(19)中华人民共和国国家知识产权局

(12)发明专利申请

(10)申请公布号 CN 108805564 A
(43)申请公布日 2018.11.13

(21)申请号 201810387096.X

(22)申请日 2018.04.26

(71)申请人 布比(北京)网络技术有限公司
地址 100094 北京市海淀区东北旺村南1号楼7层7590室

(72)发明人 蒋海 李军 翟海滨 王璟

(74)专利代理机构 北京工信联合知识产权代理有限公司 11266
代理人 贾银秋

(51)Int.Cl.
G06Q 20/38(2012.01)

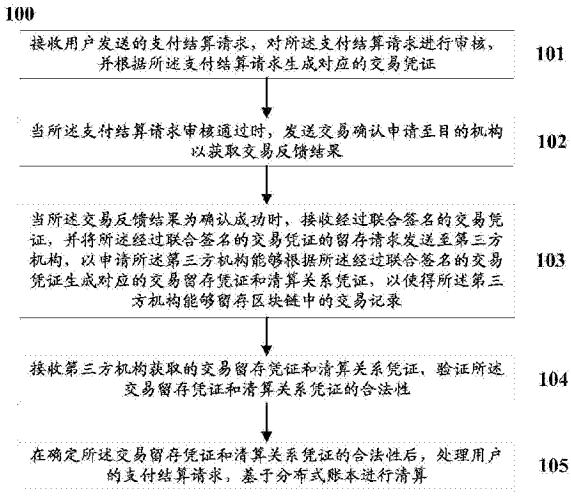
权利要求书4页 说明书12页 附图3页

(54)发明名称

一种基于区块链进行支付结算的方法及系统

(57)摘要

本发明公开了一种基于区块链进行支付结算的方法,包括:接收用户发送的支付结算请求,对所述支付结算请求进行审核,并根据所述支付结算请求生成对应的交易凭证,其中所述交易凭证为区块链中的交易记录;当所述支付结算请求审核通过时,发送交易确认申请至目的机构以获取交易反馈结果;当所述交易反馈结果为确认成功时,接收经过联合签名的交易凭证,并将留存请求发送至第三方机构,以确定交易留存凭证和清算关系凭证,以使得所述第三方机构能够留存区块链中的交易记录;接收第三方机构获取的交易留存凭证和清算关系凭证并验证合法性;在确定所述交易留存凭证和清算关系凭证的合法性后,处理用户的支付结算请求,基于分布式账本进行清算。



CN 108805564 A

1.一种基于区块链进行支付结算的方法，其特征在于，所述方法包括：

接收用户发送的支付结算请求，对所述支付结算请求进行审核，并根据所述支付结算请求生成对应的交易凭证，其中所述交易凭证为区块链中的交易记录；

当所述支付结算请求审核通过时，发送交易确认申请至目的机构以获取交易反馈结果；

当所述交易反馈结果为确认成功时，接收经过联合签名的交易凭证，并将所述经过联合签名的交易凭证的留存请求发送至第三方机构，以申请所述第三方机构能够根据所述经过联合签名的交易凭证生成对应的交易留存凭证和清算关系凭证，以使得所述第三方机构能够留存区块链中的交易记录；

接收第三方机构获取的交易留存凭证和清算关系凭证，验证所述交易留存凭证和清算关系凭证的合法性；

在确定所述交易留存凭证和清算关系凭证的合法性后，处理用户的支付结算请求，基于分布式账本进行清算。

2.根据权利要求1所述的方法，其特征在于，所述交易凭证包括：用户编号、交易凭证标识、资产地址、用户所属机构的标识、交易涉及的其他机构的标识、交易类型、资产类型、交易额度、交易涉及的机构的联合签名和交易时间戳。

3.根据权利要求2所述的方法，其特征在于，通过哈希算法获取所述交易凭证标识。

4.根据权利要求1所述的方法，其特征在于，所述对所述支付结算请求进行审核，包括：

判断提交所述支付结算请求的用户是否为发起机构的用户，包括：

如果所述支付结算请求的用户是发起机构的用户，则判断所述支付结算请求的用户是否有资格享受支付结算服务，如果是，则进行交易确认申请，反之，结束支付结算服务；

如果所述支付结算请求的用户不是发起机构的用户，则基于分布式账本查询所述支付结算请求涉及的所有机构的账户信息，并判断所述账户信息是否满足所述支付结算请求，如果满足，则进行交易确认申请，反之，结束支付结算服务。

5.根据权利要求1所述的方法，其特征在于，所述方法还包括：

在发送交易确认申请前，对所述交易凭证进行单独签名，并将经过单独签名的交易凭证发送至目的机构。

6.根据权利要求5所述的方法，其特征在于，所述目的机构确定交易反馈结果，包括：

目的机构根据所述经过单独签名的交易凭证，判断用户的支付结算请求的合法性，若合法，则对经过单独签名的交易凭证进行联合签名，并确定交易反馈结果为确认成功；若不合法，则直接确定交易反馈结果为确认失败。

7.根据权利要求5所述的方法，其特征在于，所述目的机构确定交易反馈结果，包括：

目的机构根据所述经过单独签名的交易凭证和其他辅助机构的交易请求确认结果判断用户的支付结算请求的合法性，若合法，则对经过单独签名的交易凭证进行联合签名，并确定交易反馈结果为确认成功；若不合法，则直接确定交易反馈结果为确认失败。

8.根据权利要求6或7所述的方法，其特征在于，所述方法还包括：

当所述交易反馈结果为确认失败时，拒绝用户的支付结算请求。

9.根据权利要求1所述的方法，其特征在于，所述清算关系凭证包括：清算关系凭证的标识、借方机构标识、贷方机构标识、资产借贷发生的类型、资产借贷发生的数量、贷方机构

和第三方机构的联合签名以及清算关系凭证时间戳。

10.根据权利要求1所述的方法，其特征在于，所述第三方机构处理所述经过联合签名的交易凭证的留存请求，并获取交易留存凭证和清算关系凭证的步骤包括：

第三方机构根据所述经过联合签名的交易凭证向所述支付结算请求涉及到的所有的目的机构发送交易凭证确认申请；

第三方机构接收所述支付结算请求涉及到的所有的目的机构返回的交易确认消息，以对所述经过联合签名的交易凭证的合法性进行验证，如果所述交易确认消息为确认成功，即指示所述经过联合签名的交易凭证的合法性验证通过，则根据所述经过联合签名的交易凭证生成对应的交易留存凭证和清算关系凭证。

11.根据权利要求1所述的方法，其特征在于，所述方法还包括：

第三方机构对清算关系凭证进行签名，并发送至所述支付结算请求涉及到的目的机构对清算关系凭证进行联合签名和确认；

在指示所述清算关系凭证进行联合签名和确认成功后，所述第三方机构向所述支付结算请求涉及到的所有的机构发送所述交易留存凭证和清算关系凭证。

12.根据权利要求11所述的方法，其特征在于，所述方法还包括：

在清算关系中涉及到的所有的机构收到第三方机构发送的交易留存凭证和清算关系凭证后，分别生成每个机构对应的清算凭证，并将所述每个机构对应的清算凭证在分布式账本中进行发布以获得全网的认可并存储。

13.根据权利要求12所述的方法，其特征在于，所述方法还包括：

在清算关系中涉及到的所有的机构在分布式账本中进行清算凭证的查询，确认清算关系是否已经成功执行。

14.根据权利要求12所述的方法，其特征在于，所述清算凭证包括：清算凭证标识、清算资产类型、转移资产数量、发起机构标识、目的机构标识、发起机构签名、清算凭证时间戳以及发起机构的资产来源。

15.一种基于区块链进行支付结算的系统，其特征在于，所述系统包括：

交易凭证生成模块，用于接收用户发送的支付结算请求，对所述支付结算请求进行审核，并根据所述支付结算请求生成对应的交易凭证，其中所述交易凭证为区块链中的交易记录；

交易反馈结果获取模块，用于当所述支付结算请求审核通过时，发送交易确认申请至目的机构以获取交易反馈结果；

交易留存凭证和清算关系凭证确定模块，用于当所述交易反馈结果为确认成功时，接收经过联合签名的交易凭证，并将所述经过联合签名的交易凭证的留存请求发送至第三方机构，以申请所述第三方机构能够根据所述经过联合签名的交易凭证生成对应的交易留存凭证和清算关系凭证，以使得所述第三方机构能够留存区块链中的交易记录；

合法性验证模块，用于接收第三方机构获取的交易留存凭证和清算关系凭证，验证所述交易留存凭证和清算关系凭证的合法性；

清算模块，用于在确定所述交易留存凭证和清算关系凭证的合法性后，处理用户的支付结算请求，基于分布式账本进行清算。

16.根据权利要求15所述的系统，其特征在于，所述交易凭证包括：用户编号、交易凭证

标识、资产地址、用户所属机构的标识、交易涉及的其他机构的标识、交易类型、资产类型、交易额度、交易涉及的机构的联合签名和交易时间戳。

17.根据权利要求16所述的系统，其特征在于，通过哈希算法获取所述交易凭证标识。

18.根据权利要求15所述的系统，其特征在于，所述交易凭证生成模块，对所述支付结算请求进行审核，包括：

判断提交所述支付结算请求的用户是否为发起机构的用户，包括：

如果所述支付结算请求的用户是发起机构的用户，则判断所述支付结算请求的用户是否有资格享受支付结算服务，如果是，则进行交易确认申请，反之，结束支付结算服务；

如果所述支付结算请求的用户不是发起机构的用户，则基于分布式账本查询所述支付结算请求涉及的所有机构的账户信息，并判断所述账户信息是否满足所述支付结算请求，如果满足，则进行交易确认申请，反之，结束支付结算服务。

19.根据权利要求15所述的系统，其特征在于，所述系统还包括：

交易凭证签名模块，用于在发送交易确认申请前，对所述交易凭证进行单独签名，并将经过单独签名的交易凭证发送至目的机构。

20.根据权利要求19所述的系统，其特征在于，所述交易反馈结果获取模块，确定交易反馈结果，包括：

交易反馈结果确定单元，用于根据所述经过单独签名的交易凭证，判断用户的支付结算请求的合法性，若合法，则对经过单独签名的交易凭证进行联合签名，并确定交易反馈结果为确认成功；若不合法，则直接确定交易反馈结果为确认失败。

21.根据权利要求19所述的系统，其特征在于，所述交易反馈结果获取模块，确定交易反馈结果，包括：

交易反馈结果确定单元，用于根据所述经过单独签名的交易凭证和其他辅助机构的交易请求确认结果判断用户的支付结算请求的合法性，若合法，则对经过单独签名的交易凭证进行联合签名，并确定交易反馈结果为确认成功；若不合法，则直接确定交易反馈结果为确认失败。

22.根据权利要求20或21所述的系统，其特征在于，所述系统还包括：

请求拒绝模块，用于当所述交易反馈结果为确认失败时，拒绝用户的支付结算请求。

23.根据权利要求15所述的系统，其特征在于，所述清算关系凭证，包括：清算关系凭证的标识、借方机构标识、贷方机构标识、资产借贷发生的类型、资产借贷发生的数量、贷方机构和第三方机构的联合签名以及清算关系凭证时间戳。

24.根据权利要求15所述的系统，其特征在于，所述交易留存凭证和清算关系凭证确定模块，接收经过联合签名的交易凭证的留存请求，根据所述经过联合签名的交易凭证生成对应的交易留存凭证和清算关系凭证，包括：

交易凭证确认申请发送单元，用于第三方机构根据所述经过联合签名的交易凭证向所述支付结算请求涉及到的所有的目的机构发送交易凭证确认申请；

凭证生成单元，用于第三方机构接收所述支付结算请求涉及到的所有的目的机构返回的交易确认消息，以对所述经过联合签名的交易凭证的合法性进行验证，如果所述交易确认消息为确认成功，即指示所述经过联合签名的交易凭证的合法性验证通过，则根据所述经过联合签名的交易凭证生成对应的交易留存凭证和清算关系凭证。

25.根据权利要求15所述的系统，其特征在于，所述系统还包括：

清算关系凭证签名模块，用于对清算关系凭证进行签名，并发送至所述支付结算请求涉及到的目的机构对清算关系凭证进行联合签名和确认；

交易留存凭证和清算关系凭证发送模块，用于在指示所述清算关系凭证的联合签名和确认成功后，向所述支付结算请求涉及到的所有的机构发送所述交易留存凭证和清算关系凭证。

26.根据权利要求25所述的系统，其特征在于，所述系统还包括：

清算凭证发布模块，用于在清算关系中涉及到的所有的机构收到第三方机构发送的交易留存凭证和清算关系凭证后，分别生成每个机构对应的清算凭证，并将所述每个机构对应的清算凭证在分布式账本中进行发布以获得全网的认可并存储。

27.根据权利要求26所述的系统，其特征在于，所述系统还包括：

清算关系确认模块，用于在清算关系中涉及到的所有的机构在分布式账本中进行清算凭证的查询，确认清算关系是否已经成功执行。

28.根据权利要求26所述的系统，其特征在于，所述清算凭证包括：清算凭证标识、清算资产类型、转移资产数量、发起机构标识、目的机构标识、发起机构签名、清算凭证时间戳以及发起机构的资产来源。

一种基于区块链进行支付结算的方法及系统

技术领域

[0001] 本发明涉及基于区块链的数字资产流通技术领域，并且更具体地，涉及一种基于区块链进行支付结算的方法及系统。

背景技术

[0002] 在目前所实施的资金支付和结算技术中，整个清算体系的正常运行依赖于中心化的清算机构，即基于传统银行或者清算中心的模式。然而，在当前海量交易和清算需求的背景下，基于传统银行或者清算中心的模式已无法满足要求，存在成本高、清算耗时长、复杂度高、清算中心单点故障或恶意行为导致的清算体系崩溃等缺点，对于在资金支付和结算过程中可能产生的交易纠纷、恶意交易等问题无法进行解决。

[0003] 区块链技术是使用分布式数据库来识别、记录和传播信息的点对点网络，也称为价值互联网。区块链上的信息具有即时验证、可追溯、但难以篡改和无法屏蔽的天然特性，从而创造了一套隐私、高效、安全的共享价值体系。

[0004] 因此，如何基于区块链技术实现资金支付和结算是急需解决的一个问题。

发明内容

[0005] 本发明提出一种基于区块链进行支付结算的方法及系统，以解决如何基于区块链技术实现资金支付和结算的问题。

[0006] 为了解决上述问题，根据本发明的一个方面，提供了一种基于区块链进行支付结算的方法，所述方法包括：

[0007] 接收用户发送的支付结算请求，对所述支付结算请求进行审核，并根据所述支付结算请求生成对应的交易凭证，其中所述交易凭证为区块链中的交易记录；

[0008] 当所述支付结算请求审核通过时，发送交易确认申请至目的机构以获取交易反馈结果；

[0009] 当所述交易反馈结果为确认成功时，接收经过联合签名的交易凭证，并将所述经过联合签名的交易凭证的留存请求发送至第三方机构，以申请所述第三方机构能够根据所述经过联合签名的交易凭证生成对应的交易留存凭证和清算关系凭证，以使得所述第三方机构能够留存区块链中的交易记录；

[0010] 接收第三方机构获取的交易留存凭证和清算关系凭证，验证所述交易留存凭证和清算关系凭证的合法性；

[0011] 在确定所述交易留存凭证和清算关系凭证的合法性后，处理用户的支付结算请求，基于分布式账本进行清算。

[0012] 优选地，其中所述交易凭证包括：用户编号、交易凭证标识、资产地址、用户所属机构的标识、交易涉及的其他机构的标识、交易类型、资产类型、交易额度、交易涉及的机构的联合签名和交易时间戳。

[0013] 优选地，其中通过哈希算法获取所述交易凭证标识。

[0014] 优选地，其中所述对所述支付结算请求进行审核，包括：

[0015] 判断提交所述支付结算请求的用户是否为发起机构的用户，包括：

[0016] 如果所述支付结算请求的用户是发起机构的用户，则判断所述支付结算请求的用户是否有资格享受支付结算服务，如果是，则进行交易确认申请，反之，结束支付结算服务；

[0017] 如果所述支付结算请求的用户不是发起机构的用户，则基于分布式账本查询所述支付结算请求涉及的所有机构的账户信息，并判断所述账户信息是否满足所述支付结算请求，如果满足，则进行交易确认申请，反之，结束支付结算服务。

[0018] 优选地，其中所述方法还包括：在发送交易确认申请前，对所述交易凭证进行单独签名，并将经过单独签名的交易凭证发送至目的机构。

[0019] 优选地，其中所述目的机构确定交易反馈结果，包括：

[0020] 目的机构根据所述经过单独签名的交易凭证，判断用户的支付结算请求的合法性，若合法，则对经过单独签名的交易凭证进行联合签名，并确定交易反馈结果为确认成功；若不合法，则直接确定交易反馈结果为确认失败。

[0021] 优选地，其中所述目的机构确定交易反馈结果，包括：

[0022] 目的机构根据所述经过单独签名的交易凭证和其他辅助机构的交易请求确认结果判断用户的支付结算请求的合法性，若合法，则对经过单独签名的交易凭证进行联合签名，并确定交易反馈结果为确认成功；若不合法，则直接确定交易反馈结果为确认失败。

[0023] 优选地，其中所述方法还包括：

[0024] 当所述交易反馈结果为确认失败时，拒绝用户的支付结算请求。

[0025] 优选地，其中所述清算关系凭证包括：清算关系凭证的标识、借方机构标识、贷方机构标识、资产借贷发生的类型、资产借贷发生的数量、贷方机构和第三方机构的联合签名以及清算关系凭证时间戳。

[0026] 优选地，其中所述第三方机构处理所述经过联合签名的交易凭证的留存请求，并获取交易留存凭证和清算关系凭证的步骤包括：

[0027] 第三方机构根据所述经过联合签名的交易凭证向所述支付结算请求涉及到的所有的目的机构发送交易凭证确认申请；

[0028] 第三方机构接收所述支付结算请求涉及到的所有的目的机构返回的交易确认消息，以对所述经过联合签名的交易凭证的合法性进行验证，如果所述交易确认消息为确认成功，即指示所述经过联合签名的交易凭证的合法性验证通过，则根据所述经过联合签名的交易凭证生成对应的交易留存凭证和清算关系凭证。

[0029] 优选地，其中所述方法还包括：

[0030] 第三方机构对清算关系凭证进行签名，并发送至所述支付结算请求涉及到的目的机构对清算关系凭证进行联合签名和确认；

[0031] 在指示所述清算关系凭证进行联合签名和确认成功后，所述第三方机构向所述支付结算请求涉及到的所有的机构发送所述交易留存凭证和清算关系凭证。

[0032] 优选地，其中所述方法还包括：

[0033] 在清算关系中涉及到的所有的机构收到第三方机构发送的交易留存凭证和清算关系凭证后，分别生成每个机构对应的清算凭证，并将所述每个机构对应的清算凭证在分布式账本中进行发布以获得全网的认可并存储。

[0034] 优选地，其中所述方法还包括：

[0035] 在清算关系中涉及到的所有的机构在分布式账本中进行清算凭证的查询，确认清算关系是否已经成功执行。

[0036] 优选地，其中所述清算凭证包括：清算凭证标识、清算资产类型、转移资产数量、发起机构标识、目的机构标识、发起机构签名、清算凭证时间戳以及发起机构的资产来源。

[0037] 根据本发明的另一个方面，提供了一种基于区块链进行支付结算的系统，所述系统包括：

[0038] 交易凭证生成模块，用于接收用户发送的支付结算请求，对所述支付结算请求进行审核，并根据所述支付结算请求生成对应的交易凭证，其中所述交易凭证为区块链中的交易记录；

[0039] 交易反馈结果获取模块，用于当所述支付结算请求审核通过时，发送交易确认申请至目的机构以获取交易反馈结果；

[0040] 交易留存凭证和清算关系凭证确定模块，用于当所述交易反馈结果为确认成功时，接收经过联合签名的交易凭证，并将所述经过联合签名的交易凭证的留存请求发送至第三方机构，以申请所述第三方机构能够根据所述经过联合签名的交易凭证生成对应的交易留存凭证和清算关系凭证，以使得所述第三方机构能够留存区块链中的交易记录；

[0041] 合法性验证模块，用于接收第三方机构获取的交易留存凭证和清算关系凭证，验证所述交易留存凭证和清算关系凭证的合法性；

[0042] 清算模块，用于在确定所述交易留存凭证和清算关系凭证的合法性后，处理用户的支付结算请求，基于分布式账本进行清算。

[0043] 优选地，其中所述交易凭证包括：用户编号、交易凭证标识、资产地址、用户所属机构的标识、交易涉及的其他机构的标识、交易类型、资产类型、交易额度、交易涉及的机构的联合签名和交易时间戳。

[0044] 优选地，其中通过哈希算法获取所述交易凭证标识。

[0045] 优选地，其中所述交易凭证生成模块，对所述支付结算请求进行审核，包括：

[0046] 判断提交所述支付结算请求的用户是否为发起机构的用户，包括：

[0047] 如果所述支付结算请求的用户是发起机构的用户，则判断所述支付结算请求的用户是否有资格享受支付结算服务，如果是，则进行交易确认申请，反之，结束支付结算服务；

[0048] 如果所述支付结算请求的用户不是发起机构的用户，则基于分布式账本查询所述支付结算请求涉及的所有机构的账户信息，并判断所述账户信息是否满足所述支付结算请求，如果满足，则进行交易确认申请，反之，结束支付结算服务。

[0049] 优选地，其中所述系统还包括：

[0050] 交易凭证签名模块，用于在发送交易确认申请前，对所述交易凭证进行单独签名，并将经过单独签名的交易凭证发送至目的机构。

[0051] 优选地，其中所述交易反馈结果获取模块，确定交易反馈结果，包括：

[0052] 交易反馈结果确定单元，用于根据所述经过单独签名的交易凭证，判断用户的支付结算请求的合法性，若合法，则对经过单独签名的交易凭证进行联合签名，并确定交易反馈结果为确认成功；若不合法，则直接确定交易反馈结果为确认失败。

[0053] 优选地，其中所述交易反馈结果获取模块，确定交易反馈结果，包括：

[0054] 交易反馈结果确定单元，用于根据所述经过单独签名的交易凭证和其他辅助机构的交易请求确认结果判断用户的支付结算请求的合法性，若合法，则对经过单独签名的交易凭证进行联合签名，并确定交易反馈结果为确认成功；若不合法，则直接确定交易反馈结果为确认失败。

[0055] 优选地，其中所述系统还包括：

[0056] 请求拒绝模块，用于当所述交易反馈结果为确认失败时，拒绝用户的支付结算请求。

[0057] 优选地，其中所述清算关系凭证，包括：清算关系凭证的标识、借方机构标识、贷方机构标识、资产借贷发生的类型、资产借贷发生的数量、贷方机构和第三方机构的联合签名以及清算关系凭证时间戳。

[0058] 优选地，其中所述交易留存凭证和清算关系凭证确定模块，接收经过联合签名的交易凭证的留存请求，根据所述经过联合签名的交易凭证生成对应的交易留存凭证和清算关系凭证，包括：

[0059] 交易凭证确认申请发送单元，用于第三方机构根据所述经过联合签名的交易凭证向所述支付结算请求涉及到的所有的目的机构发送交易凭证确认申请；

[0060] 凭证生成单元，用于第三方机构接收所述支付结算请求涉及到的所有的目的机构返回的交易确认消息，以对所述经过联合签名的交易凭证的合法性进行验证，如果所述交易确认消息为确认成功，即指示所述经过联合签名的交易凭证的合法性验证通过，则根据所述经过联合签名的交易凭证生成对应的交易留存凭证和清算关系凭证。

[0061] 优选地，其中所述系统还包括：

[0062] 清算关系凭证签名模块，用于对清算关系凭证进行签名，并发送至所述支付结算请求涉及到的目的机构对清算关系凭证进行联合签名和确认；

[0063] 交易留存凭证和清算关系凭证发送模块，用于在指示所述清算关系凭证的联合签名和确认成功后，向所述支付结算请求涉及到的所有的机构发送所述交易留存凭证和清算关系凭证。

[0064] 优选地，其中所述系统还包括：

[0065] 清算凭证发布模块，用于在清算关系中涉及到的所有的机构收到第三方机构发送的交易留存凭证和清算关系凭证后，分别生成每个机构对应的清算凭证，并将所述每个机构对应的清算凭证在分布式账本中进行发布以获得全网的认可并存储。

[0066] 优选地，其中所述系统还包括：

[0067] 清算关系确认模块，用于在清算关系中涉及到的所有的机构在分布式账本中进行清算凭证的查询，确认清算关系是否已经成功执行。

[0068] 优选地，其中所述清算凭证包括：清算凭证标识、清算资产类型、转移资产数量、发起机构标识、目的机构标识、发起机构签名、清算凭证时间戳以及发起机构的资产来源。

[0069] 本发明提供了一种基于区块链进行支付结算的方法及系统，采用基于区块链的分布式的计算节点和账本，解决针对交易凭证所实施的资金支付和结算问题。本发明能够支持复杂数据清算，利用账本中保存的交易凭证可以方便地查询获取账户余额，不必单独进行账户余额计算；在清算过程更加安全，数据清算不再依赖于某个或某些清算中心，避免单点故障或恶意行为引起的清算体系崩溃问题；同时，通过将清算相关的机构以及第三方机

构一并纳入分布式账本中达成共识，能够减少处理时长，提高执行效率，降低清算处理成本，并且通过第三方机构能够处理资金支付和结算过程中可能产生的交易纠纷、恶意交易等问题，保障了清算系统维护运行的健壮性。

附图说明

[0070] 通过参考下面的附图，可以更为完整地理解本发明的示例性实施方式：

[0071] 图1为根据本发明实施方式的基于区块链进行支付结算的方法100的流程图；

[0072] 图2为根据本发明实施方式的发起机构对支付结算请求进行审核的方法200的流程图；

[0073] 图3为根据本发明实施方式的基于分布式总账的数据清算处理流程300的逻辑示意图；以及

[0074] 图4为根据本发明实施方式的基于区块链进行支付结算的系统400的结构示意图。

具体实施方式

[0075] 现在参考附图介绍本发明的示例性实施方式，然而，本发明可以用许多不同的形式来实施，并且不局限于此处描述的实施例，提供这些实施例是为了详尽地且完全地公开本发明，并且向所属技术领域的技术人员充分传达本发明的范围。对于表示在附图中的示例性实施方式中的术语并不是对本发明的限定。在附图中，相同的单元/元件使用相同的附图标记。

[0076] 除非另有说明，此处使用的术语(包括科技术语)对所属技术领域的技术人员具有通常的理解含义。另外，可以理解的是，以通常使用的词典限定的术语，应当被理解为与其相关领域的语境具有一致的含义，而不应该被理解为理想化的或过于正式的意义。

[0077] 图1为根据本发明实施方式的基于区块链进行支付结算的方法100的流程图。如图1所示，本发明的实施方式提供的基于区块链进行支付结算的方法100，采用基于区块链的分布式的计算节点和账本，解决针对交易凭证所实施的资金支付和结算问题。本发明能够支持复杂数据清算，利用账本中保存的交易凭证可以方便地查询获取账户余额，不必单独进行账户余额计算；在清算过程更加安全，数据清算不再依赖于某个或某些清算中心，避免单点故障或恶意行为引起的清算体系崩溃问题；同时，通过将清算相关的机构以及第三方机构一并纳入分布式账本中达成共识，能够减少处理时长，提高执行效率，降低清算处理成本，并且通过第三方机构能够处理资金支付和结算过程中可能产生的交易纠纷、恶意交易等问题，保障了清算系统维护运行的健壮性。本发明的实施方式提供的基于区块链进行支付结算的方法100从步骤101处开始，在步骤101接收用户发送的支付结算请求，对所述支付结算请求进行审核，并根据所述支付结算请求生成对应的交易凭证，其中所述交易凭证为区块链中的交易记录。

[0078] 优选地，其中所述交易凭证包括：用户编号、交易凭证标识、资产地址、用户所属机构的标识、交易涉及的其他机构的标识、交易类型、资产类型、交易额度、交易涉及的机构的联合签名和交易时间戳。

[0079] 优选地，其中通过哈希算法获取所述交易凭证标识。

[0080] 优选地，其中所述对所述支付结算请求进行审核，包括：

[0081] 判断提交所述支付结算请求的用户是否为发起机构的用户，包括：

[0082] 如果所述支付结算请求的用户是发起机构的用户，则判断所述支付结算请求的用户是否有资格享受支付结算服务，如果是，则进行交易确认申请，反之，结束支付结算服务；

[0083] 如果所述支付结算请求的用户不是发起机构的用户，则基于分布式账本查询所述支付结算请求涉及的所有机构的账户信息，并判断所述账户信息是否满足所述支付结算请求，如果满足，则进行交易确认申请，反之，结束支付结算服务。

[0084] 比如：用户A为工商银行(即目的机构)某一用户，但在只支持建设银行(即发起机构)的某商户进行消费。

[0085] 在本发明的实施方式中，用户A提交支付结算请求，发起机构在接收用户发送的支付结算请求后，对所述支付结算请求进行审核，并根据所述支付结算请求生成对应的交易凭证，交易凭证即为区块链中的交易记录。

[0086] 本发明实施方式的发起机构对支付结算请求进行审核的过程如图2所示。

[0087] 在步骤201发起机构接收用户A提交的支付结算请求。

[0088] 在步骤202判断用户A是否为发起机构的用户，如果是，则进入步骤203；反之，进入步骤204。

[0089] 在步骤203判断所述支付结算请求的用户是否有资格享受支付结算服务，如果是，则进入步骤206进行交易确认申请；反之，进入步骤207结束支付结算服务。

[0090] 在步骤204基于分布式账本查询所述支付结算请求涉及的所有机构的账户信息。

[0091] 在步骤205判断所述账户信息是否满足所述支付结算请求，如果满足，则进入步骤206进行交易确认申请，反之，进入步骤207结束支付结算服务。

[0092] 交易凭证的结构如表1所示。其中，用户A的交易凭证标识，即用户交易凭证的标识，采用成熟HASH算法生成，保证其全网唯一性。例如SHA256算法。用户A的资产地址，即交易发起的用户标识，可以指定为该用户所具有的唯一的钱包地址。用户所属机构标识，即用户所属机构的全网唯一标识，可以通过其ID或者独有签名来标识。交易涉及的其他机构标识，即用户此次交易涉及到的其他机构，可以通过其ID或者独有签名来标识。交易类型，可以为ATM取款、存款、证券转移或消费等。资产类型，即交易的资产类型。交易额度，即可进行交易的限额，单笔或者每日。交易涉及机构联合签名，即交易所属机构、涉及其他机构的联合签名，通过该签名，标识其有效性。时间戳，即生成该凭证时间。

[0093] 表1交易凭证结构表

[0094]

用户A的交易凭证标识
用户A的资产地址
用户所属机构标识
交易涉及其他机构标识
交易类型
资产类型
交易额度
交易涉及机构联合签名
时间戳

[0095] 优选地，在步骤102当所述支付结算请求审核通过时，发送交易确认申请至目的机构以获取交易反馈结果。

[0096] 优选地，其中所述方法还包括：

[0097] 在发送交易确认申请前，对所述交易凭证进行单独签名，并将经过单独签名的交易凭证发送至目的机构。

[0098] 优选地，其中所述目的机构确定交易反馈结果，包括：

[0099] 目的机构根据所述经过单独签名的交易凭证，判断用户的支付结算请求的合法性，若合法，则对经过单独签名的交易凭证进行联合签名，并确定交易反馈结果为确认成功；若不合法，则直接确定交易反馈结果为确认失败。

[0100] 优选地，其中所述目的机构确定交易反馈结果，包括：

[0101] 目的机构根据所述经过单独签名的交易凭证和其他辅助机构的交易请求确认结果判断用户的支付结算请求的合法性，若合法，则对经过单独签名的交易凭证进行联合签名，并确定交易反馈结果为确认成功；若不合法，则直接确定交易反馈结果为确认失败。

[0102] 在本发明的实施方式中，发起机构对所述交易凭证进行单独签名，并将经过单独签名的交易凭证发送至目的机构进行交易申请确认。目的机构收到交易申请后，根据用户ID、交易资产类型、资产额度等信息判断用户的交易申请是否合法，其中在对交易合法性进行判断时，可能会需要其他机构的协助共同确定反馈结果。反馈结果确定后，目的机构将所述反馈结果发送至发起机构，如果确认成功，目的机构还会对交易凭证进行联合签名并返回至发起机构。

[0103] 优选地，在步骤103当所述交易反馈结果为确认成功时，接收经过联合签名的交易凭证，并将所述经过联合签名的交易凭证的留存请求发送至第三方机构，以申请所述第三方机构能够根据所述经过联合签名的交易凭证生成对应的交易留存凭证和清算关系凭证，以使得所述第三方机构能够留存区块链中的交易记录。

[0104] 优选地，其中所述清算关系凭证包括：清算关系凭证的标识、借方机构标识、贷方机构标识、资产借贷发生的类型、资产借贷发生的数量、贷方机构和第三方机构的联合签名以及清算关系凭证时间戳。

[0105] 优选地，其中所述第三方机构处理所述经过联合签名的交易凭证的留存请求，并获取交易留存凭证和清算关系凭证的步骤包括：

[0106] 第三方机构根据所述经过联合签名的交易凭证向所述支付结算请求涉及到的所有的目的机构发送交易凭证确认申请；

[0107] 第三方机构接收所述支付结算请求涉及到的所有的目的机构返回的交易确认消息，以对所述经过联合签名的交易凭证的合法性进行验证，如果所述交易确认消息为确认成功，即指示所述经过联合签名的交易凭证的合法性验证通过，则根据所述经过联合签名的交易凭证生成对应的交易留存凭证和清算关系凭证。

[0108] 优选地，其中所述方法还包括：

[0109] 当所述交易反馈结果为确认失败时，拒绝用户的支付结算请求。

[0110] 优选地，在步骤104接收第三方机构获取的交易留存凭证和清算关系凭证，验证所述交易留存凭证和清算关系凭证的合法性。

[0111] 优选地，其中所述方法还包括：

[0112] 第三方机构对清算关系凭证进行签名，并发送至所述支付结算请求涉及到的目的机构对清算关系凭证进行联合签名和确认；

[0113] 在指示所述清算关系凭证进行联合签名和确认成功后，所述第三方机构向所述支付结算请求涉及到的所有的机构发送所述交易留存凭证和清算关系凭证。

[0114] 在本发明的实时方式中，第三方机构根据交易凭证，向交易涉及到的所有机构发送交易凭证确认申请；涉及到的机构向第三方机构返回交易确认结果；第三方机构收到确认结果后，如果确认成功，保留交易凭证，同时根据交易内容生产一条相应地清算关系凭证；第三方机构对清算关系记录进行签名，并发送给所有贷方机构进行联合签名和确认；联合签名成功后，第三方结构向所有相关机构发送留存的交易凭证和清算关系凭证，将来可以起到监管、公证和纠纷处理的作用。发起机构收到第三方机构的交易留存凭证和清算关系凭证后，判定合法性，并处理用户的交易处理请求。

[0115] 清算关系凭证的结构如表2所示。其中，清算关系记录标识，采用成熟HASH算法生成，保证其全网唯一性。借方机构标识，即资产出借机构的全网唯一标识，采用成熟HASH算法生成，保证其全网唯一性。贷方机构标识，即资产借贷机构的全网唯一标识，采用成熟HASH算法生成，保证其全网唯一性。贷方机构、第三方机构联合签名，用于标识此交易记录的有效性。时间戳，即生成该清算关系凭证的时间。需要说明的是，清算关系中包含了交易过程中产生的手续费债务关系。比如，发起机构向用户提供服务，用户可能需要向发起机构支付一定的手续费，该手续费有由目的机构代为支付，体现在清算关系中，就是一条目的机构对发起机构的欠债。

[0116] 表2清算关系凭证结构表

[0117]

清算关系凭证标识
借方机构标识 {机构1，机构2… 机构N}
贷方机构标识 {机构1，机构2… 机构N}
资产借贷发生类型 {资产1，资产2… 资产N}
资产借贷发生数量 {数量1，数量2… 数量N}
贷方机构、第三方机构联合签名
时间戳
其他

[0118] 优选地，在步骤105在确定所述交易留存凭证和清算关系凭证的合法性后，处理用户的支付结算请求，基于分布式账本进行清算。

[0119] 优选地，其中所述方法还包括：

[0120] 在清算关系中涉及到的所有的机构收到第三方机构发送的交易留存凭证和清算关系凭证后，分别生成每个机构对应的清算凭证，并将所述每个机构对应的清算凭证在分布式账本中进行发布以获得全网的认可并存储。

[0121] 优选地，其中所述清算凭证包括：清算凭证标识、清算资产类型、转移资产数量、发起机构标识、目的机构标识、发起机构签名、清算凭证时间戳以及发起机构的资产来源。

[0122] 优选地，其中所述方法还包括：

[0123] 在清算关系中涉及到的所有的机构在分布式账本中进行清算凭证的查询，确认清算关系是否已经成功执行。

[0124] 在本发明的实施方式中，在所有清算关系中涉及的贷方机构(即目的机构)在收到第三方机构的交易留存凭证和清算关系凭证后，处理用户的支付结算请求，进行分布式账本的清算，包括：所有清算关系中涉及的贷方机构收到第三方机构的交易留存记录和清算关系凭证后，作为发起机构生成如表3所示的清算凭证。

[0125] 表3清算凭证结构表

[0126]

清算凭证标识
清算资产类型 {资产1，资产2… 资产N}
转移资产数量 {数量1，数量2… 数量N}
发起机构标识
目的机构标识 {机构1，机构2… 机构N}
发起机构签名
时间戳
发起机构资产来源 {资产转移记录1,...资产转移记录n}
其他

[0127] 所述清算凭证包括：清算记录标识，即清算记录的全网唯一标识；发起机构标识，即发起机构的全网唯一标识；目的机构标识，即目的机构的全网唯一标识；发起机构签名，即发起机构对记录进行签名，用于标识此记录的有效性；发起机构的资产来源，在分布式账户中记录了发起机构的资产来源，作为发起机构进行债务清算的资产基础。清算记录标识、发起机构标识和目的机构标识均通过HASH算法生成。发起机构将清算凭证在清算分布式账本进行发布，在取得全网共识后，清算凭证就得到了全网认可和存储，且不可更改。同时，第三方机构、各清算相关机构均可以在清算分布式账本进行清算凭证查询，根据查询结果，可以确认清算关系是否已经成功执行，同时也可用于第三方机构处理交易纠纷。

[0128] 图3为根据本发明实施方式的基于分布式总账的数据清算处理流程300的逻辑示意图。如图3所示，基于分布式总账的数据清算处理流程300包括：在步骤301，目的机构的用

户提交跨机构支付结算请求至发起机构;在步骤302,发起机构通过分布式账本查询目的机构的相关交易凭证;在步骤303,发起机构提交支付结算请求至目的机构以获取交易反馈结果;在步骤304,目的机构和其他机构协助对支付结算请求进行确认并返回结果至目的机构;在步骤305,目的机构将交易反馈结果发送至发起机构1;在步骤306,交易反馈结果指示确认成功,发起机构向第三方机构申请留存交易凭证;在步骤307,第三方机构向目的机构确认交易凭证;在步骤308,第三方机构保存交易凭证,并记录一条发起机构和目的机构的清算关系凭证;在步骤309第三方机构将交易留存凭证和清算关系凭证发送至涉及的所有机构(包括:发起机构、目的机构以及其他机构)以验证交易留存凭证和清算关系凭证的合法性;在步骤310,在确定所述交易留存凭证和清算关系凭证的合法性后,发起机构对处理用户的支付结算请求;在步骤311,发起机构和目的机构分别生成每个机构对应的清算凭证,并将所述每个机构对应的清算凭证在分布式账本中进行发布以获得全网的认可并存储;在步骤312,在清算关系中涉及到的所有的机构在分布式账本中进行清算凭证的查询,确认清算关系是否已经成功执行,同时也可用于第三方机构处理交易纠纷。

[0129] 图4为根据本发明实施方式的基于区块链进行支付结算的系统400的结构示意图。如图4所示,本发明的实施方式提供的基于区块链进行支付结算的系统400包括:交易凭证生成模块401、交易反馈结果获取模块402、交易留存凭证和清算关系凭证确定模块403、合法性验证模块404和清算模块405。优选地,在所述交易凭证生成模块401,接收用户发送的支付结算请求,对所述支付结算请求进行审核,并根据所述支付结算请求生成对应的交易凭证,其中所述交易凭证为区块链中的交易记录。

[0130] 优选地,其中所述交易凭证包括:用户编号、交易凭证标识、资产地址、用户所属机构的标识、交易涉及的其他机构的标识、交易类型、资产类型、交易额度、交易涉及的机构的联合签名和交易时间戳。优选地,其中通过哈希算法获取所述交易凭证标识。

[0131] 优选地,其中所述交易凭证生成模块,对所述支付结算请求进行审核,包括:判断提交所述支付结算请求的用户是否为发起机构的用户,包括:如果所述支付结算请求的用户是发起机构的用户,则判断所述支付结算请求的用户是否有资格享受支付结算服务,如果是,则进行交易确认申请,反之,结束支付结算服务;如果所述支付结算请求的用户不是发起机构的用户,则基于分布式账本查询所述支付结算请求涉及的所有机构的账户信息,并判断所述账户信息是否满足所述支付结算请求,如果满足,则进行交易确认申请,反之,结束支付结算服务。

[0132] 优选地,在所述交易反馈结果获取模块402,当所述支付结算请求审核通过时,发送交易确认申请至目的机构以获取交易反馈结果。

[0133] 优选地,其中所述系统还包括:交易凭证签名模块,用于在发送交易确认申请前,对所述交易凭证进行单独签名,并将经过单独签名的交易凭证发送至目的机构。

[0134] 优选地,其中所述交易反馈结果获取模块,确定交易反馈结果,包括:交易反馈结果确定单元,用于根据所述经过单独签名的交易凭证,判断用户的支付结算请求的合法性,若合法,则对经过单独签名的交易凭证进行联合签名,并确定交易反馈结果为确认成功;若不合法,则直接确定交易反馈结果为确认失败。

[0135] 优选地,其中所述交易反馈结果获取模块,确定交易反馈结果,包括:交易反馈结果确定单元,用于根据所述经过单独签名的交易凭证和其他辅助机构的交易请求确认结果

判断用户的支付结算请求的合法性，若合法，则对经过单独签名的交易凭证进行联合签名，并确定交易反馈结果为确认成功；若不合法，则直接确定交易反馈结果为确认失败。

[0136] 优选地，在所述交易留存凭证和清算关系凭证确定模块403，当所述交易反馈结果为确认成功时，接收经过联合签名的交易凭证，并将所述经过联合签名的交易凭证的留存请求发送至第三方机构，以申请所述第三方机构能够根据所述经过联合签名的交易凭证生成对应的交易留存凭证和清算关系凭证，以使得所述第三方机构能够留存区块链中的交易记录。

[0137] 优选地，其中所述清算关系凭证，包括：清算关系凭证的标识、借方机构标识、贷方机构标识、资产借贷发生的类型、资产借贷发生的数量、贷方机构和第三方机构的联合签名以及清算关系凭证时间戳。

[0138] 优选地，其中所述交易留存凭证和清算关系凭证确定模块，接收经过联合签名的交易凭证的留存请求，根据所述经过联合签名的交易凭证生成对应的交易留存凭证和清算关系凭证，包括：交易凭证确认申请发送单元和凭证生成单元。在所述交易凭证确认申请发送单元，第三方机构根据所述经过联合签名的交易凭证向所述支付结算请求涉及到的所有的目的机构发送交易凭证确认申请。在所述凭证生成单元，第三方机构接收所述支付结算请求涉及到的所有的目的机构返回的交易确认消息，以对所述经过联合签名的交易凭证的合法性进行验证，如果所述交易确认消息为确认成功，即指示所述经过联合签名的交易凭证的合法性验证通过，则根据所述经过联合签名的交易凭证生成对应的交易留存凭证和清算关系凭证。

[0139] 优选地，其中所述系统还包括：请求拒绝模块，用于当所述交易反馈结果为确认失败时，拒绝用户的支付结算请求。

[0140] 优选地，在所述合法性验证模块404，收第三方机构获取的交易留存凭证和清算关系凭证，验证所述交易留存凭证和清算关系凭证的合法性。

[0141] 优选地，其中所述系统还包括：清算关系凭证签名模块和交易留存凭证和清算关系凭证发送模块。在所述清算关系凭证签名模块，对清算关系凭证进行签名，并发送至所述支付结算请求涉及到的目的机构对清算关系凭证进行联合签名和确认。在所述交易留存凭证和清算关系凭证发送模块，在指示所述清算关系凭证的联合签名和确认成功后，向所述支付结算请求涉及到的所有的机构发送所述交易留存凭证和清算关系凭证。

[0142] 优选地，在所述清算模块405，在确定所述交易留存凭证和清算关系凭证的合法性后，处理用户的支付结算请求，基于分布式账本进行清算。

[0143] 优选地，其中所述系统还包括：清算凭证发布模块，用于在清算关系中涉及到的所有的机构收到第三方机构发送的交易留存凭证和清算关系凭证后，分别生成每个机构对应的清算凭证，并将所述每个机构对应的清算凭证在分布式账本中进行发布以获得全网的认可并存储。优选地，其中所述清算凭证包括：清算凭证标识、清算资产类型、转移资产数量、发起机构标识、目的机构标识、发起机构签名、清算凭证时间戳以及发起机构的资产来源。

[0144] 优选地，其中所述系统还包括：清算关系确认模块，用于在清算关系中涉及到的所有的机构在分布式账本中进行清算凭证的查询，确认清算关系是否已经成功执行。

[0145] 本发明的实施例的基于区块链进行支付结算的系统400与本发明的另一个实施例的基于区块链进行支付结算的方法100相对应，在此不再赘述。

[0146] 已经通过参考少量实施方式描述了本发明。然而，本领域技术人员所公知的，正如附带的专利权利要求所限定的，除了本发明以上公开的其他的实施例等同地落在本发明的范围内。

[0147] 通常地，在权利要求中使用的所有术语都根据他们在技术领域的通常含义被解释，除非在其中被另外明确地定义。所有的参考“一个/所述/该[装置、组件等]”都被开放地解释为所述装置、组件等中的至少一个实例，除非另外明确地说明。这里公开的任何方法的步骤都没必要以公开的准确的顺序运行，除非明确地说明。

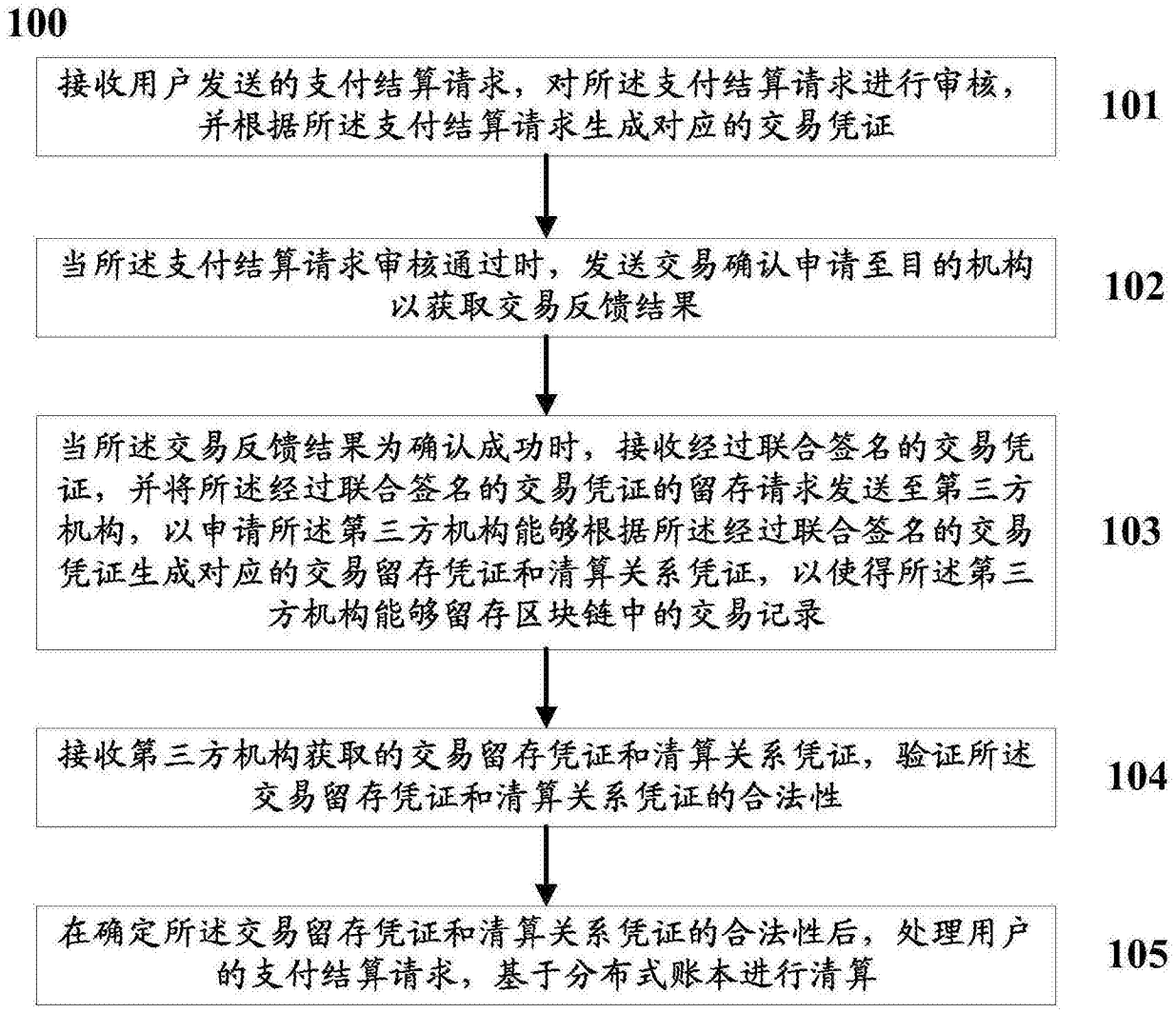

100
接收用户发送的支付结算请求，对所述支付结算请求进行审核，并根据所述支付结算请求生成对应的交易凭证
101
当所述支付结算请求审核通过时，发送交易确认申请至目的机构以获取交易反馈结果
102
当所述交易反馈结果为确认成功时，接收经过联合签名的交易凭证，并将所述经过联合签名的交易凭证的留存请求发送至第三方机构，以申请所述第三方机构能够根据所述经过联合签名的交易凭证生成对应的交易留存凭证和清算关系凭证，以使得所述第三方机构能够留存区块链中的交易记录
103
接收第三方机构获取的交易留存凭证和清算关系凭证，验证所述交易留存凭证和清算关系凭证的合法性
104
在确定所述交易留存凭证和清算关系凭证的合法性后，处理用户的支付结算请求，基于分布式账本进行清算
105

图1

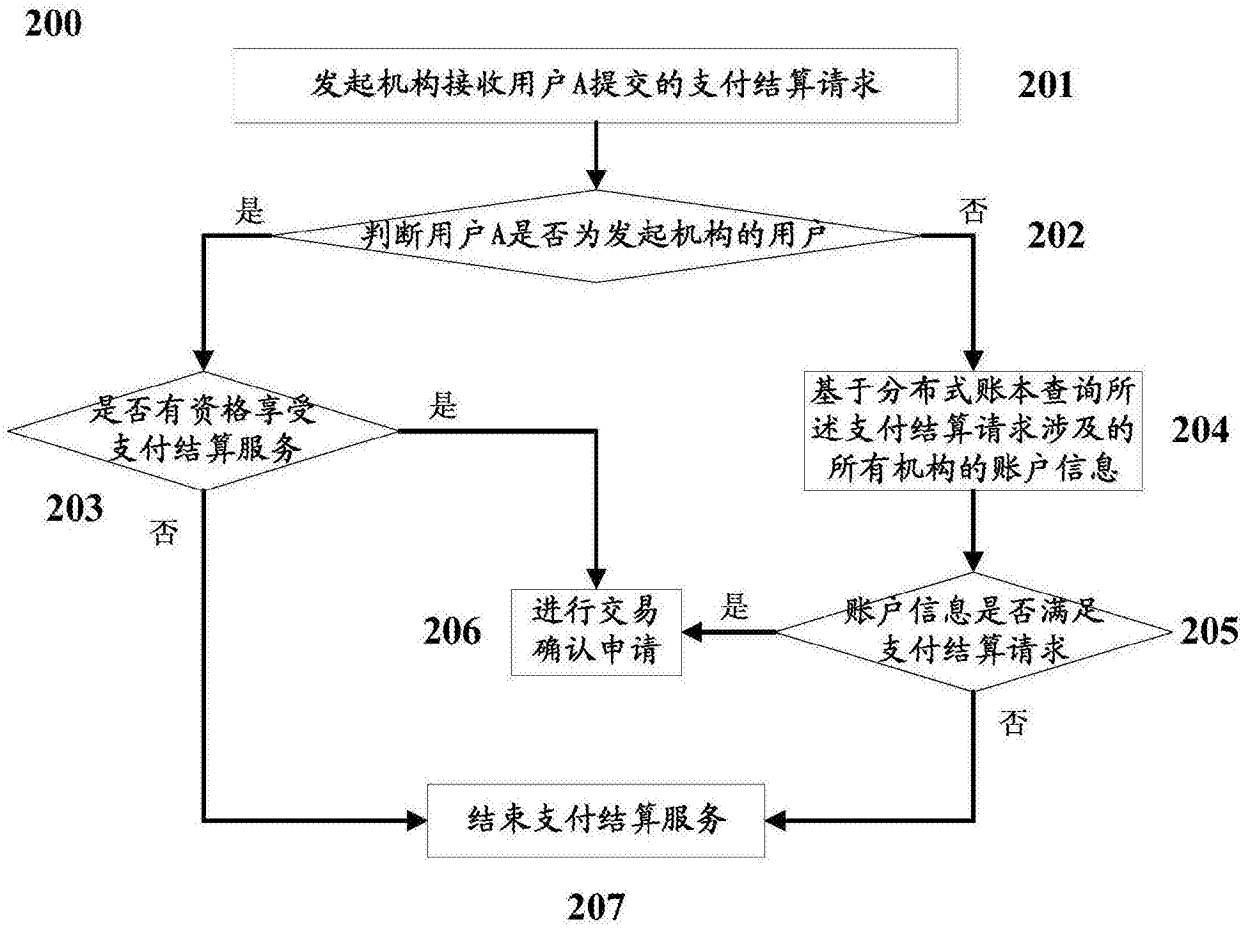

200
发起机构接收用户A提交的支付结算请求
201
判断用户A是否为发起机构的用户
是
否
202
是否有资格享受支付结算服务
是
203
否
基于分布式账本查询所述支付结算请求涉及的所有机构的账户信息
204
进行交易确认申请
206
是
账户信息是否满足支付结算请求
205
否
结束支付结算服务
207

图2

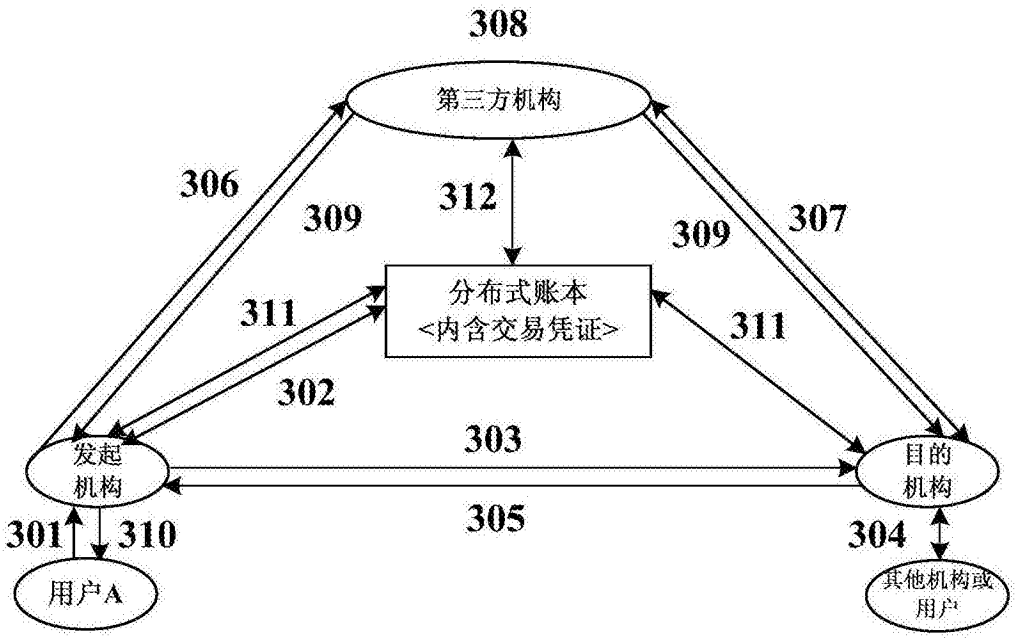

308
第三方机构
306
309
312
309
307
分布式账本
<内含交易凭证>
311
311
302
303
发起机构
目的机构
305
301
310
304
用户A
其他机构或用户

图3


400
交易凭证生成模块401
交易反馈结果获取模块402
交易留存凭证和清算关系凭证确定模块403
合法性验证模块404
清算模块405

图4