(19)中华人民共和国国家知识产权局

(12)发明专利申请

(10)申请公布号 CN 111339536 A
(43)申请公布日 2020.06.26

(21)申请号 202010412501.6

(22)申请日 2020.05.15

(71)申请人 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 韩喆 张鸿

(74)专利代理机构 北京博思佳知识产权代理有限公司 11415
代理人 申亚辉

(51)Int.Cl.
G06F 21/57(2013.01)
G06F 21/60(2013.01)
G06F 21/62(2013.01)

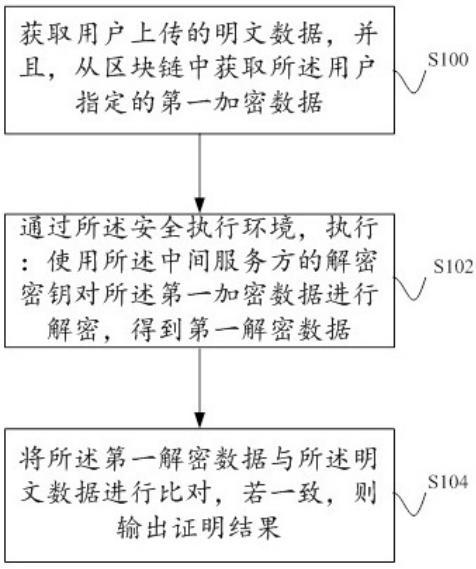
权利要求书2页 说明书7页 附图3页

(54)发明名称

一种基于安全执行环境的数据验证方法及装置

(57)摘要

公开了一种基于安全执行环境的数据验证方法及装置。可以预先在安全执行环境中写入中间服务方的解密密钥。当用户请求可信计算设备证明其拥有明文数据的所有权时，可信计算设备会从区块链中获取用户指定的第一加密数据，第一加密数据是中间服务方使用自己的加密密钥对所述明文数据进行加密后提交给区块链的。可信计算设备可以通过安全执行环境执行：使用所述中间服务方的解密密钥对所述第一加密数据进行解密，得到第一解密数据。可信计算设备如果确定明文数据和第一解密数据一致，就可以证明所述用户拥有所述明文数据的所有权。通过本方案，可以在加强对中间服务方的密钥隐私保护的前提下，证明用户拥有明文数据的所有权。



CN 111339536 A

1.一种基于安全执行环境的数据验证方法,应用于可信计算设备,所述可信计算设备中创建有安全执行环境,所述安全执行环境中存储有中间服务方的解密密钥,所述方法包括:

获取用户上传的明文数据,并且,从区块链中获取所述用户指定的第一加密数据;所述第一加密数据,是所述中间服务方使用自己的加密密钥对所述明文数据进行加密后提交给区块链的;

通过所述安全执行环境,执行:使用所述中间服务方的解密密钥对所述第一加密数据进行解密,得到第一解密数据;

将所述第一解密数据与所述明文数据进行比对,若一致,则输出证明结果,用于证明所述用户拥有所述明文数据的所有权。

2.如权利要求1所述的方法,在将所述第一解密数据与所述明文数据进行比对之前,所述方法还包括:

若确定所述第一解密数据与所述明文数据的数据格式不同,则将所述第一解密数据与所述明文数据处理成具有相同数据格式。

3.如权利要求1所述的方法,所述方法还包括:

若所述第一解密数据与所述明文数据不一致,则拒绝输出所述证明结果。

4.一种基于安全执行环境的数据验证方法,应用于可信计算设备,所述可信计算设备中创建有安全执行环境,所述安全执行环境中存储有中间服务方的解密密钥与用户的解密密钥,所述方法包括:

获取所述用户上传的第二加密数据,并且,从区块链中获取所述用户指定的第一加密数据;所述第二加密数据,是所述用户使用自己的加密密钥对所述明文数据进行加密后得到的;所述第一加密数据,是所述中间服务方使用自己的加密密钥对所述明文数据进行加密后提交给区块链的;

通过所述安全执行环境,执行以下步骤:

使用所述中间服务方的解密密钥对所述第一加密数据进行解密,得到第一解密数据,以及,使用所述用户的解密密钥对所述第二加密数据进行解密,得到第二解密数据;

将所述第一解密数据与所述第二解密数据进行比对,若一致,则输出证明结果,用于证明所述用户拥有所述明文数据的所有权。

5.如权利要求4所述的方法,通过所述安全执行环境,还执行以下步骤:

在将所述第一解密数据与所述第二解密数据进行比对之前,若确定所述第一解密数据与所述第二解密数据的数据格式不同,则将所述第一解密数据与所述第二解密数据处理成具有相同数据格式。

6.如权利要求4所述的方法,所述方法还包括:

若所述第一解密数据与所述第二解密数据不一致,则拒绝输出所述证明结果。

7.一种基于安全执行环境的数据验证装置,应用于可信计算设备,所述装置中创建有安全执行环境,所述安全执行环境中存储有中间服务方的解密密钥,所述装置包括:

获取模块,获取用户上传的明文数据,并且,从区块链中获取所述用户指定的第一加密数据;所述第一加密数据,是所述中间服务方使用自己的加密密钥对所述明文数据进行加密后提交给区块链的;

解密模块，通过所述安全执行环境，执行：使用所述中间服务方的解密密钥对所述第一加密数据进行解密，得到第一解密数据；

比对模块，将所述第一解密数据与所述明文数据进行比对，若一致，则输出证明结果，用于证明所述用户拥有所述明文数据的所有权。

8.如权利要求7所述的装置，所述装置还包括：

格式处理模块，在将所述第一解密数据与所述明文数据进行比对之前，若确定所述第一解密数据与所述明文数据的数据格式不同，则将所述第一解密数据与所述明文数据处理成具有相同数据格式。

9.一种基于安全执行环境的数据验证装置，应用于可信计算设备，所述装置中创建有安全执行环境，所述安全执行环境中存储有中间服务方的解密密钥与用户的解密密钥，所述装置包括：

获取模块，获取所述用户上传的第二加密数据，并且，从区块链中获取所述用户指定的第一加密数据；所述第二加密数据，是所述用户使用自己的加密密钥对所述明文数据进行加密后得到的；所述第一加密数据，是所述中间服务方使用自己的加密密钥对所述明文数据进行加密后提交给区块链的；

解密模块，通过所述安全执行环境，使用所述中间服务方的解密密钥对所述第一加密数据进行解密，得到第一解密数据，以及，使用所述用户的解密密钥对所述第二加密数据进行解密，得到第二解密数据；

比对模块，通过所述安全执行环境，将所述第一解密数据与所述第二解密数据进行比对，若一致，则输出证明结果，用于证明所述用户拥有所述明文数据的所有权。

10.如权利要求9所述的装置，所述装置还包括：

格式处理模块，通过所述安全执行环境，在将所述第一解密数据与所述第二解密数据进行比对之前，若确定所述第一解密数据与所述第二解密数据的数据格式不同，则将所述第一解密数据与所述第二解密数据处理成具有相同数据格式。

11.一种计算机设备，包括存储器、处理器及存储在存储器上并可在处理器上运行的计算机程序，其中，所述处理器执行所述程序时实现如权利要求1~6任一项所述的方法。

一种基于安全执行环境的数据验证方法及装置

技术领域

[0001] 本说明书实施例涉及信息技术领域，尤其涉及一种基于安全执行环境的数据验证方法及装置。

背景技术

[0002] 目前，很多用户有对自己拥有的数据进行区块链存证，又不希望自己的数据公开的需求。

[0003] 通常，用户并不会直接访问区块链网络的节点进行数据上传，而是通过一些中间服务方进行数据上传，中间服务方有对接有区块链节点的能力。具体而言，用户向中间服务方指定要存证的明文数据，中间服务方使用自己的加密密钥对获取的明文数据进行加密后，上传给对接的区块链节点，实现对加密数据的区块链存证。

[0004] 然而，上述这种方式只能证明用户是加密数据的拥有者，却很难证明用户是明文数据的所有者。

发明内容

[0005] 为了解决现有的基于区块链的数据验证方式很难证明用户是明文数据的所有者的问题，本说明书实施例提供一种基于安全执行环境的数据验证方法及装置，技术方案如下：

根据本说明书实施例的第1方面，提供一种基于安全执行环境的数据验证方法，应用于可信计算设备，所述可信计算设备中创建有安全执行环境，所述安全执行环境中存储有中间服务方的解密密钥，所述方法包括：

获取用户上传的明文数据，并且，从区块链中获取所述用户指定的第一加密数据；所述第一加密数据，是所述中间服务方使用自己的加密密钥对所述明文数据进行加密后提交给区块链的；

通过所述安全执行环境，执行：使用所述中间服务方的解密密钥对所述第一加密数据进行解密，得到第一解密数据；

将所述第一解密数据与所述明文数据进行比对，若一致，则输出证明结果，用于证明所述用户拥有所述明文数据的所有权。

[0006] 根据本说明书实施例的第2方面，提供另一种基于安全执行环境的数据验证方法，应用于可信计算设备，所述可信计算设备中创建有安全执行环境，所述安全执行环境中存储有中间服务方的解密密钥与用户的解密密钥，所述方法包括：

获取所述用户上传的第二加密数据，并且，从区块链中获取所述用户指定的第一加密数据；所述第二加密数据，是所述用户使用自己的加密密钥对所述明文数据进行加密后得到的；所述第一加密数据，是所述中间服务方使用自己的加密密钥对所述明文数据进行加密后提交给区块链的；

通过所述安全执行环境，执行以下步骤：

使用所述中间服务方的解密密钥对所述第一加密数据进行解密，得到第一解密数据，以及，使用所述用户的解密密钥对所述第二加密数据进行解密，得到第二解密数据；

将所述第一解密数据与所述第二解密数据进行比对，若一致，则输出证明结果，用于证明所述用户拥有所述明文数据的所有权。

[0007] 根据本说明书实施例的第3方面，提供一种基于安全执行环境的数据验证装置，应用于可信计算设备，所述装置中创建有安全执行环境，所述安全执行环境中存储有中间服务方的解密密钥，所述装置包括：

获取模块，获取用户上传的明文数据，并且，从区块链中获取所述用户指定的第一加密数据；所述第一加密数据，是所述中间服务方使用自己的加密密钥对所述明文数据进行加密后提交给区块链的；

解密模块，通过所述安全执行环境，执行：使用所述中间服务方的解密密钥对所述第一加密数据进行解密，得到第一解密数据；

比对模块，将所述第一解密数据与所述明文数据进行比对，若一致，则输出证明结果，用于证明所述用户拥有所述明文数据的所有权。

[0008] 根据本说明书实施例的第4方面，提供另一种基于安全执行环境的数据验证装置，应用于可信计算设备，所述装置中创建有安全执行环境，所述安全执行环境中存储有中间服务方的解密密钥与用户的解密密钥，所述装置包括：

获取模块，获取所述用户上传的第二加密数据，并且，从区块链中获取所述用户指定的第一加密数据；所述第二加密数据，是所述用户使用自己的加密密钥对所述明文数据进行加密后得到的；所述第一加密数据，是所述中间服务方使用自己的加密密钥对所述明文数据进行加密后提交给区块链的；

解密模块，通过所述安全执行环境，使用所述中间服务方的解密密钥对所述第一加密数据进行解密，得到第一解密数据，以及，使用所述用户的解密密钥对所述第二加密数据进行解密，得到第二解密数据；

比对模块，通过所述安全执行环境，将所述第一解密数据与所述第二解密数据进行比对，若一致，则输出证明结果，用于证明所述用户拥有所述明文数据的所有权。

[0009] 本说明书实施例所提供的技术方案，由可信计算设备进行数据验证，以证明用户拥有明文数据的所有权。具体地，需要在可信计算设备中创建安全执行环境，安全执行环境中存储的信息以及执行的计算过程不会泄露到安全执行环境之外，任何人(哪怕是可信计算设备的控制方)都无法访问安全执行环境以获取信息。可以预先在安全执行环境中写入中间服务方的解密密钥。当用户请求可信计算设备证明其拥有明文数据的所有权时，可信计算设备会从区块链中获取用户指定的第一加密数据，第一加密数据是中间服务方使用自己的加密密钥对所述明文数据进行加密后提交给区块链的。可信计算设备可以通过安全执行环境执行：使用所述中间服务方的解密密钥对所述第一加密数据进行解密，得到第一解密数据，从而确保中间服务方的解密密钥与解密过程(有可能通过解密过程破解加密算法)不会泄露。可信计算设备如果确定明文数据和第一解密数据一致，就可以证明所述用户拥有所述明文数据的所有权。

[0010] 通过本说明书实施例，可以在不泄露中间服务方的解密密钥的前提下，证明所述用户拥有所述明文数据的所有权。

[0011] 应当理解的是，以上的一般描述和后文的细节描述仅是示例性和解释性的，并不能限制本说明书实施例。

[0012] 此外，本说明书实施例中的任一实施例并不需要达到上述的全部效果。

附图说明

[0013] 为了更清楚地说明本说明书实施例或现有技术中的技术方案，下面将对实施例或现有技术描述中所需要使用的附图作简单地介绍，显而易见地，下面描述中的附图仅仅是本说明书实施例中记载的一些实施例，对于本领域普通技术人员来讲，还可以根据这些附图获得其他的附图。

[0014] 图1是一种基于安全执行环境的数据验证方法的流程示意图；

图2是本说明书实施例提供的另一种基于安全执行环境的数据验证方法的流程示意图；

图3是本说明书实施例提供的一种基于安全执行环境的数据验证装置的结构示意图；

图4是本说明书实施例提供的另一种基于安全执行环境的数据验证装置的结构示意图；

图5是用于配置本说明书实施例方法的一种设备的结构示意图。

具体实施方式

[0015] 在取证场景下，用户往往缺乏取证能力，因此，常常要借助中间服务方的取证能力进行取证，并进一步借助中间服务方的区块链对接能力对取证的数据进行存证。

[0016] 可见，在取证场景下，用户拥有的数据往往并不是用户直接生产的数据，而是用户请求中间服务方代为获取的数据。例如，用户自己创作了歌曲，发现某个音乐网站上架了盗版歌曲，用户请求中间服务器获取该音乐网站的网页截图，并将网页截图提交给区块链进行存证。中间服务方执行取证与存证操作后，会将取证得到的网页截图发送给用户进行存储。

[0017] 在这种对数据进行区块链存证的模式下，用户如果不想公开其要存证的数据，可以请求中间服务方在获取明文数据之后，执行存证操作之前，对明文数据进行加密。随后，中间服务方将加密数据提交给区块链进行存证。

[0018] 然而，现有的数据验证方式一般是由区块链网络来执行的。区块链网络只能证明用户是加密数据的所有者，而加密数据并不是使用用户的加密密钥加密的，而是使用中间服务方的加密密钥加密的，这就导致用户很难向第三方证明区块链中存证的加密数据实际上是自己持有的明文数据的密文。

[0019] 而在本说明书实施例中，既可以保护中间服务方的密钥隐私，又可以证明区块链中存证的加密数据实际上是用户持有的明文数据的密文。

[0020] 为了使本领域技术人员更好地理解本说明书实施例中的技术方案，下面将结合本说明书实施例中的附图，对本说明书实施例中的技术方案进行详细地描述，显然，所描述的实施例仅仅是本说明书的一部分实施例，而不是全部的实施例。基于本说明书中的实施例，本领域普通技术人员所获得的所有其他实施例，都应当属于保护的范围。

[0021] 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。

[0022] 图1是一种基于安全执行环境的数据验证方法的流程示意图，包括以下步骤：

S100：获取用户上传的明文数据，并且，从区块链中获取所述用户指定的第一加密数据。

[0023] 图1所示方法的执行主体是可信计算设备。所述可信计算设备中创建有安全执行环境，所述安全执行环境中存储有中间服务方的解密密钥。

[0024] 安全执行环境的属性为，可信计算设备没有权限获取安全执行环境中存储的信息以及安全执行环境中执行的计算过程。

[0025] 需要说明的是，本文所述的安全执行环境具体可以是硬件层面上的安全SE芯片，内置于可信计算设备中。

[0026] 此外，安全执行环境也可以是软件层面上的可信运行环境(Trusted Execution Environment，TEE)。TEE是与可信计算设备的操作系统并存的程序运行环境。

[0027] 用户需要请求可信计算设备验证数据时，一方面可以将待验证的明文数据上传给可信计算设备，另一方面可以向可信计算设备指定要比对的区块链数据即中间服务方之前向区块链提交的、使用中间服务方的加密密钥对明文数据进行加密得到的加密数据，为了描述的方便，称为第一加密数据。

[0028] S102：通过所述安全执行环境，执行：使用所述中间服务方的解密密钥对所述第一加密数据进行解密，得到第一解密数据。

[0029] 由于既不能将中间服务方的解密密钥泄露，也不能将使用中间服务方的解密密钥对第一加密数据进行解密的计算过程泄露，因此，需要在安全执行环境中使用中间服务方的解密密钥执行解密。

[0030] S104：将所述第一解密数据与所述明文数据进行比对，若一致，则输出证明结果，用于证明所述用户拥有所述明文数据的所有权。

[0031] 此外，有时，中间服务方在取证与存证阶段，发送给用户的数据的数据格式(如排列规则、编码规则)与用于生成第一解密数据的数据的数据格式不一致，但是，这两个数据格式不同的数据实际上是同一证据。

[0032] 为此，可信计算设备在将所述第一解密数据与所述明文数据进行比对之前，若确定所述第一解密数据与所述明文数据的数据格式不同，则将所述第一解密数据与所述明文数据处理成具有相同数据格式。这种将不同数据格式的数据处理成具有相同数据格式的方式一般被称为异构数据对接。

[0033] 另外，在本说明书实施例中，可信计算设备若所述第一解密数据与所述明文数据不一致，则拒绝输出所述证明结果，也可以进一步输出否定结果，用于表明所述用户不是所述明文数据的拥有者。

[0034] 此外，考虑到用户有时担心向可信计算设备上传明文数据的过程中，明文数据被他人截获。为此，本说明书实施例提供了另一种基于安全执行环境的数据验证方法。

[0035] 图2是本说明书实施例提供的另一种基于安全执行环境的数据验证方法的流程示意图，包括以下步骤：

S200：获取所述用户上传的第二加密数据，并且，从区块链中获取所述用户指定的第一加密数据。

[0036] S202：通过所述安全执行环境，使用所述中间服务方的解密密钥对所述第一加密

数据进行解密，得到第一解密数据，以及，使用所述用户的解密密钥对所述第二加密数据进行解密，得到第二解密数据。

[0037] S204：通过所述安全执行环境，将所述第一解密数据与所述第二解密数据进行比对，若一致，则输出证明结果，用于证明所述用户拥有所述明文数据的所有权。

[0038] 图2所述的方法是在图1所示的方法基础上进行改进的。此处仅对图2所示方法与图1所示方法的区别进行说明。

[0039] 在图2所示的方法中，所述安全执行环境中不仅存储有中间服务方的解密密钥，还存储有用户的解密密钥。如此，用户可以向可信计算设备上传第二加密数据即可。第二加密数据是所述用户使用自己的加密密钥对所述明文数据进行加密后得到的。

[0040] 相应的，可信计算设备还需要在安全执行环境中对第二加密数据进行解密，确保所述用户的解密密钥与对第二加密数据的解密过程不泄露。

[0041] 此外，可信计算设备还需要在安全执行环境中比对第一解密数据与第二解密数据，以确保第一解密数据与第二解密数据不泄露。

[0042] 在图2所示的方法中，也可以在将所述第一解密数据与所述第二解密数据进行比对之前，若确定所述第一解密数据与所述第二解密数据的数据格式不同，则通过所述安全执行环境，将所述第一解密数据与所述第二解密数据处理成具有相同数据格式。

[0043] 另外，若所述第一解密数据与所述第二解密数据不一致，则拒绝输出所述证明结果，也可以进一步输出失败结果，用于表明所述用户不是明文数据的所有者。

[0044] 图3是本说明书实施例提供的一种基于安全执行环境的数据验证装置的结构示意图，应用于可信计算设备，所述装置中创建有安全执行环境，所述安全执行环境中存储有中间服务方的解密密钥，所述装置包括：

获取模块301，获取用户上传的明文数据，并且，从区块链中获取所述用户指定的第一加密数据；所述第一加密数据，是所述中间服务方使用自己的加密密钥对所述明文数据进行加密后提交给区块链的；

解密模块302，通过所述安全执行环境，执行：使用所述中间服务方的解密密钥对所述第一加密数据进行解密，得到第一解密数据；

比对模块303，将所述第一解密数据与所述明文数据进行比对，若一致，则输出证明结果，用于证明所述用户拥有所述明文数据的所有权。

[0045] 所述装置还包括：

格式处理模块304，在将所述第一解密数据与所述明文数据进行比对之前，若确定所述第一解密数据与所述明文数据的数据格式不同，则将所述第一解密数据与所述明文数据处理成具有相同数据格式。

[0046] 图4是本说明书实施例提供的另一种基于安全执行环境的数据验证装置的结构示意图，应用于可信计算设备，所述装置中创建有安全执行环境，所述安全执行环境中存储有中间服务方的解密密钥与用户的解密密钥，所述装置包括：

获取模块401，获取所述用户上传的第二加密数据，并且，从区块链中获取所述用户指定的第一加密数据；所述第二加密数据，是所述用户使用自己的加密密钥对所述明文数据进行加密后得到的；所述第一加密数据，是所述中间服务方使用自己的加密密钥对所述明文数据进行加密后提交给区块链的；

解密模块402，通过所述安全执行环境，使用所述中间服务方的解密密钥对所述第一加密数据进行解密，得到第一解密数据，以及，使用所述用户的解密密钥对所述第二加密数据进行解密，得到第二解密数据；

比对模块403，通过所述安全执行环境，将所述第一解密数据与所述第二解密数据进行比对，若一致，则输出证明结果，用于证明所述用户拥有所述明文数据的所有权。

[0047] 所述装置还包括：

格式处理模块404，通过所述安全执行环境，在将所述第一解密数据与所述第二解密数据进行比对之前，若确定所述第一解密数据与所述第二解密数据的数据格式不同，则将所述第一解密数据与所述第二解密数据处理成具有相同数据格式。

[0048] 本说明书实施例还提供一种计算机设备，其至少包括存储器、处理器及存储在存储器上并可在处理器上运行的计算机程序，其中，处理器执行所述程序时实现本说明书中的客户端设备或服务端设备执行的方法。

[0049] 图5示出了本说明书实施例所提供的一种更为具体的计算设备硬件结构示意图，该设备可以包括：处理器1010、存储器1020、输入/输出接口1030、通信接口1040和总线1050。其中处理器1010、存储器1020、输入/输出接口1030和通信接口1040通过总线1050实现彼此之间在设备内部的通信连接。

[0050] 处理器1010可以采用通用的CPU(Central Processing Unit，中央处理器)、微处理器、应用专用集成电路(Application Specific Integrated Circuit，ASIC)、或者一个或多个集成电路等方式实现，用于执行相关程序，以实现本说明书实施例所提供的技术方案。

[0051] 存储器1020可以采用ROM(Read Only Memory，只读存储器)、RAM(Random Access Memory，随机存取存储器)、静态存储设备，动态存储设备等形式实现。存储器1020可以存储操作系统和其他应用程序，在通过软件或者固件来实现本说明书实施例所提供的技术方案时，相关的程序代码保存在存储器1020中，并由处理器1010来调用执行。

[0052] 输入/输出接口1030用于连接输入/输出模块，以实现信息输入及输出。输入输出/模块可以作为组件配置在设备中(图中未示出)，也可以外接于设备以提供相应功能。其中输入设备可以包括键盘、鼠标、触摸屏、麦克风、各类传感器等，输出设备可以包括显示器、扬声器、振动器、指示灯等。

[0053] 通信接口1040用于连接通信模块(图中未示出)，以实现本设备与其他设备的通信交互。其中通信模块可以通过有线方式(例如USB、网线等)实现通信，也可以通过无线方式(例如移动网络、WIFI、蓝牙等)实现通信。

[0054] 总线1050包括一通路，在设备的各个组件(例如处理器1010、存储器1020、输入/输出接口1030和通信接口1040)之间传输信息。

[0055] 需要说明的是，尽管上述设备仅示出了处理器1010、存储器1020、输入/输出接口1030、通信接口1040以及总线1050，但是在具体实施过程中，该设备还可以包括实现正常运行所必需的其他组件。此外，本领域的技术人员可以理解的是，上述设备中也可以仅包含实现本说明书实施例方案所必需的组件，而不必包含图中所示的全部组件。

[0056] 本说明书实施例还提供一种计算机可读存储介质，其上存储有计算机程序，该程序被处理器执行时实现本说明书中的客户端设备或服务端设备执行的方法。

[0057] 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)、数字多功能光盘(DVD)或其他光学存储、磁盒式磁带，磁带磁磁盘存储或其他磁性存储设备或任何其他非传输介质，可用于存储可以被计算设备访问的信息。按照本文中的界定，计算机可读介质不包括暂存电脑可读媒体(transitory media)，如调制的数据信号和载波。

[0058] 通过以上的实施方式的描述可知，本领域的技术人员可以清楚地了解到本说明书实施例可借助软件加必需的通用硬件平台的方式来实现。基于这样的理解，本说明书实施例的技术方案本质上或者说对现有技术做出贡献的部分可以以软件产品的形式体现出来，该计算机软件产品可以存储在存储介质中，如ROM/RAM、磁碟、光盘等，包括若干指令用以使得一台计算机设备(可以是个人计算机，服务设备，或者网络设备等)执行本说明书实施例各个实施例或者实施例的某些部分所述的方法。

[0059] 上述实施例阐明的系统、方法、模块或单元，具体可以由计算机芯片或实体实现，或者由具有某种功能的产品来实现。一种典型的实现设备为计算机，计算机的具体形式可以是个人计算机、膝上型计算机、蜂窝电话、相机电话、智能电话、个人数字助理、媒体播放器、导航设备、电子邮件收发设备、游戏控制台、平板计算机、可穿戴设备或者这些设备中的任意几种设备的组合。

[0060] 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，对于装置实施例而言，由于其基本相似于方法实施例，所以描述得比较简单，相关之处参见方法实施例的部分说明即可。以上所描述的装置实施例仅仅是示意性的，其中所述作为分离部件说明的模块可以是或者也可以不是物理上分开的，在实施本说明书实施例方案时可以把各模块的功能在同一个或多个软件和/或硬件中实现。也可以根据实际的需要选择其中的部分或者全部模块来实现本实施例方案的目的。本领域普通技术人员在不付出创造性劳动的情况下，即可以理解并实施。

[0061] 以上所述仅是本说明书实施例的具体实施方式，应当指出，对于本技术领域的普通技术人员来说，在不脱离本说明书实施例原理的前提下，还可以做出若干改进和润饰，这些改进和润饰也应视为本说明书实施例的保护范围。

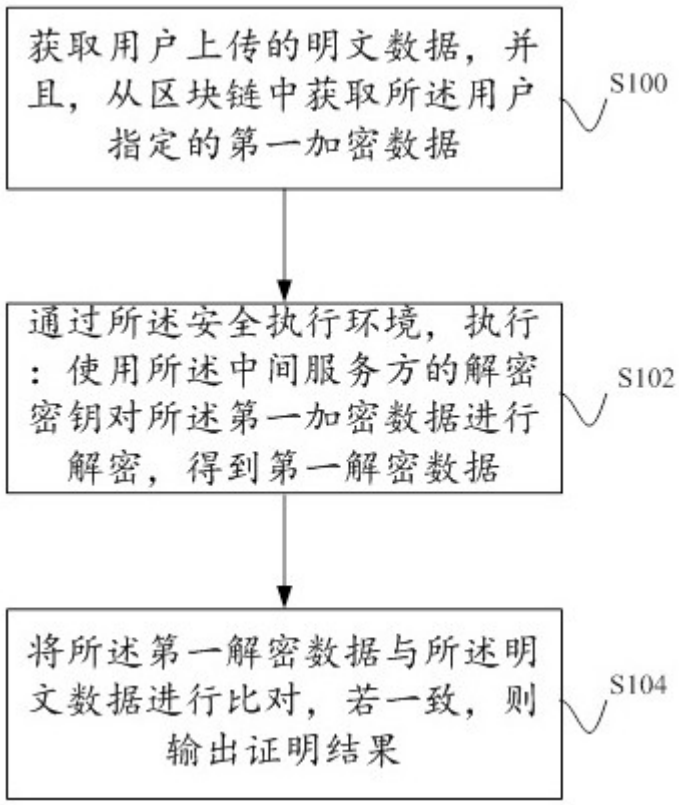

获取用户上传的明文数据，并且，从区块链中获取所述用户指定的第一加密数据
S100
通过所述安全执行环境，执行：使用所述中间服务方的解密密钥对所述第一加密数据进行解密，得到第一解密数据
S102
将所述第一解密数据与所述明文数据进行比对，若一致，则输出证明结果
S104

图1

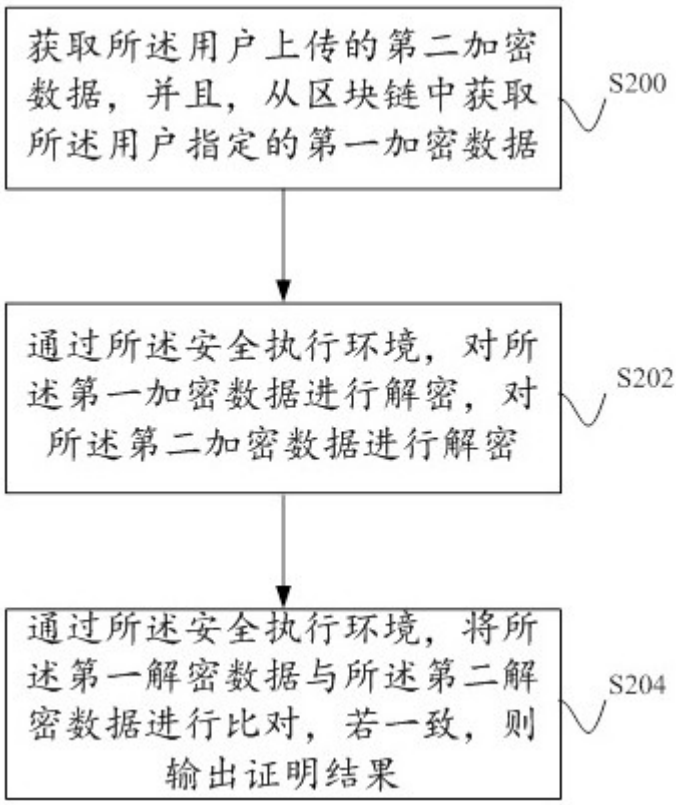

获取所述用户上传的第二加密数据，并且，从区块链中获取所述用户指定的第一加密数据
S200
通过所述安全执行环境，对所述第一加密数据进行解密，对所述第二加密数据进行解密
S202
通过所述安全执行环境，将所述第一解密数据与所述第二解密数据进行比对，若一致，则输出证明结果
S204

图2

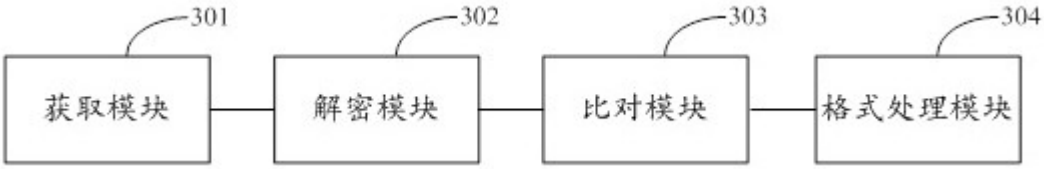

301
获取模块
302
解密模块
303
比对模块
304
格式处理模块

图3

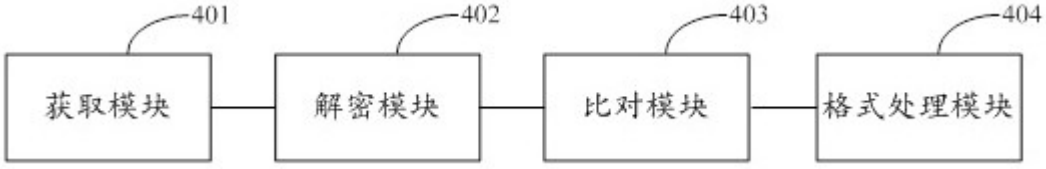

401
获取模块
402
解密模块
403
比对模块
404
格式处理模块

图4

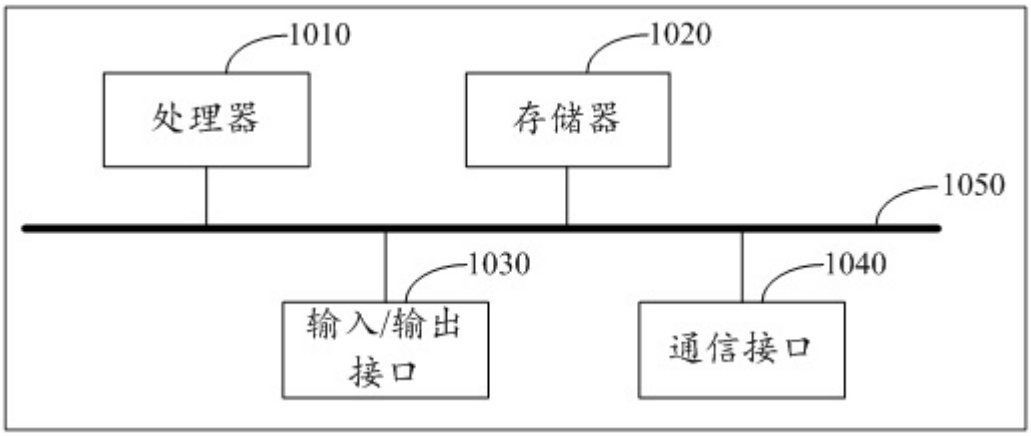


图5