

基于区块链的汇款方法及装置

技术领域

[01]本说明书一个或多个实施例涉及区块链技术领域，尤其涉及一种基于区块链的汇款方法及装置。

5 背景技术

[02]区块链是一种防篡改的、共享的数字化账本，用于记录公有或私有对等网络中的交易。交易经区块链的节点验证共识后被收录至账本，所述账本分发给网络中的所有或多数成员节点，在区块中永久记录网络中发生的资产交易的历史记录。现有的区块链资产交易模式分为两种，在 UTXO 模型下，一个交易输入只会被花费一次，而后生成新的交易输出，因此天然地具有高的交易并发性；而在账户模型下，同一个用户的每一笔交易都会更新同一个账户余额，为保证余额足够支付，一个用户的所有相关的交易需要按照一个全局的时序串行执行，否则交易会因为账户余额不足而被共识节点拒绝执行，因此账户模型下限制了并发交易的可能性。

发明内容

15 [03]有鉴于此，本说明书一个或多个实施例提供一种基于区块链的汇款方法及装置、电子设备及计算机可读存储介质。

[04]为实现上述目的，本说明书一个或多个实施例提供技术方案如下：

[05]根据本说明书一个或多个实施例的第一方面，提出了一种基于区块链的汇款方法，其中，汇出方账户包括一预备金列表；所述预备金列表包括基于汇出方账户的余额划分得到的多个预备金金额；

20 [06]所述方法包括：

[07]接收汇出方发送的用于向接收方汇款的第一交易，所述第一交易包括所述汇出方账户汇入接收方账户的汇款额，和所述汇出方从所述预备金列表中为所述第一交易分配的至少一个与所述汇款额对应的预备金金额；

[08]对所述第一交易进行第一交易验证,所述第一交易验证包括第一验证步骤,用以验证所述第一交易包括的预备金金额之和是否大于或者等于所述汇款额;如果是,所述第一交易通过所述第一验证步骤;

5 [09]如果所述第一交易通过所述第一交易验证,从所述汇出方账户的余额扣除所述汇款额,在接收方账户的余额增加所述汇款额。

[10]根据本说明书一个或多个实施例的第二方面,提出了一种基于区块链的汇款装置,其中,汇出方账户包括一预备金列表;所述预备金列表包括基于汇出方账户的余额划分得到的多个预备金金额;

[11]所述装置包括:

10 [12]接收单元,接收汇出方发送的用于向接收方汇款的第一交易,所述第一交易包括所述汇出方账户汇入接收方账户的汇款额,和所述汇出方从所述预备金列表中为所述第一交易分配的至少一个与所述汇款额对应的预备金金额;

15 [13]第一交易验证单元,对所述第一交易进行第一交易验证,所述第一交易验证单元包括第一验证模块,用以验证所述第一交易包括的预备金金额之和是否大于或者等于所述汇款额;

[14]账户更新单元,如果所述第一交易通过所述第一交易验证,从所述汇出方账户的余额扣除所述汇款额,在接收方账户的余额增加所述汇款额。

20 [15]根据本说明书一个或多个实施例的第三方面,提出了一种计算机设备,包括:存储器和处理器;所述存储器上存储有可由处理器运行的计算机程序;所述处理器运行所述计算机程序时,执行如上述基于区块链的汇款方法。

[16]根据本说明书一个或多个实施例的第四方面,提出了一种计算机可读存储介质,其上存储有计算机程序,所述计算机程序被处理器运行时,执行上述基于区块链的汇款方法所述的步骤

25 [17]本说明书提供的基于区块链的汇款方法及装置,基于账户余额生成多个预备金金额,并将多个预备金金额指定至多个汇款交易中;与现有的汇款交易是基于汇出方账户的账户余额进行交易是否足以支付的验证不同,本说明书提供的汇款方法中,区块链的节点是针对各个汇款交易所包括的预备金金额进行各个汇款交易是否足以支付的验证,对各个汇款交易的验证分别独立进行,不相互影响,从而使得基于账户模型构建的区块链可以并行发送多个汇款交易。

附图说明

[18]图 1 是一示例性实施例提供的一种基于区块链的汇款方法的流程图。

[19]图 2 是一示例性实施例提供的一种在区块链网络中设置预备金列表的流程图。

[20]图 3 是一示例性实施例提供的一种可在区块链网络中实施汇款交易的示意图。

5 [21]图 4 是一示例性实施例提供的一种在区块链网络中实施设置预备金列表并汇款交易的流程图。

[22]图 5 是一示例性实施例提供的运行本说明书实施例所提供的基于区块链的汇款装置的计算机设备结构示意图。

[23]图 6 是一示例性实施例提供的一种基于区块链的汇款装置的示意图。

10 具体实施方式

[24]这里将详细地对示例性实施例进行说明，其示例表示在附图中。下面的描述涉及附图时，除非另有表示，不同附图中的相同数字表示相同或相似的要素。以下示例性实施例中所述的实施方式并不代表与本说明书一个或多个实施例相一致的所有实施方式。相反，它们仅是与如所附权利要求书中所详述的、本说明书一个或多个实施例的一些方面相一致的装置和方法的例子。

15

[25]需要说明的是：在其他实施例中并不一定按照本说明书示出和描述的顺序来执行相应方法的步骤。在一些其他实施例中，其方法所包括的步骤可以比本说明书所描述的更多或更少。此外，本说明书中所描述的单个步骤，在其他实施例中可能被分解为多个步骤进行描述；而本说明书中所描述的多个步骤，在其他实施例中也可能被合并为单个步骤进行描述。

20

[26]图 1 是一示例性实施例提供的一种基于区块链的汇款方法的流程图，用于汇出方账户向接收方账户汇款，汇出方账户包括一预备金列表；所述预备金列表包括基于汇出方账户的余额划分得到的多个预备金金额。

[27]上述实施例所述的区块链，具体可指一个各节点通过共识机制达成的、具有分布式数据存储结构的 P2P 网络系统，该区块链内的数据分布在时间上相连的一个个“区块（block）”之内，后一区块包含前一区块的数据摘要，且根据具体的共识机制（如 POW、POS、DPOS 或 PBFT 等）的不同，达成全部或部分节点的数据全备份。本领域的技术

25

人员熟知，由于区块链系统在相应共识机制下运行，已收录至区块链数据库内的数据很难被任意的节点篡改，例如采用 Pow 共识的区块链，至少需要全网 51%算力的攻击才有可能篡改已有数据，因此区块链系统有着其他中心化数据库系统无法比拟的保证数据安全、防攻击篡改的特性。由此可知，在本说明书所提供的实施例 5 中，被收录至区块链的分布式数据库中的汇款交易及其他交易不易被攻击或篡改，从而为发布至所述区块链的分布式数据库的交易进行了存证。

[28]将上述区块链作为一个通用的管理对象状态转换的去中心化平台，上述账户就是有状态的对象，上述汇出方账户所包括的内容可以为上述汇出方账户的状态所包含的内容，本领域的技术人员熟知，账户通常包含账户余额信息。

10 [29]在本说明书中，为了支持基于汇出方的账户余额而产生的并发交易，汇出方的账户中还包括一预备金列表，该预备金列表中包括了从账户余额中划分出的多个预备金金额，从而可将上述多个预备金金额中的至少一个分配至其足以支付的一个汇款交易中；由于预备金列表可包括多个可用的预备金金额，所以汇出方可以基于多个可用的预备金金额发出多个足以支付的汇款交易。

15 [30]值得注意的是，本说明书所述的“账户”不限于外部所有账户（EOA）及合约账户（Contract），且也不限定上述预备金列表的具体表现形式，只要包含或管理上述由预备金总额划分所得的多个预备金金额的数据组织形式均属于本说明书所述的预备金列表。

[31]如图 1 所示，上述汇款方法可以包括以下步骤：

20 [32]步骤 102，接收汇出方发送的用于向接收方汇款的第一交易，所述第一交易包括所述汇出方账户汇入接收方账户的汇款额，和所述汇出方从所述预备金列表中为所述第一交易分配的至少一个与所述汇款额对应的预备金金额。

[33]上述第一交易即本说明书所述的汇款交易。上述从汇出方区块链账户向接收方区块链账户汇入（或称为转移）的汇款额对应于相应金额的资产凭证：资产凭证可以对应于 25 区块链内的代币（token）、数字资产等智能资产，资产凭证还可以对应于区块链外的现金、证券、优惠券、房产等链外资产，本说明书并不对此进行限制。

[34]该第一交易所包括的、汇出方从所述预备金列表中为第一交易所分配的至少一个与所述汇款额对应的预备金金额，可以有多种分配方式，在本说明书中不作限定。例如，汇出方账户的预备金列表中包含{5,10,15,20}四个预备金金额，对于汇款额为 10 的第一

交易，汇出方可从上述四个预备金金额中选出一个预备金金额 10（或 15 或 20），将上述一个预备金金额 10（或 15 或 20）分配至上述第一交易中；对应汇款额为 12 的第一交易，汇出方可从上述四份预备金金额中选出一个预备金金额 15（或 20），将上述一个预备金金额 15（或 20）分配至上述第一交易中，也可以从上述四个预备金金额中选出两个预备金金额 5 和 10（或 5 和 15），将上述两个预备金金额 15（或 20）分配至上述第一交易中，利用两个预备金金额之和为汇款交易提供足以支付的验证证明。值得注意的是，为防止“双花”重放的汇款交易无法通过验证，每个预备金金额不能被重复分配。

[35]在本说明书一示出的实施例中，为保证与第一交易分配的预备金金额未在其他汇款交易中被使用过，上述预备金列表中可将预备金金额进行标定，以防止基于同一预备金金额产生“双花”的交易；尤其是在预备金列表中包含多个等值的预备金金额时，验证节点不易区分某一等值的预备金金额是否在其他交易中被使用过。汇出方的账户可采用多种方式标识预备金金额。

[36]例如，在汇出方账户的预备金列表中，为各个预备金金额生成与之对应的唯一编码或标识，此时，第一交易不仅包含预备金金额，还应包含该预备金金额的唯一标识（如编码），由于已完成的汇款交易会在区块链的分布式数据库中存证，则已被用于其他已完成的汇款交易中的预备金金额的唯一标识也会随已完成的汇款交易被保存在所述区块链的分布式数据库中；所以第一交易中包含的预备金金额的唯一标识可以帮助区块链节点验证该预备金金额是否在其他汇款交易中被使用过。

[37]又如，在汇出方账户的预备金列表中，还可为各个预备金金额生成使用状态标识。当一包括预备金金额的汇款交易被验证通过，并在区块链的分布式数据库内收录该汇款交易、且更新该汇款交易的汇出方的账户余额时，该汇款交易所包含的预备金金额应在汇出方账户的预备金列表中被标识为已使用状态（状态 3），本领技术人员熟知，上述被收录在区块链的分布式数据库中的汇款交易可称为“已完成的汇款交易”。对于新的尚未完成的汇款交易，区块链中的验证节点可验证上述新的尚未完成的汇款交易中的预备金金额在汇出方账户的预备金列表中的状态是否为已使用状态：如果是已使用状态，则该项验证不通过，相应的新的尚未完成的汇款交易可以被退回；如果不是已使用状态，则该项验证通过。类似地，当该新的汇款交易通过验证后在区块链的分布式数据库中更新时，区块链节点也应将该新的汇款交易中包含的预备金金额在汇出方账户的预备金列表中更新为“已使用状态”。

[38]更优的，还未被使用过的、亦即还未被分配至任何汇款交易的预备金金额可在上述预备金列表中被标记为未使用状态（状态 1）；一预备金金额一旦被分配于一个汇款交易，该预备金金额可在汇出方账户的预备金列表中即刻被标识为被使用状态（状态 2），亦即在汇出方用户的本地保存的预备金列表中将上述预备金金额标定为被使用状态（状态 2）。由此可知，汇出方账户仅能分配未使用状态（状态 1）的预备金金额用于新的汇款交易，且在分配后将该被分配的预备金金额随即在本地更改为被使用状态（状态 2），以防止对同一预备金金额的重复分配。

[39]为保护区块链用户的账户隐私安全，在现有的一些区块链中，用户的账户余额、及汇款交易的交易额均被加密；本说明书所提供的汇款方法也可以用于隐私模式的区块链中。

[40]在一示出的实施例，区块链用户的账户余额、预备金列表所包含的预备金金额、以及汇款交易的汇款额均被加密；由于在汇出方的账户中所呈现的账户余额及预备金列表所包含的预备金金额均是加密状态，为保证区块链中的节点可对该汇款交易顺利验证、且验证通过后无需解密而可依据被加密的汇款额直接更新汇出方及接收方加密的账户余额，区块链用户的账户余额、预备金列表所包含的预备金金额、以及汇款交易的汇款额均应基于相同的同态加密算法被加密。

[41]由于第一交易所包括的汇款额及预备金金额均为加密状态，为保证上述被分配至第一交易的预备金金额足以支付本次汇款，上述第一交易中还应包括基于第一交易所包括的被加密的预备金金额和被加密的汇款额生成的第一零知识证明，用于证明为第一交易所分配的预备金金额之和大于或者等于所述汇款额。

[42]零知识证明，通常指的是证明者（被验证者）能够在不向验证者提供任何有用的信息的情况下，使验证者相信某个论断是正确的。在本说明书中，汇出方通过提供基于被加密的汇款额和第一交易所包括的被加密的预备金金额生成的第一零知识证明，使得区块链中的节点（验证者）在不获知汇款额、及预备金金额的具体值的情况下，可以验证为第一交易所分配的预备金金额的具体值之和大于或者等于所述汇款额的具体值，足以支付上述汇款交易，亦即使得区块链中的节点（验证者）基于零知识证明算法针对所述第一零知识证明进行零知识验证，以确认为所述第一交易所分配的预备金金额之和是否大于或者等于所述汇款额。

[43]本说明书并不限定上述同态加密算法的类型，可以包括加法同态加密算法或全同态加密算法，只要确保该同态加密算法能够满足加法同态并且能够支持验证一明文数据属

于某个区间的零知识证明，使得加密的汇出方账户余额可直接扣除加密的汇款额，加密的接收方账户余额可直接增加加密的汇款额，也使得汇出方能够基于加密后的汇款额及被加密的预备金金额提供零知识证明来证明汇款额不大于交易中所用的被加密的预备金金额对应的预备金金额之和。

- 5 [44]例如，上述区块链可以支持基于椭圆曲线参数 G 和 H 的 Pedersen Commitment 加密算法，用以保证区块链中被加密的数额可以在加密状态被验证数额范围、且可实现加法同态。

[45]本说明书并不限定上述第一零知识证明的具体类型，例如可以采用相关技术中的区间证明（Range Proof）技术，譬如 Bulletproofs 方案或 Borromean 环签名方案等。

- 10 [46]在又一示出的实施例，为防止区块链中某些节点作恶对区块链进行攻击，上述第一交易中还可包括基于所述被加密的汇款额生成的第二零知识证明，所述第二零知识证明用于证明所述汇款额不小于零。

[47]在本说明书又一示出的实施例中，上述第一交易还可包括汇出方账户的标识，如账户地址、或账户公钥及上述汇出方所作的电子签名，上述电子签名是汇出方使用自身的私钥对包含第一交易的汇款额、或至少一个预备金金额或上述零知识证明等内容所作的签名，用以供区块链的节点对电子签名进行验证，防止其他节点冒充汇出方而发布上述第一交易，发布错误信息、恶意扰乱交易秩序。

- 15 [48]步骤 104，对所述第一交易进行第一交易验证，所述第一交易验证包括第一验证步骤，用以验证所述第一交易包括的预备金金额之和是否大于或者等于所述汇款额；如果
20 是，所述第一交易通过所述第一验证步骤。

- [49]根据区块链所依赖的共识机制不同，区块链中负责验证交易的节点、区块链中的验证节点所遵循的验证规则也都不尽相同。例如，在比特币、以太坊等区块链公链中，区块链中的所有节点均具有验证交易的权限，比特币区块链中需验证交易的格式、签名、UTXO 的输入交易是否有效、是否未双花、输出的值是否不大于输入等内容，以太坊区块链中需验证交易的格式、签名、账户的余额是否足够支付本次交易、是否为双花交易等；而在基于 PBFT 共识算法的联盟链中，具有验证交易的权限的节点通常是预选的、信用较高的节点，联盟链的预选节点需验证的内容通常依据交易的具体内容而定制。由于本说明书所提供的基于区块链的汇款方法可以被应用在基于多种共识机制类型的区块链中，因此本说明书既不限定对上述第一交易执行验证的区块链节点的数量及类型，
- 25

也不限制上述第一交易验证所包含的内容或流程。

[50]为保证用于汇款的第一交易的正常进行，在本说明书所提供的实施例中，需至少验证第一交易所包括的预备金金额是否足以支付所述汇款额。区块链节点可以直接对比第一交易中所包含的预备金金额之和是否大于或等于第一交易的汇款额，如果是，第一交易通过上述第一验证步骤。

[51]在一示出的实施例中，如前所述，当所述预备金列表中还包括所述多个预备金金额对应的使用状态，所述使用状态包括已使用状态，所述已使用状态表示其对应的预备金金额在所述区块链的已完成的汇款交易中被使用过时，所述第一交易验证还包括：第二验证步骤，用以验证第一交易所包括的预备金金额是否在所述预备金列表中被标记为已使用状态；如果否，第一交易通过所述第二验证步骤。相应地，如果所述第一交易通过所述第一交易验证所包括的所有验证步骤，区块链节点应将所述第一交易包括的预备金金额在所述预备金列表中标记为已使用状态。

[52]更优地，上述预备金金额的使用状态还包括未使用状态和被使用状态，所述未使用状态表示与之对应的预备金金额还未被分配至已发起的汇款交易，所述被使用状态表示与之对应的预备金金额已被分配至已发起的汇款交易。汇出方节点可在本地客户端将上述至少一个预备金金额分配至上述第一交易后，将第一交易所包括的预备金金额的使用状态从“未使用”更改为“被使用”，以防止汇出方重复分配。

[53]值得注意的是，上述“未使用”“被使用”“已使用”是作为区分预备金金额的状态的三个功能性描述，在具体实现时，可以用与足以区分上述三种状态的任意标识或名称均可实现上述实施例。

[54]在又一示出的实施例中，如前所述，当所述预备金列表还包括预备金金额对应的唯一标识、所述第一交易还包括与被分配的预备金金额对应的唯一标识时，所述验证还包括：第三验证步骤，用以验证所述第一交易所包括的所述唯一标识是否在已完成的汇款交易中被使用过；如果否，所述第一交易通过所述第三验证步骤。

[55]如前所述，为保护区块链用户的隐私性，尤其是保护汇款交易的隐私性，当上述第一交易所包含的汇款额、以及上述预备金金额均被预先进行了加密处理时，由于区块链上除第一交易的汇出方之外的其他节点均不能获知该汇款额和第一交易中与所述汇款额对应的预备金金额的具体值，为保证区块链上的节点可验证为第一交易分配的预备金金额之和是否能够支付得起上述汇款额，上述第一交易还应包括基于所述第一交易所包

括的被加密的预备金金额和被加密的汇款额生成的第一零知识证明；相应的，上述第一交易验证所包括的第一验证步骤，包括：基于零知识证明算法针对所述第一零知识证明进行零知识验证，以确认为第一交易所分配的预备金金额之和是否大于或者等于所述汇款额；如果是，所述第一交易通过所述第一验证步骤。

- 5 [56]在又一示出的实施例中，如前所述，当第一交易还包括基于被加密的汇款额生成的第二零知识证明时，所述第一交易验证还包括第四验证步骤，基于零知识证明算法针对所述第二零知识证明进行零知识验证，以确认所述汇款额是否大于或者等于零；如果是，所述第一交易通过所述第四验证步骤。

- 10 [57]在又一示出的实施例中，如前所述，在本说明书又一示出的实施例中，当第一交易还包括上述汇出方所作的电子签名时，上述区块链中具有验证权限的节点还应使用汇出方的公钥对上述电子签名进行验证，以确定上述电子签名及第一交易是由该汇出方汇出的，防止其他恶意节点的仿冒行为。

- 15 [58]本说明书所提供的上述实施例中所述的“第一”、“第二”、“第三”、“第四”仅是为区分上述验证步骤，而并非用于对上述验证步骤执行的先后顺序的限定；例如，本领域的技术人员熟知，对电子签名的验证一般是验证阶段最先进行的验证步骤，但是本说明书中对以上验证步骤的执行前后顺序并不限定。

[59]步骤 106，如果所述第一交易通过所述第一交易验证，从所述汇出方账户的余额扣除所述汇款额，在接收方账户的余额增加所述汇款额。

- 20 [60]在上述第一交易通过所述第一交易验证包含的验证步骤后，上述第一交易即可被收录至区块链的区块中，上述汇出方的账户及接收方的账户应发生相应地更新：从所述汇出方账户的余额扣除所述汇款额，在接收方账户的余额增加所述汇款额。

- 25 [61]基于区块链上账户状态更新过程所依据的共识机制不同，上述执行更新汇出方、接收方的账户余额的区块链节点可以与上述执行验证交易的区块链节点为相同的节点，也可以是不同的节点；上述执行更新汇出方、接收方的账户余额的区块链节点既可以为经过共识后的一个节点，也可以为多个节点，在本发明中不作限定。

[62]当本说明书所述的汇款方法应用于隐私模式的区块链时，由于汇出方账户的余额、用于向接收方汇款的第一交易的汇款额均基于相同的同态加密算法被加密，区块链的节点可从所述汇出方账户的余额同态加密扣除所述汇款额，在接收方账户的余额同态加密增加所述汇款额，亦即：利用汇出方账户被加密的余额直接减去被加密的汇款额得到更

新后的、被加密的汇出方账户余额，利用接收方账户被加密的余额直接加上被加密的汇款额得到更新后的、被加密的接收方账户余额，无需解密上述汇出方、接收方的账户余额及第一交易的汇款额。本领域的技术人员熟知，基于同态加密算法的特性，在汇出方账户被加密的余额直接扣除被加密的汇款额所得的密文，等于使用上述同态加密算法对汇出方账户的余额直接扣除汇款额后所得的新的账户余额加密所得的密文；在接收方账户被加密的余额直接增加被加密的汇款额所得的密文，等于使用上述同态加密算法对接收方的账户余额直接增加汇款额后所得的新的账户余额加密所得的密文。

[63]本说明书的上述多个实施例提供的包含步骤 102~步骤 106 的隐私加密汇款方法，基于账户余额生成多个预备金金额，并将多个预备金金额指定至多个汇款交易中；区块链的节点是针对各个汇款交易所包括的预备金金额进行各个汇款交易是否足以支付的验证，对各个汇款交易的验证分别独立进行，不相互影响，从而使得基于账户模型构建的区块链可以并行发送多个汇款交易。而且本说明书提供的汇款方法还可适用在隐私模式的区块链中，基于上述被加密预备金金额和被加密的汇款额生成第一零知识证明，用以证明与为第一交易分配的预备金金额之和足以支付所述汇款额。由于预备金列表中包含多个被加密的预备金金额，可以分别支持多个并发的汇款交易，从而克服了现有的隐私加密汇款中，基于汇出方的账户余额为汇款额生成足以支付的零知识证明而引起的不能并发汇款交易的缺陷，在保护汇款交易数据隐私的前提下，提高了汇款交易的吞吐量。

[64]为执行上述多个实施例所述的汇款方法，汇出方的账户中需保存有上述预备金列表，以存储基于基于汇出方的账户余额划分得到的多个预备金金额；当上述预备金列表中的预备金金额被使用完毕、或剩余的预备金金额已经不再足以支付下一汇款交易、或用户根据自身的特定需求周期性更新上述预备金列表时，汇出方节点需在其账户中初始化预备金列表。上述初始化建立预备金列表（包括首次初始化及更新重置预备金列表），可通过在区块链上发布预备金列表初始化交易来实现；可选的，区块链上可以专门为初始化或更新预备金列表设置固定格式的交易，以帮助用户完成上述预备金列表的初始化。

[65]由于区块链中的多数节点均可作为汇出方执行汇款操作，因此上述初始化或更新预备金列表的执行主体可以为区块链中的多数节点。

[66]在本说明书又一示出的实施例中，如图 2 所示，上述初始化或更新预备金列表的方法包括：

[67]步骤 202，接收所述汇出方发送的用于初始化预备金列表的第二交易，所述第二交易包括基于汇出方账户的余额划分得到的多个预备金金额。

[68]上述第二交易用于初始化预备金列表。为保护用户账户的隐私安全，当区块链上用户账户的余额被同态加密时，上述多个预备金金额也应被预先进行同态加密处理，上述第二交易还包括基于被加密的所述多个预备金金额和被加密的所述汇出方账户的余额生成的第三零知识证明，用于证明与所述第二交易所包括的多个预备金金额之和小于或者等于所述汇出方账户的余额。

[69]在本说明书中，由于汇出方账户的余额及汇出方基于账户余额划分得到的多个预备金金额均基于上述的同态加密算法被加密，汇出方节点通过提供基于被加密的所述多个预备金金额和被加密的所述汇出方账户的余额生成的第三零知识证明，使得区块链中的节点（验证者）在不获知账户余额、及预备金金额的实际值（明文）情况下，可以验证第二交易中所包含的多个预备金金额之和是否不大于上述汇出方账户的余额。

[70]类似的，本说明书并不限定上述第三零知识证明的具体类型，例如可以采用相关技术中的区间证明（Range Proof）技术，譬如 Bulletproofs 方案或 Borromean 环签名方案等。

[71]在又一示出的实施例中，为保证上述被加密的预备金金额均可用于汇款交易（第一交易），防止恶意汇款对区块链造成攻击，所述第二交易还包括基于被加密的所述多个预备金金额生成的第四零知识证明，使得区块链中的节点（验证者）在不获知预备金金额的实际值（明文）情况下，可以验证所述第二交易所包括的多个预备金金额是否均大于或者等于零。

[72]在本说明书又一示出的实施例中，上述第二交易还可包括汇出方账户的标识，如账户地址、或账户公钥及上述汇出方所作的电子签名，上述电子签名是汇出方使用自身的私钥对包含第二交易的预备金列表、或上述第三零知识证明、第四零知识证明等内容所作的签名，用以供区块链的节点对电子签名进行验证，防止其他节点冒充汇出方而发布上述第二交易，发布错误信息、恶意扰乱交易秩序。

[73]步骤 204，对所述第二交易进行第二交易验证，所述第二交易验证包括第五验证步骤，用以验证所述第二交易所包括的多个预备金金额之和是否小于或者等于所述汇出方账户的余额；如果是，所述第二交易通过所述第五验证步骤。

[74]类似地，由于本说明书所提供的基于区块链的汇款方法可以被应用在基于多种共识机制类型的区块链中，因此本说明书既不限定对上述第二交易执行验证的区块链节点的数量及类型，也不限制根据区块链的验证规则对第二交易验证包含的具体内容及流程。

[75]在一示出的实施例中，当汇出方账户的余额以及所述多个预备金金额被预先进行了
同态加密处理，且所述第二交易还包括基于被加密的所述多个预备金金额和被加密的所
述汇出方账户的余额生成的第三零知识证明时，上述第二交易验证至少包括基于零知识
证明算法针对所述第三零知识证明进行零知识验证的第五验证步骤，以确认所述第二交
易所包括的多个预备金金额之和是否小于或者等于所述账户余额；如果是，所述第二交
易通过所述第五验证步骤。

[76]在又一示出的实施例中，当第二交易还包括基于被加密的所述多个预备金金额生成
的第四零知识证明时，所述第二交易验证还包括第六验证步骤，所述第六验证步骤包括：
基于零知识证明算法针对所述第四零知识证明进行零知识验证，以确认所述第二交易所
包括的多个预备金金额是否均大于或者等于零；如果是，所述第二交易通过所述第六验
证步骤。

[77]在又一示出的实施例中，如前所述，在本说明书又一示出的实施例中，当第二交易
还包括上述汇出方所作的电子签名时，上述区块链中具有验证权限的节点还应使用汇出
方的公钥对上述电子签名进行验证，以确定上述电子签名及第二交易是由该汇出方汇出
的，防止其他恶意节点的仿冒行为。

[78]与第一交易验证类似，本说明书所提供的上述实施例中所述的“第五”、“第六”
仅是为区分上述第二交易验证所包含的验证步骤，而并非用于对上述验证步骤执行的先
后顺序的限定；例如，本领域的技术人员熟知，对电子签名的验证一般是验证阶段最先
进行的验证步骤，但是本说明书中对以上验证步骤的执行前后顺序并不限定。

[79]步骤 206，如果所述第二交易通过所述第二交易验证，基于所述多个预备金金额构
建预备金列表，并将所述预备金列表更新至所述汇出方账户。

[80]在上述第二交易通过第二交易验证包括的验证步骤后，区块链节点应基于所述多个
预备金金额构建预备金列表，并将所述预备金列表更新至所述汇出方账户。

[81]基于区块链上账户状态更新过程所依据的共识机制不同，上述执行更新汇出方账户
状态的区块链节点可以与上述执行验证第二交易的区块链节点为相同的节点，也可以是
不同的节点；可以为一个节点，也可以为多个节点，在本发明中不作限定。

[82]本实施例所述的预备金列表是对上述第二交易所包含的多个预备金金额的数据组织
形式，上述预备金列表的具体表现形式不限于二维表、树形结构或其他图形结构。

[83]在又一示出的实施例中，为保证区块链节点可以方便地验证汇款交易（第一交易）

所包含的预备金金额是否在已完成汇款交易中被使用过，以防止“双花”汇款交易的产生，在初始化预备金列表的第二交易中，上述预备金列表包括的多个预备金金额应标记为未使用状态，以便在至少一个预备金金额被分配至汇款交易后，将上述至少一个预备金金额标记为被使用状态，在该汇款交易完成后，将上述至少一个预备金金额标记为已使用状态。

[84]或者，在又一示出的实施例中，为保证区块链节点可以方便地验证汇款交易（第一交易）所包含的预备金金额是否在已完成汇款交易中被使用过，以防止“双花”汇款交易的产生，在初始化预备金列表的第二交易中，上述预备金列表还包括为每个预备金金额生成的唯一标识，以便在包含上述预备金金额唯一标识的汇款交易（第一交易）完成后，在区块链的分布式数据库中存证上述预备金金额的唯一标识，进而帮助区块链的节点验证新的汇款交易所包含的预备金金额是否在已完成的汇款交易中被使用过。

[85]为了便于理解，下面以区块链网络中的汇款交易为例，对本说明书的技术方案进行详细说明。图3是一示例性实施例提供的一种在区块链网络中实施第一交易和第二交易的示意图。例如，由用户A向用户B进行区块链汇款（第一交易），在汇款之前，由用户A向区块链发布初始化或更新其账户中所包含的预备金列表的交易（第二交易）。其中，本说明书中的“用户”可以表现为所登录的用户账号，而该用户账号实际可以归属于个人或组织，本说明书并不对此进行限制。

[86]假定用户A使用的汇出方设备为用户设备1，譬如该用户设备1上登录有对应于用户A的用户账号；类似地，用户B使用的接收方设备为用户设备2。用户设备1上可以运行有区块链的客户端程序，使得该用户设备1在区块链网络中存在对应的区块链节点，比如图3所示的节点1。类似地，用户设备2上可以运行有区块链的客户端程序，使得该用户设备2在区块链网络中存在对应的区块链节点，比如图3所示的节点2。区块链网络中还可能存在其他区块链节点，比如图3所示的节点i~节点j等。通过上述的节点1、节点2、节点i~节点j等，使得用户A与用户B之间的汇款交易、及用户A发送的初始化或更新预备金列表的交易可以经由区块链网络实施，相关交易信息可以被记录至各个区块链节点分别维护的区块链账本中，可以避免发生篡改，并有助于后续查验。

[87]图4是一示例性实施例提供的在隐私保护模式的区块链网络中实施设置图3所示的用户A的预备金列表、及执行用户A向用户B发送汇款的流程图。

[88]在上述区块链中，用户A的账户余额 s_A 及用户B的账户余额 s_B 均基于同态加密算法被加密，加密后用户A的账户余额密文为 $S_A = HE(s_A)$ ，用户B的账户余额密

文为 $S_B = HE(s_B)$ ；在一实施例中，上述同态加密算法可以为 Pederson Commit 算法。

[89] 设置用户 A 的预备金列表的过程包括以下步骤：

[90] 步骤 401，用户 A 建立预备金列表 M_A ，上述预备金列表 M_A 包括用户 A 针对自身的账户余额划分得到的、被基于上述的同态加密算法 HE 加密的、多个预备金金额 $M_A[1]$ ，
5 $M_A[2]$ ，...， $M_A[L-A]$ ，并在上述预备金列表中将上述预备金金额 $M_A[1]$ ， $M_A[2]$ ，...， $M_A[L-A]$ 的使用状态标记为“未使用状态”。

[91] 具体实现时，用户 A 可对自身的全部账户余额 s_A 或部分账户余额进行划分，得到上述多个预备金金额的明文 $m_a[1]$ ， $m_a[2]$ ，...， $m_a[L-A]$ ，并基于上述同态加密算法对上述多个预备金金额加密，以得到预备金金额密文 $M_A[1]$ ， $M_A[2]$ ，...， $M_A[L-A]$ ；用户
10 A 也可以对账户余额密文 S_A 直接进行划分以得到 $M_A[1]$ ， $M_A[2]$ ，...， $M_A[L-A]$ ，并基于上述同态加密算法的进行逆运算，获知上述预备金金额密文对应的明文 $m_a[1]$ ， $m_a[2]$ ，...， $m_a[L-A]$ 。用户 A 可将上述预备金金额的明文 $m_a[1]$ ， $m_a[2]$ ，...， $m_a[L-A]$ 与密文 $M_A[1]$ ， $M_A[2]$ ，...， $M_A[L-A]$ 的对应关系独自保存，以方便用户 A 在具体的汇款交易中选取合适的预备金金额。

[92] 步骤 402，用户 A 基于 $M_A[1]$ ， $M_A[2]$ ，...， $M_A[L-A]$ 和 S_A 生成零知识证明 $PF[s_A \geq (m_a[1] + m_a[2] + \dots + m_a[L-A])]$ ，用于证明上述预备金列表 M_A 中的 $M_A[1]$ ， $M_A[2]$ ，...， $M_A[L-A]$ 对应的预备金金额 $m_a[1]$ ， $m_a[2]$ ，...， $m_a[L-A]$ 之和小于或者等于所述汇出方的账户余额 s_A ，上述零知识证明 $PF[s_A \geq (m_a[1] + m_a[2] + \dots + m_a[L-A])]$ 不使用预备金金额 $m_a[1]$ ， $m_a[2]$ ，...， $m_a[L-A]$ 及 s_A 的值，即可使验证者证明 $m_a[1]$ ， $m_a[2]$ ，...， $m_a[L-A]$ 之和小于或者等于 s_A 。在一实施例中，上述零知识证明 $PF[s_A \geq (m_a[1] + m_a[2] + \dots + m_a[L-A])]$ 可使用 Borromean 环签名方案或 Bulletproof 方案等区间证明技术。
20

[93] 步骤 403，用户 A 基于 $M_A[1]$ ， $M_A[2]$ ，...， $M_A[L-A]$ 生成零知识证明 $PF(m_a[i] \geq 0)$ ，用以证明上述预备金列表 M_A 中的 $M_A[1]$ ， $M_A[2]$ ，...， $M_A[L-A]$ 对应的预备金金额 $m_a[1]$ ， $m_a[2]$ ，...， $m_a[L-A]$ 均不小于零。上述零知识证明 $PF(m_a[i] \geq 0)$ 不使用预备金金额 $m_a[i]$ 的值即可使验证者证明 $m_a[i] \geq 0$ 。在一实施例中，上述零知识证明 $PF(m_a[i] \geq 0)$ 可使用 Borromean 环签名方案或 Bulletproof 方案等区间证明技术。
25

[94] 步骤 404，用户 A 基于 M_A ， $PF[s_A \geq (m_a[1] + m_a[2] + \dots + m_a[L-A])]$ ， $PF(m_a[i] \geq 0)$ 生成电子签名 $Sign A_s$ 。

[95] 步骤 405，用户 A 向所述区块链发送交易 T_s 以确定上述的预备金列表 M_A ，上述交

易 T_s 包括 M_A 、 $PF[s_A \geq (m_a[1]+m_a[2]+\dots+m_a[L-A])]$ 、 $PF(m_a[i] \geq 0)$ ，其中 $1 \leq i \leq L_A$ ，和 $Sign A_s$ 。

[96] 步骤 406，区块链的节点接收上述交易 T_s 。

[97] 步骤 407，区块链的节点执行对上述交易 T_s 的电子签名 $Sign A_s$ 验证，如果通过，执行下个步骤。

[98] 步骤 408，区块链的节点基于零知识证明算法对 $PF[s_A \geq (m_a[1]+m_a[2]+\dots+m_a[L-A])]$ 进行零知识验证，以确认 $m_a[1]$ ， $m_a[2]$ ， $\dots$ ， $m_a[L-A]$ 之和是否小于或者等于所述汇出方的账户余额 s_A ；如果是，执行下个步骤。

[99] 步骤 409，区块链的节点基于零知识证明算法对 $PF(m_a[i] \geq 0)$ 进行零知识验证，以
10 确认 $(m_a[i] \geq 0)$ 均不小于零，其中 $1 \leq i \leq L_A$ ；如果是，执行下个步骤。

[100] 步骤 410，区块链的节点将通过验证的交易 T_s 收录至所述区块链的分布式数据库，并将预备金列表 M_A 更新至所述用户 A 的账户状态。

[101] 至此，区块链的节点完成了对用户 A 的预备金列表 MA 的更新，本领域的技术人员熟知，在设置或更新用户 A 的预备金列表 MA 的实际实施过程中，还可包括许多
15 其他的验证步骤，例如防重放的验证等，在此不做限定；而且本说明书并不限定生成各个证明或电子签名的先后顺序，也不限定区块链中的节点对汇出方提出的交易 T_s 中各项证明或电子签名的验证的先后顺序，图 4 仅仅是本说明书提供的设置用户的预备金列表的方法的一种实施例，本说明书不限于此。

[102] 图 4 中的区块链执行用户 A 向用户 B 汇款转账的过程如下：

20 [103] 步骤 411，用户 A 基于上述同态加密算法生成汇款额密文 $S_t=HE(s_t)$ ，其中 s_t 为用户 A 向用户 B 转账的汇款额。

[104] 步骤 412，用户 A 从预备金列表 M_A 中选取一个未使用过的、且其明文 $m_A[k]$ 足以支付汇款额 s_t 的预备金金额密文 $M_A[k]$ ，并将该预备金金额密文 $M_A[k]$ 标记为被使用状态，以使 $M_A[k]$ 不可再被指定在其他新的汇款交易中。

25 [105] 步骤 413，用户 A 基于 $M_A[k]$ 和 S_t 生成零知识证明 $Pf(m_A[k] \geq s_t)$ ，用以证明 $M_A[k]$ 对应的预备金金额 $m_A[k]$ 足以支付本次汇款额 s_t ；上述零知识证明 $Pf(m_A[k] \geq s_t)$ 不使用 $m_A[k]$ 及 s_t 的值，即可使验证者证明 $m_A[k] \geq s_t$ 。

[106] 步骤 414，用户 A 基于 S_t 生成零知识证明 $Pf(s_t \geq 0)$ ，用以证明汇款额 s_t

不小于零；上述上述零知识证明 $Pf(s_t \geq 0)$ 不使用 s_t 的值，即可使验证者证明 $s_t \geq 0$ 。

[107] 步骤 415，用户 A 基于 S_t 、 $M_A[k]$ 、 $Pf(m_A[k] \geq s_t)$ 、 $Pf(s_t \geq 0)$ 生成电子签名 $Sign A_t$ 。

- 5 [108] 步骤 416，用户 A 向所述区块链发送交易 T_t 以向用户 B 汇款转账，交易 T_t 包括 S_t 、 $M_A[k]$ 、 $Pf(m_A[k] \geq s_t)$ 、 $Pf(s_t \geq 0)$ 及 $Sign A_t$ ，上述内容均未密文状态，因此保护了用户 A、B 的汇款交易隐私性。

[109] 步骤 417，区块链的节点接收上述交易 T_t 。

- 10 [110] 步骤 418，区块链的节点执行对上述交易 T_t 的电子签名 $Sign A_t$ 验证，如果通过，执行下个步骤。

[111] 步骤 419，区块链的节点验证上述 T_t 所包含的 $M_A[k]$ 是否为已使用状态；如果否，执行下个步骤。

- 15 [112] 步骤 420，区块链的节点基于零知识证明算法对 $PF(m_A[k] \geq s_t)$ 进行零知识验证，以确认 $M_A[k]$ 对应的预备金金额是否大于或者等于所述汇款额；如果是，执行下个步骤。

[113] 步骤 421，区块链的节点基于零知识证明算法对 $PF(s_t \geq 0)$ 进行零知识验证，以确认本次汇款交易的汇款额密文 S_t 对应的汇款额实际值不小于零；如果是，执行下个步骤。

- 20 [114] 步骤 422，区块链的节点将通过验证的交易 T_t 收录至所述区块链的分布式数据库，并在用户 A 的账户余额密文 S_A 同态加密扣除所述汇款额密文 S_t ，在用户 B 的账户余额密文 S_B 同态加密增加所述汇款额密文 S_t ，以使上述用户 A 的账户余额更新为 $(s_A - s_t)$ ，用户 B 的账户余额更新为 $(s_B + s_t)$ ；并将用户 A 的预备金列表 M_A 中 $M_A[k]$ 对应的状态更改为已使用状态。

- 25 [115] 图 4 所述的用户 A 向用户 B 汇款的实施例，基于在用户 A 的账户中建立预备金列表 M_A ，并为汇款交易指定足以支付汇款额的预备金金额 $M_A[k]$ ，且生成可证明上述汇款交易中的预备金金额 $M_A[k]$ 的实际值足以支付上述汇款额 S_t 的实际值的零知识证明，从而可使区块链中的节点验证并完成上述汇款交易。由于 M_A 中处于未使用状态的预备金金额 $M_A[i]$ 可以为多个，可以分别支持多个并发的汇款交易，从而克服了现有的隐私加密汇款中，基于汇出方的账户余额为汇款额生成足以支付的零知识证明而引起的不能

并发汇款交易的缺陷，在保护汇款交易数据隐私的情况下，提高了汇款交易的吞吐量。

[116] 另外，本领域的技术人员熟知，在汇款交易的实际实施过程中，还可包括许多其他的验证步骤，例如防重放的验证等，在此不做限定；而且本说明书并不限定生成各个证明或电子签名的先后顺序，也不限定区块链中的节点对汇出方提出的交易 T_i 中各项证明或电子签名的验证的先后顺序，图 4 仅仅是本说明书提供的基于区块链的汇款方法的一种实施例，本说明书不限于此。

[117] 虽然图 4 中使用连续的编号表示了用户 A 设置预备金列表及用户 A 向用户 B 汇款的过程，但是这并不表示用户 A 在每次发起汇款交易之前均需设置其账户中的预备金列表。本领域技术人员熟知，用户在注册成为该区块链的用户后的第一次汇款交易之前，需要初始化设置其账户中的预备金列表；当上述预备金列表中的被加密的预备金金额被使用完毕、或剩余的被加密的预备金金额对应的预备金金额已经不再足以支付下一汇款交易，用户才需重新设置其账户中的预备金列表；用户还根据自身的具体需求可周期性更新上述预备金列表。

[118] 图 5 是一示例性实施例提供的一种设备的示意结构图。请参考图 5，在硬件层面，该设备包括处理器 502、内部总线 504、网络接口 506、内存 508 以及非易失性存储器 510，当然还可能包括其他业务所需要的硬件。处理器 502 从非易失性存储器 510 中读取对应的计算机程序到内存 508 中然后运行，在逻辑层面上形成区块链交易装置。当然，除了软件实现方式之外，本说明书一个或多个实施例并不排除其他实现方式，比如逻辑器件抑或软硬件结合的方式等等，也就是说以下处理流程的执行主体并不限于各个逻辑单元，也可以是硬件或逻辑器件。

[119] 请参考图 6，本说明书还提供了一种基于区块链的汇款装置 60，其中，汇出方账户包括一预备金列表；所述预备金列表包括基于汇出方账户的余额划分得到的多个预备金金额；

[120] 所述装置 60 包括：

[121] 接收单元 602，接收汇出方发送的用于向接收方汇款的第一交易，所述第一交易包括所述汇出方账户汇入接收方账户的汇款额，和所述汇出方从所述预备金列表中为所述第一交易分配的至少一个与所述汇款额对应的预备金金额；

[122] 第一交易验证单元 604，对所述第一交易进行第一交易验证，所述第一交易验证单元 604 包括第一验证模块 6041，用以验证所述第一交易包括的预备金金额之和是否大

于或者等于所述汇款额;

[123] 账户更新单元 606, 如果所述第一交易通过所述第一交易验证, 从所述汇出方账户的余额扣除所述汇款额, 在接收方账户的余额增加所述汇款额。

[124] 在一示出的实施例中, 所述第一交易验证单元 604 还包括第二验证模块 6042,

- 5 用以验证所述第一交易包括的预备金金额是否在所述预备金列表中被标记为已使用状态。

[125] 在一示出的实施例中, 所述账户更新单元 606:

[126] 如果所述第一交易通过所述第一交易验证, 将所述第一交易包括的预备金金额在所述预备金列表中标记为已使用状态。

- 10 [127] 在一示出的实施例中, 所述预备金列表还包括所述多个预备金金额对应的唯一标识, 所述第一交易还包括与所述至少一个与所述汇款额对应的预备金金额对应的唯一标识;

[128] 所述第一交易验证单元还 604 包括: 第三验证模块 6043, 用以验证所述第一交易所包括的预备金金额的唯一标识是否在已完成的汇款交易中被使用过。

- 15 [129] 在一示出的实施例中, 所述汇出方账户的余额、所述接收方账户的余额、所述预备金金额以及所述汇款额被预先进行了同态加密处理;

[130] 所述第一交易还包括: 基于所述第一交易所包括的被加密的预备金金额和被加密的汇款额生成的第一零知识证明;

[131] 所述第一验证模块 6041:

- 20 [132] 基于零知识证明算法针对所述第一零知识证明进行零知识验证, 以确认为所述第一交易所分配的预备金金额之和是否大于或者等于所述汇款额;

[133] 所述账户更新单元 606:

[134] 从所述汇出方账户的余额同态加密扣除所述汇款额, 在接收方账户的余额同态加密增加所述汇款额。

- 25 [135] 在一示出的实施例中, 所述第一交易还包括: 基于被加密的汇款额生成的第二零知识证明;

[136] 所述第一交易验证单元 604 还包括第四验证模块 6044, 所述第四验证模块 6044:

基于零知识证明算法针对所述第二零知识证明进行零知识验证,以确认所述汇款额是否大于或者等于零。

[137] 在一示出的实施例中,还包括

[138] 所述接收单元 602,接收所述汇出方发送的用于初始化预备金列表的第二交易,

5 所述第二交易包括基于汇出方账户的余额划分得到的多个预备金金额;

[139] 第二交易验证单元 608,对所述第二交易进行第二交易验证,所述第二交易验证单元 608 包括第五验证模块 6085,用以验证所述第二交易所包括的多个预备金金额之和是否小于或者等于所述汇出方账户的余额;

[140] 所述账户更新单元 606,如果所述第二交易通过所述第二交易验证,基于所述多
10 个预备金金额构建预备金列表,并将所述预备金列表更新至所述汇出方账户。

[141] 在一示出的实施例中,所述汇出方账户的余额以及所述多个预备金金额被预先进行了同态加密处理;

[142] 所述第二交易还包括:基于被加密的所述多个预备金金额和被加密的所述汇出方账户的余额生成的第三零知识证明;

15 [143] 所述第五验证模块 6085:基于零知识证明算法针对所述第三零知识证明进行零知识验证,以确认所述第二交易所包括的多个预备金金额之和是否小于或者等于所述汇出方账户的余额。

[144] 在一示出的实施例中,所述第二交易还包括:基于被加密的所述多个预备金金额生成的第四零知识证明;

20 [145] 所述第二交易验证单元 608 还包括第六验证模块 6086,所述第六验证模块 6086:基于零知识证明算法针对所述第四零知识证明进行零知识验证,以确认所述第二交易所包括的多个预备金金额是否均大于或者等于零。

[146] 在一示出的实施例中,所述账户更新单元 608:

[147] 将所述预备金列表包括的每个预备金金额均标记为未使用状态。

25 [148] 在一示出的实施例中,所述预备金列表还包括为每个预备金金额生成的唯一标识。

[149] 在一示出的实施例中,所述零知识证明算法包括区间证明算法。

[150] 上述装置中各个单元和模块的功能和作用的实现过程具体详见上述方法中对应步骤的实现过程，相关之处参见方法实施例的部分说明即可，在此不再赘述。

[151] 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，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。

[152] 与上述方法实施例相对应，本说明书的实施例还提供了一种计算机设备，该计算机设备包括存储器和处理器。其中，存储器上存储有能够由处理器运行的计算机程序；
10 处理器在运行存储的计算机程序时，执行本说明书实施例中基于区块链的汇款方法的各个步骤。对基于区块链的汇款方法的各个步骤的详细描述请参见之前的内容，不再重复。

[153] 与上述方法实施例相对应，本说明书的实施例还提供了一种计算机可读存储介质，该存储介质上存储有计算机程序，这些计算机程序在被处理器运行时，执行本说明书实施例中基于区块链的汇款方法的各个步骤。对基于区块链的汇款方法的各个步骤的
15 详细描述请参见之前的内容，不再重复。

[154] 以上所述仅为本说明书的较佳实施例而已，并不用以限制本说明书，凡在本说明书的精神和原则之内，所做的任何修改、等同替换、改进等，均应包含在本说明书保护的范围之内。

[155] 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、
20 网络接口和内存。

[156] 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。

[157] 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。
25

[158] 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。

- 5 [159] 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。
- 10 [160] 本领域技术人员应明白, 本说明书的实施例可提供为方法、系统或计算机程序产品。因此, 本说明书的实施例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, 本说明书的实施例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。