

业务处理的方法和装置

技术领域

[01]本说明书一个或多个实施例涉及计算机领域，尤其涉及业务处理的方法和装置。

背景技术

- 5 [02]当前，在进行业务处理时，通常需要多方参与，例如，一项业务可以涉及一个业务发起方以及一个或多个业务相关方。随着区块链技术的发展，在业务处理的过程中利用了区块链技术存储多方交互的业务数据。

[03]业务数据记录到区块链网络上之后，可以防止个别区块链成员抵赖或者篡改数据，其一个基础就是大家参与记录，每个区块链成员都可以拿到区块链网络上的所有数据。

- 10 当业务数据中包含敏感数据时（比如用户隐私数据），如果将敏感数据写入区块链，那么这些敏感数据就会泄露给所有区块链成员。

[04]因此，希望能有改进的方案，能够在利用区块链网络存储业务数据时，不会导致敏感数据的泄露。

发明内容

- 15 [05]本说明书一个或多个实施例描述了一种业务处理的方法和装置，能够在利用区块链网络存储业务数据时，不会导致敏感数据的泄露。

[06]第一方面，提供了一种业务处理的方法，方法由业务发起方执行，并包括：

[07]针对目标业务向各业务相关方发送业务确认请求，所述业务确认请求中包括业务数据；

- 20 [08]从每个所述业务相关方接收业务确认应答，所述业务确认应答中包括第一数据块和第一签名数据；其中，所述第一数据块包括由业务相关方采用预设编码方式对所述业务数据进行编码而生成的第一编码数据、第一确认结果和所述业务相关方的标识；所述第一签名数据为利用所述业务相关方的私钥对所述第一数据块进行签名计算得到的；

- 25 [09]采用所述预设编码方式对所述业务数据进行编码，从而生成第二编码数据；以及生成第二确认结果；

- [10]利用所述业务发起方的私钥对包括第二编码数据、第二确认结果和所述业务发起方的标识的第二数据块进行签名，得到第二签名数据；
- [11]确定每个所述第一确认结果和所述第二确认结果均为确认通过时，通过区块链网络存储每个所述业务相关方的所述第一数据块和所述第一签名数据，以及所述业务发起方的
- 5 的所述第二数据块和所述第二签名数据。
- [12]在一种可能的实施方式中，所述方法还包括：
- [13]确定每个所述第一确认结果和所述第二确认结果均为确认通过时，通过所述区块链网络处理所述目标业务。
- [14]进一步地，所述通过所述区块链网络处理所述目标业务，包括：
- 10 [15]通过所述区块链网络记录所述目标业务的处理结果信息；以及，
- [16]通过所述区块链网络向每个所述业务相关方发送所述目标业务的处理结果信息，以使每个所述业务相关方处理所述目标业务。
- [17]第二方面，提供了一种业务处理的方法，方法由业务相关方执行，并包括：
- [18]从业务发起方接收针对目标业务的业务确认请求，所述业务确认请求中包括业务数
- 15 据；
- [19]根据所述业务数据，生成第一确认结果；
- [20]采用预设编码方式对所述业务数据进行编码，生成第一编码数据；
- [21]利用所述业务相关方的私钥对包含所述第一确认结果和所述第一编码数据的第一数据块进行签名，得到第一签名数据；
- 20 [22]向所述业务发起方发送业务确认应答，所述业务确认应答中包括所述第一数据块和所述第一签名数据；以使所述业务发起方确定每个所述业务相关方的确认结果均为确认通过时，通过区块链网络存储每个所述业务相关方的所述第一数据块和所述第一签名数据，以及所述业务发起方的数据。
- [23]在一种可能的实施方式中，所述方法还包括：
- 25 [24]从所述区块链网络接收所述目标业务的处理结果信息；
- [25]根据所述处理结果信息，处理所述目标业务。
- [26]第三方面，提供了一种业务处理的方法，方法由区块链网络执行，并包括：

- [27]从目标业务的业务发起方接收每个业务相关方的第一数据块和第一签名数据,以及所述业务发起方的第二数据块和第二签名数据;其中,所述第一数据块包括由业务相关方采用预设编码方式对业务数据进行编码而生成的第一编码数据、第一确认结果和所述业务相关方的标识;所述第一签名数据为利用所述业务相关方的私钥对所述第一数据块进行签名计算得到的;所述第二数据块包括由业务发起方采用所述预设编码方式对所述业务数据进行编码而生成的第二编码数据、第二确认结果和所述业务发起方的标识;所述第二签名数据为利用所述业务发起方的私钥对所述第二数据块进行签名计算得到的;
- [28]存储每个所述业务相关方的所述第一数据块和所述第一签名数据,以及所述业务发起方的所述第二数据块和所述第二签名数据。
- [29]在一种可能的实施方式中,所述存储每个所述业务相关方的所述第一数据块和所述第一签名数据,以及所述业务发起方的所述第二数据块和所述第二签名数据之后,所述方法还包括:
- [30]处理所述目标业务。
- [31]进一步地,所述处理所述目标业务,包括:
- [32]记录所述目标业务的处理结果信息;以及,
- [33]向每个所述业务相关方发送所述目标业务的处理结果信息,以使每个所述业务相关方处理所述目标业务。
- [34]进一步地,所述存储每个所述业务相关方的所述第一数据块和所述第一签名数据,以及所述业务发起方的所述第二数据块和所述第二签名数据之前,所述方法还包括:
- [35]进行如下各项核对:
- [36]核对所述业务相关方的标识和/或所述业务发起方的标识是否与所述目标业务的业务链路上的成员标识相匹配;
- [37]核对每个所述第一编码数据和所述第二编码数据是否相同;
- [38]利用每个所述业务相关方的公钥对每个所述业务相关方的所述第一数据块和所述第一签名数据进行签名验证,验证所述第一数据块和所述第一签名数据是否匹配;
- [39]利用所述业务发起方的公钥对所述业务发起方的所述第二数据块和所述第二签名数据进行签名验证,验证所述第二数据块和所述第二签名数据是否匹配;
- [40]确定所述各项核对的核对结果均为是。

[41]在一种可能的实施方式中，所述存储每个所述业务相关方的所述第一数据块和所述第一签名数据，以及所述业务发起方的所述第二数据块和所述第二签名数据，包括：

[42]将每个所述业务相关方的所述第一数据块和所述第一签名数据，以及所述业务发起方的所述第二数据块和所述第二签名数据存储在一个区块中。

5 [43]第四方面，提供了一种业务处理的装置，装置设置于业务发起方，并包括：

[44]发送单元，用于针对目标业务向各业务相关方发送业务确认请求，所述业务确认请求中包括业务数据；

10 [45]接收单元，用于从每个所述业务相关方接收业务确认应答，所述业务确认应答中包括第一数据块和第一签名数据；其中，所述第一数据块包括由业务相关方采用预设编码方式对所述业务数据进行编码而生成的第一编码数据、第一确认结果和所述业务相关方的标识；所述第一签名数据为利用所述业务相关方的私钥对所述第一数据块进行签名计算得到的；

[46]编码单元，用于采用所述预设编码方式对所述业务数据进行编码，从而生成第二编码数据；以及生成第二确认结果；

15 [47]签名单元，用于利用所述业务发起方的私钥对包括第二编码数据、第二确认结果和所述业务发起方的标识的第二数据块进行签名，得到第二签名数据；

[48]存储单元，用于确定所述接收单元接收的每个所述第一确认结果和所述编码单元生成的所述第二确认结果均为确认通过时，通过区块链网络存储所述接收单元接收的每个所述业务相关方的所述第一数据块和所述第一签名数据，以及所述业务发起方的所述第二数据块和所述第二签名数据。

20

[49]第五方面，提供了一种业务处理的装置，装置设置于业务相关方，并包括：

[50]接收单元，用于从业务发起方接收针对目标业务的业务确认请求，所述业务确认请求中包括业务数据；

[51]确认单元，用于根据所述接收单元接收的业务数据，生成第一确认结果；

25 [52]编码单元，用于采用预设编码方式对所述接收单元接收的业务数据进行编码，生成第一编码数据；

[53]签名单元，用于利用所述业务相关方的私钥对包含所述第一确认结果和所述第一编码数据的第一数据块进行签名，得到第一签名数据；

[54]发送单元，用于向所述业务发起方发送业务确认应答，所述业务确认应答中包括所述第一数据块和所述第一签名数据；以使所述业务发起方确定每个所述业务相关方的确认结果均为确认通过时，通过区块链网络存储每个所述业务相关方的所述第一数据块和所述第一签名数据，以及所述业务发起方的数据。

5 [55]第六方面，提供了一种业务处理的装置，装置设置于区块链网络，并包括：

[56]接收单元，用于从目标业务的业务发起方接收每个业务相关方的第一数据块和第一签名数据，以及所述业务发起方的第二数据块和第二签名数据；其中，所述第一数据块包括由业务相关方采用预设编码方式对业务数据进行编码而生成的第一编码数据、第一确认结果和所述业务相关方的标识；所述第一签名数据为利用所述业务相关方的私钥对
10 所述第一数据块进行签名计算得到的；所述第二数据块包括由业务发起方采用所述预设编码方式对所述业务数据进行编码而生成的第二编码数据、第二确认结果和所述业务发起方的标识；所述第二签名数据为利用所述业务发起方的私钥对所述第二数据块进行签名计算得到的；

[57]存储单元，用于存储所述接收单元接收的每个所述业务相关方的所述第一数据块和
15 所述第一签名数据，以及所述业务发起方的所述第二数据块和所述第二签名数据。

[58]第七方面，提供了一种计算机可读存储介质，其上存储有计算机程序，当所述计算机程序在计算机中执行时，令计算机执行第一方面或第二方面或第三方面的方法。

[59]第八方面，提供了一种计算设备，包括存储器和处理器，所述存储器中存储有可执行代码，所述处理器执行所述可执行代码时，实现第一方面或第二方面或第三方面的方
20 法。

[60]通过本说明书实施例提供的方法和装置，业务发起方向业务相关方发送业务数据，从而便于业务相关方对业务进行确认，但是业务相关方不会直接返回给业务发起方业务数据和确认结果，而是业务相关方对业务数据进行编码得到编码数据，将编码数据和确认结果返回给业务发起方，后续业务发起方不是直接将业务数据和确认结果存储在区块链网络中，而是将编码数据和确认结果作为一个数据块存储在区块链网络中，区块链成员不会知道业务数据，从而能够在利用区块链网络存储业务数据时，不会导致敏感数据的泄露。
25

附图说明

[61]为了更清楚地说明本发明实施例的技术方案，下面将对实施例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发明的一些实施例，对于本领域普通技术人员来讲，在不付出创造性劳动的前提下，还可以根据这些附图获得其它的附图。

[62]图 1 为本说明书披露的一个实施例的实施场景示意图；

5 [63]图 2 为图 1 所示实施场景对应的区块链记账实施场景示意图；

[64]图 3 示出根据一个实施例的业务处理的方法流程图；

[65]图 4 示出根据另一个实施例的业务处理的方法流程图；

[66]图 5 示出根据另一个实施例的业务处理的方法流程图；

[67]图 6 示出根据一个实施例的业务处理过程中各成员交互过程示意图；

10 [68]图 7 示出根据一个实施例的业务处理时序图；

[69]图 8 示出根据一个实施例的业务处理的装置的示意性框图；

[70]图 9 示出根据另一个实施例的业务处理的装置的示意性框图；

[71]图 10 示出根据另一个实施例的业务处理的装置的示意性框图；

[72]图 11 示出根据一个实施例的业务处理的系统的示意性框图。

15 具体实施方式

[73]下面结合附图，对本说明书提供的方案进行描述。

[74]图 1 为本说明书披露的一个实施例的实施场景示意图。该实施场景涉及资金交易业务，具体为转账业务，图 1 中示出精简版的转账过程，张三通过第一钱包汇款给第二钱包的李四。参照图 1，资金的流向是：第一钱包（第一成员）→资金流通银行（第二成员）→第二钱包（第三成员）。为了保障资金流转的可靠性、简化对账和缩短转账周期等原因，引入了区块链记账。

20

[75]图 2 为图 1 所示实施场景对应的区块链记账实施场景示意图。该实施场景涉及转账过程中通过区块链进行数据记录。参照图 2，第一成员加入区块链后，通过第一钱包发起交易业务，区块链记录交易数据，并且把记录的交易数据发送给所有的成员。由于在金融监管里要求，每个资金链路的参与方都需要进行风险扫描，比如反洗钱、反恐怖融资等等，这些风险扫描往往需要用户的敏感数据（比如身份证号码）。所以，交易环节

25

中需要发起风险扫描，发起风险扫描的可以为第一成员、第二成员和第三成员中的任意一个，本说明书实施例中仅以第一成员作为业务发起方来举例描述，但是可以理解的是，业务发起方并不限定于第一成员。第一成员发起风险扫描后，资金链路中的各成员进行风险扫描，并反馈扫描结果。为了防止个别成员抵赖等风险，需要将各成员进行风险扫描的详细信息和扫描结果写入区块链，但是，风险扫描的详细信息里往往包含了大量隐私信息，如果将这些信息写入区块链，那么这些信息就会被泄露出去。

[76]针对上述问题，本说明书实施例在进行业务处理时，业务数据经过编码后存储到区块链上，实现了业务信息的脱敏，从而解决业务链路的各成员对业务进行认可，并不可抵赖，不泄露业务信息。

10 [77]需要说明的是，该实施场景涉及多成员参与一个区块链业务，并且需要各成员对于业务进行认可的场景。其中，上述多成员可以仅为两个，例如，一个业务发起方，一个业务相关方，上述多成员还可以为三个或更多个，例如，一个业务发起方，多个业务相关方。

[78]此外，上述业务可以是资金交易业务，也可以是非资金交易业务。

15 [79]例如，非资金交易业务可以是汽车租赁业务。该业务可以不存在中间方，第一成员可以是中介/平台，第二成员是某个汽车提供方的租赁公司，第一成员将实际租赁人的信息明文提交给第二成员进行确认是否可以租赁，然后第二成员对上述信息进行编码，并将编码数据和确认结果一起进行签名返回给第一成员。最后第一成员将脱敏的信息放到区块链上。

20 [80]可以理解的是，本说明实施例业务处理的方法可以应用的实施场景有很多，只要是多成员参与一个区块链业务，并且需要各成员对于业务进行认可的场景均适用，在此不再赘述。

[81]图3示出根据一个实施例的业务处理的方法流程图，所述方法由业务发起方执行，例如，图2所示场景中的第一成员。如图3所示，该实施例中业务处理的方法包括以下

25 步骤：步骤31，针对目标业务向各业务相关方发送业务确认请求，所述业务确认请求中包括业务数据；步骤32，从每个所述业务相关方接收业务确认应答，所述业务确认应答中包括第一数据块和第一签名数据；其中，所述第一数据块包括由业务相关方采用预设编码方式对所述业务数据进行编码而生成的第一编码数据、第一确认结果和所述业务相关方的标识；所述第一签名数据为利用所述业务相关方的私钥对所述第一数据块进行签

名计算得到的；步骤 33，采用所述预设编码方式对所述业务数据进行编码，从而生成第二编码数据；以及生成第二确认结果；步骤 34，利用所述业务发起方的私钥对包括第二编码数据、第二确认结果和所述业务发起方的标识的第二数据块进行签名，得到第二签名数据；步骤 35，确定每个所述第一确认结果和所述第二确认结果均为确认通过时，通过区块链网络存储每个所述业务相关方的所述第一数据块和所述第一签名数据，以及所述业务发起方的所述第二数据块和所述第二签名数据。下面描述以上各个步骤的具体执行方式。

[82]首先在步骤 31，针对目标业务向各业务相关方发送业务确认请求，所述业务确认请求中包括业务数据。

10 [83]本说明书实施例中，对于业务数据包含的内容不做限定，例如，可以包括用户的姓名、身份证号码、年龄等隐私信息，但并不限于此。

[84]接着在步骤 32，从每个所述业务相关方接收业务确认应答，所述业务确认应答中包括第一数据块和第一签名数据；其中，所述第一数据块包括由业务相关方采用预设编码方式对所述业务数据进行编码而生成的第一编码数据、第一确认结果和所述业务相关方的标识；所述第一签名数据为利用所述业务相关方的私钥对所述第一数据块进行签名计算得到的。

15

[85]可以理解的是，上述业务相关方的数目可以为多个，也可以为一个。

[86]上述预设编码方式可以采用任一通过编码数据不容易获取原始数据的编码方式，例如，哈希编码方式。

20 [87]上述第一确认结果用于指示业务相关方是否认可该目标业务。

[88]上述签名数据可以用于证明身份，区块链的每个成员都有一个成员 ID 和一对公私钥，公钥是公开的，公私钥可以用于证明身份。例如，A 可以用私钥对数据 D 进行签名，得到签名串 S；A 把数据 D 和签名串 S 发送给 B；B 通过 A 的公钥，对数据 D 和签名串 S 进行验证签名，如果匹配，说明 B 收到的数据确实来自于 A。

25 [89]然后在步骤 33，采用所述预设编码方式对所述业务数据进行编码，从而生成第二编码数据；以及生成第二确认结果。

[90]可以理解的是，业务发起方与业务相关方生成编码数据的方式相同，理论上，第一编码数据与第二编码数据也应用相同，后续可以由区块链网络对二者是否相同进行核对。

[91]上述第二确认结果用于指示业务发起方是否认可该目标业务。

[92]再在步骤 34，利用所述业务发起方的私钥对包括第二编码数据、第二确认结果和所述业务发起方的标识的第二数据块进行签名，得到第二签名数据。

[93]签名计算的方式，前面已有描述，在此不做赘述。

- 5 [94]最后在步骤 35，确定每个所述第一确认结果和所述第二确认结果均为确认通过时，通过区块链网络存储每个所述业务相关方的所述第一数据块和所述第一签名数据，以及所述业务发起方的所述第二数据块和所述第二签名数据。

- [95]在一个示例中，确定每个所述第一确认结果和所述第二确认结果均为确认通过时，还可以通过所述区块链网络处理所述目标业务。例如，通过所述区块链网络记录所述目标业务的处理结果信息；以及，通过所述区块链网络向每个所述业务相关方发送所述目标业务的处理结果信息，以使每个所述业务相关方处理所述目标业务。
- 10

- [96]通过本说明书实施例提供的方法，业务发起方向业务相关方发送业务数据，从而便于业务相关方对业务进行确认，但是业务相关方不会直接返回给业务发起方业务数据和确认结果，而是业务相关方对业务数据进行编码得到编码数据，将编码数据和确认结果
- 15 返回给业务发起方，后续业务发起方不是直接将业务数据和确认结果存储在区块链网络中，而是将编码数据和确认结果作为一个数据块存储在区块链网络中，区块链成员不会知道业务数据，从而能够在利用区块链网络存储业务数据时，不会导致敏感数据的泄露。

- [97]图 4 示出根据另一个实施例的业务处理的方法流程图，所述方法由业务相关方执行，例如，图 2 所示场景中的第二成员或第三成员。如图 4 所示，该实施例中业务处理的方法包括以下步骤：步骤 41，从业务发起方接收针对目标业务的业务确认请求，所述业务确认请求中包括业务数据；步骤 42，根据所述业务数据，生成第一确认结果；步骤 43，采用预设编码方式对所述业务数据进行编码，生成第一编码数据；步骤 44，利用所述业务相关方的私钥对包含所述第一确认结果和所述第一编码数据的第一数据块进行签名，得到第一签名数据；步骤 45，向所述业务发起方发送业务确认应答，所述业务确认应答
- 20 中包括所述第一数据块和所述第一签名数据；以使所述业务发起方确定每个所述业务相关方的确认结果均为确认通过时，通过区块链网络存储每个所述业务相关方的所述第一数据块和所述第一签名数据，以及所述业务发起方的数据。下面描述以上各个步骤的具体执行方式。
- 25

[98]首先在步骤 41，从业务发起方接收针对目标业务的业务确认请求，所述业务确认请

求中包括业务数据。

[99] 本说明书实施例中，对于业务数据包含的内容不做限定，例如，可以包括用户的姓名、身份证号码、年龄等隐私信息，但并不限于此。

[100] 接着在步骤 42，根据所述业务数据，生成第一确认结果。

5 [101] 上述第一确认结果用于指示业务相关方是否认可该目标业务。

[102] 然后在步骤 43，采用预设编码方式对所述业务数据进行编码，生成第一编码数据。

[103] 可以理解的是，业务发起方与业务相关方生成编码数据的方式相同，理论上，第一编码数据与第二编码数据也应用相同，后续可以由区块链网络对二者是否相同进行
10 核对。

[104] 再在步骤 44，利用所述业务相关方的私钥对包含所述第一确认结果和所述第一编码数据的第一数据块进行签名，得到第一签名数据。

[105] 签名计算的方式，前面已有描述，在此不做赘述。

[106] 最后在步骤 45，向所述业务发起方发送业务确认应答，所述业务确认应答中包
15 括所述第一数据块和所述第一签名数据；以使所述业务发起方确定每个所述业务相关方的确认结果均为确认通过时，通过区块链网络存储每个所述业务相关方的所述第一数据块和所述第一签名数据，以及所述业务发起方的数据。

[107] 其中，所述业务发起方的数据包括所述业务发起方的所述第二数据块和所述第二签名数据，具体可以参见图 3 对应的描述。

20 [108] 在一个示例中，所述方法还包括：

[109] 从所述区块链网络接收所述目标业务的处理结果信息；

[110] 根据所述处理结果信息，处理所述目标业务。

[111] 通过本说明书实施例提供的方法，业务相关方从业务发起方接收业务数据，从而便于业务相关方对业务进行确认，但是业务相关方不会直接返回给业务发起方业务数据
25 和确认结果，而是业务相关方对业务数据进行编码得到编码数据，将编码数据和确认结果返回给业务发起方，后续业务发起方不是直接将业务数据和确认结果存储在区块链网络中，而是将编码数据和确认结果作为一个数据块存储在区块链网络中，区块链成员不会知道业务数据，从而能够在利用区块链网络存储业务数据时，不会导致敏感数据的

泄露。

[112] 图 5 示出根据另一个实施例的业务处理的方法流程图，所述方法由区块链网络执行，区块链网络可以简称为区块链，例如，图 2 所示场景中的区块链。如图 5 所示，该实施例中业务处理的方法包括以下步骤：

- 5 [113] 步骤 51，从目标业务的业务发起方接收每个业务相关方的第一数据块和第一签名数据，以及所述业务发起方的第二数据块和第二签名数据；其中，所述第一数据块包括由业务相关方采用预设编码方式对业务数据进行编码而生成的第一编码数据、第一确认结果和所述业务相关方的标识；所述第一签名数据为利用所述业务相关方的私钥对所述第一数据块进行签名计算得到的；所述第二数据块包括由业务发起方采用所述预设编
- 10 码方式对所述业务数据进行编码而生成的第二编码数据、第二确认结果和所述业务发起方的标识；所述第二签名数据为利用所述业务发起方的私钥对所述第二数据块进行签名计算得到的。

[114] 可以理解的是，业务发起方和业务相关方可以预先加入该区块链网络，成为该区块链网络的成员。

- 15 [115] 步骤 52，存储每个所述业务相关方的所述第一数据块和所述第一签名数据，以及所述业务发起方的所述第二数据块和所述第二签名数据。

[116] 在一个示例中，步骤 52 之后，所述方法还可以包括：处理所述目标业务。例如，记录所述目标业务的处理结果信息；以及，向每个所述业务相关方发送所述目标业务的处理结果信息，以使每个所述业务相关方处理所述目标业务。

- 20 [117] 在一个示例中，步骤 52 之前，所述方法还可以包括：

[118] 进行如下各项核对：

[119] 核对所述业务相关方的标识和/或所述业务发起方的标识是否与所述目标业务的业务链路上的成员标识相匹配；

[120] 核对每个所述第一编码数据和所述第二编码数据是否相同；

- 25 [121] 利用每个所述业务相关方的公钥对每个所述业务相关方的所述第一数据块和所述第一签名数据进行签名验证，验证所述第一数据块和所述第一签名数据是否匹配；

[122] 利用所述业务发起方的公钥对所述业务发起方的所述第二数据块和所述第二签名数据进行签名验证，验证所述第二数据块和所述第二签名数据是否匹配；

[123] 确定所述各项核对的核对结果均为是。

[124] 作为示例,步骤 52 具体可以将每个所述业务相关方的所述第一数据块和所述第一签名数据,以及所述业务发起方的所述第二数据块和所述第二签名数据存储在一个区块中。

5 [125] 通过本说明书实施例提供的方法,区块链网络不是直接从业务发起方接收业务数据和确认结果,而是接收编码数据和确认结果,并且将编码数据和确认结果作为一个数据块存储在区块链网络中,区块链成员不会知道业务数据,从而能够在利用区块链网络存储业务数据时,不会导致敏感数据的泄露。

10 [126] 图 6 示出根据一个实施例的业务处理过程中各成员交互过程示意图。图 7 示出根据一个实施例的业务处理时序图。参照图 6 或图 7,业务链路涉及第一成员、第二成员和第三成员,第一成员为业务发起方,第二成员和第三成员为业务相关方,业务的进行需要得到第一成员、第二成员和第三成员的许可。

15 [127] 根据另一方面的实施例,还提供一种业务处理的装置,所述装置设置于业务发起方。图 8 示出根据一个实施例的业务处理的装置的示意性框图。如图 8 所示,该装置 800 包括:

[128] 发送单元 81,用于针对目标业务向各业务相关方发送业务确认请求,所述业务确认请求中包括业务数据;

20 [129] 接收单元 82,用于从每个所述业务相关方接收业务确认应答,所述业务确认应答中包括第一数据块和第一签名数据;其中,所述第一数据块包括由业务相关方采用预设编码方式对所述业务数据进行编码而生成的第一编码数据、第一确认结果和所述业务相关方的标识;所述第一签名数据为利用所述业务相关方的私钥对所述第一数据块进行签名计算得到的;

[130] 编码单元 83,用于采用所述预设编码方式对所述业务数据进行编码,从而生成第二编码数据;以及生成第二确认结果;

25 [131] 签名单元 84,用于利用所述业务发起方的私钥对包括第二编码数据、第二确认结果和所述业务发起方的标识的第二数据块进行签名,得到第二签名数据;

[132] 存储单元 85,用于确定所述接收单元 82 接收的每个所述第一确认结果和所述编码单元 83 生成的所述第二确认结果均为确认通过时,通过区块链网络存储所述接收单元 82 接收的每个所述业务相关方的所述第一数据块和所述第一签名数据,以及所述业

务发起方的所述第二数据块和所述第二签名数据。

[133] 可选地, 作为一个实施例, 所述装置还包括:

[134] 处理单元, 用于确定所述接收单元 82 接收的每个所述第一确认结果和所述第二确认结果均为确认通过时, 通过所述区块链网络处理所述目标业务。

5 [135] 进一步地, 所述处理单元, 具体用于:

[136] 通过所述区块链网络记录所述目标业务的处理结果信息; 以及,

[137] 通过所述区块链网络向每个所述业务相关方发送所述目标业务的处理结果信息, 以使每个所述业务相关方处理所述目标业务。

[138] 通过本说明书实施例提供的装置, 发送单元 81 向业务相关方发送业务数据, 从而便于业务相关方对业务进行确认, 但是业务相关方不会直接返回给接收单元 82 业务数据和确认结果, 而是业务相关方对业务数据进行编码得到编码数据, 将编码数据和确认结果返回给接收单元 82, 后续存储单元 85 不是直接将业务数据和确认结果存储在区块链网络中, 而是将编码数据和确认结果作为一个数据块存储在区块链网络中, 区块链成员不会知道业务数据, 从而能够在利用区块链网络存储业务数据时, 不会导致敏感数据的泄露。

10

15

[139] 根据另一方面的实施例, 还提供一种业务处理的装置, 所述装置设置于业务相关方。图 9 示出根据另一个实施例的业务处理的装置的示意性框图。如图 9 所示, 该装置 900 包括:

[140] 接收单元 91, 用于从业务发起方接收针对目标业务的业务确认请求, 所述业务确认请求中包括业务数据;

20

[141] 确认单元 92, 用于根据所述接收单元 91 接收的业务数据, 生成第一确认结果;

[142] 编码单元 93, 用于采用预设编码方式对所述接收单元 91 接收的业务数据进行编码, 生成第一编码数据;

[143] 签名单元 94, 用于利用所述业务相关方的私钥对包含所述第一确认结果和所述第一编码数据的第一数据块进行签名, 得到第一签名数据;

25

[144] 发送单元 95, 用于向所述业务发起方发送业务确认应答, 所述业务确认应答中包括所述第一数据块和所述第一签名数据; 以使所述业务发起方确定每个所述业务相关方的确认结果均为确认通过时, 通过区块链网络存储每个所述业务相关方的所述第一数

据块和所述第一签名数据, 以及所述业务发起方的数据。

[145] 可选地, 作为一个实施例,

[146] 所述接收单元 91, 还用于从所述区块链网络接收所述目标业务的处理结果信息;

[147] 所述装置还包括:

5 [148] 处理单元, 用于根据所述接收单元 91 接收的处理结果信息, 处理所述目标业务。

[149] 通过本说明书实施例提供的装置, 接收单元 91 从业务发起方接收业务数据, 从而便于确认单元 92 对业务进行确认, 但是发送单元 95 不会直接返回给业务发起方业务数据和确认结果, 而是业务相关方对业务数据进行编码得到编码数据, 将编码数据和确认结果返回给业务发起方, 后续业务发起方不是直接将业务数据和确认结果存储在区块链网络中, 而是将编码数据和确认结果作为一个数据块存储在区块链网络中, 区块链成员不会知道业务数据, 从而能够在利用区块链网络存储业务数据时, 不会导致敏感数据的泄露。

10

[150] 根据另一方面的实施例, 还提供一种业务处理的装置, 所述装置设置于区块链网络, 具体地, 设置于区块链网络的节点, 可以简称为区块链。图 10 示出根据另一个实施例的业务处理的装置的示意性框图。如图 10 所示, 该装置 1000 包括:

15

[151] 接收单元 1001, 用于从目标业务的业务发起方接收每个业务相关方的第一数据块和第一签名数据, 以及所述业务发起方的第二数据块和第二签名数据; 其中, 所述第一数据块包括由业务相关方采用预设编码方式对业务数据进行编码而生成的第一编码数据、第一确认结果和所述业务相关方的标识; 所述第一签名数据为利用所述业务相关方的私钥对所述第一数据块进行签名计算得到的; 所述第二数据块包括由业务发起方采用所述预设编码方式对所述业务数据进行编码而生成的第二编码数据、第二确认结果和所述业务发起方的标识; 所述第二签名数据为利用所述业务发起方的私钥对所述第二数据块进行签名计算得到的;

20

[152] 存储单元 1002, 用于存储所述接收单元 1001 接收的每个所述业务相关方的所述第一数据块和所述第一签名数据, 以及所述业务发起方的所述第二数据块和所述第二签名数据。

25

[153] 可选地, 作为一个实施例, 所述装置还包括:

[154] 处理单元, 用于在所述存储单元 1002 存储每个所述业务相关方的所述第一数据

块和所述第一签名数据,以及所述业务发起方的所述第二数据块和所述第二签名数据之后,处理所述目标业务。

[155] 进一步地,所述处理单元,具体用于:

[156] 记录所述目标业务的处理结果信息;以及,

- 5 [157] 向每个所述业务相关方发送所述目标业务的处理结果信息,以使每个所述业务相关方处理所述目标业务。

[158] 进一步地,所述装置还包括:

[159] 核对单元,用于在所述存储单元 1002 存储每个所述业务相关方的所述第一数据块和所述第一签名数据,以及所述业务发起方的所述第二数据块和所述第二签名数据之前,进行如下各项核对:

10

[160] 核对所述业务相关方的标识和/或所述业务发起方的标识是否与所述目标业务的业务链路上的成员标识相匹配;

[161] 核对每个所述第一编码数据和所述第二编码数据是否相同;

[162] 利用每个所述业务相关方的公钥对每个所述业务相关方的所述第一数据块和所述
15 所述第一签名数据进行签名验证,验证所述第一数据块和所述第一签名数据是否匹配;

[163] 利用所述业务发起方的公钥对所述业务发起方的所述第二数据块和所述第二签名数据进行签名验证,验证所述第二数据块和所述第二签名数据是否匹配;

[164] 确定单元,用于确定所述核对单元得到的所述各项核对的核对结果均为是。

- [165] 可选地,作为一个实施例,所述存储单元 1002,具体用于将所述接收单元 1001
20 接收的每个所述业务相关方的所述第一数据块和所述第一签名数据,以及所述业务发起方的所述第二数据块和所述第二签名数据存储在一个区块中。

- [166] 通过本说明书实施例提供的装置,接收单元 1001 不是直接从业务发起方接收业务数据和确认结果,而是接收编码数据和确认结果,并且存储单元 1002 将编码数据和确认结果作为一个数据块存储在区块链网络中,区块链成员不会知道业务数据,从而能够
25 在利用区块链网络存储业务数据时,不会导致敏感数据的泄露。

[167] 根据另一方面的实施例,还提供一种业务处理的系统,所述系统包括第一成员业务系统、第二成员业务系统、区块链桥接系统和区块链。图 11 示出根据一个实施例的业务处理的系统的示意性框图。如图 11 所示,该系统的处理过程包括:

[168] 首先，第一成员（即业务发起方）向第一成员的区块链桥接系统发起交易确认请求，请求中的数据包括交易约定的明细数据（以下统称 BIZ_DATA）。

[169] 接下来，第一成员的区块链桥接系统的接收模块收到请求后，经过发送模块将数据按照约定的格式发送给交易链路上的所有成员，发送的数据包括 BIZ_DATA。

5 [170] 然后，第二成员（如果业务相关方还包括第三成员，则与第二成员采用相同的处理逻辑）的区块链桥接系统的接收模块收到请求后，将数据转发给第二成员的业务系统，进行交易确认，收到的数据包括 BIZ_DATA。第二成员进行确认后，将确认结果（以下统称 RESULT）返回给区块链桥接系统的接收模块。接收模块，将所述的 BIZ_DATA 和所述的结果传给脱敏模块处理。

10 [171] 再然后，第二成员的区块链桥接系统的脱敏模块，对所述的 BIZ_DATA 进行哈希（hash）处理（也可采用其他的编码方式），计算出对应的哈希编码（hash code）。然后，将 hash code、RESULT 传给签名模块。

[172] 再然后，第二成员的区块链桥接系统的签名模块，将所述的 hash code、RESULT 和第二成员预设的成员 ID 按照约定的格式作为一个数据块（以下统称
15 CHECK_RESULT），然后用私钥计算签名（以下统称 SIGNATURE）。

[173] 再然后，第二成员的区块链桥接系统的发送模块将所述的 CHECK_RESULT 和 SIGNATURE 返回给第一成员。

[174] 再然后，第一成员的区块链桥接系统的发送模块收到交易链路上所有成员返回的 CHECK_RESULT 和 SIGNATURE 后，解析并检查所有收到的 CHECK_RESULT 里
20 的交易确认结果（所述的 RESULT）是否都是确认通过，如果确认通过，则继续调用接入模块。

[175] 再然后，第一成员的区块链桥接系统的接入模块，将交易链路上所有成员的 CHECK_RESULT 和 SIGNATURE 发送给区块链进行处理。

[176] 再然后，区块链里的核对模块进行以下核对：解析所有的 CHECK_RESULT，
25 解析后的数据包括所述的 hash code、RESULT 和成员 ID；核对解析得到的所有成员 ID 和交易链路上的所有成员 ID 是否匹配；核对每个成员的 hash code 是否完全相同；检查每一对 CHECK_RESULT 和 SIGNATURE，通过成员 ID 拿到对应成员的公钥，利用公钥对 CHECK_RESULT 和 SIGNATURE 进行签名验证，验证是否匹配。

[177] 最后，区块链在上述核对都完成后就可以调用区块链的业务模块进行业务处理

了。

[178] 根据另一方面的实施例，还提供一种计算机可读存储介质，其上存储有计算机程序，当所述计算机程序在计算机中执行时，令计算机执行结合图 3 至图 5 中任一所描述的方法。

- 5 [179] 根据再一方面的实施例，还提供一种计算设备，包括存储器和处理器，所述存储器中存储有可执行代码，所述处理器执行所述可执行代码时，实现结合图 3 至图 5 中任一所描述的方法。

10 [180] 本领域技术人员应该可以意识到，在上述一个或多个示例中，本发明所描述的功能可以用硬件、软件、固件或它们的任意组合来实现。当使用软件实现时，可以将这些功能存储在计算机可读介质中或者作为计算机可读介质上的一个或多个指令或代码进行传输。

[181] 以上所述的具体实施方式，对本发明的目的、技术方案和有益效果进行了进一步详细说明，所应理解的是，以上所述仅为本发明的具体实施方式而已，并不用于限定本发明的保护范围，凡在本发明的技术方案的基础之上，所做的任何修改、等同替换、改进等，均应包括在本发明的保护范围之内。

15

权利要求书

1.一种业务处理的方法，所述方法由业务发起方执行，并包括：

针对目标业务向各业务相关方发送业务确认请求，所述业务确认请求中包括业务数据；

5 从每个所述业务相关方接收业务确认应答，所述业务确认应答中包括第一数据块和第一签名数据；其中，所述第一数据块包括由业务相关方采用预设编码方式对所述业务数据进行编码而生成的第一编码数据、第一确认结果和所述业务相关方的标识；所述第一签名数据为利用所述业务相关方的私钥对所述第一数据块进行签名计算得到的；

10 采用所述预设编码方式对所述业务数据进行编码，从而生成第二编码数据；以及生成第二确认结果；

利用所述业务发起方的私钥对包括第二编码数据、第二确认结果和所述业务发起方的标识的第二数据块进行签名，得到第二签名数据；

15 确定每个所述第一确认结果和所述第二确认结果均为确认通过时，通过区块链网络存储每个所述业务相关方的所述第一数据块和所述第一签名数据，以及所述业务发起方的所述第二数据块和所述第二签名数据。

2.如权利要求1所述的方法，其中，所述方法还包括：

确定每个所述第一确认结果和所述第二确认结果均为确认通过时，通过所述区块链网络处理所述目标业务。

20 3.如权利要求2所述的方法，其中，所述通过所述区块链网络处理所述目标业务，包括：

通过所述区块链网络记录所述目标业务的处理结果信息；以及，

通过所述区块链网络向每个所述业务相关方发送所述目标业务的处理结果信息，以使每个所述业务相关方处理所述目标业务。

4.一种业务处理的方法，所述方法由业务相关方执行，并包括：

25 从业务发起方接收针对目标业务的业务确认请求，所述业务确认请求中包括业务数据；

根据所述业务数据，生成第一确认结果；

采用预设编码方式对所述业务数据进行编码，生成第一编码数据；

30 利用所述业务相关方的私钥对包含所述第一确认结果和所述第一编码数据的第一数据块进行签名，得到第一签名数据；

向所述业务发起方发送业务确认应答，所述业务确认应答中包括所述第一数据块和

所述第一签名数据；以使所述业务发起方确定每个所述业务相关方的确认结果均为确认通过时，通过区块链网络存储每个所述业务相关方的所述第一数据块和所述第一签名数据，以及所述业务发起方的数据。

5.如权利要求4所述的方法，其中，所述方法还包括：

- 5 从所述区块链网络接收所述目标业务的处理结果信息；
根据所述处理结果信息，处理所述目标业务。

6.一种业务处理的方法，所述方法由区块链网络执行，并包括：

- 10 从目标业务的业务发起方接收每个业务相关方的第一数据块和第一签名数据，以及所述业务发起方的第二数据块和第二签名数据；其中，所述第一数据块包括由业务相关方采用预设编码方式对业务数据进行编码而生成的第一编码数据、第一确认结果和所述业务相关方的标识；所述第一签名数据为利用所述业务相关方的私钥对所述第一数据块进行签名计算得到的；所述第二数据块包括由业务发起方采用所述预设编码方式对所述业务数据进行编码而生成的第二编码数据、第二确认结果和所述业务发起方的标识；所述第二签名数据为利用所述业务发起方的私钥对所述第二数据块进行签名计算得到的；
15 存储每个所述业务相关方的所述第一数据块和所述第一签名数据，以及所述业务发起方的所述第二数据块和所述第二签名数据。

7.如权利要求6所述的方法，其中，所述存储每个所述业务相关方的所述第一数据块和所述第一签名数据，以及所述业务发起方的所述第二数据块和所述第二签名数据之后，所述方法还包括：

- 20 处理所述目标业务。

8.如权利要求7所述的方法，其中，所述处理所述目标业务，包括：

记录所述目标业务的处理结果信息；以及，

向每个所述业务相关方发送所述目标业务的处理结果信息，以使每个所述业务相关方处理所述目标业务。

- 25 9.如权利要求7所述的方法，其中，所述存储每个所述业务相关方的所述第一数据块和所述第一签名数据，以及所述业务发起方的所述第二数据块和所述第二签名数据之前，所述方法还包括：

进行如下各项核对：

- 30 核对所述业务相关方的标识和/或所述业务发起方的标识是否与所述目标业务的业务链路上的成员标识相匹配；

核对每个所述第一编码数据和所述第二编码数据是否相同；

利用每个所述业务相关方的公钥对每个所述业务相关方的所述第一数据块和所述第一签名数据进行签名验证, 验证所述第一数据块和所述第一签名数据是否匹配;

利用所述业务发起方的公钥对所述业务发起方的所述第二数据块和所述第二签名数据进行签名验证, 验证所述第二数据块和所述第二签名数据是否匹配;

5 确定所述各项核对的核对结果均为是。

10.如权利要求6所述的方法, 其中, 所述存储每个所述业务相关方的所述第一数据块和所述第一签名数据, 以及所述业务发起方的所述第二数据块和所述第二签名数据, 包括:

10 将每个所述业务相关方的所述第一数据块和所述第一签名数据, 以及所述业务发起方的所述第二数据块和所述第二签名数据存储在一个区块中。

11.一种业务处理的装置, 所述装置设置于业务发起方, 并包括:

发送单元, 用于针对目标业务向各业务相关方发送业务确认请求, 所述业务确认请求中包括业务数据;

15 接收单元, 用于从每个所述业务相关方接收业务确认应答, 所述业务确认应答中包括第一数据块和第一签名数据; 其中, 所述第一数据块包括由业务相关方采用预设编码方式对所述业务数据进行编码而生成的第一编码数据、第一确认结果和所述业务相关方的标识; 所述第一签名数据为利用所述业务相关方的私钥对所述第一数据块进行签名计算得到的;

20 编码单元, 用于采用所述预设编码方式对所述业务数据进行编码, 从而生成第二编码数据; 以及生成第二确认结果;

签名单元, 用于利用所述业务发起方的私钥对包括第二编码数据、第二确认结果和所述业务发起方的标识的第二数据块进行签名, 得到第二签名数据;

25 存储单元, 用于确定所述接收单元接收的每个所述第一确认结果和所述编码单元生成的所述第二确认结果均为确认通过时, 通过区块链网络存储所述接收单元接收的每个所述业务相关方的所述第一数据块和所述第一签名数据, 以及所述业务发起方的所述第二数据块和所述第二签名数据。

12.如权利要求11所述的装置, 其中, 所述装置还包括:

处理单元, 用于确定所述接收单元接收的每个所述第一确认结果和所述第二确认结果均为确认通过时, 通过所述区块链网络处理所述目标业务。

30 13.如权利要求12所述的装置, 其中, 所述处理单元, 具体用于:

通过所述区块链网络记录所述目标业务的处理结果信息; 以及,

通过所述区块链网络向每个所述业务相关方发送所述目标业务的处理结果信息，以使每个所述业务相关方处理所述目标业务。

14.一种业务处理的装置，所述装置设置于业务相关方，并包括：

接收单元，用于从业务发起方接收针对目标业务的业务确认请求，所述业务确认请

5 求中包括业务数据；

确认单元，用于根据所述接收单元接收的业务数据，生成第一确认结果；

编码单元，用于采用预设编码方式对所述接收单元接收的业务数据进行编码，生成第一编码数据；

10 签名单元，用于利用所述业务相关方的私钥对包含所述第一确认结果和所述第一编码数据的第一数据块进行签名，得到第一签名数据；

发送单元，用于向所述业务发起方发送业务确认应答，所述业务确认应答中包括所述第一数据块和所述第一签名数据；以使所述业务发起方确定每个所述业务相关方的确认结果均为确认通过时，通过区块链网络存储每个所述业务相关方的所述第一数据块和所述第一签名数据，以及所述业务发起方的数据。

15 15.如权利要求 14 所述的装置，其中，

所述接收单元，还用于从所述区块链网络接收所述目标业务的处理结果信息；

所述装置还包括：

处理单元，用于根据所述接收单元接收的处理结果信息，处理所述目标业务。

16.一种业务处理的装置，所述装置设置于区块链网络，并包括：

20 接收单元，用于从目标业务的业务发起方接收每个业务相关方的第一数据块和第一签名数据，以及所述业务发起方的第二数据块和第二签名数据；其中，所述第一数据块包括由业务相关方采用预设编码方式对业务数据进行编码而生成的第一编码数据、第一确认结果和所述业务相关方的标识；所述第一签名数据为利用所述业务相关方的私钥对所述第一数据块进行签名计算得到的；所述第二数据块包括由业务发起方采用所述预设

25 编码方式对所述业务数据进行编码而生成的第二编码数据、第二确认结果和所述业务发起方的标识；所述第二签名数据为利用所述业务发起方的私钥对所述第二数据块进行签名计算得到的；

存储单元，用于存储所述接收单元接收的每个所述业务相关方的所述第一数据块和所述第一签名数据，以及所述业务发起方的所述第二数据块和所述第二签名数据。

30 17.如权利要求 16 所述的装置，其中，所述装置还包括：

处理单元，用于在所述存储单元存储每个所述业务相关方的所述第一数据块和所述

第一签名数据, 以及所述业务发起方的所述第二数据块和所述第二签名数据之后, 处理所述目标业务。

18.如权利要求 17 所述的装置, 其中, 所述处理单元, 具体用于:

记录所述目标业务的处理结果信息; 以及,

- 5 向每个所述业务相关方发送所述目标业务的处理结果信息, 以使每个所述业务相关方处理所述目标业务。

19.如权利要求 17 所述的装置, 其中, 所述装置还包括:

核对单元, 用于在所述存储单元存储每个所述业务相关方的所述第一数据块和所述第一签名数据, 以及所述业务发起方的所述第二数据块和所述第二签名数据之前, 进行
10 如下各项核对:

核对所述业务相关方的标识和/或所述业务发起方的标识是否与所述目标业务的业务链路上的成员标识相匹配;

核对每个所述第一编码数据和所述第二编码数据是否相同;

- 15 利用每个所述业务相关方的公钥对每个所述业务相关方的所述第一数据块和所述第一签名数据进行签名验证, 验证所述第一数据块和所述第一签名数据是否匹配;

利用所述业务发起方的公钥对所述业务发起方的所述第二数据块和所述第二签名数据进行签名验证, 验证所述第二数据块和所述第二签名数据是否匹配;

确定单元, 用于确定所述核对单元得到的所述各项核对的核对结果均为是。

- 20.如权利要求 16 所述的装置, 其中, 所述存储单元, 具体用于将所述接收单元接收的每个所述业务相关方的所述第一数据块和所述第一签名数据, 以及所述业务发起方的所述第二数据块和所述第二签名数据存储在一个区块中。
20

21.一种计算机可读存储介质, 其上存储有计算机程序, 当所述计算机程序在计算机中执行时, 令计算机执行权利要求 1-10 中任一项的所述的方法。

- 22.一种计算设备, 包括存储器和处理器, 所述存储器中存储有可执行代码, 所述处理器执行所述可执行代码时, 实现权利要求 1-10 中任一项的所述的方法。
25