

(12) 按照专利合作条约所公布的国际申请

(19) 世界知识产权组织
国际局

(43) 国际公布日
2021年2月18日 (18.02.2021)

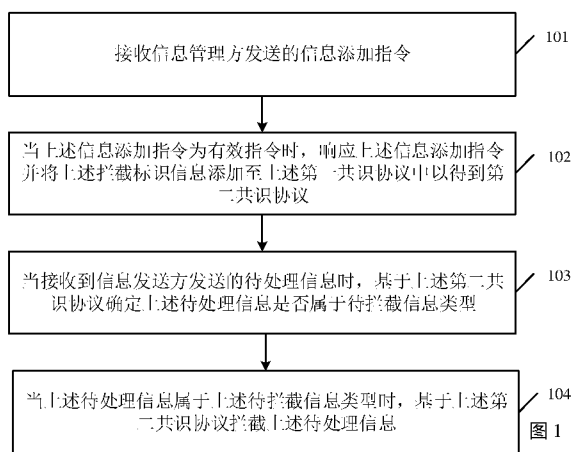


(10) 国际公布号
WO 2021/027504 A1

- (51) 国际专利分类号:
H04L 29/06 (2006.01)
- (21) 国际申请号: PCT/CN2020/103255
- (22) 国际申请日: 2020年7月21日 (21.07.2020)
- (25) 申请语言: 中文
- (26) 公布语言: 中文
- (30) 优先权:
201910751646.6 2019年8月15日 (15.08.2019) CN
- (71) 申请人: 深圳壹账通智能科技有限公司(ONE CONNECT SMART TECHNOLOGY CO., LTD. (SHENZHEN)) [CN/CN]; 中国广东省深圳市前海深港合作区前湾一路1号A栋201
- 室 (入驻深圳市前海商务秘书有限公司), Guangdong 518000 (CN)。
- (72) 发明人: 冯承勇 (FENG, Chengyong); 中国广东省深圳市前海深港合作区前湾一路1号A栋201室 (入驻深圳市前海商务秘书有限公司), Guangdong 518000 (CN)。
- (74) 代理人: 广州三环专利商标代理有限公司 (SCIHEAD IP LAW FIRM); 中国广东省广州市越秀区先烈中路80号汇华商贸大厦1508室, Guangdong 510070 (CN)。
- (81) 指定国(除另有指明, 要求每一种可提供的国家保护): AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DJ, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, IT,

(54) Title: CONSENSUS PROTOCOL-BASED INFORMATION PROCESSING METHOD, AND RELATED DEVICE

(54) 发明名称: 基于共识协议的信息处理方法及相关装置



- 101 Receive an information adding instruction sent by an information management party
- 102 If the information adding instruction is a valid instruction, add, in response to the information adding instruction, interception identifier information to a first consensus protocol to obtain a second consensus protocol
- 103 Upon receiving information to be processed that is sent by an information sending party, determine, on the basis of the second consensus protocol, whether the information belongs to an information type to be intercepted
- 104 If so, intercept the information on the basis of the second consensus protocol

(57) Abstract: An embodiment of the present application discloses a consensus protocol-based information processing method, realizable in a blockchain. The method is applicable to transaction verification. The method comprises: receiving an information adding instruction sent by an information management party; if the information adding instruction is a valid instruction, adding, in response to the information adding instruction, interception identifier information to a first consensus protocol to obtain a second consensus protocol; upon receiving information to be processed that is sent by an information sending party, determining, on the basis of the second con-

WO 2021/027504 A1

JO, JP, KE, KG, KH, KN, KP, KR, KW, KZ, LA, LC, LK, LR, LS, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SA, SC, SD, SE, SG, SK, SL, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, WS, ZA, ZM, ZW。

(84) 指定国(除另有指明, 要求每一种可提供的地区保护): ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, ST, SZ, TZ, UG, ZM, ZW), 欧亚 (AM, AZ, BY, KG, KZ, RU, TJ, TM), 欧洲 (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, KM, ML, MR, NE, SN, TD, TG)。

本国际公布:

— 包括国际检索报告(条约第21条(3))。

sensus protocol, whether the information belongs to an information type to be intercepted; and if so, intercepting the information on the basis of the second consensus protocol. The embodiment of the present application enables intercepting information of an information type to be intercepted on the basis of a consensus protocol, thereby improving information processing, and providing wide applicability.

(57) 摘要: 本申请实施例公开了一种基于共识协议的信息处理方法, 可在区块链中实现。该方法适用于交易验证。该方法包括: 接收信息管理方发送的信息添加指令; 当信息添加指令为有效指令时, 响应信息添加指令并将拦截标识信息添加至第一共识协议中以得到第二共识协议; 当接收到信息发送方发送的待处理信息时, 基于第二共识协议确定待处理信息是否属于待拦截信息类型; 当待处理信息属于待拦截信息类型时, 基于第二共识协议拦截待处理信息。采用本申请实施例, 可基于共识协议拦截属于待拦截信息类型的信息, 可提高信息处理水平, 适用性高。

基于共识协议的信息处理方法及相关装置

[0001] 本申请要求于2019年08月15日提交中国专利局、申请号为201910751646.6，发明名称为“基于共识协议的信息处理方法及相关装置”的中国专利申请的优先权，其全部内容通过引用结合在本申请中。

技术领域

[0002] 本申请涉及计算机技术领域，尤其涉及一种基于共识协议的信息处理方法及相关装置。

背景技术

[0003] 区块链是分布式数据存储、点对点传输、共识机制、加密算法等技术集合的创新型技术。近年来，区块链网络在创建前期就已经完成了内部共识协议的配置，从而区块链网络中的节点依据区块链网络内嵌的共识协议，完成对进入区块链网络的信息的验证和确认。

[0004] 发明人意识到，在创建区块链之后，现有技术中的共识协议以固定且不可修改的形式配置于区块链网络中，无法满足区块链创建者日渐增加或变化的信息处理需求。

发明概述

技术问题

[0005] 本申请实施例提供一种基于共识协议的信息处理方法及相关装置，可基于共识协议实现对属于待拦截信息类型的信息进行拦截，提高信息识别能力和处理水平，适用性高。

问题的解决方案

技术解决方案

[0006] 第一方面，本申请实施例提供一种基于共识协议的信息处理方法，该方法包括。

[0007] 接收信息管理方发送的信息添加指令，上述信息添加指令中携带拦截标识信息，上述信息添加指令用于指示向第一共识协议中添加上述拦截标识信息，上述

拦截标识信息用于确定接收到的信息是否属于待拦截信息类型。

[0008] 当上述信息添加指令为有效指令时，响应上述信息添加指令并将上述拦截标识信息添加至上述第一共识协议中以得到第二共识协议。

[0009] 当接收到信息发送方发送的待处理信息时，基于上述第二共识协议确定上述待处理信息是否属于上述待拦截信息类型。

[0010] 当上述待处理信息属于上述待拦截信息类型时，基于上述第二共识协议拦截上述待处理信息。

[0011] 第二方面，本申请实施例提供了一种基于共识协议的信息处理装置，该信息处理装置包括。

[0012] 接收单元，用于接收信息管理方发送的信息添加指令，上述信息添加指令中携带拦截标识信息，上述信息添加指令用于指示向第一共识协议中添加上述拦截标识信息，上述拦截标识信息用于确定接收到的信息是否属于待拦截信息类型。

[0013] 响应单元，用于当上述接收单元接收到的上述信息添加指令为有效指令时，响应上述信息添加指令并将上述拦截标识信息添加至上述第一共识协议中以得到第二共识协议。

[0014] 确定单元，用于当接收到信息发送方发送的待处理信息时，基于上述响应单元得到的上述第二共识协议确定上述待处理信息是否属于上述待拦截信息类型。

[0015] 拦截单元，用于当上述待处理信息属于上述待拦截信息类型时，基于上述第二共识协议拦截上述待处理信息。

[0016] 第三方面，本申请实施例提供了一种终端设备，该终端设备包括存储器和处理器，所述处理器、和所述存储器相互连接，其中，所述存储器用于存储计算机程序，所述计算机程序包括程序指令，所述处理器用于执行所述存储器的所述程序指令，其中。

[0017] 接收信息管理方发送的信息添加指令，所述信息添加指令中携带拦截标识信息，所述信息添加指令用于指示向第一共识协议中添加所述拦截标识信息，所述拦截标识信息用于确定接收到的信息是否属于待拦截信息类型。

[0018] 当所述信息添加指令为有效指令时，响应所述信息添加指令并将所述拦截标识

信息添加至所述第一共识协议中以得到第二共识协议。

[0019] 当接收到信息发送方发送的待处理信息时，基于所述第二共识协议确定所述待处理信息是否属于所述待拦截信息类型。

[0020] 当所述待处理信息属于所述待拦截信息类型时，基于所述第二共识协议拦截所述待处理信息。

[0021] 第四方面，本申请实施例提供了一种计算机可读存储介质，所述计算机可读存储介质存储有计算机程序，所述计算机程序包括程序指令，所述程序指令被处理器执行时，用于实现以下步骤。

[0022] 接收信息管理方发送的信息添加指令，所述信息添加指令中携带拦截标识信息，所述信息添加指令用于指示向第一共识协议中添加所述拦截标识信息，所述拦截标识信息用于确定接收到的信息是否属于待拦截信息类型。

[0023] 当所述信息添加指令为有效指令时，响应所述信息添加指令并将所述拦截标识信息添加至所述第一共识协议中以得到第二共识协议。

[0024] 当接收到信息发送方发送的待处理信息时，基于所述第二共识协议确定所述待处理信息是否属于所述待拦截信息类型。

[0025] 当所述待处理信息属于所述待拦截信息类型时，基于所述第二共识协议拦截所述待处理信息。

发明的有益效果

有益效果

[0026] 在本申请实施例中，在将信息添加指令中携带的拦截标识信息添加至共识协议后可得到具备确定接收到的信息是否属于待拦截信息类型的新的共识协议。当接收到信息发送方发送的待处理信息时，可基于新的共识协议拦截属于待拦截信息类型的待处理信息，进而提升信息处理水平，适用性更高。

对附图的简要说明

附图说明

[0027] 图1是本申请实施例提供的基于共识协议的信息处理方法的一流程示意图。

[0028] 图2是本申请实施例提供的基于共识协议的信息处理方法的另一流程示意图。

[0029] 图3是本申请实施例提供的基于共识协议的信息处理装置的结构示意图。

[0030] 图4是本申请实施例提供的终端设备的结构示意图。

发明实施例

本发明的实施方式

[0031] 本申请实施例提供的基于共识协议的信息处理方法（为方便描述，可简称本申请实施例提供的方法）可适用于各个领域、各个行业中的各个企业的区块链网络，也可适用于基于共识协议实现信息处理的信息系统等，在此不做限制。为方便描述，下面可以某一个领域和/或某一个行业中的某一个区块链网络为例，对本申请实施例提供的方法进行描述。区块链网络具体可指一个由各节点通过共识协议达成的、具有分布式数据存储结构的网络系统，且根据具体的共识协议的不同，达成全部或部分节点的信息全备份。由于区块链网络在相应共识协议下运行，区块链网络与相应共识协议之间存在既定的配置联系，因此为了基于共识协议能够实现对某些特定信息的拦截，故可通过向共识协议中添加拦截标识信息以使共识协议能够确定出需要拦截的信息，进而对需要拦截的信息进行拦截。其中，上述共识协议包括但不限于工作量证明机制（Proof of Work, PoW）、权益证明机制（Proof of Stake, PoS）、股份授权证明机制（Delegated Proof of Stake, DPoS）、实用拜占庭机制（Practical Byzantine Fault Tolerance, PBFT）以及Ripple共识算法，在此不做限制。

[0032] 下面将结合图1至图4对本申请实施例提供的方法及相关装置进行说明。参见图1，图1是本申请实施例提供的基于共识协议的信息处理方法的一流程示意图。本申请实施例提供的方法可包括如下步骤101-104。

[0033] 101、接收信息管理方发送的信息添加指令。

[0034] 在一些可行的实施方式中，在向共识协议中添加的拦截标识信息之前，区块链网络中的区块链节点可先接收信息管理方发送的信息添加指令。其中，上述信息添加指令中携带有拦截标识信息，上述拦截标识信息用于确定接收到的信息是否属于待拦截信息类型。例如，当区块链节点接收到信息管理方发送的信息添加指令中携带的拦截标识信息为“虚拟账户”，并将拦截标识信息“虚拟账户”添加至共识协议后，共识协议可基于拦截标识信息“虚拟账户”判断区块

链节点接收到的信息是否携带有“虚拟账户”信息。当区块链节点接收到的信息中包含有“虚拟账户”信息时，可将区块链节点接收到的信息确定为待拦截信息类型，也就是说此时区块链节点需要对此时接收到的信息进行拦截。其中，上述信息管理方可以是区块链网络的管理设备，也可以是共识协议的开发终端等，在此不做限制。

[0035] 在一些可行的实施方式中，为了保证信息管理方将上述信息添加指令发送至区块链节点的过程中，上述信息添加指令的指令信息不被篡改，因此信息管理方在生成信息添加指令之后，可对上述信息添加指令信息进行加密处理。例如，信息管理方可采用区块链网络的公钥对上述信息添加指令进行加密得到上述信息添加指令对应的密文信息，并将所述密文信息发送至区块链节点。再例如，信息管理方可对上述信息添加指令进行哈希运算，得到上述信息添加指令的唯一摘要信息。同时采用信息管理方的私钥对上述唯一摘要信息进行加密以得到上述信息添加指令的数字签名，并将上述数字签名与上述信息添加指令的密文信息一起发送至区块链节点。其中，上述唯一摘要信息是将上述信息添加指令进行哈希运算后得到的一个固定长度的唯一的字符串，该字符串的具体表现形式在此不做限制。

[0036] 在一些可行的实施方式中，区块链节点在接收信息管理方发送的信息添加指令之前，为了防止接收到错误指令或者接收到被篡改的指令，可对上述信息添加指令进行指令有效性验证。当信息管理方将采用区块链网络的公钥对上述信息添加指令进行加密得到的密文信息发送至区块链节点时，若区块链节点采用区块链网络的私钥对上述密文信息成功解密，则证明上述密文信息没有被篡改，也就是说上述信息添加指令为有效指令。当区块链节点在接收到上述密文信息的同时也接收到上述信息添加指令对应的数字签名时，可采用区块链网络的私钥对上述密文信息进行解密，得到信息添加指令。在通过对上述密文信息进行解密得到信息添加指令之后，对该信息添加指令进行哈希运算得到该信息添加指令对应的实际唯一摘要信息。同时，采用信息管理方的公钥对接收到的数字签名进行解密，得到信息管理方发送的信息添加指令对应的唯一摘要信息。将上述实际唯一摘要信息与上述唯一摘要信息进行对比，如果两者信息一致，则

证明上述密文信息和上述数字签名没有被篡改，也就是说上述信息添加指令为有效指令。可选的，在对上述密文信息和/或上述数字签名进行解密之前，也可先判断上述信息管理方发送的信息添加指令中是否包含区块链节点的身份标识。如果上述信息添加指令中不包含区块链节点的身份标识，则说明上述信息添加指令不是发送至区块链节点的指令信息，此时区块链节点不对上述信息添加指令做任何处理。相反，如果上述信息添加指令中包含区块链节点的身份标识，则证明上述信息添加指令时发送至区块链节点的指令信息，此时区块链节点可对上述信息添加指令进行指令有效性验证。其中，上述身份标识可以是特定的数字、字母以及字符的一种或多种组合，具体表现形式在此不做限制。需要特别说明的是，验证上述信息添加指令中是否包括区块链节点的身份标识信息的过程可根据实际应用场景确定，在此不做限制。

[0037] 102、当上述信息添加指令为有效指令时，响应上述信息添加指令并将上述拦截标识信息添加至上述第一共识协议中以得到第二共识协议。

[0038] 在一些可行的实施方式中，由于现有的共识协议都是以固定且不可修改的形式配置与区块链网络中，仅根据不同的应用场景采用不同的共识协议对信息进行处理。因此，当上述信息添加指令为有效指令时，可响应上述信息添加指令并将上述信息添加指令中携带的拦截标识信息添加至第一共识协议中得到第二共识协议，以使上述第二共识协议能够识别区块链节点接收到的信息中是否包含上述拦截标识信息。其中，上述第一共识协议可以为在特定应用场景下对应的共识协议，上述第二共识协议为在上述第一共识协议基础之上添加了拦截标识信息之后生成的具备识别出拦截标识信息能力的新的共识协议。需要特别说明的是，上述第二共识协议与上述第一共识协议的区别仅限于上述第二共识协议可识别出区块链节点接收的信息中是否包含上述拦截标识信息，第二共识协议与第一共识协议部署于区块链网络上的配置信息等完全一致，在此不再赘述。

[0039] 在一些可行的实施方式中，在将上述信息添加指令中携带的拦截标识信息添加至上述第一共识协议中时，可在更新上述第一共识协议的过程中通过向上述第一共识协议中增加识别拦截标识信息的命令，以达到在不影响上述第一共识协议原功能的情况下在上述第一共识协议中添加拦截标识信息的识别功能，并将

添加识别功能后的第一共识协议确定为第二共识协议。或者，可选的，可将识别上述拦截标识信息的功能生成识别功能脚本并将该识别功能脚本部署于上述第一共识协议中以得到第二共识协议。当基于上述第二共识协议识别区块链节点接收到的任一信息中是否包含上述拦截标识信息时，上述第二共识协议通过上述识别功能脚本的脚本路径，调用上述识别功能脚本以识别区块链节点接收到的信息中是否包含上述拦截标识信息。需要特别说明的是，上述识别拦截标识信息的命令和上述识别功能脚本中均包含上述拦截标识信息，且包含的拦截标识信息可作为具体识别过程中的识别依据。同时，在将上述信息添加指令中携带的拦截标识信息添加至上述第一共识协议中的具体方式包括但不限于上述所示的实现方式，具体可根据实际应用场景确定，在此不做限制。

[0040] 103、当接收到信息发送方发送的待处理信息时，基于上述第二共识协议确定上述待处理信息是否属于待拦截信息类型。

[0041] 在一些可行的实施方式中，在得到上述第二共识协议之后，当区块链节点接收到信息发送方发送的待处理信息时，区块链节点可通过上述第二共识协议判断上述待处理信息中是否包含上述拦截标识信息。其中，上述信息发送方包括但不限于交易发起平台、身份验证平台、用户管理平台以及产品供应方等，在此不做限制。若上述待处理信息中包含上述拦截标识信息，则确定上述待处理信息属于上述待拦截信息类型。若上述待处理信息中不包含上述拦截标识信息，则确定上述待处理信息不属于上述待拦截信息类型。需要特别说明的是，由于上述待处理信息有多种信息来源，因此当信息发送方将上述待处理信息发送至区块链节点时，上述待处理信息的信息表现形式可能与上述第二共识协议中的拦截标识信息的信息表现性质不一致。例如，当上述拦截标识信息为二进制字符串时，上述信息发送方发送的待处理信息可能为数字与字母的组合形式，两种信息表现形式无法进行比较识别，此时上述第二共识协议不能基于上述拦截标识信息确定上述待处理信息是否属于待拦截信息类型。因此，当区块链节点接收到信息发送方发送的待处理信息时，可判断上述待处理信息的信息表现形式与上述第二共识协议中的拦截标识信息的信息表现形式是否一致，若一致，则基于上述第二共识协议确定上述待处理信息是否属于待拦截信息。若不一致

，则可对上述拦截标识信息或者上述待处理信息进行信息处理以使上述拦截标识信息与上述待处理信息的信息表现形式一致，进而基于上述第二共识协议确定上述待处理信息是否属于待拦截信息。

[0042] 在一些可行的实施方式中，在基于上述第二共识协议确定上述待处理信息是否属于待拦截信息类型时，可基于上述第二共识协议中的拦截标识信息从预设信息库中确定出与上述拦截标识信息语义一致，且属于上述待拦截信息类型的至少一个目标信息。其中，上述预设信息库中的信息可以是基于互联网、数据库或者其他存储空间中获取的常见拦截信息，也可以是由信息发送方、信息接收方以及信息管理方预先指定的拦截信息，具体来源不做限制。当区块链节点接收到信息发送方发送的待处理信息后，可确定上述待处理信息中是否包含上述至少一个目标信息中的任一目标信息，当上述待处理信息中包含上述任一目标信息，则确定上述待处理信息属于上述待拦截信息类型。当上述待处理信息中不包含上述至少一个目标信息中的任何目标信息时，可确定上述待处理信息不属于上述待拦截信息类型。在基于预设信息库中的至少一个目标信息来确定上述待处理信息是否属于上述待拦截信息类型时，多个目标信息可扩大上述待拦截信息类型的范围，从而提升确定上述待处理信息是否属于待拦截信息类型的准确度和全面性，适用性更高。

[0043] 104、当上述待处理信息属于上述待拦截信息类型时，基于上述第二共识协议拦截上述待处理信息。

[0044] 在一些可行的实施方式中，当基于上述第二共识协议确定信息发送方发送的待处理信息属于上述待拦截信息类型时，可基于上述第二共识协议拦截上述待处理信息。可选的，在具体的待处理信息拦截过程中，上述第二共识协议可选择不对上述待处理信息进行验证。也就是说，当上述待处理信息属于上述待拦截信息类型时，即使区块链节点接收到上述待处理信息，由于上述第二共识协议不对上述待处理信息进行验证，因此上述待处理信息在未得到第二共识协议的验证的情况下，区块链节点不会将上述待处理信息写入区块链，也不会通过区块链网络将上述待处理信息发送至任一信息接收方，从而达到拦截上述待处理信息的目的。在上述第二共识协议拒绝对上述待处理信息进行验证的情况下，

区块链节点可删除上述待处理信息以降低区块链网络资源消耗。可选的，区块链节点在删除上述待处理信息之后，或者在上述第二共识协议拒绝对上述待处理信息进行验证的情况下，可生成拒绝指令并将该拒绝指令发送至上述信息发送方。其中上述拒绝指令可以是数字、字母以及其他符号的一种或多种组合序列，在此不做限制。此外，当上述拒绝指令中包含有修改指示信息时，上述信息发送方可在接收到上述拒绝指令之后，根据上述拒绝指令中修改指示信息来修改上述被拦截的待处理信息，并将修改后的待处理信息重新发送至区块链节点。

[0045] 在一些可行的实施方式中，当上述待处理信息不属于上述待拦截信息类型时，可基于上述第一共识协议和或者上述第二共识协议中的既定协议内容对上述待处理信息进行验证。例如，当上述第一共识协议和上述的第二共识协议PoW机制时，可基于上述待处理信息中所指示的工作量为上述信息发送方提供相应的报酬。当上述第一共识协议和上述第二共识协议为重要程度证明机制时，可基于上述待处理信息中所指示的信息发送方的重要程度来分配相关资源。当区块链节点基于上述第一共识协议或者上述第二共识协议对上述待处理信息进行验证处理之后，可将得到的结果信息写入区块链网络中进而通过区块链网络将上述结果信息发送至与区块链网络连接的各信息接收方，其中，上述信息接收方包括但不限于账户管理平台、数据结算平台以及信息发布平台等，在此不做限制。

[0046] 由于在将拦截标识信息添加至上述第一共识协议得到上述第二共识协议之后，上述第二共识协议会一直确定区块链节点接收到的任何待处理信息是否属于待拦截信息类型，因此当不需要拦截包含上述拦截标识信息的待处理信息时，需要删除上述第二共识协议中的拦截标识信息。请参见图2，图2是本申请实施例提供的基于共识协议的信息处理方法的另一流程示意图。本申请实施例提供的基于共识协议的信息处理方法的另一流程示意图中包括如下步骤201-203。

[0047] 201、接收信息管理方发送的信息删除指令。

[0048] 在一些可行的实施方式中，当不需要拦截包含上述拦截标识信息的待处理信息时，可接收信息管理方发送的信息删除指令。其中，由于上述第二共识协议中

可能包含多个拦截标识信息，因此上述信息删除指令中需要包含具体的拦截标识信息以删除上述第二共识协议中对应的拦截标识信息。例如，当区块链节点将多个拦截标识信息“虚拟账户”、“密码”添加至上述第一共识协议得到第二共识协议后，基于上述第二共识协议可拦截包含有“虚拟账户”、“密码”信息的待处理信息。当不需要拦截包含有“虚拟账户”信息的待处理信息时，信息管理方可生成包含有“虚拟账户”信息的信息删除指令以删除上述第二共识协议中的拦截标识信息“虚拟账户”。需要特别说明的是，当信息管理方生成上述信息删除指令时，可对上述信息删除指令进行加密处理，具体实现方式可参见步骤101中所示，在此不再赘述。

[0049] 202、当上述信息删除指令为有效指令时，响应上述信息删除指令并删除第二共识协议中的拦截信息标识以得到第三共识协议。

[0050] 在一些可行的实施方式中，在信息管理方生成信息删除指令并将上述信息删除指令发送至区块链节点后，区块链节点可对上述信息删除指令的身份标识和/或指令有效性进行验证，具体实现方式可参见步骤101中所示，在此不再赘述。当上述信息删除指令为有效指令时，区块链节点可响应上述信息删除指令并基于上述信息删除指令中所包含的拦截标识信息删除上述第二共识协议中对应的拦截标识信息，进而得到第三共识协议。例如，当上述第二共识协议中包含拦截标识信息“虚拟账户”、“密码”，也就是说在基于上述第二共识协议拦截包含有“虚拟账户”、“密码”信息的待处理信息时，如果上述信息删除指令中包含有“虚拟账户”信息时，可删除上述第二共识协议中的拦截标识信息“虚拟账户”。在此基础上得到的第三共识协议中只包含拦截标识信息“密码”，也就是说此时上述第三共识协议只拦截包含有“密码”信息的待处理信息，不再对包含“虚拟账户”信息的待处理信息进行拦截。

[0051] 203、当接收到信息发送方发送的待处理信息时，基于上述第三共识协议对上述待处理信息进行处理。

[0052] 在一些可行的实施方式中，由于区块链节点在响应上述信息删除指令并删除上述第二共识协议中与所述信息删除指令对应的拦截标识信息之后，得到的第三共识实现协议中可能还包括至少一个其他拦截标识信息。因此，此时接收到信息

管理方发送的待处理信息之后，可基于上述第三共识协议中的拦截标识信息对上述待处理信息进行拦截。或者当删除上述第二共识协议中唯一的拦截标识信息时，可基于此时得到的第三共识协议或者上述第一共识协议对上述待处理信息进行处理，具体处理方式可参见步骤104中所示，在此不再赘述。

[0053] 在本申请实施例中，在将信息添加指令中携带的拦截标识信息添加至共识协议后可得到具备确定接收到的信息是否属于待拦截信息类型的共识协议。当接收到信息发送方发送的待处理信息时，可基于新的共识协议拦截属于待拦截信息类型的待处理信息，进而提升信息处理水平。同时，通过信息删除指令可删除共识协议中的拦截标识信息，从而灵活调整待拦截信息类型，灵活性强，适用性更高。

[0054] 参见图3，图3是本申请实施例提供的基于共识协议的信息处理装置的结构示意图。本申请实施例提供的信息处理装置包括。

[0055] 接收单元31，用于接收信息管理方发送的信息添加指令，上述信息添加指令中携带拦截标识信息，上述信息添加指令用于指示向第一共识协议中添加上述拦截标识信息，上述拦截标识信息用于确定接收到的信息是否属于待拦截信息类型。

[0056] 响应单元32，用于当上述接收单元31接收到的上述信息添加指令为有效指令时，响应上述信息添加指令并将上述拦截标识信息添加至上述第一共识协议中以得到第二共识协议。

[0057] 确定单元33，用于当接收到信息发送方发送的待处理信息时，基于上述响应单元32得到的上述第二共识协议确定上述待处理信息是否属于上述待拦截信息类型。

[0058] 拦截单元34，用于当上述待处理信息属于上述待拦截信息类型时，基于上述第二共识协议拦截上述待处理信息。

[0059] 在一些可行的实施方式中，上述信息处理装置还包括。

[0060] 解密单元35，用于当上述信息添加指令中包括指令处理对象的身份标识时，将上述数字签名进行解密得到第一解密信息，将上述密文信息进行解密得到第二解密信息。

- [0061] 上述确定单元33，还用于当上述第一解密信息与上述第二解密信息一致时，确定上述信息添加指令为有效指令。
- [0062] 在一些可行的实施方式中，上述确定单元33用于。
- [0063] 确定上述待处理信息中是否包括上述第二共识协议中的拦截标识信息。
- [0064] 当上述待处理信息中包括上述拦截标识信息时，确定上述待处理信息属于上述待拦截信息类型。
- [0065] 在一些可行的实施方式中，上述确定单元33用于。
- [0066] 从预设信息库中确定出与上述拦截标识信息语义一致，且属于上述待拦截信息类型的至少一个目标信息。
- [0067] 确定上述待处理信息中是否包括上述至少一个目标信息中的任一目标信息，当上述待处理信息中包括上述任一目标信息时，确定上述待处理信息属于上述待拦截信息类型。
- [0068] 在一些可行的实施方式中，上述接收单元31还用于。
- [0069] 接收信息管理方发送的信息删除指令。
- [0070] 上述响应单元32，还用于当上述信息删除指令为有效指令时，响应上述信息删除指令并删除上述第二共识协议中的拦截标识信息，以在接收到上述信息发送方发送的任一信息时，基于已删除上述拦截标识信息之后的共识协议对上述任一信息进行处理。
- [0071] 在一些可行的实施方式中，上述信息处理装置包括。
- [0072] 删除单元36，用于删除上述待处理信息以拒绝将上述待处理信息发送至信息接收方。
- [0073] 或者，删除上述待处理信息并向上述待处理信息发送方发送拒绝指令，以使上述信息发送方修改上述待处理信息的信息内容并发送修改信息内容后的信息。
- [0074] 具体实现中，上述基于共识协议的信息处理装置可通过其内置的各个模块和/单元执行如上图1至图2中各个步骤所提供的实现方式。例如，上述接收单元31可用于接收信息管理方发送的信息添加指令等实现方式，具体可参见上述各个步骤所提供的实现方式，在此不再赘述。上述响应单元32可用于当上述接收单元31接收到的上述信息添加指令为有效指令时，响应上述信息添加指令并将上

述拦截标识信息添加至上述第一共识协议中以得到第二共识协议等实现方式，具体可参见上述各个步骤所提供的实现方式，在此不再赘述。上述确定单元33可用于当接收到信息发送方发送的待处理信息时，基于上述响应单元32得到的上述第二共识协议确定上述待处理信息是否属于上述待拦截信息类型等实现方式，具体可参见上述各个步骤所提供的实现方式，在此不再赘述。上述拦截单元34可用于当上述待处理信息属于上述待拦截信息类型时，基于上述第二共识协议拦截上述待处理信息将等实现方式，具体可参见上述各个步骤所提供的实现方式，在此不再赘述。上述解密单元35可用于当上述信息添加指令中包括指令处理对象的身份标识时，将上述数字签名进行解密得到第一解密信息等实现方式，具体可参见上述各个步骤所提供的实现方式，在此不再赘述。上述删除单元36可用于删除上述待处理信息以拒绝将上述待处理信息发送至信息接收方等实现方式，具体可参见上述各个步骤所提供的实现方式，在此不再赘述。

[0075] 在本申请实施例中，在将信息添加指令中携带的拦截标识信息添加至共识协议后可得到具备确定接收到的信息是否属于待拦截信息类型的共识协议。当接收到信息发送方发送的待处理信息时，可基于新的共识协议拦截属于待拦截信息类型的待处理信息，进而提升信息处理水平。同时，通过信息删除指令可删除共识协议中的拦截标识信息，从而灵活调整待拦截信息类型，灵活性强，适用性更高。

[0076] 参见图4，图4是本申请实施例提供的终端设备的结构示意图。如图4所示，本实施例中的终端设备可以包括。一个或多个处理器41和存储器42。上述处理器41和存储器42通过总线43连接。存储器42用于存储计算机程序，该计算机程序包括程序指令，处理器41用于执行存储器42存储的程序指令，执行如下操作。

[0077] 接收信息管理方发送的信息添加指令，上述信息添加指令中携带拦截标识信息，上述信息添加指令用于指示向第一共识协议中添加上述拦截标识信息，上述拦截标识信息用于确定接收到的信息是否属于待拦截信息类型。

[0078] 当上述信息添加指令为有效指令时，响应上述信息添加指令并将上述拦截标识信息添加至上述第一共识协议中以得到第二共识协议。

[0079] 当接收到信息发送方发送的待处理信息时，基于上述第二共识协议确定上述待

处理信息是否属于上述待拦截信息类型。

[0080] 当上述待处理信息属于上述待拦截信息类型时，基于上述第二共识协议拦截上述待处理信息。

[0081] 在一些可行的实施方式中，上述信息添加指令中包括密文信息和数字签名，上述处理器41还用于。

[0082] 若上述信息添加指令中包括指令处理对象的身份标识，则将上述数字签名进行解密得到第一解密信息，将上述密文信息进行解密得到第二解密信息。

[0083] 若上述第一解密信息与上述第二解密信息一致，则确定上述信息添加指令为有效指令。

[0084] 在一些可行的实施方式中，上述处理器41用于。

[0085] 确定上述待处理信息中是否包括上述第二共识协议中的拦截标识信息。

[0086] 若上述待处理信息中包括上述拦截标识信息，则确定上述待处理信息属于上述待拦截信息类型。

[0087] 在一些可行的实施方式中，上述处理器41用于。

[0088] 从预设信息库中确定出与上述拦截标识信息语义一致，且属于上述待拦截信息类型的至少一个目标信息。

[0089] 确定上述待处理信息中是否包括上述至少一个目标信息中的任一目标信息，若上述待处理信息中包括上述任一目标信息，则确定上述待处理信息属于上述待拦截信息类型。

[0090] 在一些可行的实施方式中，上述处理器41还用于。

[0091] 接收信息管理方发送的信息删除指令。

[0092] 当上述信息删除指令为有效指令时，响应上述信息删除指令并删除上述第二共识协议中的拦截标识信息，以在接收到上述信息发送方发送的任一信息时，基于已删除上述拦截标识信息之后的共识协议对上述任一信息进行处理。

[0093] 在一些可行的实施方式中，上述处理器41还用于。

[0094] 删除上述待处理信息以拒绝将上述待处理信息发送至信息接收方。

[0095] 或者，删除上述待处理信息并向上述待处理信息发送方发送拒绝指令，以使上述信息发送方修改上述待处理信息的信息内容并发送修改信息内容后的信息。

- [0096] 应当理解，在一些可行的实施方式中，上述处理器41可以是中央处理单元 (central processing unit, CPU)，该处理器41还可以是其他通用处理器、数字信号处理器 (digital signal processor, DSP)、专用集成电路 (application specific integrated circuit, ASIC)、现成可编程门阵列 (field-programmable gate array, FPGA) 或者其他可编程逻辑器件、分立门或者晶体管逻辑器件、分立硬件组件等。通用处理器可以是微处理器或者该处理器也可以是任何常规的处理器等。
- [0097] 该存储器42可以包括只读存储器和随机存取存储器，并向处理器41提供指令和数据。存储器42的一部分还可以包括非易失性随机存取存储器。例如，存储器42还可以存储设备类型的信息。
- [0098] 具体实现中，上述终端设备可通过其内置的各个功能模块执行如上述图1至图2中各个步骤所提供的实现方式，具体可参见上述各个步骤所提供的实现方式，在此不再赘述。
- [0099] 在本申请实施例中，在将信息添加指令中携带的拦截标识信息添加至共识协议后可得到具备确定接收到的信息是否属于待拦截信息类型的共识协议。当接收到信息发送方发送的待处理信息时，可基于新的共识协议拦截属于待拦截信息类型的待处理信息，进而提升信息处理水平。同时，通过信息删除指令可删除共识协议中的拦截标识信息，从而灵活调整待拦截信息类型，灵活性强，适用性更高。
- [0100] 本申请实施例还提供一种计算机可读存储介质，该计算机可读存储介质存储有计算机程序，被处理器41执行以实现图1至图2中各个步骤所提供的方法，具体可参见上述各个步骤所提供的实现方式，在此不再赘述。其中，所述计算机可读存储介质可以是非易失性，也可以是易失性的。
- [0101] 上述计算机可读存储介质可以是前述任一实施例提供的任务处理装置或者上述终端设备的内部存储单元，例如电子设备的硬盘或内存。该计算机可读存储介质也可以是该电子设备的外部存储设备，例如该电子设备上配备的插接式硬盘，智能存储卡 (smart media card, SMC)，安全数字 (secure digital, SD) 卡，闪存卡 (flash card) 等。上述计算机可读存储介质还可以包括磁碟、光

盘、随机存储记忆体 (random access memory, RAM) 或只读存储记忆体 (read-only memory, ROM) 等。进一步地, 该计算机可读存储介质还可以既包括该电子设备的内部存储单元也包括外部存储设备。该计算机可读存储介质用于存储该计算机程序以及该电子设备所需的其他程序和数据。该计算机可读存储介质还可以用于暂时地存储已经输出或者将要输出的数据。

[0102] 以上所述, 仅为本申请的具体实施方式, 但本申请的保护范围并不局限于此, 任何熟悉本技术领域的技术人员在本申请揭露的技术范围内, 可轻易想到变化或替换, 都应涵盖在本申请的保护范围之内。因此, 本申请的保护范围应以所述权利要求的保护范围为准。

权利要求书

- [权利要求 1] 一种基于共识协议的信息处理方法，其中，所述方法包括：
接收信息管理方发送的信息添加指令，所述信息添加指令中携带拦截标识信息，所述信息添加指令用于指示向第一共识协议中添加所述拦截标识信息，所述拦截标识信息用于确定接收到的信息是否属于待拦截信息类型；
当所述信息添加指令为有效指令时，响应所述信息添加指令并将所述拦截标识信息添加至所述第一共识协议中以得到第二共识协议；
当接收到信息发送方发送的待处理信息时，基于所述第二共识协议确定所述待处理信息是否属于所述待拦截信息类型；
当所述待处理信息属于所述待拦截信息类型时，基于所述第二共识协议拦截所述待处理信息。
- [权利要求 2] 根据权利要求1所述的方法，其中，所述信息添加指令中包括密文信息和数字签名，所述接收信息管理方发送的信息添加指令之后，所述方法还包括：
若所述信息添加指令中包括指令处理对象的身份标识，则将所述数字签名进行解密得到第一解密信息，将所述密文信息进行解密得到第二解密信息；
若所述第一解密信息与所述第二解密信息一致，则确定所述信息添加指令为有效指令。
- [权利要求 3] 根据权利要求1或2所述的方法，其中，所述基于所述第二共识协议确定所述待处理信息是否属于所述待拦截信息类型包括：
确定所述待处理信息中是否包括所述第二共识协议中的拦截标识信息；
若所述待处理信息中包括所述拦截标识信息，则确定所述待处理信息属于所述待拦截信息类型。
- [权利要求 4] 根据权利要求1或2所述的方法，其中，所述基于所述第二共识协议确定所述待处理信息是否属于待拦截信息类型包括：

从预设信息库中确定出与所述拦截标识信息语义一致，且属于所述待拦截信息类型的至少一个目标信息；

确定所述待处理信息中是否包括所述至少一个目标信息中的任一目标信息，若所述待处理信息中包括所述任一目标信息，则确定所述待处理信息属于所述待拦截信息类型。

[权利要求 5] 根据权利要求1至4任一项所述的方法，其中，所述方法还包括：

接收信息管理方发送的信息删除指令；

当所述信息删除指令为有效指令时，响应所述信息删除指令并删除所述第二共识协议中的拦截标识信息，以在接收到所述信息发送方发送的任一信息时，基于已删除所述拦截标识信息之后的共识协议对所述任一信息进行处理。

[权利要求 6] 根据权利要求1至5任一项所述的方法，其中，所述基于所述第二共识协议拦截所述待处理信息包括：

删除所述待处理信息以拒绝将所述待处理信息发送至信息接收方；

或者，删除所述待处理信息并向所述待处理信息发送方发送拒绝指令，以使所述信息发送方修改所述待处理信息的信息内容并发送修改信息内容后的信息。

[权利要求 7] 一种基于共识协议的信息处理装置，其中，所述信息处理装置包括：

接收单元，用于接收信息管理方发送的信息添加指令，所述信息添加指令中携带拦截标识信息，所述信息添加指令用于指示向第一共识协议中添加所述拦截标识信息，所述拦截标识信息用于确定接收到的信息是否属于待拦截信息类型；

响应单元，用于当所述接收单元接收到的所述信息添加指令为有效指令时，响应所述信息添加指令并将所述拦截标识信息添加至所述第一共识协议中以得到第二共识协议；

确定单元，用于当接收到信息发送方发送的待处理信息时，基于所述响应单元得到的所述第二共识协议确定所述待处理信息是否属于所述待拦截信息类型；

拦截单元，用于当所述待处理信息属于所述待拦截信息类型时，基于所述第二共识协议拦截所述待处理信息。

[权利要求 8] 根据权利要求7所述的信息处理装置，其中，所述信息处理装置包括：

解密单元，用于当所述信息添加指令中包括指令处理对象的身份标识时，将所述数字签名进行解密得到第一解密信息，将所述密文信息进行解密得到第二解密信息；

所述确定单元，用于当所述第一解密信息与所述第二解密信息一致时，确定所述信息添加指令为有效指令。

[权利要求 9] 一种终端设备，其中，包括存储器和处理器，所述处理器、和所述存储器相互连接，其中，所述存储器用于存储计算机程序，所述计算机程序包括程序指令，所述处理器用于执行所述存储器的所述程序指令，其中：

接收信息管理方发送的信息添加指令，所述信息添加指令中携带拦截标识信息，所述信息添加指令用于指示向第一共识协议中添加所述拦截标识信息，所述拦截标识信息用于确定接收到的信息是否属于待拦截信息类型；

当所述信息添加指令为有效指令时，响应所述信息添加指令并将所述拦截标识信息添加至所述第一共识协议中以得到第二共识协议；

当接收到信息发送方发送的待处理信息时，基于所述第二共识协议确定所述待处理信息是否属于所述待拦截信息类型；

当所述待处理信息属于所述待拦截信息类型时，基于所述第二共识协议拦截所述待处理信息。

[权利要求 10] 根据权利要求9所述的终端设备，其中，所述信息添加指令中包括密文信息和数字签名，所述接收信息管理方发送的信息添加指令之后，所述终端设备还包括：

若所述信息添加指令中包括指令处理对象的身份标识，则将所述数字签名进行解密得到第一解密信息，将所述密文信息进行解密得到第二

解密信息；

若所述第一解密信息与所述第二解密信息一致，则确定所述信息添加指令为有效指令。

[权利要求 11] 根据权利要求9或10所述的终端设备，其中，所述基于所述第二共识协议确定所述待处理信息是否属于所述待拦截信息类型包括：
确定所述待处理信息中是否包括所述第二共识协议中的拦截标识信息；
；
若所述待处理信息中包括所述拦截标识信息，则确定所述待处理信息属于所述待拦截信息类型。

[权利要求 12] 根据权利要求9或10所述的终端设备，其中，所述基于所述第二共识协议确定所述待处理信息是否属于待拦截信息类型包括：
从预设信息库中确定出与所述拦截标识信息语义一致，且属于所述待拦截信息类型的至少一个目标信息；
确定所述待处理信息中是否包括所述至少一个目标信息中的任一目标信息，若所述待处理信息中包括所述任一目标信息，则确定所述待处理信息属于所述待拦截信息类型。

[权利要求 13] 根据权利要求9至12任一项所述的终端设备，其中，所述终端设备还包括：
接收信息管理方发送的信息删除指令；
当所述信息删除指令为有效指令时，响应所述信息删除指令并删除所述第二共识协议中的拦截标识信息，以在接收到所述信息发送方发送的任一信息时，基于已删除所述拦截标识信息之后的共识协议对所述任一信息进行处理。

[权利要求 14] 根据权利要求9至13任一项所述的终端设备，其中，所述基于所述第二共识协议拦截所述待处理信息包括：
删除所述待处理信息以拒绝将所述待处理信息发送至信息接收方；
或者，删除所述待处理信息并向所述待处理信息发送方发送拒绝指令，以使所述信息发送方修改所述待处理信息的信息内容并发送修改信

息内容后的信息。

- [权利要求 15] 一种计算机可读存储介质，其中，所述计算机可读存储介质存储有计算机程序，所述计算机程序包括程序指令，所述程序指令被处理器执行时，用于实现以下步骤：
- 接收信息管理方发送的信息添加指令，所述信息添加指令中携带拦截标识信息，所述信息添加指令用于指示向第一共识协议中添加所述拦截标识信息，所述拦截标识信息用于确定接收到的信息是否属于待拦截信息类型；
- 当所述信息添加指令为有效指令时，响应所述信息添加指令并将所述拦截标识信息添加至所述第一共识协议中以得到第二共识协议；
- 当接收到信息发送方发送的待处理信息时，基于所述第二共识协议确定所述待处理信息是否属于所述待拦截信息类型；
- 当所述待处理信息属于所述待拦截信息类型时，基于所述第二共识协议拦截所述待处理信息。

- [权利要求 16] 根据权利要求15所述的计算机可读存储介质，其中，所述信息添加指令中包括密文信息和数字签名，所述程序指令被处理器执行时，还用于实现以下步骤：
- 若所述信息添加指令中包括指令处理对象的身份标识，则将所述数字签名进行解密得到第一解密信息，将所述密文信息进行解密得到第二解密信息；
- 若所述第一解密信息与所述第二解密信息一致，则确定所述信息添加指令为有效指令。

- [权利要求 17] 根据权利要求15或16所述的计算机可读存储介质，其中，所述程序指令被处理器执行时，还用于实现以下步骤：
- 确定所述待处理信息中是否包括所述第二共识协议中的拦截标识信息；
- 若所述待处理信息中包括所述拦截标识信息，则确定所述待处理信息属于所述待拦截信息类型。

- [权利要求 18] 根据权利要求15或16所述的计算机可读存储介质，其中，所述程序指令被处理器执行时，还用于实现以下步骤：
从预设信息库中确定出与所述拦截标识信息语义一致，且属于所述待拦截信息类型的至少一个目标信息；
确定所述待处理信息中是否包括所述至少一个目标信息中的任一目标信息，若所述待处理信息中包括所述任一目标信息，则确定所述待处理信息属于所述待拦截信息类型。
- [权利要求 19] 根据权利要求15至18任一项所述的计算机可读存储介质，其中，所述程序指令被处理器执行时，还用于实现以下步骤：
接收信息管理方发送的信息删除指令；
当所述信息删除指令为有效指令时，响应所述信息删除指令并删除所述第二共识协议中的拦截标识信息，以在接收到所述信息发送方发送的任一信息时，基于已删除所述拦截标识信息之后的共识协议对所述任一信息进行处理。
- [权利要求 20] 根据权利要求15至19任一项所述的计算机可读存储介质，其中，所述程序指令被处理器执行时，还用于实现以下步骤：
删除所述待处理信息以拒绝将所述待处理信息发送至信息接收方；
或者，删除所述待处理信息并向所述待处理信息发送方发送拒绝指令，以使所述信息发送方修改所述待处理信息的信息内容并发送修改信息内容后的信息。

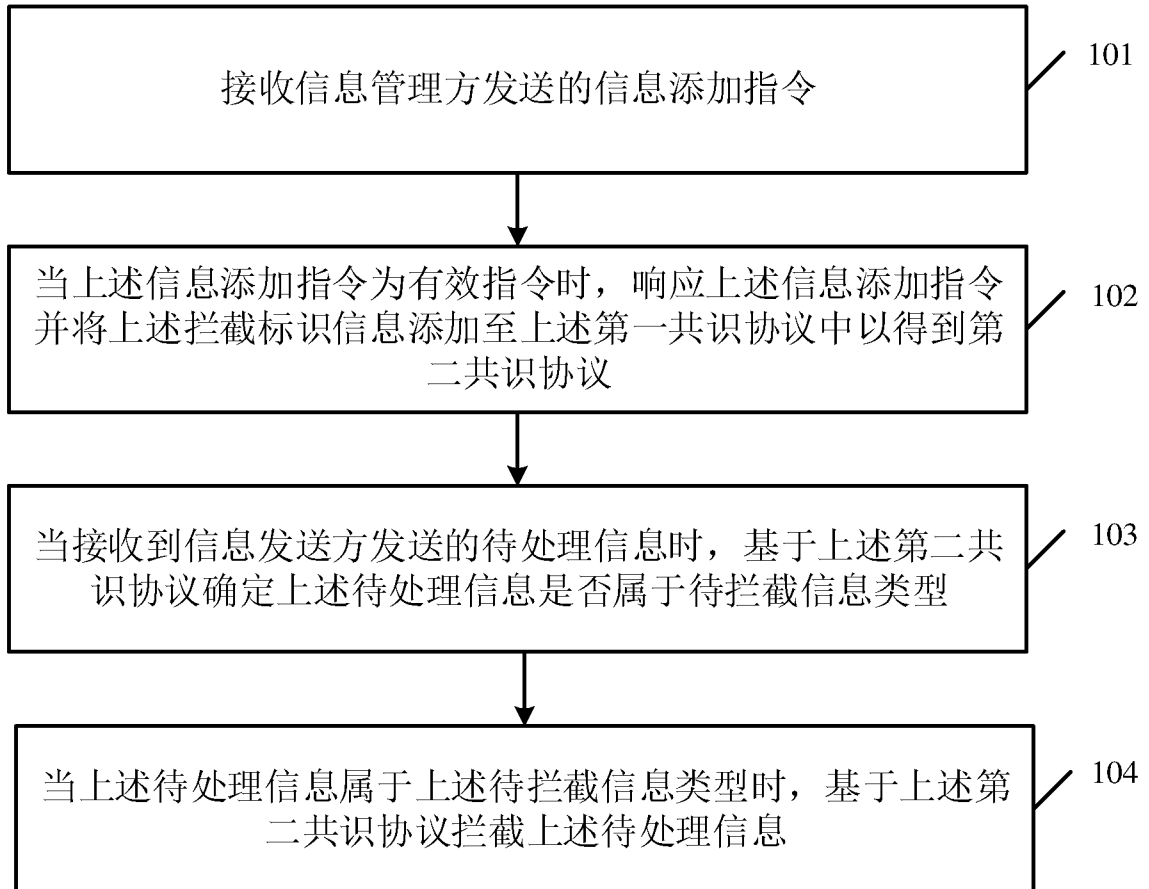


图 1

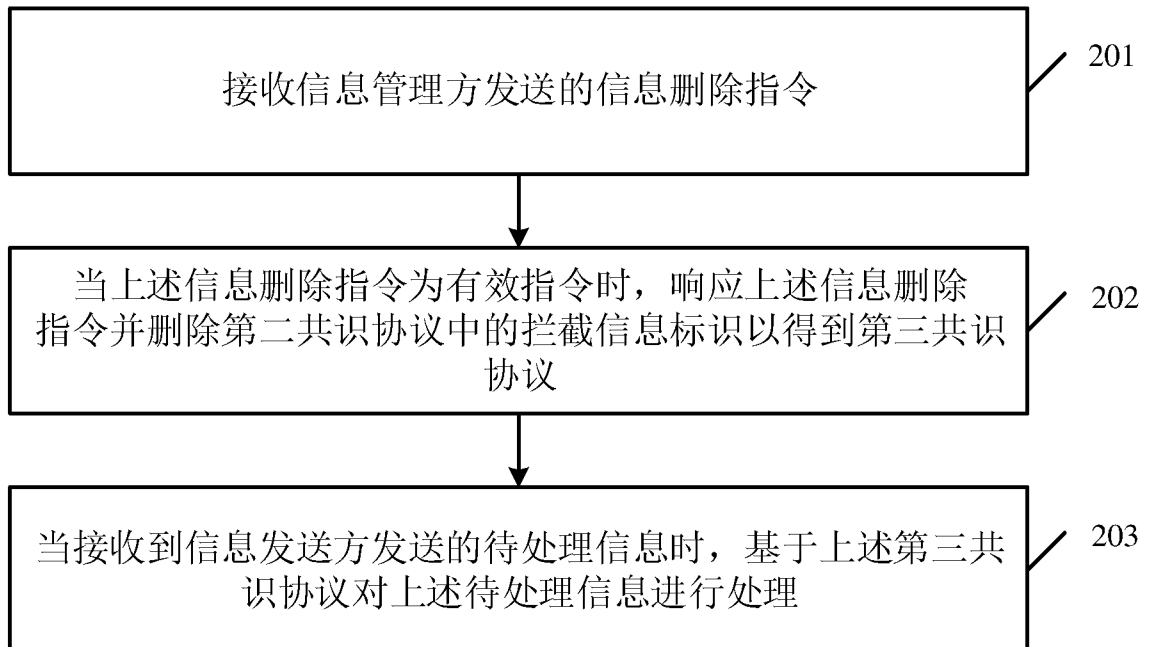


图 2

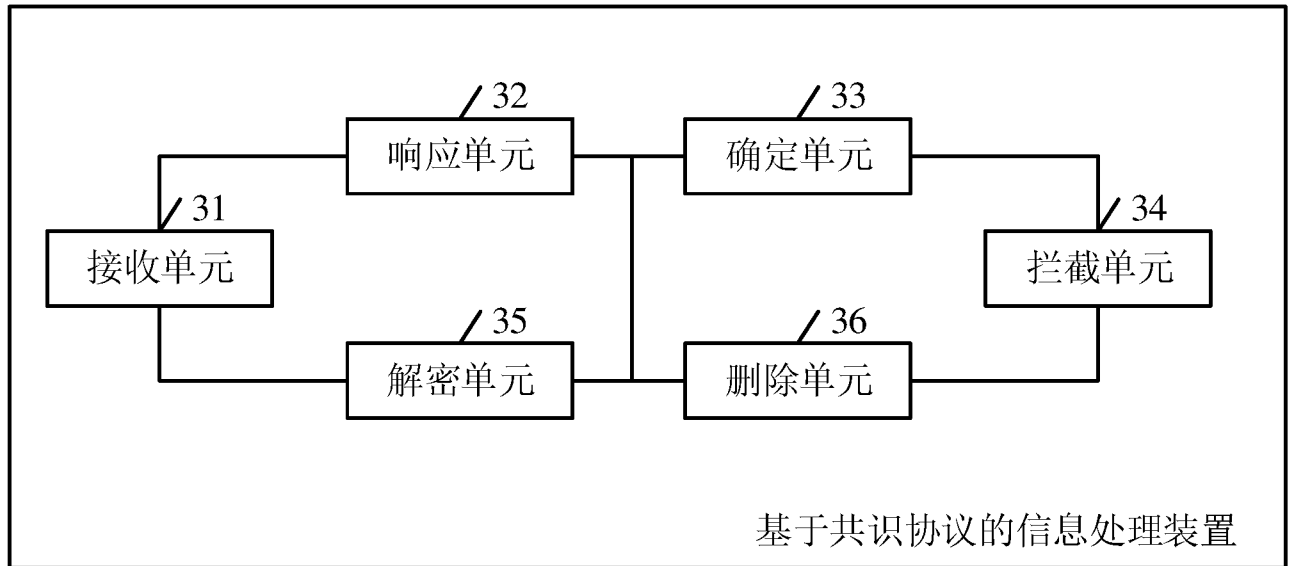


图 3

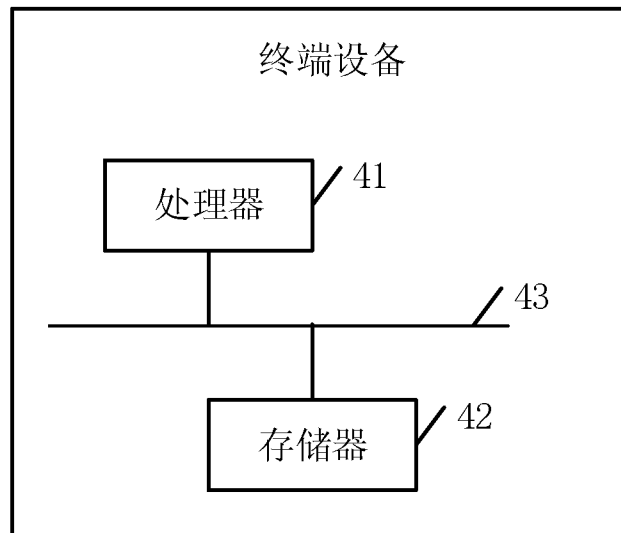


图 4

INTERNATIONAL SEARCH REPORT

International application No.

PCT/CN2020/103255

A. CLASSIFICATION OF SUBJECT MATTER		
H04L 29/06(2006.01)i		
According to International Patent Classification (IPC) or to both national classification and IPC		
B. FIELDS SEARCHED		
Minimum documentation searched (classification system followed by classification symbols)		
H04L,H04W,H04Q		
Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched		
Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)		
CNPAT, WPI, EPODOC, GOOGLE, CNKI: 共识, 区块链, 添加, 更新, 更改, 修改, 拦截, 过滤, 筛选, 删除, 密码, 标识, 账户, 账号, 关键词, 关键字, 工作量证明, 权益证明, 股份授权证明, 实用拜占庭, consensus, block chain, add, update, modify, filter, intercept, delete, code, ID, account, key, POW, POS, DPOS, PBFT		
C. DOCUMENTS CONSIDERED TO BE RELEVANT		
Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
PX	CN 110602051 A (SHENZHEN ONECONNECT TECHNOLOGY CO., LTD.) 20 December 2019 (2019-12-20) claims 1-10	1-20
X	CN 110119428 A (TENCENT TECHNOLOGY SHENZHEN CO., LTD.) 13 August 2019 (2019-08-13) description paragraphs 46-92, figures 1-6	1-20
A	WO 2017204943 A1 (MASTERCARD INTERNATIONAL INCORPORATED) 30 November 2017 (2017-11-30) entire document	1-20
A	WO 2019072312 A2 (ALIBABA GROUP HOLDING LIMITED) 18 April 2019 (2019-04-18) entire document	1-20
A	CN 110070445 A (SHENZHEN QIANHAI WEBANK CO., LTD.) 30 July 2019 (2019-07-30) entire document	1-20
<input checked="" type="checkbox"/> Further documents are listed in the continuation of Box C. <input checked="" type="checkbox"/> See patent family annex.		
* Special categories of cited documents: "A" document defining the general state of the art which is not considered to be of particular relevance "E" earlier application or patent but published on or after the international filing date "L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified) "O" document referring to an oral disclosure, use, exhibition or other means "P" document published prior to the international filing date but later than the priority date claimed "T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention "X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone "Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art "&" document member of the same patent family		
Date of the actual completion of the international search		Date of mailing of the international search report
11 September 2020		28 September 2020
Name and mailing address of the ISA/CN		Authorized officer
China National Intellectual Property Administration (ISA/ CN) No. 6, Xitucheng Road, Jimenqiao Haidian District, Beijing 100088 China		
Facsimile No. (86-10)62019451		Telephone No.

INTERNATIONAL SEARCH REPORT

International application No.

PCT/CN2020/103255

C. DOCUMENTS CONSIDERED TO BE RELEVANT		
Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	周启惠 等 (ZHOU, Qihui et al.). "基于区块链的防护物联网设备DDoS攻击方法 (DDoS Defense Method of IoT Devices Based on Blockchain)" <i>应用科学学报 (Journal of Applied Sciences)</i> , 31 March 2019 (2019-03-31), entire document	1-20
.....		

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.

PCT/CN2020/103255

Patent document cited in search report			Publication date (day/month/year)	Patent family member(s)	Publication date (day/month/year)
CN	110602051	A	20 December 2019	None	
CN	110119428	A	13 August 2019	None	
WO	2017204943	A1	30 November 2017	US 2017344987 A1	30 November 2017
				CN 109313752 A	05 February 2019
				EP 3446272 A1	27 February 2019
				US 2019139043 A1	09 May 2019
				IN 201817007048 A	29 June 2018
				SG 11201808086 A1	30 October 2018
WO	2019072312	A2	18 April 2019	KR 20200083930 A	09 July 2020
				JP 2020505799 A	20 February 2020
				CN 110383279 A	25 October 2019
				EP 3574461 A2	04 December 2019
				PH 12019501157 A1	02 March 2020
				US 2020128043 A1	23 April 2020
				SG 11201904383 A1	27 June 2019
				IN 201947019308 A	03 July 2020
CN	110070445	A	30 July 2019	None	

<p>A. 主题的分类</p> <p>H04L 29/06 (2006.01) i</p> <p>按照国际专利分类(IPC)或者同时按照国家分类和IPC两种分类</p>																							
<p>B. 检索领域</p> <p>检索的最低限度文献(标明分类系统和分类号)</p> <p>H04L, H04W, H04Q</p> <p>包含在检索领域中的除最低限度文献以外的检索文献</p> <p>在国际检索时查阅的电子数据库(数据库的名称, 和使用的检索词(如使用))</p> <p>CNPAT, WPI, EPDOC, GOOGLE, CNKI:共识, 区块链, 添加, 更新, 更改, 修改, 拦截, 过滤, 筛选, 删除, 密码, 标识, 账户, 账号, 关键词, 关键字, 工作量证明, 权益证明, 股份授权证明, 实用拜占庭, consensus, block chain, add, update, modify, filter, intercept, delete, code, ID, account, key, POW, POS, DPOS, PBFT</p>																							
<p>C. 相关文件</p> <table border="1"> <thead> <tr> <th>类型*</th> <th>引用文件, 必要时, 指明相关段落</th> <th>相关的权利要求</th> </tr> </thead> <tbody> <tr> <td>PX</td> <td>CN 110602051 A (深圳壹账通智能科技有限公司) 2019年 12月 20日 (2019 - 12 - 20) 权利要求1-10</td> <td>1-20</td> </tr> <tr> <td>X</td> <td>CN 110119428 A (腾讯科技深圳有限公司) 2019年 8月 13日 (2019 - 08 - 13) 说明书第46-92段, 图1-6</td> <td>1-20</td> </tr> <tr> <td>A</td> <td>WO 2017204943 A1 (MASTERCARD INTERNATIONAL INCORPORATED) 2017年 11月 30日 (2017 - 11 - 30) 全文</td> <td>1-20</td> </tr> <tr> <td>A</td> <td>WO 2019072312 A2 (ALIBABA GROUP HOLDING LIMITED) 2019年 4月 18日 (2019 - 04 - 18) 全文</td> <td>1-20</td> </tr> <tr> <td>A</td> <td>CN 110070445 A (深圳前海微众银行股份有限公司) 2019年 7月 30日 (2019 - 07 - 30) 全文</td> <td>1-20</td> </tr> <tr> <td>A</td> <td>周启惠等. "基于区块链的防护物联网设备DDoS攻击方法" 应用科学学报, 2019年 3月 31日 (2019 - 03 - 31), 全文</td> <td>1-20</td> </tr> </tbody> </table>			类型*	引用文件, 必要时, 指明相关段落	相关的权利要求	PX	CN 110602051 A (深圳壹账通智能科技有限公司) 2019年 12月 20日 (2019 - 12 - 20) 权利要求1-10	1-20	X	CN 110119428 A (腾讯科技深圳有限公司) 2019年 8月 13日 (2019 - 08 - 13) 说明书第46-92段, 图1-6	1-20	A	WO 2017204943 A1 (MASTERCARD INTERNATIONAL INCORPORATED) 2017年 11月 30日 (2017 - 11 - 30) 全文	1-20	A	WO 2019072312 A2 (ALIBABA GROUP HOLDING LIMITED) 2019年 4月 18日 (2019 - 04 - 18) 全文	1-20	A	CN 110070445 A (深圳前海微众银行股份有限公司) 2019年 7月 30日 (2019 - 07 - 30) 全文	1-20	A	周启惠等. "基于区块链的防护物联网设备DDoS攻击方法" 应用科学学报, 2019年 3月 31日 (2019 - 03 - 31), 全文	1-20
类型*	引用文件, 必要时, 指明相关段落	相关的权利要求																					
PX	CN 110602051 A (深圳壹账通智能科技有限公司) 2019年 12月 20日 (2019 - 12 - 20) 权利要求1-10	1-20																					
X	CN 110119428 A (腾讯科技深圳有限公司) 2019年 8月 13日 (2019 - 08 - 13) 说明书第46-92段, 图1-6	1-20																					
A	WO 2017204943 A1 (MASTERCARD INTERNATIONAL INCORPORATED) 2017年 11月 30日 (2017 - 11 - 30) 全文	1-20																					
A	WO 2019072312 A2 (ALIBABA GROUP HOLDING LIMITED) 2019年 4月 18日 (2019 - 04 - 18) 全文	1-20																					
A	CN 110070445 A (深圳前海微众银行股份有限公司) 2019年 7月 30日 (2019 - 07 - 30) 全文	1-20																					
A	周启惠等. "基于区块链的防护物联网设备DDoS攻击方法" 应用科学学报, 2019年 3月 31日 (2019 - 03 - 31), 全文	1-20																					
<p><input type="checkbox"/> 其余文件在C栏的续页中列出。</p> <p><input checked="" type="checkbox"/> 见同族专利附件。</p>																							
<p>* 引用文件的具体类型:</p> <p>"A" 认为不特别相关的表示了现有技术一般状态的文件</p> <p>"E" 在国际申请日的当天或之后公布的在先申请或专利</p> <p>"L" 可能对优先权要求构成怀疑的文件, 或为确定另一篇引用文件的公布日而引用的或者因其他特殊理由而引用的文件(如具体说明的)</p> <p>"O" 涉及口头公开、使用、展览或其他方式公开的文件</p> <p>"P" 公布日先于国际申请日但迟于所要求的优先权日的文件</p> <p>"T" 在申请日或优先权日之后公布, 与申请不相抵触, 但为了理解发明之理论或原理的在后文件</p> <p>"X" 特别相关的文件, 单独考虑该文件, 认定要求保护的发明不是新颖的或不具有创造性</p> <p>"Y" 特别相关的文件, 当该文件与另一篇或者多篇该类文件结合并且这种结合对于本领域技术人员为显而易见时, 要求保护的发明不具有创造性</p> <p>"&" 同族专利的文件</p>																							
<p>国际检索实际完成的日期</p> <p>2020年 9月 11日</p>		<p>国际检索报告邮寄日期</p> <p>2020年 9月 28日</p>																					
<p>ISA/CN的名称和邮寄地址</p> <p>中国国家知识产权局(ISA/CN) 中国北京市海淀区蓟门桥西土城路6号 100088</p> <p>传真号 (86-10)62019451</p>		<p>授权官员</p> <p>赵新蕾</p> <p>电话号码 86-(10)-53961623</p>																					

国际检索报告
关于同族专利的信息

国际申请号

PCT/CN2020/103255

检索报告引用的专利文件			公布日 (年/月/日)	同族专利			公布日 (年/月/日)
CN	110602051	A	2019年 12月 20日	无			
CN	110119428	A	2019年 8月 13日	无			
WO	2017204943	A1	2017年 11月 30日	US	2017344987	A1	2017年 11月 30日
				CN	109313752	A	2019年 2月 5日
				EP	3446272	A1	2019年 2月 27日
				US	2019139043	A1	2019年 5月 9日
				IN	201817007048	A	2018年 6月 29日
				SG	11201808086	A1	2018年 10月 30日
WO	2019072312	A2	2019年 4月 18日	KR	20200083930	A	2020年 7月 9日
				JP	2020505799	A	2020年 2月 20日
				CN	110383279	A	2019年 10月 25日
				EP	3574461	A2	2019年 12月 4日
				PH	12019501157	A1	2020年 3月 2日
				US	2020128043	A1	2020年 4月 23日
				SG	11201904383	A1	2019年 6月 27日
				IN	201947019308	A	2020年 7月 3日
CN	110070445	A	2019年 7月 30日	无			