(19)中华人民共和国国家知识产权局

(12)发明专利

(10)授权公告号 CN 111814156 B
(45)授权公告日 2022.04.29

(21)申请号 202010921425.1
(22)申请日 2020.09.04
(65)同一申请的已公布的文献号
申请公布号 CN 111814156 A
(43)申请公布日 2020.10.23
(73)专利权人 支付宝(杭州)信息技术有限公司
地址 310000 浙江省杭州市西湖区西溪路556号8层B段801-11
(72)发明人 杨文玉 杨仁慧 刘勤 陈远 李书博 张盛 熊琴
(74)专利代理机构 北京晋德允升知识产权代理有限公司 11623
代理人 王戈
(51)Int.Cl.
G06F 21/57(2013.01)
G06F 21/64(2013.01)
审查员 胡学岭

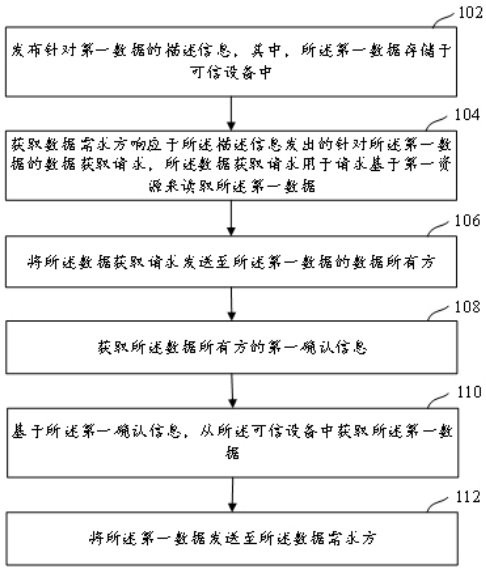
权利要求书7页 说明书17页 附图3页

(54)发明名称

一种基于可信设备的数据获取方法、装置及设备

(57)摘要

本说明书实施例公开了一种基于可信设备的数据获取方法、装置及设备，涉及区块链技术领域。所述方案包括：发布针对第一数据的描述信息，其中，所述第一数据存储于可信设备中；获取数据需求方响应于所述描述信息发出的针对所述第一数据的数据获取请求，所述数据获取请求用于请求基于第一资源来读取所述第一数据；将所述数据获取请求发送至所述第一数据的数据所有方；获取所述数据所有方的第一确认信息；基于所述第一确认信息，从所述可信设备中获取所述第一数据；将所述第一数据发送至所述数据需求方。



CN 111814156 B

1.一种基于可信设备的数据获取方法,包括:

发布针对第一数据的描述信息,其中,所述第一数据存储于可信设备中;所述可信设备为可插拔设备,所述可插拔设备部署有可信执行环境;所述第一数据为个人的隐私数据;所述可信设备为所述第一数据的数据所有方的设备;所述第一数据为所述可信设备从可信数据源获得的数据;所述可信数据源为数据提供方;所述描述信息是在所述可信设备中采用安全应用程序处理生成的;

获取数据需求方响应于所述描述信息发出的针对所述第一数据的数据获取请求,所述数据获取请求用于请求基于第一资源来读取所述第一数据;

将所述数据获取请求发送至所述第一数据的所述数据所有方;

获取所述数据所有方的第一确认信息;

基于所述第一确认信息,从所述可信设备中获取所述第一数据;

将所述第一数据发送至所述数据需求方。

2.如权利要求1所述的方法,所述可信执行环境与操作系统层隔离。

3.如权利要求2所述的方法,所述可插拔设备为U盘。

4.如权利要求2所述的方法,所述可信设备基于所述可信执行环境从所述数据所有方的终端上获取所述第一数据。

5.如权利要求4所述的方法,所述可信设备基于所述可信执行环境从所述数据所有方的终端上获取所述第一数据,具体包括:

所述可信设备通过所述可信执行环境中的代码中预先定义的接口从所述数据所有方的终端上获取所述第一数据。

6.如权利要求1所述的方法,在将所述第一数据发送至所述数据需求方之后,所述方法还包括:

获取所述数据需求方的第二确认信息,所述第二确认信息表示所述数据需求方已接收所述第一数据;

将所述第一数据从所述可信设备中删除。

7.如权利要求1所述的方法,在将所述第一数据发送至所述数据需求方之后,所述方法还包括:

获取所述数据需求方的第三确认信息,所述第三确认信息表示所述数据需求方已接收所述第一数据;

在区块链网络中存储所述第一数据与所述数据需求方的对应关系;

更新所述第一数据的使用记录。

8.如权利要求7所述的方法,所述方法还包括:

将所述第一数据与所述数据需求方的对应关系发送至所述可信设备中进行存储;

将所述第一数据的使用记录发送至所述可信设备中进行存储。

9.如权利要求1所述的方法,在发布针对第一数据的描述信息之前,所述方法还包括;

接收数据所有方的第一数据;

采用安全应用程序对所述第一数据进行处理,得到所述第一数据的描述信息。

10.根据权利要求1所述的方法,将所述第一数据发送至所述数据需求方,具体包括:

采用安全应用程序将所述第一数据发送至所述数据需求方,所述安全应用程序为所述

数据所有方选择的程序。

11.如权利要求1所述的方法,在从所述可信设备中获取所述第一数据之前,所述方法还包括:

确定是否接收到所述数据需求方的所述第一资源,得到第一判断结果;

所述从所述可信设备中获取所述第一数据,具体包括:

当所述第一判断结果为是,从所述可信设备中获取所述第一数据。

12.如权利要求11所述的方法,所述方法还包括:

判断是否接收到所述数据需求方的第四确认信息,得到第二判断结果,所述第四确认信息表示所述数据需求方已接收所述第一数据;

当所述第二判断结果为是,将所述第一资源转发至所述数据所有方。

13.如权利要求1所述的方法,所述第一资源为数据资源或者货币资源。

14.如权利要求1所述的方法,在从所述可信设备中获取所述第一数据之前,所述方法还包括:

将所述数据所有方的私钥发送至所述数据需求方;

所述将所述第一数据发送至所述数据需求方,具体包括:

采用所述数据所有方的公钥对所述第一数据加密;

将加密后的所述第一数据发送至所述数据需求方。

15.如权利要求1所述的方法,所述将所述第一数据发送至所述数据需求方,具体包括:

采用所述数据需求方的公钥对所述第一数据加密;

将加密后的所述第一数据发送至所述数据需求方。

16.一种基于可信设备的数据获取方法,包括:

发布数据需求方针对第一数据的需求信息;

获取数据所有方针对所述需求信息的数据提供信息,所述数据提供信息用于提示所述数据需求方需要提供第一资源来读取所述第一数据;所述第一数据存储于可信设备中;所述可信设备为可插拔设备,所述可插拔设备部署有可信执行环境;所述第一数据为个人的隐私数据;所述可信设备为所述第一数据的所述数据所有方的设备;所述第一数据为所述可信设备从可信数据源获得的数据;所述可信数据源为数据提供方;

将所述数据提供信息发送至所述数据需求方;

获取所述数据需求方的第一确认信息;

基于所述第一确认信息,从所述可信设备中获取所述第一数据;

将所述第一数据发送至所述数据需求方。

17.如权利要求16所述的方法,所述可信执行环境与操作系统层隔离。

18.如权利要求17所述的方法,所述可插拔设备为U盘。

19.如权利要求17所述的方法,所述可信设备基于所述可信执行环境从所述数据所有方的终端上获取所述第一数据。

20.如权利要求19所述的方法,所述可信设备基于所述可信执行环境从所述数据所有方的终端上获取所述第一数据,具体包括:

所述可信设备通过所述可信执行环境中的代码中预先定义的接口从所述数据所有方的终端上获取所述第一数据。

21.如权利要求16所述的方法,在将所述第一数据发送至所述数据需求方之后,所述方法还包括:

获取所述数据需求方的第二确认信息,所述第二确认信息表示所述数据需求方已接收所述第一数据;

将所述第一数据从所述可信设备中删除。

22.如权利要求16所述的方法,在将所述第一数据发送至所述数据需求方之后,所述方法还包括:

获取所述数据需求方的第三确认信息,所述第三确认信息表示所述数据需求方已接收所述第一数据;

在区块链网络中存储所述第一数据与所述数据需求方的对应关系;

更新所述第一数据的使用记录。

23.如权利要求22所述的方法,所述方法还包括:

将所述第一数据与所述数据需求方的对应关系发送至所述可信设备中进行存储;

将所述第一数据的使用记录发送至所述可信设备中进行存储。

24.根据权利要求16所述的方法,将所述第一数据发送至所述数据需求方,具体包括:

采用安全应用程序将所述第一数据发送至所述数据需求方,所述安全应用程序为所述数据所有方选择的程序。

25.如权利要求16所述的方法,所述第一资源为数据资源或者货币资源。

26.如权利要求16所述的方法,在从所述可信设备中获取所述第一数据之前,所述方法还包括:

将所述数据所有方的私钥发送至所述数据需求方;

所述将所述第一数据发送至所述数据需求方,具体包括:

采用所述数据所有方的公钥对所述第一数据加密;

将加密后的所述第一数据发送至所述数据需求方。

27.一种基于可信设备的数据获取装置,包括:

描述信息发布模块,用于发布针对第一数据的描述信息,其中,所述第一数据存储于可信设备中;所述可信设备为可插拔设备,所述可插拔设备部署有可信执行环境;所述第一数据为个人的隐私数据;所述可信设备为所述第一数据的数据所有方的设备;所述第一数据为所述可信设备从可信数据源获得的数据;所述可信数据源为数据提供方;所述描述信息是在所述可信设备中采用安全应用程序处理生成的;

数据获取请求获取模块,用于获取数据需求方响应于所述描述信息发出的针对所述第一数据的数据获取请求,所述数据获取请求用于请求基于第一资源来读取所述第一数据;

数据获取请求发送模块,用于将所述数据获取请求发送至所述第一数据的所述数据所有方;

第一确认信息获取模块,用于获取所述数据所有方的第一确认信息;

第一数据获取模块,用于基于所述第一确认信息,从所述可信设备中获取所述第一数据;

第一数据发送模块,用于将所述第一数据发送至所述数据需求方。

28.如权利要求27所述的装置,所述可信执行环境与操作系统层隔离。

29.如权利要求28所述的装置,所述可插拔设备为U盘。

30.如权利要求28所述的装置,所述可信设备基于所述可信执行环境从所述数据所有方的终端上获取所述第一数据。

31.如权利要求30所述的装置,所述可信设备基于所述可信执行环境从所述数据所有方的终端上获取所述第一数据,具体包括:

所述可信设备通过所述可信执行环境中的代码中预先定义的接口从所述数据所有方的终端上获取所述第一数据。

32.如权利要求27所述的装置,所述装置还包括:

第二确认信息获取模块,用于获取所述数据需求方的第二确认信息,所述第二确认信息表示所述数据需求方已接收所述第一数据;

第一数据删除模块,用于将所述第一数据从所述可信设备中删除。

33.如权利要求27所述的装置,所述装置还包括:

第三确认信息获取模块,用于获取所述数据需求方的第三确认信息,所述第三确认信息表示所述数据需求方已接收所述第一数据;

对应关系存储模块,用于在区块链网络中存储所述第一数据与所述数据需求方的对应关系;

使用记录更新模块,用于更新所述第一数据的使用记录。

34.如权利要求33所述的装置,所述装置还包括:

对应关系发送模块,用于将所述第一数据与所述数据需求方的对应关系发送至所述可信设备中进行存储;

使用记录发送模块,用于将所述第一数据的使用记录发送至所述可信设备中进行存储。

35.如权利要求27所述的装置,所述装置还包括;

第一数据接收模块,用于接收数据所有方的第一数据;

第一数据处理模块,用于采用安全应用程序对所述第一数据进行处理,得到所述第一数据的描述信息。

36.根据权利要求27所述的装置,所述第一数据发送模块,具体用于采用安全应用程序将所述第一数据发送至所述数据需求方,所述安全应用程序为所述数据所有方选择的程序。

37.如权利要求27所述的装置,所述装置还包括:

第一判断模块,用于确定是否接收到所述数据需求方的所述第一资源,得到第一判断结果;

所述第一数据获取模块,具体用于当所述第一判断结果为是,从所述可信设备中获取所述第一数据。

38.如权利要求37所述的装置,所述装置还包括:

第二判断模块,用于判断是否接收到所述数据需求方的第四确认信息,得到第二判断结果,所述第四确认信息表示所述数据需求方已接收所述第一数据;

第一资源转发模块,用于当所述第二判断结果为是,将所述第一资源转发至所述数据所有方。

39.如权利要求27所述的装置,所述第一资源为数据资源或者货币资源。

40.如权利要求27所述的装置,所述装置还包括:

私钥发送模块,用于将所述数据所有方的私钥发送至所述数据需求方;

所述第一数据发送模块,具体包括:

第一加密单元,用于采用所述数据所有方的公钥对所述第一数据加密;

第一发送单元,用于将加密后的所述第一数据发送至所述数据需求方。

41.如权利要求27所述的装置,所述第一数据发送模块,具体包括:

第二加密单元,用于采用所述数据需求方的公钥对所述第一数据加密;

第二发送单元,用于将加密后的所述第一数据发送至所述数据需求方。

42.一种基于可信设备的数据获取装置,包括:

需求信息发布模块,用于发布数据需求方针对第一数据的需求信息;

数据提供信息获取模块,用于获取数据所有方针对所述需求信息的数据提供信息,所述数据提供信息用于提示所述数据需求方需要提供第一资源来读取所述第一数据;所述第一数据存储于可信设备中;所述可信设备为可插拔设备,所述可插拔设备部署有可信执行环境;所述第一数据为个人的隐私数据;所述可信设备为所述第一数据的所述数据所有方的设备;所述第一数据为所述可信设备从可信数据源获得的数据;所述可信数据源为数据提供方;

数据提供信息发送模块,用于将所述数据提供信息发送至所述数据需求方;

第一确认信息获取模块,用于获取所述数据需求方的第一确认信息;

第一数据获取模块,用于基于所述第一确认信息,从所述可信设备中获取所述第一数据;

第一数据发送模块,用于将所述第一数据发送至所述数据需求方。

43.如权利要求42所述的装置,所述可信执行环境与操作系统层隔离。

44.如权利要求43所述的装置,所述可插拔设备为U盘。

45.如权利要求43所述的装置,所述可信设备基于所述可信执行环境从所述数据所有方的终端上获取所述第一数据。

46.如权利要求45所述的装置,所述可信设备基于所述可信执行环境从所述数据所有方的终端上获取所述第一数据,具体包括:

所述可信设备通过所述可信执行环境中的代码中预先定义的接口从所述数据所有方的终端上获取所述第一数据。

47.如权利要求42所述的装置,所述装置还包括:

第二确认信息获取模块,用于获取所述数据需求方的第二确认信息,所述第二确认信息表示所述数据需求方已接收所述第一数据;

第一数据删除模块,用于将所述第一数据从所述可信设备中删除。

48.如权利要求42所述的装置,所述装置还包括:

第三确认信息获取模块,用于获取所述数据需求方的第三确认信息,所述第三确认信息表示所述数据需求方已接收所述第一数据;

对应关系存储模块,用于在区块链网络中存储所述第一数据与所述数据需求方的对应关系;

使用记录更新模块，用于更新所述第一数据的使用记录。

49.如权利要求48所述的装置，所述装置还包括：

对应关系发送模块，用于将所述第一数据与所述数据需求方的对应关系发送至所述可信设备中进行存储；

使用记录发送模块，用于将所述第一数据的使用记录发送至所述可信设备中进行存储。

50.根据权利要求42所述的装置，所述第一数据发送模块，具体用于采用安全应用程序将所述第一数据发送至所述数据需求方，所述安全应用程序为所述数据所有方选择的程序。

51.如权利要求42所述的装置，所述第一资源为数据资源或者货币资源。

52.如权利要求42所述的装置，在从所述可信设备中获取所述第一数据之前，所述装置还包括：

私钥发送模块，用于将所述数据所有方的私钥发送至所述数据需求方；

所述第一数据发送模块，具体包括：

第一加密单元，用于采用所述数据所有方的公钥对所述第一数据加密；

第一发送单元，用于将加密后的所述第一数据发送至所述数据需求方。

53.一种基于可信设备的数据获取设备，包括：

至少一个处理器；以及，

与所述至少一个处理器通信连接的存储器；其中，

所述存储器存储有可被所述至少一个处理器执行的指令，所述指令被所述至少一个处理器执行，以使所述至少一个处理器能够：

发布针对第一数据的描述信息，其中，所述第一数据存储于可信设备中；所述可信设备为可插拔设备，所述可插拔设备部署有可信执行环境；所述第一数据为个人的隐私数据；所述可信设备为所述第一数据的数据所有方的设备；所述第一数据为所述可信设备从可信数据源获得的数据；所述可信数据源为数据提供方；所述描述信息是在所述可信设备中采用安全应用程序处理生成的；

获取数据需求方响应于所述描述信息发出的针对所述第一数据的数据获取请求，所述数据获取请求用于请求基于第一资源来读取所述第一数据；

将所述数据获取请求发送至所述第一数据的所述数据所有方；

获取所述数据所有方的第一确认信息；

基于所述第一确认信息，从所述可信设备中获取所述第一数据；

将所述第一数据发送至所述数据需求方。

54.一种基于可信设备的数据获取设备，包括：

至少一个处理器；以及，

与所述至少一个处理器通信连接的存储器；其中，

所述存储器存储有可被所述至少一个处理器执行的指令，所述指令被所述至少一个处理器执行，以使所述至少一个处理器能够：

发布数据需求方针对第一数据的需求信息；

获取数据所有方针对所述需求信息的数据提供信息，所述数据提供信息用于提示所述

数据需求方需要提供第一资源来读取所述第一数据;所述第一数据存储于可信设备中;所述可信设备为可插拔设备,所述可插拔设备部署有可信执行环境;所述第一数据为个人的隐私数据;所述可信设备为所述第一数据的所述数据所有方的设备;所述第一数据为所述可信设备从可信数据源获得的数据;所述可信数据源为数据提供方;

将所述数据提供信息发送至所述数据需求方;

获取所述数据需求方的第一确认信息;

基于所述第一确认信息,从所述可信设备中获取所述第一数据;

将所述第一数据发送至所述数据需求方。

55.一种计算机可读介质,其上存储有计算机可读指令,所述计算机可读指令可被处理器执行以实现权利要求1至26中任一项所述的基于可信设备的数据获取方法。

一种基于可信设备的数据获取方法、装置及设备

技术领域

[0001] 本申请涉及区块链技术领域，尤其涉及一种基于可信设备的数据获取方法、装置及设备。

背景技术

[0002] 与物品相同，个人数据尤其是隐私数据也可以作为一种商品进行交易，例如，一个人的疾病治疗期间的用药数据以及用药期间的身份状况数据，可以被用来参考从而研发新的药物。那么，这样就出现了对个人隐私数据的供求市场。基于个人数据的隐私性，为了在交易过程不泄露个人数据，因此，亟需一种对个人隐私数据进行可信交易的方法。

发明内容

[0003] 为解决上述技术问题，本说明书实施例是这样实现的：

[0004] 第一方面，本说明书实施例提供的一种基于可信设备的数据获取方法，包括：

[0005] 发布针对第一数据的描述信息，其中，所述第一数据存储于可信设备中；

[0006] 获取数据需求方响应于所述描述信息发出的针对所述第一数据的数据获取请求，所述数据获取请求用于请求基于第一资源来读取所述第一数据；

[0007] 将所述数据获取请求发送至所述第一数据的数据所有方；

[0008] 获取所述数据所有方的第一确认信息；

[0009] 基于所述第一确认信息，从所述可信设备中获取所述第一数据；

[0010] 将所述第一数据发送至所述数据需求方。

[0011] 第二方面，本说明书实施例提供的一种基于可信设备的数据获取方法，包括：

[0012] 发布数据需求方针对第一数据的需求信息；

[0013] 获取数据所有方针对所述需求信息的数据提供信息，所述数据提供信息用于提示所述数据需求方需要提供第一资源来读取所述第一数据；所述第一数据存储于可信设备中；

[0014] 将所述数据提供信息发送至所述数据需求方；

[0015] 获取所述数据需求方的第一确定信息；

[0016] 基于所述第一确认信息，从所述可信设备中获取所述第一数据；

[0017] 将所述第一数据发送至所述数据需求方。

[0018] 第三方面，本说明书实施例提供的一种基于可信设备的数据获取装置，包括：

[0019] 描述信息发布模块，用于发布针对第一数据的描述信息，其中，所述第一数据存储于可信设备中；

[0020] 数据获取请求获取模块，用于获取数据需求方响应于所述描述信息发出的针对所述第一数据的数据获取请求，所述数据获取请求用于请求基于第一资源来读取所述第一数据；

[0021] 数据获取请求发送模块，用于将所述数据获取请求发送至所述第一数据的数据所

有方；

[0022] 第一确认信息获取模块，用于获取所述数据所有方的第一确认信息；

[0023] 第一数据获取模块，用于基于所述第一确认信息，从所述可信设备中获取所述第一数据；

[0024] 第一数据发送模块，用于将所述第一数据发送至所述数据需求方。

[0025] 第四方面，本说明书实施例提供的一种基于可信设备的数据获取装置，包括：

[0026] 需求信息发布模块，用于发布数据需求方针对第一数据的需求信息；

[0027] 数据提供信息获取模块，用于获取数据所有方针对所述需求信息的数据提供信息，所述数据提供信息用于提示所述数据需求方需要提供第一资源来读取所述第一数据；所述第一数据存储于可信设备中；

[0028] 数据提供信息发送模块，用于将所述数据提供信息发送至所述数据需求方；

[0029] 第一确认信息获取模块，用于获取所述数据需求方的第一确定信息；

[0030] 第一数据获取模块，用于基于所述第一确认信息，从所述可信设备中获取所述第一数据；

[0031] 第一数据发送模块，用于将所述第一数据发送至所述数据需求方。

[0032] 第五方面，本说明书实施例提供的一种基于可信设备的数据获取设备，包括：

[0033] 至少一个处理器；以及，

[0034] 与所述至少一个处理器通信连接的存储器；其中，

[0035] 所述存储器存储有可被所述至少一个处理器执行的指令，所述指令被所述至少一个处理器执行，以使所述至少一个处理器能够：

[0036] 发布针对第一数据的描述信息，其中，所述第一数据存储于可信设备中；

[0037] 获取数据需求方响应于所述描述信息发出的针对所述第一数据的数据获取请求，所述数据获取请求用于请求基于第一资源来读取所述第一数据；

[0038] 将所述数据获取请求发送至所述第一数据的数据所有方；

[0039] 获取所述数据所有方的第一确认信息；

[0040] 基于所述第一确认信息，从所述可信设备中获取所述第一数据；

[0041] 将所述第一数据发送至所述数据需求方。

[0042] 第六方面，本说明书实施例提供的一种基于可信设备的数据获取设备，包括：

[0043] 至少一个处理器；以及，

[0044] 与所述至少一个处理器通信连接的存储器；其中，

[0045] 所述存储器存储有可被所述至少一个处理器执行的指令，所述指令被所述至少一个处理器执行，以使所述至少一个处理器能够：

[0046] 发布数据需求方针对第一数据的需求信息；

[0047] 获取数据所有方针对所述需求信息的数据提供信息，所述数据提供信息用于提示所述数据需求方需要提供第一资源来读取所述第一数据；所述第一数据存储于可信设备中；

[0048] 将所述数据提供信息发送至所述数据需求方；

[0049] 获取所述数据需求方的第一确定信息；

[0050] 基于所述第一确认信息，从所述可信设备中获取所述第一数据；

[0051] 将所述第一数据发送至所述数据需求方。

[0052] 第七方面，本说明书实施例提供的一种计算机可读介质，其上存储有计算机可读指令，所述计算机可读指令可被处理器执行以实现一种基于可信设备的数据获取方法。

[0053] 本说明书一个实施例实现了能够达到以下有益效果：通过可信设备中存储第一数据，在供求平台上只发布第一数据的描述信息，可以有效的保护第一数据不被窃取。且，第一数据存储在可信设备上，可以保证第一数据的数据源可信，而且防止第一数据被篡改。

附图说明

[0054] 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申请中记载的一些实施例，对于本领域普通技术人员来讲，在不付出创造性劳动性的前提下，还可以根据这些附图获得其他的附图。

[0055] 图1为本说明书实施例提供的一种基于可信设备的数据获取方法的流程示意图；

[0056] 图2为本说明书实施例提供的另一种基于可信设备的数据获取方法的流程示意图；

[0057] 图3为本说明书实施例提供的对应于图1的一种基于可信设备的数据获取装置的结构示意图；

[0058] 图4为本说明书实施例提供的对应于图2的一种基于可信设备的数据获取装置的结构示意图；

[0059] 图5为本说明书实施例提供的一种基于可信设备的数据获取设备的结构示意图。

具体实施方式

[0060] 为使本说明书一个或多个实施例的目的、技术方案和优点更加清楚，下面将结合本说明书具体实施例及相应的附图对本说明书一个或多个实施例的技术方案进行清楚、完整地描述。显然，所描述的实施例仅是本说明书的一部分实施例，而不是全部的实施例。基于本说明中的实施例，本领域普通技术人员在没有做出创造性劳动前提下所获得的所有其他实施例，都属于本说明书一个或多个实施例保护的范围。

[0061] 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。

[0062] 数据作为一种资源，其流动性和可获取性是很多数据应用和产业发展的基础，但数据交换和共享过程中的隐私保护一直是产业发展的一大挑战。不同于物品的交易过程，数据的交易过程，尤其是隐私数据，需要更加安全的执行环境。现有技术中，通常是将数据进行加密后进行传输，但是加密后的数据也可以被破解，从而造成数据泄露。

[0063] 本方案的将进行交易的数据存储在可信设备中，可以保证交易数据的隐私性、不被篡改，可信设备可以从可信数据源获取数据，从而保证数据源可信。具体地，依赖本地化的可信采集软件从数据源获取个人信息，私有化部署在数据源所在网络环境中。流转网络依托区块链技术，形成公有云的可信流转服务。其中，交易的数据可以以明文、密文、特征向量三种模式输出，依托可信应用进行计算。

[0064] 本方案基于可信网络中数据的供求发布信息进行数据推送。如：将数据的描述信息推送给有需求的用户，或者将需求信息发送给可能有相关数据的用户。

[0065] 可以由数据所有方或数据需求方触发交易，并由另一方进行确认，从而达成共识完成交易。其中，可以以智能合约的方式完成交易。另外，交易的数据可以是数据的完整数据，也可以是通过完整数据进行计算得到的数值或者结果，这与供求双方交易的数据种类有关系。

[0066] 其中，数据的交易过程在供求平台中进行，该供求平台可以是中心化的平台，也可以是去中心化的平台，如区块链网络。

[0067] 区块链(Block chain)，可以理解为是多个区块顺序存储构成的数据链，每个区块的区块头都包含有本区块的时间戳、前一个区块信息的哈希值和本区块信息的哈希值，由此实现区块与区块之间的相互验证，构成不可篡改的区块链。每个区块都可以理解为是一个数据块(存储数据的单元)。区块链作为一种去中心化的数据库，是一串使用密码学方法相互关联产生的数据块，每一个数据块中包含了一次网络交易的信息，用于验证其信息的有效性(防伪)和生成下一个区块。区块与区块首尾相连形成的链，即为区块链。若需要修改块内数据，则需要修改此区块之后所有区块的内容，并将区块链网络中所有节点备份的数据进行修改。因此，区块链具有难以篡改、删除的特点，在数据已保存至区块链后，其作为一种保持内容完整性的方法具有可靠性。

[0068] 区块链技术主要具有以下四个特点：

[0069] (1)去中心化：无需第三方介入，可以实现点对点的交易、协调和协作。在区块链网络中，没有任何一个机构或个人可以实现对全局数据的控制，而任一节点停止工作都不会影响系统整体运作，这种去中心化的网络将极大地提升数据安全性。

[0070] (2)不可篡改性：区块链利用加密技术来验证与存储数据、利用分布式共识算法来新增和更新数据，区块链需要各节点参与验证交易和出块；修改任一数据需要变更所有后续记录，修改单节点数据难度极大。

[0071] (3)公开透明与可溯源性：写入的区块内容将备份复制到各节点中，各节点都拥有最新的完整数据库拷贝且所有的记录信息都是公开的。任何人通过公开的接口都可查询区块数据。区块链中的每一笔交易通过链式存储固化到区块数据中，同时通过密码学算法对所有区块的所有交易记录进行叠加式哈希(HASH)摘要处理，因此可追溯到任何一笔历史交易数据。

[0072] (4)集体维护性：区块链网络的去中心化的特征决定了它的集体维护性。传统中心化机构通常要身兼三职：数据存储者、数据管理者和数据分析者。区块链网络则以对等的方式由各参与方共同维护。各方权责明确，无需向第三方机构让渡权利，实现共同协作。

[0073] 区块链核心关键技术主要涉及到以下几个方面：

[0074] (1)共识机制：由于区块链系统中没有一个中心，因此需要有一个预设的规则来指导各方节点在数据处理上达成一致，所有的数据交互都要按照严格的规则和共识进行。

[0075] (2)密码学技术：密码学技术是区块链的核心技术之一，目前的区块链应用中采用了很多现代密码学的经典算法，主要包括：哈希算法、对称加密、非对称加密、数字签名等。

[0076] (3)分布式存储：区块链是一种点对点网络上的分布账本，每个参与的节点都将独立完整地存储写入区块数据信息。分布式存储区别于传统中心化存储的优势主要体现在两个方面：一、每个节点上备份数据信息，避免了由于单点故障导致的数据丢失。二、每个节点上的数据都独立存储，可以有效规避他人恶意篡改历史数据。

[0077] (4)智能合约:智能合约允许在没有第三方的情况下进行可信交易,只要一方达成了协议预先设定的目标,合约将会自动执行交易。这些交易可追踪且不可逆转。智能合约具有透明可信、自动执行、强制履约的优点。

[0078] 接下来,将针对说明书实施例提供的一种基于可信设备的数据获取方法结合附图进行具体说明:

[0079] 图1为本说明书实施例提供的一种基于可信设备的数据获取方法的流程示意图。从程序角度而言,流程的执行主体可以为搭载于应用服务器的程序或应用客户端。

[0080] 如图1所示,该流程可以包括以下步骤:

[0081] 步骤102:发布针对第一数据的描述信息,其中,所述第一数据存储于可信设备中。

[0082] 第一数据可以是文字、图片、视频等可以采用数字形式进行传输的数据。第一数据可以是个人的隐私数据,也可以是创作的文字、图片、视频等作品。

[0083] 可信设备可以理解为通过软件或者硬件的方式形成的拥有可信环境的设备,可以是部署了可信执行环境(Trusted Execution Environment, TEE)的硬件设备,还可以是通过设置可信任的安全应用程序(Trusted APP)的硬件设备。可信设备可以是一个移动通讯工具、服务器、平板电脑、或者是不可擦洗的存储设备等。

[0084] 可信设备可以为第一数据的数据所有方的设备,如果第一数据的提供方即为数据所有方,如创造的文学作品、视频或照片等,那么数据所有方可以直接将第一数据存储在可信设备中。如果第一数据的提供方不是数据所有方,如,张三的银行流水,提供方为银行,但是所有方为张三,这种情况下,可以限定:所述第一数据为所述可信设备从可信数据源获得的数据。例如,张三可以在银行的网站上申请工资流水,然后,银行会将工资流水发送至张三提供的一个邮箱地址中,然后,可以在可信设备中预先植入程序,按照程序定义的接口,从所述邮箱地址中获取银行发送的工资流水。其中,TEE可以起到硬件黑箱作用,在TEE中执行的代码和数据即便是操作系统层都无法偷窥,只有通过代码中预先定义的接口才能对其进行操作。因此,可信设备可以通过TEE中的代码中预先定义的接口获取可信数据。以获取工资流水例,可以预先在TEE中植入与邮箱地址对应的接口,由于TEE中的代码不能被篡改,因此可以保证可信设备获取的工资流水是从规定的地址获取的,因此获取的工资流水是可信的。

[0085] 一种更加方便的实施方式,所述可信设备为可插拔设备,所述可插拔设备部署有可信执行环境。可选的,可插拔设备为U盘。另外,所述U盘基于可信执行环境从所述数据所有方的终端上获取所述第一数据。具体的,所述可信设备通过所述可信执行环境中的代码中预先定义的接口从所述数据所有方获取所述第一数据。

[0086] 为了增加可信U盘的安全性,可信U盘会有统一的序列号,而且会绑定首次连接的硬件设备,可信U盘只能与绑定设备进行通讯。而且,可信U盘中的数据只可增加和删除,无法进行修改。

[0087] 为了保护第一数据不泄露,在平台上发布的是第一数据的描述信息。描述信息可以是第一数据的数据类型、总体结构等等。

[0088] 其中,根据用户数据得到描述信息的过程可以在可信U盘中执行,也可以在供求平台构建的可信网络中的可信环境中进行处理,例如采用TAPP进行安全计算。以医疗病例信息为例,描述信息可以是疾病名称、病患的年龄、用药种类或者用药时间等。

[0089] 一种实施方式:所述描述信息是在所述可信设备中采用安全应用程序处理生成的。基于可信U盘中搭载的ISV软件,从可信数据源处获取用户的个人信息,利用可信U盘中的TAPP功能处理用户个人信息,得到用户数据的描述信息,并在供求网络里进行发布。

[0090] 另一种实施方式:接收数据所有方的第一数据;采用安全应用程序对所述第一数据进行处理,得到所述第一数据的描述信息。需要指出的是,供求平台通过部署可信执行环境以构建可信网络。具体的,本方案可以通过硬件或者软件的方式,将供求网络构建成可信网络,完成对隐私数据的保护。

[0091] 当供求网络为区块链网络时,每个区块链节点都可以通过虚拟机执行智能合约的创建和调用。包含智能合约的交易和交易的执行结果都存储在区块链账本上,或者是区块链中每个全量节点存储全部账本的方式,对于隐私保护来说是一个挑战。隐私保护可以通过多种技术来实现,例如密码学技术(如同态加密Homomorphic encryption,或零知识证明Zero-knowledge proof),再如硬件隐私技术和网络隔离技术等。其中硬件隐私保护技术典型的包括可信执行环境(Trusted Execution Environment, TEE)。

[0092] 例如,区块链节点均可以通过TEE实现区块链交易的安全执行环境。TEE是基于CPU硬件的安全扩展,且与外部完全隔离的可信执行环境。目前工业界十分关注TEE的方案,几乎所有主流的芯片和软件联盟都有自己的TEE解决方案,比如软件方面的TPM(Trusted Platform Module,可信赖平台模块)以及硬件方面的SGX(Software Guard Extensions,软件保护扩展)、ARM Trustzone(信任区)和AMD PSP(Platform Security Processor,平台安全处理器)等。TEE可以起到硬件黑箱作用,在TEE中执行的代码和数据即便是操作系统层都无法偷窥,只有通过代码中预先定义的接口才能对其进行操作。在效率方面,由于TEE的黑箱性质,在TEE中进行运算的是明文数据,而不是同态加密中复杂的密码学运算,计算过程效率几乎没有损失。因此,通过在区块链节点上部署TEE环境,可以在性能损失相对较小的前提下很大程度上满足区块链场景下的隐私需求。

[0093] 以SGX技术为例。区块链节点可以基于SGX技术创建enclave(围圈或飞地),以作为用于执行区块链交易的TEE。其中,区块链节点利用CPU中新增的处理器指令,在内存中可以分配一部分区域 EPC(Enclave Page Cache,围圈页面缓存或飞地页面缓存),以用于驻留上述的enclave。上述EPC对应的内存区域被CPU内部的内存加密引擎MEE(Memory Encryption Engine)加密,该内存区域中的内容(enclave中的代码和数据)只有在CPU内核中才能够被解密,且用于加解密的密钥只有在EPC启动时生成并存储在CPU中。可见,enclave的安全边界只包含其自身和CPU,无论是特权或非特权软件都无法访问enclave,即便是操作系统管理员和VMM(Virtual Machine Monitor,虚拟机监视器;或称为Hypervisor)也无法影响enclave中的代码和数据,因而具有极高的安全性,并且在上述安全性保障的前提下,CPU能够在enclave中对明文形式的区块链交易进行处理,具有极高的运算效率,从而兼顾了数据安全性和计算效率。而对于进、出TEE的数据,可以是加密的,从而保障数据的隐私。

[0094] 区块链网络(Block Chain Network),是利用块链式数据结构来验证与存储数据、利用分布式节点共识算法来生成和更新数据、利用密码学的方式保证数据传输和访问的安全、利用由自动化脚本代码组成的智能合约来编程和操作数据的一种全新的分布式基础架构与计算方式。区块链网络是由多个节点组成的,每个节点向区块链网络广播信息或者区

块时，所有节点都能接收到，并对接收到的区块进行验证。在对该区块验证通过的节点数在整个区块链网络总节点数中的占比大于预设阈值时，则确定为区块链网络对该区块验证通过，所有节点接收该区块并存储在本地的节点空间中。节点可以理解为是服务器、终端等具有存储功能的电子设备。其中，区块链网络主要分为公有链、联盟链和私有链。

[0095] 步骤104：获取数据需求方响应于所述描述信息发出的针对所述第一数据的数据获取请求，所述数据获取请求用于请求基于第一资源来读取所述第一数据。

[0096] 当第一数据的数据需求方在供求平台中看到所述第一数据的描述信息时，会在平台上发起读取所述第一数据的申请。数据需求方也可以称为数据使用方。

[0097] 另外，为了读取所述第一数据，可以由数据需求方或者数据所有方规定需要付出什么样的资源来交换。其中，第一资源可以是数字资源或货币资源。数据所有方可以限定第一资源的类型和数量。数据需求方也可以申请采用其他方式来申请数据所有方的同意。

[0098] 当第一资源是数据所有方规定的时候，针对第一数据的描述信息还可以包括第一资源。

[0099] 步骤106：将所述数据获取请求发送至所述第一数据的数据所有方。

[0100] 供求平台(网络)的用户可以是个人用户，也可以是企业用户之类。为了便于加强隐私保护，供求平台发布的描述信息中，可以包括也可以不包括第一数据的数据所有方，数据需求方可以不知道数据所有方的身份信息。那么，需要由供求平台将数据获取请求转发至第一数据的数据所有方。

[0101] 数据所有方也可以称为数据持有方、数据属主方等。

[0102] 步骤108：获取所述数据所有方的第一确认信息。

[0103] 如果数据所有方同意将数据需求方的数据获取请求，会回复一个同意的确认信息。为了让数据所有方理解数据需求方购买第一数据的用途，可以在数据获取请求中注明数据需求方的基础数据和购买用途。对于个人用户，这些基础数据可以包括个人的姓名、性别、国籍、证件类型、证件号码、年龄、职业、手机号码、联系地址等信息中的部分或者全部。对于企业用户，这些基础数据可以包括企业的名称、营业执照编号、营业场所地址、法定代表人的姓名、证件类型、证件号码和有效期限等信息中的部分或者全部。

[0104] 上述基础信息在平台上非公开信息，只对第一数据的数据所有方公开。

[0105] 步骤110：基于所述第一确认信息，从所述可信设备中获取所述第一数据。可以采用安全应用程序执行步骤110。其中，所述可信设备可以通过所述可信执行环境中的代码中预先定义的接口从所述数据所有方获取所述第一数据。

[0106] 步骤112：将所述第一数据发送至所述数据需求方。

[0107] 当数据所有方同意将第一数据卖给数据需求方时，当满足一定条件的时候，如收到数据需求方提供的第一资源时，供求平台可以从可信设备获取第一数据，然后将第一数据发送至数据需求方。这整个过程可以采用智能合约来完成。

[0108] 为了提高安全性，将所述第一数据发送至所述数据需求方，具体可以采用安全应用程序将所述第一数据发送至所述数据需求方，所述安全应用程序为所述数据所有方选择的程序。

[0109] 上述方法可以防止第一数据被发送给其他用户，或者被盗用。另外，供求平台在整个过程中，只是一个中介，负责数据的可信传输，并不储存第一数据。

[0110] 应当理解，本说明书一个或多个实施例所述的方法其中部分步骤的顺序可以根据实际需要相互交换，或者其中的部分步骤也可以省略或删除。

[0111] 图1中的方法，通过可信设备中存储第一数据，在供求平台上只发布第一数据的描述信息，可以有效的保护第一数据不被窃取。且，第一数据存储在可信设备上，可以保证第一数据的数据源可信，而且防止第一数据被篡改。

[0112] 另外，在传输过程中，还可以对第一数据进行加密。为了第一数据只发给数据需求方，可以采用所述数据需求方的公钥对所述第一数据加密；将加密后的所述第一数据发送至所述数据需求方。在区块链网络中，各区块链节点的公钥是公开的，因此，可以直接获取数据需求方的公钥，来对第一数据进行加密。而数据需求方的私钥只有数据需求方自己保存，因此，加密后的第一数据只有数据需求方才可以解密后读取。

[0113] 另外，还可以采用数据所有方的公钥对第一数据进行加密，然后将所述加密后的第一数据和数据所有方的私钥发送给数据需求方进行解密。

[0114] 具体的，在从所述可信设备中获取所述第一数据之前，所述方法还可以包括：

[0115] 将所述数据所有方的私钥发送至所述数据需求方；

[0116] 所述将所述第一数据发送至所述数据需求方，具体可以包括：

[0117] 采用所述数据所有方的公钥对所述第一数据加密；

[0118] 将加密后的所述第一数据发送至所述数据需求方。

[0119] 其中，“将所述数据所有方的私钥发送至所述数据需求方”这个步骤相当于第一数据的读取权限授权的过程。这个过程只能保证第一数据只会被有读取权限的用户读取，其他没有权限的用户没有办法读取。

[0120] 另外，数据需求方针对第一数据的数据获取请求即可以是获取第一数据的使用权，还可以是获取第一数据的所有权。

[0121] 当数据需求方针对第一数据的数据获取请求是获取第一数据的所有权时，在将所述第一数据发送至所述数据需求方之后，所述方法还可以包括：

[0122] 获取所述数据需求方的第二确认信息，所述第二确认信息表示所述数据需求方已接收所述第一数据；

[0123] 将所述第一数据从所述可信设备中删除。

[0124] 该方法中，数据需求方针对第一数据的数据获取请求是获取第一数据的所有权，当收到所述数据需求方已经接收到第一数据后，则需要将可信设备中第一数据删除。另外一种可实施的方式，步骤“从所述可信设备中获取所述第一数据”，可以是对所述可信设备对所述第一数据进行类似于“剪切”操作，即对可信设备中的第一数据进行删除，而且第一数据存储在平台内的缓存中。当数据需求方接收到第一数据之后，再将平台缓存中的第一数据删除。

[0125] 当数据需求方针对第一数据的数据获取请求是获取第一数据的使用权时，在将所述第一数据发送至所述数据需求方之后，所述方法还可以包括：

[0126] 获取所述数据需求方的第三确认信息，所述第三确认信息表示所述数据需求方已接收所述第一数据；

[0127] 在区块链网络中存储所述第一数据与所述数据需求方的对应关系；

[0128] 更新所述第一数据的使用记录。

[0129] 该方法中，会在区块链网络中存储第一数据每次的交易信息，记录购买方是谁，购买次数是多少。其中，使用记录可以是第一数据被多少用户读取，还可以记录哪个时间段读取第一数据的用户更多。例如，第一数据为文学作品或视频作品时，可以根据各个数据的读取情况，分析哪种数据更受其他用户的喜欢，从而可以对其他用户进行同类型的数据推荐。

[0130] 另外，还可以将上述“所述第一数据与所述数据需求方的对应关系”和“使用记录”发送至数据需求方，具体的可以存储可信设备中。

[0131] 可选的，所述方法还可以包括：

[0132] 将所述第一数据与所述数据需求方的对应关系发送至所述可信设备中进行存储；

[0133] 将所述第一数据的使用记录发送至所述可信设备中进行存储。

[0134] 数据需求方根据第一数据的使用记录可以分析第一数据是否受欢迎，哪些数据受欢迎，可以有针对性的对数据进行更新。

[0135] 可选的，在从所述可信设备中获取所述第一数据之前，所述方法还包括：

[0136] 确定是否接收到所述数据需求方的所述第一资源，得到第一判断结果；

[0137] 所述从所述可信设备中获取所述第一数据，具体包括：

[0138] 当所述第一判定结果为是，从所述可信设备中获取所述第一数据；

[0139] 判断是否接收到所述数据需求方的第四确认信息，所述第四确认信息表示所述数据需求方已接收所述第一数据，得到第二判断结果；

[0140] 当所述第二判断结果为是，将所述第一资源转发至所述数据所有方。

[0141] 上述方法，提供了如何基于第一资源完成对第一数据的交易过程。

[0142] 当第一资源为货币资源时，假设第一数据为一部文学作品，如果需要获取该文学作品的时候，则需要支付相应的货币，假设为19元。首先需要，用户支付19元，这19元存储在平台的账户中，然后平台将第一数据发送至用户，当用户读取该第一数据后，再将这19元转移到数据所有方的账户中。

[0143] 当第一资源为数字资源时，假设如第一数据为病例信息，而病例信息的所有方的是一个医疗研究机构，为了获取更多的病例信息，可以要求用于交换第一数据的第一资源也为病例信息，以做到信息共享，实现共赢。此时，和货币资源的处理方式基本相同，可以将第一资源暂存在平台上，等数据需求方接收到第一数据之后，再将第一资源发送至数据所有方。另外，还可以采用对第一数据进行加密的方式来对第一资源进行加密，这里不再重复。

[0144] 图1的方法是数据供应的角度进行撰写的。图2为本说明书实施例提供的另一种基于可信设备的数据获取方法的流程示意图。图2是从数据需求的角度进行描述的。如图2所示，所述方法可以包括以下步骤：

[0145] 步骤202：发布数据需求方针对第一数据的需求信息。

[0146] 此处的需求信息可以和图1中的描述信息相对应，需求信息可以指出需求的数据种类等，如什么样的病例。需求信息还可以指出可以支付什么样的资源用来换取所述第一数据。

[0147] 步骤204：获取数据所有方针对所述需求信息的数据提供信息，所述数据提供信息用于提示所述数据需求方需要提供第一资源来读取所述第一数据；所述第一数据存储于可信设备中。

[0148] 数据提供信息可以包括数据所有方能够提供的数据什么，可以有简单的描述，以便于数据需求方判断是否是其需要的数据。另外，还可以注明能够提供的数据存储于可信设备中。

[0149] 步骤206：将所述数据提供信息发送至所述数据需求方。

[0150] 步骤208：获取所述数据需求方的第一确定信息。

[0151] 如果数据需求方同意以数据提供信息中指出的方式提供第一数据，则回复一个肯定的答复。

[0152] 步骤210：基于所述第一确认信息，从所述可信设备中获取所述第一数据。

[0153] 步骤212：将所述第一数据发送至所述数据需求方。

[0154] 可选的，所述可信设备为所述数据所有方的设备。

[0155] 可选的，所述第一数据为所述可信设备从可信数据源获得的数据。

[0156] 可选的，所述可信设备为可插拔设备，所述可插拔设备部署有可信执行环境，所述可信执行环境与操作系统层隔离。

[0157] 可选的，所述可插拔设备为U盘。

[0158] 可选的，所述可信设备基于所述可信执行环境从所述数据所有方的终端上获取所述第一数据。

[0159] 可选的，所述可信设备基于所述可信执行环境从所述数据所有方的终端上获取所述第一数据，具体可以包括：

[0160] 所述可信设备通过所述可信执行环境中的代码中预先定义的接口从所述数据所有方的终端上获取所述第一数据。

[0161] 可选的，在将所述第一数据发送至所述数据需求方之后，所述方法还可以包括：

[0162] 获取所述数据需求方的第二确认信息，所述第二确认信息表示所述数据需求方已接收所述第一数据；

[0163] 将所述第一数据从所述可信设备中删除。

[0164] 可选的，在将所述第一数据发送至所述数据需求方之后，所述方法还可以包括：

[0165] 获取所述数据需求方的第三确认信息，所述第三确认信息表示所述数据需求方已接收所述第一数据；

[0166] 在区块链网络中存储所述第一数据与所述数据需求方的对应关系；

[0167] 更新所述第一数据的使用记录。

[0168] 可选的，所述方法还可以包括：

[0169] 将所述第一数据与所述数据需求方的对应关系发送至所述可信设备中进行存储；

[0170] 将所述第一数据的使用记录发送至所述可信设备中进行存储。

[0171] 可选的，将所述第一数据发送至所述数据需求方，具体可以包括：

[0172] 采用安全应用程序将所述第一数据发送至所述数据需求方，所述安全应用程序为所述数据所有方选择的程序。

[0173] 可选的，所述第一资源为数据资源或者货币资源。

[0174] 可选的，在从所述可信设备中获取所述第一数据之前，所述方法还可以包括：

[0175] 将所述数据所有方的私钥发送至所述数据需求方；

[0176] 所述将所述第一数据发送至所述数据需求方，具体包括：

[0177] 采用所述数据所有方的公钥对所述第一数据加密；

[0178] 将加密后的所述第一数据发送至所述数据需求方。

[0179] 上述扩展方案可以参照图1对应部分的描述，这里不再重复论述。

[0180] 基于同样的思路，本说明书实施例还提供了上述方法对应的装置。图3为本说明书实施例提供的对应于图1的一种基于可信设备的数据获取装置的结构示意图。如图3所示，该装置可以包括：

[0181] 描述信息发布模块302，用于发布针对第一数据的描述信息，其中，所述第一数据存储于可信设备中；

[0182] 数据获取请求获取模块304，用于获取数据需求方响应于所述描述信息发出的针对所述第一数据的数据获取请求，所述数据获取请求用于请求基于第一资源来读取所述第一数据；

[0183] 数据获取请求发送模块306，用于将所述数据获取请求发送至所述第一数据的数据所有方；

[0184] 第一确认信息获取模块308，用于获取所述数据所有方的第一确认信息；

[0185] 第一数据获取模块310，用于基于所述第一确认信息，从所述可信设备中获取所述第一数据；

[0186] 第一数据发送模块312，用于将所述第一数据发送至所述数据需求方。

[0187] 基于图3的装置，本说明书实施例还提供了该装置的一些具体实施方案，下面进行说明。

[0188] 可选的，所述可信设备为所述数据所有方的设备。

[0189] 可选的，所述第一数据为所述可信设备从可信数据源获得的数据。

[0190] 可选的，所述可信设备为可插拔设备，所述可插拔设备部署有可信执行环境，所述可信执行环境与操作系统层隔离。

[0191] 可选的，所述可插拔设备为U盘。

[0192] 可选的，所述可信设备基于所述可信执行环境从所述数据所有方的终端上获取所述第一数据。

[0193] 可选的，所述可信设备基于所述可信执行环境从所述数据所有方的终端上获取所述第一数据，具体可以包括：

[0194] 所述可信设备通过所述可信执行环境中的代码中预先定义的接口从所述数据所有方的终端上获取所述第一数据。

[0195] 可选的，所述装置还可以包括：

[0196] 第二确认信息获取模块，用于获取所述数据需求方的第二确认信息，所述第二确认信息表示所述数据需求方已接收所述第一数据；

[0197] 第一数据删除模块，用于将所述第一数据从所述可信设备中删除。

[0198] 可选的，所述装置还可以包括：

[0199] 第三确认信息获取模块，用于获取所述数据需求方的第三确认信息，所述第三确认信息表示所述数据需求方已接收所述第一数据；

[0200] 对应关系存储模块，用于在区块链网络中存储所述第一数据与所述数据需求方的对应关系；

[0201] 使用记录更新模块，用于更新所述第一数据的使用记录。

[0202] 可选的，所述装置还可以包括：

[0203] 对应关系发送模块，用于将所述第一数据与所述数据需求方的对应关系发送至所述可信设备中进行存储；

[0204] 使用记录发送模块，用于将所述第一数据的使用记录发送至所述可信设备中进行存储。

[0205] 可选的，所述装置还可以包括；

[0206] 第一数据接收模块，用于接收数据所有方的第一数据；

[0207] 第一数据处理模块，用于采用安全应用程序对所述第一数据进行处理，得到所述第一数据的描述信息。

[0208] 可选的，所述描述信息是在所述可信设备中采用安全应用程序处理生成的。

[0209] 可选的，所述第一数据发送模块312，具体用于采用安全应用程序将所述第一数据发送至所述数据需求方，所述安全应用程序为所述数据所有方选择的程序。

[0210] 可选的，所述装置还可以包括：

[0211] 第一判断模块，用于确定是否接收到所述数据需求方的所述第一资源，得到第一判断结果；

[0212] 所述第一数据获取模块310，具体用于当所述第一判定结果为是，从所述可信设备中获取所述第一数据。

[0213] 可选的，所述装置还可以包括：

[0214] 第二判断模块，用于判断是否接收到所述数据需求方的第四确认信息，得到第二判断结果，所述第四确认信息表示所述数据需求方已接收所述第一数据；

[0215] 第一资源转发模块，用于当所述第二判断结果为是，将所述第一资源转发至所述数据所有方。

[0216] 可选的，所述第一资源为数据资源或者货币资源。

[0217] 可选的，所述装置还可以包括：

[0218] 私钥发送模块，用于将所述数据所有方的私钥发送至所述数据需求方；

[0219] 所述第一数据发送模块312，具体可以包括：

[0220] 第一加密单元，用于采用所述数据所有方的公钥对所述第一数据加密；

[0221] 第一发送单元，用于将加密后的所述第一数据发送至所述数据需求方。

[0222] 可选的，所述第一数据发送模块312，具体可以包括：

[0223] 第二加密单元，用于采用所述数据需求方的公钥对所述第一数据加密；

[0224] 第二发送单元，用于将加密后的所述第一数据发送至所述数据需求方。

[0225] 图4为本说明书实施例提供的对应于图2的一种基于可信设备的数据获取装置的结构示意图。如图4所示，该装置可以包括：

[0226] 需求信息发布模块402，用于发布数据需求方针对第一数据的需求信息；

[0227] 数据提供信息获取模块404，用于获取数据所有方针对所述需求信息的数据提供信息，所述数据提供信息用于提示所述数据需求方需要提供第一资源来读取所述第一数据；所述第一数据存储于可信设备中；

[0228] 数据提供信息发送模块406，用于将所述数据提供信息发送至所述数据需求方；

[0229] 第一确认信息获取模块408，用于获取所述数据需求方的第一确定信息；

[0230] 第一数据获取模块410，用于基于所述第一确认信息，从所述可信设备中获取所述第一数据；

[0231] 第一数据发送模块412，用于将所述第一数据发送至所述数据需求方。

[0232] 基于图4的装置，本说明书实施例还提供了该装置的一些具体实施方案，下面进行说明。

[0233] 可选的，所述可信设备为所述数据所有方的设备。

[0234] 可选的，所述第一数据为所述可信设备从可信数据源获得的数据。

[0235] 可选的，所述可信设备为可插拔设备，所述可插拔设备部署有可信执行环境，所述可信执行环境与操作系统层隔离。

[0236] 可选的，所述可插拔设备为U盘。

[0237] 可选的，所述可信设备基于所述可信执行环境从所述数据所有方的终端上获取所述第一数据。

[0238] 可选的，所述可信设备基于所述可信执行环境从所述数据所有方的终端上获取所述第一数据，具体可以包括：

[0239] 所述可信设备通过所述可信执行环境中的代码中预先定义的接口从所述数据所有方的终端上获取所述第一数据。

[0240] 可选的，所述装置还可以包括：

[0241] 第二确认信息获取模块，用于获取所述数据需求方的第二确认信息，所述第二确认信息表示所述数据需求方已接收所述第一数据；

[0242] 第一数据删除模块，用于将所述第一数据从所述可信设备中删除。

[0243] 可选的，所述装置还可以包括：

[0244] 第三确认信息获取模块，用于获取所述数据需求方的第三确认信息，所述第三确认信息表示所述数据需求方已接收所述第一数据；

[0245] 对应关系存储模块，用于在区块链网络中存储所述第一数据与所述数据需求方的对应关系；

[0246] 使用记录更新模块，用于更新所述第一数据的使用记录。

[0247] 可选的，所述装置还可以包括：

[0248] 对应关系发送模块，用于将所述第一数据与所述数据需求方的对应关系发送至所述可信设备中进行存储；

[0249] 使用记录发送模块，用于将所述第一数据的使用记录发送至所述可信设备中进行存储。

[0250] 可选的，所述第一数据发送模块412，具体用于采用安全应用程序将所述第一数据发送至所述数据需求方，所述安全应用程序为所述数据所有方选择的程序。

[0251] 可选的，所述第一资源为数据资源或者货币资源。

[0252] 可选的，所述装置还可以包括：

[0253] 私钥发送模块，用于将所述数据所有方的私钥发送至所述数据需求方；

[0254] 所述第一数据发送模块412，具体包括：

[0255] 第一加密单元，用于采用所述数据所有方的公钥对所述第一数据加密；

[0256] 第一发送单元，用于将加密后的所述第一数据发送至所述数据需求方。

[0257] 基于同样的思路，本说明书实施例还提供了上述方法对应的设备。

[0258] 图5为本说明书实施例提供的一种基于可信设备的数据获取设备的结构示意图。如图5所示，设备500可以包括：

[0259] 至少一个处理器510；以及，

[0260] 与所述至少一个处理器通信连接的存储器530；其中，

[0261] 所述存储器530存储有可被所述至少一个处理器510执行的指令520，所述指令被所述至少一个处理器510执行，以使所述至少一个处理器510能够：

[0262] 发布针对第一数据的描述信息，其中，所述第一数据存储于可信设备中；

[0263] 获取数据需求方响应于所述描述信息发出的针对所述第一数据的数据获取请求，所述数据获取请求用于请求基于第一资源来读取所述第一数据；

[0264] 将所述数据获取请求发送至所述第一数据的数据所有方；

[0265] 获取所述数据所有方的第一确认信息；

[0266] 基于所述第一确认信息，从所述可信设备中获取所述第一数据；

[0267] 将所述第一数据发送至所述数据需求方。

[0268] 或者，以使所述至少一个处理器510能够：

[0269] 发布数据需求方针对第一数据的需求信息；

[0270] 获取数据所有方针对所述需求信息的数据提供信息，所述数据提供信息用于提示所述数据需求方需要提供第一资源来读取所述第一数据；所述第一数据存储于可信设备中；

[0271] 将所述数据提供信息发送至所述数据需求方；

[0272] 获取所述数据需求方的第一确定信息；

[0273] 基于所述第一确认信息，从所述可信设备中获取所述第一数据；

[0274] 将所述第一数据发送至所述数据需求方。

[0275] 基于同样的思路，本说明书实施例还提供了上述方法对应的计算机可读介质。计算机可读介质上存储有计算机可读指令，所述计算机可读指令可被处理器执行以实现以下方法：

[0276] 发布针对第一数据的描述信息，其中，所述第一数据存储于可信设备中；

[0277] 获取数据需求方响应于所述描述信息发出的针对所述第一数据的数据获取请求，所述数据获取请求用于请求基于第一资源来读取所述第一数据；

[0278] 将所述数据获取请求发送至所述第一数据的数据所有方；

[0279] 获取所述数据所有方的第一确认信息；

[0280] 基于所述第一确认信息，从所述可信设备中获取所述第一数据；

[0281] 将所述第一数据发送至所述数据需求方。

[0282] 或者，所述计算机可读指令可被处理器执行以实现以下方法：

[0283] 发布数据需求方针对第一数据的需求信息；

[0284] 获取数据所有方针对所述需求信息的数据提供信息，所述数据提供信息用于提示所述数据需求方需要提供第一资源来读取所述第一数据；所述第一数据存储于可信设备中；

[0285] 将所述数据提供信息发送至所述数据需求方；

[0286] 获取所述数据需求方的第一确定信息；

[0287] 基于所述第一确认信息，从所述可信设备中获取所述第一数据；

[0288] 将所述第一数据发送至所述数据需求方。

[0289] 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，对于图5所示的基于可信设备的数据获取设备而言，由于其基本相似于方法实施例，所以描述的比较简单，相关之处参见方法实施例的部分说明即可。

[0290] 在20世纪90年代，对于一个技术的改进可以很明显地区分是硬件上的改进(例如，对二极管、晶体管、开关等电路结构的改进)还是软件上的改进(对于方法流程的改进)。然而，随着技术的发展，当今的很多方法流程的改进已经可以视为硬件电路结构的直接改进。设计人员几乎都通过将改进的方法流程编程到硬件电路中来得到相应的硬件电路结构。因此，不能说一个方法流程的改进就不能用硬件实体模块来实现。例如，可编程逻辑器件(Programmable Logic Device, PLD)(例如现场可编程门阵列(Field Programmable Gate Array，FPGA))就是这样一种集成电路，其逻辑功能由用户对器件编程来确定。由设计人员自行编程来把一个数字符系统“集成”在一片PLD上，而不需要请芯片制造厂商来设计和制作专用的集成电路芯片。而且，如今，取代手工地制作集成电路芯片，这种编程也多半改用“逻辑编译器(logic compiler)”软件来实现，它与程序开发撰写时所用的软件编译器相类似，而要编译之前的原始代码也得用特定的编程语言来撰写，此称之为硬件描述语言(Hardware Description Language，HDL)，而HDL也并非仅有一种，而是有许多种，如ABEL(Advanced Boolean Expression Language)、AHDL(Altera Hardware Description Language)、Confluence、CUPL(Cornell University Programming Language)、HDCal、JHDL(Java Hardware Description Language)、Lava、Lola、MyHDL、PALASM、RHDL(Ruby Hardware Description Language)等，目前最普遍使用的是VHDL(Very-High-Speed Integrated Circuit Hardware Description Language)与Verilog。本领域技术人员也应该清楚，只需要将方法流程用上述几种硬件描述语言稍作逻辑编程并编程到集成电路中，就可以很容易得到实现该逻辑方法流程的硬件电路。

[0291] 控制器可以按任何适当的方式实现，例如，控制器可以采取例如微处理器或处理器以及存储可由该(微)处理器执行的计算机可读程序代码(例如软件或固件)的计算机可读介质、逻辑门、开关、专用集成电路(Application Specific Integrated Circuit，ASIC)、可编程逻辑控制器和嵌入微控制器的形式，控制器的例子包括但不限于以下微控制器：ARC 625D、Atmel AT91SAM、Microchip PIC18F26K20 以及Silicone Labs C8051F320，存储器控制器还可以被实现为存储器的控制逻辑的一部分。本领域技术人员也知道，除了以纯计算机可读程序代码方式实现控制器以外，完全可以通过将方法步骤进行逻辑编程来使得控制器以逻辑门、开关、专用集成电路、可编程逻辑控制器和嵌入微控制器等的形式来实现相同功能。因此这种控制器可以被认为是一种硬件部件，而对其内包括的用于实现各种功能的装置也可以视为硬件部件内的结构。或者甚至，可以将用于实现各种功能的装置视为既可以是实现方法的软件模块又可以是硬件部件内的结构。

[0292] 上述实施例阐明的系统、装置、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。具体的，计算机例如可以为个人计算机、膝上型计算机、蜂窝电话、相机电话、智能电话、个人数字符助理、媒体播放器、导航设备、电子邮件设备、游戏控制台、平板计算机、可穿戴设备或者这些设备中的任何设备的组合。

[0293] 为了描述的方便，描述以上装置时以功能分为各种单元分别描述。当然，在实施本申请时可以把各单元的功能在同一个或多个软件和/或硬件中实现。

[0294] 本领域内的技术人员应明白，本发明的实施例可提供为方法、系统、或计算机程序产品。因此，本发明可采用完全硬件实施例、完全软件实施例、或结合软件和硬件方面的实施例的形式。而且，本发明可采用在一个或多个其中包含有计算机可用程序代码的计算机可用存储介质(包括但不限于磁盘存储器、CD-ROM、光学存储器等)上实施的计算机程序产品的形式。

[0295] 本发明是参照根据本发明实施例的方法、设备(系统)、和计算机程序产品的流程图和/或方框图来描述的。应理解可由计算机程序指令实现流程图和/或方框图中的每一流程和/或方框、以及流程图和/或方框图中的流程和/或方框的结合。可提供这些计算机程序指令到通用计算机、专用计算机、嵌入式处理机或其他可编程数据处理设备的处理器以产生一个机器，使得通过计算机或其他可编程数据处理设备的处理器执行的指令产生用于实现在流程图一个流程或多个流程和/或方框图一个方框或多个方框中指定的功能的装置。

[0296] 这些计算机程序指令也可存储在能引导计算机或其他可编程数据处理设备以特定方式工作的计算机可读存储器中，使得存储在该计算机可读存储器中的指令产生包括指令装置的制造品，该指令装置实现在流程图一个流程或多个流程和/或方框图一个方框或多个方框中指定的功能。

[0297] 这些计算机程序指令也可装载到计算机或其他可编程数据处理设备上，使得在计算机或其他可编程设备上执行一系列操作步骤以产生计算机实现的处理，从而在计算机或其他可编程设备上执行的指令提供用于实现在流程图一个流程或多个流程和/或方框图一个方框或多个方框中指定的功能的步骤。

[0298] 在一个典型的配置中，计算设备包括一个或多个处理器(CPU)、输入/输出接口、网络接口和内存。

[0299] 内存可能包括计算机可读介质中的非永久性存储器，随机存取存储器(RAM)和/或非易失性内存等形式，如只读存储器(ROM)或闪存(flash RAM)。内存是计算机可读介质的示例。

[0300] 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)、快闪记忆体或其他内存技术、只读光盘只读存储器(CD-ROM)、数字符多功能光盘(DVD)或其他光学存储、磁盒式磁带，磁带式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。

[0301] 还需要说明的是，术语“包括”、“包含”或者其任何其他变体意在涵盖非排他性的

包含，从而使得包括一系列要素的过程、方法、商品或者设备不仅包括那些要素，而且还包括没有明确列出的其他要素，或者是还包括为这种过程、方法、商品或者设备所固有的要素。在没有更多限制的情况下，由语句“包括一个……”限定的要素，并不排除在包括所述要素的过程、方法、商品或者设备中还存在另外的相同要素。

[0302] 本领域技术人员应明白，本申请的实施例可提供为方法、系统或计算机程序产品。因此，本申请可采用完全硬件实施例、完全软件实施例或结合软件和硬件方面的实施例的形式。而且，本申请可采用在一个或多个其中包含有计算机可用程序代码的计算机可用存储介质(包括但不限于磁盘存储器、CD-ROM、光学存储器等)上实施的计算机程序产品的形式。

[0303] 本申请可以在由计算机执行的计算机可执行指令的一般上下文中描述，例如程序模块。一般地，程序模块包括执行特定任务或实现特定抽象数据类型的例程、程序、对象、组件、数据结构等等。也可以在分布式计算环境中实践本申请，在这些分布式计算环境中，由通过通信网络而被连接的远程处理设备来执行任务。在分布式计算环境中，程序模块可以位于包括存储设备在内的本地和远程计算机存储介质中。

[0304] 以上所述仅为本申请的实施例而已，并不用于限制本申请。对于本领域技术人员来说，本申请可以有各种更改和变化。凡在本申请的精神和原理之内所作的任何修改、等同替换、改进等，均应包含在本申请的权利要求范围之内。

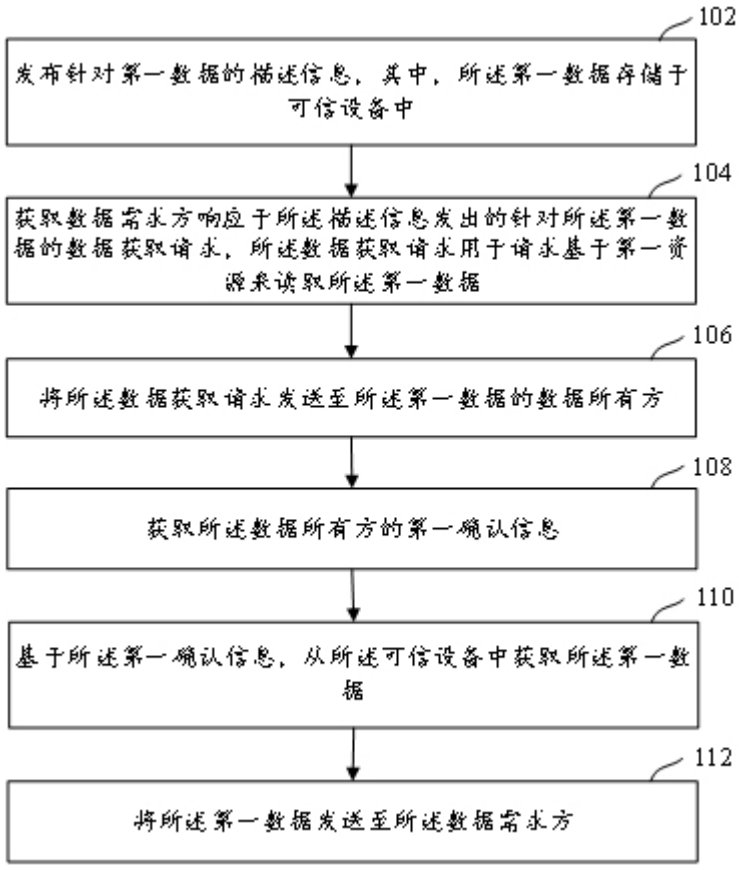

102
发布针对第一数据的描述信息，其中，所述第一数据存储于可信设备中
104
获取数据需求方响应于所述描述信息发出的针对所述第一数据的数据获取请求，所述数据获取请求用于请求基于第一资源来读取所述第一数据
106
将所述数据获取请求发送至所述第一数据的数据所有方
108
获取所述数据所有方的第一确认信息
110
基于所述第一确认信息，从所述可信设备中获取所述第一数据
112
将所述第一数据发送至所述数据需求方

图1

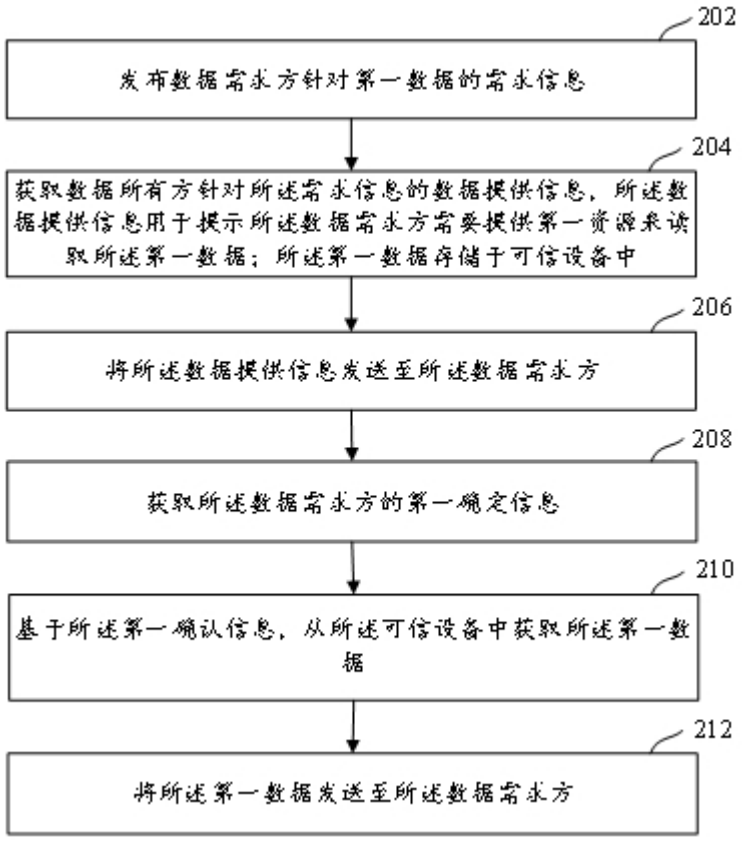

202
发布数据需求方针对第一数据的需求信息
204
获取数据所有方针对所述需求信息的数据提供信息，所述数据提供信息用于提示所述数据需求方需要提供第一资源来读取所述第一数据；所述第一数据存储于可信设备中
206
将所述数据提供信息发送至所述数据需求方
208
获取所述数据需求方的第一确定信息
210
基于所述第一确认信息，从所述可信设备中获取所述第一数据
212
将所述第一数据发送至所述数据需求方

图2

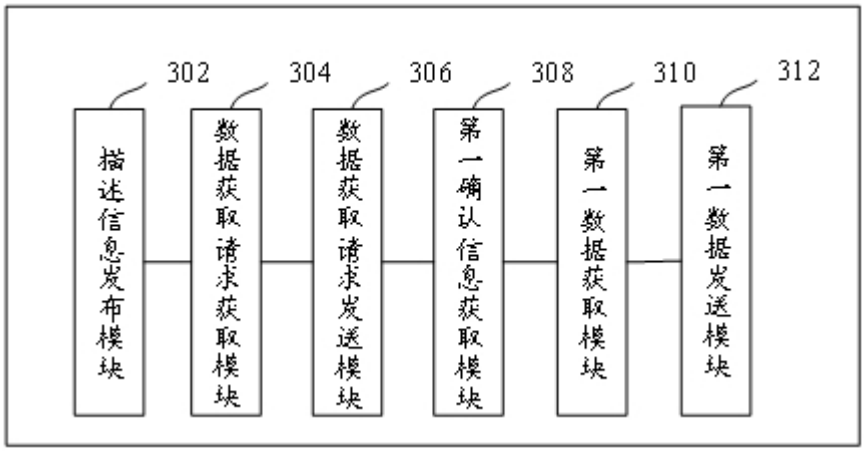

302
描述信息发布模块
304
数据获取请求获取模块
306
数据获取请求发送模块
308
第一确认信息获取模块
310
第一数据获取模块
312
第一数据发送模块

图3

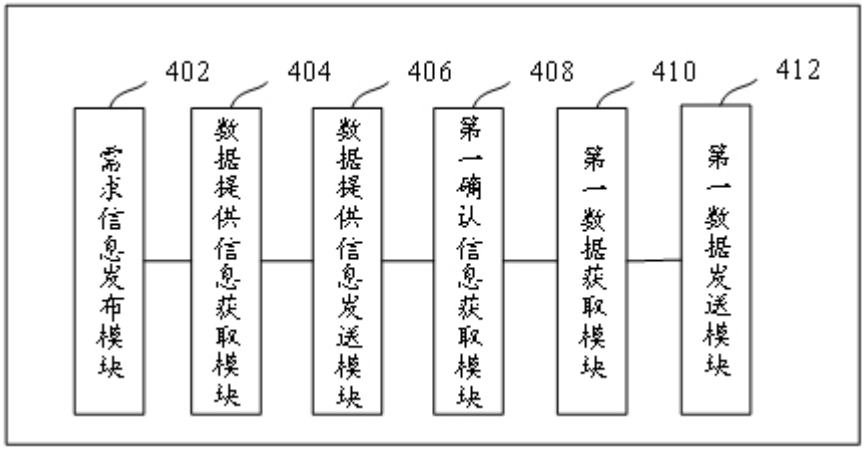

402
404
406
408
410
412
需求信息发布模块
数据提供信息获取模块
数据提供信息发送模块
第一确认信息获取模块
第一数据获取模块
第一数据发送模块

图4

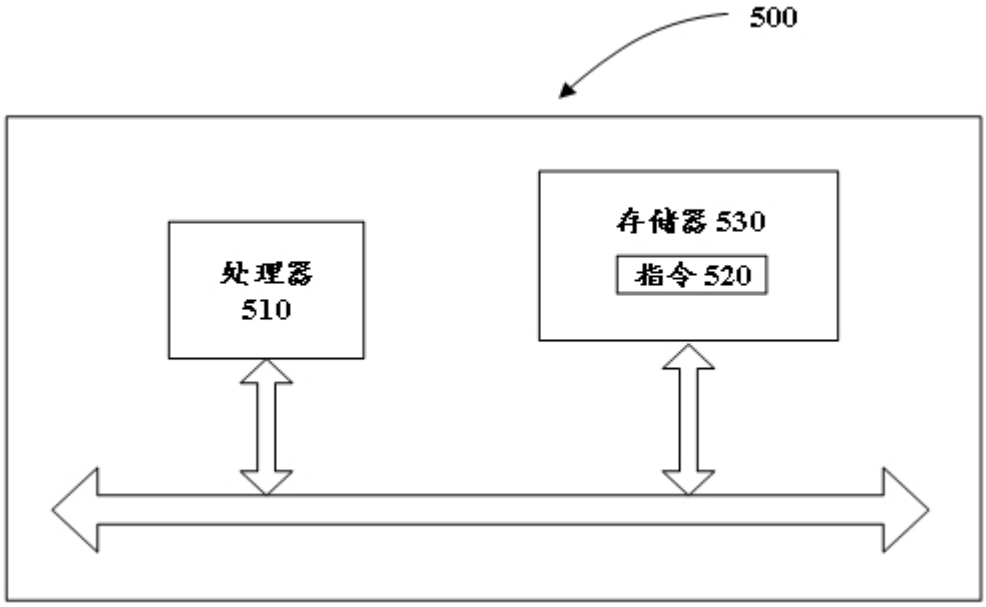

500
处理器
510
存储器 530
指令 520

图5