(19)中华人民共和国国家知识产权局

(12)发明专利

(10)授权公告号 CN 113781048 B
(45)授权公告日 2022.02.22

(21)申请号 202111347947.6

(22)申请日 2021.11.15

(65)同一申请的已公布的文献号
申请公布号 CN 113781048 A

(43)申请公布日 2021.12.10

(73)专利权人 环球数科集团有限公司
地址 518063 广东省深圳市南山区粤海街道高新南九道10号深圳湾科技生态园10栋B座17层01-03号

(72)发明人 张卫平 丁烨 岑全 李显阔

(74)专利代理机构 北京清控智云知识产权代理事务所(特殊普通合伙) 11919
代理人 马肃

(51)Int.Cl.
G06Q 20/38(2012.01)
G06Q 20/40(2012.01)

(56)对比文件
CN 109767220 A,2019.05.17
WO 2020150741 A1,2020.07.23

审查员 罗丽

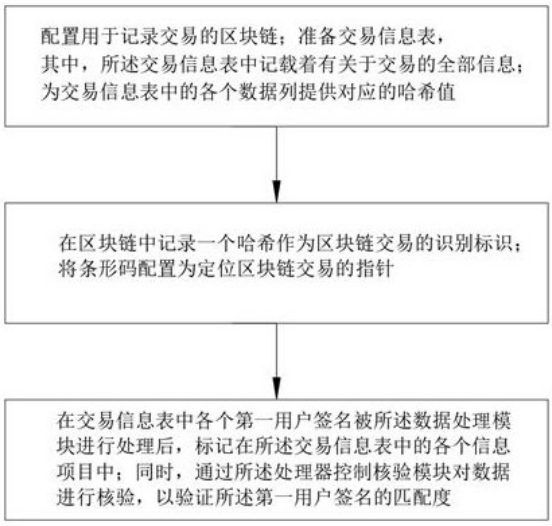
权利要求书3页 说明书10页 附图4页

(54)发明名称

一种基于区块链的交易信息校验及结算方法

(57)摘要

本发明提供了一种基于区块链的交易信息校验及结算方法,包括配置用于记录交易的区块链;准备交易信息表,为交易信息表中的各个数据列提供对应的哈希值;在区块链中记录一个哈希作为区块链交易的识别标识;将条形码配置为定位区块链交易的指针;在交易信息表上插入条形码,并将交易信息表交给数据处理模块;数据处理模块在处理器的控制下对交易信息表中的数据进行处理时。本发明通过采用从交易信息表中提取多个信息段,并将信息段数与数据库中对应的信息进行比较,确定信息段的数量是否与数据库中的相应信息匹配,若存在出入,则该订单不存在或者错误,则不对其进行核验与结算,以实现资源的高效利用。



CN 113781048 B

1.一种基于区块链的交易信息校验及结算方法，其特征在于，所述方法包括配置用于记录交易的区块链；

准备交易信息表，其中，所述交易信息表中记载着有关于交易的全部信息；为交易信息表中的各个数据列提供对应的哈希值；

在区块链中记录一个哈希作为区块链交易的识别标识；将条形码配置为定位区块链交易的指针；在交易信息表上插入条形码，并将交易信息表发送给数据处理模块；

所述数据处理模块在处理器的控制下对所述交易信息表中的数据进行处理时，通过服务器与外部的区块链进行数据传输或者共享；

在交易信息表中各个第一用户签名被所述数据处理模块进行处理后，标记在所述交易信息表中的各个信息项目中；同时，通过所述处理器控制核验模块对数据进行核验，以验证所述第一用户签名的匹配度；

所述核验模块对数据进行核验时，对所述交易信息数据进行筛选的过程中，需要根据下式对所述第一用户签名的数据集Quality进行获取，

$$\text{Quality} = \frac{n+1}{2}\log_2(n+1) - 1$$

对筛选形成的第一签名的数据集Quality进行拆分生成一个交易信息数组ANSER=[a1，a2，…，an-1，an]，n为交易信息数据的项数，an表示第n个项签名值；对所述匹配度Suitability进行一次核验通过下式进行确定；

$$\text{Suitability}_t = \frac{ANSER}{N_i}$$

式中，N_i为区块链网络中的广播的第一用户签名；t为进行匹配核验的次数，在对所述匹配度Suitability进行初次核验后，还需要根据不同交易信息选择最佳的所述交易信息数据，以保证数据的精准性；对于最佳的所述交易信息数据，还需要满足二次核验，二次核验根据下式进行，

$$Suitability'_t = \frac{1}{n}\sum_{t=1}^{n} AS_m$$

其中，t为进行匹配核验的次数，满足t∈n，n为所述交易信息数据的项数；AS_M为所述信息数据与N_i的契合度；

$$AS_m = \frac{T(Suitability_t, T_k)}{n}$$

其中，T(*)用于记录验证时所满足条件的次数；Tk为设定的校准阈值，若$Suitability_t$为不低于Tk，则表示匹配度较好；若$Suitability_t$为低于Tk，表示匹配度不好，则需要重新选择另一组交易信息进行验证；

选择匹配度最佳的第一用户签名所对应的交易数据，并将该数据传输至所述核验模块，并由所述核验模块生成与用户账户相关联的数据结构，其中，所述数据结构包括对先前数据结构的引用，从所述数据结构中提取与用户账户相关联的交易信息，并将所述用户账户相关联的所有交易信息传输到辅助子账户中，以确定用户账户中存在的各个交易数据；所述辅助子账户包括与所述用户账户存在交易的所有账户，以确定源交易信息的初始发行

者；

其中，由所述核验模块使用第一私有加密密钥基于数据结构生成第一用户签名，并使用与用户账户相关联的交易信息建立与服务提供商的验证请求；所述验证请求包括向服务提供商发送与数据结构相关联的签名请求，并由所述核验模块接收一次性密码以响应该签名请求；

由所述核验模块发送包括一次性密码的验证指示，并且向所述服务提供商发送该验证指示；

所述服务提供商接收所述验证指示后，使用第二私有加密密钥基于数据结构生成第二用户签名，以验证交易信息的真伪；

其中，所述服务提供商包括与区块链网络数据连接，并为区块链网络提供数据来源的设备；

若验证通过后，由所述核验模块将包括第一用户签名和第二用户签名的数据结构传输到区块链网络进行验证。

2.根据权利要求1所述的一种基于区块链的交易信息校验及结算方法，其特征在于，响应所述核验模块访问区块链网络提出验证请求，根据区块链网络指令向所述区块链网络提供所请求的信息；通过所述核验模块的请求信息匹配对应的交易信息所对应的请求哈希；同时，响应扫描交易信息表上的条形码，访问区块链交易中的至少一个哈希值；

通过所述核验模块访问区块链交易中的至少一个哈希，将请求哈希与区块链交易中的至少一个哈希进行比较；并验证区块链交易中存在的与至少一个哈希匹配的请求哈希，以确定所述交易信息表是真实的；当验证交易信息表是真实的，将第一消息传送到区块链网络进行广播，其中，第一消息包括验证区块链交易中的交易信息表是真实的反馈消息、以及哈希值的验证消息。

3.根据权利要求2所述的一种基于区块链的交易信息校验及结算方法，其特征在于，所述服务提供商在验证通过后，为辅助子账户启动了解客户程序，以确定辅助子账户是否包含在已知帐户列表中，并通过为数据结构生成第二用户签名来完成签名请求；

其中，若确定辅助子账户的了解客户程序执行不成功，取消与数据结构相关联的签名请求；

若确定辅助子账户的了解客户程序执行成功，通过为数据结构生成第二个用户签名来完成签名请求；

所述了解客户程序用于对所述用户账户的可用性进行检验，以确定该用户账户的可用性，其中，所述了解客户程序执行不成功，则该用户账户不可用；所述了解客户程序执行成功，则该用户账户为可用。

4.根据权利要求3所述的一种基于区块链的交易信息校验及结算方法，其特征在于，所述方法包括若所述请求哈希与所述区块链交易中的至少一个哈希不匹配，则确定所述交易信息表不是真正的交易信息表；根据确定的不真实的交易信息表，向区块链网络发送第二条消息，其中，第二条消息通知所述核验模块检查所请求的信息，并向所述用户进行反馈，同时记录反馈结果和所述核验模块的检查结果。

5.根据权利要求4所述的一种基于区块链的交易信息校验及结算方法，其特征在于，将所述交易信息的至少一部分存储在所述交易信息表中的非区块链位置；所述区块链网络被

配置为向所述核验模块提供验证服务，并根据所述验证服务的验证历史，将验证过的交易信息表上传到区块链网络；

在核验交易信息表的过程中，从交易信息表中提取多个信息段，并将信息段数与数据库中对应的信息进行比较，确定信息段的数量是否与数据库中的相应信息匹配。

6.根据权利要求5所述的一种基于区块链的交易信息校验及结算方法，其特征在于，所述方法还包括由处理装置通过区块链网络接收访问用户账户的特征的请求；同时从与处理装置通信的数据库中获取用户账户的交易信息，自动将用户账户的交易中的至少一个与来自用户的辅助子账户的交易信息中的至少一个进行匹配，

其中，至少一个用户账户的交易信息和从辅助子账户向用户账户发出的至少一个交易对应，以实现交易信息的匹配，若不存在，则抛弃该交易信息的数据；同时，选择用户账户的交易信息中的至少一个匹配的交易信息，生成对用户账户的第一所有权验证来自辅助子账户的一笔或多笔交易信息，以使得用户能够基于第一次所有权验证访问用户账户的特征；其中，所述特征包括交易信息的原始交易方。

7.根据权利要求6所述的一种基于区块链的交易信息校验及结算方法，其特征在于，处理装置根据用户对用户账户的所有权的第一次验证，更新用户的身份保证等级，并允许用户访问与用户账户相关联的特征；

其中，若用户账户的交易信息中的至少一个与来自辅助子账户的交易信息中的至少一个匹配；则通过处理装置将用户账户的交易信息和辅助子账户的交易信息存储在数据库中。

8.根据权利要求7所述的一种基于区块链的交易信息校验及结算方法，其特征在于，所述方法包括从交易信息表中提取多个信息段，将信息段数与数据库中对应的信息进行比较，以确定信息段的数量是否与数据库中的相应信息匹配；

若与数据库中相应的交易信息匹配的信息段数量超过设定阈值，则将第一消息传送到区块链网络；

若与数据库中的相应信息不匹配的信息段数量未超过设定阈值，则向区块链网络发送第二消息；

其中，第一消息包括验证交易信息表是真实的交易信息表；第二消息包括通知请求者检查交易信息表的核验结果。

一种基于区块链的交易信息校验及结算方法

技术领域

[0001] 本发明涉及数据处理技术领域，尤其涉及一种基于区块链的交易信息校验及结算方法。

背景技术

[0002] 随着区块链技术的发展，区块链技术广泛应用到各个场景中，而区块链的某些应用场景中，需要核验各交易节点的账户资源总额。例如：区块链中的核验应用，需要确认某交易节点在某一时间点的交易信息总额(通常为数字货币)。而目前通常采用的资源核验方式是获取每一条交易的交易明细，进行计算与比对，从而实现对核验各交易节点的账户资源总额，因此需要被核验的节点暴露交易明细，才能完成资源核验。因此，目前在对被核验的节点进行资源核验时，获取的数据过于暴露，容易导致被核验的节点的数据泄露，安全性低。

[0003] 如CN108960604B现有技术公开了一种信息处理的方法、系统及装置，企业管理是各企业机构都要面对的问题，企业的类型不同、规模不同，所适用的企业管理方法均不相同。现有技术中的企业管理方法和系统往往需要大量的人工录入数据，而且随着目前对企业整体和对企业中各部门单位的投入产出比的追求，现有技术越来越难以简单、高效且自动化的量化企业中各部门的投入产出比。

[0004] 另一种典型的如CN103247003B的现有技术公开的一种面向事件处理的分布式程序化交易系统，随着中国金融行业的飞速发展，IT系统在金融行业得到了广泛应用，而其中，程序化交易系统正在被更多的投资者接受。而市场上的现有的系统，都在着重开发本领域的单个功能，例如虽然拥有高速运算能力的系统，却缺乏高效的下单性能，导致量化投资的策略无法完美进行。并且，客户在进行量化投资时，往往会想要根据自己的想法和需求打造合适的交易工具，但却又苦于寻找既拥有精准的行情数据、资讯数据，又具备完善的开发能力，并且提供高效的运算和交易能力的系统。

[0005] 为了解决本领域普遍存在安全性差、获取的数据过于暴露、核验过程复杂、人工录入数据强度高、数据交互性差和应用场景小等等问题，作出了本发明。

发明内容

[0006] 本发明的目的在于，针对目前交易信息核验所存在的不足，提出了一种基于区块链的交易信息校验及结算方法。

[0007] 为了克服现有技术的不足，本发明采用如下技术方案：

[0008] 一种基于区块链的交易信息校验及结算方法，所述方法包括配置用于记录交易的区块链；

[0009] 准备交易信息表，其中，所述交易信息表中记载着有关于交易的全部信息；为交易信息表中的各个数据列提供对应的哈希值；

[0010] 在区块链中记录一个哈希作为区块链交易的识别标识；将条形码配置为定位区块

链交易的指针;在交易信息表上插入条形码,并将交易信息表交给数据处理模块;

[0011] 所述数据处理模块在处理器的控制下对所述交易信息表中的数据进行处理时,通过服务器与外部的区块链进行数据传输或者共享;

[0012] 在交易信息表中各个第一用户签名被所述数据处理模块进行处理后,标记在所述交易信息表中的各个信息项目中;同时,通过所述处理器控制核验模块对数据进行核验,以验证所述第一用户签名的匹配度;

[0013] 所述核验模块对数据进行核验时,先对所述交易信息数据进行筛选的过程中,需要根据下式对所述第一用户签名的数据集Quality进行获取,

[0014] $$\text{Quality} = \frac{n+1}{2}\log_2(n+1) - 1$$

[0015] 对筛选形成的第一签名的数据集Quality进行拆分生成一个交易信息数组ANSER=[a1,a2,…,an-1,an]:n为项数,an表示第n个项签名值;根据用于对所述匹配度Suitability进行一次核验的通过下式进行确定;

[0016] $$\text{Suitability}_t = \frac{ANSER}{N_i}$$

[0017] 式中,Ni为区块链网络中的广播的第一用户签名;在对所述匹配度Suitability进行初次核验后,还需要根据不同交易信息选择最佳的所述交易信息数据,以保证数据的精准性;对于最佳的所述交易信息数据,还需要满足二次核验,二次核验根据下式进行,

[0018] $$\text{Suitability} = \frac{1}{n}\sum_{t=1}^{n} AS_{\text{M}}$$

[0019] 其中,t为进行匹配核验的次数,满足t∈n,n为所述信息数据的项数;ASM为所述信息数据与Ni为的契合度;

[0020] $$AS_{\text{M}} = \frac{T\left(\text{Suitability}\,..T_{\text{k}}\right)}{n}$$

[0021] 其中,T(*)为时间函数,用于记录验证时所满足条件的次数;Tk为设定的校准阈值,若Suitability为不低于Tk,则表示匹配度较好;若Suitability为低于Tk,表示匹配度不好,则需要重新选择另一组交易信息进行验证;

[0022] 选择匹配度最佳的第一用户签名所对应的交易数据,并将该数据传输至所述核验模块,并由所述核验模块生成与用户账户相关联的数据结构,其中,所述数据结构包括对先前数据结构的引用,从所述数据结构中提取与用户账户相关联的交易信息,并将所述用户账户相关联的所有交易信息传输到辅助子账户中,以确定用户账户中存在的各个交易数据;所述辅助子账户包括与所述用户账户存在交易的所有账户,以确定源交易信息的初始发行者;

[0023] 其中,由所述核验模块使用第一私有加密密钥基于数据结构生成第一用户签名,并使用与用户账户相关联的交易信息建立与服务提供商的验证请求;所述验证请求包括向服务提供商发送与数据结构相关联的签名请求,并由所述核验模块接收一次性密码以响应该签名请求;

[0024] 并由所述核验模块发送包括一次性密码的验证指示,并且向所述服务提供商发送该验证指示;

[0025] 所述服务提供商接收所述验证指示后，使用第二私有加密密钥基于数据结构生成第二用户签名，以验证交易信息的真伪；

[0026] 其中，所述服务提供商包括与区块链网络数据连接，并为区块链网络提供数据来源的设备；

[0027] 若验证通过后，由所述核验模块将包括第一用户签名和第二用户签名的数据结构传输到区块链网络进行验证。

[0028] 可选的，响应所述核验模块访问区块链网络提出验证请求，根据区块链网络指令向所述区块链网络提供所请求的信息；通过所述核验模块的请求信息匹配对应的交易信息所对应的请求哈希；同时，响应扫描交易信息表上的条形码，访问区块链交易中的至少一个哈希值；

[0029] 通过所述核验模块访问区块链交易中的至少一个哈希，将请求哈希与区块链交易中的至少一个哈希进行比较；并验证区块链交易中存在的与至少一个哈希匹配的请求哈希，以确定所述交易信息表是真实的；当验证交易信息表是真实的，将第一消息传送到区块链网络进行广播，其中，第一消息包括验证区块链交易中的交易信息表是真实的反馈消息、以及哈希值的验证消息。

[0030] 可选的，所述服务提供商在验证通过后，为辅助子账户启动了解客户程序，以确定辅助子账户是否包含在已知帐户列表中，并通过为数据结构生成第二用户签名来完成签名请求；

[0031] 其中，若确定辅助子账户的了解客户程序执行不成功，取消与数据结构相关联的签名请求；

[0032] 若确定辅助子账户的了解客户程序执行成功，通过为数据结构生成第二个用户签名来完成签名请求；

[0033] 所述了解客户程序用于对所述用户账户的可用性进行检验，以确定该用户账户的可用性，其中，所述了解客户程序执行不成功，则该用户账户不可用；所述了解客户程序执行成功，则该用户账户为可用。

[0034] 可选的，所述方法包括若所述请求哈希与所述区块链交易中的至少一个哈希不匹配，则确定所述交易信息表不是真正的交易信息表；根据确定的不真实的交易信息表，向区块链网络发送第二条消息，其中，第二条消息通知所述核验模块检查所请求的信息，并向所述用户进行反馈，同时记录反馈结果和所所述核验模块的检查结果。

[0035] 可选的，将所述交易信息的至少一部分存储在所述交易信息表中的非区块链位置；所述区块链网络被配置为向所述核验模块提供验证服务，并根据所述验证服务的验证历史，将验证过的交易信息表上传到区块链网络；

[0036] 在核验交易信息表的过程中，从交易信息表中提取多个信息段，并将信息段数与数据库中对应的信息进行比较，确定信息段的数量是否与数据库中的相应信息匹配。

[0037] 可选的，所述方法还包括由处理装置通过区块链网络接收访问用户账户的特征的请求；同时从与处理装置通信的数据库中获取用户账户的交易信息，自动将用户账户的交易中的至少一个与来自用户的辅助子账户的交易信息中的至少一个进行匹配，

[0038] 其中，至少一个用户账户的交易信息和从辅助子账户向用户账户发出的至少一个交易对应，以实现交易信息的匹配，若不存在，则抛弃该交易信息的数据；

[0039] 同时，选择用户账户的交易信息中的至少一个匹配的交易信息，生成对用户账户的第一所有权验证来自辅助子账户的一笔或多笔交易信息，以使得用户能够基于第一次所有权验证访问用户账户的特征；其中，所述特征包括交易信息的原始交易方。

[0040] 可选的，处理装置根据用户对用户账户的所有权的第一次验证，更新用户的身份保证等级，并允许用户访问与用户账户相关联的特征；

[0041] 其中，若用户账户的交易信息中的至少一个与来自辅助子账户的交易信息中的至少一个匹配；则通过处理装置将用户账户的交易信息和辅助子账户的交易信息存储在数据库中。

[0042] 可选的，所述方法包括从交易信息表中提取多个信息段，将信息段数与数据库中对应的信息进行比较，以确定信息段的数量是否与数据库中的相应信息匹配；

[0043] 若与数据库中相应的交易信息匹配的信息段数量超过设定阈值，则将第一消息传送到区块链网络；

[0044] 若与数据库中的相应信息不匹配的信息段数量未超过设定阈值，则向区块链网络发送第二消息；

[0045] 其中，第一消息包括验证交易信息表是真实的交易信息表；第二消息包括通知请求者检查交易信息表的核验结果。

[0046] 本发明所取得的有益效果是：

[0047] 1.通过所述服务器用于对外部的数据进行交互或者传输，以实现接收或传输数据，同时结合处理器和服务器搭建起区块链网络，以实现对数据的传输或者共享；

[0048] 2.通过所述处理器控制核验模块对数据进行核验，以验证所述第一用户签名的匹配度；

[0049] 3.通过所述核验模块访问区块链交易中的至少一个哈希，将请求哈希与区块链交易中的至少一个哈希进行比较；验证区块链交易中的至少一个哈希匹配的请求哈希，以提升交易信息表的真实性；

[0050] 4.通过采用了解客户程序用于对所述用户账户的可用性进行检验，以确定该用户账户的可用性，实时掌握账户的可用性，以提供在线核验与结算的服务；

[0051] 5.通过从交易信息表中提取多个信息段，并将信息段数与数据库中对应的信息进行比较，确定信息段的数量是否与数据库中的相应信息匹配，若存在出入，则该订单不存在或者错误，则不对其进行核验与结算，以实现资源的高效利用。

附图说明

[0052] 从以下结合附图的描述可以进一步理解本发明。图中的部件不一定按比例绘制，而是将重点放在示出实施例的原理上。在不同的视图中，相同的附图标记指定对应的部分。

[0053] 图1为本发明对交易信息表进行处理的控制流程示意图。

[0054] 图2为本发明所述处理模块处理交易信息表的控制流程示意图。

[0055] 图3为本发明所述核验模块对交易信息进行核验时的控制流程示意图。

[0056] 图4为本发明所述交易信息表的方框示意图。

[0057] 图5为本发明所述服务提供商的核验流程示意图。

具体实施方式

[0058] 为了使得本发明的目的、技术方案及优点更加清楚明白，以下结合其实施例，对本发明进行进一步详细说明；应当理解，此处所描述的具体实施例仅用于解释本发明，并不用于限定本发明。对于本领域技术人员而言，在查阅以下详细描述之后，本实施例的其它系统、方法和/或特征将变得显而易见。旨在所有此类附加的系统、方法、特征和优点都包括在本说明书内、包括在本发明的范围内，并且受所附权利要求书的保护。在以下详细描述描述了所公开的实施例的另外的特征，并且这些特征根据以下将详细描述将是显而易见的。

[0059] 本发明实施例的附图中相同或相似的标号对应相同或相似的部件；在本发明的描述中，需要理解的是，若有术语“上”、“下”、“左”、“右”等指示的方位或位置关系为基于附图所示的方位或位置关系，仅是为了便于描述本发明和简化描述，而不是指示或暗示所指的装置或组件必须具有特定的方位、以特定的方位构造和操作，因此附图中描述位置关系的用语仅用于示例性说明，不能理解为对本专利的限制，对于本领域的普通技术人员而言，可以根据具体情况理解上述术语的具体含义。

[0060] 实施例一：根据图1-图5，提供一种基于区块链的交易信息校验及结算系统，所述系统包括服务器、处理器、数据处理模块、核验模块和服务提供商，所述处理器分别与所述服务器、所述数据处理模块和所述核验模块控制连接，并基于所述处理器对所述数据处理模块和是所述核验模块进行精准的控制。同时，所述服务器用于对外部的数据进行交互或者传输，以实现接收或传输数据；在本实施例中，通过所述服务器建立起区块链网络，以实现对数据的传输或者共享；其中，所述服务提供商包括对数据提供传输或者能对交易进行监管的设备或传输媒介。

[0061] 所述数据处理模块用于对交易数据进行处理；所述核验模块用于对交易数据或者交易数据的数据结构进行核验；

[0062] 另外，本实施例还提供一种基于区块链的交易信息校验及结算方法，所述方法基于上述的系统进行运行，以实现对交易数据的高效的处理。其中，所述方法包括配置用于记录交易的区块链；准备交易信息表，其中，所述交易信息表中记载着有关于交易的全部信息；为交易信息表中的各个数据列提供对应的哈希值；

[0063] 在区块链中记录一个哈希作为区块链交易的识别标识；将条形码配置为定位区块链交易的指针；在交易信息表上插入条形码，并将交易信息表交给数据处理模块；

[0064] 所述数据处理模块在处理器的控制下对所述交易信息表中的数据进行处理时，通过服务器与外部的区块链进行数据传输或者共享；所述交易信息表中有若干个交易信息，且各个所述交易信息均设置对应的第一用户签名；

[0065] 在交易信息表中各个用户的第一用户签名被所述数据处理模块进行处理后，标记在所述交易信息表中的各个信息项目中；同时，通过所述处理器控制核验模块对数据进行核验，以验证所述第一用户签名的匹配度；

[0066] 所述核验模块对数据进行核验时，先对所述交易信息数据进行筛选的过程中，需要根据下式对所述第一用户签名的数据集Quality进行获取，

[0067] $$\mathrm{Quality} = \frac{n+1}{2}\log_2(n+1) - 1$$

[0068] 其中，n为项数，且当n的项数很多时超过1000项时，上式等价转换为：

[0069] $Quality=\log_2(n+1)-1$

[0070] 对筛选形成的第一签名的数据集Quality进行拆分生成一个交易信息数组ANSER＝[a1,a2,…,an-1,an]:n为项数,an表示第n个项签名值;根据用于对所述匹配度Suitability进行一次核验的通过下式进行确定;

[0071] $$\mathrm{Suitability}_t=\frac{ANSER}{N_i}$$

[0072] 式中,N_i为区块链网络中的广播的第一用户签名;

[0073] 另外,在对所述匹配度Suitability进行初次核验后,还需要根据不同交易信息选择最佳的所述交易信息数据,以保证数据的精准性;对于最佳的所述交易信息数据,还需要满足二次核验,二次核验根据下式进行,

[0074] $$\mathrm{Suitability}=\frac{1}{n}\sum_{t=1}^{n}AS_M$$

[0075] 其中,t为进行匹配核验的次数,满足t∈n,n为所述信息数据的项数;AS_M为所述信息数据与N_i为的契合度;

[0076] $$AS_M=\frac{T\left(\mathrm{Suitability}\,..T_k\right)}{n}$$

[0077] 其中,T(*)为时间函数,用于记录验证时所满足条件的次数;T_k为设定的校准阈值,若Suitability为不低于T_k,则表示匹配度较好;若Suitability为低于T_k,表示匹配度不好,则需要重新选择另一组交易信息进行验证;

[0078] 在确定一组交易信息后,选择匹配度最佳的第一用户签名所对应的数据,并将该数据传输至所述核验模块,并由所述核验模块生成与用户账户相关联的数据结构,其中,所述数据结构包括对先前数据结构的引用,从所述数据结构中提取与用户账户相关联的交易信息,并将所述用户账户相关联的所有交易信息传输到辅助子账户中,以确定用户账户中存在的各个交易数据;

[0079] 所述用户账户包括辅助子账户,其中,所述辅助子账户包括与所述用户账户存在交易的所有账户;

[0080] 由所述核验模块使用第一私有加密密钥基于数据结构生成第一用户签名;并使用与用户账户相关联的交易信息建立与服务提供商的验证请求;其中,所述数据结构包括但是不局限于以下列举的几种:数据的格式、数据的类型、交易的指示类型和交易信息的范围等;

[0081] 所述验证请求包括向服务提供商发送与数据结构相关联的签名请求,并由所述核验模块接收一次性密码以响应该签名请求;

[0082] 由所述核验模块发送包括一次性密码的验证指示,并且向所述服务提供商发送该验证指示;

[0083] 所述服务提供商接收所述验证指示后,使用第二私有加密密钥基于数据结构生成第二用户签名,以验证交易信息的真伪;

[0084] 其中,所述服务提供商包括与区块链网络进行数据连接,并为区块链网络提供交易数据和提供服务的设备或者商家;

[0085] 所述用户账户在进行交易的过程中,所述一次性密码也可由用户账户相关联的基

于密钥散列消息认证码或基于时间的密码生成器来生成。

[0086] 若交易信息的验证通过后，由所述核验模块将包括第一用户签名和第二用户签名的数据结构传输到区块链网络进行验证。

[0087] 经过所述区块链网路进行验证时，把该验证请求的响应反馈至所述服务提供商；

[0088] 若是经过所述区块链网路并未验证通过时，则把该交易信息不是用户账户中的饿交易，可以把其抛弃。

[0089] 响应所述核验模块访问区块链网络提出验证请求，根据区块链网络指令向所述区块链网络提供所请求的信息；通过所述核验模块的请求信息匹配对应的交易信息所对应的请求哈希；同时，响应扫描交易信息表上的条形码，访问区块链交易中的至少一个哈希值；

[0090] 通过所述核验模块访问区块链交易中的至少一个哈希，将请求哈希与区块链交易中的至少一个哈希进行比较；并验证区块链交易中存在的与至少一个哈希匹配的请求哈希，以确定所述交易信息表是真实的；当验证交易信息表是真实的，将第一消息传送到区块链网络进行广播，其中，第一消息包括验证区块链交易的交易信息表是真实的反馈消息、以及哈希值的验证消息。

[0091] 可选的，所述服务提供商在验证通过后，为辅助子账户启动了解客户程序，以确定辅助子账户是否包含在已知帐户列表中，并通过为数据结构生成第二用户签名来完成签名请求；所述辅助子账户被配置为所述用户账户向外传输的识别代表账号，在与外部的区块链网络中进行通信时，用户账户存在交易信息或交易活动，则在所述账户列表中进行显示。

[0092] 其中，若确定辅助子账户的了解客户程序执行不成功，取消与数据结构相关联的签名请求；若确定辅助子账户的了解客户程序执行成功，通过为数据结构生成第二个用户签名来完成签名请求；

[0093] 其中，所述了解客户程序用于对所述用户账户的可用性进行检验，以确定该用户账户的可用性，其中，所述了解客户程序执行不成功，则该用户账户不可用；所述了解客户程序执行成功，则该用户账户为可用。

[0094] 了解客户程序可以收集和分析与辅助子账户相关的身份信息、将辅助子账户与已知方列表进行比较，根据辅助子账户的交易行为计算交易风险或交易行为，并根据预期行为和记录的行为监控辅助子账户的交易，如果了解客户程序不成功，交易可能会被取消。

[0095] 否则，如果另一方是已知的或了解客户程序成功，则服务提供商可以用其私钥签署交易并将交易发送到区块链网络。

[0096] 可选的，所述方法还包括若所述请求哈希与所述区块链交易中的至少一个哈希不匹配，则确定所述交易信息表不是真正的交易信息表；根据确定的不真实的交易信息表，向区块链网络发送第二条消息，其中，第二条消息通知所述核验模块检查所请求的交易信息，并向用户进行反馈，同时，记录向用户反馈的结果和所所述核验模块的检查结果。

[0097] 在实际使用的过程中，所述用户登录用户账户后，通过移动终端进行用户的操作的用户输入，响应于用户输入建立与交易服务的交易订单，并请求要创建的交易的数字签名。根据交易服务的所述交易订单向用户发送具有一次性密码的验证请求。同时，所述用户基于交易订单的触发，在移动终端输入一次性密码以确认其身份。然后，根据用户的输入生成并用其私钥签署交易数据结构。

[0098] 用户用私钥对交易数据结构进行签名，并将交易数据结构传输到区块链网络。

[0099] 可选的，将所述交易信息的至少一部分存储在所述交易信息表中的非区块链位置；其中，所述交易信息包括需要核验或结算的部分数据、不需要核算的数据；对于不需要核算的数据则把其存储在非区块链位置中，其中，在存储单元中开设有两个区域，这两个区域分别对应于区块链位置和非区块链位置。需要核算的交易数据和不需要核算的交易数据均对应存储在区块链位置和非区块链位置中。

[0100] 所述区块链网络被配置为向所述核验模块提供验证服务，并根据所述验证服务的验证历史，将验证过的交易信息表上传到区块链网络；

[0101] 在核验交易信息表的过程中，从交易信息表中提取多个信息段，并将信息段数与数据库中对应的信息进行比较，确定信息段的数量是否与数据库中的相应信息匹配。

[0102] 可选的，所述方法包括由处理装置通过区块链网络接收访问用户账户的特征的请求；同时从与处理装置通信的数据库中获取用户账户的交易信息，自动将用户账户的交易中的至少一个与来自用户的辅助子账户的交易信息中的至少一个进行匹配，

[0103] 其中，至少一个用户账户的交易信息和从辅助子账户向用户账户发出的至少一个交易对应，以实现交易信息的匹配，若不存在，则抛弃该交易信息的数据；

[0104] 同时，选择用户账户的交易信息中的至少一个匹配的交易信息，生成对用户账户的第一所有权验证来自辅助子账户的一笔或多笔交易信息，以使得用户能够基于第一次所有权验证访问用户账户的特征；其中，所述特征包括交易信息的原始交易方。

[0105] 可选的，处理装置根据用户对用户账户的所有权的第一次验证，更新用户的身份保证等级，并允许用户访问与用户账户相关联的特征；

[0106] 其中，若用户账户的交易信息中的至少一个与来自辅助子账户的交易信息中的至少一个匹配；则通过处理装置将用户账户的交易信息和辅助子账户的交易信息存储在数据库中。

[0107] 所述核验模块向辅助子账户发出的一笔或多笔交易，并随着辅助子账户的一项或多项交易的发布而更新辅助子账户的一项或多项交易。

[0108] 其中，使用区块链网络的数据流来聚合辅助子账户的交易信息；同时，利用自动匹配的交易自动生成用户对辅助子账户所有权的二次验证。二次验证的步骤包括：将用户账户的交易信息中的至少一个与辅助子账户的交易信息中的用户账户的一笔或多笔交易信息与辅助子账户的一笔或多笔交易的交易信息的金额进行匹配；使用用户账户的交易信息和辅助子账户的交易信息来验证交易的触发者；其中，用户账户的交易信息由与用户账户相关联的服务发出。

[0109] 若所述用户账户中存在相关联的服务，且该服务被广播在所述区块链网络中，则所述用户账户中的交易信息为真实的。

[0110] 另外，通过所述辅助子账户所有权的二次验证之后，验证所述用户账户中的交易信息所对应的交易金额，使得所述交易金额能够被精准的核对。当对，对某一个交易信息表中订单金额进行确定后，则通过从交易信息表中对交易信息进行比对，以对所述交易信息进行比对，以验证交易信息的准确，防止任何一方对交易信息进行篡改。

[0111] 可选的，所述方法包括从交易信息表中提取多个信息段，将信息段数与数据库中对应的信息进行比较，以确定信息段的数量是否与数据库中的相应信息匹配；其中，所述数据库为所述用户账户中供存储各个交易信息的数据库；

[0112] 若与数据库中相应的交易信息匹配的信息段数量超过设定阈值，则将第一消息传送到区块链网络；

[0113] 若与数据库中的相应信息不匹配的信息段数量未超过设定阈值，则向区块链网络发送第二消息；

[0114] 其中，第一消息包括验证交易信息表是真实的交易信息表；第二消息包括通知请求者检查交易信息表的核验结果。

[0115] 实施例二：本实施例应当理解为至少包含前述任一一个实施例的全部特征，并在其基础上进一步改进，根据图1-图5，所述核验或者结算方法还包括：根据各个用户访问所述区块链网路时，提供对各个用户的注册请求，以获得各个用户对应的用户账户；当完成注册操作后，通过注册后形成的用户账户进行交易订单或者交易活动；

[0116] 同时，对于不同的交易订单，需要对用户账户进行评分，若评分低于设定的购买资格阈值，则不能对特定的交易订单进行下单；

[0117] 通过以下方式注册用户：验证用户的身份；为用户创建唯一的用户标识符和用户记录；创建一个智能合约规则来管理涉及用户的交易信息，以及将唯一的用户标识符、用户记录发布到交易信息表中。

[0118] 其中，注册过程还包括搜索公开可用的数据集以定位用户身份的最可能匹配、制定一系列用户必须回答的基于知识的认证问题、使用评分引擎从收集的关于用户的交易行为的数据计算用户置信度分数。利用所述交易信息表来验证用户的身份和购买资格；验证所述用户的身份和购买资格包括将用户身份与公共和专用观察列表相比较以确认购买资格。

[0119] 其中，所述专用观察列表包括与用户的购买行为相关联的交易订单和交易数据；

[0120] 其中，由处理器执行计算机程序代码使交易和身份验证系统利用私有许可的交易信息表执行智能合约规则来控制和记录所述用户交易订单。

[0121] 其中，所述交易信息表包括金融机构为用户创建的交易记录。

[0122] 通过评分引擎对用户的交易行为进行验证，以实现对所述用户行为的评估或者评分；评估步骤包括：把用户注册时形成的用户账户的交易信息表传输至所述评分引擎中。

[0123] 所述评分引擎接收所述用户的交易信息表后，通过评分引擎操作以聚合交易的属性，以确定与交易相关联的数据的准确性。

[0124] 其中，智能合约规则包括根据监管要求和信任分数控制交易的逻辑。如：对某种特种设备的购买需要进行监管、低于信任分数的控制阈值等。

[0125] 当把所述交易信息表通过所述区块链网络进行传输的过程中，需要通过区块链的特性触发共识机制；其中，所述共识机制由区块链本身的性质决定。

[0126] 在本实施例中，通过与所述区块链网络连接共识引擎，其中，所述共识引擎用于对所述交易信息表中的各个交易信息进行区块链的节点的投票，在很短的时间内完成对交易的验证和确认，以使得对区块链网络中的所有交易信息进行确定。

[0127] 其中，所述共识引擎被配置为：向节点子集提供单个交易的详细信息，每个节点确定交易信息表的状态并预测处理单个交易产生的交易信息表状态；

[0128] 根据指定数量的节点子集预测相同的交易信息表状态，将单个交易与其他交易排序；并将有序交易广播到所有节点，并更新所述交易信息表。

[0129] 在上述实施例中，对各个实施例的描述都各有侧重，某个实施例中没有详述或记载的部分，可以参见其它实施例的相关描述。

[0130] 虽然上面已经参考各种实施例描述了本发明，但是应当理解，在不脱离本发明的范围的情况下，可以进行许多改变和修改。也就是说上面讨论的方法，系统和设备是示例。各种配置可以适当地省略，替换或添加各种过程或组件。例如，在替代配置中，可以以与所描述的顺序不同的顺序执行方法，和/或可以添加，省略和/或组合各种部件。而且，关于某些配置描述的特征可以以各种其他配置组合，如可以以类似的方式组合配置的不同方面和元素。此外，随着技术发展其中的元素可以更新，即许多元素是示例，并不限制本公开或权利要求的范围。

[0131] 在说明书中给出了具体细节以提供对包括实现的示例性配置的透彻理解。然而，可以在没有这些具体细节的情况下实践配置例如，已经示出了众所周知的电路，过程，算法，结构和技术而没有不必要的细节，以避免模糊配置。该描述仅提供示例配置，并且不限制权利要求的范围，适用性或配置。相反，前面对配置的描述将为本领域技术人员提供用于实现所描述的技术的使能描述。在不脱离本公开的精神或范围的情况下，可以对元件的功能和布置进行各种改变。

[0132] 综上，其旨在上述详细描述被认为是例示性的而非限制性的，并且应当理解，以上这些实施例应理解为仅用于说明本发明而不用于限制本发明的保护范围。在阅读了本发明的记载的内容之后，技术人员可以对本发明作各种改动或修改，这些等效变化和修饰同样落入本发明权利要求所限定的范围。

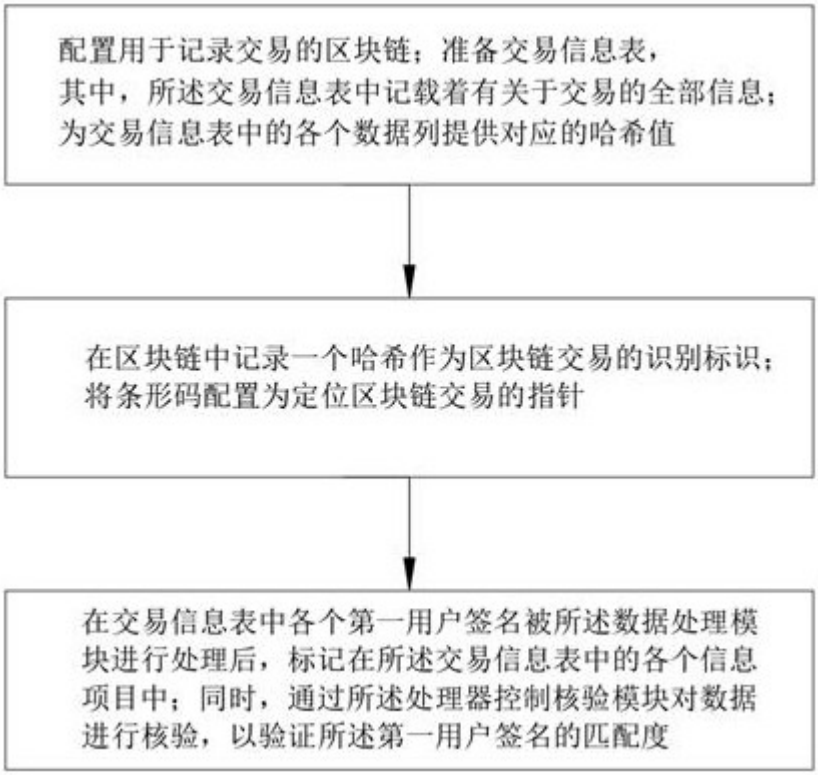

配置用于记录交易的区块链；准备交易信息表，
其中，所述交易信息表中记载着有关于交易的全部信息；
为交易信息表中的各个数据列提供对应的哈希值
在区块链中记录一个哈希作为区块链交易的识别标识；
将条形码配置为定位区块链交易的指针
在交易信息表中各个第一用户签名被所述数据处理模块进行处理后，标记在所述交易信息表中的各个信息项目中；同时，通过所述处理器控制核验模块对数据进行核验，以验证所述第一用户签名的匹配度

图1

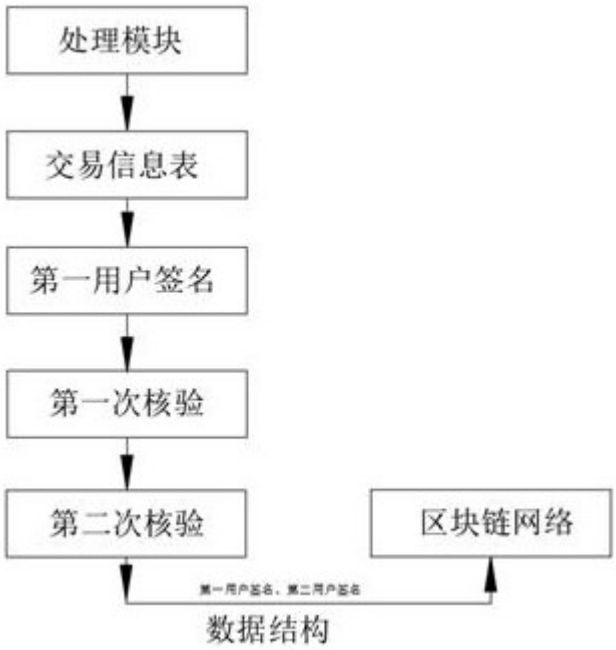

处理模块
交易信息表
第一用户签名
第一次核验
第二次核验
区块链网络
第一用户签名、第二用户签名
数据结构

图2

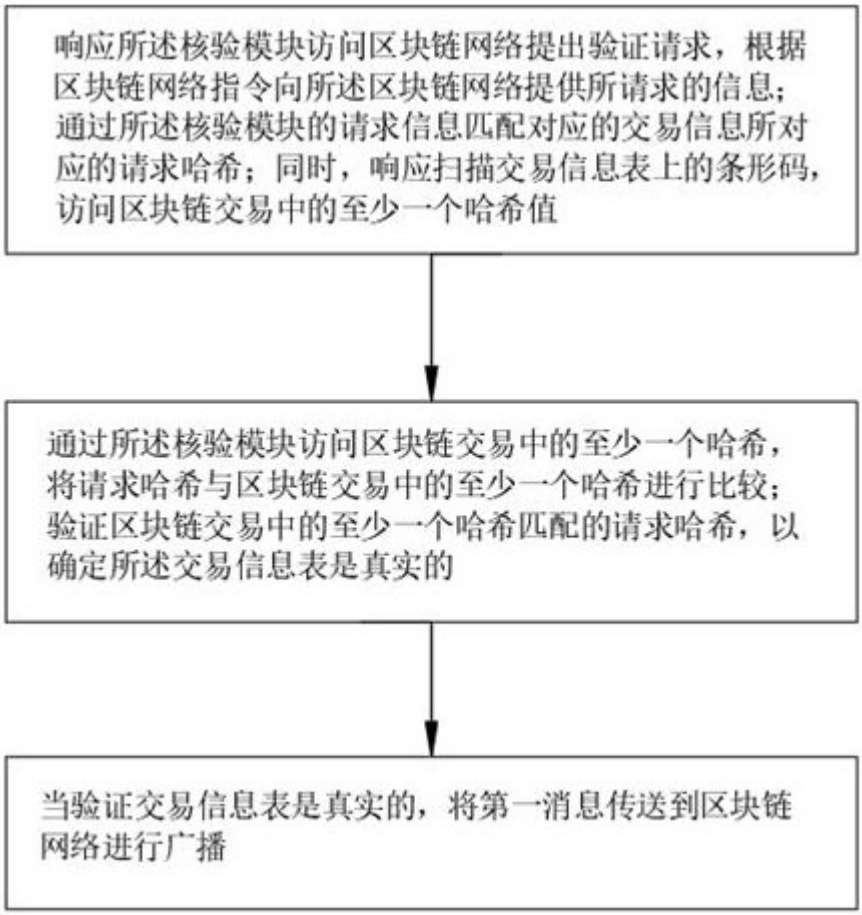

响应所述核验模块访问区块链网络提出验证请求，根据区块链网络指令向所述区块链网络提供所请求的信息；通过所述核验模块的请求信息匹配对应的交易信息所对应的请求哈希；同时，响应扫描交易信息表上的条形码，访问区块链交易中的至少一个哈希值
通过所述核验模块访问区块链交易中的至少一个哈希，将请求哈希与区块链交易中的至少一个哈希进行比较；验证区块链交易中的至少一个哈希匹配的请求哈希，以确定所述交易信息表是真实的
当验证交易信息表是真实的，将第一消息传送到区块链网络进行广播

图3

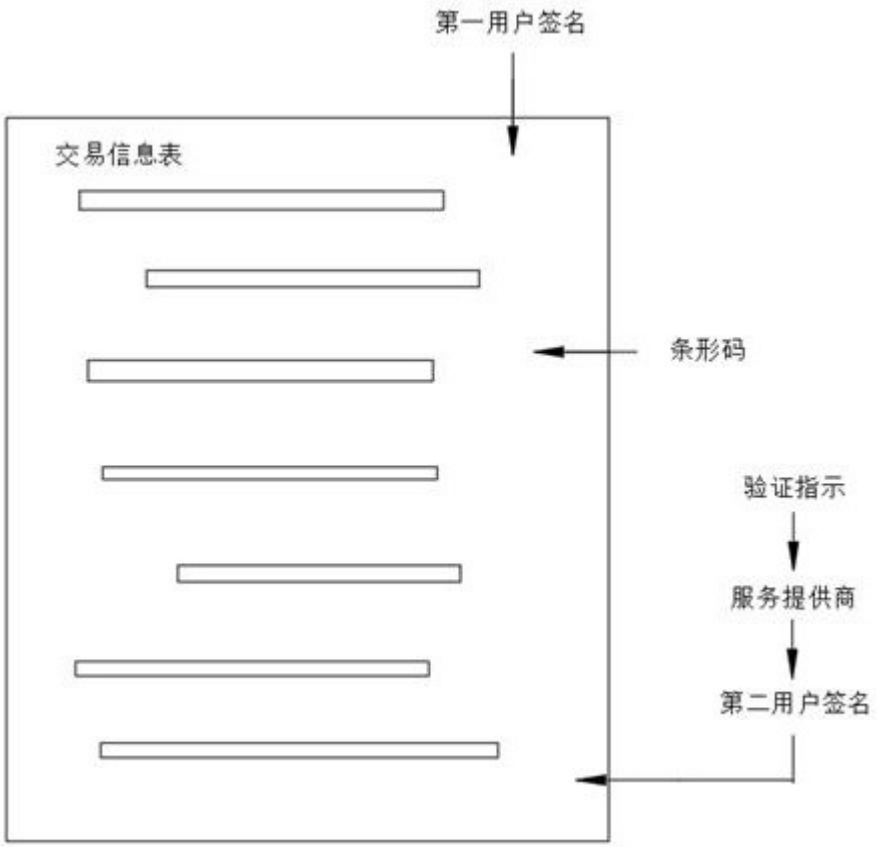


图4

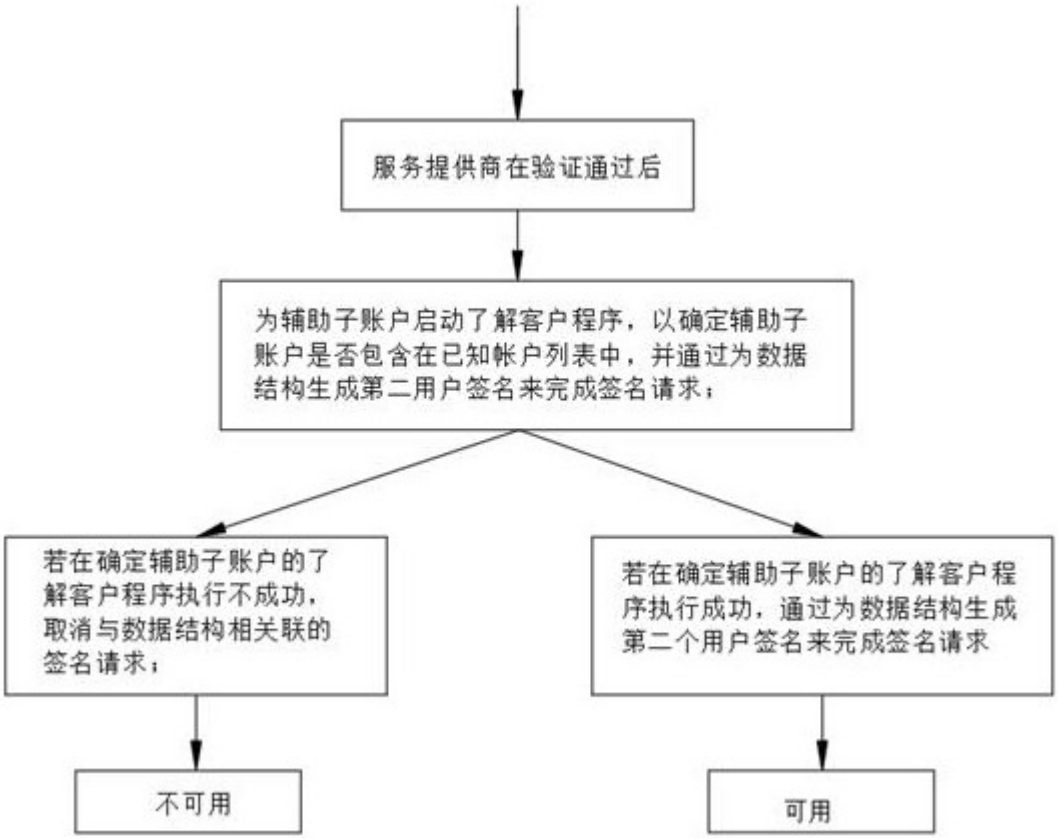

服务提供商在验证通过后
为辅助子账户启动了解客户程序，以确定辅助子账户是否包含在已知帐户列表中，并通过为数据结构生成第二用户签名来完成签名请求；
若在确定辅助子账户的了解客户程序执行不成功，取消与数据结构相关联的签名请求；
若在确定辅助子账户的了解客户程序执行成功，通过为数据结构生成第二个用户签名来完成签名请求
不可用
可用

图5