所发起的请求的第一处理次数，以及，确认其它节点对于该节点用户所发起的请求的第二处理次数；根据所述第一处理次数和第二处理次数，判断是否延迟处理所述请求。

[92]与第一方面对应的，本说明书实施例还提供一种盟链的可信度验证系统，包括客户
25 端和联盟链网络，所述联盟链网络包括多个节点；在客户端生成交易，并通过对接节点将所述交易上链存证后，

[93]客户端获取联盟链中的多个节点地址；

[94]根据所述多个节点地址，发送简单支付验证 SPV 请求至所述多个节点，其中，所述

SPV 请求中包含所述交易的摘要哈希;

[95]联盟链网络中的任一节点接收所述 SPV 请求, 基于所述摘要哈希执行 SPV 验证, 验证所述交易是否存在于所述联盟链中, 并返回验证结果至客户端;

5 [96]客户端基于所述多个节点分别返回的验证结果的一致程度, 确定所述联盟链的可信度。

[97]进一步地, 在所述系统中, 客户端随机获取联盟链中的多个节点地址; 或者, 客户端获取联盟链中包含所述对接节点地址的多个节点地址。

[98]进一步地, 在所述系统中, 客户端根据所述多个节点地址, 发送交易位置查询请求至所述多个节点, 其中, 所述交易位置查询请求中包含所述交易的摘要哈希; 任一节点
10 接收所述位置查询请求, 基于所述摘要哈希各自查询所述摘要哈希所对应的交易在所述联盟链中的位置信息, 并返回所述位置查询结果至客户端; 客户端基于所述多个节点分别返回的位置查询结果的一致程度, 验证包含所述交易信息的联盟链的可信度。

[99]进一步地, 在所述系统中, 在客户端获取联盟链中的多个节点地址之前, 联盟链中的任一节点确定自身的白名单, 并广播白名单至联盟链中的其它节点, 以便其它节点
15 根据所述白名单确定是否执行 SPV 验证处理; 所述交易 SPV 请求中包含所述交易的摘要哈希, 包括: 所述 SPV 请求包含所述交易的摘要哈希和所述客户端标识; 任一节点接收所述 SPV 请求之后, 还包括: 确定所述 SPV 请求所包含的客户端标识是否处于白名单中, 若否, 不执行 SPV 验证处理。

[100] 进一步地, 在所述系统中, 该节点确定自身对于其它节点用户所发起的 SPV 的
20 第一处理次数, 以及, 确认其它节点对于该节点用户所发起的 SPV 的第二处理次数; 根据所述第一处理次数和第二处理次数, 判断是否延迟处理所述 SPV 请求。

[101] 进一步地, 在所述系统中, 所述客户端, 针对所述多个节点中的任一节点, 判断对该节点的 SPV 请求的发送次数是否到达阈值, 若是, 对该节点延迟发送 SPV 请求。

[102] 与第二方面对应的, 本说明书实施例还提供一种联盟链的可信度验证装置, 在
25 用户生成交易, 并通过对接节点将所述交易上链存证后, 如图 5 所示, 图 5 为本说明书实施例所提供的一种可信度验证装置的结构示意图, 所述装置包括:

[103] 获取模块 501, 获取联盟链中的多个节点地址;

[104] 发送模块 503, 根据所述多个节点地址, 发送简单支付验证 SPV 请求至所述多

个节点，其中，所述 SPV 请求中包含所述交易的摘要哈希；

[105] 接收模块 505，接收所述多个节点分别返回的验证结果；

[106] 验证模块 507，根据所述多个节点分别返回的验证结果的一致程度，确定所述联盟链的可信度。

5 [107] 进一步地，所述获取模块 501，随机获取联盟链中的多个节点地址；或者，获取联盟链中包含所述对接节点地址的多个节点地址。

[108] 进一步地，所述发送模块 503 还用于，根据所述多个节点地址，发送交易位置查询请求至所述多个节点，其中，所述交易位置查询请求中包含所述交易的摘要哈希；所述接收模块 505，接收所述多个节点分别返回的位置查询结果；所述验证模块 507，

10 基于所述多个节点分别返回的位置查询结果的一致程度，验证包含所述交易信息的联盟链的可信度。

[109] 进一步地，所述发送模块 503，针对所述多个节点中的任一节点，判断对该节点的交易 SPV 请求的发送次数是否到达阈值，若是，对该节点延迟发送 SPV 请求。

[110] 与第三方面对应的，本说明书实施例还提供一种联盟链中的请求处理装置，位于所述联盟链中的节点上，如图 6 所示，图 6 为本说明书实施例所提供的一种请求处理装置的结构示意图，所述装置包括：

15

[111] 确定模块 601，所述节点确定自身节点用户的用户标识，并从确定出由用户标识组成的白名单，其中，所述用户标识用于标识用户身份，以及，用于标识和该用户对接的节点；

20 [112] 发送模块 603，发送白名单至联盟链中的其它节点，以便其它节点根据所述白名单确定是否执行非自身节点用户所发送的请求，所述请求包括交易位置查询请求或者简单支付验证 SPV 请求，所述请求中包含目标交易的摘要哈希。

[113] 进一步地，所述装置还包括，接收模块 605，接收任一用户所发送的请求，所述请求中还包括用户标识；判断模块 607，判断所述用户标识是否处于白名单中，若否，

25 不对请求执行处理。

[114] 进一步地，所述接收模块 605，接收任一用户所发送的请求，所述请求中还包括用户标识，当所述用户标识所对应的用户非自身节点用户时：所述确定模块 601 还用于，确定该节点对于其它节点用户所发起的请求的第一处理次数，以及，确认其它节点对于

该节点用户所发起的请求的第二处理次数；所述判断模块 607 还用于根据所述第一处理次数和第二处理次数，判断是否延迟处理所述请求。

5 [115] 本说明书实施例还提供一种计算机设备，其至少包括存储器、处理器及存储在存储器上并可在处理器上运行的计算机程序，其中，处理器执行所述程序时实现图 3 所示的联盟链的可信度验证方法。

[116] 本说明书实施例还提供一种计算机设备，其至少包括存储器、处理器及存储在存储器上并可在处理器上运行的计算机程序，其中，处理器执行所述程序时实现图 4 所示的联盟链中的请求处理方法。

10 [117] 图 7 示出了本说明书实施例所提供的一种更为具体的计算设备硬件结构示意图，该设备可以包括：处理器 1010、存储器 1020、输入/输出接口 1030、通信接口 1040 和总线 1050。其中处理器 1010、存储器 1020、输入/输出接口 1030 和通信接口 1040 通过总线 1050 实现彼此之间在设备内部的通信连接。

15 [118] 处理器 1010 可以采用通用的 CPU（Central Processing Unit，中央处理器）、微处理器、应用专用集成电路（Application Specific Integrated Circuit，ASIC）、或者一个或多个集成电路等方式实现，用于执行相关程序，以实现本说明书实施例所提供的技术方案。

20 [119] 存储器 1020 可以采用 ROM（Read Only Memory，只读存储器）、RAM（Random Access Memory，随机存取存储器）、静态存储设备，动态存储设备等形式实现。存储器 1020 可以存储操作系统和其他应用程序，在通过软件或者固件来实现本说明书实施例所提供的技术方案时，相关的程序代码保存在存储器 1020 中，并由处理器 1010 来调用执行。

25 [120] 输入/输出接口 1030 用于连接输入/输出模块，以实现信息输入及输出。输入输出/模块可以作为组件配置在设备中（图中未示出），也可以外接于设备以提供相应功能。其中输入设备可以包括键盘、鼠标、触摸屏、麦克风、各类传感器等，输出设备可以包括显示器、扬声器、振动器、指示灯等。

[121] 通信接口 1040 用于连接通信模块（图中未示出），以实现本设备与其他设备的通信交互。其中通信模块可以通过有线方式（例如 USB、网线等）实现通信，也可以通过无线方式（例如移动网络、WIFI、蓝牙等）实现通信。

[122] 总线 1050 包括一通路，在设备的各个组件（例如处理器 1010、存储器 1020、

输入/输出接口 1030 和通信接口 1040) 之间传输信息。

[123] 需要说明的是, 尽管上述设备仅示出了处理器 1010、存储器 1020、输入/输出接口 1030、通信接口 1040 以及总线 1050, 但是在具体实施过程中, 该设备还可以包括实现正常运行所必需的其他组件。此外, 本领域的技术人员可以理解的是, 上述设备中也可以仅包含实现本说明书实施例方案所必需的组件, 而不必包含图中所示的全部组件。

[124] 本说明书实施例还提供一种计算机可读存储介质, 其上存储有计算机程序, 该程序被处理器执行时实现图 3 所示的联盟链的可信度验证方法。

[125] 本说明书实施例还提供另一种计算机可读存储介质, 其上存储有计算机程序, 该程序被处理器执行时实现图 4 所示的联盟链中的请求处理方法。

10 [126] 计算机可读介质包括永久性和非永久性、可移动和非可移动媒体可以由任何方法或技术来实现信息存储。信息可以是计算机可读指令、数据结构、程序的模块或其他数据。计算机的存储介质的例子包括, 但不限于相变内存 (PRAM)、静态随机存取存储器 (SRAM)、动态随机存取存储器 (DRAM)、其他类型的随机存取存储器 (RAM)、只读存储器 (ROM)、电可擦除可编程只读存储器 (EEPROM)、快闪记忆体或其他
15 内存技术、只读光盘只读存储器 (CD-ROM)、数字多功能光盘 (DVD) 或其他光学存储、磁盒式磁带, 磁带磁磁盘存储或其他磁性存储设备或任何其他非传输介质, 可用于存储可以被计算设备访问的信息。按照本文中的界定, 计算机可读介质不包括暂存电脑可读媒体 (transitory media), 如调制的数据信号和载波。

[127] 通过以上的实施方式的描述可知, 本领域的技术人员可以清楚地了解到本说明书
20 书实施例可借助软件加必需的通用硬件平台的方式来实现。基于这样的理解, 本说明书实施例的技术方案本质上或者说对现有技术做出贡献的部分可以以软件产品的形式体现出来, 该计算机软件产品可以存储在存储介质中, 如 ROM/RAM、磁碟、光盘等, 包括若干指令用以使得一台计算机设备 (可以是个人计算机, 服务器, 或者网络设备等) 执行本说明书实施例各个实施例或者实施例的某些部分所述的方法。

25 [128] 上述实施例阐明的系统、方法、模块或单元, 具体可以由计算机芯片或实体实现, 或者由具有某种功能的产品来实现。一种典型的实现设备为计算机, 计算机的具体形式可以是个人计算机、膝上型计算机、蜂窝电话、相机电话、智能电话、个人数字助理、媒体播放器、导航设备、电子邮件收发设备、游戏控制台、平板计算机、可穿戴设备或者这些设备中的任意几种设备的组合。

[129] 本说明书中的各个实施例均采用递进的方式描述，各个实施例之间相同相似的部分互相参见即可，每个实施例重点说明的都是与其他实施例的不同之处。尤其，对于方法实施例而言，由于其基本相似于方法实施例，所以描述得比较简单，相关之处参见方法实施例的部分说明即可。以上所描述的方法实施例仅仅是示意性的，其中所述作为

5 分离部件说明的模块可以是或者也可以不是物理上分开的，在实施本说明书实施例方案时可以把各模块的功能在同一个或多个软件和/或硬件中实现。也可以根据实际的需要选择其中的部分或者全部模块来实现本实施例方案的目的。本领域普通技术人员在不付出创造性劳动的情况下，即可以理解并实施。

[130] 以上所述仅是本说明书实施例的具体实施方式，应当指出，对于本技术领域的

10 普通技术人员来说，在不脱离本说明书实施例原理的前提下，还可以做出若干改进和润饰，这些改进和润饰也应视为本说明书实施例的保护范围。

权利要求书

1、一种联盟链的可信度验证方法，在客户端生成交易，并通过对接节点将所述交易上链存证后，包括：

客户端获取联盟链中的多个节点地址；

5 根据所述多个节点地址，发送简单支付验证 SPV 请求至所述多个节点，其中，所述 SPV 请求中包含所述交易的摘要哈希；

任一节点接收所述 SPV 请求，基于所述摘要哈希执行 SPV 验证，验证所述交易是
否存在于所述联盟链中，并返回验证结果至客户端；

10 客户端基于所述多个节点分别返回的验证结果的一致程度，确定所述联盟链的可信度。

2、如权利要求 1 所述的方法，客户端获取联盟链中的多个节点地址，包括：

客户端随机获取联盟链中的多个节点地址；或者，

客户端获取联盟链中包含所述对接节点地址的多个节点地址。

3、如权利要求 1 所述的方法，还包括：

15 客户端根据所述多个节点地址，发送交易位置查询请求至所述多个节点，其中，所述交易位置查询请求中包含所述交易的摘要哈希；

任一节点接收所述位置查询请求，基于所述摘要哈希各自查询所述摘要哈希所对应的交易在所述联盟链中的位置信息，并返回所述位置查询结果至客户端；

20 客户端基于所述多个节点分别返回的位置查询结果的一致程度，验证包含所述交易信息的联盟链的可信度。

4、如权利要求 1 所述的方法，在客户端获取联盟链中的多个节点地址之前，所述方法还包括：

联盟链中的任一节点确定自身的白名单，并广播白名单至联盟链中的其它节点，以便其它节点根据所述白名单确定是否执行 SPV 验证处理；

25 所述 SPV 请求中包含所述交易的摘要哈希，包括：所述 SPV 请求包含所述交易的摘要哈希和所述客户端标识；

任一节点接收所述 SPV 请求之后，还包括：确定所述 SPV 请求所包含的客户端标识是否处于白名单中，若否，不执行 SPV 验证处理。

30 5、如权利要求 1 所述的方法，在任一节点接收所述 SPV 请求之后，所述方法还包括：

该节点确定自身对于其它节点用户所发起的 SPV 请求的第一处理次数，以及，确

认其它节点对于该节点用户所发起的 SPV 请求的第二处理次数;

根据所述第一处理次数和第二处理次数, 判断是否延迟处理所述 SPV 请求。

6、如权利要求 1 所述的方法, 发送 SPV 请求至所述多个节点, 包括:

针对所述多个节点中的任一节点, 判断对该节点的 SPV 请求的发送次数是否到达

5 阈值, 若是, 对该节点延迟发送 SPV 请求。

7、一种联盟链的可信度验证方法, 在用户生成交易, 并通过对接节点将所述交易上链存证后, 包括:

获取联盟链中的多个节点地址;

10 根据所述多个节点地址, 发送简单支付验证 SPV 请求至所述多个节点, 其中, 所述 SPV 请求中包含所述交易的摘要哈希;

根据所述多个节点分别返回的验证结果的一致程度, 确定所述联盟链的可信度。

8、如权利要求 7 所述的方法, 获取联盟链中的多个节点地址, 包括:

随机获取联盟链中的多个节点地址; 或者,

获取联盟链中包含所述对接节点地址的多个节点地址。

15 9、如权利要求 7 所述的方法, 还包括:

根据所述多个节点地址, 发送交易位置查询请求至所述多个节点, 其中, 所述交易位置查询请求中包含所述交易的摘要哈希;

基于所述多个节点分别返回的位置查询结果的一致程度, 验证包含所述交易信息的联盟链的可信度。

20 10、如权利要求 7 所述的方法, 发送 SPV 请求至所述多个节点, 包括:

针对所述多个节点中的任一节点, 判断对该节点的 SPV 请求的发送次数是否到达阈值, 若是, 对该节点延迟发送 SPV 请求。

11、一种联盟链中的请求处理方法, 在节点为联盟链中的节点时, 包括:

25 所述节点确定自身节点用户的用户标识, 并从确定出由用户标识组成的白名单, 其中, 所述用户标识用于标识用户身份, 以及, 用于标识和该用户对接的节点;

发送白名单至联盟链中的其它节点, 以便其它节点根据所述白名单确定是否执行非自身节点用户所发送的请求, 所述请求包括交易位置查询请求或者简单支付验证 SPV 请求, 所述请求中包含目标交易的摘要哈希。

12、如权利要求 11 所述的请求处理方法, 包括:

30 节点接收任一用户所发送的请求, 所述请求中还包括用户标识;

判断所述用户标识是否处于白名单中, 若否, 不对请求执行处理。

13、如权利要求 11 所述的方法，还包括：

接收任一用户所发送的请求，所述请求中还包括用户标识，当所述用户标识所对应的用户非自身节点用户时：

- 5 确定该节点对于其它节点用户所发起的请求的第一处理次数，以及，确认其它节点对于该节点用户所发起的请求的第二处理次数；
- 根据所述第一处理次数和第二处理次数，判断是否延迟处理所述请求。

14、一种联盟链的可信度验证系统，包括客户端和联盟链网络，所述联盟链网络包括多个节点，在客户端生成交易，并通过对接节点将所述交易上链存证后，

客户端获取联盟链中的多个节点地址；

- 10 根据所述多个节点地址，发送简单支付验证 SPV 请求至所述多个节点，其中，所述 SPV 请求中包含所述交易的摘要哈希；

联盟链网络中的任一节点接收所述 SPV 请求，基于所述摘要哈希执行 SPV 验证，验证所述交易是否存在于所述联盟链中，并返回验证结果至客户端；

- 15 客户端基于所述多个节点分别返回的验证结果的一致程度，确定所述联盟链的可信度。

15、如权利要求 14 所述的系统，客户端随机获取联盟链中的多个节点地址；或者，客户端获取联盟链中包含所述对接节点地址的多个节点地址。

16、如权利要求 14 所述的系统，

- 20 客户端根据所述多个节点地址，发送交易位置查询请求至所述多个节点，其中，所述交易位置查询请求中包含所述交易的摘要哈希；

任一节点接收所述位置查询请求，基于所述摘要哈希各自查询所述摘要哈希所对应的交易在所述联盟链中的位置信息，并返回所述位置查询结果至客户端；

客户端基于所述多个节点分别返回的位置查询结果的一致程度，验证包含所述交易信息的联盟链的可信度。

- 25 17、如权利要求 14 所述的系统，在客户端获取联盟链中的多个节点地址之前，

联盟链中的任一节点确定自身的白名单，并广播白名单至联盟链中的其它节点，以便其它节点根据所述白名单确定是否执行 SPV 验证处理；

所述 SPV 请求中包含所述交易的摘要哈希，包括：所述 SPV 请求包含所述交易的摘要哈希和所述客户端标识；

- 30 任一节点接收所述 SPV 请求之后，还包括：确定所述 SPV 请求所包含的客户端标识是否处于白名单中，若否，不执行 SPV 验证处理。

18、如权利要求 14 所述的系统，在任一节点接收所述 SPV 之后，

该节点确定自身对于其它节点用户所发起的 SPV 的第一处理次数，以及，确认其它节点对于该节点用户所发起的 SPV 的第二处理次数；

根据所述第一处理次数和第二处理次数，判断是否延迟处理所述 SPV 请求。

- 5 19、如权利要求 14 所述的系统，所述客户端，针对所述多个节点中的任一节点，判断对该节点的 SPV 请求的发送次数是否到达阈值，若是，对该节点延迟发送 SPV 请求。

20、一种联盟链的可信度验证装置，在用户生成交易，并通过对接节点将所述交易上链存证后，包括：

- 10 获取模块，获取联盟链中的多个节点地址；
发送模块，根据所述多个节点地址，发送简单支付验证 SPV 请求至所述多个节点，其中，所述 SPV 请求中包含所述交易的摘要哈希；
接收模块，接收所述多个节点分别返回的验证结果；
验证模块，根据所述多个节点分别返回的验证结果的一致程度，确定所述联盟链的
15 可信度。

21、如权利要求 20 所述的装置，所述获取模块随机获取联盟链中的多个节点地址；或者，获取联盟链中包含所述对接节点地址的多个节点地址。

22、如权利要求 20 所述的装置，还包括：

- 所述发送模块还用于，根据所述多个节点地址，发送交易位置查询请求至所述多个
20 节点，其中，所述交易位置查询请求中包含所述交易的摘要哈希；
所述接收模块，接收所述多个节点分别返回的位置查询结果；
所述验证模块，基于所述多个节点分别返回的位置查询结果的一致程度，验证包含所述交易信息的联盟链的可信度。

- 23、如权利要求 20 所述的装置，所述发送模块，针对所述多个节点中的任一节点，
25 判断对该节点的交易 SPV 请求的发送次数是否到达阈值，若是，对该节点延迟发送 SPV 请求。

24、一种联盟链中的请求处理请求处理装置，位于所述联盟链中的节点上，包括：

确定模块，所述节点确定自身节点用户的用户标识，并从确定出由用户标识组成的白名单，其中，所述用户标识用于标识用户身份，以及，用于标识和该用户对接的节点；

- 30 发送模块，发送白名单至联盟链中的其它节点，以便其它节点根据所述白名单确定是否执行非自身节点用户所发送的请求，所述请求包括交易位置查询请求或者简单支付

验证 SPV 请求，所述请求中包含目标交易的摘要哈希。

25、如权利要求 24 所述的装置，包括：

接收模块，节点接收任一用户所发送的请求，所述请求中还包括用户标识；

判断模块，判断所述用户标识是否处于白名单中，若否，不对请求执行处理。

5 26、如权利要求 24 所述的请求处理装置，

所述接收模块，接收任一用户所发送的请求，所述请求中还包括用户标识，当所述用户标识所对应的用户非自身节点用户时：

所述确定模块还用于，确定该节点对于其它节点用户所发起的请求的第一处理次数，以及，确认其它节点对于该节点用户所发起的请求的第二处理次数；

10 所述判断模块还用于根据所述第一处理次数和第二处理次数，判断是否延迟处理所述请求。

27、一种计算机设备，包括存储器、处理器及存储在存储器上并可在处理器上运行的计算机程序，其中，所述处理器执行所述程序时实现如权利要求 7 至 10 任一项所述的方法。

15 28、一种计算机设备，包括存储器、处理器及存储在存储器上并可在处理器上运行的计算机程序，其中，所述处理器执行所述程序时实现如权利要求 11 至 13 任一项所述的方法。