

基于区块链的支付控制方法、装置、设备及介质

相关申请的交叉引用

本申请要求于 2022 年 8 月 26 日提交的，申请名称为“基于区块链的支付控制方法、装置、设备及介质”的、中国专利申请号为“202211038105.7”的优先权，该中国专利申请的全部内容通过引用结合在本申请中。

技术领域

本申请涉及互联网技术领域，具体而言，涉及一种支付控制方法、装置、电子设备及计算机可读存储介质。

背景技术

证券是多种经济权益凭证的统称，是证明证券持有人有权按其券面所载内容取得应有权益的书面证明。按其性质，不同证券分为证据证券、凭证证券、有价证券等等。有些证券是可以在市场上流通的，证券的存在活跃了金融、经济和投资，证券一般包括股票、债券、基金、权证等等。

目前，用户想要使用证券账户上的资金时，必须先将证券账户上的资金通过银证转账功能转出到银行账户，然后才能将银行账户上的资金用于消费。

因此，相关技术中对证券账户上的资金进行使用的业务流程繁琐，需要较多的身份验证和交易验证，降低了支付系统的业务吞吐量，进而造成证券账户的交易效率和安全性较低的问题。

技术方案

为解决上述技术问题，本申请的实施例提供了一种支付控制方法、装置、电子设备及计算机可读存储介质，能提升支付场景的数据吞吐性能，提升支付的实时性和安全性。

根据本申请实施例的一个方面，提供了一种支付控制方法，包括：对请求方发起的针对证券账户的支付请求进行验证；其中，所述支付请求中包含支付金额以及收款方；若验证通过，则根据所述支付金额对所述证券账户执行资金扣除处理，从所述请求方对应的支付额度中扣除所述支付金额对应的额度，并指示辅助支付平台向所述收款方转入所述支付金额；将所述支付额度对应的资金转移到所述辅助支付平台中，生成交易结果；通过智能合约对所述交易结果进行验证，并在验证通过之后将支付过程中生成的数据上传至区块链中。

根据本申请实施例的一个方面，提供了一种支付控制装置，包括：支付验证模块，配置为对请求方发起的针对证券账户的支付请求进行验证；其中，所述支付请求中包含支付金额以及收款方；支付处理模块，配置为若验证通过，则根据所述支付金额对所述证券账户执行资金扣除处理，从所述请求方对应的支付额度中扣除所述支付金额对应的额度，并指示辅助支付平台向所述收款方转入所述支付金额；交易结果生成模块，配置为将所述支付额度对应的资金转移到所述辅助支付平台中，生成交易结果；

数据上传模块，配置为通过智能合约对所述交易结果进行验证，并在验证通过之后将支付过程中生成的数据上传至区块链中。

根据本申请实施例的一个方面，提供了一种电子设备，包括一个或多个处理器；存储装置，用于存储一个或多个程序，当一个或多个程序被电子设备执行时，使得电子设备实现如上的支付控制方法。

根据本申请实施例的一个方面，提供了一种计算机可读存储介质，其上存储有计算机程序，计算机程序被处理器执行时实现如上的支付控制方法。

根据本申请实施例的一个方面，提供了一种计算机程序产品，该计算机程序产品包括计算机请求，该计算机请求被处理器执行时实现如上的支付控制方法。

在本申请的实施例提供的技术方案中，通过对请求方发起的针对证券账户的支付请求进行验证，若验证通过，则根据支付金额对证券账户执行资金扣除处理，并从请求方对应的支付额度中扣除支付金额对应的额度，并指示辅助支付平台向收款方转入支付金额，将支付额度对应的资金转移到辅助支付平台中，通过智能合约对所述交易结果进行验证，并在验证通过之后将支付过程中生成的数据上传至区块链中。一方面解决了由于证券账户中的资金不能直接使用，而银证转账又存在资金使用效率低下的问题，简化了用户使用证券账户中的资金的步骤，进而提升了支付场景的数据吞吐性能，并提升了支付的实时性和交易效率；另一方面通过区块链中的智能合约技术对支付和交易过程进行验证，并将整个交易过程中生成的数据上链，提高了交易支付的安全性和可靠性。

应当理解的是，以上的一般描述和后文的细节描述仅是示例性和解释性的，并不能限制本申请。

附图说明

此处的附图被并入说明书中并构成本说明书的一部分，示出了符合本申请的实施例，并与说明书一起用于解释本申请的原理。显而易见地，下面描述中的附图仅仅是本申请的一些实施例，对于本领域普通技术者来讲，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他的附图。在附图中：

- 图 1 是可以应用本申请实施例的技术方案的示例性应用环境的示意图；
- 图 2 是本申请的一示例性实施例示出的支付控制方法的流程图；
- 图 3 是本申请的一示例性实施例示出的区块链的结构示意图；
- 图 4 是本申请的一示例性实施例示出的对支付请求进行支付验证的示意图；
- 图 5 是本申请的一示例性实施例示出的对动态验证码的验证过程的示意图；
- 图 6 是本申请的一示例性实施例示出的身份验证界面的示意图；
- 图 7 是本申请的一示例性实施例示出的支付选择界面的示意图；
- 图 8 是本申请的另一示例性实施例示出的支付控制方法的流程图；
- 图 9 是本申请的一示例性实施例示出的绑定选择界面的示意图；
- 图 10 是本申请的一示例性实施例示出的对虚拟证券支付卡与证券账户进行绑定的示意图；
- 图 11 是本申请的一示例性实施例示出的对虚拟证券支付卡的支付数据进行查询的界面示意图；
- 图 12 是本申请的一示例性实施例示出的对虚拟证券支付卡执行冻结处理的示意图；
- 图 13 是本申请的一示例性实施例示出的对虚拟证券支付卡执行支付额度调整处理的示意图；
- 图 14 是本申请的一示例性实施例示出的虚拟证券支付卡管理软件的统一建模语言的示意图；
- 图 15 是本申请的另一示例性实施例示出的支付控制方法的流程图；
- 图 16 是本申请的一示例性实施例示出的支付控制装置的框图；
- 图 17 是适于用来实现本申请实施例的电子设备的计算机系统的结构示意图。

具体实施方式

这里将详细地对示例性实施例执行说明，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描述的实施方式并不代表与本发明相同的所有实施方式。相反，它们仅是与如所附权利要求书中所详述的、本发明的一些方面相同的装置和方法的例子。

附图中所示的方框图仅仅是功能实体，不一定必须与物理上独立的实体相对应。即，可以采用应用程序形式来实现这些功能实体，或在一个或多个硬件模块或集成电路中实现这些功能实体，或在不同网络和/或处理器装置和/或微控制器装置中实现这些功能实体。

附图中所示的流程图仅是示例性说明，不是必须包括所有的内容和操作/步骤，也不是必须按所描述的顺序执行。例如，有的操作/步骤还可以分解，而有的操作/步骤可以合并或部分合并，因此实际执行的顺序有可能根据实际情况改变。

需要说明的是，在本申请中提及的“多个”是指两个或者两个以上。“和/或”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。字符“/”一般表示前后关联对象是一种“或”的关系。

相关技术中，当用户需要使用证券账户中的资金时，需要先将证券账户中的可用资金通过银证转账的方式转出到银行账户上，然后才能将银行账户上的资金用于消费。但是，这导致用户每次有资金使用需求时，都需要去执行一次银证转账，导致资金使用的步骤复杂，且由于银证转账的时效性差，在执行银证转账操作后，资金并不能立即转入银行账户，导致不能及时满足用户的资金使用需求，再者，用户不能很好的把握从证券账户转入银行账户的资金量，导致资金使用效率低下。

基于此，本申请的实施例提出一种支付控制方法、装置、电子设备及计算机可读存储介质，以解决上述技术问题。

下面对本申请实施例所提供的支付控制方法进行说明，其中，图 1 是本申请中支付控制方法涉及的一种实施环境的示意图。如图 1 所示，该实施环境包括终端 110 和服务器 120，终端 110 和服务器 120 可以通过有线或无线通信方式进行直接或间接地连接，本申请在此不做限制。

终端 110 可以是智能手机、平板电脑、笔记本电脑、台式计算机、智能音箱、智能手表、车载终端等，但并不局限于此。终端 110 可以泛指多个终端中的一个，本实施例仅以终端 110 来举例说明。本领域技术人员可以知晓，上述终端的数量可以更多或更少。比如上述终端可以仅为一个，或者上述终端为几十个或几百个，或者更多数量，此时上述图像处理方法的实施环境还包括其他终端。本申请实施例对终端的数量和设备类型不加以限定。

服务器 120 可以是独立的物理服务器，也可以是多个物理服务器构成的服务器集群或者分布式系统，还可以是提供云服务、云数据库、云计算、云函数、云存储、网络服务、云通信、中间件服务、域名服务、安全服务、内容分发网络（Content Delivery Network，CDN）、以及大数据和人工智能平台等基础云计算服务的云服务器。服务器 120 用于为终端 110 运行的应用程序提供后台服务。

在一些实施例中，上述的无线网络或有线网络使用标准通信技术和/或协议。网络通常为因特网，但也可以是任何网络，包括但不限于局域网(Local Area Network, LAN)、城域网(Metropolitan Area Network, MAN)、广域网(Wide Area Network, WAN)、移动、有线或者无线网络、专用网络或者虚拟专用网络的任何组合)。在一些实施例中，使用包括超文本标记语言(Hyper Text Mark-up Language, HTML)、可扩展标记语言(Extensible Markup Language, XML)等的技术和/或格式来代表通过网络交换的数据。此外还可以使用诸如安全套接字层(Secure Socket Layer, SSL)、传输层安全(Transport Layer Security, TLS)、虚拟专用网络(Virtual Private Network, VPN)、网际协议安全(Internet Protocol Security,

IPsec)等常规加密技术来加密所有或者一些链路。在另一些实施例中,还可以使用定制和/或专用数据通信技术取代或者补充上述数据通信技术。

可以理解的是,在本申请的具体实施方式中,涉及到账户信息、用户数据以及交易数据等相关的数据,当本申请实施例运用到具体产品或技术中时,需要获得用户许可、同意或者授权,且相关数据的收集、使用和处理遵守相关国家和地区的相关法律法规和标准。

本申请实施例的基于区块链的支付控制方法可以由服务器120来执行,也可以由终端110来执行,还可以是由服务器120和终端110共同执行。其中,终端110执行本申请实施例的基于区块链的支付控制方法也可以是由安装在其上的客户端来执行。

请参阅图2,图2是本申请的一个实施例示出的基于区块链的支付控制方法的流程图。如图2所示,基于区块链的支付控制方法至少包括步骤S210至步骤S240,详细介绍如下:

步骤S210,对请求方发起的针对证券账户的支付请求进行验证;其中,支付请求中包含支付金额以及收款方。

需要说明的是,证券账户是指证券登记结算机构为投资者设立的,用于准确记载投资者所持的证券种类、名称、数量及相应权益和变动情况的账册,以用于证券产品的交易。

示例性的,服务器可以设置有虚拟证券支付卡,将至少一个证券账户与虚拟证券支付卡绑定,以建立证券账户与虚拟证券支付卡之间的支付链接,即请求方可以通过调用虚拟证券支付卡对证券账户中的资金进行使用。

虚拟证券支付卡为基于卡片数据在终端上进行实体支付卡模拟以实现支付的功能。其中,该虚拟证券支付卡可以存在对应的实体卡片,也可以不存在对应的实体卡片,该虚拟证券支付卡可以在终端进行展示,例如通过卡片形式、二维码形式等进行展示,本申请对此不做限制。

示例性的,终端上可以安装有具备支付功能的支付软件,支付软件绑定有虚拟证券支付卡,通过检测请求方在支付软件上针对虚拟证券支付卡执行的支付操作,生成支付请求。例如,终端上还安装有购物软件,请求方在购物软件中浏览并选中产品后,购物软件向用户显示多个支付方式,请求方可以从多个支付方式中选择一个进行支付,每一种支付方式对应一个支付软件,然后被选中的支付软件发起针对虚拟证券支付卡中绑定的证券账户的支付请求,其中,该支付请求中将被请求方选中的产品对应的产品总价作为支付金额,将被请求方选中的产品的售卖方作为收款方。

本申请实施例中,对请求方发起的支付请求进行验证,如验证该支付请求中携带的支付订单信息是否正确,以及验证发起的支付请求的请求方与证券账户对应的账户信息是否一致等,本申请对此不进行限定。

步骤S220,若验证通过,则根据支付金额对证券账户执行资金扣除处理,并从请求方对应的支付额度中扣除支付金额对应的额度,并指示辅助支付平台向所述收款方转入支付金额。

辅助支付平台为可以直接进行资金转账的平台,该辅助支付平台可以为银行账户、第三方支付平台等,第三方支付平台可以为安装于终端的支付软件,本申请在此不做限定。需要理解的是,本申请实施例中的辅助支付平台中的可用资金额度默认大于支付请求中的支付金额。

可以理解的是,服务器中存储有每个请求方对应的支付额度,支付额度用于约束该请求方在预设时间段内可以使用的金额上限,以及记录请求方在预设时间段内的资金使用情况。例如,请求方A的支付额度为5000元/月,则请求方A一个月内最高可以使用5000元。

示例性的,可以是针对请求方的虚拟证券支付卡设定支付额度,即该虚拟证券支付卡包含的每个证券账户进行的支付均会关联至该虚拟证券支付卡的支付额度中;也可以是针对虚拟证券支付卡包含的每

个证券账户均设定一个支付额度，即每个证券账户进行的支付关联至每个证券账户对应的支付额度中；也可以是针对虚拟证券支付卡设定一个总支付额度，以及针对该虚拟证券支付卡包含的每个证券账户均设定一个子支付额度，即每个证券账户在预设时间段内进行支付的资金数量均不超过子支付额度的前提下，各个证券账户在预设时间段内进行支付的资金数量的总和不超过总支付额度。对于支付额度的设定可以根据实际应用情况进行灵活选择，本申请对此不做限定。

服务器在对支付请求验证通过后，向证券账户中扣除与支付金额对应资金至服务器预设的总资金账户中，然后向辅助支付平台发送支付指令，以使辅助支付平台向收款方转入支付金额，以保证收款方可以及时接收到支付金额，提高支付完成的效率，并从请求方对应的支付额度中扣除支付金额对应的额度，以记录请求方的资金使用情况。

步骤 S230，将支付额度对应的资金转移到辅助支付平台中，生成交易结果。

由于支付额度记录了请求方在预设时间段内的资金使用情况，因此可以通过查询请求方在预设时间段内支付额度的变化，获知辅助支付平台的资金转移量，进而服务器向辅助支付平台转入资金转移量对应的资金。

其中，可以是每间隔预设时间段则根据支付额度的变化向辅助支付平台进行一次资金转移处理，以减少服务器于辅助支付平台之间的交互次数，节约计算资源；也可以是每完成一个支付请求对应的支付任务则向辅助支付平台进行一次资金转移处理，以保证辅助支付平台可以在进行垫付后及时接收到垫付的金额，保证资金流通的实时性，本申请对此不进行限定。

在一些实施方式中，将支付额度对应的资金转移到辅助支付平台中，包括：获取预设时间段内辅助支付平台对应的支付额度的额度变化值；将额度变化值对应的资金转移到辅助支付平台中。

例如，可以是每间隔 24 小时则服务器与辅助支付平台进行一次对账，对账过程可以为：服务器检测在 24 小时内请求方对应的支付额度的额度变化值，然后接收辅助支付平台发送的在 24 小时内针对该请求方向所有收款方转入的支付金额的总额，然后服务器判断支付额度的额度变化值与支付金额的总额是否一致，若一致则向辅助支付平台转移额度变化值对应的资金。

在一些实施方式中，该基于区块链的支付控制方法可以应用于区块链网络的节点，该区块链网络的节点可以为接入区块链网络中的任一节点，该节点可以为任意形式的计算设备，如服务器、终端等。然后，在区块链网络中采用智能合约对服务器以及辅助支付平台之间的资金转移过程进行约束。

需要说明的是，智能合约是一种旨在以信息化方式传播、验证或执行合同的计算机协议，其目的是提供优于传统合约的安全方法，并减少与合约相关的其他交易成本，它允许在没有第三方的情况下进行可信交易，这些交易可追踪且不可逆转。

示例性的，区块链网络的节点可以接收终端提交的针对证券账户的支付请求，然后对证券账户执行资金扣除处理，以将证券账户中的资金转移至区块链网络的节点中的总资金账户中。然后，调用智能合约确定该总资金账户中与支付请求的支付金额对应的资金，将这些资金的状态修改为锁定状态，并指示辅助支付平台向收款方转入对应数量的支付金额，以保证收款方可以及时接收到支付金额，提高支付完成的效率。其中，对总资金账户中与支付金额对应的资金进行锁定是指除执行智能合约的节点可以对该资金进行操作之外，其它节点均不可以对该资金进行操作。

在检测到辅助支付平台完成支付后，接收辅助支付平台反馈的交易结果，并对该交易结果进行验证，若交易结果为支付成功，则调用智能合约将总资金账户中与支付金额对应的资金转移到辅助支付平台中。

步骤 S240，通过智能合约对所述交易结果进行验证，并在验证通过之后将支付过程中生成的数据上传至区块链中。

由于区块链中智能合约具有自动化履约,执行规则及逻辑透明,结果公开且无法篡改的特征,所以,在辅助支付平台实施支付任务后,由智能合约对其交易结果验证,保证了验证结果的准确性和公正性,简化了证券账户中的支付任务执行的复杂度。并在验证通过之后将支付过程中生成的数据上传至区块链中,其中,支付过程中生成的数据包括但不限于:证券账户的支付请求以及对支付请求的验证结果;资金扣除过程生成的交易数据,例如支付金额对应的额度、支付方式等等。

其中,区块链是一种按照时间顺序将数据区块以顺序相连的方式组合成的一种链式数据结构,并以密码学方式保证数据不可篡改和不可伪造的分布式账本。多个独立的分布式节点(即区块链网络的节点)保存相同的记录。区块链技术实现了去中心化,成为了可信的数字资产存储、转移和交易的基石。

以图3所示的区块链的结构示意图为例,每当有新的数据需要写入区块链,这些数据会汇总到一个区块中,添加在已有区块链的末端,通过共识算法保证每个节点新添加的区块是完全相同的。每个区块内记录了若干条交易记录,同时包含了前一个区块的哈希值,所有区块就是通过这种方式保存前一个区块中的值,按顺序相连,组成了区块链。区块链中下一个区块的区块头中会存储前一个区块的哈希值,当前一个区块中的交易数据发生变化时,本区块的哈希值也会随之改变,因此通过上传至区块链网络中的交易数据难以被篡改,在区块链上进行支付交易实现了支付过程的公开透明,提高了支付的可靠性。

在一些实施方式中,支付请求对应的证券账户中可以使用的资金可以是资金余额中的具体数额;也可以是证券账户中的虚拟资源进行资金兑换后的具体数额,如该证券账户中存在购买的基金、股票等,可以将证券账户中当前可以进行交易的虚拟资源对应的资金数额作为可以进行转移的资金。其中,证券账户中当前可以进行交易的虚拟资源是指当前可以进行卖出处理的虚拟资源。通过将虚拟资源也作为可以进行交易的资金,丰富了资金来源,提高了用户使用体验。

本申请可以通过在支付请求验证通过后,对证券账户执行资金扣除处理,并指示辅助支付平台对支付金额进行垫付,以向收款方转入对应的支付金额,进而保证能够及时完成支付业务,然后向辅助支付平台转入该辅助支付平台之前垫付的具体金额,以完成支付流程,解决了由于证券账户中的资金不能直接使用,而银证转账又存在资金使用效率低下的问题,简化了用户使用证券账户中的资金的步骤,进而提升了支付场景的数据吞吐性能,并提升了支付的实时性。

请参阅图4,图4是一实施例提供的对请求方发起的针对证券账户的支付请求进行验证的示意图。

如图4所示,请求方通过终端向服务器发送虚拟证券支付卡的使用请求,服务器根据虚拟证券支付卡的使用请求向终端发送该虚拟证券支付卡的交易密码获取请求,以使终端根据交易密码获取请求向请求方显示交易密码输入框。进而服务器获取终端反馈的请求方向交易密码输入框输入的交易密码,并根据预先与该虚拟证券支付卡关联保存的交易密码校验终端反馈的交易密码是否正确。若交易密码正确则再向终端发送该虚拟证券支付卡的动态验证码获取请求,若动态验证码正确则对支付请求的身份验证为通过,进而调用虚拟证券支付卡。

其中,动态验证码的验证过程可以如图5所示:

步骤 S510,请求方触发动态验证码确认按钮,该动态验证码确认按钮是终端根据动态验证码获取请求向请求方显示的;

步骤 S520,终端向服务器发送动态验证码获取指令,并使该终端显示动态验证码输入框;

步骤 S530,服务器向短信息服务(Short Message Service, SMS)平台转发动态验证码获取指令;

步骤 S540, SMS 平台根据动态验证码获取指令向预设的终端发送动态验证码,其中,预设的终端是指虚拟证券支付卡对应的用户识别卡(Subscriber Identity Module, SIM)所处的终端,该预设的终端与前述提到的发送动态验证码获取指令的终端可以为同一终端,也可以为不同终端;

步骤 S550, 终端将请求方动态验证码输入框输入的动态验证码发送给服务器;

步骤 S560, 服务器将接收到的动态验证码转发给 SMS 平台;

步骤 S570, SMS 平台校验接收到的动态验证码与向预设的终端发送的动态验证码是否一致;

步骤 S580, SMS 平台向服务器反馈校验结果, 若 SMS 平台校验接收到的动态验证码与向预设的终端发送的动态验证码一致, 则向服务器反馈校验通过, 若 SMS 平台校验接收到的动态验证码与向预设的终端发送的动态验证码不一致, 则向服务器反馈校验不通过。

通过结合交易密码和动态验证码对支付请求对应的请求方进行身份验证, 以通过多种验证方式提高身份验证的准确性, 保证支付安全。

在一些实施方式中, 如图 6 所示, 终端在选择使用虚拟证券支付卡进行支付时, 进入虚拟证券支付卡对应的身份验证界面, 该身份验证界面可以设置多个验证方式选择按钮, 如验证方式选择按钮包括“人脸验证”、“指纹验证”、“声音验证”。然后, 根据请求方选择的验证方式获取对应的身份验证信息, 如当请求方选择的验证方式为“人脸验证”时, 则通过终端上的图像获取装置获取请求方的人脸信息; 当请求方选择的验证方式为“指纹验证”时, 则通过终端上的指纹获取装置获取请求方的指纹信息; 当请求方选择的验证方式为“声音验证”时, 则通过终端上的声音获取装置获取请求方的声音信息。通过设置多个验证方式, 并根据请求方选择的验证方式进行身份验证, 以提高请求方进行身份验证的多样性和选择性, 进而提升请求方的使用体验。

然后, 终端根据得到的身份验证信息以及该支付请求关联的订单信息生成支付请求, 并将支付请求发送给服务器。服务器中存储有各个请求方的身份信息, 服务器接收到终端上传的支付请求后, 根据存储的身份信息对支付请求中的身份验证信息进行身份验证, 并对支付请求中的订单信息进行订单验证。其中, 对支付请求中的订单信息进行订单验证可以为检测该订单信息是否正确, 如检测该订单信息的签名信息是否正确, 以有效辨别伪造的订单信息, 保证支付的安全性。

如果身份验证以及订单验证均通过后, 则对支付请求进行支付验证的验证结果为通过; 如果身份验证以及订单验证中的任一者不通过, 则对支付请求进行支付验证的验证结果为不通过。

支付请求对应的证券账户可以是请求方直接指定的证券账户, 也可以是服务器跟支付请求对该请求方对应的多个证券账户进行筛选后得到的。

例如, 若支付验证通过, 则获取虚拟证券支付卡包含的每个证券账户的可用额度。然后, 将可用额度大于或等于支付金额的证券账户作为待支付的证券账户。可以理解的是, 一个虚拟证券支付卡可以绑定有多个证券账户, 将可用额度大于或等于支付金额的证券账户作为待支付的证券账户, 以保证后续可以正确的对待支付的证券账户执行支付操作。

可用额度是指请求方可以使用的资金数量。

在一些实施例中, 证券账户的可用额度可以根据证券账户的资金总额得到。例如, 证券账户的资金总额可以是该证券账户的资金余额中的具体数额, 也可以是资金余额中的具体数额与证券账户中的虚拟资源进行资金兑换后的具体数额进行相加后的和, 本申请对此不做限定。

示例性的, 根据支付额度得到每个证券账户的资金剩余可用额度, 然后将每个证券账户的资金剩余可用额度和每个证券账户的资金总额中的最小值作为每个证券账户对应的可用额度。例如, 证券账户包括证券账户 A 和证券账户 B, 证券账户 A 的资金总额为 100 元, 证券账户 B 的资金总额为 700 元, 针对虚拟证券支付卡设定的支付额度为每天 1000 元, 根据查询该虚拟证券支付卡在当天的历史支付记录得到该虚拟证券支付卡已经支付过 600 元, 则每个证券账户的资金剩余可用额度为 400 元, 进而证券账户 A 的可用额度为 100 元, 证券账户 B 的可用额度为 400 元。

在一些实施例中,当可用额度大于或等于支付金额的证券账户为多个时,可以获取这些证券账户的优先级,将优先级最高的证券账户作为待支付的证券账户。优先级可以是对每个证券账户预先设定的,还可以是根据每个证券账户的使用频率、可信度等信息动态设定的,本申请对此不做限定。

在一些实施例中,如图7所示,当可用额度大于或等于支付金额的证券账户为多个时,可以向终端发送待支付证券账户的支付选择指令,终端根据待支付证券账户的选择指令向请求方显示待支付证券账户的支付选择界面,例如,通过该支付选择界面显示的证券账户包括证券账户A和证券账户B,每个证券账户对应不同的选择按钮。终端接收到请求方在待支付证券账户的支付选择界面上执行的选择操作,并根据该选择操作向服务器反馈待支付的证券账户。

本申请实施例通过对支付请求进行支付验证,保证了支付过程的安全性,且根据虚拟证券支付卡包含的证券账户的可用额度,对证券账户预先进行一次筛选,以保证得到的待支付的证券账户满足支付要求,以避免由于证券账户中的可用额度不足而导致的支付失败,从而避免程序浪费。

在一些实施方式中,当虚拟证券支付卡中包含的证券账户中没有可用额度大于或等于支付金额的证券账户时,可以对虚拟证券支付卡中包含的每个证券账户的多个可用额度进行相加,若相加后的可用额度大于或等于支付金额,则将进行相加的证券账户均作为待支付的证券账户,以提高支付成功率,提高请求方的使用体验。

请参阅图8,图8是根据另一示例性实施例示出的一种基于区块链的支付控制方法的流程图。如图8所示,在一示例性的实施例中,在步骤S210对请求方发起的针对证券账户的支付请求进行验证之前,还可以包括如下步骤:

步骤S810,根据请求方发起的针对证券账户的绑定请求,确定可以用于支付的证券账户。

可以用于支付的证券账户是指该证券账户中存在可以进行支付的资金。

其中,一个虚拟证券支付卡可以和多个证券账户进行绑定,一个证券账户也可以和多个虚拟证券支付卡绑定,本申请对此不做限定。

需要说明的是,虚拟证券支付卡以及证券账户均存在对应的用户信息,虚拟证券支付卡和证券账户之间的用户信息可以相同,也可以不同。如考虑到虚拟证券支付卡和证券账户的安全性以及为了便于后续进行管理,需要虚拟证券支付卡和证券账户之间的用户信息相同;而考虑到虚拟证券支付卡与证券账户之间绑定的灵活性,则虚拟证券支付卡和证券账户之间的用户信息可以不相同;或者可以根据虚拟证券支付卡和证券账户对应的可信度,根据可信度选择对应的绑定策略,以使虚拟证券支付卡和证券账户之间的绑定方法更加贴合实际情况。虚拟证券支付卡和证券账户之间的绑定方法具体可以根据实际情况进行灵活选择,本申请对此不做限定。

在一些实施方式中,根据请求方发起的针对证券账户的绑定请求,确定可以用于支付的证券账户,包括:查询请求方对应的证券账户的证券账户状态;根据证券账户状态为正常状态的证券账户的历史交易信息,计算证券账户状态为正常状态的证券账户的可信度;将可信度满足预设条件的证券账户作为可以用于支付的证券账户。

在一些实施例中,请求方对应的证券账户可以是与请求方存在关联的证券账户。例如,服务器获取请求方所操作的虚拟证券支付卡对应的身份信息,包括:用户名称、身份标识、身份图像等。用户名称是指用户的姓名,身份标识可以是用户的身份证号,也可以是用户的护照编号,还可以是其他唯一标识该用户身份的标识。身份图像是指与身份标识对应的头像信息,比如,如果身份标识为身份证号,那么身份信息为身份证上的头像信息,如果身份标识为护照编号,那么相应的头像信息为护照上的头像信息。该虚拟证券支付卡,可以具有自身的虚拟卡片标识,该虚拟卡片标识可以由持卡用户的身份信息组

成，以便将持卡用户的身份信息与虚拟卡片联系起来，如通过持卡用户的身份信息查询所有证券账户，将与该持卡用户的身份信息匹配的证券账户作为与请求方对应的证券账户。

在一些实施例中，请求方对应的证券账户可以是该请求方对应的终端中所有证券软件中的证券账户。如查询请求方对应的终端中的所有证券软件的证券账户登录记录，将该登录记录中涉及的所有证券账号作为虚拟证券支付卡对应的证券账户。

证券账户的证券账户状态可以包括正常状态、冻结状态等。证券账户状态为正常状态的证券账户是指可以正常使用的账户，如可以正常使用证券账户内的资金余额，正常进行证券交易等；证券账户状态为冻结状态的证券账户是指可以不正常使用的账户，如不可以进行账户登录，不可以正常进行证券交易等。

其中，可信度的计算可以是根据请求方的历史交易信息计算该请求方的可信度，例如，查询历史交易信息中是否存在被标记为违规的交易信息，若被标记为违规的交易信息的数量越多，则该请求方的可信度就越低，若被标记为违规的交易信息的数量越少，则该请求方的可信度就越高。

通过证券账户状态为正常状态的证券账户的历史交易信息计算证券账户状态为正常状态的证券账户的可信度，例如，查询历史交易信息中是否存在被标记为违规的交易信息，若被标记为违规的交易信息的数量越多，则该证券账户的可信度就越低，若被标记为违规的交易信息的数量越少，则该证券账户的可信度就越高。然后，将可信度满足预设条件的证券账户作为可以用于支付的证券账户，进而提高后续的证券账户绑定的效率。

具体的，我们在确定证券账户的可信度时，获取证券账户的历史交易信息，提取其中的违规交易信息，并进行计数得到违规次数Num_vio以及对应的违规订单总额Tra_vio，同时统计历史交易信息中的正常交易次数Num_nor以及对应的正常交易总额Tra_nor，计算交易差额参数Par_var为：

$$\text{Par_var} = \frac{\log_2 \text{Tra_nor} - \log_2 \text{Tra_vio}}{\text{Num_nor} - \text{Num_vio}}$$

之后，基于交易差额参数Par_var、违规次数Num_vio以及证券账户的账户的社交活跃参数Par_act计算可信度为：

$$\text{Par_act} = \alpha \cdot \text{Par_act} \cdot \frac{|\text{Par_var}|}{\text{Num_vio}}$$

其中， α 表示可信因子。上述方式通过根据证券账户中的违规交易信息、等信息计算能得到可信度，以通过可信度来衡量证券账户的安全和信誉问题，进而可以基于证券账户可信度的高低来做出相应的处理，提高了交易的安全性和可靠性。

其中，可信度满足预设条件的证券账户可以是可信度大于或等于可信度阈值的证券账户；也可以是根据证券账户的可信度对这些证券账户进行排序后，序列前预设数量的证券账户。

在计算得到可信度之后，本实施例中可以基于可信度对上述交易数据和支付过程中生成的数据进行标签处理，作为评估上述信息可信程度的参数进行上链，提高了上链数据的可靠性和客观性。

步骤 S820，发送可以用于支付的证券账户至请求方，以接收请求方针对可以用于支付的证券账户反馈的证券账户选择信息，得到待绑定的证券账户。

示例性的，请参阅图 9，图 9 为对可以用于支付的证券账户进行选择的界面示意图，如图 9 所示，服务器向终端发送可以用于支付的证券账户，终端根据接收到的可以用于支付的证券账户向请求方显示证券账户的绑定选择界面，例如，通过该绑定选择界面显示的证券账户包括证券账户 A、证券账户 B 和证券账户 C，每个证券账户对应不同的选择按钮。然后请求方针对该绑定选择界面执行证券账户选择操作，并在终端检测到请求方触发“确定”按钮后，根据请求方当前选择的证券账户 A 和证券账户 B 向

服务器反馈待绑定的证券账户，进而服务器得到待绑定的证券账户为证券账户 A 和证券账户 B，以使请求方可以仅通过一次证券账户绑定操作绑定多个证券账户，简化证券账户绑定的流程，提高用户使用体验。

在一些实施方式中，发送可以用于支付的证券账户至请求方，以接收请求方针对可以用于支付的证券账户反馈的证券账户选择信息，得到待绑定的证券账户，包括：响应于证券账户选择信息，向请求方发送证券账户验证请求；接收请求方根据证券账户验证请求反馈的证券账户验证信息；根据证券账户验证信息对被选中的证券账户进行证券账户验证；若证券账户验证通过，则将被选中的证券账户作为待绑定的证券账户。

可以理解的是，为了保证每个证券账户的安全，针对每个证券账户均设置有证券账户验证步骤，以将证券账户验证通过的被选中的证券账户作为待绑定的证券账户。

示例性的，可以是请求方触发证券账户的选择控件后，显示该证券账户的证券账户验证界面，以对该证券账户执行对应的证券账户验证，只有在该证券账户验证通过后，才表明该证券账户被选择成功，否则表明该证券账户选择失败。

步骤 S830，建立与待绑定的证券账户之间的支付链接。

示例性的，可以是建立虚拟证券支付卡与待绑定的证券账户之间的支付链接，虚拟证券支付卡与待绑定的证券账户之间的支付链接是指可以通过该虚拟证券支付卡来调用被绑定的证券账户。通过将证券账户绑定至虚拟证券支付卡，则可以直接调用虚拟证券支付卡使用证券账户中的资金，提高了证券账户资金的使用效率。

以图 10 为例对证券账户的支付链接建立过程进行说明，如图 10 所示，服务器根据证券账户绑定请求确定是否存在可以用于支付的证券账户。若存在可以用于支付的证券账户，则检测是否存在指定货币的证券账户。若存在指定货币的证券账户，则接收请求方针对可以用于支付且为指定货币的证券账户反馈的证券账户选择信息，得到待绑定的证券账户。然后，向终端发送针对待绑定的证券账户的交易密码校验请求，以对请求方通过终端反馈的交易密码进行校验。若交易密码校验成功则对建立虚拟证券支付卡与待绑定的证券账户之间的支付链接；若交易密码校验不成功，则通过终端提示请求方再次进行校验。然后，建立虚拟证券支付卡与待绑定的证券账户之间的支付链接，完成证券账户绑定步骤。

在一些实施方式中，建立与待绑定的证券账户之间的支付链接，还包括：获取请求方的用户信息；根据用户信息得到的请求方的可信度；根据请求方的可信度生成请求方对应的支付额度；根据请求方对应的支付额度建立与待绑定的证券账户之间的支付链接。

示例性的，可以获取请求方操作的虚拟证券支付卡对应的用户信息，以根据得到的用户信息得到该请求方的可信度，进而根据请求方的可信度生成请求方对应的支付额度，再建立虚拟证券支付卡与待绑定的证券账户之间的支付链接。可以理解的是，请求方的可信度越高，则请求方对应的支付额度越高；请求方的可信度越低，则请求方对应的支付额度越低。

在一些实施例中，还可以根据请求方的可信度确定该请求方在预设时间段内的资金使用次数、支付过程中的身份验证等级等。例如，若请求用户的可信度越高，则预设时间段内的资金使用次数越多、支付过程中的身份验证等级越低；若请求用户的可信度越低，则预设时间段内的资金使用次数越少、支付过程中的身份验证等级越高。其中，支付过程中的身份验证等级是指支付过程中采用的验证方式的等级，如根据请求用户的可信度判断支付过程中的身份验证等级为低级时，则对应的验证方式可以为交易密码验证；根据请求用户的可信度判断支付过程中的身份验证等级为中级时，则对应的验证方式可以为人脸识别验证；根据请求用户的可信度判断支付过程中的身份验证等级为高级时，则对应的验证方式可

以为人脸识别验证以及动态验证码验证。通过请求用户的可信度自动生成支付链接相应的参数,以使建立的与证券账户之间的支付链接更加贴合请求方的实际情况,在提高支付的安全性的前提下,提升用户的使用体验。

在一些实施方式中,对虚拟证券支付卡的开通过程进行说明:响应于请求方发起的虚拟证券支付卡开通请求,获取虚拟证券支付卡开通请求对应的请求用户的用户信息;对用户信息进行用户身份验证,并根据用户信息对应的信用度生成支付配置参数;若用户身份验证通过,则根据用户信息生成虚拟证券支付卡。

其中,可以是终端显示用户信息填写界面,根据用户信息填写界面收集请求用户的用户信息;还可以是请求方通过虚拟证券支付卡管理软件发起虚拟证券支付卡开通请求,请求方的用户信息可以是根据该虚拟证券支付卡管理软件当前登录的账户标识获取的用户信息,本申请对此不做限定。

得到请求方的用户信息后,对用户信息进行用户身份验证,如通过终端获取当前用户的人脸信息、指纹信息、声音信息、验证码信息等中的至少一种,以校验获取的信息与用户信息是否一致,若一致则表明用户身份验证通过。在用户身份验证通过后,则根据用户信息生成虚拟证券支付卡。

在一些实施方式中,方法还包括:接收请求方发起的针对证券账户的支付数据查询请求,支付数据查询请求中携带有待查询支付数据的数据类型;根据数据类型匹配对应的数据显示策略,以及查询数据类型对应的支付数据记录;将数据显示策略以及支付数据记录发送给请求方,以使请求方对应的终端根据数据显示策略对支付数据记录进行显示。

通过为不同数据类型的待查询支付数据设置不同的显示策略,以对待查询支付数据进行区分,使终端侧能够对待查询支付数据更加清晰的进行显示,便于阅读。

其中,支付数据查询请求可以是针对指定的证券账户的请求,也可以是针对虚拟证券支付卡中所有证券账户的请求,本申请对此不进行限定。

以支付数据查询请求为针对虚拟证券支付卡中所有证券账户的请求为例进行说明。

如图 11 所示,待查询支付数据的数据类型包括账单明细、返现明细,当支付数据查询请求中携带的待查询支付数据的数据类型为账单明细时,匹配的数据显示策略为第一数据显示策略;当支付数据查询请求中携带的待查询支付数据的数据类型为返现明细时,匹配的数据显示策略为第二数据显示策略。

其中,账单明细用于显示与该虚拟证券支付卡关联的所有资金支出记录与资金退还记录,返现明细用于显示与该虚拟证券支付卡关联的所有因消费而产生的返现记录。

在一些实施例中,可以根据日期和类型对账单明细或返现明细进行筛选,如账单明细的类型包括消费、退款,返现明细的类型包括已到账、已失效、待到账、已退回。进一步的,当终端检测到明细被点击时,可以跳转至被点击明细对应的明细详情界面,以展示该条明细的详情内容。

因为账单明细的显示界面和返现明细的显示界面之间存在差异,可以对账单明细的显示界面和返现明细的显示界面设置不同的子类来封装界面差异对应的代码。然后,根据账单明细和返现明细的枚举值生成各自的明细列表、明细详情、明细筛选项的请求以及列表的标题、详情的标题等。通过枚举值预定义列出所有值的标识符来定义一个有序集合,进而实现数据一致性。

在一些实施方式中,还可以对虚拟证券支付卡执行冻结或解冻处理和额度调整处理。

请参阅图 12,图 12 为对虚拟证券支付卡执行冻结处理的示意图,如图 12 所示,接收请求方发起的针对虚拟证券支付卡的冻结请求,根据冻结请求检测该虚拟证券支付卡是否处于冻结状态,若不处于冻结状态执行冻结账户;向终端发送交易密码验证请求,以得到请求方向终端输入的交易密码,进而校验该交易密码是否正确,并在校验成功之后检测账户的冻结状态是否成功,校验成功则弹出冻结成功提

示,不成功则返回重新处理。可以理解的是,对虚拟证券支付卡执行解冻处理的过程与上述对虚拟证券支付卡执行冻结处理的过程类似,再次不做赘述。

请参阅图 13,图 13 为对虚拟证券支付卡执行支付额度调整处理的示意图,如图 13 所示,接收请求方发起的针对虚拟证券支付卡的支付额度调整请求,根据支付额度调整请求检测该虚拟证券支付卡是否处于冻结状态,若不处于冻结状态则获取请求方向终端输入的修改额度,进而校验该修改额度是否超过修改阈值,若没有超过修改阈值则提示是否对该修改额度进行保存,若接收到请求方的取消保存的指示,则提示请求方是否重新输入修改额度;若接收到请求方的确定保存的指示,则向终端发送交易密码验证请求,以得到请求方向终端输入的交易密码,进而校验该交易密码是否正确,若正确则根据修改额度的值修改支付额度。

在一些实施方式中,请参阅图 14,图 14 为向终端提供的虚拟证券支付卡管理软件的统一建模语言(Unified Model Language, UML)的示意图,接下来结合图 14 对各个类进行说明:

“支付卡数据中心”用于维护“支付卡模型”及相关的信息,并维护相关的缓存操作,对外提供本地虚拟证券支付卡信息的读写入口。

“支付卡模型”用于提供虚拟证券支付卡的参数结构。

“首页”主要提供虚拟证券支付卡及虚拟证券支付卡管理软件的账户信息、功能入口等。

“账户信息视图”是首页的主视图,提供返现列表的访问入口、完成存在证券账户绑定且未被冻结的虚拟证券支付卡的“正常视图”,以及未完成账户证券账户绑定或者已经被冻结的虚拟证券支付卡的“异常视图”。

“正常视图”中的虚拟证券支付卡需要通过“动态验证码类”进行动态验证码验证,通过“卡片信息弹窗”来获取到虚拟证券支付卡的卡号、安全码、有效期等信息。

“异常视图”分别提供对“证券账户绑定类”及“虚拟证券支付卡管理类”的访问入口,以便进行证券账户的绑定和虚拟证券支付卡的解冻、支付额度调整等操作。

“功能区视图”用于提供对“账单列表”及“卡片管理类”的访问入口,“明细详情”用于查询“账单列表”和“返现列表”中的单项账单或返现的详情信息。

其中,针对“账单列表”和“返现列表”抽象出了“交易明细基类”来封装所有相同的界面显示逻辑,将不同的界面逻辑进行剥离,以减少界面开发的代码数量,便于后续对界面显示的相关代码进行维护和管理。

在一些实施方式中,请参阅图 15,图 15 是本申请的一个实施例示出的基于区块链的支付控制方法的流程图,请参阅图 15,该基于区块链的支付控制方法至少包括步骤 S1510 至步骤 S1580,详细介绍如下:

步骤 S1510,终端向第三方支付平台发送针对证券账户的支付请求,支付请求中包含支付金额、收款方以及虚拟证券支付卡的标识。

步骤 S1520,第三方支付平台将支付请求转发给辅助支付平台。

步骤 S1530,辅助支付平台根据该支付请求向服务器发送验证请求;

步骤 S1540,服务器根据验证请求对支付请求进行验证,若服务器对支付请求进行验证的验证结果为通过,则根据支付金额对证券账户执行资金扣除处理,并从请求方对应的支付额度中扣除支付金额对应的额度,并向辅助支付平台发送支付指令;

步骤 S1550,辅助支付平台根据支付指令向收款方转入支付金额,并向第三方支付平台以及服务器反馈交易结果;

步骤 S1560, 服务器将支付额度对应的资金转移到辅助支付平台中。

本申请可以通过在支付请求验证通过后, 对证券账户执行资金扣除处理, 并指示辅助支付平台对支付金额进行垫付, 以向收款方转入对应的支付金额, 进而保证能够及时完成支付业务, 然后向辅助支付平台转入该辅助支付平台之前垫付的具体金额, 以完成支付流程, 解决了由于证券账户中的资金不能直接使用, 而银证转账又存在资金使用效率低下的问题, 简化了用户使用证券账户中的资金的步骤, 进而提升了支付场景的数据吞吐性能, 并提升了支付的实时性。

图 16 是本申请的一个实施例示出的支付控制装置的框图, 如图 16 所示, 该装置包括:

支付验证模块 1610, 配置为对请求方发起的针对证券账户的支付请求进行验证; 其中, 支付请求中包含支付金额以及收款方;

支付处理模块 1620, 配置为若验证通过, 则根据支付金额对证券账户执行资金扣除处理, 并从请求方对应的支付额度中扣除支付金额对应的额度, 并指示辅助支付平台向收款方转入支付金额;

资金转移模块 1630, 配置为将支付额度对应的资金转移到辅助支付平台中, 生成交易结果;

数据上传模块 1640, 配置为通过智能合约对所述交易结果进行验证, 并在验证通过之后将支付过程中生成的数据上传至区块链中。

在本申请的一个实施例中, 资金转移模块 1630 可以包括:

额度变化值确定单元, 配置为获取预设时间段内辅助支付平台对应的支付额度的额度变化值;

转移单元, 配置为将额度变化值对应的资金转移到辅助支付平台中。

在本申请的一个实施例中, 支付控制装置还包括证券账户确定单元、证券账户选择单元以及支付链接建立单元, 在根据请求方发起的针对虚拟证券支付卡的支付请求, 确定虚拟证券支付卡中包含的待支付的证券账户之前, 还包括:

证券账户确定单元, 配置为根据请求方发起的针对证券账户的绑定请求, 确定可以用于支付的证券账户;

证券账户选择单元, 配置为发送可以用于支付的证券账户至请求方, 以接收请求方针对可以用于支付的证券账户反馈的证券账户选择信息, 得到待绑定的证券账户;

支付链接建立单元, 配置为建立与待绑定的证券账户之间的支付链接。

在本申请的一个实施例中, 证券账户确定单元可以包括:

证券账户状态查询单元, 配置为查询请求方对应的证券账户的证券账户状态;

证券账户可信度计算单元, 配置为根据证券账户状态为正常状态的证券账户的历史交易信息, 计算证券账户状态为正常状态的证券账户的可信度;

可支付确定单元, 配置为将可信度满足预设条件的证券账户作为可以用于支付的证券账户。

在本申请的一个实施例中, 证券账户选择单元可以包括:

证券账户验证请求单元, 配置为响应于证券账户选择信息, 向请求方发送证券账户验证请求;

证券账户验证信息接收单元, 配置为接收请求方根据证券账户验证请求反馈的证券账户验证信息;

验证单元, 配置为根据证券账户验证信息对被选中的证券账户进行证券账户验证;

待绑定确认单元, 配置为若证券账户验证通过, 则将被选中的证券账户作为待绑定的证券账户。

在本申请的一个实施例中, 支付链接建立单元包括:

用户信息获取单元, 配置为获取所述请求方的用户信息;

请求方可信度确定单元, 配置为根据所述用户信息得到的所述请求方的可信度;

支付额度确认单元, 配置为根据所述请求方的可信度生成所述请求方对应的支付额度;

支付链接建立单元,配置为根据所述请求方对应的支付额度建立与所述待绑定的证券账户之间的支付链接。

在本申请的一个实施例中,支付控制装置还可以包括:

支付数据查询请求接收单元,配置为接收请求方发起的针对证券账户的支付数据查询请求,支付数据查询请求中携带有待查询支付数据的数据类型;

数据显示策略以及支付数据记录确定单元,配置为根据数据类型匹配对应的数据显示策略,以及查询数据类型对应的支付数据记录;

查询反馈单元,配置为将数据显示策略以及支付数据记录发送给请求方,以使请求方对应的终端根据数据显示策略对支付数据记录进行显示。

在该示例性的支付控制装置中,通过智能合约对待支付的证券账户中需要用于支付的资金进行锁定,并通过辅助支付平台对收款方进行资金转移,以保证能够及时完成支付业务,然后在智能合约确定辅助支付平台完成支付后,再对待支付的证券账户中被锁定的资金发出转移操作,以将待支付的证券账户中与支付金额对应的资金转移到辅助支付平台中,解决了由于证券账户中的资金不能直接使用,而银证转账又存在资金使用效率低下的问题,简化了用户使用证券账户中的资金的步骤,有利于提高证券账户的资金的使用效率,提高证券账户的资金使用的安全性。

需要说明的是,上述实施例所提供的基于区块链的支付控制装置与上述实施例所提供的基于区块链的支付控制方法属于同一构思,其中各个模块和单元执行操作的具体方式已经在方法实施例进行了详细描述,此处不再赘述。上述实施例所提供的基于区块链的支付控制装置在实际应用中,可以根据需要而将上述功能分配由不同的功能模块完成,即将装置的内部结构划分成不同的功能模块,以完成以上描述的全部或者部分功能,本处也不对此进行限制。

图17示出了适于用来实现本申请实施例的电子设备的计算机系统的结构示意图。

需要说明的是,图17示出的电子设备的计算机系统1700仅是一个示例,不应对本申请实施例的功能和使用范围带来任何限制。

如图17所示,电子设备1700以通用计算设备的形式表现。电子设备1700的组件可以包括但不限于:上述至少一个处理单元1710、上述至少一个存储单元1720、连接不同系统组件(包括存储单元1720和处理单元1710)的总线1730、显示单元1740。

其中,存储单元存储有程序代码,程序代码可以被处理单元1710执行,使得处理单元1710执行本说明书上述“示例性方法”部分中描述的根据本公开各种示例性实施例的步骤。

存储单元1720可以包括易失性存储单元形式的可读介质,例如随机存取存储单元(RAM)1721和/或高速缓存存储单元1722,还可以进一步包括只读存储单元(ROM)1723。

存储单元1720还可以包括具有一组(至少一个)程序模块1725的程序/实用工具1724,这样的程序模块1725包括但不限于:操作系统、一个或者多个应用程序、其它程序模块以及程序数据,这些示例中的每一个或某种组合中可能包括网络环境的实现。

总线1730可以为表示几类总线结构中的一种或多种,包括存储单元总线或者存储单元控制器、外围总线、图形加速端口、处理单元或者使用多种总线结构中的任意总线结构的局域总线。

电子设备1700也可以与一个或多个外部设备1770(例如键盘、指向设备、蓝牙设备等)通信,还可与一个或者多个使得用户能与该电子设备1700交互的设备通信,和/或与使得该电子设备1700能与一个或多个其它计算设备进行通信的任何设备(例如路由器、调制解调器等等)通信。这种通信可以通过输入/输出(I/O)接口1750进行。并且,电子设备1700还可以通过网络适配器1760与一个或者多个网络(例

如局域网(LAN), 广域网(WAN)和/或公共网络, 例如因特网)通信。如图所示, 网络适配器 1760 通过总线 1730 与电子设备 1700 的其它模块通信。应当明白, 尽管图中未示出, 可以结合电子设备 1700 使用其它硬件和/或应用程序模块, 包括但不限于: 微代码、设备驱动器、冗余处理单元、外部磁盘驱动阵列、RAID 系统、磁带驱动器以及数据备份存储系统等。

特别地, 根据本申请的实施例, 上文参考流程图描述的过程可以被实现为计算机应用程序。例如, 本申请的实施例包括一种计算机程序产品, 其包括承载在计算机可读介质上的计算机程序, 该计算机程序包含用于执行流程图所示的方法的计算机程序。在该计算机程序被处理单元 1710 执行时, 执行本申请的系统中限定的各种功能。

需要说明的是, 本申请实施例所示的计算机可读介质可以是计算机可读信号介质或者计算机可读存储介质或者是上述两者的任意组合。计算机可读存储介质例如可以是电、磁、光、电磁、红外线、或半导体的系统、装置或器件, 或者任意以上的组合。计算机可读存储介质的更具体的例子可以包括但不限于: 具有一个或多个导线的电连接、便携式计算机磁盘、硬盘、随机访问存储器(RAM)、只读存储器(ROM)、可擦式可编程只读存储器(Erasable Programmable Read Only Memory, EPROM)、闪存、光纤、便携式紧凑磁盘只读存储器(Compact Disc Read-Only Memory, CD-ROM)、光存储器件、磁存储器件、或者上述的任意合适的组合。在本申请中, 计算机可读存储介质可以是任何包含或存储程序的有形介质, 该程序可以被请求执行系统、装置或者器件使用或者与其结合使用。而在本申请中, 计算机可读的信号介质可以包括在基带中或者作为载波一部分传播的数据信号, 其中承载了计算机可读的计算机程序。这种传播的数据信号可以采用多种形式, 包括但不限于电磁信号、光信号或上述的任意合适的组合。计算机可读的信号介质还可以是计算机可读存储介质以外的任何计算机可读介质, 该计算机可读介质可以发送、传播或者传输用于由请求执行系统、装置或者器件使用或者与其结合使用的程序。计算机可读介质上包含的计算机程序可以用任何适当的介质传输, 包括但不限于: 无线、有线等等, 或者上述的任意合适的组合。

附图中的流程图和框图, 图示了按照本申请各种实施例的系统、方法和计算机程序产品的可能实现的体系架构、功能和操作。其中, 流程图或框图中的每个方框可以代表一个模块、程序段、或代码的一部分, 上述模块、程序段、或代码的一部分包含一个或多个用于实现规定的逻辑功能的可执行请求。也应当注意, 在有些作为替换的实现中, 方框中所标注的功能也可以以不相同于附图中所标注的顺序发生。例如, 两个接连地表示的方框实际上可以基本并行地执行, 它们有时也可以按相反的顺序执行, 这依所涉及的功能而定。也要注意的, 框图或流程图中的每个方框、以及框图或流程图中的方框的组合, 可以用执行规定的功能或操作的专用的基于硬件的系统来实现, 或者可以用专用硬件与计算机请求的组合来实现。

描述于本申请实施例中所涉及到的单元可以通过应用程序的方式实现, 也可以通过硬件的方式来实现在, 所描述的单元也可以设置在处理器中。其中, 这些单元的名称在某种情况下并不构成对该单元本身的限定。

本申请的另一方面还提供了一种计算机可读存储介质, 其上存储有计算机程序, 该计算机程序被处理器执行时实现如前的基于区块链的支付控制方法。该计算机可读存储介质可以是上述实施例中描述的设备中所包含的, 也可以是单独存在, 而未装配入该电子设备中。

本申请的另一方面还提供了一种计算机程序产品或计算机程序, 该计算机程序产品或计算机程序包括计算机请求, 该计算机请求存储在计算机可读存储介质中。计算机设备的处理器从计算机可读存储介质读取该计算机请求, 处理器执行该计算机请求, 使得该计算机设备执行上述各个实施例中提供的基于

区块链的支付控制方法。

上述内容，仅为本申请的较佳示例性实施例，并非用于限制本申请的实施方案，本领域普通技术人员根据本申请的主要构思和精神，可以十分方便地进行相应的变通或修改，故本申请的保护范围应以权利要求书所要求的保护范围为准。

权利要求书

1、一种基于区块链的支付控制方法，包括：

对请求方发起的针对证券账户的支付请求进行验证；其中，所述支付请求中包含支付金额以及收款方；

若验证通过，则根据所述支付金额对所述证券账户执行资金扣除处理，从所述请求方对应的支付额度中扣除所述支付金额对应的额度，并指示辅助支付平台向所述收款方转入所述支付金额；

将所述支付额度对应的资金转移到所述辅助支付平台中，生成交易结果；

通过智能合约对所述交易结果进行验证，并在验证通过之后将支付过程中生成的数据上传至区块链中。

2、根据权利要求1所述的方法，其中，所述将所述支付额度对应的资金转移到所述辅助支付平台中，包括：

获取预设时间段内所述辅助支付平台对应的支付额度的额度变化值；

将所述额度变化值对应的资金转移到所述辅助支付平台中。

3、根据权利要求1所述的方法，其中，在所述对请求方发起的针对证券账户的支付请求进行验证之前，还包括：

根据请求方发起的针对证券账户的绑定请求，确定可以用于支付的证券账户；

发送所述可以用于支付的证券账户至所述请求方，以接收所述请求方针对所述可以用于支付的证券账户反馈的证券账户选择信息，得到待绑定的证券账户；

建立与所述待绑定的证券账户之间的支付链接。

4、根据权利要求3所述的方法，其中，所述根据请求方发起的针对证券账户的绑定请求，确定可以用于支付的证券账户，包括：

查询所述请求方对应的证券账户的证券账户状态；

根据所述证券账户状态为正常状态的证券账户的历史交易信息，计算所述证券账户状态为正常状态的证券账户的可信度；

将所述可信度满足预设条件的证券账户作为可以用于支付的证券账户。

5、根据权利要求3所述的方法，其中，所述发送所述可以用于支付的证券账户至所述请求方，以接收所述请求方针对所述可以用于支付的证券账户反馈的证券账户选择信息，得到待绑定的证券账户，包括：

响应于所述证券账户选择信息，向所述请求方发送证券账户验证请求；

接收所述请求方根据所述证券账户验证请求反馈的证券账户验证信息；

根据所述证券账户验证信息对被选中的证券账户进行证券账户验证；

若所述证券账户验证通过，则将所述被选中的证券账户作为待绑定的证券账户。

6、根据权利要求3所述的方法，其中，所述建立与所述待绑定的证券账户之间的支付链接，包括：

获取所述请求方的用户信息；

根据所述用户信息得到的所述请求方的可信度；

根据所述请求方的可信度生成所述请求方对应的支付额度；

根据所述请求方对应的支付额度建立与所述待绑定的证券账户之间的支付链接。

7、根据权利要求1至6任一项所述的方法，其中，所述方法还包括：

接收所述请求方发起的针对所述证券账户的支付数据查询请求,所述支付数据查询请求中携带有待查询支付数据的数据类型;

根据所述数据类型匹配对应的数据显示策略,以及查询所述数据类型对应的支付数据记录;

将所述数据显示策略以及所述支付数据记录发送给所述请求方,以使所述请求方对应的终端根据所述数据显示策略对所述支付数据记录进行显示。

8、一种支付控制装置,所述装置包括:

支付验证模块,配置为对请求方发起的针对证券账户的支付请求进行验证;其中,所述支付请求中包含支付金额以及收款方;

支付处理模块,配置为若验证通过,则根据所述支付金额对所述证券账户执行资金扣除处理,从所述请求方对应的支付额度中扣除所述支付金额对应的额度,并指示辅助支付平台向所述收款方转入所述支付金额;

交易结果生成模块,配置为将所述支付额度对应的资金转移到所述辅助支付平台中,生成交易结果;

数据上传模块,配置为通过智能合约对所述交易结果进行验证,并在验证通过之后将支付过程中生成的数据上传至区块链中。

9、一种电子设备,包括:

一个或多个处理器;

存储装置,用于存储一个或多个程序,当所述一个或多个程序被所述电子设备执行时,使得所述电子设备实现如权利要求1至7中任一项所述的支付控制方法。

10、一种计算机可读介质,其上存储有计算机程序,所述计算机程序被处理器执行时实现如权利要求1至7中任一项所述的支付控制方法。

11、一种计算机程序产品,所述计算机程序产品包括计算机请求,所述计算机请求被处理器执行时实现如权利要求1至7中任一项所述的支付控制方法。