

一种数据审计的方法及装置

技术领域

本申请涉及信息技术领域，尤其涉及一种数据审计的方法及装置。

5 背景技术

审计作为一种监督机制，在现代社会中有着重要的作用。目前，随着网络发展，审计的内容的种类也越来越多。例如，对用户保险公司的投保情况进行审计，对用户的贷款情况进行审计，对用户的资产进行审计等等。服务提供方可根据审计结果，确定是否对用户提供服务，或者提
10 供何种服务。

由于市场开放，同一种服务在市场中可能存在多个服务提供方。而用户可就同一种业务，在多个提供该业务的服务提供方处执行该业务，使得各服务提供方均执行了针对同一用户的同一种业务，也就是多头类型的业务。

15 下面以贷款业务为例进行说明，在现有技术中，当单一放贷方提供的贷款不能满足用户需求时，用户还可向多个放贷方提出贷款请求，以获得更多的贷款，也就是多头借贷。

而由于用户的还款能力是存在上限的，若对同一用户提供的贷款过多可能会导致坏账。这就使得提供贷款业务的任一放贷方，为了降低贷款业务的风险，可在执行业务前先确定该用户在其他放贷方处已经获得的贷款
20 总额，进而判断是否可提供贷款业务。

例如，假设用户 a 需要 100 万元贷款，由于其在银行 b 获得的贷款（假设为 30 万元），并不能满足用户 a 的需求，所以用户 a 还可以继续向银行 c 以及银行 d 发起贷款请求。则银行 c 以及银行 d 可先确定用户 a 在其他银行
25 获得的贷款总额，以确定是否贷款给该用户 a。

但是，由于用户在一个放贷方获得的贷款额属于该放贷方的隐私数据，

所以该放贷方通常不希望将用户获得的贷款额提供给第三方（如，其他用户或者其他放贷方）。通过现有的安全多方计算方法，虽然可以在保证各放贷方的隐私数据不泄露的情况下，确定用户在各放贷方的贷款总额，但是由于进行安全多方计算时采用的均为加密的数据，使得难以对各放贷方进行审计。

基于现有技术，本说明书提供一种新的数据审计的方法及装置。

发明内容

本说明书实施例提供一种数据审计的方法及装置，用于解决现有多头类型的业务中，由于用户在各计算节点处的业务数据等属于各计算节点自身的隐私数据，导致难以对多头类型的业务进行审计的问题。

本说明书实施例采用下述技术方案：

一种数据审计的方法，包括：

接收针对查询结果的审计请求；

15 针对每个计算节点，获取该计算节点为获得所述查询结果而生成加密数据时所采用的密钥，以及获取该计算节点存储在可信存储空间中的待审计数据；其中，该计算节点存储在所述可信存储空间中的待审计数据中包含：该计算节点接收到的其他计算节点发送的加密数据，和/或该计算节点生成的加密数据；

20 根据获取的各计算节点的密钥，对各待审计数据中的加密数据进行解密处理，得到各计算节点的原始数据；

根据得到的原始数据对各计算节点进行审计。

一种数据审计的方法，包括：

计算节点接收代理方发送的针对查询结果的审计请求；

25 将为获得所述查询结果而生成各加密数据时所采用的密钥返回所述代理方，以使所述代理方根据所述密钥，对从可信存储空间中获取的各待审计数据中由所述计算节点生成的加密数据进行解密处理，确定所述计算节

点的原始数据，并根据确定出的原始数据对所述计算节点进行审计。

一种数据审计装置，包括：

接收模块，接收针对查询结果的审计请求；

- 5 获取模块，针对每个计算节点，获取该计算节点为获得所述查询结果而生成加密数据时所采用的密钥，以及获取该计算节点存储在可信存储空间中的待审计数据；其中，该计算节点存储在所述可信存储空间中的待审计数据中包含：该计算节点接收到的其他计算节点发送的加密数据，和/或该计算节点生成的加密数据；

- 10 解密模块，根据获取的各计算节点的密钥，对各待审计数据中的加密数据进行解密处理，得到各计算节点的原始数据；

审计模块，根据得到的原始数据对各计算节点进行审计。

一种数据审计装置，包括：

接收模块，接收代理方发送的针对查询结果的审计请求；

- 15 发送模块，将为获得所述查询结果而生成各加密数据时所采用的密钥返回所述代理方，以使所述代理方根据所述密钥，对从可信存储空间中获取的各待审计数据中由所述数据审计装置生成的加密数据进行解密处理，确定所述数据审计装置的原始数据，并根据确定出的原始数据对所述数据审计装置进行审计。

- 20 一种代理方设备，包括：一个或多个处理器及存储器，存储器存储有程序，并且被配置成由一个或多个处理器执行以下步骤：

接收针对查询结果的审计请求；

- 25 针对每个计算节点，获取该计算节点为获得所述查询结果而生成加密数据时所采用的密钥，以及获取该计算节点存储在可信存储空间中的待审计数据；其中，该计算节点存储在所述可信存储空间中的待审计数据中包含：该计算节点接收到的其他计算节点发送的加密数据，和/或该计算节点生成的加密数据；

根据获取的各计算节点的密钥，对各待审计数据中的加密数据进行解

密处理，得到各计算节点的原始数据；

根据得到的原始数据对各计算节点进行审计。

一种计算节点，包括：一个或多个处理器及存储器，存储器存储有程序，并且被配置成由一个或多个处理器执行以下步骤：

5 计算节点接收代理方发送的针对查询结果的审计请求；

将为获得所述查询结果而生成各加密数据时所采用的密钥返回所述代理方，以使所述代理方根据所述密钥，对从可信存储空间中获取的各待审计数据中由所述计算节点生成的加密数据进行解密处理，确定所述计算节点的原始数据，并根据确定出的原始数据对所述计算节点进行审计。

10 本说明书实施例采用的上述至少一个技术方案能够达到以下有益效果：

通过本说明书提供的方法及装置，针对每个计算节点，该计算节点存储在可信存储空间中的待审计数据中包含该计算节点接收到的其他计算节点发送的加密数据，和/或该计算节点生成的加密数据。而当代理方接收到
15 针对查询结果的审计请求时，可针对每个计算节点，获取该计算节点为获得所述查询结果而生成加密数据时所采用的密钥，以及从可信存储空间中获取该计算节点存储的待审计数据。则代理方可根据获取的各计算节点的密钥，对从可信存储空间获取的各待审计数据中包含的加密数据进行解密，得到各计算节点的原始数据，并根据得到的原始数据对各计算节点进行审
20 计。由于用于存证的待审计数据是加密数据，所以避免了各计算节点的隐私数据的泄露。同时，存储在可信存储空间中又降低了待审计数据被篡改的可能性。因此，通过本说明书提供的方法及装置可对执行多头类型的业务的各计算节点进行审计，为多头类型的业务的展开提供了更好的基础。

25 附图说明

此处所说明的附图用来提供对本申请的进一步理解，构成本申请的一

部分，本申请的示意性实施例及其说明用于解释本申请，并不构成对本申请的不当限定。在附图中：

图 1 为放贷方发送加密数据以及存储待审计数据的示意图；

图 2 为本说明书实施例提供的一种数据审计的过程；

5 图 3 为本说明书实施例提供的一种数据审计装置的结构示意图；

图 4 为本说明书实施例提供的另一种数据审计装置的结构示意图；

图 5 为本说明书实施例提供的一种代理方设备的结构示意图；

图 6 为本说明书实施例提供的另一种计算节点的结构示意图。

10 具体实施方式

在本说明书提供的审计过程中，审计的目标是进行安全多方计算的各计算方。该审计过程可根据接收到的针对查询结果的审计请求开始进行，该查询结果可为根据安全多方计算确定出的。

15 现有安全多方计算方法中，参与计算的各计算方，可将原始数据进行加密后得到的各加密数据，发送给其他计算方。同理，针对每个计算方，该计算方还可接收其他计算方发送的加密数据，并在通过安全多方计算后，使任一计算方在无法还原出其他计算方的原始数据的情况下，得到各计算方的原始数据对应的综合数据。为了对安全多方计算中的各计算方进行审计，在进行安全多方计算的过程中，各计算方可确定待审计数据，并存储
20 在可信存储空间中。

通常，现有安全多方计算主要采用基于茫然传输（Oblivious Transfer，OT）的安全多方算法，以及采用基于秘密分享（Secret Sharing，SS）的安全多方算法。而由于上述两种算法的计算过程存在差异，确定的待审计数据也不完全相同，因此为方便描述，本说明书以采用基于茫然传输
25 （Oblivious Transfer，OT）的安全多方算法进行计算为例说明。

具体以多头借贷场景为例进行说明。各计算方可为各放贷方，针对每个放贷方，该放贷方确定出的原始数据可为用户在该放贷方处的贷款数额。

在本说明书中的多头借贷场景中，可由用户发起对自身的贷款总额的借贷查询请求，或者也可由放贷方发起针对用户的贷款总额的借贷查询请求。其中，当由用户发起借贷查询请求时，可由代理方接收该借贷查询请求，并发送给各放贷方。

- 5 针对每个放贷方，该放贷方可先根据该借贷查询请求确定原始数据（即，用户在该放贷方的贷款额），再根据预设的密钥对该原始数据进行加密，生成对应该原始数据的各加密数据，然后再将生成的各加密数据分别发送给其他放贷方。其中，该放贷方用于加密的密钥，可根据采用的安全多方算法确定（如，在基于 OT 的安全多方算法中，该密钥可根据 RSA 算
- 10 法确定）。并且，该放贷方根据原始数据生成的各加密数据可以是不同的加密数据，因此分别发送给其他放贷方的加密数据是不相同的。

- 之后，该放贷方在接收到其他放贷方发送的加密数据后，还可根据自身确定出的原始数据以及接收到的各加密数据，进行安全多方计算，得到该查询请求的查询结果（如，在多头借贷场景中可计算得到用户的贷款总
- 15 额），最后再将该查询结果返回给用户。

- 其中，为了方便后续可对该查询结果进行审计，该放贷方可将接收到的其他放贷方发送的加密数据，作为待审计数据存储于可信存储空间中。其中，该可信存储空间可以是区块链，或者可信数据库。该可信数据库可为该放贷方的数据库，或者第三方数据库，当可信存储空间为区块链时，
- 20 可以避免放贷方存储的加密数据被篡改。

- 由于存储在可信存储空间中的加密数据为其他放贷方生成的加密数据，因此为了方便确定加密数据是哪个放贷方生成的，每个放贷方在发送加密数据时还可将该放贷方自身的标识，以及该标识与该加密数据的对应关系发送给其他放贷方，如图 1 所示。

- 25 图 1 为各放贷方在接收到借贷查询请求后，发送确定出的加密数据的示意图。其中，可见代理方 A 向多个放贷方 B~D 发送借贷查询请求后，各放贷方分别确定出多个加密数据。如放贷方 B 根据借贷查询请求确定出原

始数据 X，并对 X 加密生成加密数据 b1 以及加密数据 b2，等等。并且，各放贷方在发送各加密数据时，可同时将自身的标识与加密数据的对应关系也发送给其他放贷方。例如，放贷方 B 发送的加密数据为 b1+B 表示加密数据 b1 与标识 B 对应，等等。于是，各放贷方可接收到其他放贷方发送的加密数据，并作为待审计数据存储在区块链中。例如，放贷方 B 将接收到的 c1+C 以及 d1+D 作为待审计数据存储在区块链中。则存储在区块链中的待审计数据中包含与加密数据对应的放贷方的标识。

更进一步地，针对每个放贷方，该放贷方可能接收到针对不同用户的借贷查询请求，因此为了区分根据不同借贷查询请求确定出的加密数据，该放贷方还可将借贷查询请求的流水号与确定出的各加密数据一同发送给其他放贷方。

继续沿用上例，假设代理方 A 确定出该借贷查询请求的流水号为 001，则以放贷方 B 为例，该放贷方 B 发送给放贷方 C 的加密数据可为：b1+B+001，以表示加密数据 b1 是由放贷方 B 根据流水号 001 的借贷查询请求生成的。于是，当代理方确定出借贷查询请求的查询结果时，还可将该流水号作为查询结果的流水号，以表示该查询结果是根据哪一个查询请求的获得的。

另外，当该审计请求为用户通过代理方发起的，各放贷方还可将待审计数据在可信存储空间中的存储地址返回代理方，以使代理方建立该借贷查询请求（或查询结果）的流水号与各存储地址的对应关系并存储，以便后续进行审计时可根据各存储地址获取各待审计数据。

需要说明的是，除了上述基于 OT 的安全多方算法以外，还可采用基于 SS 的安全多方算法。而在基于 SS 算法的安全多方算法的计算过程中，各放贷方除了可将接收到的其他放贷方发送的加密数据作为待审计数据以外，还可以将自身生成的加密数据作为待审计数据，并将待审计数据存储于可信存储空间中，则在图 1 所示的存储过程中，各放贷方可将自身生成的加密数据以及接收到的加密数据，作为待审计数据存储于区块链中。

在采用 SS 算法时, 针对每个放贷方, 该放贷方对原始数据进行加密的流程可为: 首先, 接收查询请求, 其次, 将查询请求对应的原始数据进行加密, 得到若干加密数据, 之后, 从所述若干加密数据中确定部分加密数据, 作为待分发加密数据, 并将每个待分发加密数据分别发送给其他放贷方, 然后, 对所述若干加密数据中未发送的加密数据的部分或全部, 以及接收到的其他放贷方发送的加密数据进行处理, 最后, 将得到的处理结果发送给代理方, 以使所述代理方根据该放贷方发送的处理结果以及其他放贷方发送的处理结果进行数据统计, 确定查询结果。

另外, 在各放贷方对原始数据进行加密后, 对于任意一方来说, 只有获取到不小于门限值 k 个数量的加密数据时, 才能还原出该原始数据, 而获取到小于门限值 k 个数量的加密数据时, 将无法还原出该原始数据。例如, 假设放贷方采用多项式形式的 SS 算法, 该多项式形式如下:

$$F(X) = (A_0 + A_1X + A_2X^2 + \dots + A_{k-1}X^{k-1}) \bmod q$$

其中, 该多项式中的 A_0 表示该原始数据, 即需要进行加密的数据, $A_1 \sim A_{k-1}$ 则是该公式的系数, 这些系数可以根据实际需求来进行确定。 q 表示除数, 该除数同样可以根据实际需求来进行选定, k 即为上述提到的门限值。在该多项式中, 当 X 取不同的值时, 即可求出不同的 $F(X)$, 而不同的 $F(X)$ 即代表了不同的加密数据。

在放贷方确定待分发的加密数据时, 该放贷方可以从确定出的若干加密数据选取小于 k 个数量的加密数据作为待分发加密数据, 并将各待分发加密数据分别发送给其他的放贷方。例如, 该放贷方可以通过确定出的公式, 依次确定出 $F(1) \sim F(11)$, $F(1) \sim F(11)$ 即是依次发送给其他放贷方 1~11 的 11 个待分发加密数据。

进一步地, 针对每个放贷方, 该放贷方在向各其他放贷方发送待分发加密数据的过程中, 也将接收其他放贷方发送的根据查询请求确定出的加密数据。这样, 该放贷方可以将自身生成的若干加密数据中未发送的加密

数据的部分或全部，以及接收到的其他放贷方发送的加密数据进行处理，并得到相应的处理结果。

其中，该放贷方在对加密数据进行处理时，可以采用求和算法，将自身生成的若干加密数据中未发送的加密数据的部分或全部，以及接收到的
5 其他放贷方发送的加密数据进行加和，并将和值发送给代理方。

最后，代理方可接收各放贷方放的处理结果，并通过 SS 算法中的拉格朗日差值公式，确定出用户在各放贷方的贷款总额，作为查询结果。其中，由于各放贷方是将通过统计处理得到的和值发送给代理方的，这样，代理方是无法通过得到的各和值，分别确定出各放贷方存储的该查询计请求对
10 应的原始数据，而只是能够通过获取到的各和值进行数据统计。

基于上述的安全多方计算的过程，各计算方将待审计数据存储于可信存储空间中，使得后续可对各计算方进行如图 2 所示审计过程。

为使本说明书的目的、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申请技术方案进行清楚、完整地描述。显然，所描述的实施例仅是本申请一部分实施例，而不是全部的实施例。基
15 于说明书中的实施例，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，都属于本申请保护的范围。

以下结合附图，详细说明本申请各实施例提供的技术方案。

图 2 为说明书实施例提供的一种数据审计的过程，具体可包括以下步
20 骤：

S100: 接收针对查询结果的审计请求。

在本说明书一个或多个实施例中，该数据审计过程可应用于多头类型的业务场景中，对多个服务提供方进行审计。例如，假设用户 a 申请在保险公司 e 处上保险，则保险公司 e 可向其他保险公司发送查询请求，以通过
25 安全多方计算确定用户 a 在各保险公司的投保总额。则当用户 a 对该保险公司 e 得到的投保总额存在疑义时，可通过代理方发起针对该查询结果的审计请求，从而对进行安全多方计算的数据进行审计。当然，若该保险公司 e

对该投保总额存在疑义时，也可由该保险公司额 e 发起针对该查询结果的审计请求。在本说明书中并不限定由哪一方发起该审计请求，并且也不限定该多头类型的业务具体为何种业务。

为了方便描述，后续以代理方根据用户发起的审计请求，向各放贷方
5 发送审计请求，以多头借贷为本说明书提供的数据审计过程的业务场景进行说明。该查询请求可为借贷查询请求，计算节点为进行安全多方计算的各参与方，具体可为提供借贷服务的放贷方。代理方为接收审计请求，并执行审计过程的执行主体。具体该代理方可以是一个软件服务端，其可以集成在与各放贷方无利害关系的第三方的设备上，或者集成在某个放贷方
10 设备上，本说明书对此不做限定。

另外，由于本说明书中的审计请求是针对查询结果的，因此在代理方接收到审计请求之前，各放贷方还应该接收到查询请求，并根据该查询请求进行过安全多方计算，并确定出该查询结果。具体可参考前述对于安全多方计算的描述。

15 S102: 针对每个计算节点，获取该计算节点为获得所述查询结果而生成加密数据时所采用的密钥，以及获取该计算节点存储在可信存储空间中的待审计数据；其中，该计算节点存储在所述可信存储空间中的待审计数据中包含：该计算节点接收到的其他计算节点发送的加密数据，和/或该计算节点生成的加密数据。

20 在本说明书实施例中，如在步骤 S100 所述的各放贷方（即各计算节点）在根据借贷查询请求执行查询业务的过程中，已经将待审计数据存储在可信存储空间中作为存证。因此，该代理方可针对每个放贷方，从该放贷方处获取该放贷方为获得该查询结果而生成加密数据时所采用的密钥，以及从可信存储空间中获取该放贷方存储的待审计数据，以便继执行后续步骤。

25 具体的，在本说明书中该审计请求中可携带有该查询结果的流水号。其中，该查询结果的流水号，具体可以是获取该查询结果而发起的借贷查询请求的流水号，则若代理方存储有流水号与存储地址的对应关系，则

可由代理方根据该流水号确定各放贷方存储在可信存储空间中的待审计数据的存储地址，进而从可信存储空间中获取各待审计数据。而若根据借贷查询请求执行业务的过程是由各放贷方执行的，没有经过代理方，代理方未存储流水号与存储地址的对应关系，则代理方可将该审计请求发送给各放贷方，以使各放贷方根据该审计请求，确定与该查询结果的流水号对应的待审计数据在可信存储空间中的存储地址，并根据确定出的存储地址从可信存储空间中获取待审计数据，以返回该代理方。或者，各放贷方在接收到该审计请求时，也可将根据该查询结果的流水号确定出的待审计数据在可信存储空间中的存储地址返回该代理方。而代理方可根据各放贷方返回的存储地址，从可信存储空间中获取各待审计数据。

另外，由于密钥是各放贷方的隐私，所以需要由代理方将审计请求发送给各放贷方，并由各放贷方将为获得该查询结果而生成加密数据时所采用的密钥提供给代理方。

需要说明的是，针对每个放贷方，若在步骤 S100 中，该放贷方是基于 OT 进行的安全多方计算，该放贷方是将接收到的其他放贷方发送的加密数据，作为待审计数据存储在可信存储空间中的，则代理方获取的该放贷方存储的待审计数据中，没有该放贷方生成的加密数据。而若在步骤 S100 中，该放贷方是基于 SS 进行的安全多方计算，该放贷方可将自身根据借贷查询请求生成的加密数据以及接收到的其他放贷方发送的加密数据，作为待审计数据存储在可信存储空间中，则代理方获取的该放贷方存储的待审计数据中包括该放贷方生成的加密数据。

S104: 根据获取的各计算节点的密钥，对各待审计数据中的加密数据进行解密处理，得到各计算节点的原始数据。

在本说明书实施例中，待审计数据中包含的是各放贷方对原始数据加密得到的加密数据，因此根据获取的各密钥对待审计数据进行解密处理，则可得到各放贷方的原始数据。

具体的，针对每个放贷方存储在可信存储空间中的待审计数据，该待

审计数据中包含不同放贷方生成的加密数据，以及与各加密数据分别对应的放贷方的标识。其中，与加密数据对应的放贷方的标识为生成该加密数据的放贷方的标识。于是，当代理方获取各放贷方存储在可信存储空间中的各待审计数据后，可以根据与加密数据对应的标识，确定每个放贷方生

5 成的各加密数据。

并且，由于针对每个放贷方，该放贷方在对原始数据加密后，得到的各加密数据不同，所以代理方可在获取该放贷方的所有加密数据之后，再根据该放贷方的密钥对该放贷方生成的各加密数据进行解密，得到该放贷方的原始数据。当然，根据采用的安全多方算法的不同，该代理方也可以

10 在获取超过门限值数量的该放贷方的加密数据后，根据该放贷方的密钥对已获取的放贷方生成的各加密数据进行解密，得到该放贷方的原始数据，本说明书对此不做限定。

S106: 根据得到的原始数据对各计算节点进行审计。

在本说明书中，当代理方确定各放贷方的原始数据后，便可根据得到

15 的各放贷方的原始数据，对各放贷方进行审计。例如，代理方可以对各放贷方原始数据是否真实进行审计，从而确定各放贷方在根据借贷查询请求进行安全多方计算时是否对数据进行篡改。当然，在本说明书中，并不限定具体采用何种方式对各放贷方进行审计。

另外，在本说明书中，针对每个放贷方，若该放贷方在根据查询请求

20 执行查询业务时，对进行安全多方计算的所需的原始数据进行篡改（如，对确定出用户在该放贷方的贷款数额进行篡改）。则用于存证的待审计数据，是该放贷方对篡改后的数据进行加密得到。因此使得代理方无法通过步骤 S104 得到的原始数据，判断该放贷方是否对原始数据进行篡改。

需要说明的是，本说明书中所述的原始数据，为进行安全多方计算时

25 各放贷方的加密对象，而非放贷方存储的真实数据。

例如，某银行确定出原始数据为“10 万元”，假设该银行在进行安全多方计算时将使用的原始数据篡改为“100 万元”，并对篡改后的原始数据进行

加密，将得到各加密数据发送给安全多方计算的其他参与方。则通过步骤 S104 代理方解密得到的该银行原始数据为“100 万元”。但是，该银行存储的真实数据仍为“10 万元”。

于是，在本申请步骤 S106 中，代理方还可获取各放贷方在执行放贷业务时的电子单据，并根据该电子单据中记录的贷款额，对该放贷方根据查询请求确定出的原始数据进行审计。当然，代理方也可采用人工审计的方法，对各放贷方进行审计。

例如，继续沿用上例，进一步假设用户在向银行贷款时，银行根据放贷业务生成用户贷款额对应的电子单据为：“30 万元”。则代理方还可获取该银行存储的电子单据，并根据该电子单据以及确定出的该银行的原始数据，对该银行进行审计。

基于图 2 所示的数据审计过程，计算节点存储的待审计数据中包含的是其他计算节点生成的加密数据和/或自身生成的加密数据，一方面减少了计算节点篡改待审计数据的动机，另一方面若该计算节点对自身存证的加密数据篡改，则在后续审计时可导致代理方无法解密得到原始数据，可直接确定存在有问题的计算节点。另外，由于密钥作为隐私数据是由各计算节点存储的，所以即使第三方获取了某个计算节点生成的加密数据，也无法还原出原始数据。可见通过本说明书提供的方法，在进行安全多方计算的同时对加密数据进行存证，实现了对各计算节点进行审计的可能，为多头类型的业务的展开提供了更好的基础。

另外，由于在步骤 S102 中代理方可获取各放贷方根据审计请求提供的密钥，所以为了防止放贷方的隐私数据泄露给他人，该代理方在向各放贷方发送审计请求之前，还可判断该用户是否有查看隐私数据的权限。同理，各放贷方在接收到审计请求时，也可判断该代理方和/或发起审计的用户是否有获取隐私数据的权限。

具体的，该代理方可先获取该用户的身份信息，以根据该身份信息判断该用户是否有发起审计的权限。若是，则发送审计请求，若否则不发送。

或者，由该代理方将用户的身份信息携带在审计请求中发送给各放贷方，并由各放贷方确定该用户有审计权限时，再返回密钥。本说明书的一个实施例中，由于在审计时，发起审计的一方可查看原始数据，因此可在确定用户具有查看或者获取隐私数据的权限时，确定用户具有发起审计的权限。

5 例如，该代理方可判断该用户是否是针对自己的借贷情况发起审计请求，若是则确定该用户具有发起审计的权限。或者，当放贷方接收审计请求时，判断代理方是否获得了用户的授权等等。当然也可采用其他方法，本说明书不限定如何判断发起审计的用户和/或代理方是否具有发起审计的权限。

10 进一步地，在本说明书中上述实施例中是在多头借贷场景中应用的数据审计过程为例进行说明的。当然，该数据审计方法也可应用在其他业务场景中。

 例如，在对用户上保情况进行审计的场景中，该查询请求可为保险查询请求，确定出的查询结果可为用户在各保险服务提供方的总投保额，各
15 计算节点可为保险服务提供方的设备。在对用户的资产情况进行审计的场景中，该查询请求可为资产查询请求，确定出的查询结果可为用户的总资产，各计算节点可为银行、保险公司、房产交易中心等等机构或者企业的设备。本说明书对于该数据审计方法应用在何种业务场景中不做限定。

 需要说明的是，本说明书实施例所提供方法的各步骤的执行主体均可
20 以是同一设备，或者，该方法也由不同设备作为执行主体。比如，步骤 S100 和步骤 S102 的执行主体可以为设备 1，步骤 S102 的执行主体可以为设备 2；或者，步骤 S100 的执行主体可以为设备 1，步骤 S102 和步骤 S104 的执行主体可以为设备 2；等等。上述对本说明书特定实施例进行了描述。其它实施例在所附权利要求书的范围内。在一些情况下，在权利要求书中记载的
25 动作或步骤可以按照不同于实施例中的顺序来执行并且仍然可以实现期望的结果。另外，在附图中描绘的过程不一定要求示出的特定顺序或者连续顺序才能实现期望的结果。在某些实施方式中，多任务处理和并行处理也

是可以的或者可能是有利的。

基于图 2 所示的数据审计方法，本说明书实施例还提供一种数据审计装置，如图 3 所示。

图 3 为本说明书实施例提供的一种数据审计装置的结构示意图，包括：

5 接收模块 300，接收针对查询结果的审计请求；

获取模块 302，针对每个计算节点，获取该计算节点为获得所述查询结果而生成加密数据时所采用的密钥，以及获取该计算节点存储在可信存储空间中的待审计数据；其中，该计算节点存储在所述可信存储空间中的待审计数据中包含：该计算节点接收到的其他计算节点发送的加密数据，和/

10 或该计算节点生成的加密数据；

解密模块 304，根据获取的各计算节点的密钥，对各待审计数据中的加密数据进行解密处理，得到各计算节点的原始数据；

审计模块 306，根据得到的原始数据对各计算节点进行审计。

针对每个计算节点，该计算节点生成的加密数据为：对为获得所述查

15 询结果而确定出的原始数据进行加密后得到的，所述原始数据为：该计算节点接收到请求获得所述查询结果的查询请求后，根据所述查询请求确定的，该计算节点生成的加密数据由该计算节点发送给其他计算节点进行安全多方计算。

所述装置还包括：

20 存证模块 308，接收该计算节点返回的与所述查询结果的流水号对应的存储地址，建立所述存储地址与所述流水号的对应关系并存储。

所述审计请求中携带有所述查询结果的流水号，获取模块 302，根据已存储的各流水号与各存储地址之间的对应关系，确定与所述审计请求中携带的流水号对应的存储地址，并根据确定出的存储地址从所述可信存储空间中获取所述待审计数据。

25

所述待审计数据中还包含与加密数据对应的计算节点的标识，其中，与加密数据对应的计算节点的标识为生成该加密数据的计算节点的标识，

获取模块 302, 针对每个计算节点, 根据该计算节点的标识, 从获取到的各待审计数据中, 确定由该计算节点生成的各加密数据, 根据该计算节点的密钥, 对确定出的各加密数据进行解密处理。

所述可信存储空间至少包括: 区块链。

5 另外本说明书实施例还提供另一种数据审计装置, 如图 4 所示。

图 4 为本说明书实施例提供的一种数据审计装置的结构示意图, 包括:

接收模块 400, 接收代理方发送的针对查询结果的审计请求;

发送模块 402, 将为获得所述查询结果而生成各加密数据时所采用的密钥返回所述代理方, 以使所述代理方根据所述密钥, 对从可信存储空间中
10 获取的各待审计数据中由所述数据审计装置生成的加密数据进行解密处理, 确定所述数据审计装置的原始数据, 并根据确定出的原始数据对所述数据审计装置进行审计。

所述装置还包括:

存证模块 404, 接收请求获得所述查询结果的查询请求, 根据所述查询
15 请求, 确定原始数据, 根据所述密钥对所述原始数据进行加密, 得到各加密数据。

存证模块 404, 将各加密数据分别发送给其他计算节点, 以使其他计算节点将接收到的加密数据, 和/或所述其他计算节点生成的加密数据, 作为待审计数据存储于可信存储空间中, 并将所述待审计数据的存储地址返回
20 所述代理方。

其中, 所述数据审计装置可为根据所述查询请求进行安全多方计算的参与方。

基于图 2 所述的数据审计方法, 本说明书对应提供一种代理方设备, 如图 5 所示, 包括: 一个或多个处理器及存储器, 存储器存储有程序, 并
25 且被配置成由一个或多个处理器执行以下步骤:

接收针对查询结果的审计请求;

针对每个计算节点, 获取该计算节点为获得所述查询结果而生成加密

数据时所采用的密钥，以及获取该计算节点存储在可信存储空间中的待审计数据；其中，该计算节点存储在所述可信存储空间中的待审计数据中包含：该计算节点接收到的其他计算节点发送的加密数据，和/或该计算节点生成的加密数据；

- 5 根据获取的各计算节点的密钥，对各待审计数据中的加密数据进行解密处理，得到各计算节点的原始数据；

根据得到的原始数据对各计算节点进行审计。

另外，本说明书对应提供一种计算节点，如图 6 所示，包括：一个或多个处理器及存储器，存储器存储有程序，并且被配置成由一个或多个处

- 10 理器执行以下步骤：

计算节点接收代理方发送的针对查询结果的审计请求；

将为获得所述查询结果而生成各加密数据时所采用的密钥返回所述代理方，以使所述代理方根据所述密钥，对从可信存储空间中获取的各待审计数据中由所述计算节点生成的加密数据进行解密处理，确定所述计算节点

- 15 的原始数据，并根据确定出的原始数据对所述计算节点进行审计。

需要说明的是，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，对于本申请实施例提供的移动终端以及服务器而言，由于其基本相似于方法实施例，所以描述的比较简单，相关

- 20 之处参见方法实施例的部分说明即可。

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

- 25 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、RHDH(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。

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。

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。

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。

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。

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。

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

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。

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5 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。

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。

10 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。

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、20 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。

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25 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。

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。

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。

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，对于系统实施例而言，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。

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。

权利要求书

1、一种数据审计的方法，包括：

接收针对查询结果的审计请求；

5 针对每个计算节点，获取该计算节点为获得所述查询结果而生成加密数据时所采用的密钥，以及获取该计算节点存储在可信存储空间中的待审计数据；其中，该计算节点存储在所述可信存储空间中的待审计数据中包含：该计算节点接收到的其他计算节点发送的加密数据，和/或该计算节点生成的加密数据；

10 根据获取的各计算节点的密钥，对各待审计数据中的加密数据进行解密处理，得到各计算节点的原始数据；

根据得到的原始数据对各计算节点进行审计。

2、如权利要求 1 所述的方法，针对每个计算节点，该计算节点生成的加密数据为：对为获得所述查询结果而确定出的原始数据进行加密后得到的；

15 所述原始数据为：该计算节点接收到请求获得所述查询结果的查询请求后，根据所述查询请求确定的；

该计算节点生成的加密数据由该计算节点发送给其他计算节点进行安全多方计算。

20 3、如权利要求 1 所述的方法，获取该计算节点存储在所述可信存储空间中的待审计数据之前，所述方法还包括：

接收该计算节点返回的与所述查询结果的流水号对应的存储地址；

建立所述存储地址与所述流水号的对应关系并存储。

4、如权利要求 3 所述的方法，所述审计请求中携带有所述查询结果的流水号；

25 获取该计算节点存储在所述可信存储空间中的待审计数据，具体包括：根据已存储的各流水号与各存储地址之间的对应关系，确定与所述审

计请求中携带的流水号对应的存储地址，并根据确定出的存储地址从所述可信存储空间中获取所述待审计数据。

5、如权利要求 1 所述的方法，所述待审计数据中还包含与加密数据对应的计算节点的标识，其中，与加密数据对应的计算节点的标识为生成该

5 加密数据的计算节点的标识；

根据获取的各计算节点的密钥，对各待审计数据中的加密数据进行解密处理，具体包括：

针对每个计算节点，根据该计算节点的标识，从获取到的各待审计数据中，确定由该计算节点生成的各加密数据；

10 根据该计算节点的密钥，对确定出的各加密数据进行解密处理。

6、如权利要求 1 所述的方法，所述可信存储空间至少包括：区块链。

7、一种数据审计的方法，包括：

计算节点接收代理方发送的针对查询结果的审计请求；

15 代理方，以使所述代理方根据所述密钥，对从可信存储空间中获取的各待审计数据中由所述计算节点生成的加密数据进行解密处理，确定所述计算节点的原始数据，并根据确定出的原始数据对所述计算节点进行审计。

8、如权利要求 7 所述的方法，生成各加密数据，具体包括：

接收请求获得所述查询结果的查询请求；

20 根据所述查询请求，确定原始数据；

根据所述密钥对所述原始数据进行加密，得到各加密数据。

9、如权利要求 8 所述的方法，得到各加密数据之后，所述方法还包括：

25 将各加密数据分别发送给其他计算节点，以使其他计算节点将接收到的加密数据，和/或所述其他计算节点生成的加密数据，作为待审计数据存储于可信存储空间中，并将所述待审计数据的存储地址返回所述代理方。

10、一种数据审计装置，包括：

接收模块，接收针对查询结果的审计请求；

获取模块，针对每个计算节点，获取该计算节点为获得所述查询结果而生成加密数据时所采用的密钥，以及获取该计算节点存储在可信存储空间中的待审计数据；其中，该计算节点存储在所述可信存储空间中的待审计数据中包含：该计算节点接收到的其他计算节点发送的加密数据，和/或

5 该计算节点生成的加密数据；

解密模块，根据获取的各计算节点的密钥，对各待审计数据中的加密数据进行解密处理，得到各计算节点的原始数据；

审计模块，根据得到的原始数据对各计算节点进行审计。

11、一种数据审计装置，包括：

10 接收模块，接收代理方发送的针对查询结果的审计请求；

发送模块，将为获得所述查询结果而生成各加密数据时所采用的密钥返回所述代理方，以使所述代理方根据所述密钥，对从可信存储空间中获取的各待审计数据中由所述数据审计装置生成的加密数据进行解密处理，确定所述数据审计装置的原始数据，并根据确定出的原始数据对所述数据

15 审计装置进行审计。

12、一种代理方设备，包括：一个或多个处理器及存储器，存储器存储有程序，并且被配置成由一个或多个处理器执行以下步骤：

接收针对查询结果的审计请求；

针对每个计算节点，获取该计算节点为获得所述查询结果而生成加密数据时所采用的密钥，以及获取该计算节点存储在可信存储空间中的待审计数据；其中，该计算节点存储在所述可信存储空间中的待审计数据中包含：该计算节点接收到的其他计算节点发送的加密数据，和/或该计算节点生成的加密数据；

20 根据获取的各计算节点的密钥，对各待审计数据中的加密数据进行解密处理，得到各计算节点的原始数据；

根据得到的原始数据对各计算节点进行审计。

13、一种计算节点，包括：一个或多个处理器及存储器，存储器存储

有程序，并且被配置成由一个或多个处理器执行以下步骤：

计算节点接收代理方发送的针对查询结果的审计请求；

将为获得所述查询结果而生成各加密数据时所采用的密钥返回所述代理方，以使所述代理方根据所述密钥，对从可信存储空间中获取的各待审

- 5 计数据中由所述计算节点生成的加密数据进行解密处理，确定所述计算节点的原始数据，并根据确定出的原始数据对所述计算节点进行审计。