

基于区块链的汇款汇路管理

技术领域

[01]本公开涉及区块链技术领域，具体涉及一种基于区块链的汇款汇路管理方法和装置。

背景技术

[02]目前，区块链可以通过执行汇款交易合约对汇款交易提供服务。当汇款发起方需要发起目标汇款交易时，汇款发起方需要先通过金融平台的中心化系统，查询目标汇款交易的参与方的可用汇款汇路。如果汇款发起方查询到的可用汇款汇路与目标汇款交易所需的汇款汇路匹配，那么用户可以通过调用汇款交易合约的方式，在区块链上发起目标汇款交易，此时，区块链可以通过执行汇款交易合约来记录目标汇款交易的交易结果。

[03]也就是说，目标汇款交易的参与方的可用汇款汇路都是通过中心化系统维护的。在一些情况下，当汇款发起方通过中心化系统查询可用汇款汇路时，中心化系统会由于系统错误，导致维护的可用汇款汇路错误，从而向汇款发起方返回错误的结果，降低用户体验。例如，原本参与方的可用汇款汇路与目标汇款交易所需的汇款汇路匹配，但是由于中心化系统错误，导致维护的参与方的可用汇款汇路错误，将参与方的可用汇款汇路记录为不可用的汇款汇路，并向汇款发起方返回了“不匹配，或不存在可用汇款汇路”等错误的结果，导致汇款发起方无法发起目标汇款交易，降低用户体验。

发明内容

[04]有鉴于此，本公开实施例致力于提供一种基于区块链的汇款汇路管理方法，以降低中心化系统维护可用汇款汇路时发生错误的可能性，提高用户体验。

[05]第一方面，提供一种基于区块链的汇款汇路管理方法，所述区块链上存储有第一智能合约，所述第一智能合约用于管理目标汇款交易的多个参与方中的至少一个参与方的可用汇款汇路，所述至少一个参与方的可用汇款汇路用于指示所述至少一个参与方能够为所述目标汇款交易提供的可用汇款汇路，所述至少一个参与方包括第一参与方，所述方法包括：从所述第一参与方接收所述第一智能合约的第一调用请求，所述第一调用请求用于设置所述第一参与方的可用汇款汇路；根据所述第一调用请求，在所述第一智能合约中设置所述第一参与方的可用汇款汇路。

[06]第二方面，提供一种基于区块链的汇款汇路管理方法，所述区块链上存储有第一智能合约，所述第一智能合约用于管理目标汇款交易的多个参与方中的至少一个参与方的可用汇款汇路，所述至少一个参与方的可用汇款汇路用于指示所述至少一个参与方能够

为所述目标汇款交易提供的可用汇款汇路，所述至少一个参与方包括第一参与方，所述方法应用于所述第一参与方，所述方法包括：获取所述第一参与方的可用汇款汇路；向所述区块链发送所述第一智能合约的第一调用请求，所述第一调用请求用于设置所述第一参与方的可用汇款汇路。

[07]第三方面，提供一种基于区块链的汇款汇路管理装置，所述区块链上存储有第一智能合约，所述第一智能合约用于管理目标汇款交易的多个参与方中的至少一个参与方的可用汇款汇路，所述至少一个参与方的可用汇款汇路用于指示所述至少一个参与方能够为所述目标汇款交易提供的可用汇款汇路，所述至少一个参与方包括第一参与方，所述装置包括：接收模块，用于从所述第一参与方接收所述第一智能合约的第一调用请求，所述第一调用请求用于设置所述第一参与方的可用汇款汇路；处理模块，用于根据所述第一调用请求，在所述第一智能合约中设置所述第一参与方的可用汇款汇路。

[08]第四方面，提供一种基于区块链的汇款汇路管理装置，所述区块链上存储有第一智能合约，所述第一智能合约用于管理目标汇款交易的多个参与方中的至少一个参与方的可用汇款汇路，所述至少一个参与方的可用汇款汇路用于指示所述至少一个参与方能够为所述目标汇款交易提供的可用汇款汇路，所述至少一个参与方包括第一参与方，所述装置应用于所述第一参与方，所述装置包括：获取模块，用于获取所述第一参与方的可用汇款汇路；发送模块，用于向所述区块链发送所述第一智能合约的第一调用请求，所述第一调用请求用于设置所述第一参与方的可用汇款汇路。

[09]第五方面，提供一种基于区块链的汇款汇路管理装置，包括存储器和处理器，所述存储器中存储有可执行代码，所述处理器被配置为执行所述可执行代码，以实现如第一方面或第二方面所述的方法。

[10]第六方面，提供一种计算机可读存储介质，其上存储有可执行代码，当所述可执行代码被执行时，能够实现如第一方面或第二方面所述的方法。

[11]第七方面，提供一种计算机程序产品，包括可执行代码，当所述可执行代码被执行时，能够实现如第一方面或第二方面所述的方法。

[12]本公开实施例的方案是在区块链上通过第一智能合约来维护目标汇款交易的参与方的可用汇款汇路，使得作为区块链用户的参与方，可以通过调用第一智能合约来自主地维护可用汇款汇路。避免了传统的通过中心化系统来维护参与方的可用汇款汇路的方案中，由于中心化系统错误，而导致参与方的可用汇款汇路错误，有利于降低中心化系统

维护可用汇款汇路时发生错误的可能性，提高用户体验。

附图说明

[13]图 1 为本公开实施例适用的区块链的架构的示意图。

[14]图 2 为资方 A 发起目标汇款交易的示意性流程图。

[15]图 3 为本公开实施例的基于区块链的汇款汇路管理方法的示意性流程图。

[16]图 4 为本公开实施例的第一智能合约的更新过程的示意性流程图。

[17]图 5 是本公开实施例的第一智能合约的使用过程的示意性流程图。

[18]图 6 是本公开实施例的第一智能合约的查询过程的示意性流程图。

[19]图 7 是本公开实施例的基于区块链的汇款汇路管理装置的示意性结构图。

[20]图 8 是本公开另一实施例的基于区块链的汇款汇路管理装置的示意性结构图。

[21]图 9 是本公开又一实施例提供的基于区块链的汇款汇路管理装置的示意性结构图。

[22]图 10 是本公开又一实施例提供的基于区块链的汇款汇路管理装置的示意性结构图。

具体实施方式

[23]下面将结合本公开实施例中的附图，对本公开实施例中的技术方案进行清楚、完整地描述，显然，所描述的实施例仅是本公开一部分实施例，而不是全部的实施例。

[24]为了便于理解本公开的方案，下文先结合图 1 介绍本公开适用的区块链架构，以及涉及的一些概念。

[25]区块链架构。

[26]图 1 为本公开实施例适用的区块链的架构的示意图。图 1 所示的架构 100 包括区块链节点 110 和用户节点 120。

[27]区块链 (Blockchain) 是一个典型的分布式协同系统，多方共同维护一个不断增长的分布式数据记录，这些记录的数据通过密码学技术保护内容和时序，使得任何一方难以篡改、抵赖、造假。

[28]在区块链中，数据 (例如，打包交易数据、交易执行结果等) 可以以区块 (Block) 的形式被封装。区块彼此之间可以通过前向的应用彼此链接形成“链”，即区块链。在一些实现方式中，每个区块记录着上一个区块的哈希值、本区块中的交易集合、本区块

的哈希等基础数据。

[29]通常，区块链的用户节点 120 可以通过客户端与区块链节点 110 进行通信。在一些情况下，用户节点 120 可以将需要存储的数据，以提交交易（Transaction）的方式发送给关联的一个或多个区块链节点 110。其中，交易可以理解为区块链上的一个事务请求，用来承载具体业务操作数据的结构。区块链上所有针对世界状态的变化操作均可以是基于交易来完成的。

[30]相应地，区块链节点 110 在验证数据的有效性之后，可以通过全网广播的方式将数据广播至每个区块链节点 110。这样，每个区块链节点 110 都记录有全量的、一致的数据。

[31]例如，在本公开实施例的进行汇款交易的场景中，上述区块链节点 110 可以是具有执行汇款相关功能的节点，例如，记录汇款交易的交易状态等。相应地，上述用户节点 120 可以包括位于汇款发起方的用户节点，例如，资方 A 的用户节点 122。上述用户节点 120 还可以包括执行汇款的汇款机构的用户节点，例如，汇款银行的用户节点 121。上述用户节点 120 还可以接收汇款的收款机构的用户节点，例如，收款银行的用户节点 123。

[32]在一些实现方式中，上述区块链节点 110 可以是服务器，或者其他具有计算能力的设备。上述用户节点 120 可以是服务器、移动终端，或者其他具有计算能力的设备。

[33]智能合约（Smart Contracts）。

[34]智能合约是一套以数字形式定义的承诺，包括合约参与方可以在上面执行这些承诺的协议。或者说，智能合约可以理解为部署在计算机系统上的一段程序，当智能合约的触发条件被满足时，智能合约可以被自动地执行。

[35]区块链的出现为智能合约的实现提供了技术支撑。将智能合约以数字化的形式写入区块链中，由区块链技术的特性保障智能合约的存储、读取、执行整个过程透明可跟踪、不可篡改。另一方面，可以由区块链自带的共识算法构建出一套状态机系统，使得智能合约能够高效地运行。

[36]在一些实现方式中，用户可以通过向区块链系统提交交易的方式，调用智能合约，并对智能合约中记录的数据进行设置，并将设置后的智能合约存储在区块链中。相应地，当智能合约的特定条件被触发后，区块链节点可以执行智能合约，并记录智能合约的执行结果，智能合约的执行状态。

[37]目前，区块链可以通过执行汇款交易合约来为汇款交易提供服务。当汇款发起方需要发起目标汇款交易时，汇款发起方需要先通过金融平台的中心化系统，查询目标汇款交易的参与方的可用汇款汇路，其中，可用汇款汇路可以理解为可以进行汇款交易的付款方和收款方之间的路径。如果汇款发起方查询到的可用汇款汇路与目标汇款交易所需的汇款汇路匹配，那么用户可以通过调用汇款交易合约的方式，在区块链上发起目标汇款交易，此时，区块链可以通过执行汇款交易合约来记录目标汇款交易的交易结果。

[38]下文结合图 2 以汇款发起方为资方 A 发起目标汇款交易为例，介绍目标汇款交易的发起过程。假设资方 A 需要向资方 B 进行目标汇款交易，且该目标汇款交易所需的汇款汇路为汇款机构 A 向汇款机构 B 进行汇款。另外，中心化系统中会记录汇款机构 A 的可用汇款汇路。

[39]在步骤 S210 中，资方 A 需要向中心化系统发送查询请求，以查询汇款机构 A 的可用汇款汇路。

[40]在步骤 S220 中，如果汇款机构 A 的可用汇款汇路中未记录汇款机构 A 向汇款机构 B 的汇款汇路，即汇款机构 A 的可用汇款汇路与目标汇款交易所需的汇款汇路不匹配，资方 A 不向区块链发起目标汇款交易。

[41]在步骤 S230 中，如果汇款机构 A 的可用汇款汇路中记录有汇款机构 A 向汇款机构 B 的汇款汇路，即汇款机构 A 的可用汇款汇路与目标汇款交易所需的汇款汇路匹配时，资方 A 可以通过调用区块链中的汇款交易合约的方式，来记录链下执行的目标汇款交易的交易状态。其中，上述交易状态包括：等待对方确认、交易成功、交易失败等。

[42]在步骤 S240 中，区块链执行汇款交易合约，以记录链下执行的目标汇款交易的交易状态。

[43]然而，如上文所述，目标汇款交易的参与方的可用汇款汇路都是通过中心化系统维护的。在一些情况下，当汇款发起方通过中心化系统查询可用汇款汇路时，中心化系统会由于系统错误，导致维护的可用汇款汇路错误，从而向汇款发起方返回错误的结果。例如，原本参与方的可用汇款汇路与目标汇款交易所需的汇款汇路匹配，但是由于中心化系统错误，导致维护的参与方的可用汇款汇路错误，将参与方的可用汇款汇路记录为不可用的汇款汇路，并向汇款发起方返回了“不匹配，或不存在可用汇款汇路”等的错误结果，导致汇款发起方无法发起目标汇款交易，降低用户体验。

[44]另一方面，由于中心化系统存在作恶的可能性，通过中心化系统来维护参与方的可

用汇款汇路，可能导致可用汇款汇路的安全性降低。

[45]因此，为了避免上述问题，本公开提供了一种基于区块链的汇款汇路管理方法，即在区块链上通过第一智能合约来维护上述参与方的可用汇款汇路，使得作为区块链用户的参与方，可以通过调用第一智能合约来自主地维护可用汇款汇路，有利于降低中心化系统维护可用汇款汇路时发生错误的可能性，提高用户体验。

[46]另一方面，在区块链上通过第一智能合约来维护上述参与方的可用汇款汇路，有利于提高可用汇款汇路的安全性。

[47]下文结合图 3 介绍本公开实施例的基于区块链的汇款汇路管理方法。为了便于理解，先介绍本公开实施例的第一智能合约。

[48]第一智能合约用于管理目标汇款交易的多个参与方中的至少一个参与方的可用汇款汇路。其中至少一个参与方的可用汇款汇路用于指示至少一个参与方能够为目标汇款交易提供的可用汇款汇路。因此，第一智能合约也可以称为“汇路管理合约”。

[49]假设目标汇款交易所需的汇款汇路为从银行 A 向银行 B 进行汇款交易，也就是说，目标汇款交易的多个参与方包括银行 A 和银行 B。表 1 示出了本公开实施例中第一智能合约记录可用汇款汇路的一种可能的实现方式。

表 1

参与方的可用汇款汇路	
用户地址	汇路列表
银行 A	银行 A-银行 B，银行 A 分行 1-银行 A 分行 3
银行 B	银行 B-银行 A，银行 B 分行 2-银行 B 分行 3，银行 B-银行 C

[50]参见表 1，第一智能合约中记录有银行 A 和银行 B 的可用汇款汇路。其中，银行 A 的可用汇款汇路包括：银行 A 与银行 B 之间的汇款汇路；银行 A 分行 1 与银行 A 分行 2 之间的汇款汇路。银行 B 的可用汇款汇路包括：银行 B 与银行 A 之间的汇款汇路；银行 B 分行 2 与银行 B 分行 3 之间的汇款汇路；以及银行 B 与银行 C 之间的汇款汇路。

[51]需要说明的是，上述可用汇款汇路用于指示汇款交易可以使用的路径，并不用于限定执行汇款交易时的汇款方向。例如，可用汇款汇路“银行 A-银行 B”可以用于指示在银行 A 和银行 B 之间进行汇款交易，也就是说，可以从银行 A 向银行 B 进行汇款，也可以从银行 B 向银行 A 进行汇款。

[52]另外，第一智能合约还可以记录其他机构的可用汇款汇路，例如，可以记录银行 D 的可用汇款汇路。本公开实施例对此不作限定。

[53]在一些情况下，可用汇款汇路可能对汇款使用的货币种类有限制。例如，对于可用汇款汇路“银行 A-银行 B”而言，该可用汇款汇路仅支持货币种类 1（例如，人民币）的汇款方式。这样，在上述第一智能合约中还可以记录每条可用汇款汇路支持的货币种类。例如，可以按照“银行 A -银行 B -货币种类”这一格式，在第一智能合约中记录。当然，对于对货币种类没有限制的可用汇款汇路而言，也可以不记录可用汇款汇路支持的货币种类。本公开实施例对此不作限定。

[54]为了便于查询第一智能合约，可以为上述第一智能合约设置查询接口，以便区块链的其他用户可以通过查询接口来查询第一智能合约中记录的可用汇款汇路。另外，为了便于更新第一智能合约，还可以为上述第一智能合约设置更新接口，这样，参与方可以通过更新接口来调用第一智能合约，以对第一智能合约中记录的可用汇款汇路进行更新。上述第一智能合约的查询、更新的过程将在下文结合图 4 至图 6 介绍，为了简洁，在此不再赘述。

[55]另外，本公开对上述第一智能合约的创建过程不作限定，上述第一智能合约可以是区块链的供应商创建并部署在区块链中的，以便区块链的用户（例如，上述目标汇款交易的参与方）通过更新接口来调用，并在第一智能合约中记录参与方的可用汇款汇路。当然，上述第一智能合约还可以是区块链的用户创建并部署在区块链中的，例如，可以是目标汇款交易的参与方创建的，这样目标汇款交易的参与方在创建第一智能合约的过程中，可以直接将可用的汇款汇路连同第一智能合约一起部署在区块链上。

[56]图 3 是本公开实施例的区块链的汇款汇路管理方法的示意性流程图。图 3 所示的方法包括步骤 S310 至步骤 S330。图 3 所示的方法可以应用于图 1 所示的区块链架构中，这样，执行步骤 S310 的第一参与方可以是区块链的用户 120，例如，汇款银行的用户节点 121 或者收款银行的用户节点 123。相应地，执行步骤 S320 和步骤 S330 的区块链节点可以是架构 100 中可以与用户 120 通信的一个或多个区块链节点 110。

[57]在步骤 S310 中，第一参与方获取第一参与方的可用汇款汇路。

[58]上述第一参与方的可用汇款汇路可以理解为第一参与方的待上链的可用汇款汇路。例如，可以是第一参与方需要更新的可用汇款汇路。又例如，可以是第一参与方新创建的可用汇款汇路。

[59]在步骤 S320 中，区块链节点从第一参与方接收第一智能合约的第一调用请求。

[60]上述第一参与方为参与目标汇款交易的多个参与方中的一个。上述第一参与方可以是执行目标汇款交易的汇款银行，上述第一参与方还可以是执行目标汇款交易的收款银行。

[61]上述第一调用请求用于设置第一参与方的可用汇款汇路。在一些实现方式中，上述设置可以理解为创建，此时，第一调用请求可以理解为用于创建第一参与方的可用汇款汇路。在另一些实现方式中，上述设置可以理解为更新，此时，第一调用请求可以理解为用于更新第一参与方的可用汇款汇路。

[62]在步骤 S330 中，区块链节点根据第一调用请求，在第一智能合约中设置第一参与方的可用汇款汇路。

[63]通常，为了提高可用汇款汇路的安全性，在步骤 S330 之前，区块链节点可以对第一参与方进行用户鉴权，以确定第一参与方有权利对可用汇款汇路进行设置。例如，确认第一参与方是链上用户，并且第一参与方的角色为银行，此时，第一参与方有权利对可用汇款汇路进行设置。在一些实现方式中，上述用户鉴权可以基于公钥和数据签名来实现。具体地，区块链节点可以存有第一参与方的公钥，并且，第一参与方在设置可用汇款汇路时，可以使用第一参与方的私钥对可用汇款汇路进行数字签名，这样，当区块链节点收到第一参与方上传的可用汇款汇路时，区块链节点可以使用第一参与方的公钥对可用汇款汇路上的数字签名进行验证，如果验证通过，那么第一参与方有权利设置可用汇款汇路。相反，如果验证不通过，那么第一参与方没有权利设置可用汇款汇路。

[64]另外，为了确认第一参与方设置的可用汇款汇路的合法性，在步骤 S330 之前，区块链节点还可以对第一参与方上传的可用汇款汇路进行合法性验证。在一些实现方式中，区块链可以按照汇款汇路指定的可用汇款汇路的格式（例如，可以是表 1 中所示出的格式），来确定可用汇款汇路涉及的汇款方和收款方是不是都是合法的链上用户，如果汇款方和收款方都是合法的链上用户，区块链节点可以确定第一参与方设置的可用汇款汇路是合法的，那么区块链节点可以在第一智能合约维护可用汇款汇路。相反，如果汇款方和/或收款方不是合法的链上用户，区块链节点可以确定第一参与方设置的可用汇款汇路是不合法的，那么区块链节点不会对可用汇款汇路进行维护。

[65]在一些实现方式中，上述区块链节点确定可用汇款汇路涉及的汇款方和收款方是不是合法的链上用户，可以通过汇款方、收款方是不是具有对应的链上用户来判断。例如，

区块链节点可以存有全部链上用户的链上用户名和该用户的链下用户名之间的对应关系，并且上述可用汇款汇路的汇款方、收款方使用的是汇款方、收款方的链下用户名（例如，银行的名称），此时，区块链可以基于上述映射关系，以及汇款方、收款方的链下用户名，来判断汇款方、收款方是否具有对应的链上用户名，以便确定汇款方、收款方是不是合法的链上用户。

[66]为了便于理解本公开，下文以对第一智能合约更新为例，结合图 4 介绍本公开实施例的第一智能合约的更新过程。需要说明的是，图 4 主要介绍对第一智能合约进行更新的方法流程，关于第一参与方、第一智能合约、可用汇款汇路、用户鉴权、合法性验证等内容的相关介绍可以参见上文，为了简洁，在此不再赘述。

[67]图 4 是本公开实施例的第一智能合约的更新过程的示意性流程图。图 4 所示的方法包括步骤 S410 至步骤 S460。

[68]在步骤 S410 中，第一参与方设置更新后的可用汇款汇路列表。

[69]第一参与方可以通过调用第一智能合约的更新接口，来输入第一可用汇款汇路列表。

[70]在步骤 S420 中，区块链节点对第一参与方进行用户鉴权。

[71]上述更新后的汇款汇路是通过第一参与方的私钥进行数字签名的。区块链节点可以基于第一参与方的公钥对数字签名进行验证，以确定第一参与方进行用户鉴权，如果用户鉴权通过，可以执行步骤 S430。如果用户鉴权不通过，则更新失败，执行步骤 S440 结束更新流程。

[72]在步骤 S430 中，区块链节点对可用汇款汇路列表中的可用汇款汇路进行合法性验证。

[73]如果合法性验证通过，则执行步骤 S450。如果合法性验证不通过，则更新失败，执行步骤 S440。

[74]在步骤 S450 中，区块链节点将第一智能合约中的可用汇款汇路更新为上述第一可用汇款汇路列表。

[75]在步骤 S460 中，第一智能合约更新成功。

[76]区块链节点可以将上述第一可用汇款汇路列表作为第一智能合约的数据，持久化存储在区块链中。

[77]需要说明的是，本公开对上述步骤 S420 和步骤 S430 之间的执行顺序不作限定。上述步骤 S430 也可以在步骤 S420 之前执行，此时，当步骤 S430 的合法性验证为通过时，

可以执行步骤 S420，并且只有当步骤 S420 的用户鉴权结果也为通过时，才能继续执行步骤 S450。当然，步骤 S420 和步骤 S430 也可以同时执行，即只有当步骤 S420 的用户鉴权结果以及步骤 S430 的合法性验证同时为通过时，才能执行步骤 S450。

[78]如上文所述，在传统的汇款交易发起过程中，汇款发起方需要先去中心化系统查询参与方的可用汇款汇路。但是，在一些情况下，汇款发起方可能并没按照流程先查询可用汇款汇路，而是直接在链上发起了第一交易执行请求，以请求第一参与方执行目标汇款交易。此时，如果目标汇款交易所需的汇款汇路与第一参与方的可用汇款汇路不匹配，便需要第一参与方确认可用汇款汇路与目标汇款交易所需的汇款汇路不匹配，之后链上发起的第一交易才能关闭。然而，第一参与方如果不能及时确认，第一交易的交易状态便会一直停滞，并处于“等待第一参与方确认”的状态，这样，汇款发起方便无法及时获知第一交易最终的执行结果，降低了用户体验。

[79]为了避免上述问题，本公开还提供一种区块链的汇款汇路管理方法，将第一智能合约中记录的可用汇款汇路与目标汇款交易所需的汇款汇路进行匹配，得到匹配结果，并基于匹配结果自动推进第一交易的交易状态，避免了传统的汇款交易提交方式下，由于第一参与方无法及时确认，导致第一交易的交易状态停滞，汇款发起方便无法及时获知第一交易最终的执行结果，有利于提高用户体验。

[80]继续参见图 3，上述方法还可以包括步骤 S340 至步骤 S360。

[81]在步骤 S340 中，从第二参与方接收第一交易执行请求，第一交易执行请求用于请求第一参与方执行目标汇款交易。

[82]上述第二参与方可以是目标汇款交易的发起方，例如，可以是上文介绍的资方 A。

[83]在步骤 S350 中，响应于第一交易执行请求，调用第一智能合约，以查询目标汇款交易所需的汇款汇路与第一参与方的可用汇款汇路是否匹配。

[84]若目标汇款交易所需的汇款汇路与第一参与方的可用汇款汇路匹配，可以理解为，第一参与方的可用汇款汇路中包含目标汇款交易所需的汇款汇路。例如，目标汇款交易所需的汇款汇路为从银行 A 向银行 B 汇款，此时，如果银行 A 作为第一参与方，并参见表 1 可知，银行 A 的可用汇款汇路中包含“银行 A-银行 B”，那么银行 A 的可用汇款汇路与目标汇款交易所需的汇款汇路匹配。

[85]若目标汇款交易所需的汇款汇路与第一参与方的可用汇款汇路不匹配，可以理解为，第一参与方的可用汇款汇路中不包含目标汇款交易所需的汇款汇路。例如，目标汇款交

易所需的汇款汇路为从银行 A 向银行 C 汇款，此时，如果银行 A 作为第一参与方，并参见表 1 可知，银行的可用汇款汇路中并不包含“银行 A-银行 C”的汇款汇路，那么银行 A 的可用汇款汇路与目标汇款交易所需的汇款汇路不匹配。

[86]在步骤 S360 中，如果目标汇款交易所需的汇款汇路与第一参与方的可用汇款汇路不匹配，终止目标汇款交易。

[87]上述终止目标汇款交易可以理解为，将第一交易的交易状态设置为终止。

[88]在一些实现方式中，上述结合步骤 S340 至步骤 S360 介绍的方案，可以通过调用合约的方式，来向区块链发起目标汇款交易。也就是说，上述第二参与方可以通过调用合约的方式，请求第一参与方执行目标汇款交易。或者说，上述第一交易执行请求为第二智能合约的调用请求，第二智能合约用于执行目标汇款交易，并且，第二智能合约的状态用于表示目标汇款交易的交易状态。因此，第二智能合约又称为“汇款交易合约”。其中，第二智能合约可以包含目标汇款交易的交易信息。例如，目标汇款交易的发起方信息，目标汇款交易的收款方信息，目标汇款交易所需的汇款汇路以及目标汇款交易的交易详情等。

[89]为了将上述匹配结果，与第二智能合约的状态关联起来，可以在第二智能合约中设置第一智能合约的地址，这样，在执行第二智能合约的过程中，便可以基于地址来调用第一智能合约，以查询目标汇款交易所需的汇款汇路与第一参与方的可用汇款汇路是否匹配。如果目标汇款交易所需的汇款汇路与第一参与方的可用汇款汇路不匹配，那么可以终止目标汇款交易，并将第二智能合约的状态设置为关闭。如果目标汇款交易所需的汇款汇路与第一参与方的可用汇款汇路匹配，那么可以将第二智能合约的状态推进到下一个状态（例如，等待参与方确认当前交易）。

[90]如上文介绍，区块链上的参与方都可以作为区块链的用户，通过调用第一智能合约的方式来设置各自的可用汇款汇路。也就是说，第一智能合约中会记录多个参与方的可用汇款汇路，此时，在一些情况下，就可能存在汇款汇路 1 对于参与方 1 而言是可用汇款汇路，但是汇款汇路 1 对于参与方 2 而言却不是可用汇款汇路。此时，如果在进行匹配的过程中，仅匹配了参与方 1 的可用汇款汇路，那么匹配结果变为匹配，但其实汇款汇路 1 并不是可用汇款汇路，那么就会导致目标汇款交易失败。

[91]假如汇款汇路 1 原本为银行 A 和银行 B 之间的可用汇款汇路，但是处于一些原因，银行 B 和银行 A 需要对可用汇款汇路进行更新，将汇款汇路 1 更新为不可用的汇款汇

路。但是只有银行 B 更新成功，银行 A 未更新成功，此时汇款汇路 1 虽然不再是银行 A 和银行 B 之间的可用汇款汇路，但是它依然记录在银行 A 中的可用汇款汇路中。此时，如果发起的目标汇款交易所需的汇款汇路刚好是可用汇款汇路 1，并且在仅使用银行 A 的可用汇款汇路进行匹配的情况下，匹配结果就会是匹配，从而会导致目标汇款交易失败。

[92]因此，为了提高上述匹配结果的准确率，在匹配的过程中可以使用目标汇款交易所需的汇款汇路，与目标汇款交易的多个参与方的可用汇款汇路分别进行匹配，只有在所有的匹配结果为匹配的情况下，汇款汇路才是真正的可用汇款汇路。继续参见上文汇款汇路 1 的场景，此时，将汇款汇路 1 分别与银行 A 的可用汇款汇路以及银行 B 的可用汇款汇路分别进行匹配，那么汇款汇路 1 与银行 A 的可用汇款汇路的匹配结果为匹配，汇款汇路 1 与银行 B 的可用汇款汇路的匹配结果为不匹配，最终，汇款汇路 1 对应的匹配结果变为不匹配，那么便可以终止目标汇款交易。

[93]为了便于理解本公开，下文以在执行第二智能合约的过程中，调用第一智能合约为例，结合图 5 介绍本公开实施例的第一智能合约的使用过程。需要说明的是，图 5 主要介绍使用第一智能合约的方法流程，关于第一参与方、第一智能合约、可用汇款汇路、用户鉴权、合法性校验等内容的相关介绍可以参见上文，为了简洁，在此不再赘述。

[94]图 5 是本公开实施例的第一智能合约的使用过程的示意性流程图。图 5 所示的方法包括步骤 S510 至步骤 S590。

[95]在步骤 S510 中，汇款发起方向区块链节点发送第二智能合约的调用请求。

[96]该调用请求用于请求第一参与方执行目标汇款交易。其中，目标汇款交易所需的汇款汇路为第一参与方与第二参与方之间的汇款汇路。

[97]在步骤 S520 中，区块链节点对汇款发起方进行用户鉴权。

[98]上述汇款发起方会使用私钥对第二智能合约的调用请求进行签名，相应地，区块链节点在接收到上述第二智能合约的调用请求之后，可以使用汇款发起方的公钥对数字签名进行验证。如果用户鉴权结果为通过，执行步骤 S530。如果用户鉴权结果为不通过，执行步骤 S540，关闭目标汇款交易。

[99]在步骤 S530 中，区块链节点对第二智能合约进行合法性校验。

[100]上述合法性校验用于校验目标汇款交易的交易参数是否完备。例如，需要在第二智能合约中指定目标汇款交易的汇款机构以及收款机构的链上账户，目标汇款交易涉及的

汇款币种等信息。

[101]如果合法性校验结果为通过,执行步骤 S550。如果合法性校验结果为通过,执行步骤 S540,关闭目标汇款交易。

[102]在步骤 S550 中,从第二智能合约中提取目标汇款交易所需的汇款汇路。

[103]在步骤 S560 中,区块链节点调用第一智能合约,以查询目标汇款交易所需的汇款汇路分别与汇款机构以及收款机构的可用汇款汇路是否匹配。

[104]在执行第二智能合约的过程中,可以自动调用 2 次第一智能合约的查询接口,分别查询汇款机构的可用汇款汇路以及收款机构的可用汇款汇路是否都与目标汇款交易所需的汇款汇路匹配。如果汇款机构的可用汇款汇路以及收款机构的可用汇款汇路,都与目标汇款交易所需的汇款汇路匹配,执行步骤 S570。如果汇款机构的可用汇款汇路和/或收款机构的可用汇款汇路,都与目标汇款交易所需的汇款汇路不匹配,执行步骤 S540,关闭目标汇款交易。

[105]在步骤 S570 中,区块链节点将第二智能合约的状态推进为“等待参与方确认当前交易”。

[106]在步骤 S580 中,目标汇款交易的参与方确认第二智能合约对应的目标汇款交易。

[107]目标汇款交易的参与方可以通过拉块解析等方式,从区块链节点中获取第二智能合约中记录的目标汇款交易的交易信息。当目标汇款交易的参与方基于目标汇款交易的交易信息,确认链下的汇款交易执行无误后,可以调用第二智能合约的确认接口,来确认目标汇款交易。

[108]在步骤 S590 中,确认目标汇款交易的所有参与方是否均确认。

[109]在收到目标汇款交易的参与方的确认后,第二智能合约自动触发处理逻辑,来查询目标汇款交易所有的参与方是否均已确认目标汇款交易。如果目标汇款交易所有的参与方均确认,第二智能合约自动推进状态为终态,指示目标汇款交易成功,即步骤 S600。

[110]需要说明的是,本公开对上述步骤 S520 和步骤 S530 之间的执行顺序不作限定。上述步骤 S530 也可以在步骤 S520 之前执行,此时,当步骤 S530 的合法性验证为通过时,可以执行步骤 S520,并且只有当步骤 S520 的用户鉴权结果也为通过时,才能继续执行步骤 S550。当然,步骤 S520 和步骤 S530 也可以同时执行,即只有当步骤 S520 的用户鉴权结果以及步骤 S530 的合法性验证同时为通过时,才能执行步骤 S550。

[111]上文以第二智能合约调用第一智能合约的方式为例，结合图 5 介绍了本公开实施例的第一智能合约的使用过程。在本公开实施例中，还可以仅通过第一智能合约的查询接口来查询可用汇款汇路。下文结合图 6 介绍本公开实施例的第一智能合约的查询过程。需要说明的是，图 6 主要介绍使用第一智能合约的方法流程，关于第一参与方、第一智能合约、可用汇款汇路等内容的相关介绍可以参见上文，为了简洁，在此不再赘述。

[112]图 6 是本公开实施例的第一智能合约的查询过程的示意性流程图。图 6 所示的方法包括步骤 S610 至步骤 S620。

[113]在步骤 S610 中，区块链节点从第三参与方接收第一智能合约的第二调用请求，第二调用请求用于查询第一参与方的可用汇款汇路。

[114]在步骤 S620 中，区块链节点向第三参与方返回第一参与方的可用汇款汇路。

[115]上文结合图 1 至图 6，详细描述了本公开的方法实施例，下面结合图 7 至图 10，详细描述本公开的装置实施例。应理解，方法实施例的描述与装置实施例的描述相互对应，因此，未详细描述的部分可以参见前面方法实施例。

[116]图 7 是本公开实施例的基于区块链的汇款汇路管理装置的示意性结构图。图 7 所示的装置可以为区块链上的区块链节点，该区块链上存储有第一智能合约，第一智能合约用于管理目标汇款交易的多个参与方中的至少一个参与方的可用汇款汇路，至少一个参与方的可用汇款汇路用于指示至少一个参与方能够为目标汇款交易提供的可用汇款汇路，至少一个参与方包括第一参与方。上述装置 700 包括：接收模块 710 和处理模块 720。

[117]接收模块 710 可以被配置为从第一参与方接收第一智能合约的第一调用请求，第一调用请求用于设置第一参与方的可用汇款汇路。

[118]处理模块 720 可以被配置为根据第一调用请求，在第一智能合约中设置第一参与方的可用汇款汇路。

[119]可选地，在一些实施例中，多个参与方包括第二参与方，接收模块 710 还可以被配置为从第二参与方接收第一交易执行请求，第一交易执行请求用于请求第一参与方执行目标汇款交易；处理模块 720 可以被配置为响应于第一交易执行请求，调用第一智能合约，以查询目标汇款交易所需的汇款汇路与第一参与方的可用汇款汇路是否匹配；以及，如果目标汇款交易所需的汇款汇路与第一参与方的可用汇款汇路不匹配，终止目标汇款交易。

[120]可选地，在一些实施例中，多个参与方包括第三参与方，接收模块 710 可以被配置

为从第三参与方接收第一智能合约的第二调用请求,第二调用请求用于查询第一参与方的可用汇款汇路;处理模块 720 可以被配置为向第三参与方返回第一参与方的可用汇款汇路。

[121]可选地,在一些实施例中,接收模块 710 可以被配置为从第一参与方接收第一智能合约的第三调用请求,第三调用请求用于更新第一参与方的可用汇款汇路;处理模块 720 可以被配置为基于第三调用请求,在第一智能合约中更新第一参与方的可用汇款汇路。

[122]可选地,在一些实施例中,第一智能合约还用于管理第一参与方的可用汇款汇路支持的货币种类。

[123]图 8 是本公开另一实施例的基于区块链的汇款汇路管理装置的示意性结构图。该区块链上存储有第一智能合约,第一智能合约用于管理目标汇款交易的多个参与方中的至少一个参与方的可用汇款汇路,至少一个参与方的可用汇款汇路用于指示至少一个参与方能够为目标汇款交易提供的可用汇款汇路,至少一个参与方包括第一参与方,装置应用于第一参与方。装置 800 包括:获取模块 810 和发送模块 820。

[124]获取模块 810,被配置为获取第一参与方的可用汇款汇路;发送模块 820,被配置为向区块链发送第一智能合约的第一调用请求,第一调用请求用于设置第一参与方的可用汇款汇路。

[125]可选地,在一些实施例中,发送模块 820 可以被配置为向区块链发送第一智能合约的第三调用请求,第三调用请求用于更新第一参与方的可用汇款汇路。

[126]可选地,在一些实施例中,第一智能合约还用于管理第一参与方的可用汇款汇路支持的货币种类。

[127]图 9 是本公开又一实施例提供的基于区块链的汇款汇路管理装置的示意性结构图。图 9 所示的装置 900 可以是区块链中的任意区块链节点。该装置 900 例如可以是具有计算功能的计算设备。比如,装置 900 可以是服务器。装置 900 可以包括存储器 910 和处理器 920。存储器 910 可用于存储可执行代码。处理器 920 可用于执行所述存储器 910 中存储的可执行代码,以实现前文描述的各个方法中的步骤。在一些实施例中,该装置 900 还可以包括网络接口 930,处理器 920 与外部设备的数据交换可以通过该网络接口 930 实现。

[128]图 10 是本公开又一实施例提供的基于区块链的汇款汇路管理装置的示意性结构图。图 10 所示的装置 1000 可以是区块链中的客户端所在的节点。该装置 1000 例如可以是

具有计算功能的计算设备。比如，装置 1000 可以是服务器或者移动终端。装置 1000 可以包括存储器 1010 和处理器 1020。存储器 1010 可用于存储可执行代码。处理器 1020 可用于执行所述存储器 1010 中存储的可执行代码，以实现前文描述的各个方法中的步骤。在一些实施例中，该装置 900 还可以包括网络接口 1030，处理器 1020 与外部设备的数据交换可以通过该网络接口 1030 实现。

[129]应理解，在本公开实施例中，该处理器可以采用通用的中央处理器（central processing unit, CPU），该处理器还可以是其他通用处理器、数字信号处理器（digital signal processor, DSP）、专用集成电路（application specific integrated circuit, ASIC）、现成可编程门阵列（field programmable gate array, FPGA）或者其他可编程逻辑器件、分立门或者晶体管逻辑器件、分立硬件组件等。通用处理器可以是微处理器或者该处理器也可以是任何常规的处理器等，用于执行相关程序，以实现本公开实施例所提供的技术方案。

[130]该存储器可以包括只读存储器和随机存取存储器，并向处理器提供指令和数据。处理器的一部分还可以包括非易失性随机存取存储器。例如，处理器还可以存储设备类型的信息。

[131]在实现过程中，上述方法的各步骤可以通过处理器中的硬件的集成逻辑电路或者软件形式的指令完成。结合本公开实施例所公开的用于请求上行传输资源的方法可以直接体现为硬件处理器执行完成，或者用处理器中的硬件及软件模块组合执行完成。软件模块可以位于随机存储器，闪存、只读存储器，可编程只读存储器或者电可擦写可编程存储器、寄存器等本领域成熟的存储介质中。该存储介质位于存储器，处理器读取存储器中的信息，结合其硬件完成上述方法的步骤。为避免重复，这里不再详细描述。

[132]应理解，本文中术语“和/或”，仅仅是一种描述关联对象的关联关系，表示可以存在三种关系，例如，A 和/或 B，可以表示：单独存在 A，同时存在 A 和 B，单独存在 B 这三种情况。另外，本文中字符“/”，一般表示前后关联对象是一种“或”的关系。

[133]应理解，在本公开的各种实施例中，上述各过程的序号的大小并不意味着执行顺序的先后，各过程的执行顺序应以其功能和内在逻辑确定，而不应对本公开实施例的实施过程构成任何限定。

[134]在本公开所提供的几个实施例中，应该理解到，所揭露的系统、装置和方法，可以通过其它的方式实现。例如，以上所描述的装置实施例仅仅是示意性的，例如，所述单

元的划分, 仅仅为一种逻辑功能划分, 实际实现时可以有另外的划分方式, 例如多个单元或组件可以结合或者可以集成到另一个系统, 或一些特征可以忽略, 或不执行。另一点, 所显示或讨论的相互之间的耦合或直接耦合或通信连接可以是通过一些接口, 装置或单元的间接耦合或通信连接, 可以是电性, 机械或其它的形式。

[135]所述作为分离部件说明的单元可以是或者也可以不是物理上分开的, 作为单元显示的部件可以是或者也可以不是物理单元, 即可以位于一个地方, 或者也可以分布到多个网络单元上。可以根据实际的需要选择其中的部分或者全部单元来实现本实施例方案的目的。

[136]另外, 在本公开各个实施例中的各功能模块可以集成在一个模块中, 也可以是各个模块单独存在, 也可以两个或两个以上模块集成在一个模块中。

[137]在上述实施例中, 可以全部或部分地通过软件、硬件、固件或者其任意组合来实现。当使用软件实现时, 可以全部或部分地以计算机程序产品的形式实现。所述计算机程序产品包括一个或多个计算机指令。在计算机上加载和执行所述计算机程序指令时, 全部或部分地产生按照本公开实施例所述的流程或功能。所述计算机可以是通用计算机、专用计算机、计算机网络、或者其他可编程装置。所述计算机指令可以存储在计算机可读存储介质中, 或者从一个计算机可读存储介质向另一个计算机可读存储介质传输, 例如, 所述计算机指令可以从一个网站站点、计算机、服务器或数据中心通过有线(例如同轴电缆、光纤、数字用户线(digital subscriber Line, DSL))或无线(例如红外、无线、微波等)方式向另一个网站站点、计算机、服务器或数据中心进行传输。所述计算机可读存储介质可以是计算机能够读取的任何可用介质或者是包含一个或多个可用介质集成的服务器、数据中心等数据存储设备。所述可用介质可以是磁性介质,(例如, 软盘、硬盘、磁带)、光介质(例如, 数字通用光盘(digital video disc, DVD))或者半导体介质(例如, 固态硬盘(solid state disk, SSD))等。

[138]以上所述, 仅为本公开的具体实施方式, 但本公开的保护范围并不局限于此, 任何熟悉本技术领域的技术人员在本公开揭露的技术范围内, 可轻易想到变化或替换, 都应涵盖在本公开的保护范围之内。因此, 本公开的保护范围应以所述权利要求的保护范围为准。

权利要求书

1、一种基于区块链的汇款汇路管理方法，所述区块链上存储有第一智能合约，所述第一智能合约用于管理目标汇款交易的多个参与方中的至少一个参与方的可用汇款汇路，所述至少一个参与方的可用汇款汇路用于指示所述至少一个参与方能够为所述目标汇款交易提供的可用汇款汇路，所述至少一个参与方包括第一参与方，

所述方法包括：

从所述第一参与方接收所述第一智能合约的第一调用请求，所述第一调用请求用于设置所述第一参与方的可用汇款汇路；

根据所述第一调用请求，在所述第一智能合约中设置所述第一参与方的可用汇款汇路。

2、如权利要求1所述的方法，所述多个参与方包括第二参与方，所述方法还包括：

从所述第二参与方接收第一交易执行请求，所述第一交易执行请求用于请求所述第一参与方执行所述目标汇款交易；

响应于所述第一交易执行请求，调用所述第一智能合约，以查询所述目标汇款交易所需的汇款汇路与所述第一参与方的可用汇款汇路是否匹配；

如果所述目标汇款交易所需的汇款汇路与所述第一参与方的可用汇款汇路不匹配，终止所述目标汇款交易。

3、根据权利要求1所述的方法，所述多个参与方包括第三参与方，所述方法还包括：

从所述第三参与方接收所述第一智能合约的第二调用请求，所述第二调用请求用于查询所述第一参与方的可用汇款汇路；

向所述第三参与方返回所述第一参与方的可用汇款汇路。

4、根据权利要求1所述的方法，所述方法还包括：

从所述第一参与方接收所述第一智能合约的第三调用请求，所述第三调用请求用于更新所述第一参与方的可用汇款汇路；

基于所述第三调用请求，在所述第一智能合约中更新所述第一参与方的可用汇款汇路。

5、如权利要求1-4中任一项所述的方法，所述第一智能合约还用于管理所述第一参与方的可用汇款汇路支持的货币种类。

6、一种基于区块链的汇款汇路管理方法，所述区块链上存储有第一智能合约，所述第一智能合约用于管理目标汇款交易的多个参与方中的至少一个参与方的可用汇款

汇路,所述至少一个参与方的可用汇款汇路用于指示所述至少一个参与方能够为所述目标汇款交易提供的可用汇款汇路,所述至少一个参与方包括第一参与方,所述方法应用于所述第一参与方,

所述方法包括:

获取所述第一参与方的可用汇款汇路;

向所述区块链发送所述第一智能合约的第一调用请求,所述第一调用请求用于设置所述第一参与方的可用汇款汇路。

7、根据权利要求6所述的方法,所述方法还包括:

向所述区块链发送所述第一智能合约的第三调用请求,所述第三调用请求用于更新所述第一参与方的可用汇款汇路。

8、如权利要求6或7所述的方法,所述第一智能合约还用于管理所述第一参与方的可用汇款汇路支持的货币种类。

9、一种基于区块链的汇款汇路管理装置,所述区块链上存储有第一智能合约,所述第一智能合约用于管理目标汇款交易的多个参与方中的至少一个参与方的可用汇款汇路,所述至少一个参与方的可用汇款汇路用于指示所述至少一个参与方能够为所述目标汇款交易提供的可用汇款汇路,所述至少一个参与方包括第一参与方,

所述装置包括:

接收模块,被配置为从所述第一参与方接收所述第一智能合约的第一调用请求,所述第一调用请求用于设置所述第一参与方的可用汇款汇路;

处理模块,被配置为根据所述第一调用请求,在所述第一智能合约中设置所述第一参与方的可用汇款汇路。

10、如权利要求9所述的装置,所述多个参与方包括第二参与方,

所述接收模块,被配置为从所述第二参与方接收第一交易执行请求,所述第一交易执行请求用于请求所述第一参与方执行所述目标汇款交易;

所述处理模块,被配置为响应于所述第一交易执行请求,调用所述第一智能合约,以查询所述目标汇款交易所需的汇款汇路与所述第一参与方的可用汇款汇路是否匹配;

所述处理模块,被配置为如果所述目标汇款交易所需的汇款汇路与所述第一参与方的可用汇款汇路不匹配,终止所述目标汇款交易。

11、根据权利要求9所述的装置,所述多个参与方包括第三参与方,

所述接收模块,被配置为从所述第三参与方接收所述第一智能合约的第二调用请求,所述第二调用请求用于查询所述第一参与方的可用汇款汇路;

所述处理模块，被配置为向所述第三参与方返回所述第一参与方的可用汇款汇路。

12、根据权利要求 9 所述的装置，

所述接收模块，被配置为从所述第一参与方接收所述第一智能合约的第三调用请求，所述第三调用请求用于更新所述第一参与方的可用汇款汇路；

所述处理模块，被配置为基于所述第三调用请求，在所述第一智能合约中更新所述第一参与方的可用汇款汇路。

13、如权利要求 9-12 中任一项所述的装置，所述第一智能合约还用于管理所述第一参与方的可用汇款汇路支持的货币种类。

14、一种基于区块链的汇款汇路管理装置，所述区块链上存储有第一智能合约，所述第一智能合约用于管理目标汇款交易的多个参与方中的至少一个参与方的可用汇款汇路，所述至少一个参与方的可用汇款汇路用于指示所述至少一个参与方能够为所述目标汇款交易提供的可用汇款汇路，所述至少一个参与方包括第一参与方，所述装置应用于所述第一参与方，

所述装置包括：

获取模块，被配置为获取所述第一参与方的可用汇款汇路；

发送模块，被配置为向所述区块链发送所述第一智能合约的第一调用请求，所述第一调用请求用于设置所述第一参与方的可用汇款汇路。

15、根据权利要求 14 所述的装置，

所述发送模块，被配置为向所述区块链发送所述第一智能合约的第三调用请求，所述第三调用请求用于更新所述第一参与方的可用汇款汇路。

16、如权利要求 14 或 15 所述的装置，所述第一智能合约还用于管理所述第一参与方的可用汇款汇路支持的货币种类。

17、一种基于区块链的汇款汇路管理装置，包括存储器和处理器，所述存储器中存储有可执行代码，所述处理器被配置为执行所述可执行代码，以实现权利要求 1-5 中任一项所述的方法。

18、一种基于区块链的汇款汇路管理装置，包括存储器和处理器，所述存储器中存储有可执行代码，所述处理器被配置为执行所述可执行代码，以实现权利要求 6-8 中任一项所述的方法。