

基于区块链的信息处理方法、装置和计算机可读存储介质

本申请要求于2019年04月19日提交的申请号为201910319332.9、发明名称为“基于区块链的信息处理方法、装置和计算机可读存储介质”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

本申请涉及计算机技术领域，尤其涉及基于区块链的信息处理方法、装置和计算机可读存储介质。

背景技术

随着计算机技术的发展，区块链数据处理技术不断发展。区块链技术（blockchain technology, BT），也被称之为分布式账本技术，是一种互联网数据库技术，其特点是去中心化且公开透明，让每个人均可参与数据库记录。区块链目前主要包括公有链、私有链、联盟链、许可链以及混合链。

基于区块链技术进行交易需要考虑交易信息的安全性。目前采用的方案是基于明文敏感词库实现的，具体地，服务提供方维护一个明文敏感词库，当用户需要进行内容检测和过滤时，将原始内容发送到服务器端，由服务器端使用明文敏感词库对用户提供的原始内容进行比对和过滤，然后将结果返回给客户端，客户端拿到过滤后的内容和检测结果即可以进行后续处理。

然而，目前采用的敏感词库是以明文的形式维护在中心化的机构中的，当需要更新敏感词库的时候，通常是使用一个明文的敏感词库文件来同步最新的敏感词，因此，敏感词库的载体文件如果在同步的过程中发生泄漏，则会导致交易信息出现安全隐患，引起一系列的社会危害。

发明内容

本申请实施例提供了一种基于区块链的信息处理方法、装置和计算机可读存储介质，在对于索引信息的记录不再以明文形式进行维护，而是对区块链交易过程中涉及到索引信息的索引进行记录，由此形成变体索引信息，变体索引信息不会直接显示索引信息的具体内容，而是以索引形式进行维护，从而不易出现安全隐患，提升信息维护的安全性。

本申请一方面提供一种基于区块链的信息处理方法，由网络节点设备执行，包括：

获取原始索引信息集合，其中，所述原始索引信息集合中包括至少一个原始索引信息，每个原始索引信息包括明文形式的敏感内容；

获取待匹配区块中的信息，其中，所述信息包括信息内容以及信息索引，所述信息内容与所述信息索引具有对应关系；

通过所述原始索引信息集合对所述信息中的所述信息内容进行匹配，得到匹配结果；

当所述匹配结果指示匹配成功时，根据所述匹配结果生成变体索引信息集合，其中，所述变体索引信息集合包括至少一个变体索引信息，所述变体索引信息包括所述信息中的与所述信息内容对应的所述索引信息。

本申请一方面提供一种基于区块链的信息处理方法，由网络节点设备执行，包括：

接收请求信息，其中，所述请求信息中携带待检测信息索引；

通过变体索引信息集合对所述请求信息中携带的所述待检测信息索引进行检测，得到检测结果，其中，所述变体索引信息集合包括至少一个变体索引信息，所述变体索引信息包括信息中的信息索引；

获取所述待检测信息索引所对应的信息内容；

根据所述检测结果对所述待检测信息索引所对应的信息内容进行处理,得到已处理信息;发送所述已处理信息,以展示所述已处理信息。

本申请一方面提供一种基于区块链的数据处理装置,包括:

获取模块,用于获取原始索引信息集合,其中,所述原始索引信息集合中包括至少一个原始索引信息,每个原始索引信息包括明文形式的敏感内容;

所述获取模块,还用于获取待匹配区块中的信息,其中,所述信息包括信息内容以及信息索引,所述信息内容与所述信息索引具有对应关系;

匹配模块,用于通过所述获取模块获取的所述原始索引信息集合对所述信息中的所述信息内容进行匹配,得到匹配结果;

生成模块,用于当所述匹配模块得到的所述匹配结果指示匹配成功时,根据所述匹配结果生成变体索引信息集合,其中,所述变体索引信息集合包括至少一个变体索引信息,所述变体索引信息包括所述信息中的与所述信息内容对应的所述信息索引。

在一种可能的设计中,所述匹配模块,用于通过所述原始索引信息集合对第一信息内容进行匹配,其中,所述第一信息内容属于所述信息;

若所述第一信息内容属于第一区块中的最后一个信息,则对第二区块中的信息内容进行匹配,其中,所述第一区块属于所述待匹配区块的一个区块,所述第二区块属于所述待匹配区块的另一个区块,且所述第二区块为所述第一区块相邻的下一个区块;

若所述第一信息内容不为第一区块中的最后一个信息,则获取所述第一区块中的第二信息内容,通过所述原始索引信息集合对所述第二信息内容进行匹配,其中,所述第二信息内容为所述第一信息内容相邻的下一个信息内容。

在一种可能的设计中,所述生成模块,用于当所述匹配结果为所述信息与所述原始索引信息集合中的原始索引信息匹配成功时,获取所述原始索引信息的敏感级别;

获取所述信息索引中的哈希值、块内索引以及区块高度,其中,所述块内索引表示所述信息在所述待匹配区块的位置;

根据所述原始索引信息的敏感级别、所述哈希值、所述块内索引以及所述区块高度,生成所述变体索引信息集合。

在一种可能的设计中,基于区块链的数据处理装置还包括处理模块;

所述处理模块,用于在所述生成模块根据所述匹配结果生成变体索引信息集合之后,接收请求信息,其中,所述请求信息中携带待检测信息索引;

通过所述变体索引信息集合对所述待检测信息索引进行检测,得到检测结果;

根据所述检测结果对所述请求信息进行处理。

在一种可能的设计中,所述处理模块,用于根据所述待检测信息索引确定目标哈希值;

通过所述变体索引信息集合对所述目标哈希值进行匹配;

若所述目标哈希值与所述变体索引信息集合中的变体索引信息匹配成功,则确定所述待检测信息索引所对应的信息内容属于敏感信息;

若所述目标哈希值与所述变体索引信息集合中的变体索引信息匹配失败,则确定所述待检测信息索引所对应的信息内容属于安全信息。

在一种可能的设计中,所述处理模块,用于根据所述待检测信息索引确定目标块内索引以及目标区块高度;

通过所述变体索引信息集合对所述目标块内索引以及所述目标区块高度进行匹配;

若所述目标块内索引以及所述目标区块高度与所述变体索引信息集合中的变体索引信息匹配成功,则确定所述待检测信息索引属于敏感交易信息;

若所述目标块内索引以及所述目标区块高度与所述变体索引信息集合中的变体索引信息匹配失败,则确定所述待检测信息索引所对应的信息内容属于安全信息。

在一种可能的设计中,所述处理模块,用于若所述待检测信息索引所对应的信息内容属于安全信息,则根据所述待检测信息索引获取目标信息内容;

向所述客户端发送所述目标信息内容,以使所述客户端展示所述目标信息内容。

在一种可能的设计中,所述处理模块,用于若所述待检测信息索引所对应的信息内容属于敏感信息,则根据所述待检测信息索引确定目标敏感级别以及目标业务类型;

根据所述目标敏感级别以及所述目标业务类型,判断是否展示所述待检测信息索引所对应的目标信息内容;

若确定不展示所述目标信息内容,则向所述客户端发送提示信息,以使所述客户端展示所述提示信息,其中,所述提示信息用于提示用户所述目标信息内容属于所述敏感信息;

若确定展示所述目标信息内容,则对所述目标信息内容进行处理,得到处理后的目标信息内容,向所述客户端发送所述处理后的目标信息内容,以使所述客户端展示所述处理后的目标信息内容。

在一种可能的设计中,所述处理模块,用于获取所述目标信息内容;

通过所述原始索引信息集合对所述目标信息内容进行匹配,确定所述目标信息内容中的目标索引信息;

将所述目标信息内容中的所述目标索引信息进行屏蔽,得到所述处理后的目标信息内容。

本申请一方面提供一种基于区块链的数据处理装置,包括:

接收模块,用于接收请求信息,其中,所述请求信息中携带待检测信息索引;

检测模块,用于通过变体索引信息集合对所述请求信息中携带的所述待检测信息索引进行检测,得到检测结果,其中,所述变体索引信息集合包括至少一个变体索引信息,所述变体索引信息包括信息中的信息索引;

获取模块,用于获取所述待检测信息索引所对应的信息内容;

处理模块,用于根据所述检测结果对所述待检测信息索引所对应的信息内容进行处理,得到已处理信息;

发送模块,用于发送所述已处理信息,以展示所述已处理信息。

本申请一方面提供一种网络节点设备,包括:存储器和处理器;

其中,所述存储器用于存储程序;

所述处理器用于执行所述存储器中的程序,包括如下步骤:

获取原始索引信息集合,其中,所述原始索引信息集合中包括至少一个原始索引信息,每个原始索引信息包括明文形式的敏感内容;

获取待匹配区块中的信息,其中,所述信息包括信息内容以及信息索引,所述信息内容与所述信息索引具有对应关系;

通过所述原始索引信息集合对所述信息中的所述信息内容进行匹配,得到匹配结果;

当所述匹配结果指示匹配成功时,根据所述匹配结果生成变体索引信息集合,其中,所述变体索引信息集合包括至少一个变体索引信息,所述变体索引信息包括所述信息中的与所述信息内容对应的所述信息索引。

本申请一方面提供一种网络节点设备,包括:存储器和处理器;

其中,所述存储器用于存储程序;

所述处理器用于执行所述存储器中的程序,包括如下步骤:

接收请求信息,其中,所述请求信息中携带待检测信息索引;

通过变体索引信息集合对所述请求信息中携带的所述待检测信息索引进行检测,得到检测结果,其中,所述变体索引信息集合包括至少一个变体索引信息,所述变体索引信息包括信息中的信息索引;

获取所述待检测信息索引所对应的信息内容;

根据所述检测结果对所述待检测信息索引所对应的信息内容进行处理,得到已处理信息;

发送所述已处理信息,以展示所述已处理信息。

本申请的一方面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中存储有指令,当其在计算机上运行时,使得计算机执行上述所述的方法。

从以上技术方案可以看出，本申请实施例具有以下优点：

本申请实施例中，提供了一种基于区块链的信息处理方法，首先获取原始索引信息集合，其中，原始索引信息集合中包括至少一个原始索引信息，每个原始索引信息包括明文形式的敏感内容，然后获取待匹配区块中的信息，其中，信息包括信息内容以及信息索引，信息内容与信息索引具有对应关系，再通过原始索引信息集合对信息中的信息内容进行匹配，得到匹配结果，当匹配结果指示匹配成功时，根据匹配结果生成变体索引信息集合，其中，变体索引信息集合包括至少一个变体索引信息，变体索引信息包括信息中的与信息内容对应的信息索引。通过上述方式，在对于索引信息的记录不再以明文形式进行维护，而是对区块链交易过程中涉及到索引信息的信息索引进行记录，由此形成变体索引信息，变体索引信息不会直接显示索引信息的具体内容，而是以信息索引的形式进行维护，从而不易出现安全隐患，提升信息维护的安全性。

附图说明

图1为本申请实施例中基于区块链的信息处理系统的一个架构示意图；

图2为本申请实施例中区块的一个组成结构示意图；

图3为本申请实施例中基于区块链的信息处理方法一个实施例示意图；

图4为本申请实施例中变体索引信息集合的一个更新流程示意图；

图5为本申请实施例中变体索引信息集合的一个应用流程示意图；

图6为本申请实施例中变体索引信息集合的一个应用流程示意图；

图7为本申请实施例中基于区块链的信息处理方法一个实施例示意图；

图8为本申请实施例中客户端展示已处理交易信息的一个流程示意图；

图9为本申请实施例中基于区块链的信息处理装置一个实施例示意图；

图10为本申请实施例中基于区块链的信息处理装置一个实施例示意图；

图11为本申请实施例中基于区块链的信息处理装置一个实施例示意图；

图12为本申请实施例中网络节点设备一个结构示意图。

具体实施方式

本申请实施例提供了一种基于区块链的信息处理方法、装置和计算机可读存储介质，在对于索引信息的记录不再以明文形式进行维护，而是对区块链交易过程中涉及到索引信息的信息索引进行记录，由此形成变体索引信息，变体索引信息不会直接显示索引信息的具体内容，而是以索引形式进行维护，从而不易出现安全隐患，提升信息维护的安全性。

本申请的说明书和权利要求书及上述附图中的术语“第一”、“第二”、“第三”、“第四”等（如果存在）是用于区别类似的对象，而不必用于描述特定的顺序或先后次序。应该理解这样使用的数据在适当情况下可以互换，以便这里描述的本申请的实施例例如能够以除了在这里图示或描述的那些以外的顺序实施。此外，术语“包括”和“对应于”以及他们的任何变形，意图在于覆盖不排他的包含，例如，包含了一系列步骤或单元的过程、方法、系统、产品或设备不必限于清楚地列出的那些步骤或单元，而是可包括没有清楚地列出的或对于这些过程、方法、产品或设备固有的其它步骤或单元。

应理解，本申请所提供的信息处理方法可应用于区块链系统，区块链（Blockchain）是一种由多方共同维护，使用密码学保证传输和访问安全，能够实现数据一致存储、难以篡改、防止抵赖的记账技术，也称为分布式账本技术（Distributed Ledger Technology）。典型的区块链以块-链结构存储数据。

本申请具体可以应用于区块链的公有链、私有链或者联盟链等，其中，公有链无官方组织以及管理机构，无中心服务器，参与的节点按照系统规则自由接入网络，不受控制，节点间基于共识机制开展工作。私有链建立在一个集团内部，系统的运作规则根据集团要求进行

设定, 修改或者读取权限都被进行了一定的限制, 同时保留着区块链的真实性和部分去中心化的特性。联盟链由若干机构联合发起, 介于公有链和私有链之间, 兼具部分去中心化的特性, 这区块链上的读权限可能是公开的, 也有可能是部分公开的, 也就是说通过内部指定多个预选的节点为记账人, 记账人争夺记账权限, 其他接入节点可以参与交易, 但不过问记账过程。

为了便于理解, 本申请提出了一种基于区块链的信息处理的方法, 该方法应用于图 1 所示的信息处理系统, 请参阅图 1, 图 1 为本申请实施例中基于区块链的信息处理系统的一个架构示意图, 如图所示, 信息处理系统架构可以包括分布式节点(如网络节点设备 1、网络节点设备 2、网络节点设备 3、网络节点设备 4、网络节点设备 5 以及网络节点设备 6), 各个分布式节点之间通过通信链路进行连接, 比如可以通过有线通信链路或无线通信链路进行连接等, 多个分布式节点共同组成了区块链网络。需要说明的是, 图 1 中所示的分布式节点的数目(6 个)仅为示意性的, 根据实际需要可以部署任意数目的分布式节点。

在本申请的一个实施例中, 网络节点设备可以根据区块链网络中的公共配置参数(比如节点数目、区块大小以及每隔多久生成一个区块等)的更新信息生成交易信息, 然后在区块链网络中广播该交易信息, 进而区块链网络中的各个网络节点设备可以对该交易信息进行验证和确认。当区块链网络中的各个网络节点设备对该交易信息达成共识之后, 可以根据该交易信息对公共配置参数进行更新, 实现了在区块链节点运行中对公共配置参数进行更新的目的, 提高了公共配置参数的更新效率。

对于上述区块链中的任意一个网络节点设备而言, 用户可以通过客户端与该网络节点设备发起交易请求, 该交易请求携带待检测信息索引。网络节点设备采用变体索引信息集合对交易请求中的待检测信息索引进行检测, 得到检测结果。如果检测结果表示待检测信息索引不存在敏感信息, 那么该网络节点设备可从其他网络节点设备中获取交易请求对应的目标信息内容, 并向客户端发送目标信息内容, 客户端以明文的形式展示目标信息内容。反之, 如果检测结果表示待检测信息索引存在敏感信息, 则需要对涉及索引信息的目标信息内容进行完全屏蔽或者部分屏蔽。需要说明的是, 客户端部署于终端设备上, 其中, 终端设备包含但不限于平板电脑、笔记本电脑、掌上电脑、手机及个人电脑(Personal Computer, PC), 此处不做限定。

请参阅图 2, 图 2 为本申请实施例中区块链的一个组成结构示意图, 如图所示, 区块链由多个区块组成, 区块是在区块链网络中的数据组织单元, 由链表来将区块进行串联。区块包括区块头和区块主体, 区块头包括前一区块的哈希值、本区块时间戳、区块高度以及其他信息。其中, 前一区块的哈希值用于将该区块与区块链中前一区块相连接, 本区块时间戳用于确定区块生成时间, 区块高度用于表示区块在区块链中的位置。其他信息包括区块主体的 Merkle 数根, 难度目标和随机值等。区块主体包括交易信息, 比如“A 向 B 转账 50 比特币”, 每条交易信息对应一个哈希值, 哈希值能够唯一而精准地标识某条交易信息, 每个区块维护相同的交易信息。

结合上述介绍, 下面将对本申请中基于区块链的信息处理方法进行介绍, 基于区块链的信息处理方法可以由计算机设备执行, 计算机设备可以是如图 1 中的网络节点设备, 请参阅图 3, 本申请实施例中基于区块链的信息处理方法一个实施例包括:

101、获取原始索引信息集合, 其中, 原始索引信息集合中包括至少一个原始索引信息, 每个原始索引信息包括明文形式的敏感内容;

本实施例中, 网络节点设备中的信息处理装置首先需要获取一个原始索引信息集合, 原始索引信息集合中包括与色情、暴力、反动以及诈骗等信息相关的词汇和短语集合, 原始索引信息集合具体可以是一个词库, 表现为表结构, 请参阅表 1, 表 1 为原始索引信息集合的一个示意。

表 1

列名	数据类型	说明
ID	Int32	原始索引信息唯一 ID
敏感级别	Int8	敏感级别： 1：普通敏感 2：中级敏感 3：特别敏感
索引信息内容	String	原始的敏感内容，可以是普通文字或者正则表达式

如表 1 所示，一个原始索引信息对应唯一的标识（identification，ID），原始索引信息通常是一个词语，也可以是一个字或者一句话等。敏感级别表示原始索引信息的敏感程度，对不同级别的原始索引信息可执行不同的处理。索引信息内容就是具体到某个词语或者句子，可以表现为普通文字，也可以表现为正则表达式。其中，ID 对应的数据类型是有符号 32 比特（bit）整数，占 4 个字节。敏感级别对应的数据类型是符号 8bit 整数，占 1 个字节。索引信息内容对应的数据类型是字符串（String）。可以理解的是，表 1 仅为一个示意，不应理解为对原始索引信息集合的限定。

102、获取待匹配区块中的信息，其中，信息包括信息内容以及信息索引，信息内容与信息索引具有对应关系；

本实施例中，信息处理装置获取待匹配区块中的信息。假设区块链中有 N 个区块，这 N 个区块均可以作为待匹配区块，每个区块具有对应的信息，信息具体包括信息内容以及信息索引，其中，信息内容包括用户自定义的字段，信息索引可以包括哈希值、块内索引（Index）以及区块高度。

可以理解的是，每个区块具有一个区块高度，区块高度表示区块在区块链中的位置，即距离首个区块的位置。第一个区块的区块高度定义为 0，后续的区块高度在此基础上依次递增，区块高度并不是区块的唯一标识符，因为可能出现区块链分叉，导致同一个高度有 2 个或多个区块。即一个区块有唯一的一个区块高度，但一个区块高度不对应唯一的一个区块。区块中的每条信息内容对应唯一的哈希值。每条信息内容具有一个块内索引，假设区块链是一个账本，区块是账本中的一页纸，每条信息内容记录在纸内的某一行，那么块内索引就是指信息内容在账本的第几页第几行。

103、通过原始索引信息集合对信息中的信息内容进行匹配，得到匹配结果；

本实施例中，信息处理装置将信息内容中的每条信息内容与原始索引信息集合中的原始索引信息进行匹配，得到每条信息内容的匹配结果。比如，信息内容 1 为“A 给 B 代充五万人民币”，“代充”这个词语属于原始索引信息集合中的原始索引信息，因此，匹配结果指示匹配成功，信息内容 1 属于敏感交易。信息内容 2 为“A 向 C 转账 100 人民币”，这条信息中不包括原始索引信息集合中的原始索引信息，因此，信息内容 2 是安全交易。

104、当匹配结果指示匹配成功时，根据匹配结果生成变体索引信息集合，其中，变体索引信息集合包括至少一个变体索引信息，变体索引信息包括信息中的与信息内容对应的信息索引。

本实施例中，信息处理装置基于交易信息的匹配结果，当匹配结果指示匹配成功时，生成一个变体索引信息集合，变体索引信息集合中包括至少一个变体索引信息，变体索引信息包括信息中的信息索引。请参阅表 2，表 2 为变体索引信息集合的一个示意。

表 2

列名	数据类型	说明
哈希值	String	原始索引信息所在交易的哈希值
敏感级别	Int8	敏感级别： 1：普通敏感 2：中级敏感 3：特别敏感
区块高度	Int64	原始索引信息所在区块高度
块内索引	Int16	原始索引信息所在区块内的索引

如表 2 所示，哈希值表示原始索引信息在信息内容所对应的哈希值。敏感级别表示原始索引信息的敏感程度，对不同级别的原始索引信息可执行不同的处理。区块高度表示原始索引信息所在区块的区块高度。块内索引表示原始索引信息所在区块的信息。其中，哈希值对应的数据类型是 String。敏感级别对应的数据类型是 Int8。区块高度对应的数据类型是 Int64。块内索引对应的数据类型是 Int16。可以理解的是，表 2 仅为一个示意，不应理解为对变体索引信息集合的限定。

本申请实施例中，提供了一种基于区块链的信息处理方法，首先获取原始索引信息集合，其中，原始索引信息集合中包括至少一个原始索引信息，每个原始索引信息包括明文形式的敏感内容，然后获取待匹配区块中的信息，其中，信息包括信息内容以及信息索引，信息内容与信息索引具有对应关系，再通过原始索引信息集合对信息中的信息内容进行匹配，得到匹配结果，当匹配结果指示匹配成功时，根据匹配结果生成变体索引信息集合，其中，变体索引信息集合包括至少一个变体索引信息，变体索引信息包括信息中的与信息内容对应的信息索引。通过上述方式，在对于索引信息的记录不再以明文形式进行维护，而是对区块链交易过程中涉及到索引信息的信息索引进行记录，由此形成变体索引信息，变体索引信息不会直接显示索引信息的具体内容，而是以信息索引的形式进行维护，从而不易出现安全隐患，提升信息维护的安全性。

可选地，在上述图 3 对应的实施例的基础上，本申请实施例提供基于区块链的信息处理方法一个可选实施例中，通过原始索引信息集合对信息中的信息内容进行匹配，可以包括：

通过原始索引信息集合对第一信息内容进行匹配，其中，第一信息内容属于信息；

若第一信息内容属于第一区块中的最后一个信息，则对第二区块中的信息内容进行匹配，其中，第一区块属于待匹配区块的一个区块，第二区块属于待匹配区块的另一个区块，且第二区块为第一区块相邻的下一个区块；

若第一信息内容不为第一区块中的最后一个信息，则获取第一区块中的第二信息内容，通过原始索引信息集合对第二信息内容进行匹配，其中，第二信息内容为第一信息内容相邻的下一个信息内容。

本实施例中，介绍一种通过原始索引信息集合对交易信息中的信息内容进行匹配的方法。具体地，先对第一区块中的第一信息内容进行匹配，如果第一信息内容是第一区块中的最后一个信息，则获取第二区块的第一条信息内容进行匹配，第二区块是第一区块的下一个区块。如果第一信息内容不是第一区块中的最后一个信息，那么从第一区块中获取第二信息内容，再通过原始索引信息集合对第二信息内容进行匹配。直至各个区块中每条信息所对应的信息

内容都完成匹配。

为了便于说明，请参阅图 4，图 4 为本申请实施例中变体索引信息集合的一个更新流程示意图，如图所示：

步骤 S1 中，开始进行原始索引信息匹配；

步骤 S2 中，区块高度表示为 N，区块中包括 X 个信息内容，将 N 初始化为 1，将 X 初始化为 0；

步骤 S3 中，扫描当前区块的信息内容中第 X 个信息内容；

步骤 S4 中，判断第 X 个信息内容中是否存在原始索引信息，比如是否存在敏感词，若存在原始索引信息，则执行步骤 S5，若不存在原始索引信息，则执行步骤 S6；

步骤 S5 中，若第 X 个信息内容存在原始索引信息，则需要记录该 N 值和 X 值，此外，还可以记录第 X 个信息内容所对应的哈希值，也就是将 N 值计入至变体索引信息集合的区块高度字段，X 计入块内索引字段，哈希值计入哈希值字段；

步骤 S6 中，若第 X 个信息内容不存在原始索引信息，那么继续判断当前这个区块是否还具有下一条信息内容，如果具有下一条信息内容，则执行步骤 S7，反之，如果该区块不具有下一条信息内容，则执行步骤 S8；

步骤 S7 中，在高度为 N 的区块中存在下一条信息内容的情况下，将继续加载该区块的下一个信息内容，即对 X 加 1，即 $X=X+1$ ，然后再次执行步骤 S3 至步骤 S6；

步骤 S8 中，在高度为 N 的区块中不存在下一条信息内容的情况下，需要判断是否还具有下一个区块高度所对应的区块，也就是检测是否还有下一个 N 值，若存在，则执行步骤 S10，若不存在，则执行步骤 S9；

步骤 S9 中，在不存在下一个区块高度所对应区块的情况下，将继续等待新区块的产生；

步骤 S10 中，在存在下一个区块高度所对应区块的情况下，需要循环加载下一个区块高度所对应的区块，同时改变 N 值和 X 值，即 $N=N+1$ ， $X=0$ 。

其次，本申请实施例中，提供了一种通过原始索引信息集合对交易信息进行匹配的方法，即通过原始索引信息集合对第一信息内容进行匹配，若第一信息内容属于第一区块中的最后一个交易信息，则对第二区块中的信息内容进行匹配，若第一信息内容不为第一区块中的最后一个交易信息，则获取第一区块中的第二信息内容，通过原始索引信息集合对第二信息内容进行匹配。通过上述方式，在实际匹配过程中，是针对每个区块中的每条信息内容进行匹配，由此实现区块的全量扫描，从而有利于生成更完整的变体索引信息集合。

可选地，在上述图 3 对应的实施例的基础上，本申请实施例提供基于区块链的信息处理方法一个可选实施例中，根据匹配结果生成变体索引信息集合，可以包括：

当匹配结果为信息与原始索引信息集合中的原始索引信息匹配成功时，获取原始索引信息的敏感级别；

获取信息索引中的哈希值、块内索引以及区块高度，其中，块内索引表示信息在待匹配区块的位置；

根据原始索引信息的敏感级别、哈希值、块内索引以及区块高度，生成变体索引信息集合。

本实施例中，将介绍三种变体索引信息集合的表现形式。若匹配结果为信息中的信息内容与原始索引信息集合中的原始索引信息匹配成功，则获取原始索引信息的敏感级别，具体地，以一个信息内容为例，假设信息内容 A 与原始索引信息集合中的原始索引信息 A 匹配成功，则获取原始索引信息 A 的敏感级别。此外，还可以获取信息内容 A 的哈希值以及块内索引，假设信息内容 A 属于区块 M，那么可以获取区块 M 的区块高度。根据上述信息，请参阅表 3，表 3 为变体索引信息集合的一个示意。

表 3

列名	数据类型	说明
----	------	----

哈希值	String	原始索引信息所在交易的哈希值
敏感级别	Int8	敏感级别： 1：普通敏感 2：中级敏感 3：特别敏感
区块高度	Int64	原始索引信息所在区块高度
块内索引	Int16	原始索引信息所在区块内的索引

由表 3 可见，变体索引信息集合可包括原始索引信息的敏感级别、哈希值、块内索引以及区块高度。

请参阅表 4，表 4 为变体索引信息集合的另一个示意。

表 4

列名	数据类型	说明
哈希值	String	原始索引信息所在交易的哈希值
敏感级别	Int8	敏感级别： 1：普通敏感 2：中级敏感 3：特别敏感

由表 4 可见，变体索引信息集合可包括原始索引信息的敏感级别以及哈希值。
请参阅表 5，表 5 为变体索引信息集合的另一个示意。

表 5

列名	数据类型	说明
敏感级别	Int8	敏感级别： 1：普通敏感 2：中级敏感 3：特别敏感
区块高度	Int64	原始索引信息所在区块高度
块内索引	Int16	原始索引信息所在区块内的索引

由表 5 可见，变体索引信息集合可包括原始索引信息的敏感级别、块内索引以及区块高度，生成变体索引信息集合。

其次，本申请实施例中，提供了一种生成变体索引信息集合的方式，若匹配结果为信息

内容与原始索引信息集合中的原始索引信息匹配成功，则获取原始索引信息的敏感级别，然后可以获取信息索引中的哈希值、块内索引以及区块高度，其中，块内索引表示信息内容在待匹配区块的位置，最后可以根据原始索引信息的敏感级别、哈希值、块内索引以及区块高度，生成变体索引信息集合，或，根据原始索引信息的敏感级别以及哈希值，生成变体索引信息集合，或，根据原始索引信息的敏感级别、块内索引以及区块高度，生成变体索引信息集合。通过上述方式，生成的变体索引信息集合可以包括不同的信息，这里列举了三种可用的变体索引信息集合，可根据实际需求进行信息匹配，从而提升方案的灵活性和实用性。

可选地，在上述图 3 对应的实施例的基础上，本申请实施例提供基于区块链的信息处理方法第三个可选实施例中，根据匹配结果生成变体索引信息集合之后，还可以包括：

接收请求信息，其中，请求信息中携带待检测信息索引；

通过变体索引信息集合对待检测信息索引进行检测，得到检测结果；

根据检测结果对请求信息进行处理。

本实施例中，介绍了一种变体索引信息集合的应用方法。当用户请求展示信息时，可通过客户端发送请求信息，信息处理装置接收该请求信息，其中，请求信息中携带待检测信息索引，待检测信息索引属于原始请求的内容。信息处理装置将待检测信息索引与变体索引信息集合中的变体索引信息进行检测，得到检测结果。最后，根据检测结果选择对请求信息的处理方式。

再次，本申请实施例中，提供了一种变体索引信息集合的应用方法，在生成变体索引信息集合之后，还可以接收客户端发送的请求信息，然后通过变体索引信息集合对待检测信息索引进行检测，得到检测结果，最后根据检测结果对请求信息进行处理。通过上述方式，利用变体索引信息集合对信息索引进行检测，可以有效地解决区块链内容安全监管给区块链应用带来的风险，以便将信息索引传递给各个区块链服务的提供者，避免直接传递原始索引信息所带来的安全隐患。

可选地，在上述图 3 对应的实施例的基础上，本申请实施例提供基于区块链的信息处理方法一个可选实施例中，通过变体索引信息集合对待检测信息索引进行检测，得到检测结果，包括：

根据待检测信息索引确定目标哈希值；

通过变体索引信息集合对目标哈希值进行匹配；

若目标哈希值与变体索引信息集合中的变体索引信息匹配成功，则确定待检测信息索引所对应的信息内容属于敏感信息；

若目标哈希值与变体索引信息集合中的变体索引信息匹配失败，则确定待检测信息索引所对应的信息内容属于安全信息。

本实施例中，介绍了一种对待检测信息索引进行检测的方式，为了便于介绍，下面将结合图 5 进行说明，请参阅图 5，图 5 为本申请实施例中变体索引信息集合的一个应用流程图，具体地：

步骤 A1 中，首先获取用户发起的请求信息，根据该请求信息确定对应的待检测信息索引，根据该待检测信息索引获取相应的目标哈希值；

步骤 A2 中，获取更新后的变体索引信息集合，由于区块的数量会有变化，所以变体索引信息集合通常也会进行实时更新；

步骤 A3 中，通过变体索引信息集合对目标哈希值进行匹配，即判断目标哈希值是否命中变体索引信息集合中的哈希值，若匹配失败，则从步骤 A4 开始执行，若匹配成功，则从步骤 A7 开始执行；

步骤 A4 中，若目标哈希值与变体索引信息集合中的变体索引信息匹配失败，则确定待检测信息索引属于安全信息，此时可以从其他区块上获取目标哈希值所对应的目标信息内容；

步骤 A5 中，对目标信息内容进行解码，目标信息内容可以是序列化或比特数组形态的数据，对目标信息内容进行解码之后，可以得到可供肉眼阅读的结构化数据，即得到明文

目标信息内容；

步骤 A6 中，向客户端反馈明文的目标信息内容，可供客户端进行展示；

步骤 A7 中，若目标哈希值与变体索引信息集合中的变体索引信息匹配成功，则确定待检测信息索引属于敏感信息，此时，需要根据业务需求判断是否需要完全屏蔽目标信息内容的展示，若需要完全屏蔽，则执行步骤 A11，若不需要完全屏蔽，则执行步骤 A8；

步骤 A8 中，若不需要完全屏蔽目标信息内容，则可以从其他区块上获取目标哈希值所对应的目标信息内容；

步骤 A9 中，对目标信息内容进行解码，目标信息内容可以是序列化或比特数组形态的数据，对目标信息内容进行解码之后，可以得到可供肉眼阅读的结构化数据，即得到明文的目标信息内容；

步骤 A10 中，采用原始索引信息集合对明文的目标信息内容进行匹配，得到相应的目标索引信息，对目标信息内容中的目标索引信息进行屏蔽，然后向客户端反馈屏蔽目标索引信息后的目标信息内容，可供客户端进行展示；

步骤 A11 中，若需要完全屏蔽目标信息内容，则可以直接提示用户当前的目标信息内容涉及到敏感内容，因此已被屏蔽。

进一步地，本申请实施例中，提供了一种通过变体索引信息集合对待检测信息索引进行检测，得到检测结果的方法。首先根据待检测信息索引确定目标哈希值，然后通过变体索引信息集合对目标哈希值进行匹配，若目标哈希值与变体索引信息集合中的变体索引信息匹配成功，则确定待检测信息索引属于敏感交易信息，若目标哈希值与变体索引信息集合中的变体索引信息匹配失败，则确定待检测信息索引属于安全交易信息。通过上述方式，当用户请求浏览指定的交易时，将用户提交的待查询的哈希值与变体索引信息集合进行匹配，如果该哈希值命中变体索引信息集合，则进行相应的屏蔽处理，如果该哈希值未命中变体索引信息集合，则以明文的形式展示用户想浏览的交易信息，从而提升交易信息公开的安全性。

可选地，在上述图 3 对应的实施例的基础上，本申请实施例提供基于区块链的信息处理方法一个可选实施例中，通过变体索引信息集合对待检测信息索引进行检测，得到检测结果，可以包括：

根据待检测信息索引确定目标块内索引以及目标区块高度；

通过变体索引信息集合对目标块内索引以及目标区块高度进行匹配；

若目标块内索引以及目标区块高度与变体索引信息集合中的变体索引信息匹配成功，则确定待检测信息索引属于敏感交易信息；

若目标块内索引以及目标区块高度与变体索引信息集合中的变体索引信息匹配失败，则确定待检测信息索引所对应的信息内容属于安全信息。

本实施例中，介绍了另一种对待检测信息索引进行检测的方式，为了便于介绍，下面将结合图 6 进行说明，请参阅图 6，图 6 为本申请实施例中变体索引信息集合的一个应用流程示意图，具体地：

步骤 B1 中，首先获取用户发起的请求信息，根据该请求信息确定对应的待检测信息索引，根据该待交易信息获取相应的目标区块高度与目标块内索引；

步骤 B2 中，获取更新后的变体索引信息集合，由于区块的数量会有变化，所以变体索引信息集合通常也会进行实时更新；

步骤 B3 中，通过变体索引信息集合对目标区块高度与目标块内索引进行匹配，即判断目标区块高度与目标块内索引是否同时命中变体索引信息集合中的区块高度与块内索引，若匹配失败，则从步骤 B4 开始执行，若匹配成功，则从步骤 B7 开始执行；

步骤 B4 中，若目标区块高度与目标块内索引与变体索引信息集合中的变体索引信息匹配失败，则确定待检测信息索引属于安全交易信息，此时可以从其他区块上获取目标区块高度与目标块内索引所对应的目标信息内容；

步骤 B5 中，对目标信息内容进行解码，目标信息内容可以是序列化或比特数组形态的

数据,对目标信息内容进行解码之后,可以得到可供肉眼阅读的结构化数据,即得到明文的目标信息内容;

步骤 B6 中,向客户端反馈明文的目标信息内容,可供客户端进行展示;

步骤 B7 中,若目标区块高度与目标块内索引与变体索引信息集合中的变体索引信息匹配成功,则确定待检测信息索引属于敏感信息,此时,需要根据业务需求判断是否需要完全屏蔽目标信息内容的展示,若需要完全屏蔽,则执行步骤 B11,若不需要完全屏蔽,则从步骤 B8 开始执行;

步骤 B8 中,若不需要完全屏蔽目标信息内容,则可以从其他区块上获取目标区块高度与目标块内索引所对应的目标信息内容;

步骤 B9 中,对目标信息内容进行解码,目标信息内容可以是序列化或比特数组形态的数据,对目标信息内容进行解码之后,可以得到可供肉眼阅读的结构化数据,即得到明文的目标信息内容;

步骤 B10 中,采用原始索引信息集合对明文的目标信息内容进行匹配,得到相应的目标索引信息,对目标信息内容中的目标索引信息进行屏蔽,然后向客户端反馈屏蔽目标索引信息后的目标信息内容,可供客户端进行展示;

步骤 B11 中,若需要完全屏蔽目标信息内容,则可以直接提示用户当前的目标信息内容涉及到敏感内容,因此已被屏蔽。

进一步地,本申请实施例中,提供了一种通过变体索引信息集合对待检测信息索引进行检测,得到检测结果的方法。即首先根据待检测信息索引确定目标块内索引以及目标区块高度,然后通过变体索引信息集合对目标块内索引以及目标区块高度进行匹配,若目标块内索引以及目标区块高度与变体索引信息集合中的变体索引信息匹配成功,则确定待检测信息索引所对应的信息属于敏感信息,若目标块内索引以及目标区块高度与变体索引信息集合中的变体索引信息匹配失败,则确定待检测信息索引所对应的信息属于安全信息。通过上述方式,当用户请求浏览指定的交易时,将用户提交的待查询的块内索引以及区块高度与变体索引信息集合进行匹配,如果块内索引以及区块高度命中变体索引信息集合,则进行相应的屏蔽处理,如果该块内索引以及区块高度未命中变体索引信息集合,则以明文的形式展示用户想浏览的信息,从而提升信息公开的安全性。

可选地,在上述图 3 对应的第三个至第五个实施例中任一项的基础上,本申请实施例提供基于区块链的信息处理方法一个可选实施例中,根据检测结果对请求信息进行处理,包括:

若待检测信息索引所对应的信息内容属于安全信息,则根据待检测信息索引获取目标信息内容;

向客户端发送目标信息内容,以使客户端展示目标信息内容。

本实施例中,基于上述图 5 中的步骤 A4、步骤 A5 和步骤 A6,以及图 6 中的 B4、步骤 B5 和步骤 B6,当确定待检测信息索引所对应的信息内容属于安全信息时,根据请求信息获取待检测信息索引所对应的目标信息内容,即从其他区块上获取目标信息内容,对目标信息内容进行解码之后直接发送至客户端,由客户端以明文的方式展示目标信息内容。

更进一步地,本申请实施例中,提供了一种根据检测结果对待检测信息索引所对应的目标信息内容进行处理的方法,若待检测信息索引属于安全交易信息,则根据待检测信息索引获取目标信息内容,向客户端发送目标信息内容,以使客户端展示目标信息内容。通过上述方式,对于安全的信息索引所对应的信息而言,可以以明文形式在客户端上展示完整的信息内容,在保证安全性的同时向用户提供更为完整的信息,从而提升方案的可靠性和可行性。

可选地,在上述图 3 对应的实施例中任一项的基础上,本申请实施例提供基于区块链的信息处理方法一个可选实施例中,根据检测结果对请求信息进行处理,可以包括:

若待检测信息索引所对应的信息内容属于敏感信息,则根据待检测信息索引确定目标敏感级别以及目标业务类型;

根据目标敏感级别以及目标业务类型,判断是否展示待检测信息索引所对应的目标信息

内容；

若确定不展示目标信息内容，则向客户端发送提示信息，以使客户端展示提示信息，其中，提示信息用于提示用户目标信息内容属于敏感信息；

若确定展示目标信息内容，则对目标信息内容进行处理，得到处理后的目标信息内容。

本实施例中，介绍了一种根据检测结果对待检测信息索引所对应的目标信息内容进行处理的方式。如果待检测信息索引所对应的信息内容属于敏感信息，则根据待检测信息索引确定目标敏感级别以及目标业务类型，不同的业务需求往往对应不同的敏感级别和业务类型。由此，根据目标敏感级别以及目标业务类型，判断是否展示请求信息所对应的目标信息内容，如果不展示目标信息内容，则向客户端发送提示信息，比如“本次交易信息涉及敏感内容，不予以展示”，从而提示用户目标信息内容属于敏感交易信息。如果需要展示目标信息内容，则对目标信息内容进行处理，得到处理后的目标信息内容，即对目标信息内容中的目标索引信息进行屏蔽，得到已处理交易信息。

具体地，不同业务对敏感级别和业务类型的要求可能不同，请参阅表 6，表 6 为不同业务需求与敏感级别和业务类型之间的对应关系一个示意。

表 6

业务需求	敏感级别	业务类型	展示情况
A	普通敏感	电子合同业务	交易信息部分展示
B	特别敏感	电子合同业务	交易信息不展示
C	特别敏感	票据业务	交易信息不展示
D	特别敏感	比特币业务	交易信息不展示
E	中级敏感	电子合同业务	交易信息部分展示

由表 6 可知，对于业务 A 而言，目标敏感级别为普通敏感，目标业务类型为电子合同业务，此时，只需要屏蔽目标信息内容中的目标索引信息即可。对于业务 B 而言，目标敏感级别为特别敏感，目标业务类型为电子合同业务，此时，需要屏蔽整个目标信息内容。

更进一步地，本申请实施例中，提供了一种根据检测结果对目标信息内容进行处理的方法，若待检测信息索引所对应的信息内容属于敏感信息，则根据待检测信息索引确定目标敏感级别以及目标业务类型，然后根据目标敏感级别以及目标业务类型，判断是否展示待检测信息索引所对应的目标信息内容，若不展示目标信息内容，则向客户端发送提示信息，以使客户端展示提示信息，若展示目标信息内容，则对目标信息内容进行处理，得到处理后的目标信息内容。通过上述方式，还可以根据具体的业务需求选择是否对敏感信息进行完全屏蔽，从而提升了信息处理的灵活性。

可选地，本申请实施例提供基于区块链的信息处理方法一个可选实施例中，对目标信息内容进行处理，得到处理后的目标信息内容，可以包括：

获取目标信息内容；

通过原始索引信息集合对目标信息内容进行匹配，确定目标信息内容中的目标索引信息；

将目标信息内容中的目标索引信息进行屏蔽，得到处理后的目标信息内容。

本实施例中，介绍一种对目标信息内容进行处理的方式，首先根据请求信息，从其他区块上获取指定哈希值所对应的目标信息内容，与待检测信息索引不同的是，目标信息内容是用户可以自定义的字段，而待检测信息索引是一个系统生成的信息。

在获取到目标信息内容之后，假设目标信息内容为“A 向 B 索要身份证号码信息”，通过原始索引信息集合对该目标信息内容进行匹配，确定目标信息内容中的目标索引信息为“身份证号码”，于是对目标索引信息进行屏蔽，从而得到已处理交易信息，比如“A 向 B 索要*****信息”。信息处理装置向客户端发送已处理交易信息，此时，客户端会展示“A 向 B 索要*****信息”。

再进一步地，本申请实施例中，提供了一种对目标信息内容进行处理的方法，即获取目标信息内容，然后通过原始索引信息集合对目标信息内容进行匹配，确定目标信息内容中的

目标索引信息，再将目标信息内容中的目标索引信息进行屏蔽，得到已处理交易信息，最后向客户端发送已处理交易信息，以使客户端展示已处理交易信息。通过上述方式，可以仅对部分索引信息进行屏蔽，由此可以提升信息安全性，同时，对于非索引信息的部分予以展示，有利于用户对部分信息的获取，从而提升方案的可行性。

结合上述介绍，下面将对本申请中基于区块链的信息处理方法进行介绍，该基于区块链的信息处理方法可以由基于区块链的数据处理装置执行，该基于区块链的数据处理装置设置于网络节点设备中。请参阅图 7，本申请实施例中基于区块链的信息处理方法一个实施例包括：

201、接收请求信息，其中，请求信息中携带待检测信息索引；

本实施例中，当用户请求展示交易相关的信息时，可通过客户端发送请求信息，信息处理装置接收该请求信息，其中，请求信息中携带待检测信息索引，待检测信息索引属于原始请求的内容。

202、通过变体索引信息集合对请求信息中携带的待检测信息索引进行检测，得到检测结果，其中，变体索引信息集合包括至少一个变体索引信息，变体索引信息包括信息中的信息索引；

本实施例中，信息处理装置将待检测信息索引与变体索引信息集合中的变体索引信息进行检测，得到检测结果。可以理解的是，对交易请求中的待检测信息索引进行检测的方式可以参阅图 3 对应的实施例，此处不做赘述。变体索引信息集合中包括至少一个变体索引信息，变体索引信息是索引的形式。具体可以参阅表 3、表 4 以及表 5，且变体索引信息集合的生成方式如图 3 对应的实施例，此处不做赘述。

在一个示例中，上述步骤 202 包括如下几个子步骤：

1、根据待检测信息索引确定目标哈希值；

2、通过变体索引信息集合对目标哈希值进行匹配；

3、若目标哈希值与变体索引信息集合中的变体索引信息匹配成功，则确定待检测信息索引所对应的信息内容属于敏感信息；

4、若目标哈希值与变体索引信息集合中的变体索引信息匹配失败，则确定待检测信息索引所对应的信息内容属于安全信息。

在另一个示例中，上述步骤 202 包括如下几个子步骤：

1、根据待检测信息索引确定目标块内索引以及目标区块高度；

2、通过变体索引信息集合对目标块内索引以及目标区块高度进行匹配；

3、若目标块内索引以及目标区块高度与变体索引信息集合中的变体索引信息匹配成功，则确定待检测信息索引所对应的信息内容属于敏感交易信息；

4、若目标块内索引以及目标区块高度与变体索引信息集合中的变体索引信息匹配失败，则确定待检测信息索引所对应的信息内容属于安全信息。

203、获取待检测信息索引所对应的信息内容；

本实施例中，信息处理装置获取该待检测信息索引所对应的信息内容，具体可以从其他区块上获取相应的信息内容。

204、根据检测结果对待检测信息索引所对应的信息内容进行处理，得到已处理交易信息；

本实施例中，信息处理装置根据检测结果对该信息内容进行处理，如果待检测信息索引指示该信息内容是安全的，则直接以明文的形式展示该信息内容。如果待检测信息索引指示该信息内容是不安全的，则可以根据业务需求，对该信息内容进行完全屏蔽，得到已处理交易信息，或者对该信息内容进行部分屏蔽，得到已处理交易信息。

可选地，上述步骤 204 包括如下几个子步骤：

1、若待检测信息索引所对应的信息内容属于敏感信息，则根据待检测信息索引确定目标敏感级别以及目标业务类型；

2、根据目标敏感级别以及目标业务类型，判断是否展示待检测信息索引所对应的目标信

息内容；

3、若确定展示目标信息内容，则对目标信息内容进行处理，得到已处理信息。205、向客户端发送已处理交易信息，以使客户端展示已处理交易信息。

本实施例中，信息处理装置可以设置在客户端之中，也可以设置在客户端之外；信息处理装置向客户端发送已处理交易信息，以使所述客户端展示已处理交易信息，其中，该客户端具体可以是指区块链浏览器。为了便于介绍，请参阅图 8，图 8 为本申请实施例中客户端展示已处理交易信息的一个流程示意图，图 8 中的信息处理装置设置在客户端之中，如图所示，具体地：

步骤 C1 中，用户通过客户端触发一个请求，即请求查看交易相关的信息；

步骤 C2 中，信息处理装置通过本地区块搜索其他相关的区块；

步骤 C3 中，信息处理装置根据用户发起的请求解码相关区块上的区块信息，得到交易信息；

步骤 C4 中，信息处理装置将交易信息与变体索引信息集合中的变体索引信息进行匹配；

步骤 C5 中，如果匹配得到该信息中存在敏感内容，则屏蔽信息中的敏感内容，比如敏感词或者敏感字等；

步骤 C6 中，信息处理装置向用户展示屏蔽后的信息。

可选地，上述方法还包括如下几个步骤：

1、获取原始索引信息集合，其中，原始索引信息集合中包括至少一个原始索引信息，每个原始索引信息包括明文形式的敏感内容；

2、获取待匹配区块中的信息，其中，信息包括信息内容以及信息索引，信息内容与信息索引具有对应关系；

3、通过原始索引信息集合对信息中的信息内容进行匹配，得到匹配结果；

4、当匹配结果指示匹配成功时，根据匹配结果生成变体索引信息集合，其中，变体索引信息集合包括至少一个变体索引信息，变体索引信息包括信息中的与信息内容对应的信息索引。

可选地，此步骤包括如下几个子步骤：

4.1、当匹配结果为信息与原始索引信息集合中的原始索引信息匹配成功时，获取原始索引信息的敏感级别；

4.2、获取信息索引中的哈希值、块内索引以及区块高度，其中，块内索引表示信息在待匹配区块的位置；

4.3、根据原始索引信息的敏感级别、哈希值、块内索引以及区块高度，生成变体索引信息集合。

有关检测结果的获取过程、已处理信息的获取流程和变体索引信息集合的生成方式可参见上文实施例，此处不再赘述。

本申请实施例中，提供了一种基于区块链的信息处理方法，首先接收客户端发送的交易请求，然后通过变体索引信息集合对交易请求中携带的待检测信息索引进行检测，得到检测结果，再获取待检测信息索引所对应的目标信息内容，最后根据检测结果对目标信息内容进行处理，得到已处理交易信息，向客户端发送已处理交易信息，以使客户端展示已处理交易信息；通过上述方式，利用变体索引信息集合对交易信息进行检测，可以有效地解决区块链内容安全监管给区块链应用带来的风险，以便将索引信息传递给各个区块链服务的提供者，避免直接传递原始索引信息集合所带来的安全隐患。此外，还可以对交易进行处理，得到已处理交易信息，传输已处理交易信息能够进一步提升方案的安全性。

可选地，本申请实施例还提供了一种基于区块链的信息处理方法，该方法包括如下几个步骤：

第一、接收请求信息，其中，请求信息中携带待检测信息索引；

第二、根据待检测信息索引确定目标块内索引以及目标区块高度；

第三、通过变体索引信息集合对目标块内索引以及目标区块高度进行匹配，其中，变体索引信息集合包括至少一个变体索引信息，变体索引信息包括信息中的与信息内容对应的信息索引；

第四、若目标块内索引以及目标区块高度与变体索引信息集合中的变体索引信息匹配成功，则确定待检测信息索引所对应的信息内容属于敏感交易信息；

第五、若目标块内索引以及目标区块高度与变体索引信息集合中的变体索引信息匹配失败，则确定待检测信息索引所对应的信息内容属于安全信息；

第六、根据检测结果对请求信息进行处理。

有关上述步骤的介绍说明可参见上文实施例，此处不再赘述。

下面对本申请中的基于区块链的信息处理装置进行详细描述，请参阅图 9，图 9 为本申请实施例中基于区块链的信息处理装置一个实施例示意图，信息处理装置 30 包括：

获取模块 301，用于获取原始索引信息集合，其中，所述原始索引信息集合中包括至少一个原始索引信息，每个原始索引信息包括明文形式的敏感内容；

所述获取模块 301，还用于获取待匹配区块中的信息，其中，所述信息包括信息内容以及信息索引，所述信息内容与所述信息索引具有对应关系；

匹配模块 302，用于通过所述获取模块 301 获取的所述原始索引信息集合对所述信息中的所述信息内容进行匹配，得到匹配结果；

生成模块 303，用于当所述匹配模块 302 得到的所述匹配结果指示匹配成功时，根据所述匹配结果生成变体索引信息集合，其中，所述变体索引信息集合包括至少一个变体索引信息，所述变体索引信息包括所述信息中的与所述信息内容对应的所述信息索引。

本实施例中，获取模块 301 获取原始索引信息集合，其中，所述原始索引信息集合中包括至少一个原始索引信息，每个原始索引信息包括明文形式的敏感内容，所述获取模块 301 获取待匹配区块中的信息，其中，所述信息包括信息内容以及信息索引，所述信息内容与所述信息索引具有对应关系，匹配模块 302 通过所述获取模块 301 获取的所述原始索引信息集合对所述信息中的所述信息内容进行匹配，得到匹配结果，生成模块 303 当所述匹配模块 302 得到的所述匹配结果指示匹配成功时，根据所述匹配结果生成变体索引信息集合，其中，所述变体索引信息集合包括至少一个变体索引信息，所述变体索引信息包括所述信息中的与所述信息内容对应的所述信息索引。

本申请实施例中，提供了一种基于区块链的信息处理装置，首先获取原始索引信息集合，其中，原始索引信息集合中包括至少一个原始索引信息，每个原始索引信息包括明文形式的敏感内容，然后获取待匹配区块中的信息，其中，信息包括信息内容以及信息索引，信息内容与信息索引具有对应关系，再通过原始索引信息集合对信息中的信息内容进行匹配，得到匹配结果，当匹配结果指示匹配成功时，根据匹配结果生成变体索引信息集合，其中，变体索引信息集合包括至少一个变体索引信息，变体索引信息包括信息中的与信息内容对应的信息索引。通过上述方式，在对于索引信息的记录不再以明文形式进行维护，而是对区块链交易过程中涉及到索引信息的信息索引进行记录，由此形成变体索引信息，变体索引信息不会直接显示索引信息的具体内容，而是以信息索引的形式进行维护，从而不易出现安全隐患，提升信息维护的安全性。

可选地，在上述图 9 所对应的实施例的基础上，本申请实施例提供的信息处理装置 30 的另一实施例中，

所述匹配模块 302，具体用于通过所述原始索引信息集合对第一信息内容进行匹配，其中，所述第一信息内容属于所述信息；

若所述第一信息内容属于第一区块中的最后一个信息，则对第二区块中的信息内容进行匹配，其中，所述第一区块属于所述待匹配区块的一个区块，所述第二区块属于所述待匹配区块的另一个区块，且所述第二区块为所述第一区块相邻的下一个区块；

若所述第一信息内容不为第一区块中的最后一个信息，则获取所述第一区块中的第二信

息内容,通过所述原始索引信息集合对所述第二信息内容进行匹配,其中,所述第二信息内容为所述第一信息内容相邻的下一个信息内容。

其次,本申请实施例中,提供了一种通过原始索引信息集合对交易信息进行匹配的方法,即通过原始索引信息集合对第一信息内容进行匹配,若第一信息内容属于第一区块中的最后一个交易信息,则对第二区块中的信息内容进行匹配,若第一信息内容不为第一区块中的最后一个交易信息,则获取第一区块中的第二信息内容,通过原始索引信息集合对第二信息内容进行匹配。通过上述方式,在实际匹配过程中,是针对每个区块中的每条信息内容进行匹配,由此实现区块的全量扫描,从而有利于生成更完整的变体索引信息集合。

可选地,在上述图9所对应的实施例的基础上,本申请实施例提供的信息处理装置30的另一实施例中,

所述生成模块303,具体用于当匹配结果为信息与原始索引信息集合中的原始索引信息匹配成功时,获取原始索引信息的敏感级别;

获取信息索引中的哈希值、块内索引以及区块高度,其中,块内索引表示信息在待匹配区块的位置;

根据原始索引信息的敏感级别、哈希值、块内索引以及区块高度,生成变体索引信息集合。

其次,本申请实施例中,提供了一种生成变体索引信息集合的方式,若匹配结果为信息内容与原始索引信息集合中的原始索引信息匹配成功,则获取原始索引信息的敏感级别,然后可以获取信息索引中的哈希值、块内索引以及区块高度,其中,块内索引表示信息内容在待匹配区块的位置,最后可以根据原始索引信息的敏感级别、哈希值、块内索引以及区块高度,生成变体索引信息集合,或,根据原始索引信息的敏感级别以及哈希值,生成变体索引信息集合,或,根据原始索引信息的敏感级别、块内索引以及区块高度,生成变体索引信息集合。通过上述方式,生成的变体索引信息集合可以包括不同的信息,这里列举了三种可用的变体索引信息集合,可根据实际需求进行信息匹配,从而提升方案的灵活性和实用性。

可选地,在上述图9所对应的实施例的基础上,请参阅图10,本申请实施例提供的信息处理装置30的另一实施例中,信息处理装置30还包括处理模块304;

所述处理模块304,用于在所述生成模块303根据所述匹配结果生成变体索引信息集合之后,接收请求信息,其中,所述请求信息中携带待检测信息索引;

通过所述变体索引信息集合对所述待检测信息索引进行检测,得到检测结果;

根据所述检测结果对所述请求信息进行处理。

再次,本申请实施例中,提供了一种变体索引信息集合的应用方法,在生成变体索引信息集合之后,还可以接收客户端发送的请求信息,然后通过变体索引信息集合对待检测信息索引进行检测,得到检测结果,最后根据检测结果对请求信息进行处理。通过上述方式,利用变体索引信息集合对信息索引进行检测,可以有效地解决区块链内容安全监管给区块链应用带来的风险,以便将信息索引传递给各个区块链服务的提供者,避免直接传递原始索引信息所带来的安全隐患。

进一步地,本申请实施例中,提供了一种通过变体索引信息集合对待检测信息索引进行检测,得到检测结果的方法。首先根据待检测信息索引确定目标哈希值,然后通过变体索引信息集合对目标哈希值进行匹配,若目标哈希值与变体索引信息集合中的变体索引信息匹配成功,则确定待检测信息索引属于敏感交易信息,若目标哈希值与变体索引信息集合中的变体索引信息匹配失败,则确定待检测信息索引属于安全交易信息。通过上述方式,当用户请求浏览指定的交易时,将用户提交的待查询的哈希值与变体索引信息集合进行匹配,如果该哈希值命中变体索引信息集合,则进行相应的屏蔽处理,如果该哈希值未命中变体索引信息集合,则以明文的形式展示用户想浏览的交易信息,从而提升交易信息公开的安全性。

可选地,在上述图10所对应的实施例的基础上,本申请实施例提供的信息处理装置30的另一实施例中,

所述处理模块 304，具体用于根据所述待检测信息索引确定目标哈希值；

通过所述变体索引信息集合对所述目标哈希值进行匹配；

若所述目标哈希值与所述变体索引信息集合中的变体索引信息匹配成功，则确定所述待检测信息索引所对应的信息内容属于敏感信息；

若所述目标哈希值与所述变体索引信息集合中的变体索引信息匹配失败，则确定所述待检测信息索引所对应的信息内容属于安全信息。

进一步地，本申请实施例中，提供了一种通过变体索引信息集合对待检测信息索引进行检测，得到检测结果的方法。即首先根据待检测信息索引确定目标块内索引以及目标区块高度，然后通过变体索引信息集合对目标块内索引以及目标区块高度进行匹配，若目标块内索引以及目标区块高度与变体索引信息集合中的变体索引信息匹配成功，则确定待检测信息索引所对应的信息内容属于敏感信息，若目标块内索引以及目标区块高度与变体索引信息集合中的变体索引信息匹配失败，则确定待检测信息索引所对应的信息内容属于安全信息。通过上述方式，当用户请求浏览指定的交易时，将用户提交的待查询的块内索引以及区块高度与变体索引信息集合进行匹配，如果块内索引以及区块高度命中变体索引信息集合，则进行相应的屏蔽处理，如果该块内索引以及区块高度未命中变体索引信息集合，则以明文的形式展示用户想浏览的信息，从而提升信息公开的安全性。

可选地，在上述图 10 所对应的实施例的基础上，本申请实施例提供的信息处理装置 30 的另一实施例中，

所述处理模块 304，具体用于根据所述待检测信息索引确定目标块内索引以及目标区块高度；

通过所述变体索引信息集合对所述目标块内索引以及所述目标区块高度进行匹配；

若所述目标块内索引以及所述目标区块高度与所述变体索引信息集合中的变体索引信息匹配成功，则确定所述待检测信息索引属于敏感交易信息；

若所述目标块内索引以及所述目标区块高度与所述变体索引信息集合中的变体索引信息匹配失败，则确定所述待检测信息索引所对应的信息内容属于安全信息。

进一步地，本申请实施例中，提供了一种通过变体索引信息集合对待检测信息索引进行检测，得到检测结果的方法。即首先根据待检测信息索引确定目标块内索引以及目标区块高度，然后通过变体索引信息集合对目标块内索引以及目标区块高度进行匹配，若目标块内索引以及目标区块高度与变体索引信息集合中的变体索引信息匹配成功，则确定待检测信息索引所对应的信息内容属于敏感信息，若目标块内索引以及目标区块高度与变体索引信息集合中的变体索引信息匹配失败，则确定待检测信息索引所对应的信息内容属于安全信息。通过上述方式，当用户请求浏览指定的交易时，将用户提交的待查询的块内索引以及区块高度与变体索引信息集合进行匹配，如果块内索引以及区块高度命中变体索引信息集合，则进行相应的屏蔽处理，如果该块内索引以及区块高度未命中变体索引信息集合，则以明文的形式展示用户想浏览的信息，从而提升信息公开的安全性。

可选地，在上述图 10 所对应的实施例的基础上，本申请实施例提供的信息处理装置 30 的另一实施例中，

所述处理模块 304，具体用于若待检测信息索引所对应的信息内容属于安全信息，则根据待检测信息索引获取目标信息内容；

向客户端发送目标信息内容，以使客户端展示目标信息内容。

更进一步地，本申请实施例中，提供了一种根据检测结果对待检测信息索引所对应的目标信息内容进行处理的方法，若待检测信息索引属于安全交易信息，则根据待检测信息索引获取目标信息内容，向客户端发送目标信息内容，以使客户端展示目标信息内容。通过上述方式，对于安全的信息索引所对应的信息而言，可以以明文形式在客户端上展示完整的信息内容，在保证安全性的同时向用户提供更为完整的信息，从而提升方案的可靠性和可行性。

可选地，在上述图 10 所对应的实施例的基础上，本申请实施例提供的信息处理装置 30

的另一实施例中，

所述处理模块 304，具体用于若所述待检测信息索引所对应的信息内容属于敏感信息，则根据所述待检测信息索引确定目标敏感级别以及目标业务类型；

根据所述目标敏感级别以及所述目标业务类型，判断是否展示所述待检测信息索引所对应的目标信息内容；

若确定不展示所述目标信息内容，则向所述客户端发送提示信息，以使所述客户端展示所述提示信息，其中，所述提示信息用于提示用户所述目标信息内容属于所述敏感信息；

若确定展示所述目标信息内容，则对所述目标信息内容进行处理，得到处理后的目标信息内容，向所述客户端发送所述处理后的目标信息内容，以使所述客户端展示所述处理后的目标信息内容。

更进一步地，本申请实施例中，提供了一种根据检测结果对目标信息内容进行处理的方法，若待检测信息索引所对应的信息内容属于敏感信息，则根据待检测信息索引确定目标敏感级别以及目标业务类型，然后根据目标敏感级别以及目标业务类型，判断是否展示待检测信息索引所对应的目标信息内容，若不展示目标信息内容，则向客户端发送提示信息，以使客户端展示提示信息，若展示目标信息内容，则对目标信息内容进行处理，得到处理后的目标信息内容。通过上述方式，还可以根据具体的业务需求选择是否对敏感信息进行完全屏蔽，从而提升了信息处理的灵活性。

可选地，在上述图 10 所对应的实施例的基础上，本申请实施例提供的信息处理装置 30 的另一实施例中，

所述处理模块 304，具体用于获取目标信息内容；

通过原始索引信息集合对目标信息内容进行匹配，确定目标信息内容中的目标索引信息；

将目标信息内容中的目标索引信息进行屏蔽，得到所述处理后的目标信息内容。

再进一步地，本申请实施例中，提供了一种对目标信息内容进行处理的方法，即获取目标信息内容，然后通过原始索引信息集合对目标信息内容进行匹配，确定目标信息内容中的目标索引信息，再将目标信息内容中的目标索引信息进行屏蔽，得到已处理交易信息，最后向客户端发送已处理交易信息，以使客户端展示已处理交易信息。通过上述方式，可以仅对部分索引信息进行屏蔽，由此可以提升信息安全性，同时，对于非索引信息的部分予以展示，有利于用户对部分信息的获取，从而提升方案的可行性。

下面对本申请中的基于区块链的信息处理装置进行详细描述，请参阅图 11，图 11 为本申请实施例中基于区块链的信息处理装置又一个实施例示意图，信息处理装置 40 包括：

接收模块 401，用于接收请求信息，其中，所述请求信息中携带待检测信息索引；

检测模块 402，用于通过变体索引信息集合对所述接收模块 401 接收的所述请求信息中携带的所述待检测信息索引进行检测，得到检测结果，其中，所述变体索引信息集合包括至少一个变体索引信息，所述变体索引信息包括信息中的信息索引；

获取模块 403，用于获取所述待检测信息索引所对应的信息内容；

处理模块 404，用于根据所述检测模块 402 检测到的所述检测结果，对所述获取模块 403 获取的所述待检测信息索引所对应的信息内容进行处理，得到已处理交易信息；

发送模块 405，用于向所述客户端发送所述处理模块 404 处理得到的所述已处理交易信息，以使所述客户端展示所述已处理交易信息。

可选地，所述检测模块 402，用于：

根据所述待检测信息索引确定目标哈希值；

通过所述变体索引信息集合对所述目标哈希值进行匹配；

若所述目标哈希值与所述变体索引信息集合中的变体索引信息匹配成功，则确定所述待检测信息索引所对应的信息内容属于敏感信息；

若所述目标哈希值与所述变体索引信息集合中的变体索引信息匹配失败，则确定所述待检测信息索引所对应的信息内容属于安全信息。

可选地，所述检测模块 402，用于：

根据所述待检测信息索引确定目标块内索引以及目标区块高度；

通过所述变体索引信息集合对所述目标块内索引以及所述目标区块高度进行匹配；

若所述目标块内索引以及所述目标区块高度与所述变体索引信息集合中的变体索引信息匹配成功，则确定所述待检测信息索引所对应的信息内容属于敏感交易信息；

若所述目标块内索引以及所述目标区块高度与所述变体索引信息集合中的变体索引信息匹配失败，则确定所述待检测信息索引所对应的信息内容属于安全信息。

可选地，所述处理模块 404，用于：

若所述待检测信息索引所对应的信息内容属于敏感信息，则根据所述待检测信息索引确定目标敏感级别以及目标业务类型；

根据所述目标敏感级别以及所述目标业务类型，判断是否展示所述待检测信息索引所对应的目标信息内容；

若确定展示所述目标信息内容，则对所述目标信息内容进行处理，得到所述已处理信息。

可选地，所述信息处理装置 40 还包括：匹配模块和生成模块（图中未示出）。

所述获取模块 403，还用于获取原始索引信息集合，其中，所述原始索引信息集合中包括至少一个原始索引信息，每个原始索引信息包括明文形式的敏感内容；

所述获取模块 403，还用于获取待匹配区块中的所述信息，其中，所述信息包括信息内容以及所述信息索引，所述信息内容与所述信息索引具有对应关系；

匹配模块，用于通过所述原始索引信息集合对所述信息中的所述信息内容进行匹配，得到匹配结果；

生成模块，用于当所述匹配结果指示匹配成功时，根据所述匹配结果生成变体索引信息集合，其中，所述变体索引信息集合包括至少一个变体索引信息，所述变体索引信息包括所述信息中的与所述信息内容对应的所述信息索引。

可选地，所述生成模块，用于：

当所述匹配结果为所述信息与所述原始索引信息集合中的原始索引信息匹配成功时，获取所述原始索引信息的敏感级别；

获取所述信息索引中的哈希值、块内索引以及区块高度，其中，所述块内索引表示所述信息在所述待匹配区块的位置；

根据所述原始索引信息的敏感级别、所述哈希值、所述块内索引以及所述区块高度，生成所述变体索引信息集合。

本实施例中，接收模块 401 接收请求信息，其中，所述请求信息中携带待检测信息索引，检测模块 402 通过变体索引信息集合对所述接收模块 401 接收的所述请求信息中携带的所述待检测信息索引进行检测，得到检测结果，其中，所述变体索引信息集合包括至少一个变体索引信息，所述变体索引信息包括信息中的信息索引，获取模块 403 获取所述待检测信息索引所对应的信息内容，处理模块 404 根据所述检测模块 402 检测到的所述检测结果，对所述获取模块 403 获取的所述待检测信息索引所对应的信息内容进行处理，得到已处理交易信息，发送模块 405 向所述客户端发送所述处理模块 404 处理得到的所述已处理交易信息，以使所述客户端展示所述已处理交易信息。

本申请实施例中，提供了一种基于区块链的信息处理方法，首先接收客户端发送的交易请求，然后通过变体索引信息集合对交易请求中携带的待检测信息索引进行检测，得到检测结果，再获取待检测信息索引所对应的目标信息内容，最后根据检测结果对目标信息内容进行处理，得到已处理交易信息，向客户端发送已处理交易信息，以使客户端展示已处理交易信息；通过上述方式，利用变体索引信息集合对交易信息进行检测，可以有效地解决区块链内容安全监管给区块链应用带来的风险，以便将索引信息传递给各个区块链服务的提供者，避免直接传递原始索引信息集合所带来的安全隐患。此外，还可以对交易进行处理，得到已处理交易信息，传输已处理交易信息能够进一步提升方案的安全性。

图 12 是本申请实施例提供的一种网络节点设备结构示意图, 该网络节点设备 500 可因配置或性能不同而产生比较大的差异, 可以包括一个或一个以上中央处理器 (central processing units, CPU) 522 (例如, 一个或一个以上处理器) 和存储器 532, 一个或一个以上存储应用程序 542 或数据 544 的存储介质 530 (例如一个或一个以上海量存储设备)。其中, 存储器 532 和存储介质 530 可以是短暂存储或持久存储。存储在存储介质 530 的程序可以包括一个或一个以上模块 (图示没标出), 每个模块可以包括对网络节点设备中的一系列指令操作。更进一步地, 中央处理器 522 可以设置为与存储介质 530 通信, 在网络节点设备 500 上执行存储介质 530 中的一系列指令操作。

网络节点设备 500 还可以包括一个或一个以上电源 526, 一个或一个以上有线或无线网络接口 550, 一个或一个以上输入输出接口 558, 和/或, 一个或一个以上操作系统 541, 例如 Windows Server™, Mac OS X™, Unix™, Linux™, FreeBSD™ 等等。

上述实施例中由网络节点设备所执行的步骤可以基于该图 12 所示的网络节点设备结构。

本申请实施例中 CPU 522 用于执行如下步骤:

获取原始索引信息集合, 其中, 所述原始索引信息集合中包括至少一个原始索引信息, 每个原始索引信息包括明文形式的敏感内容;

获取待匹配区块中的信息, 其中, 所述信息包括信息内容以及信息索引, 所述信息内容与所述信息索引具有对应关系;

通过所述原始索引信息集合对所述信息中的所述信息内容进行匹配, 得到匹配结果;

当所述匹配结果指示匹配成功时, 根据所述匹配结果生成变体索引信息集合, 其中, 所述变体索引信息集合包括至少一个变体索引信息, 所述变体索引信息包括所述信息中的与所述信息内容对应的所述信息索引。

本申请实施例中 CPU 522 用于执行如下步骤:

接收请求信息, 其中, 所述请求信息中携带待检测信息索引;

通过变体索引信息集合对所述请求信息中携带的所述待检测信息索引进行检测, 得到检测结果, 其中, 所述变体索引信息集合包括至少一个变体索引信息, 所述变体索引信息包括信息中的信息索引;

获取所述待检测信息索引所对应的信息内容;

根据所述检测结果对所述待检测信息索引所对应的信息内容进行处理, 得到已处理交易信息;

向所述客户端发送所述已处理交易信息, 以使所述客户端展示所述已处理交易信息。

所属领域的技术人员可以清楚地了解到, 为描述的方便和简洁, 上述描述的系统、装置和单元的具体工作过程, 可以参考前述方法实施例中的对应过程, 在此不再赘述。

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

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

另外, 在本申请各个实施例中的各功能单元可以集成在一个处理单元中, 也可以是各个单元单独物理存在, 也可以两个或两个以上单元集成在一个单元中。上述集成的单元既可以采用硬件的形式实现, 也可以采用软件功能单元的形式实现。

所述集成的单元如果以软件功能单元的形式实现并作为独立的产品销售或使用时, 可以存储在一个计算机可读取存储介质中。基于这样的理解, 本申请的技术方案本质上或者说对

现有技术做出贡献的部分或者该技术方案的全部或部分可以以软件产品的形式体现出来，该计算机软件产品存储在一个存储介质中，包括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，或者网络设备等等）执行本申请各个实施例所述方法的全部或部分步骤。而前述的存储介质包括：U 盘、移动硬盘、只读存储器（read-only memory, ROM）、随机存取存储器（random access memory, RAM）、磁碟或者光盘等各种可以存储程序代码的介质。

以上所述，以上实施例仅用以说明本申请的技术方案，而非对其限制；尽管参照前述实施例对本申请进行了详细的说明，本领域的普通技术人员应当理解：其依然可以对前述各实施例所记载的技术方案进行修改，或者对其中部分技术特征进行等同替换；而这些修改或者替换，并不使相应技术方案的本质脱离本申请各实施例技术方案的精神和范围。

权利要求书

1、一种基于区块链的信息处理方法，由网络节点设备执行，包括：

获取原始索引信息集合，其中，所述原始索引信息集合中包括至少一个原始索引信息，每个原始索引信息包括明文形式的敏感内容；

获取待匹配区块中的信息，其中，所述信息包括信息内容以及信息索引，所述信息内容与所述信息索引具有对应关系；

通过所述原始索引信息集合对所述信息中的所述信息内容进行匹配，得到匹配结果；

当所述匹配结果指示匹配成功时，根据所述匹配结果生成变体索引信息集合，其中，所述变体索引信息集合包括至少一个变体索引信息，所述变体索引信息包括所述信息中的与所述信息内容对应的所述信息索引。

2、根据权利要求1所述的方法，其中，所述通过所述原始索引信息集合对所述信息中的所述信息内容进行匹配，包括：

通过所述原始索引信息集合对第一信息内容进行匹配，其中，所述第一信息内容属于所述信息；

若所述第一信息内容属于第一区块中的最后一个信息，则对第二区块中的信息内容进行匹配，其中，所述第一区块属于所述待匹配区块的一个区块，所述第二区块属于所述待匹配区块的另一个区块，且所述第二区块为所述第一区块相邻的下一个区块；

若所述第一信息内容不为第一区块中的最后一个信息，则获取所述第一区块中的第二信息内容，通过所述原始索引信息集合对所述第二信息内容进行匹配，其中，所述第二信息内容为所述第一信息内容相邻的下一个信息内容。

3、根据权利要求1所述的方法，其中，所述根据所述匹配结果生成变体索引信息集合，包括：

当所述匹配结果为所述信息与所述原始索引信息集合中的原始索引信息匹配成功时，获取所述原始索引信息的敏感级别；

获取所述信息索引中的哈希值、块内索引以及区块高度，其中，所述块内索引表示所述信息在所述待匹配区块的位置；

根据所述原始索引信息的敏感级别、所述哈希值、所述块内索引以及所述区块高度，生成所述变体索引信息集合。

4、根据权利要求3所述的方法，其中，所述根据所述匹配结果生成变体索引信息集合之后，所述方法还包括：

接收请求信息，其中，所述请求信息中携带待检测信息索引；

通过所述变体索引信息集合对所述待检测信息索引进行检测，得到检测结果；

根据所述检测结果对所述请求信息进行处理。

5、根据权利要求4所述的方法，其中，所述通过所述变体索引信息集合对所述待检测信息索引进行检测，得到检测结果，包括：

根据所述待检测信息索引确定目标哈希值；

通过所述变体索引信息集合对所述目标哈希值进行匹配；

若所述目标哈希值与所述变体索引信息集合中的变体索引信息匹配成功，则确定所述待检测信息索引所对应的信息内容属于敏感信息；

若所述目标哈希值与所述变体索引信息集合中的变体索引信息匹配失败，则确定所述待检测信息索引所对应的信息内容属于安全信息。

6、根据权利要求4所述的方法，其中，所述通过所述变体索引信息集合对所述待检测信息索引进行检测，得到检测结果，包括：

根据所述待检测信息索引确定目标块内索引以及目标区块高度；

通过所述变体索引信息集合对所述目标块内索引以及所述目标区块高度进行匹配；

若所述目标块内索引以及所述目标区块高度与所述变体索引信息集合中的变体索引信息匹配成功，则确定所述待检测信息索引所对应的信息内容属于敏感交易信息；

若所述目标块内索引以及所述目标区块高度与所述变体索引信息集合中的变体索引信息匹配失败，则确定所述待检测信息索引所对应的信息内容属于安全信息。

7、根据权利要求4至6中任一项所述的方法，其中，所述根据所述检测结果对所述请求信息进行处理，包括：

若所述待检测信息索引所对应的信息内容属于安全信息，则根据所述待检测信息索引获取目标信息内容；

向客户端发送所述目标信息内容，以使所述客户端展示所述目标信息内容。

8、根据权利要求7所述的方法，其中，所述根据所述检测结果对所述请求信息进行处理，包括：

若所述待检测信息索引所对应的信息内容属于敏感信息，则根据所述待检测信息索引确定目标敏感级别以及目标业务类型；

根据所述目标敏感级别以及所述目标业务类型，判断是否展示所述待检测信息索引所对应的目标信息内容；

若确定不展示所述目标信息内容，则向所述客户端发送提示信息，以使所述客户端展示所述提示信息，其中，所述提示信息用于提示用户所述目标信息内容属于所述敏感信息；

若确定展示所述目标信息内容，则对所述目标信息内容进行处理，得到处理后的目标信息内容，向所述客户端发送所述处理后的目标信息内容，以使所述客户端展示所述处理后的目标信息内容。

9、根据权利要求8所述的方法，其中，所述对所述目标信息内容进行处理，得到处理后的目标信息内容，包括：

获取所述目标信息内容；

通过所述原始索引信息集合对所述目标信息内容进行匹配，确定所述目标信息内容中的目标索引信息；

将所述目标信息内容中的所述目标索引信息进行屏蔽，得到所述处理后的目标信息内容。

10、一种基于区块链的信息处理方法，由网络节点设备执行，包括：

接收请求信息，其中，所述请求信息中携带待检测信息索引；

通过变体索引信息集合对所述请求信息中携带的所述待检测信息索引进行检测，得到检测结果，其中，所述变体索引信息集合包括至少一个变体索引信息，所述变体索引信息包括信息中的信息索引；

获取所述待检测信息索引所对应的信息内容；

根据所述检测结果对所述待检测信息索引所对应的信息内容进行处理，得到已处理信息；

发送所述已处理信息，以展示所述已处理信息。

11、根据权利要求10所述的方法，其中，所述通过变体索引信息集合对所述待检测信息索引进行检测，得到检测结果，包括：

根据所述待检测信息索引确定目标哈希值；

通过所述变体索引信息集合对所述目标哈希值进行匹配；

若所述目标哈希值与所述变体索引信息集合中的变体索引信息匹配成功，则确定所述待检测信息索引所对应的信息内容属于敏感信息；

若所述目标哈希值与所述变体索引信息集合中的变体索引信息匹配失败，则确定所述待检测信息索引所对应的信息内容属于安全信息。

12、根据权利要求10所述的方法，其中，所述通过变体索引信息集合对所述待检测信息索引进行检测，得到检测结果，包括：

根据所述待检测信息索引确定目标块内索引以及目标区块高度；

通过所述变体索引信息集合对所述目标块内索引以及所述目标区块高度进行匹配；

若所述目标块内索引以及所述目标区块高度与所述变体索引信息集合中的变体索引信息匹配成功，则确定所述待检测信息索引所对应的信息内容属于敏感交易信息；

若所述目标块内索引以及所述目标区块高度与所述变体索引信息集合中的变体索引信息匹配失败，则确定所述待检测信息索引所对应的信息内容属于安全信息。

13、根据权利要求10所述的方法，其中，所述根据所述检测结果对所述待检测信息索引所对应的信息内容进行处理，得到已处理信息，包括：

若所述待检测信息索引所对应的信息内容属于敏感信息，则根据所述待检测信息索引确定目标敏感级别以及目标业务类型；

根据所述目标敏感级别以及所述目标业务类型，判断是否展示所述待检测信息索引所对应的目标信息内容；

若确定展示所述目标信息内容，则对所述目标信息内容进行处理，得到所述已处理信息。

14、根据权利要求10至13中任一项所述的方法，其中，所述方法还包括：

获取原始索引信息集合，其中，所述原始索引信息集合中包括至少一个原始索引信息，每个原始索引信息包括明文形式的敏感内容；

获取待匹配区块中的所述信息，其中，所述信息包括信息内容以及所述信息索引，所述信息内容与所述信息索引具有对应关系；

通过所述原始索引信息集合对所述信息中的所述信息内容进行匹配，得到匹配结果；

当所述匹配结果指示匹配成功时，根据所述匹配结果生成变体索引信息集合，其中，所述变体索引信息集合包括至少一个变体索引信息，所述变体索引信息包括所述信息中的与所述信息内容对应的所述信息索引。

15、根据权利要求14所述的方法，其中，所述根据所述匹配结果生成变体索引信息集合，包括：

当所述匹配结果为所述信息与所述原始索引信息集合中的原始索引信息匹配成功时，获取所述原始索引信息的敏感级别；

获取所述信息索引中的哈希值、块内索引以及区块高度，其中，所述块内索引表示所述信息在所述待匹配区块的位置；

根据所述原始索引信息的敏感级别、所述哈希值、所述块内索引以及所述区块高度，生成所述变体索引信息集合。

16、一种基于区块链的数据处理装置，包括：

获取模块，用于获取原始索引信息集合，其中，所述原始索引信息集合中包括至少一个原始索引信息，每个原始索引信息包括明文形式的敏感内容；

所述获取模块，还用于获取待匹配区块中的信息，其中，所述信息包括信息内容以及信息索引，所述信息内容与所述信息索引具有对应关系；

匹配模块，用于通过所述获取模块获取的所述原始索引信息集合对所述信息中的所述信息内容进行匹配，得到匹配结果；

生成模块，用于当所述匹配模块得到的所述匹配结果指示匹配成功时，根据所述匹配结果生成变体索引信息集合，其中，所述变体索引信息集合包括至少一个变体索引信息，所述变体索引信息包括所述信息中的与所述信息内容对应的所述信息索引。

17、一种基于区块链的数据处理装置，包括：

接收模块，用于接收请求信息，其中，所述请求信息中携带待检测信息索引；

检测模块，用于通过变体索引信息集合对所述请求信息中携带的所述待检测信息索引进行检测，得到检测结果，其中，所述变体索引信息集合包括至少一个变体索引信息，所述变体索引信息包括信息中的信息索引；

获取模块，用于获取所述待检测信息索引所对应的信息内容；

处理模块，用于根据所述检测结果对所述待检测信息索引所对应的信息内容进行处理，得到已处理信息；

发送模块，用于发送所述已处理信息，以展示所述已处理信息。

18、一种网络节点设备，包括：存储器和处理器；

其中，所述存储器用于存储程序；

所述处理器用于执行所述存储器中的程序，实现如权利要求 1 至 9 中任一项所述的方法。

19、一种网络节点设备，包括：存储器和处理器；

其中，所述存储器用于存储程序；

所述处理器用于执行所述存储器中的程序，实现如权利要求 10 至 15 中任一项所述的方法。

20、一种计算机可读存储介质，包括指令，当其在计算机上运行时，使得计算机执行如权利要求 1 至 9 中任一项所述的方法，或执行如权利要求 10 至 15 中任一项所述的方法。