(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 108305071 A
(43)申请公布日 2018.07.20

(21)申请号 201711459260.5

(22)申请日 2017.12.28

(71)申请人 中国人民银行数字货币研究所
地址 100070 北京市丰台区科学城中核路5号2号楼

(72)发明人 姚前

(74)专利代理机构 中原信达知识产权代理有限责任公司 11219
代理人 张一军 杨晓伟

(51)Int.Cl.
G06Q 20/38(2012.01)
G06Q 20/36(2012.01)
G06F 21/60(2013.01)
G06F 21/62(2013.01)

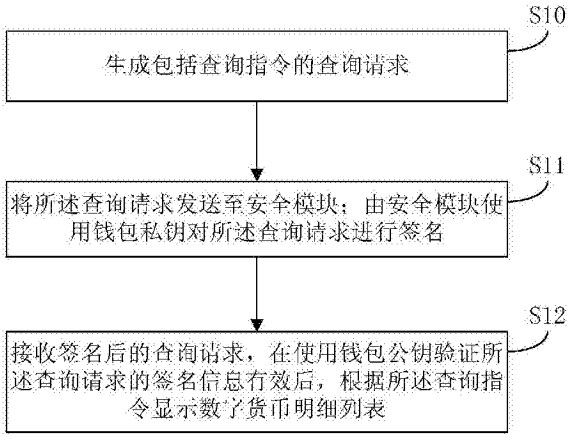
权利要求书3页 说明书10页 附图3页

(54)发明名称

一种查询数字货币明细信息的方法和装置

(57)摘要

本发明公开了一种查询数字货币明细信息的方法和装置，涉及计算机技术领域。该方法的一具体实施方式包括：生成包括查询指令的查询请求；将所述查询请求发送至安全模块；由安全模块使用钱包私钥对所述查询请求进行签名；接收签名后的查询请求，在使用钱包公钥验证所述查询请求的签名信息有效后，根据所述查询指令显示数字货币明细列表。该实施方式能够保证用户查询数字货币明细信息时的安全性。



CN 108305071 A

1.一种查询数字货币明细信息的方法，其特征在于，包括：

生成包括查询指令的查询请求；

将所述查询请求发送至安全模块；由安全模块使用钱包私钥对所述查询请求进行签名；

接收签名后的查询请求，在使用钱包公钥验证所述查询请求的签名信息有效后，根据所述查询指令显示数字货币明细列表。

2.根据权利要求1所述的方法，其特征在于，在根据所述查询指令显示数字货币明细列表的步骤前，还包括：

根据所述查询指令查询本地存放的数字货币，根据查询结果生成数字货币明细列表。

3.根据权利要求1所述的方法，其特征在于，所述查询请求还包括钱包标识和钱包证书；在生成包括查询指令的查询请求的步骤前，还包括：

显示查询指令列表；

根据用户的选择确定查询指令；

获取与所述查询指令相匹配的钱包标识和钱包证书。

4.根据权利要求1所述的方法，其特征在于，在显示数字货币明细列表的步骤后，还包括：

对所述数字货币明细列表中的数字货币的状态进行验证；其中，数字货币的状态包括其真伪、是否有效、金额、所有者公钥、发行机构名称、有效期限中的至少一种。

5.根据权利要求4所述的方法，其特征在于，对所述数字货币明细列表中的数字货币的状态进行验证的步骤，包括：

根据用户的选择确定待验证数字货币；

生成包括所述待验证数字货币的数字货币字串的验证请求；

将所述验证请求发送至安全模块，由安全模块使用钱包私钥对所述验证请求进行签名；

接收签名后的验证请求，在使用钱包公钥验证所述验证请求的签名信息有效后，将签名后的验证请求发送至数字货币验证机构；

接收并显示所述数字货币验证机构返回的验证结果。

6.根据权利要求5所述的方法，其特征在于，所述验证请求还包括验证指令，在生成包括所述待验证数字货币的数字货币字串的验证请求的步骤前，还包括：

根据待验证数字货币的数字货币字串生成验证指令；所述验证指令用于补充数字货币字串的信息、实现符合查询规范的格式转换或补充所有者授权查询信息中的至少一种；所述验证指令包括验证请求选项，所述验证请求选项用于指定真伪、是否有效、金额、所有者公钥、发行机构名称、有效期限中的至少一种作为验证内容。

7.根据权利要求5所述的方法，其特征在于，数字货币验证机构使用机构私钥对验证结果进行签名；接收并显示所述数字货币验证机构返回的验证结果的步骤，包括：

接收所述数字货币验证机构返回的验证结果；

将验证结果发送至安全模块；由安全模块使用机构公钥对所述验证结果的签名信息进行验证；

若签名信息有效，则显示所述验证结果。

8.一种查询数字货币明细信息的装置，其特征在于，包括：

查询请求生成模块，用于生成包括查询指令的查询请求；

查询请求签名模块，用于将所述查询请求发送至安全模块；由安全模块使用钱包私钥对所述查询请求进行签名；

明细列表显示模块，用于接收签名后的查询请求，在使用钱包公钥验证所述查询请求的签名信息有效后，根据所述查询指令显示数字货币明细列表。

9.根据权利要求8所述的装置，其特征在于，所述明细列表显示模块还用于：

根据所述查询指令查询本地存放的数字货币，根据查询结果生成数字货币明细列表。

10.根据权利要求8所述的装置，其特征在于，所述查询请求还包括钱包标识和钱包证书；所述装置还包括：

查询指令选择模块，用于显示查询指令列表；根据用户的选择确定查询指令；以及获取与所述查询指令相匹配的钱包标识和钱包证书。

11.根据权利要求8所述的装置，其特征在于，所述装置还包括：

状态验证模块，用于对所述数字货币明细列表中的数字货币的状态进行验证；其中，数字货币的状态包括其真伪、是否有效、金额、所有者公钥、发行机构名称、有效期限中的至少一种。

12.根据权利要求11所述的装置，其特征在于，所述状态验证模块还用于：根据用户的选择确定待验证数字货币；生成包括所述待验证数字货币的数字货币字串的验证请求；将所述验证请求发送至安全模块，由安全模块使用钱包私钥对所述验证请求进行签名；接收签名后的验证请求，在使用钱包公钥验证所述验证请求的签名信息有效后，将签名后的验证请求发送至数字货币验证机构；以及接收并显示所述数字货币验证机构返回的验证结果。

13.根据权利要求12所述的装置，其特征在于，所述验证请求还包括验证指令，所述状态验证模块还用于：

根据待验证数字货币的数字货币字串生成验证指令；所述验证指令用于补充数字货币字串的信息、实现符合查询规范的格式转换或补充所有者授权查询信息中的至少一种；所述验证指令包括验证请求选项，所述验证请求选项用于指定真伪、是否有效、金额、所有者公钥、发行机构名称、有效期限中的至少一种作为验证内容。

14.根据权利要求12所述的装置，其特征在于，数字货币验证机构使用机构私钥对验证结果进行签名；所述状态验证模块还用于：

接收所述数字货币验证机构返回的验证结果；

将验证结果发送至安全模块，由安全模块使用机构公钥对所述验证结果的签名信息进行验证；

若签名信息有效，则显示所述验证结果。

15.一种查询数字货币明细信息的电子设备，其特征在于，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一个或多个处理器执行，使得所述一个或多个处理器实现如权利要求1-7中任一所述的方法。

16.一种计算机可读介质，其上存储有计算机程序，其特征在于，所述程序被处理器执行时实现如权利要求1-7中任一所述的方法。

一种查询数字货币明细信息的方法和装置

技术领域

[0001] 本发明涉及计算机技术领域，尤其涉及一种查询数字货币明细信息的方法和装置。

背景技术

[0002] 现有的以比特币为代表的虚拟货币，其实现原理均基于数字化的账户体系，涉及此类虚拟货币的查询功能均依赖该账户系统完成，用户终端只是提供账户访问的入口。

[0003] 本发明技术方案中所指的数字货币，则是以加密货币字串的形式存在的真实数据，可以理解为数字化的纸币或硬币，数字货币的字串等信息存放于本地的数字货币钱包中。如何保证用户使用数字货币钱包查询数值货币明细信息时的安全，是本发明希望解决的问题。

发明内容

[0004] 有鉴于此，本发明实施例提供一种查询数字货币明细信息的方法和装置，能够保证用户查询数字货币明细信息时的安全性。

[0005] 为实现上述目的，根据本发明实施例的一个方面，提供了一种查询数字货币明细信息的方法，包括：

[0006] 生成包括查询指令的查询请求；

[0007] 将所述查询请求发送至安全模块；由安全模块使用钱包私钥对所述查询请求进行签名；

[0008] 接收签名后的查询请求，在使用钱包公钥验证所述查询请求的签名信息有效后，根据所述查询指令显示数字货币明细列表。

[0009] 可选的，在根据所述查询指令显示数字货币明细列表的步骤前，还包括：

[0010] 根据所述查询指令查询本地存放的数字货币，根据查询结果生成数字货币明细列表。

[0011] 可选的，所述查询请求还包括钱包标识和钱包证书；在生成包括查询指令的查询请求的步骤前，还包括：

[0012] 显示查询指令列表；

[0013] 根据用户的选择确定查询指令；

[0014] 获取与所述查询指令相匹配的钱包标识和钱包证书。

[0015] 可选的，在显示数字货币明细列表的步骤后，还包括：

[0016] 对所述数字货币明细列表中的数字货币的状态进行验证；其中，数字货币的状态包括其真伪、是否有效、金额、所有者公钥、发行机构名称、有效期限中的至少一种。

[0017] 可选的，对所述数字货币明细列表中的数字货币的状态进行验证的步骤，包括：

[0018] 根据用户的选择确定待验证数字货币；

[0019] 生成包括所述待验证数字货币的数字货币字串的验证请求；

[0020] 将所述验证请求发送至安全模块，由安全模块使用钱包私钥对所述验证请求进行签名；

[0021] 接收签名后的验证请求，在使用钱包公钥验证所述验证请求的签名信息有效后，将签名后的验证请求发送至数字货币验证机构；

[0022] 接收并显示所述数字货币验证机构返回的验证结果。

[0023] 可选的，所述验证请求还包括验证指令，在生成包括所述待验证数字货币的数字货币字串的验证请求的步骤前，还包括：

[0024] 根据待验证数字货币的数字货币字串生成验证指令；所述验证指令用于补充数字货币字串的信息、实现符合查询规范的格式转换或补充所有者授权查询信息中的至少一种；所述验证指令包括验证请求选项，所述验证请求选项用于指定真伪、是否有效、金额、所有者公钥、发行机构名称、有效期限中的至少一种作为验证内容。

[0025] 数字货币验证机构使用机构私钥对验证结果进行签名；接收并显示所述数字货币验证机构返回的验证结果的步骤，包括：

[0026] 接收所述数字货币验证机构返回的验证结果；

[0027] 将验证结果发送至安全模块；由安全模块使用机构公钥对所述验证结果的签名信息进行验证；

[0028] 若签名信息有效，则显示所述验证结果。

[0029] 为实现上述目的，根据本发明实施例的另一个方面，提供了一种查询数字货币明细信息的装置，包括：

[0030] 查询请求生成模块，用于生成包括查询指令的查询请求；

[0031] 查询请求签名模块，用于将所述查询请求发送至安全模块；由安全模块使用钱包私钥对所述查询请求进行签名；

[0032] 明细列表显示模块，用于接收签名后的查询请求，在使用钱包公钥验证所述查询请求的签名信息有效后，根据所述查询指令显示数字货币明细列表。

[0033] 可选的，所述明细列表显示模块还用于：

[0034] 根据所述查询指令查询本地存放的数字货币，根据查询结果生成数字货币明细列表。

[0035] 可选的，所述查询请求还包括钱包标识和钱包证书；所述装置还包括：

[0036] 查询指令选择模块，用于显示查询指令列表；根据用户的选择确定查询指令；以及获取与所述查询指令相匹配的钱包标识和钱包证书。

[0037] 可选的，所述装置还包括：

[0038] 状态验证模块，用于对所述数字货币明细列表中的数字货币的状态进行验证；其中，数字货币的状态包括其真伪、是否有效、金额、所有者公钥、发行机构名称、有效期限中的至少一种。

[0039] 可选的，所述状态验证模块还用于：根据用户的选择确定待验证数字货币；生成包括所述待验证数字货币的数字货币字串的验证请求；将所述验证请求发送至安全模块，由安全模块使用钱包私钥对所述验证请求进行签名；接收签名后的验证请求，在使用钱包公钥验证所述验证请求的签名信息有效后，将签名后的验证请求发送至数字货币验证机构；以及接收并显示所述数字货币验证机构返回的验证结果。

[0040] 可选的，所述状态验证模块还用于：将签名后的验证请求发送至功能执行模块；功能执行模块使用钱包公钥验证所述验证请求中的签名信息是否有效；若确定所述签名信息有效，则由功能执行模块将签名后的验证请求发送至数字货币验证机构。

[0041] 可选的，所述验证请求还包括验证指令，所述状态验证模块还用于：

[0042] 根据待验证数字货币的数字货币字串生成验证指令；所述验证指令用于补充数字货币字串的信息、实现符合查询规范的格式转换或补充所有者授权查询信息中的至少一种；所述验证指令包括验证请求选项，所述验证请求选项用于指定真伪、是否有效、金额、所有者公钥、发行机构名称、有效期限中的至少一种作为验证内容。

[0043] 可选的，数字货币验证机构使用机构私钥对验证结果进行签名；所述状态验证模块还用于：

[0044] 接收所述数字货币验证机构返回的验证结果；

[0045] 将验证结果发送至安全模块，由安全模块使用机构公钥对所述验证结果的签名信息进行验证；

[0046] 若签名信息有效，则显示所述验证结果。

[0047] 为实现上述目的，根据本发明实施例的再一个方面，提供了一种查询数字货币明细信息的电子设备，包括：

[0048] 一个或多个处理器；

[0049] 存储装置，用于存储一个或多个程序，

[0050] 当所述一个或多个程序被所述一个或多个处理器执行，使得所述一个或多个处理器至少实现：

[0051] 生成包括查询指令的查询请求；

[0052] 将所述查询请求发送至安全模块；由安全模块使用钱包私钥对所述查询请求进行签名；

[0053] 接收签名后的查询请求，在使用钱包公钥验证所述查询请求的签名信息有效后，根据所述查询指令显示数字货币明细列表。

[0054] 为实现上述目的，根据本发明实施例的又一个方面，提供一种计算机可读介质，其上存储有计算机程序，所述程序被处理器执行时至少实现：

[0055] 生成包括查询指令的查询请求；

[0056] 将所述查询请求发送至安全模块；由安全模块使用钱包私钥对所述查询请求进行签名；

[0057] 接收签名后的查询请求，在使用钱包公钥验证所述查询请求的签名信息有效后，根据所述查询指令显示数字货币明细列表。

[0058] 上述发明中的一个实施例具有如下优点或有益效果：因为采用了安全模块对查询请求进行签名，由功能执行模块验证签名后再显示数字货币明细列表的技术手段，确保查询请求来源可靠，从而避免用户的数字货币信息发生泄漏，达到了提高查询安全性的技术效果。

[0059] 上述的非惯用的可选方式所具有的进一步效果将在下文中结合具体实施方式加以说明。

附图说明

[0060] 附图用于更好地理解本发明，不构成对本发明的不当限定。其中：

[0061] 图1是根据本发明实施例的查询数字货币明细信息的方法的主要步骤的示意图；

[0062] 图2是根据本发明实施例的查询数字货币明细信息的装置的主要模块的示意图；

[0063] 图3是基于本发明实施例中查询数字货币明细信息的方法所构建的查询系统的通信过程示意图；

[0064] 图4是本发明实施例可以应用于其中的示例性系统架构图；

[0065] 图5是适于用来实现本发明实施例的终端设备或服务器的计算机系统的结构示意图。

具体实施方式

[0066] 以下结合附图对本发明的示范性实施例做出说明，其中包括本发明实施例的各种细节以助于理解，应当将它们认为仅仅是示范性的。因此，本领域普通技术人员应当认识到，可以对这里描述的实施例做出各种改变和修改，而不会背离本发明的范围和精神。同样，为了清楚和简明，以下的描述中省略了对公知功能和结构的描述。

[0067] 图1是根据本发明实施例的查询数字货币明细信息的方法的主要步骤的示意图。

[0068] 如图1所示，根据本发明实施例提供的一种查询数字货币明细信息的方法，包括：

[0069] S10，功能执行模块生成包括查询指令的查询请求。本步骤中的查询指令是指用于查询数字货币明细信息的指令，该指令由用户选择或者输入。

[0070] S11，功能模块将所述查询请求发送至安全模块；由安全模块使用钱包私钥对所述查询请求进行签名。本步骤中出现的钱包私钥和后续步骤中出现的钱包公钥相互匹配，钱包私钥和钱包公钥在用户开通数字货币钱包的过程中、在安全模块内部生成，其中，钱包私钥在安全模块内部具有极高的保密性和安全性，钱包公钥可以在网络公开或伴随签名后的信息发送至接受者，接受者获取到钱包公钥后即可对签名信息进行验证。

[0071] S12，安全模块将签名后的查询请求发送至功能执行模块。功能执行模块用于实现钱包的主要业务功能，本实施例中提供的数字货币明细信息是其功能的一部分。

[0072] S13，功能执行模块接收签名后的查询请求，在使用钱包公钥验证所述查询请求的签名信息有效后，根据所述查询指令显示数字货币明细列表。其中，数字货币明细列表保存在功能执行模块本地，由功能执行模块进行管理；在数字货币明细列表中，包含各数字货币的数字货币字串，还可以包括该数字货币发行机构的验证指令、金额、发行机构名称、生产日期等等。

[0073] 本实施例的方案中，包括终端系统、安全模块和功能执行模块三侧；其中，终端系统用于提供显示界面和接收用户的指令，功能执行模块用于实现数字货币钱包的主要业务功能，安全模块为功能执行模块与终端系统或外部的通信过程提供签名以及签名验证的功能，提供安全保障。

[0074] 从上面所述可以看出，本实施例提供的查询数字货币明细信息的方法，因为采用了安全模块对查询请求进行签名，由功能执行模块验证签名后再显示数字货币明细列表的技术手段，确保查询请求来源可靠，从而避免用户的数字货币信息发生泄漏，达到了提高查

询安全性的技术效果。

[0075] 步骤S13中，在根据所述查询指令显示数字货币明细列表的步骤前，还包括：

[0076] 功能执行模块根据所述查询指令查询本地存放的数字货币，根据查询结果生成数字货币明细列表。

[0077] 本申请中所指的数字货币不同于现有的虚拟货币。现有的虚拟货币没有实体的数据，而是通过维护账本来记录用户所持货币额，用户实际并不持有任何资金或资产；而本申请中的数字货币则是以加密形式存在的字串，存放于用户终端的数字货币钱包(即本实施例中的功能执行模块)中。由于具备上述区别，因此在查询数字货币明细信息时，不需要联网查询账本，而只需查询并统计本地存放的数字货币即可。

[0078] 在一些可选的实施例中，所述查询请求还包括钱包标识和钱包证书；步骤S10中，在生成包括查询指令的查询请求的步骤前，还包括：

[0079] 功能执行模块显示查询指令列表；根据用户的选择确定查询指令；获取与所述查询指令相匹配的钱包标识和钱包证书。

[0080] 本实施例中，查询指令列表除包括数字货币明细查询指令之外，还可以包括例如交易明细查询指令、关联银行账户查询指令等。为了提供更加全面的信息，在显示查询指令列表的同时，还可以显示钱包概要信息，包括例如钱包所有者名称、钱包服务机构名称、钱包类型、当前存放有效币余额或者币总数等。钱包标识用于唯一确定一个数字货币钱包，钱包证书包含有前文提到的钱包公钥；即本实施例中的查询请求中包含有查询指令、钱包标识和钱包证书三部分信息，钱包标识便于准确地定位到特定钱包、钱包证书便于获取到钱包公钥，提高查询过程的可靠性。

[0081] 在一些可选的实施例中，在步骤S13中，显示数字货币明细列表的步骤后，还包括：

[0082] 对所述数字货币明细列表中的数字货币的状态进行验证。其中，数字货币的状态包括但不限于数字货币的真伪、是否有效、金额、所有者公钥、发行机构名称、有效期限中的至少一种。

[0083] 对所述数字货币明细列表中的数字货币的有效性进行验证的步骤，包括：

[0084] 根据用户的选择确定待验证数字货币；生成包括所述待验证数字货币的数字货币字串的验证请求；将所述验证请求发送至安全模块，由安全模块使用钱包私钥对所述验证请求进行签名；接收签名后的验证请求，在使用钱包公钥验证所述验证请求的签名信息有效后，将签名后的验证请求发送至数字货币验证机构；接收并显示所述数字货币验证机构返回的验证结果。

[0085] 数字货币验证机构是负责对数字货币的状态进行管理的机构，在接受到验证请求后，数字货币验证机构首先使用发送方的钱包公钥对该验证请求进行签名验证，若验证通过，则进一步对验证请求中所包含的数字货币字串的状态进行核查验证，并将验证结果以数字货币验证机构私钥签名后发送至用户终端；除验证数字货币的真伪或是否有效外，在验证数字货币的其他状态时，还需要验证是否已经取得所有者授权。

[0086] 由于用户是通过终端系统下达的验证请求，因此需要确保该请求的安全性。安全模块首先对该请求进行签名，由钱包的功能执行模块验证签名有效后，再将其发送至相关数字货币验证机构。

[0087] 所述验证请求还包括验证指令，在生成包括所述待验证数字货币的数字货币字串

的验证请求的步骤前，还包括：

[0088] 根据待验证数字货币的数字货币字串生成验证指令；所述验证指令用于补充数字货币字串的信息、实现符合查询规范的格式转换或补充所有者授权查询信息中的至少一种。

[0089] 图2是根据本发明实施例的查询数字货币明细信息的装置的主要模块的示意图。

[0090] 如图2所示，根据本发明的另一实施例，提供一种查询数字货币明细信息的装置200，包括：

[0091] 查询请求生成模块201，用于生成包括查询指令的查询请求；

[0092] 查询请求签名模块202，用于将所述查询请求发送至安全模块203；由安全模块203使用钱包私钥对所述查询请求进行签名；

[0093] 明细列表显示模块204，用于接收签名后的查询请求，在使用钱包公钥验证所述查询请求的签名信息有效后，根据所述查询指令显示数字货币明细列表。

[0094] 在一些可选的实施例中，所述明细列表显示模块204还用于：

[0095] 根据所述查询指令查询本地存放的数字货币，根据查询结果生成数字货币明细列表。

[0096] 在一些可选的实施例中，所述查询请求还包括钱包标识和钱包证书；所述装置200还包括：

[0097] 查询指令选择模块205，用于显示查询指令列表；根据用户的选择确定查询指令；以及获取与所述查询指令相匹配的钱包标识和钱包证书。

[0098] 在一些可选的实施例中，所述装置200还包括：

[0099] 状态验证模块206，用于对所述数字货币明细列表中的数字货币的有效性进行验证。其中，数字货币的状态包括其真伪、是否有效、金额、所有者公钥、发行机构名称、有效期限中的至少一种。

[0100] 在一些可选的实施例中，所述状态验证模块206还用于：根据用户的选择确定待验证数字货币；生成包括所述待验证数字货币的数字货币字串的验证请求；使用钱包私钥对所述验证请求进行签名；将签名后的验证请求发送至数字货币验证机构；以及接收并显示所述数字货币验证机构返回的验证结果。

[0101] 在一些可选的实施例中，所述状态验证模块206还用于：将签名后的验证请求发送至功能执行模块203；功能执行模块203使用钱包公钥验证所述验证请求中的签名信息是否有效；若确定所述签名信息有效，则由功能执行模块203将签名后的验证请求发送至数字货币验证机构。

[0102] 在一些可选的实施例中，所述验证请求还包括验证指令，所述状态验证模块206还用于：

[0103] 根据待验证数字货币的数字货币字串生成验证指令；所述验证指令用于补充数字货币字串的信息、实现符合查询规范的格式转换或补充所有者授权查询信息中的至少一种。

[0104] 图3是基于本发明实施例中查询数字货币明细信息的方法所构建的查询系统的通信过程示意图。

[0105] 如图3所示，本实施例提供的查询系统300包括终端钱包合约功能执行模块32、终

端安全模块33和数字货币验证机构34;用户31为使用者。其中,终端钱包合约功能执行模块32对应于在前方法实施例中的功能执行模块,终端安全模块33对应于在前方法实施例中的安全模块;终端钱包合约功能执行模块32和终端安全模块33可以为软件模块,也可作为合一的硬件或各自独立的硬件,还可以是由软硬件结合构成的组件。终端钱包合约功能执行模块32主要用于实现数字货币钱包业务功能,终端安全模块33则用于维持数字货币钱包的安全性,例如对终端钱包合约功能执行模块32发送或接收的信息进行签名和签名验证。

[0106] 基于查询系统300,用户31实现的查询过程包括:

[0107] 301.用户31登录本地数字货币钱包。

[0108] 302.在用户31登录钱包后,选择并进入查询界面,由终端钱包合约功能执行模块32控制显示钱包概要信息和查询指令列表。钱包概要信息主要包括钱包所有者名称、钱包服务机构名称、钱包类型、当前存放有效币余额或者币总数。查询指令列表主要包括交易明细查询指令、关联银行账户查询指令、数字货币明细查询指令等。

[0109] 303.用户31通过点击等方式选择数字货币明细查询指令,选择结果被发送至终端钱包合约功能执行模块32。

[0110] 304.终端钱包合约功能执行模块32根据用户选择的数字货币明细查询指令,生成包括钱包标识、证书、数字货币明细查询指令的数字货币明细查询请求。

[0111] 305.终端钱包合约功能执行模块32将数字货币明细查询指令发送给终端安全模块33。

[0112] 306.终端安全模块33使用钱包私钥签名数字货币明细查询请求,并将签名后的数字货币明细查询请求发送至终端钱包合约功能执行模块32。

[0113] 307.终端钱包合约功能执行模块32使用钱包公钥验证数字货币明细查询请求的签名信息.

[0114] 308.终端钱包合约功能执行模块32在验证通过后,控制显示数字货币明细列表,数字货币明细查询列表包含数字货币字串以及发行机构验证指令、金额、发行机构名称、生产日期。其中,在显示数字货币明细列表之前,终端钱包合约功能执行模块32查询本地存放的全部数字货币,并根据查询结果生成该明细列表。

[0115] 309.用户31通过点击等方式选择数字货币明细列表中的特定数字货币,选择结果被发送至终端安全模块33。

[0116] 310.终端钱包合约功能执行模块32根据该特定数字货币生成数字货币验证请求。数字货币验证请求中包括该特定数字货币的字串和验证指令;其中,验证指令由终端安全模块33和终端钱包合约功能执行模块32生成的,主要是对待验证数字货币子串的信息的补充或者符合查询规范的格式转换。

[0117] 311.终端钱包合约功能执行模块32将数字货币验证请求发送至终端安全模块33。

[0118] 312.终端安全模块33用钱包私钥签名数字货币验证请求,并将签名后的数字货币验证请求发送至终端钱包合约功能执行模块32。

[0119] 313.终端钱包合约功能执行模块32使用钱包公钥验证数字货币验证请求中的签名信息。

[0120] 314.验证通过后,终端钱包合约功能执行模块32将数字货币验证请求发送至数字货币验证机构34。

[0121] 315.数字货币验证机构34根据数字货币验证请求，验证该特定数字货币的有效性，主要为该数字货币的真伪、是否有效、金额、所有者公钥、发行机构名称、有效期限等；以及在验证完成后，使用数字货币验证机构的机构私钥对验证结果签名。

[0122] 316.数字货币验证机构34将验证结果发送至终端钱包合约功能执行模块32。

[0123] 317.终端钱包合约功能执行模块32将验证结果发送至终端安全模块33。

[0124] 318.终端安全模块33用机构公钥对验证结果的签名信息进行验证。验证私钥和验证公钥是数字货币验证机构34持有的、相互匹配的一对秘钥，在此不再赘述。

[0125] 319.在验证通过后，终端钱包合约功能执行模块32向用户31显示验证结果。

[0126] 图4示出了可以应用本发明实施例的查询数字货币明细信息的方法或查询数字货币明细信息的装置的示例性系统架构400。

[0127] 如图4所示，系统架构400可以包括终端设备401、402、403，网络404和服务器405。网络404用以在终端设备401、402、403和服务器405之间提供通信链路的介质。网络404可以包括各种连接类型，例如有线、无线通信链路或者光纤电缆等等。

[0128] 用户可以使用终端设备401、402、403通过网络404与服务器405交互，以接收或发送消息等。终端设备401、402、403上可以安装有各种数字货币钱包应用。

[0129] 终端设备401、402、403可以是具有显示屏并且支持网页浏览的各种电子设备，包括但不限于智能手机、平板电脑、膝上型便携计算机和台式计算机等等。

[0130] 服务器405可以是提供各种服务的服务器，例如对用户利用终端设备401、402、403所运行的数字货币钱包提供验证功能的后台管理服务器。

[0131] 需要说明的是，本发明实施例所提供的查询数字货币明细信息的方法一般由终端设备401、402、403，相应地，查询数字货币明细信息的装置一般终端设备401、402、403中。

[0132] 应该理解，图4中的终端设备、网络和服务器的数目仅仅是示意性的。根据实现需要，可以具有任意数目的终端设备、网络和服务器。

[0133] 根据本发明的实施例，本发明还提供了一种电子设备和一种可读存储介质。

[0134] 图5是适于用来实现本发明实施例的终端设备或服务器的计算机系统的结构示意图。

[0135] 下面参考图5，其示出了适于用来实现本发明实施例的终端设备的计算机系统500的结构示意图。图5示出的终端设备仅仅是一个示例，不应对本发明实施例的功能和使用范围带来任何限制。

[0136] 如图5所示，计算机系统500包括中央处理单元(CPU)501，其可以根据存储在只读存储器(ROM)502中的程序或者从存储部分508加载到随机访问存储器(RAM)503中的程序而执行各种适当的动作和处理。在RAM 503中，还存储有系统500操作所需的各种程序和数据。CPU 501、ROM 502以及RAM 503通过总线504彼此相连。输入/输出(I/O)接口505也连接至总线504。

[0137] 以下部件连接至I/O接口505：包括键盘、鼠标等的输入部分506；包括诸如阴极射线管(CRT)、液晶显示器(LCD)等以及扬声器等的输出部分507；包括硬盘等的存储部分508；以及包括诸如LAN卡、调制解调器等的网络接口卡的通信部分509。通信部分509经由诸如因特网的网络执行通信处理。驱动器510也根据需要连接至I/O接口505。可拆卸介质511，诸如磁盘、光盘、磁光盘、半导体存储器等等，根据需要安装在驱动器510上，以便于从其上读出

的计算机程序根据需要被安装入存储部分508。

[0138] 特别地，根据本发明的实施例，上文主要步骤的示意图描述的过程可以被实现为计算机软件程序。例如，本发明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主要步骤的示意图所示的方法的程序代码。在这样的实施例中，该计算机程序可以通过通信部分509从网络上被下载和安装，和/或从可拆卸介质511被安装。在该计算机程序被中央处理单元(CPU)501执行时，执行本发明的系统中限定的上述功能。

[0139] 需要说明的是，本发明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——但不限于——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(EPROM或闪存)、光纤、便携式紧凑磁盘只读存储器(CD-ROM)、光存储器件、磁存储器件、或者上述的任意合适的组合。在本发明中，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，该程序可以被指令执行系统、装置或者器件使用或者与其结合使用。而在本发明中，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程序代码。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指令执行系统、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程序代码可以用任何适当的介质传输，包括但不限于：无线、电线、光缆、RF等等，或者上述的任意合适的组合。

[0140] 附图中的流程图和框图，图示了按照本发明各种实施例的系统、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。在这点上，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指令。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。也要注意的是，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指令的组合来实现。

[0141] 描述于本发明实施例中所涉及到的模块可以通过软件的方式实现，也可以通过硬件的方式来实现。所描述的模块也可以设置在处理器中，例如，可以描述为：一种处理器包括查询请求生成模块201、查询请求签名模块202、功能执行模块203、查询指令选择模块204和状态验证模块205。其中，这些模块的名称在某种情况下并不构成对该模块本身的限定，例如，功能执行模块还可以被描述为“用于在使用钱包公钥验证所述查询请求的签名信息有效后，根据所述查询指令显示数字货币明细列表的模块”。

[0142] 作为另一方面，本发明还提供了一种计算机可读介质，该计算机可读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，而未装配入该设备中。上述计算

机可读介质承载有一个或者多个程序，当上述一个或者多个程序被一个该设备执行时，使得该设备包括：

[0143] 生成包括查询指令的查询请求；

[0144] 使用钱包私钥对所述查询请求进行签名；

[0145] 将签名后的查询请求发送至功能执行模块；

[0146] 功能执行模块在使用钱包公钥验证所述查询请求的签名信息有效后，根据所述查询指令显示数字货币明细列表。

[0147] 根据本发明实施例的技术方案，因为采用了安全模块对查询请求进行签名，由功能执行模块验证签名后再显示数字货币明细列表的技术手段，确保查询请求来源可靠，从而避免用户的数字货币信息发生泄漏，达到了提高查询安全性的技术效果。

[0148] 上述具体实施方式，并不构成对本发明保护范围的限制。本领域技术人员应该明白的是，取决于设计要求和其他因素，可以发生各种各样的修改、组合、子组合和替代。任何在本发明的精神和原则之内所作的修改、等同替换和改进等，均应包含在本发明保护范围之内。

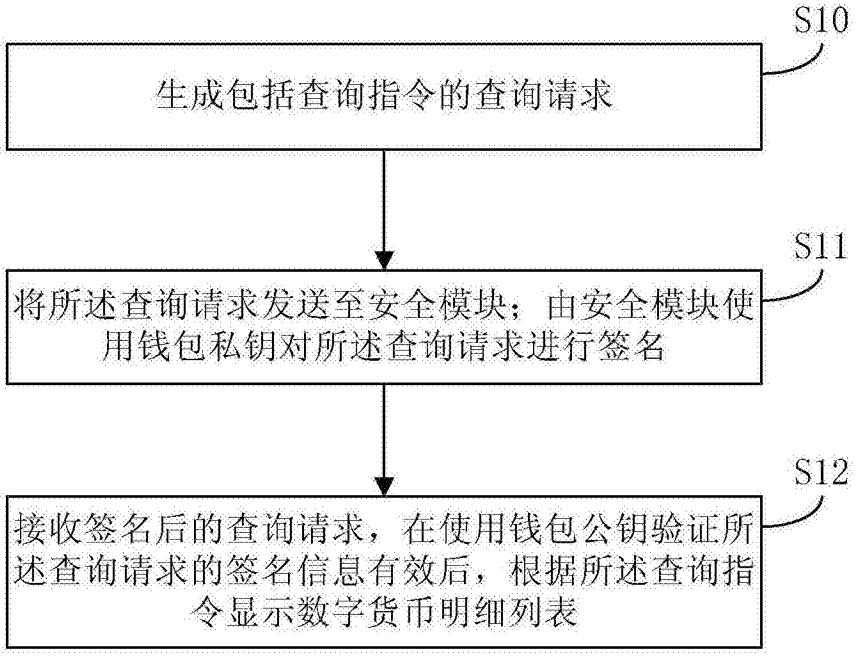

S10
生成包括查询指令的查询请求
S11
将所述查询请求发送至安全模块；由安全模块使用钱包私钥对所述查询请求进行签名
S12
接收签名后的查询请求，在使用钱包公钥验证所述查询请求的签名信息有效后，根据所述查询指令显示数字货币明细列表

图1

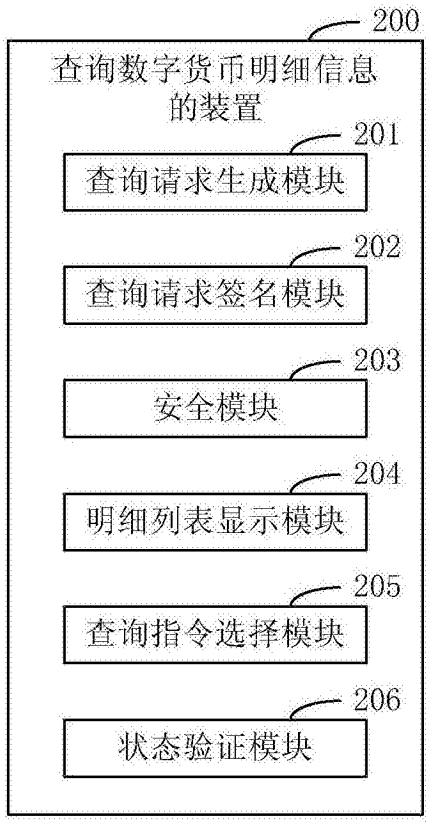

200
查询数字货币明细信息的装置
201
查询请求生成模块
202
查询请求签名模块
203
安全模块
204
明细列表显示模块
205
查询指令选择模块
206
状态验证模块

图2

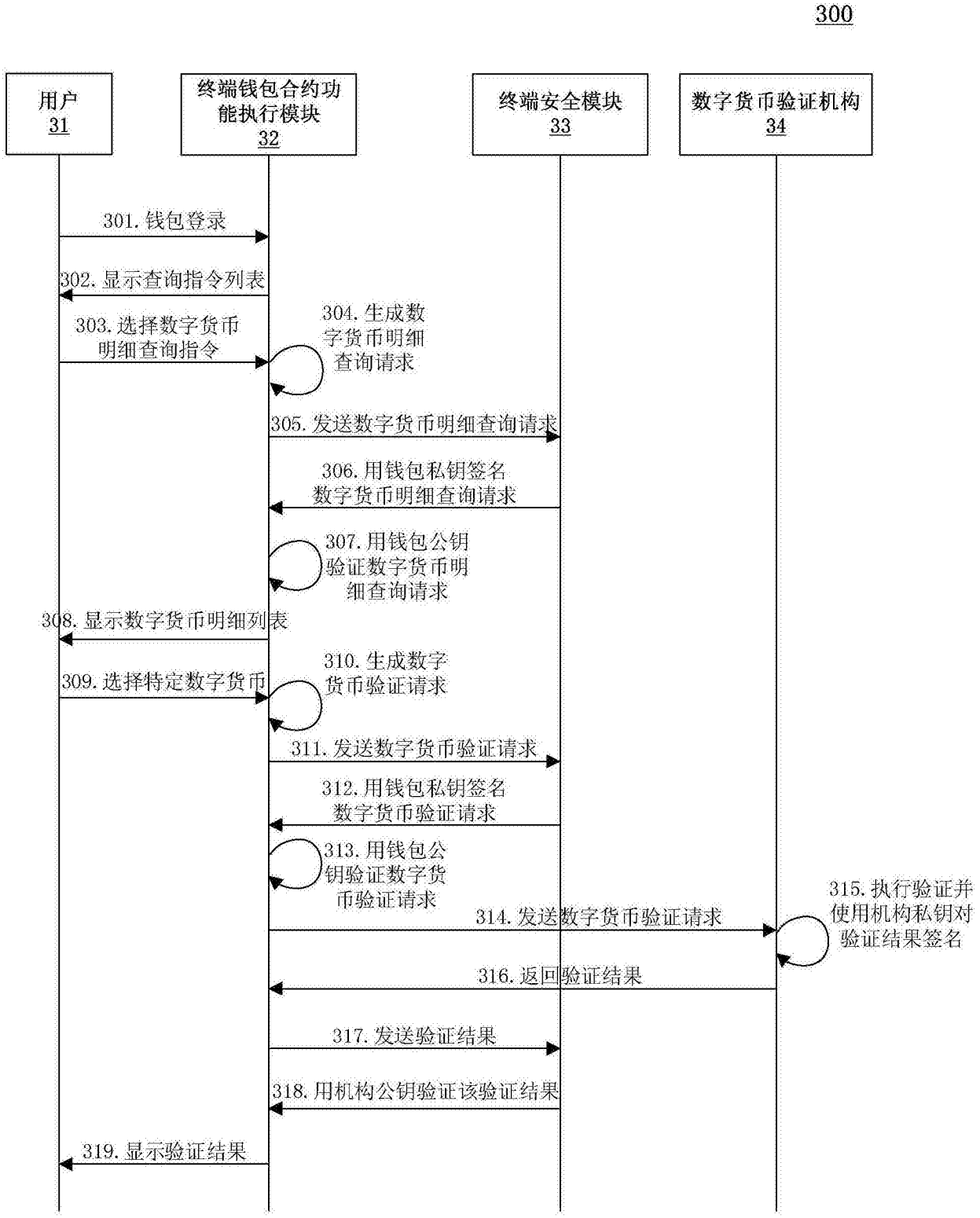

300
用户
31
终端钱包合约功能执行模块
32
终端安全模块
33
数字货币验证机构
34
301. 钱包登录
302. 显示查询指令列表
303. 选择数字货币明细查询指令
304. 生成数字货币明细查询请求
305. 发送数字货币明细查询请求
306. 用钱包私钥签名数字货币明细查询请求
307. 用钱包公钥验证数字货币明细查询请求
308. 显示数字货币明细列表
309. 选择特定数字货币
310. 生成数字货币验证请求
311. 发送数字货币验证请求
312. 用钱包私钥签名数字货币验证请求
313. 用钱包公钥验证数字货币验证请求
314. 发送数字货币验证请求
315. 执行验证并使用机构私钥对验证结果签名
316. 返回验证结果
317. 发送验证结果
318. 用机构公钥验证该验证结果
319. 显示验证结果

图3

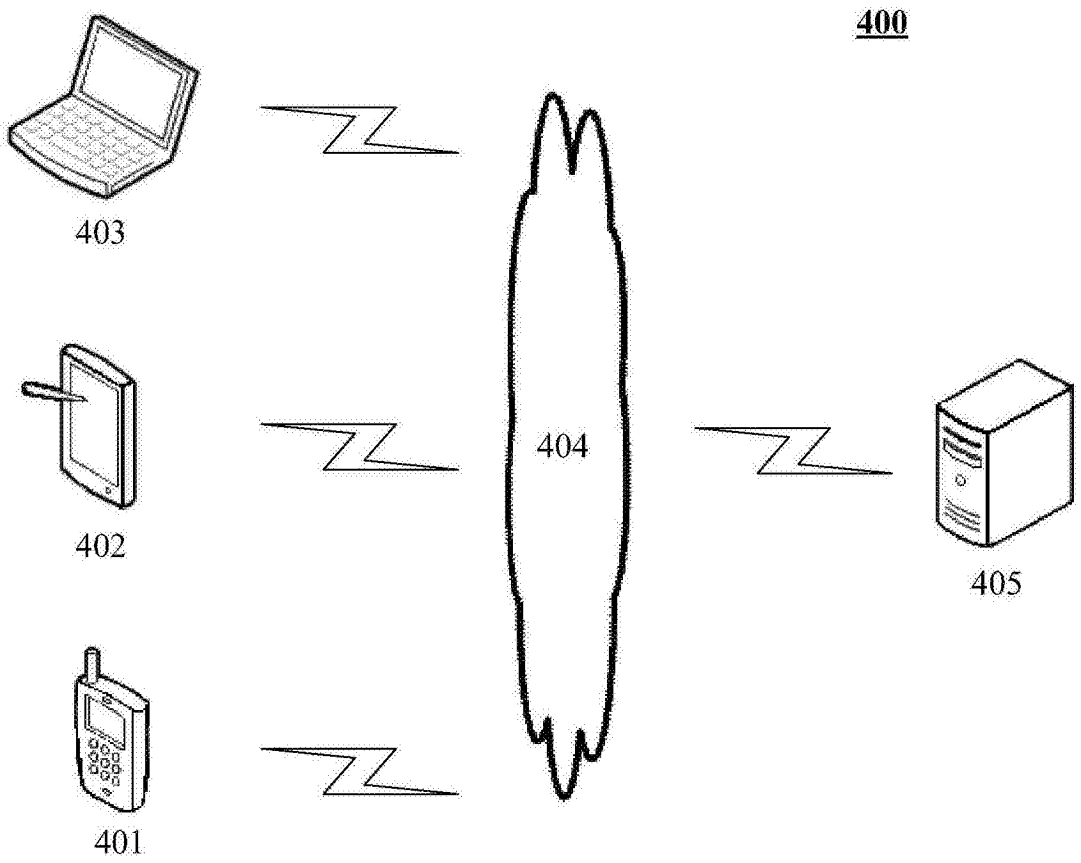

400
403
404
402
405
401

图4

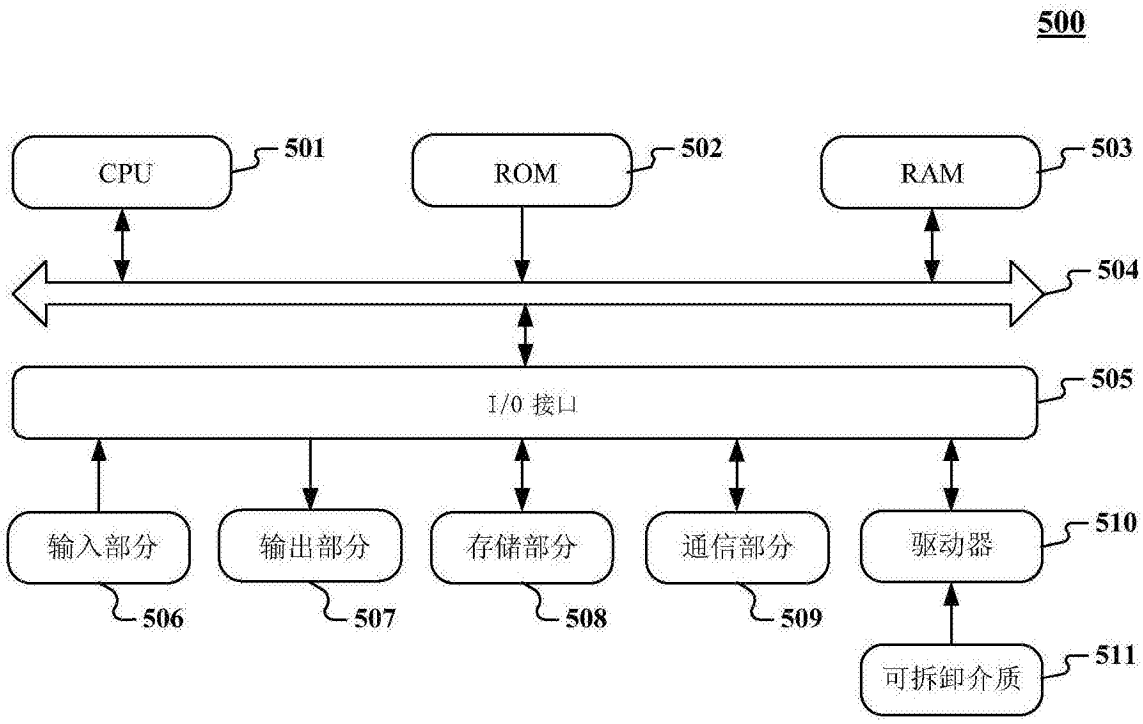

500
CPU
501
ROM
502
RAM
503
504
I/O 接口
505
输入部分
506
输出部分
507
存储部分
508
通信部分
509
驱动器
510
可拆卸介质
511

图5