说　明　书

交易处理方法、装置、交易系统、存储介质和计算机系统

技术领域

本说明书一个或多个实施例涉及计算机领域，尤其涉及一种交易处理方法、装置、交易系统、存储介质和计算机系统。

背景技术

交易系统中通常可以存储用户注册的账户所持有相关资源的余额，前述交易系统可以是中心化的商品交易或资产交易平台，或者是去中心化的区块链系统。基于隐私保护的需要，交易系统中存储的余额可以是采用同态加密算法对明文余额加密得到的密文余额，用户向交易平台发起的交易请求中可以包括，采用该同态加密算法对明文交易金额加密得到的密文交易金额，交易系统可以根据密文交易金额更新相关账户的密文余额。

希望有一种新的技术方案，以期交易系统能够更加准确的处理交易请求。

发明内容

本说明书一个或多个实施例中提供了一种交易处理方法、装置、交易系统、存储介质和计算机系统，可以避免并不会导致相关账户发生余额透支的交易请求，被交易系统错误的确定为未通过合法性验证的异常请求而并不对其正确处理，有利于交易系统更加准确的处理交易请求，从而进一步的提高用户体验。

本说明书提供了一种交易处理方法，所述方法由交易系统执行，所述交易系统对各账户存储其对应的余额队列，所述余额队列包括按时间先后依次添加至队尾的若干密文余额，所述方法包括：接收交易请求，其中包括第一账户、第二账户、第一密文余额，以及至少利用所述第一账户的公钥对交易金额进行同态加密得到的第一密文交易金额；响应于确认所述交易请求合法，执行第一更新和第二更新；其中，所述第一更新包括：确定所述第一账户所对应第一余额队列队尾的密文余额与所述第一密文交易金额间的密文差值，将所述密文差值加入所述第一余额队列作为更新队尾，并删除所述第一余额队列中除所述更新队尾外的其它密文余额；所述第二更新包括：将所述第二账户所对应第二余额队列队尾的密文余额与第二密文交易金额间的密文和值添加至所述第二余额队列队尾，其中所述第二密文交易金额是对所述交易金额进行同态加密得到的，并且对于所述第二账户可解密。

本说明书提供了一种交易处理方法，所述方法涉及的交易系统对各账户存储其对应的余额队列，所述余额队列包括按时间先后依次添加至队尾的若干密文余额，所述方法通过第一账户对应的终端执行，所述方法包括：从所述交易系统获取，所述第一账户所对应第一余额队列中的第一密文余额；确定交易金额以及作为支付目标的第二账户，并至少利用所述第一账户的公钥对交易金额进行同态加密，获得第一密文交易金额；向所述交易系统发送交易请求，其中包括所述第一账户、所述第二账户、所述第一密文余额以及所述第一密文交易金额，使所述交易系统在确认所述交易请求合法后，对所述第一余额队列进行第一更新，以及对所述第二账户对应的第二余额队列进行第二更新。

本说明书提供了一种计算机系统，包括存储器、处理器及存储在所述存储器上并可在所述处理器上运行的计算机程序，所述计算器程序用于实现交易系统，所述交易系统对各账户存储其对应的余额队列，所述余额队列包括按时间先后依次添加至队尾的若干密文余额，所述处理器执行所述计算机程序时实现如下步骤：接收交易请求，其中包括第一账户、第二账户、第一密文余额，以及至少利用所述第一账户的公钥对交易金额进行同态加密得到的第一密文交易金额；响应于确认所述交易请求合法，执行第一更新和第二更新；其中，所述第一更新包括：确定所述第一账户所对应第一余额队列队尾的密文余额与所述第一密文交易金额间的密文差值，将所述密文差值加入所述第一余额队列作为更新队尾，并删除所述第一余额队列中除所述更新队尾外的其它密文余额；所述第二更新包括：将所述第二账户所对应第二余额队列队尾的密文余额与第二密文交易金额间的密文和值添加至所述第二余额队列队尾，其中所述第二密文交易金额是对所述交易金额进行同态加密得到的，并且对于所述第二账户可解密。

本说明书提供了一种计算机系统，包括存储器、处理器及存储在所述存储器上并可在所述处理器上运行的计算机程序，所述计算器程序涉及的交易系统对各账户存储其对应的余额队列，所述余额队列包括按时间先后依次添加至队尾的若干密文余额，所述处理器执行所述计算机程序时实现如下步骤：从所述交易系统获取，所述第一账户所对应第一余额队列中的第一密文余额；确定交易金额以及作为支付目标的第二账户，并至少利用所述第一账户的公钥对交易金额进行同态加密，获得第一密文交易金额；向所述交易系统发送交易请求，其中包括所述第一账户、所述第二账户、所述第一密文余额以及所述第一密文交易金额，使所述交易系统在确认所述交易请求合法后，对所述第一余额队列进行第一更新，以及对所述第二账户对应的第二余额队列进行第二更新。

本说明书提供了一种交易系统，所述交易系统对各账户存储其对应的余额队列，所述

余额队列包括按时间先后依次添加至队尾的若干密文余额，所述交易系统包括：接收单元，配置为接收交易请求，其中包括第一账户、第二账户、第一密文余额，以及至少利用所述第一账户的公钥对交易金额进行同态加密得到的第一密文交易金额；响应单元，配置为响应于确认所述交易请求合法，执行第一更新和第二更新；所述第一更新包括：确定所述第一账户所对应第一余额队列队尾的密文余额与所述第一密文交易金额间的密文差值，将所述密文差值加入所述第一余额队列作为更新队尾，并删除所述第一余额队列中除所述更新队尾外的其它密文余额；所述第二更新包括：将所述第二账户所对应第二余额队列队尾的密文余额与第二密文交易金额间的密文和值添加至所述第二余额队列队尾，其中所述第二密文交易金额是对所述交易金额进行同态加密得到的，并且对于所述第二账户可解密。

本说明书提供了一种交易处理装置，所述装置涉及的交易系统对各账户存储其对应的余额队列，所述余额队列包括按时间先后依次添加至队尾的若干密文余额，所述装置部署于对应第一账户对应的终端，所述装置包括：获取单元，配置为从所述交易系统获取，所述第一账户所对应第一余额队列中的第一密文余额；配置单元，配置为确定交易金额以及作为支付目标的第二账户，并至少利用所述第一账户的公钥对交易金额进行同态加密，获得第一密文交易金额；发送单元，配置为向所述交易系统发送交易请求，其中包括所述第一账户、所述第二账户、所述第一密文余额以及所述第一密文交易金额，使所述交易系统在确认所述交易请求合法后，对所述第一余额队列进行第一更新，以及对所述第二账户对应的第二余额队列进行第二更新。

本说明书提供了一种计算机可读非易失性存储介质，所述存储介质存储有计算机程序，所述计算机程序被处理器执行时实现上述的交易处理方法。

本说明书实施例中采用的技术方案能够达到以下有益效果中的至少一项：交易系统对各账户存储其对应的余额队列，通过特定的队列更新策略来确保任意账户在当前时刻下持有相关资源的明文余额，不小于该账户所对应余额队列中按时间先后依次添加至队尾的任意密文余额所对应的明文余额；当期望从第一账户向第二账户转移前述资源时，则可以使用第一账户所对应第一余额队列中的任意密文余额来发起交易请求，交易系统对交易请求进行合法性验证时，只需要确认交易请求中所包括的密文余额属于第一余额队列，即可获知该交易请求不会导致第一账户发生余额透支，避免将该交易请求被错误的确定为未通过合法性验证的异常请求而并不对其正确处理，有利于交易系统更加准确的处理交易请求。

附图说明

为了更清楚地说明本说明书实施例的技术方案，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。

图 1 为本说明书实施例中所提供技术方案的技术场景示意图；

图 2 为本说明书实施例中提供的一种交易处理方法的流程图；

图 3 为本说明书实施例中提供的一种交易系统的结构示意图；

图 4 为本说明书实施例中提供的一种交易处理装置的结构示意图；

图 5 为本说明书实施例中提供的一种计算机系统的结构示意图。

具体实施方式

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说明书技术方案进行清楚、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，都属于本说明书保护的范围。

图 1 为本说明书实施例中所提供技术方案的技术场景示意图。参见图 1 所示，基于隐私保护的需要，用户注册在交易系统中的账户所持有某种资源的余额，可能并不以明文存储的存储方式直接存储于交易系统中，而是存储采用某种同态加密算法对明文余额加密得到的密文余额。例如，对用户 1、用户 2、用户 3、用户 4 依次注册在交易系统中的账户 A1、A2、A3 和 A4，账户 A1、A2、A3、A4 在某个时刻 t1 下实际持有资源 S1 的余额可能依次是 x11、x21、x31 和 x41，则交易系统中可能并不直接存储明文余额 x11、x21、x31 和 x41，而是存储采用某种同态加密算法和各相关账户公钥，对明文余额 x11、x21、x31 和 x41 进行同态加密后得到的密文余额 E（x11）、E（x21）、E（x31）和 E（x41）。

用户可以从交易系统中查询其注册的账户所持有某种资源的密文余额，通过该账户的私钥对密文余额进行解密即可获知明文余额；进而可以基于明文余额的大小向交易系统发起交易请求，实现将该账户所持有该资源的部分或全部余额转移给其它账户。示例性的，用户 1 可在 t1 时刻，通过终端从交易系统中查询到账户 A1 所持有资源 S1 的密文余额 E（x11），并利用账户 A1 的私钥 sk1 对密文余额 E（x11）进行解密，从而获知账户 A1 所持有资源 S1 的余额 x11；当确定出需要转移至其它账户如 A2 的交易金额为不小于 0 的 y1 之后，即可利用账户 A1 的公钥 pk1 对交易金额 y1 进行同态加密，获得密文交易金额 E（y1），并向交易系统发送交易请求 Q1，用于请求从账户 A1 向账户 A2 转移交易金额为 y1 的资源 S1，使交易系统对密文交易金额 E（y1）和密文余额 E（x11）进行相关同态运算，进而在

时刻 t1 之后的某个时刻 t2 完成将账户 A1 所持有资源 S1 的密文余额，由 E（x11）更新为 E（x11-y1），以及对应的将账户 A2 所持有资源 S1 的密文余额由 E（x21）更新为 E（x21+y1）。

因交易系统无法获知密文余额所对应的明文余额，同时又需要避免发生余额透支，交易系统在执行交易请求前，需要验证交易请求的合法性；只有在确认交易请求合法后，才会正确执行交易请求，最终实现按照交易请求的期望实现在相关账户间对资源进行转移。

在一种可能的实施方式中，对交易请求进行合法性验证时，交易系统需要验证其对发起交易请求的账户存储的密文余额，与交易请求中所包括的密文余额是否相同，如果不同则说明该交易请求可能导致发起交易请求的账户发生余额透支，该交易请求将会因未通过合法性验证而被确定为不会被正确执行的异常请求，导致该交易请求执行失败。

该实施方式中，对于部分并不会导致发起交易请求的账户发生余额透支的正常交易请求，同样可能被错误的确定为未通过合法性验证而执行失败，严重影响用户体验。

举例来说，假设用户 2 在 t3 时刻从交易系统查询到账户 A2 持有资源 S1 的密文余额为 E（x21+y1），在 t6 时刻通过账户 A2 和密文余额 E（x2+y1）发起交易请求 Q3，交易请求 Q3 用于请求从账户 A2 向账户 A4 转移交易金额为 y3 的资源 S1，其中交易金额 y3 不小于 0。除此之外，继续假设用户 3 在位于 t3 时刻与 t6 时刻之间的 t4 时刻，从交易系统查询到账户 A3 所持有资源 S1 的密文余额为 E（x31），交易系统在位于 t4 时刻与 t6 时刻之间的 t5 时刻，完成处理用户 3 通过账户 A3 和密文余额 E（x31）发起的交易请求 Q2，交易请求 Q2 用于请求从账户 A3 向账户 A2 转移交易金额为 y2 的资源 S1，交易请求 Q2 的成功处理将导致交易系统对账户 A2 存储的密文余额由 E（x21+y1）变更为 E（x21+y1+y2），以及导致账户 A3 的密文余额由 E（X31）更新为 E（x31-y2），其中 y2 不小于 0。此种情况下，交易请求 Q3 中账户 A2 的密文余额 E（x21+y1）所对应明文余额 x21+y1，小于交易系统在 t6 时刻对账户 A2 存储的密文余额 E（x21+y1+y2）所对应明文余额 x21+y1+y2，即交易请求 Q3 并不会导致账户 A2 发生余额透支；然而，交易系统却会因交易请求 Q2 所包括的密文余额 E（x21+y1），不同于交易系统在当前时刻下对账户 A2 存储的密文余额 E（x21+y1+y2），确认交易请求 Q3 未通过合法性验证，交易请求 Q3 将发生执行失败。

鉴于此，本说明书实施例中提供了一种交易处理方法、装置、交易系统、存储介质和计算机系统。交易系统对各账户存储其对应的余额队列，通过特定的队列更新策略来确保任意账户在当前时刻下持有相关资源的明文余额，不小于该账户所对应余额队列中按时间先后依次添加至队尾的任意密文余额所对应的明文余额；当期望从第一账户向第二账户转移前述资源时，则可以使用第一账户所对应第一余额队列中的任意密文余额来发起交易请

求，交易系统对交易请求进行合法性验证时，只需要确认交易请求中所包括的密文余额属于第一余额队列，即可确认该交易请求不会导致第一账户发生余额透支，避免将该交易请求错误的确定为未通过合法性验证的异常请求而执行失败，同时有利于提高用户体验。

前述交易系统可以管理一种或多种资源；其中前述的资源可以是各种可能的合法货币或者各种可能的合法数字资源。对于交易系统管理的任意资源（记为资源 S1）而言，交易系统可以对注册在交易系统中的多个账户存储其各自对应的余额队列。对于交易系统中所存储的任意余额队列，该余额队列中包括按时间先后依次添加至队尾的若干密文余额；该若干密文余额中的任意密文余额，其对该余额队列所对应的账户可解密，即可以使用该余额队列所对应账户的私钥正确解密出属于该余额队列的任意密文余额所对应的明文余额。

前述交易系统可以包括中心化的商品交易或资产管理平台，或者也可以包括去中心化的区块链系统。当前述交易系统包括区块链系统的情况下，该区块链系统中可以部署一个或多个智能合约，一个智能合约用于管理一种或多种资源；对通过该一个或多个智能合约管理的任意资源 S1 而言，如果注册在区块链系统中的任意账户持有资源 S1，则用于管理资源 S1 的智能合约的合约状态中，可以存储与该账户以及资源 S1 对应的余额队列。

下面结合图 1 所示的技术场景，详细描述本说明书实施例中提供的交易处理方法。

图 2 为本说明书实施例中提供的一种交易处理方法的流程图。该方法示例性描述了通过终端与交易系统进行信息交互，实现从第一账户向第二账户转移资源 S1 的过程。

如前所述，该交易系统中可以对多个账户存储其各自对应的余额队列，该多个账户中包括前述的第一账户和第二账户。需要说明的是，该多个账户各自对应的余额队列可以对应相同种类的资源（记为资源 S1），例如对应相同种类的货币或者数字资源，等等。

参照图 2 所示，该方法可以包括但不限于如下步骤 S201~步骤 S209 中的部分或全部。

当持有第一账户的第一用户期望从第一账户向交易系统中的其它账户，转移第一账户所持有的部分或全部资源 S1 时，第一用户可以触发终端执行如下步骤 S201~步骤 S205。

步骤 S201，从交易系统获取，第一账户所对应第一余额队列中的第一密文余额。

终端可以向交易系统发送包含第一账户的余额查询请求。交易系统可以根据余额查询请求中所包括的第一账户，向终端返回当前时刻下对第一账户存储的第一余额队列，进而由第一用户从终端向其呈现的第一余额队列中选择一个密文余额作为第一密文余额；或者交易系统也可以根据余额查询请求中所包括的第一账户，按照某种预设策略，从当前时刻下对第一账户存储的第一余额队列中，选择一个密文余额作为第一密文余额并返回给终端。

当交易系统包括区块链系统，而且该区块链系统中部署有用于管理资源 S1 的智能合

约，该智能合约的合约状态中对持有资源 S1 的多个账户存储其各自对应的余额队列的情况下，余额查询请求例如可以包括用于调用该智能合约中第二函数的第二交易。与之相应的，作为一种优选实施方式，区块链系统中的区块链节点可以根据该第二交易执行该智能合约中的第二函数，实现根据第一账户，将位于第一余额队列队首的密文余额确定为第一密文余额，并将该第一密文余额返回给终端。其中，将位于第一余额队列队首的密文余额作为第一密文余额返回给终端的有益效果，将在下文中详细分析而未在此处具体陈述。

步骤 S203，确定交易金额以及作为支付目标的第二账户，并至少利用第一账户的公钥对交易金额进行同态加密，获得第一密文交易金额。

下面以第一账户是前述的账户 A1，第二账户是前述的账户 A2，第一密文余额是前述的密文余额 E（x11），交易金额是前述的交易金额 y1 为例进行示例性描述。

终端可利用账户 A1 的私钥 sk1，对密文余额 E（x11）进行解密，获得对应的明文余额 x11 并呈现给持有账户 A1 的用户 1。用户 1 可根据实际业务需要，向终端提供期望接收资源 S1 的账户 A2 以及交易金额 y1，其中 y1 应当不小于 0 且不大于明文余额 x11。终端则可以至少利用账户 A1 的公钥 pk1 对交易金额 y1 进行同态加密，获得第一密文交易金额。

终端可利用账户 A1 的公钥 pk1 对交易金额 y1 进行同态加密，获得对账户 A1 可解密的第一密文交易金额 E（pk1，y1）。此种情况下，终端还可以利用账户 A2 的公钥 pk2 对交易金额 y1 进行同态加密，获得对账户 A2 可解密的第二密文交易金额 E（pk2，y1）。

或者，终端可以利用账户 A1 的公钥 pk1 和账户 A2 的公钥 pk2 对交易金额 y1 进行同态加密，获得对账户 A1 和账户 A2 均可解密的组合密文 E（pk1，pk2，y1）。该组合密文即为前述至少利用第一账户的公钥对交易金额进行同态加密，获得的第一密文交易金额。

对交易金额进行同态加密时所使用的同态加密算法可以是仅满足加法同态的部分同态加密算法，或者也可以是同时满足加法同态和乘法同态的全同态加密算法，例如基于椭圆曲线的 ElGamal 加密算法以及其变体，在此并不对其做任何限制。

步骤 S205，向交易系统发送交易请求，其中至少包括第一账户、第二账户、第一密文余额以及第一密文交易金额。

接续前文的示例，第一密文交易金额可以是对第一账户和第二账户均可解密的组合密文。或者，第一密文交易金额是仅对第一账户可解密的 E（pk1，y1），此种情况下终端向交易系统发送的交易请求中还包括仅对第二账户可解密的第二密文交易金额 E（pk2，y1）。

交易请求中，还可以包括终端利用第一密文余额生成的第一零知识证明$proof_1$，用于向交易系统证明第一密文余额与第一密文交易金额间的明文差值不小于 0，即证明第一密

文余额对应的明文余额，不小于第一密文交易金额对应的明文交易金额。

交易请求中，还可以包括终端利用第一密文交易金额生成的第二零知识证明$proof_2$，用于向交易系统证明第一密文交易金额对应的明文交易金额不小于 0。

当交易请求中同时包括仅对第一账户可解密的第一密文交易金额以及仅对第二账户可解密的第二密文交易金额的情况下：交易请求中，还可以包括由终端生成的第三零知识证明$proof_3$，用于向交易系统证明，第一密文交易金额和第二密文交易金额是对作为隐私数据的相同交易金额进行同态加密得到的。

当交易请求中同时包括仅对第一账户可解密的第一密文交易金额以及仅对第二账户可解密的第二密文交易金额的情况下：交易请求中，还可以包括由终端生成的第四零知识证明$proof_4$，用于向交易系统证明，第二密文交易金额是根据第二账户的公钥 pk2 对作为隐私数据的明文交易金额进行同态加密得到的。

当交易请求中所包括的第一密文交易金额为对第一账户和第二账户均可解密的组合密文的情况下：交易请求中，还可以包括由终端生成的第五零知识证明$proof_5$，用于向交易系统证明，利用第一账户的私钥 sk1 对第一密文交易金额解密得到的明文交易金额，相同于利用第二账户的私钥 sk2 对第一密文交易金额解密得到的明文交易金额。

当交易系统包括区块链系统，该区块链系统中部署有用于管理资源 S1 的智能合约的情况下，交易请求可以包括用于调用该智能合约中第一函数的第一交易。其中该第一交易的发起方（from）字段包括第一账户，接收方（to）字段包括该智能合约的合约地址，数据（data）字段至少包括第一函数的标识信息、第一密文余额以及第一密文交易金额。除此之外，在第一交易的 data 字段还可以包括，前文所述的第二密文交易金额、第一零知识证明$proof_1$、第二零知识证明$proof_2$、第三零知识证明$proof_3$、第四零知识证明$proof_4$以及第五零知识证明$proof_5$等各项信息中的一项或多项。

交易系统在接收到来自终端的交易请求后，将会对该交易请求的合法性进行验证。

即，交易系统会执行如下步骤 S207，验证交易请求是否合法。

合法性验证过程中，至少需要执行验证项 1：确认交易请求中所包括的第一密文余额是否属于第一余额队列；如果是则验证项 1 通过验证。除此之外，依赖于交易请求中所包括的其它具体内容，合法性验证过程还可能需要执行如下示例的一个或多个验证项。

当交易请求中包括第一零知识证明$proof_1$的情况下，还需要执行验证项 2：根据第一零知识证明$proof_1$，验证第一密文余额与第一密文交易金额间对应的明文差值是否不小于 0；如果是则确认验证项 2 通过验证。

当交易请求中包括第二零知识证明$proof_2$的情况下，还需要执行验证项 3，根据第二零知识证明$proof_2$，确认交易金额是否不小于 0；如果是则验证项 3 通过验证。

当交易请求中包括第三零知识证明$proof_3$的情况下，还需要执行验证项 4，根据第三零知识证明$proof_3$，确认第一密文交易金额和第二密文交易金额是对作为隐私数据的相同交易金额进行同态加密得到的；如果是则确认验证项 4 通过验证。

当交易请求中包括第四零知识证明$proof_4$的情况下，还需要执行验证项 5，根据第四零知识证明$proof_4$，确认第二密文交易金额是否是根据第二账户的公钥对作为隐私数据的交易金额进行同态加密得到的；如果是则确认验证项 5 通过验证。

当交易请求中包括第五零知识证明$proof_5$的情况下，还需要执行验证项 6，根据第五零知识证明$proof_5$，确认利用第一账户的私钥对第一密文交易金额解密得到的交易金额，是否相同于利用第二账户的私钥对第一密文交易金额解密得到的交易金额，如果是则确认验证项 6 通过验证。

当交易系统需要对交易请求执行的全部验证项均通过验证的情况下，即当交易系统确认第一密文余额属于第一账户对应的第一余额队列，并且交易请求中所包括的各个零知识证明均通过验证的情况下，确认该交易请求的合法性通过验证，可接着执行如下步骤 S209。

步骤 S209，交易系统执行第一更新和第二更新；其中，第一更新包括：确定第一账户所对应第一余额队列队尾的密文余额与第一密文交易金额间的密文差值，将密文差值加入第一余额队列作为更新队尾，并删除第一余额队列中除更新队尾外的其它密文余额；第二更新包括：将第二账户所对应第二余额队列队尾的密文余额与第二密文交易金额间的密文和值添加至第二余额队列队尾，其中第二密文交易金额是对交易金额进行同态加密得到的，并且对于第二账户可解密。

当交易系统包括区块链系统，该区块链系统中部署有用于管理资源 S1 的智能合约的情况下，交易请求包括用于调用该智能合约中第一函数的第一交易的情况下，前述的步骤 S207 和步骤 S209 可以由区块链系统中的区块链节点执行。更具体地说，区块链节点可以根据第一交易执行该智能合约中的第一函数，从而实现前述步骤 S207 和步骤 S209。

下面示例性描述在处理交易请求的过程中执行第一更新和第二更新的具体过程。

接续前文的示例，请继续参见图 1 所示。

交易请求 Q1 用于请求从账户 A1 向账户 A2 转移交易金额为 y1 的资源 S1。交易系统在开始执行交易请求 Q1 时，账户 A1 对应的第一余额队列为[E(x11)]，账户 A2 对应的第二余额队列为[E(x21)]。交易系统在执行第一更新的过程中，可确定余额队列[E(x11)]队尾

的密文余额 E(x11)与第一密文交易金额间的密文差值 E(x11-y1)，将密文差值 E(x11-y1)添加至余额队列[E(x11)]队尾，形成 E(x11-y1)被作为更新队尾的余额队列[E(x11)，E(x11-y1)]，进而删除该余额队列[E(x11)，E(x11-y1)]中除更新队尾 E(x11-y1)外的其余密文余额，最终使账户 A1 对应的余额队列由[E(x11)]更新为 [E(x11-y1)]；交易系统在执行第二更新的过程中，可确定余额队列[E(x21)]队尾的密文余额 E(x21)与第一密文交易金额间的密文和值 E(x21+y1)，将密文和值 E(x21+y1)添加至[E(x21)]队尾，最终使账户 A2 对应的余额队列由[E(x21)]更新为 [E(x21)，E(x21+y1)]。换而言之，交易系统在 t2 时刻完成执行交易请求 Q1 后，对账户 A1 存储余额队列 E(x11-y1)，对账户 A2 存储余额队列[E(x21)，E(x21+y1)]。

交易请求 Q2 用于请求从账户 A3 向账户 A2 转移交易金额为 y2 的资源 S1。与交易请求 Q1 的处理过程相似，交易系统在开始执行交易请求 Q1 时，账户 A3 对应的余额队列为[E(x31)]，账户 A2 对应的余额队列为[E(x21)，E（x21+y1）]。执行交易请求 Q2 的过程中，将会通过执行第一更新，将对账户 A3 存储的余额队列由[E(x31)]更新为 [E(x31-y2)]，以及通过执行第二更新，将对账户 A2 存储的余额队列由[E(x21)，E(x21+y1)]更新为[E(x21)，E(x21+y1)，E(x21+y1+y2)]。即，交易系统在 t5 时刻完成执行交易请求 Q2 后，对账户 A3 存储余额队列[E(x31-y2)]，对账户 A2 存储余额队列[E(x21)，E(x21+y1)，E(x21+y1+y2)]。

交易请求 Q3 用于请求从账户 A2 向账户 A4 转移交易金额为 y3 的资源 S1。用户 2 在位于 t2 时刻之后的 t3 时刻从交易系统查询的第一密文余额，既可以是账户 A2 在 t3 时刻下实际持有资源 S1 的明文余额 x21+y1 所对应的密文余额 E（x21+y1），也可以是账户 A2 在 t3 时刻下所对应余额队列中的其它密文余额例如[E(x21)]。当交易系统在位于 t6 时刻之后的某个时刻开始处理交易请求 Q2 时，账户 A2 对应的余额队列为[E(x21)，E(x21+y1)，E(x21+y1+y2)]，账户 A4 对应的余额队列为[E(x41)。与交易请求 Q1 的处理过程相似，执行交易请求 Q3 的过程中，将会通过执行第一更新，将对账户 A2 存储的余额队列由[E(x21)，E(x21+y1)，E(x21+y1+y2)]更新为[E(x21+y1+y2-y3)]，以及通过执行第二更新，将对账户 A4 存储的余额队列由[E(x41)]更新为[E(x41)， E(x41+y3)]。即，完成执行交易请求 Q3 后，对账户 A2 存储余额队列[E(x21+y1+y2-y3)]，对账户 A4 存储余额队列[E(x41)，E(x41+y3)]。

通过前述示例的过程可以确保，交易系统对任意账户所持有相关资源存储的余额队列中，位于余额队列队尾的密文余额所对应明文余额，即是对应账户在当前时刻下实际持有相关资源的余额；余额队列队尾的密文余额所对应的明文余额，不小于该余额队列中的其它任意密文余额所对应的明文余额。如此，交易系统仅需要验证由某个账户发起的交易请求所使用的密文余额，属于该账户对应的余额队列，即可确认该交易请求不会导致该账户

发生余额透支，避免交易系统错误的将该交易请求确认为未通过合法性验证的异常请求。

当交易系统包括区块链系统的情况下，区块链系统中的区块链节点还可以响应于区块链系统生成任意第 k 个区块，从余额队列中删除位于目标密文余额之前的其它密文余额，目标密文余额是因执行属于前 k 个区块的交易而最晚加入余额队列队尾的密文余额。如此可避免区块链系统在连续的多个区块内，因执行用于向同一个账户转移相同资源例如资源 S1 的多个第一交易而导致该账户所对应余额队列的长度过大。示例性的，请继续参照图 1 所示，此处假设，区块链系统在 t2 时刻之后生成了区块高度为 k 的区块，在 t3 时刻之前仍未生成去区块高度为 k+1 的下一个区块，即区块链系统可能在 t2 时刻与 t3 时刻之间的某个时刻 t7 生成了区块 k，那么对于区块链系统在 t7 时刻对账户 A2 存储的余额队列[E(x21)，E(x21+y1)]，因执行属于前 k 个区块的交易而最晚加入账户 A2 所对应余额队列的目标密文余额则是 E(x21+y1)，因此可以对余额队列[E(x21)，E(x21+y1)]中位于目标密文余额 E(x21+y1)之前的其它密文余额如 E(x21)作删除处理，即区块链系统中的区块链节点可能在 t7 时刻之后实施将账户 A2 对应的余额队列由[E(x21)，E(x21+y1)]更新为 E(x21+y1)。

当交易系统包括区块链系统的情况下，在区块链系统生成任意区块 k 后，在区块链节点生成区块 k+1 前，任意账户所对应余额队列的队首可能是因执行属于前 k 个区块的交易而最晚添加到该余额队列中的，除队首外的其它密文余额则可能是因执行属于第 k+1 个区块的交易而添加到该余额队列中的；其中需要注意的是除队首外的其它密文余额，可能因属于第 k+1 个区块的相关交易因故重新执行（例如并行执行具有时间先后顺序的多个第一交易之后，发现部分第一交易存在冲突而需要对该部分第一交易按照时间顺序重新执行）而发生变更。因此，回看前文，当交易系统包括区块链系统的情况下，将位于第一余额队列队首的密文余额作为第一密文余额，可以避免因第一余额队列中除队首外的密文余额因故发生变更后，导致未能使用正确的并且属于第一余额队列的密文余额来发起交易请求。

与前述方法实施例基于相同的构思，本说明书实施例中提供了一种交易系统 300，所述交易系统 300 对各账户存储其对应的余额队列，所述余额队列包括按时间先后依次添加至队尾的若干密文余额。参照图 3 所示，所述交易系统 300 包括：接收单元 301，配置为接收交易请求，其中包括第一账户、第二账户、第一密文余额，以及至少利用所述第一账户的公钥对交易金额进行同态加密得到的第一密文交易金额；响应单元 303，配置为响应于确认所述交易请求合法，执行第一更新和第二更新；所述第一更新包括：确定所述第一账户所对应第一余额队列队尾的密文余额与所述第一密文交易金额间的密文差值，将所述密文差值加入所述第一余额队列作为更新队尾，并删除所述第一余额队列中除所述更新队

尾外的其它密文余额；所述第二更新包括：将所述第二账户所对应第二余额队列队尾的密文余额与第二密文交易金额间的密文和值添加至所述第二余额队列队尾，其中所述第二密文交易金额是对所述交易金额进行同态加密得到的，并且对于所述第二账户可解密。

与前述方法实施例基于相同的构思，本说明书实施例中提供了一种交易处理装置 400，所述装置 400 涉及的交易系统对各账户存储其对应的余额队列，所述余额队列包括按时间先后依次添加至队尾的若干密文余额，所述装置 400 部署于对应第一账户对应的终端。参照图 4 所示，所述装置 400 包括：获取单元 401，配置为从所述交易系统获取，所述第一账户所对应第一余额队列中的第一密文余额；配置单元 403，配置为确定交易金额以及作为支付目标的第二账户，并至少利用所述第一账户的公钥对交易金额进行同态加密，获得第一密文交易金额；发送单元 405，配置为向所述交易系统发送交易请求，其中包括所述第一账户、所述第二账户、所述第一密文余额以及所述第一密文交易金额，使所述交易系统在确认所述交易请求合法后，对所述第一余额队列进行第一更新，以及对所述第二账户对应的第二余额队列进行第二更新。

为了描述的方便，描述以上装置时以功能分为各种单元/模块分别描述。当然，在实施本说明书时可以把各模块/单元的功能在同一个或多个软件和/或硬件中实现。

The specification also provides a computer-readable non-transitory storage medium, wherein the storage medium stores a computer program, which, when executed by a processor, can be used to perform one or more steps of one or more methods described or illustrated herein or provides functionality described or illustrated herein. Herein, the computer-readable non-transitory storage medium or media may include one or more semiconductor-based or other integrated circuits (ICs) (such, as for example, field-programmable gate arrays (FPGAs) or application-specific ICs (ASICs)), hard disk drives (HDDs), hybrid hard drives (HHDs), optical discs, optical disc drives (ODDs), magneto-optical discs, magneto-optical drives, floppy diskettes, floppy disk drives (FDDs), magnetic tapes, solid-state drives (SSDs), RAM-drives, SECURE DIGITAL cards or drives, any other suitable computer-readable non-transitory storage media, or any suitable combination of two or more of these, where appropriate. A computer-readable non-transitory storage medium may be volatile, non-volatile, or a combination of volatile and non-volatile, where appropriate.

The specification also provides a computer system. FIG. 5 illustrates an example computer system 1000. In particular embodiments, one or more computer systems 1000 perform one or more steps of one or more methods described or illustrated herein. In particular embodiments,

one or more computer systems 1000 provide functionality described or illustrated herein. In particular embodiments, software running on one or more computer systems 1000 performs one or more steps of one or more methods described or illustrated herein or provides functionality described or illustrated herein. Particular embodiments include one or more portions of one or more computer systems 1000. Herein, reference to a computer system may encompass a computing device, and vice versa, where appropriate. Moreover, reference to a computer system may encompass one or more computer systems, where appropriate.

This disclosure contemplates any suitable number of computer systems 1000. This disclosure contemplates computer system 1000 taking any suitable physical form. As example and not by way of limitation, computer system 1000 may be an embedded computer system, a system-on-chip (SOC), a single-board computer system (SBC) (such as, for example, a computer-on-module (COM) or system-on-module (SOM)), a desktop computer system, a laptop or notebook computer system, an interactive kiosk, a mainframe, a mesh of computer systems, a mobile telephone, a personal digital assistant (PDA), a server, a tablet computer system, or a combination of two or more of these. Where appropriate, computer system 1000 may include one or more computer systems 1000; be unitary or distributed; span multiple locations; span multiple machines; span multiple data centers; or reside in a cloud, which may include one or more cloud components in one or more networks. Where appropriate, one or more computer systems 1000 may perform without substantial spatial or temporal limitation one or more steps of one or more methods described or illustrated herein. As an example and not by way of limitation, one or more computer systems 1000 may perform in real time or in batch mode one or more steps of one or more methods described or illustrated herein. One or more computer systems 1000 may perform at different times or at different locations one or more steps of one or more methods described or illustrated herein, where appropriate.

In particular embodiments, computer system 1000 includes a processor 1002, memory 1004, storage 1006, an input/output (I/O) interface 1008, a communication interface 1010, and a bus 1012. Although this disclosure describes and illustrates a particular computer system having a particular number of particular components in a particular arrangement, this disclosure contemplates any suitable computer system having any suitable number of any suitable components in any suitable arrangement.

In particular embodiments, processor 1002 includes hardware for executing instructions, such as those making up a computer program. As an example and not by way of limitation, to execute instructions, processor 1002 may retrieve (or fetch) the instructions from an internal register, an internal cache, memory 1004, or storage 1006; decode and execute them; and then

write one or more results to an internal register, an internal cache, memory 1004, or storage 1006. In particular embodiments, processor 1002 may include one or more internal caches for data, instructions, or addresses. This disclosure contemplates processor 1002 including any suitable number of any suitable internal caches, where appropriate. As an example and not by way of limitation, processor 1002 may include one or more instruction caches, one or more data caches, and one or more translation lookaside buffers (TLB s). Instructions in the instruction caches may be copies of instructions in memory 1004 or storage 1006, and the instruction caches may speed up retrieval of those instructions by processor 1002. Data in the data caches may be copies of data of 80 in memory 1004 or storage 1006 for instructions executing at processor 1002 to operate on; the results of previous instructions executed at processor 1002 for access by subsequent instructions executing at processor 1002 or for writing to memory 1004 or storage 1006; or other suitable data. The data caches may speed up read or write operations by processor 1002. The TLBs may speed up virtual-address translation for processor 1002. In particular embodiments, processor 1002 may include one or more internal registers for data, instructions, or addresses. This disclosure contemplates processor 1002 including any suitable number of any suitable internal registers, where appropriate. Where appropriate, processor 1002 may include one or more arithmetic logic units (ALUs); be a multi-core processor; or include one or more processors 1002. Although this disclosure describes and illustrates a particular processor, this disclosure contemplates any suitable processor.

In particular embodiments, memory 1004 includes main memory for storing instructions for processor 1002 to execute or data for processor 1002 to operate on. As an example and not by way of limitation, computer system 1000 may load instructions from storage 1006 or another source (such as, for example, another computer system 1000) to memory 1004. Processor 1002 may then load the instructions from memory 1004 to an internal register or internal cache. To execute the instructions, processor 1002 may retrieve the instructions from the internal register or internal cache and decode them. During or after execution of the instructions, processor 1002 may write one or more results (which may be intermediate or final results) to the internal register or internal cache. Processor 1002 may then write one or more of those results to memory 1004. In particular embodiments, processor 1002 executes only instructions in one or more internal registers or internal caches or in memory 1004 (as opposed to storage 1006 or elsewhere) and operates only on data in one or more internal registers or internal caches or in memory 1004 (as opposed to storage 1006 or elsewhere). One or more memory buses (which may each include an address bus and a data bus) may couple processor 1002 to memory 1004. Bus 1012 may include one or more memory buses, as described below. In particular embodiments, one or more memory

management units (MMUs) reside between processor 1002 and memory 1004 and facilitate accesses to memory 1004 requested by processor 1002. In particular embodiments, memory 1004 includes random access memory (RAM). This RAM may be volatile memory, where appropriate. Where appropriate, this RAM may be dynamic RAM (DRAM) or static RAM (SRAM). Moreover, where appropriate, this RAM may be single-ported or multi-ported RAM. This disclosure contemplates any suitable RAM. Memory 1004 may include one or more memories 1004, where appropriate. Although this disclosure describes and illustrates particular memory, this disclosure contemplates any suitable memory.

In particular embodiments, storage 1006 includes mass storage for data or instructions. As an example and not by way of limitation, storage 1006 may include a hard disk drive (HDD), a floppy disk drive, flash memory, an optical disc, a magneto-optical disc, magnetic tape, or a Universal Serial Bus (USB) drive or a combination of two or more of these. Storage 1006 may include removable or non-removable (or fixed) media, where appropriate. Storage 1006 may be internal or external to computer system 1000, where appropriate. In particular embodiments, storage 1006 is non-volatile, solid-state memory. In particular embodiments, storage 1006 includes read-only memory (ROM). Where appropriate, this ROM may be mask-programmed ROM, programmable ROM (PROM), erasable PROM (EPROM), electrically erasable PROM (EEPROM), electrically alterable ROM (EAROM), or flash memory or a combination of two or more of these. This disclosure contemplates mass storage 1006 taking any suitable physical form. Storage 1006 may include one or more storage control units facilitating communication between processor 1002 and storage 1006, where appropriate. Where appropriate, storage 1006 may include one or more storages 1006. Although this disclosure describes and illustrates particular storage, this disclosure contemplates any suitable storage.

In particular embodiments, I/O interface 1008 includes hardware, software, or both, providing one or more interfaces for communication between computer system 1000 and one or more I/O devices. Computer system 1000 may include one or more of these I/O devices, where appropriate. One or more of these I/O devices may enable communication between a person and computer system 1000. As an example and not by way of limitation, an I/O device may include a keyboard, keypad, microphone, monitor, mouse, printer, scanner, speaker, still camera, stylus, tablet, touch screen, trackball, video camera, another suitable I/O device or a combination of two or more of these. An I/O device may include one or more sensors. This disclosure contemplates any suitable I/O devices and any suitable I/O interfaces 1008 for them. Where appropriate, I/O interface 1008 may include one or more device or software drivers enabling processor 1002 to drive one or more of these I/O devices. I/O interface 1008 may include one or more I/O

interfaces 1008, where appropriate. Although this disclosure describes and illustrates a particular I/O interface, this disclosure contemplates any suitable I/O interface.

In particular embodiments, communication interface 1010 includes hardware, software, or both providing one or more interfaces for communication (such as, for example, packet-based communication) between computer system 1000 and one or more other computer systems 1000 or one or more networks. As an example and not by way of limitation, communication interface 1010 may include a network interface controller (NIC) or network adapter for communicating with an Ethernet or other wire-based network or a wireless NIC (WNIC) or wireless adapter for communicating with a wireless network, such as a WI-FI network. This disclosure contemplates any suitable network and any suitable communication interface 1010 for it. As an example and not by way of limitation, computer system 1000 may communicate with an ad hoc network, a personal area network (PAN), a local area network (LAN), a wide area network (WAN), a metropolitan area network (MAN), or one or more portions of the Internet or a combination of two or more of these. One or more portions of one or more of these networks may be wired or wireless. As an example, computer system 1000 may communicate with a wireless PAN (WPAN) (such as, for example, a BLUETOOTH WPAN), a WI-FI network, a WI-MAX network, a cellular telephone network (such as, for example, a Global System for Mobile Communications (GSM) network), or other suitable wireless network or a combination of two or more of these. Computer system 1000 may include any suitable communication interface 1010 for any of these networks, where appropriate. Communication interface 1010 may include one or more communication interfaces 1010, where appropriate. Although this disclosure describes and illustrates a particular communication interface, this disclosure contemplates any suitable communication interface.

In particular embodiments, bus 1012 includes hardware, software, or both coupling components of computer system 1000 to each other. As an example and not by way of limitation, bus 1012 may include an Accelerated Graphics Port (AGP) or other graphics bus, an Enhanced Industry Standard Architecture (EISA) bus, a front-side bus (FSB), a HYPERTRANSPORT (HT) interconnect, an Industry Standard Architecture (ISA) bus, an INFINIBAND interconnect, a low-pin-count (LPC) bus, a memory bus, a Micro Channel Architecture (MCA) bus, a Peripheral Component Interconnect (PCI) bus, a PCI-Express (PCIe) bus, a serial advanced technology attachment (SATA) bus, a Video Electronics Standards Association local (VLB) bus, or another suitable bus or a combination of two or more of these. Bus 1012 may include one or more buses 1012, where appropriate. Although this disclosure describes and illustrates a particular bus, this disclosure contemplates any suitable bus or interconnect.

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。

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。

以上所述仅为本说明书的实施例而已，并不用于限制本说明书。对于本领域技术人员来说，本说明书可以有各种更改和变化。凡在本说明书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

1．一种交易处理方法，由交易系统执行，所述交易系统对各账户存储其对应的余额队列，所述余额队列包括按时间先后依次添加至队尾的若干密文余额，所述方法包括：

接收交易请求，其中包括第一账户、第二账户、第一密文余额，以及至少利用所述第一账户的公钥对交易金额进行同态加密得到的第一密文交易金额；

响应于确认所述交易请求合法，执行第一更新和第二更新；其中，

所述第一更新包括：确定所述第一账户所对应第一余额队列队尾的密文余额与所述第一密文交易金额间的密文差值，将所述密文差值加入所述第一余额队列作为更新队尾，并删除所述第一余额队列中除所述更新队尾外的其它密文余额；

所述第二更新包括：将所述第二账户所对应第二余额队列队尾的密文余额与第二密文交易金额间的密文和值添加至所述第二余额队列队尾，其中所述第二密文交易金额是对所述交易金额进行同态加密得到的，并且对于所述第二账户可解密。

2．根据权利要求 1 所述的方法，所述确认所述交易请求合法，包括：确认所述第一密文余额属于所述第一余额队列。

3．根据权利要求 1 所述的方法，所述交易请求还包括第一零知识证明；其中，所述确认所述交易请求合法，还包括：基于所述第一零知识证明，验证所述第一密文余额与所述第一密文交易金额间对应的明文差值不小于 0。

4．根据权利要求 1 所述的方法，所述交易请求还包括第二零知识证明；其中，所述确认所述交易请求合法，还包括：根据所述第二零知识证明，验证所述交易金额不小于 0。

5．根据权利要求 1 所述的方法，所述交易请求还包括所述第二密文交易金额，所述第二密文交易金额是利用所述第二账户的公钥对所述交易金额进行同态加密得到的。

6．根据权利要求 5 所述的方法，所述交易请求还包括第三零知识证明；其中，所述确认所述交易请求合法，还包括：根据所述第三零知识证明，验证所述第一密文交易金额和所述第二密文交易金额是对作为隐私数据的相同交易金额进行同态加密得到的。

7．根据权利要求 5 所述的方法，所述交易请求还包括第四零知识证明；其中，所述确认所述交易请求合法，还包括：根据所述第四零知识证明，验证所述第二密文交易金额是根据所述第二账户的公钥对作为隐私数据的交易金额进行同态加密得到的。

8．根据权利要求 1 所述的方法，所述第一密文交易金额是利用所述第一账户的公钥和所述第二账户的公钥对所述交易金额进行同态加密得到的组合密文；其中，所述第二密文交易金额为所述第一密文交易金额。

9．根据权利要求 8 所述的方法，所述交易请求还包括第五零知识证明；其中，所述确认所述交易请求合法，还包括：根据所述第五零知识证明，验证利用所述第一账户的私钥对所述第一密文交易金额解密得到的交易金额，相同于利用所述第二账户的私钥对所述第一密文交易金额解密得到的交易金额。

10．根据权利要求 1-9 中任一项所述的方法，所述交易系统包括部署有智能合约的区块链系统，所述方法由所述区块链系统中的区块链节点执行；所述余额队列存储于所述智能合约的合约状态中，所述交易请求包括用于调用所述智能合约中第一函数的第一交易。

11．根据权利要求 10 所述的方法，所述方法还包括：响应于所述区块链系统生成任意第 k 个区块，从所述余额队列中删除位于目标密文余额之前的其它密文余额，所述目标密文余额是因执行属于前 k 个区块的交易而最晚加入所述余额队列队尾的密文余额。

12．根据权利要求 11 所述的方法，所述方法还包括：

从终端接收用于调用所述智能合约中第二函数的第二交易，其中包括所述第一账户；

根据所述第二交易执行所述第二函数，实现根据所述第一账户，将位于所述第一余额队列队首的密文余额确定为第一密文余额；

向所述终端发送所述第一密文余额，使所述终端发起所述交易请求。

13．一种交易处理方法，所述方法涉及的交易系统对各账户存储其对应的余额队列，所述余额队列包括按时间先后依次添加至队尾的若干密文余额，所述方法通过第一账户对应的终端执行，所述方法包括：

从所述交易系统获取，所述第一账户所对应第一余额队列中的第一密文余额；

确定交易金额以及作为支付目标的第二账户，并至少利用所述第一账户的公钥对交易金额进行同态加密，获得第一密文交易金额；

向所述交易系统发送交易请求，其中包括所述第一账户、所述第二账户、所述第一密文余额以及所述第一密文交易金额，使所述交易系统在确认所述交易请求合法后，对所述第一余额队列进行第一更新，以及对所述第二账户对应的第二余额队列进行第二更新。

14．一种计算机系统，包括存储器、处理器及存储在所述存储器上并可在所述处理器上运行的计算机程序，所述计算器程序用于实现交易系统，所述交易系统对各账户存储其对应的余额队列，所述余额队列包括按时间先后依次添加至队尾的若干密文余额，所述处理器执行所述计算机程序时实现如下步骤：

接收交易请求，其中包括第一账户、第二账户、第一密文余额，以及至少利用所述第一账户的公钥对交易金额进行同态加密得到的第一密文交易金额；

响应于确认所述交易请求合法，执行第一更新和第二更新；其中，

所述第一更新包括：确定所述第一账户所对应第一余额队列队尾的密文余额与所述第一密文交易金额间的密文差值，将所述密文差值加入所述第一余额队列作为更新队尾，并删除所述第一余额队列中除所述更新队尾外的其它密文余额；

所述第二更新包括：将所述第二账户所对应第二余额队列队尾的密文余额与第二密文交易金额间的密文和值添加至所述第二余额队列队尾，其中所述第二密文交易金额是对所述交易金额进行同态加密得到的，并且对于所述第二账户可解密。

15．一种计算机系统，包括存储器、处理器及存储在所述存储器上并可在所述处理器上运行的计算机程序，所述计算器程序涉及的交易系统对各账户存储其对应的余额队列，所述余额队列包括按时间先后依次添加至队尾的若干密文余额，所述处理器执行所述计算机程序时实现如下步骤：

从所述交易系统获取，所述第一账户所对应第一余额队列中的第一密文余额；

确定交易金额以及作为支付目标的第二账户，并至少利用所述第一账户的公钥对交易金额进行同态加密，获得第一密文交易金额；

向所述交易系统发送交易请求，其中包括所述第一账户、所述第二账户、所述第一密文余额以及所述第一密文交易金额，使所述交易系统在确认所述交易请求合法后，对所述第一余额队列进行第一更新，以及对所述第二账户对应的第二余额队列进行第二更新。

16．一种交易系统，所述交易系统对各账户存储其对应的余额队列，所述余额队列包括按时间先后依次添加至队尾的若干密文余额，所述交易系统包括：

接收单元，配置为接收交易请求，其中包括第一账户、第二账户、第一密文余额，以及至少利用所述第一账户的公钥对交易金额进行同态加密得到的第一密文交易金额；

响应单元，配置为响应于确认所述交易请求合法，执行第一更新和第二更新；其中，

所述第一更新包括：确定所述第一账户所对应第一余额队列队尾的密文余额与所述第一密文交易金额间的密文差值，将所述密文差值加入所述第一余额队列作为更新队尾，并删除所述第一余额队列中除所述更新队尾外的其它密文余额；

所述第二更新包括：将所述第二账户所对应第二余额队列队尾的密文余额与第二密文交易金额间的密文和值添加至所述第二余额队列队尾，其中所述第二密文交易金额是对所述交易金额进行同态加密得到的，并且对于所述第二账户可解密。

17．一种交易处理装置，所述装置涉及的交易系统对各账户存储其对应的余额队列，所述余额队列包括按时间先后依次添加至队尾的若干密文余额，所述装置部署于对应第一

账户对应的终端，所述装置包括：

获取单元，配置为从所述交易系统获取，所述第一账户所对应第一余额队列中的第一密文余额；

配置单元，配置为确定交易金额以及作为支付目标的第二账户，并至少利用所述第一账户的公钥对交易金额进行同态加密，获得第一密文交易金额；

发送单元，配置为向所述交易系统发送交易请求，其中包括所述第一账户、所述第二账户、所述第一密文余额以及所述第一密文交易金额，使所述交易系统在确认所述交易请求合法后，对所述第一余额队列进行第一更新，以及对所述第二账户对应的第二余额队列进行第二更新。

18．一种计算机可读非易失性存储介质，所述存储介质存储有计算机程序，所述计算机程序被处理器执行时实现上述权利要求 1-13 中任一项所述的方法。