(12) 按照专利合作条约所公布的国际申请

(19) 世界知识产权组织
国 际 局

(43) 国际公布日
2020 年 7 月 2 日 (02.07.2020)

WIPO | PCT

(10) 国际公布号
WO 2020/133069 A1

(51) 国际专利分类号:
G06Q 20/08 (2012.01)

(21) 国际申请号: PCT/CN2018/124368

(22) 国际申请日: 2018 年 12 月 27 日 (27.12.2018)

(25) 申请语言: 中文

(26) 公布语言: 中文

(71) 申请人: 合肥达朴汇联科技有限公司 (**HEFEI DAPPWORKS TECHNOLOGY CO., LTD.**) [CN/CN]; 中国安徽省合肥市高新区望江西路 2800 号创新产业园二期 J2 楼 C 座10层, Anhui 230031 (CN)。

(72) 发明人: 张焱 (**ZHANG, Yan**); 中国安徽省合肥市高新区望江西路 2800 号创新产业园二期 J2 楼 C 座 10 层, Anhui 230031 (CN)。 施逸 (**SHI, Yi**); 中国安徽省合肥市高新区望江西路 2800 号创新产业园二期J2楼C座10层, Anhui 230031 (CN)。 王星棋 (**WANG, Antonio**); 中国安徽省合肥市高新区望江西路2800号创新产业园二期J2楼C座10层, Anhui 230031 (CN)。

(74) 代理人: 中科专利商标代理有限责任公司 (**CHINA SCIENCE PATENT & TRADEMARK AGENT LTD.**); 中国北京市海淀区西三环北路87号4-1105室, Beijing 100089 (CN)。

(81) 指定国 (除另有指明，要求每一种可提供的国家保护): AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DJ, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, JO, JP, KE, KG, KH, KN, KP, KR, KW, KZ, LA, LC, LK, LR, LS, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SA, SC, SD, SE, SG, SK, SL,

(54) **Title:** DATA PROCESSING METHOD AND APPARATUS FOR BLOCK CHAIN

(54) 发明名称: 区块链的数据处理方法和装置

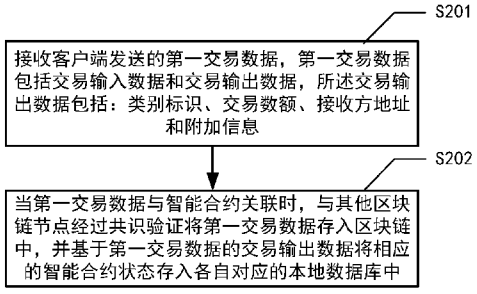

图 2

S201 Receive first transaction data sent by a client, the first transaction data comprising transaction input data and transaction output data, the transaction output data comprising: a category identifier, transaction amount, a recipient address and additional information

S202 When the first transaction data is associated with a smart contract, store the first transaction data into a block chain after consensus verification with other block chain nodes, and store, on the basis of the transaction output data of the first transaction data, the corresponding smart contract status into respective corresponding local databases

(57) **Abstract:** A data processing method for a block chain, adapted to an unspent transaction output system of a block chain, and applied to block chain nodes. The method comprises: receiving first transaction data sent by a client, the first transaction data comprising transaction input data and transaction output data, the transaction output data comprising: a category identifier, transaction amount, a recipient address and additional information (S201); and when the first transaction data is associated with a smart contract, storing the first transaction data into a block chain after consensus verification with other block chain nodes, and storing, on the basis of the transaction output data, the corresponding smart contract status into respective corresponding local databases (S202). Further provided are a data processing apparatus for a block chain, a computer device and a computer readable storage medium.

(57) 摘要: 一种区块链的数据处理方法，适配于区块链的未花费交易输出体系，应用于区块链节点，包括：接收客户端发送的第一交易数据，第一交易数据包括交易输入数据和交易输出数据；所述交易输出数据包括：类别标识、交易数额、接收方地址和附加信息（S201）；当第一交易数据与智能合约关联时，与其他区块链节点经过共识验证将第一交易数据存入区块链中，并基于所述交易输出数据将相应的智能合约状态存入各自对应的本地数据库中（S202）。还提供了一种区块链的数据处理装置、计算机设备和计算机可读存储介质。

WO 2020/133069 A1

[见续页]

SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW。

(84) **指定国**(除另有指明，要求每一种可提供的地区保护)：ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, ST, SZ, TZ, UG, ZM, ZW), 欧亚 (AM, AZ, BY, KG, KZ, RU, TJ, TM), 欧洲 (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, KM, ML, MR, NE, SN, TD, TG)。

本国际公布:

— 包括国际检索报告(条约第21条(3))。

区块链的数据处理方法和装置

技术领域

本公开涉及互联网技术领域，更具体地，涉及一种区块链的数据处理方法和装置。

背景技术

区块链是一种分布式记账技术。由于区块链具有去中心化，不可篡改，代码本身保证信任、无需第三方信任担保的优点而得到广泛重视。而区块链技术中的智能合约更是将区块链的代码信任优点发挥的淋漓尽致。智能合约是将合同条款通过使用计算机语言编写并保存于区块链中，当一个预先设定的条件被触发时，智能合约自动执行相应的合同条款。

UTXO 全称 Unspent Transaction Output，即未花费交易输出，它是由中本聪创造。 在比特币的账本体系中，并没有账户或者余额，它有的只是 UTXO。用户余额的计算方法是把该用户所拥有的 UTXO 全部加起来的总额。比特币的 UTXO 体系比当前电子银行系统中的账户体系更贴近我们日常生活中的现金，一个个 UTXO 如同钱包中的一张张钞票。由于 UTXO 体系不存在账户，该体系比账户体系具备更加地去中心化，更符合现实中现金实际使用方式的优点。

然而，由于当前的智能合约系统，如以太坊和 eos，都是基于账户体系创建，无法与 UTXO 体系兼容。并且由于 UTXO 体系是一种无状态模型，无法将智能合约运行中产生的状态进行存储。

发明内容

有鉴于此，本公开提供了一种改进的区块链的数据处理方法和装置。

本公开的一个方面提供了一种区块链的数据处理方法，适配于区块链的未花费交易输出体系，该方法应用于区块链节点，包括：接收客户端发送的第一交易数据，第一交易数据包括交易输入数据和交易输出数据。第一交易数据的交易输出数据包括：类别标识、交易数额、接收方地址和附加信息，其中，所述类别标识用于表征第一交易数据是否与智能合约关联，所述附加信息用于在第一交易数据与智能合约关联时表征该智能合约运行所需的信息。当第一交易数据与智能合约关联时，本区块链节点与其他区块链节点经过共识验证将第一

交易数据存入区块链中，并基于第一交易数据的交易输出数据将相应的智能合约状态存入各自对应的本地数据库中。

根据本公开的实施例，当第一交易数据为发布智能合约的交易数据时，所述类别标识表征第一交易数据与智能合约关联，所述交易数额为第一数值，所述第一数值大于零，所述接收方地址为所述智能合约的地址，所述附加信息包括所述智能合约的代码。上述与其他区块链节点经过共识验证将所述第一交易数据存入区块链中，并基于第一交易数据的交易输出数据将相应的智能合约状态存入各自对应的本地数据库中包括：将第一交易数据打包至新的区块并发送至其他区块链节点，使得各区块链节点经过共识验证将所述新的区块加入区块链时基于所述附加信息初始化所述智能合约，将初始化后的状态存入各自对应的本地数据库中。

根据本公开的实施例，上述方法还包括：在基于所述附加信息初始化所述智能合约之后，构造初始找零数据，所述初始找零数据的交易输入数据为所述第一交易数据的交易输入数据，所述初始找零数据的交易输出数据的接收方地址为所述客户端的地址，所述初始找零数据的交易输出数据的交易数额为初始找零数值，所述初始找零数值等于所述交易输入数据的实际交易数额减去所述第一数值后的余额。将所述初始找零数据发送至其他区块链节点，使得各区块链节点经过共识验证将所述初始找零数据存入区块链中。

根据本公开的实施例，当第一交易数据为触发智能合约的交易数据时，所述类别标识表征第一交易数据与智能合约关联，所述交易数额为第二数值，所述接收方地址为所述智能合约的地址，所述附加信息包括所述智能合约的执行指令；上述与其他区块链节点经过共识验证将所述第一交易数据存入区块链中，并基于所述交易输出数据将相应的智能合约状态存入各自对应的本地数据库中包括：将所述第一交易数据打包至新的区块并发送至其他区块链节点，使得各区块链节点经过共识验证将所述新的区块加入区块链时基于所述附加信息运行所述智能合约，将运行后的状态存入各自对应的本地数据库中。

根据本公开的实施例，上述方法还包括：在基于所述附加信息运行所述智能合约之后，构造第二交易数据，第二交易数据包括交易输入数据和交易输出数据，第二交易数据的交易输入数据为第一交易数据的交易输出数据，第二交易数据包括第一交易输出数据，第二交易数据的第一交易输出数据的接收方地址为本节点的地址，第二交易数据的第一交易输出数据的交易数额为第三数值。

将第二交易数据发送至其他区块链节点，使得各区块链节点经过共识验证将第二交易数据存入区块链中。

根据本公开的实施例，第二交易数据还包括第二交易输出数据，第二交易数据的第二交易输出数据的接收方地址为运行所述智能合约后的结果所指示的地址，第二交易数据的第二交易输出数据的交易数额为第四数值，所述第四数值表征运行所述智能合约后的结果所指示的数额。

根据本公开的实施例，第二交易数据还包括第三交易输出数据，第二交易数据的第三交易输出数据的接收方地址为客户端的地址，第二交易数据的第三交易输出数据的交易数额为第五数值，该第五数值等于第二数值减去第三数值和第四数值后的余额。

根据本公开的实施例，上述基于所述附加信息初始化所述智能合约包括：基于所述智能合约的代码使用虚拟机初始化所述智能合约；并且/或者，所述基于所述附加信息运行所述智能合约包括：基于所述智能合约的执行指令使用虚拟机运行所述智能合约。

根据本公开的实施例，所述类别标识和所述接收方地址在所述交易输出数据的数据结构中占据同一区域；或者，所述类别标识和所述接收方地址在所述交易输出数据的数据结构中占据不同的区域。

本公开的另一个方面提供了一种区块链的数据处理装置，适配于区块链的未花费交易输出体系，所述装置应用于区块链节点，包括：接收模块和管理模块。接收模块用于接收客户端发送的第一交易数据，所述第一交易数据包括交易输入数据和交易输出数据。第一交易数据的交易输出数据包括：类别标识、交易数额、接收方地址和附加信息，其中，所述类别标识用于表征所述第一交易数据是否与智能合约关联，所述附加信息用于在所述第一交易数据与智能合约关联时表征所述智能合约运行所需的信息。管理模块用于当所述第一交易数据与智能合约关联时，与其他区块链节点经过共识验证将所述第一交易数据存入区块链中，并基于所述交易输出数据将相应的智能合约状态存入各自对应的本地数据库中。

根据本公开的实施例，当所述第一交易数据为发布智能合约的交易数据时，所述类别标识表征第一交易数据与智能合约关联，所述交易数额为第一数值，所述第一数值大于零，所述接收方地址为所述智能合约的地址，所述附加信息包括所述智能合约的代码。管理模块与其他区块链节点经过共识验证将所述第

一交易数据存入区块链中，并基于所述交易输出数据将相应的智能合约状态存入各自对应的本地数据库中包括：管理模块用于将所述第一交易数据打包至新的区块并发送至其他区块链节点，使得各区块链节点经过共识验证将所述新的区块加入区块链时基于所述附加信息初始化所述智能合约，将初始化后的状态存入各自对应的本地数据库中。

根据本公开的实施例，上述装置还包括初始找零模块，用于在基于所述附加信息初始化所述智能合约之后，构造初始找零数据，所述初始找零数据的交易输入数据为所述第一交易数据的交易输入数据，所述初始找零数据的交易输出数据的接收方地址为所述客户端的地址，所述初始找零数据的交易输出数据的交易数额为初始找零数值，所述初始找零数值等于所述交易输入数据的实际交易数额减去所述第一数值后的余额；将所述初始找零数据发送至其他区块链节点，使得各区块链节点经过共识验证将所述初始找零数据存入区块链中。

根据本公开的实施例，当所述第一交易数据为触发智能合约的交易数据时，所述类别标识表征第一交易数据与智能合约关联，所述交易数额为第二数值，所述接收方地址为所述智能合约的地址，所述附加信息包括所述智能合约的执行指令。管理模块与其他区块链节点经过共识验证将所述第一交易数据存入区块链中，并基于所述交易输出数据将相应的智能合约状态存入各自对应的本地数据库中包括：管理模块用于将所述第一交易数据打包至新的区块并发送至其他区块链节点，使得各区块链节点经过共识验证将所述新的区块加入区块链时基于所述附加信息运行所述智能合约，将运行后的状态存入各自对应的本地数据库中。

根据本公开的实施例，上述装置还包括辅助管理模块，用于在基于所述附加信息运行所述智能合约之后，构造第二交易数据，所述第二交易数据包括交易输入数据和交易输出数据，所述第二交易数据的交易输入数据为所述第一交易数据的交易输出数据，所述第二交易数据包括第一交易输出数据，第二交易数据的第一交易输出数据的接收方地址为本节点的地址，第二交易数据的第一交易输出数据的交易数额为第三数值；将所述第二交易数据发送至其他区块链节点，使得各区块链节点经过共识验证将所述第二交易数据存入区块链中。

根据本公开的实施例，所述第二交易数据还包括第二交易输出数据，第二交易数据的第二交易输出数据的接收方地址为运行所述智能合约后的结果所指

示的地址，第二交易数据的第二交易输出数据的交易数额为第四数值，所述第四数值表征运行所述智能合约后的结果所指示的数额。

根据本公开的实施例，第二交易数据还包括第三交易输出数据，第二交易数据的第三交易输出数据的接收方地址为客户端的地址，第二交易数据的第三交易输出数据的交易数额为第五数值，所述第五数值等于第二数值减去第三数值和第四数值后的余额。

根据本公开的实施例，管理模块基于所述附加信息初始化所述智能合约包括：管理模块用于基于所述智能合约的代码使用虚拟机初始化所述智能合约；并且/或者，管理模块基于所述附加信息运行所述智能合约包括：管理模块用于基于所述智能合约的执行指令使用虚拟机运行所述智能合约。

根据本公开的实施例，所述类别标识和所述接收方地址在所述交易输出数据的数据结构中占据同一区域；或者，所述类别标识和所述接收方地址在所述交易输出数据的数据结构中占据不同的区域。

本公开的另一个方面提供了一种计算机设备，包括存储器、处理器及存储在存储器上并可在处理器上运行的计算机程序，所述处理器执行所述程序时，实现如上所述的方法。

本公开的另一个方面提供了一种计算机可读存储介质，其上存储有可执行指令，该指令被处理器执行时使处理器执行如上所述的方法。

本公开的另一方面提供了一种计算机程序，所述计算机程序包括计算机可执行指令，所述指令在被执行时用于实现如上所述的方法。

根据本公开的实施例，可以至少部分地解决/减轻/抑制/甚至避免现有 UTXO 体系无法支持智能合约的问题，通过改进 UTXO 体系的数据结构，在第一交易数据的交易输出数据中增加了用于表征第一交易数据是否与智能合约关联的类别标识以及用于表征该与第一交易数据关联的智能合约运行所需的信息的附加信息，使之能够适应与智能合约相关的交易数据，且在各区块链节点将第一交易数据存入区块链的同时在本地记录相应的智能合约的状态，能够支持各种复杂程度的智能合约。

附图说明

通过以下参照附图对本公开实施例的描述，本公开的上述以及其他目的、特征和优点将更为清楚，在附图中：

图 1 示意性示出了根据本公开实施例的可以应用区块链的数据处理方法和装置的示例性系统架构；

图 2 示意性示出了根据本公开的实施例的区块链的数据处理方法的流程图；

图 3A 示意性示出了根据本公开的实施例的第一交易数据的交易输出数据的数据结构；

图 3B 示意性示出了根据本公开的实施例的第二交易数据的交易输入数据和交易输出数据的数据结构；

图 4 示意性示出了根据本公开的实施例的区块链的数据处理装置的框图；

图 5 示意性示出了根据本公开的另一实施例的区块链的数据处理装置的框图；以及

图 6 示意性示出了根据本公开实施例的适于实现区块链的数据处理方法的计算机设备的框图。

具体实施方式

以下，将参照附图来描述本公开的实施例。但是应该理解，这些描述只是示例性的，而并非要限制本公开的范围。在下面的详细描述中，为便于解释，阐述了许多具体的细节以提供对本公开实施例的全面理解。然而，明显地，一个或多个实施例在没有这些具体细节的情况下也可以被实施。此外，在以下说明中，省略了对公知结构和技术的描述，以避免不必要地混淆本公开的概念。

在此使用的术语仅仅是为了描述具体实施例，而并非意在限制本公开。在此使用的术语“包括”、“包含”等表明了所述特征、步骤、操作和/或部件的存在，但是并不排除存在或添加一个或多个其他特征、步骤、操作或部件。

在此使用的所有术语（包括技术和科学术语）具有本领域技术人员通常所理解的含义，除非另外定义。应注意，这里使用的术语应解释为具有与本说明书的上下文相一致的含义，而不应以理想化或过于刻板的方式来解释。

在使用类似于“A、B 和 C 等中至少一个”这样的表述的情况下，一般来说应该按照本领域技术人员通常理解该表述的含义来予以解释（例如，“具有 A、B 和 C 中至少一个的系统”应包括但不限于单独具有 A、单独具有 B、单独具有 C、具有 A 和 B、具有 A 和 C、具有 B 和 C、和/或具有 A、B、C 的系统等）。在使用类似于“A、B 或 C 等中至少一个”这样的表述的情况下，一般来说应该按照本领域技术人员通常理解该表述的含义来予以解释（例如，“具有 A、B

或 C 中至少一个的系统”应包括但不限于单独具有 A、单独具有 B、单独具有 C、具有 A 和 B、具有 A 和 C、具有 B 和 C、和/或具有 A、B、C 的系统等）。本领域技术人员还应理解，实质上任意表示两个或更多可选项目的转折连词和/或短语，无论是在说明书、权利要求书还是附图中，都应被理解为给出了包括这些项目之一、这些项目任一方、或两个项目的可能性。例如，短语“A 或 B”应当被理解为包括“A”或“B”、或“A 和 B”的可能性。

本公开的实施例提供了一种区块链的数据处理方法和装置。该方法适配于区块链的未花费交易输出（UTXO, Unspent Transaction Output）体系，该方法应用于区块链节点，包括交易数据接收过程和交易数据管理过程。在交易数据接收过程中，接收第一交易数据，第一交易数据包括交易输入数据和交易输出数据。交易输出数据除现有的交易数额和接收方地址之外，还包括用于表征所述第一交易数据是否与智能合约关联的类别标识以及用于表征智能合约运行所需的信息的附加信息。然后进入交易数据管理过程，与其他区块链节点经过共识验证将所述第一交易数据存入区块链中并在各自本地记录相应的智能合约状态。

图 1 示意性示出了根据本公开实施例的可以应用区块链的数据处理方法和装置的示例性系统架构 100。需要注意的是，图 1 所示仅为可以应用本公开实施例的系统架构的示例，以帮助本领域技术人员理解本公开的技术内容，但并不意味着本公开实施例不可以用于其他设备、系统、环境或场景。

如图 1 所示，根据该实施例的系统架构 100 可以包括多个电子设备（101~107）。电子设备（101~107）可以是个人电脑（personal computer，PC）、网络服务器、数据库服务器等。电子设备（101~107）中的每一个电子设备可以具有相同或不同的计算能力。

作为一种实施方式，多个电子设备之间可以相互通信，构成区块链网络，每个电子设备作为该区块链网络中的一个区块链节点，各区块链节点维护相同的区块链数据库（下文中统称为“区块链”）。此外，在系统架构 100 中，各区块链节点分别可以与不同的服务提供方和/或客户端的计算设备（如服务器/服务器集群、终端设备等）通信，即分别作为各服务提供方和/或客户端对应的区块链节点，每个服务提供方和/或客户端可以通过相应的区块链节点在区块链中进行数据的读写等操作。

应该理解，图 1 中的电子设备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电子设备。

本公开实施例提供的区块链的数据处理方法可以运行于图 1 所示的电子设备中。

图 2 示意性示出了根据本公开的实施例的区块链的数据处理方法的流程图。

如图 2 所示，该方法适配于区块链的未花费交易输出（UTXO）体系，该方法由区块链节点执行，从区块链节点侧说明本公开所提供的区块链的数据处理过程。

该方法包括在操作 S201，接收客户端发送的第一交易数据，所述第一交易数据包括交易输入数据和交易输出数据，所述交易输出数据包括：类别标识、交易数额、接收方地址和附加信息。

需要说明的是，UTXO 体系是区块链网络的一种记账模式，该记账模式的特点是：每笔交易都会花费先前交易的产出，并产生新的产出，这些产出可能会在未来通过交易消耗，所有未花费的交易都保存在每个完全同步的节点中，用户的钱包跟踪与用户拥有的所有地址相关联的未花费的交易的列表，并且钱包的余额被计算为这些未花费的交易的总和。

本操作中，第一交易数据采用 UTXO 体系的数据结构，包括交易输入数据和交易输出数据，交易输入数据中包括客户端实际发出的交易数额，而交易输出数据中除了现有 UTXO 体系的数据结构中必需的交易数额和接收方地址之外，还包括类别标识和附加信息，其中，类别标识用于表征第一交易数据是否与智能合约关联，附加信息用于在第一交易数据与智能合约关联时表征该与第一交易数据关联的智能合约运行所需的信息。

然后，在操作 S202，当第一交易数据与智能合约关联时，与其他区块链节点经过共识验证将第一交易数据存入区块链中，并基于第一交易数据的交易输出数据将相应的智能合约状态存入各自对应的本地数据库中。

本操作中，在第一交易数据的交易输出数据中的类别标识表明第一交易数据与智能合约相关联时，各区块链节点一方面经过共识验证将第一交易数据存入区块链，另一方面还基于第一交易数据的交易输出数据中的附加信息将与第一交易数据相关联的的智能合约的相应状态各自保存于本地。

可见，图 2 所示的方法改进了 UTXO 体系的数据结构，在第一交易数据的交易输出数据中增加了用于表征第一交易数据是否与智能合约关联的类别标识以及用于表征该与第一交易数据关联的智能合约运行所需的信息的附加信息，使之能够适应与智能合约相关的交易数据，且在各区块链节点将第一交易数据

存入区块链的同时在本地记录相应的智能合约的状态，能够支持各种复杂程度的智能合约，解决了现有 UTXO 体系无法支持智能合约的问题。

在本公开的一个实施例中，在改进了 UTXO 体系的数据结构中，类别标识和所述接收方地址在所述交易输出数据的数据结构中占据同一区域；或者，所述类别标识和所述接收方地址在所述交易输出数据的数据结构中占据不同的区域。可以根据需要进行配置，在此不做限定。

在本公开的一个实施例中，第一交易数据为发布智能合约的交易数据，此时，第一交易数据的交易输出数据中的类别标识表征第一交易数据与智能合约关联，第一交易数据的交易输出数据中的交易数额为第一数值，第一数值为大于零的数值，第一交易数据的交易输出数据中的接收方地址为所述智能合约的地址，第一交易数据的交易输出数据中的附加信息包括与第一交易数据相关联的智能合约的代码，也就是想要发布的智能合约的代码。

则上述操作 S202 与其他区块链节点经过共识验证将第一交易数据存入区块链中，并基于第一交易数据的交易输出数据将相应的智能合约状态存入各自对应的本地数据库中包括：当本节点是造块者节点时，将第一交易数据打包至新的区块并发送至其他区块链节点，使得各区块链节点经过共识验证将该新的区块加入区块链时基于第一交易数据的交易输出数据中的附加信息初始化智能合约，将初始化后的状态存入各自对应的本地数据库中；当本节点不是造块者节点时，接收造块者节点发送的新的区块，该新的区块中打包有第一交易数据，与其他各区块链节点经过共识验证将该新的区块加入区块链时基于第一交易数据的交易输出数据中的附加信息初始化智能合约，将初始化后的状态存入各自对应的本地数据库中。

依据本实施例，客户端想要发布智能合约时，构造包含交易输出数据的第一交易数据，在交易输出数据的类别标识中记录第一交易数据与智能合约关联，将智能合约作为交易接收方，在交易输出数据的接收方地址中记录该智能合约的地址，在交易输出数据的附加信息中记录该智能合约的代码，在交易输出数据的交易数额中记录大于零的第一数值。客户端将第一交易数据发送至区块链节点，造块者节点在打包该第一交易数据到新的区块中时，初始化相应智能合约并将初始化后的状态保存在本地数据库中，其他全节点在同步区块链时，当收到造块者节点创建的该新的区块时，在区块验证阶段也会初始化该智能合约并将初始化后的状态保存在各自的本地数据库中。该过程一方面将智能合约的

代码部署至区块链中，利用区块链的不可篡改性保证后续智能合约可以按照预先约定的规则准确无误地执行操作，另一方面将智能合约初始化后的状态记录在区块链节点本地，既可以记录智能合约的变化状态又无需像现有的账户/余额体系那样将智能合约状态记录在区块链上，极大地节省了区块链传输带宽和存储空间。

其中可选地，上述各区块链节点基于附加信息初始化所述智能合约包括：基于所述智能合约的代码使用虚拟机初始化所述智能合约。

进一步地，作为一个可选的实施例，在客户端发出第一交易数据后，由于UTXO 体系中交易数据的输入是账户中未花费的之前的交易输出，如同钱包中的一张张钞票，其面额是确定的，不能随意更改，因此很容易出现交易输入与交易输出的交易数额不相同的情形，如果第一交易数据的交易输出数据中的交易数额与交易输入数据中的实际交易数据不相符时，需要构造初始找零数据进行找零。具体地，图 2 所示的方法还包括：在基于所述附加信息初始化所述智能合约之后，构造初始找零数据，所述初始找零数据的交易输入数据为第一交易数据的交易输入数据，第一交易数据的交易输入数据中包括客户端关于第一交易数据实际发出的交易数额，称之为实际交易数额。所述初始找零数据的交易输出数据的接收方地址为发出第一交易数据的客户端的地址，所述初始找零数据的交易输出数据的交易数额为初始找零数值，该初始找零数值等于该客户端发出的实际交易数额减去所述第一数值后的余额。本实施例实现了在发布智能合约时交易数额的多退少补，然后将所述初始找零数据发送至其他区块链节点，使得各区块链节点经过共识验证将所述初始找零数据存入区块链中，以在区块链中记录初始找零这一事件。

在本公开的另一个实施例中，在智能合约已经按照上述实施例在区块链中部署之后，还可以进行智能合约的触发执行过程，此时，第一交易数据为触发智能合约的交易数据，第一交易数据的交易输出数据中的类别标识表征第一交易数据与智能合约关联，第一交易数据的交易输出数据中的交易数额为第二数值，第一交易数据的交易输出数据中的接收方地址为所述智能合约的地址，第一交易数据的交易输出数据中的附加信息包括智能合约的执行指令。

则上述上述操作 S202 与其他区块链节点经过共识验证将所述第一交易数据存入区块链中，并基于所述交易输出数据将相应的智能合约状态存入各自对应的本地数据库中包括：当本节点是造块者节点时，将所述第一交易数据打包至

新的区块并发送至其他区块链节点，使得各区块链节点经过共识验证将所述新的区块加入区块链时基于所述附加信息运行所述智能合约，将运行后的状态存入各自对应的本地数据库中；当本节点不是造块者节点时，接收造块者节点发送的新的区块，该新的区块中打包有第一交易数据，与其他各区块链节点经过共识验证将所述新的区块加入区块链时基于所述附加信息运行所述智能合约，将运行后的状态存入各自对应的本地数据库中。

依据本实施例，客户端想要向区块链中部署的智能合约发布指令时，构造包含交易输出数据的第一交易数据，在交易输出数据的类别标识中记录第一交易数据与智能合约关联，将智能合约作为交易接收方，在交易输出数据的接收方地址中记录该智能合约的地址，在交易输出数据的附加信息中记录该智能合约的执行指令，在交易输出数据的交易数额中记录智能合约运行所需的第二数值。客户端将第一交易数据发送至区块链节点，造块者节点在打包该第一交易数据到新的区块中时，运行该智能合约并将运行后的状态保存在本地数据库中，其他全节点在同步区块链时，当收到造块者节点创建的该新的区块时，在区块验证阶段也会运行该智能合约并将运行后的状态保存在各自的本地数据库中。该过程将智能合约执行各任务后的运行状态记录在区块链节点本地，能够支持图灵完备的智能合约，且无需像现有的账户/余额体系那样将智能合约状态记录在区块链上，极大地节省了区块链传输带宽和存储空间。

其中可选地，上述各区块链节点基于所述附加信息运行所述智能合约包括：基于所述智能合约的执行指令使用虚拟机运行所述智能合约。

进一步地，作为一个可选的实施例，在客户端发出第一交易数据后，由于 UTXO 体系中交易数据的输入是账户中未花费的之前的交易输出，如同钱包中的一张张钞票，其面额是确定的，不能随意更改，因此很容易出现交易输入与交易输出的交易数额不相同的情形，如果第一交易数据的交易输出数据中的交易数额与交易输入数据中的实际交易数据不相符时，需要构造初始找零数据进行找零。具体地，图 2 所示的方法还包括：在基于所述附加信息运行所述智能合约之后，构造初始找零数据，所述初始找零数据的交易输入数据为第一交易数据的交易输入数据，第一交易数据的交易输入数据中包括客户端关于第一交易数据实际发出的交易数额，称之为实际交易数额。所述初始找零数据的交易输出数据的接收方地址为发出第一交易数据的客户端的地址，所述初始找零数据的交易输出数据的交易数额为初始找零数值，该初始找零数值等于该客户端

发出的实际交易数额减去所述第二数值后的余额。本实施例实现了在触发执行智能合约时交易数额的多退少补，然后将所述初始找零数据发送至其他区块链节点，使得各区块链节点经过共识验证将所述初始找零数据存入区块链中，以在区块链中记录初始找零这一事件。

以及，进一步地，作为一个可选的实施例，图 2 所示的方法还包括：在基于所述附加信息运行所述智能合约之后，构造第二交易数据，所述第二交易数据包括交易输入数据和交易输出数据，所述第二交易数据的交易输入数据为所述第一交易数据的交易输出数据，所述第二交易数据的交易输出数据包括第一交易输出数据，当本节点为造块者节点时，所述第一交易输出数据的接收方地址为本节点的地址，当本节点不是造块者节点时，所述第一交易输出数据的接收方地址为造块者节点的地址，所述第一交易输出数据的交易数额为第三数值。将所述第二交易数据发送至其他区块链节点，使得各区块链节点经过共识验证将所述第二交易数据存入区块链中。

可以看出，第二交易数据中的第一交易输出数据表示向运行智能合约的造块者节点发放的手续费，以对造块者节点进行激励，保证基于 UTXO 体系的交易管理顺利有序进行。

此外，在本公开的一个实施例中，除表示给造块者节点的手续费的输出数据之外，上述第二交易数据还包括第二交易输出数据，该第二交易输出数据的接收方地址为运行所述智能合约后的结果所指示的地址，该第二交易输出数据的交易数额为第四数值，所述第四数值表征运行所述智能合约后的结果所指示的数额。

可以看出，第二交易数据中的第二交易输出数据表示按照智能合约指令运行智能合约后的结果所指示的地址，例如可以是将一部分交易数额存储于智能合约中，或者可以是将一部分交易数额发给指令执行结果所指示的其他客户端的地址等等，根据智能合约预先约定的内容而定，在此不做限定，以满足发送第一交易数据的客户端运行智能合约的需求。

此外，在本公开的另一个实施例中，除表示给造块者节点的手续费以及智能合约正常运行所需的费用之外，上述第二交易数据还包括第三交易输出数据，所述第三交易输出数据的接收方地址为客户端的地址，所述第三交易输出数据的交易数额为第五数值，所述第五数值等于第二数值减去第三数值和第四数值后的余额。

可以看出，第二交易数据中的第三交易输出数据表示在运行智能合约后生成对应于向客户端找零的交易输出，在客户端发出的第一交易数据的交易数额超过手续费以及运行结果所需的费用后向客户端找零，确保交易公平进行。

下面参考图 3A~图 3B，结合具体实施例对图 2 所示的方法做进一步说明。

图 3A 示意性示出了根据本公开的实施例的第一交易数据的交易输出数据的数据结构。

如图 3A 所示，第一交易数据的交易输出数据采用了改进的 UTXO 体系的数据结构，左边为现有的以 UTXO 体系的数据结构表示的交易输出数据（Txout'），右边为本公开提供的第一交易数据的交易输出数据（Txout）。

可以看到，在现有的比特币区块链的交易输出数据 Txout'的数据结构中，publicKeyHash 项用于指示接收方地址，value 项用于指示交易数额。而在本公开改进的第一交易数据的交易输出数据 Txout 的数据结构中，修改原有的 publicKeyHash 的数据格式，当第一交易数据与智能合约无关时，在该数据前加前缀 n 以表示此为普通地址，当第一交易数据与智能合约关联时，在该数据前加前缀 s 以表示此为智能合约地址，该前缀 n/s 即为表示第一交易数据与智能合约是否关联的类别标识，并且在该 Txout 数据结构中，增加一个额外的 smart contract / operation 项，该项表示附加信息，用于存储智能合约代码或是客户端发出的智能合约执行指令。

基于上述改进的 Txout 数据结构，本公开实施例中的第一交易数据可以是支持用于存储与识别智能合约的交易数据。

当客户端发布智能合约 A 时，构造一个第一交易数据，该第一交易数据包括交易输入数据和交易输出数据，交易输入数据包括客户端实际发出的交易数额，交易输出数据 Txout 包括：交易数额（Value）项为 0.0001， 接收方地址（n/s+PubKeyHash）项使用 s 开头的字符串作为交易接收方，以表示此地址为智能合约地址，在附加信息（smart contract / operation）项中填入智能合约 A 的代码（smart contract）。

客户端将第一交易数据发送至区块链节点，造块者节点在打包该第一交易数据到区块中的同时，需使用虚拟机运行智能合约 A 并将初始化后的状态保存在自己的计算机数据库中。其余全节点在同步区块链时，当收到此区块时，在区块验证阶段也会运行智能合约 A 并将初始化后的状态保存在自己的计算机数据库中。

此外，如果第一交易数据的交易输入数据中的实际交易金额大于交易输入数据中的交易数额时，进一步构造生成初始找零数据，该输出找零数据的接收方地址为发出第一交易数据的客户端的地址，该输出找零数据的交易数额等于实际交易数额减去 0.0001 后得到的余额。

进一步地，当客户端向智能合约 A 发送执行指令时，构造一个第一交易数据，该第一交易数据包括交易输入数据和交易输出数据，交易输入数据包括客户端实际发出的交易数额，交易输出数据 Txout 包括：交易数额（Value）项为运行智能合约 A 所需交易数额，其中接收方地址（n/s+PubKeyHash）项填入所需执行的智能合约 A 的地址(s+PubKeyHash)，在附加信息（smart contract / operation）项中填入所需执行的指令（operation）。

客户端将第一交易数据发送至区块链节点，造块者节点在打包该交易到区块中时，使用相应的智能合约 A 运行执行指令并更新本地保存的智能合约 A 的状态。其余全节点在同步区块链时，当收到此区块时，在区块验证阶段也会运行智能合约指令并更新自己本地的智能合约 A 的状态。

此外，如果第一交易数据的交易输入数据中的实际交易金额大于交易输入数据中的交易数额时，进一步构造生成初始找零数据，该输出找零数据的接收方地址为发出第一交易数据的客户端的地址，该输出找零数据的交易数额等于实际交易数额减去交易数额（Value）项的数值后得到的余额。

图 3B 示意性示出了根据本公开的实施例的第二交易数据的交易输入数据和交易输出数据的数据结构。

如图 3B 所示，在基于所述附加信息运行所述智能合约之后，构造第二交易数据，第二交易数据包括交易输入数据和交易输出数据，第二交易数据的交易输入数据为如图 3A 中右边所示的第一交易数据的交易输出数据 Txout，第二交易数据的交易输出数据包括第一交易输出数据 Txout1、第二交易输出数据 Txout2 和第三交易输出数据 Txout3。

第一交易输出数据 Txout1 的接收方地址 n +PubKeyHash 为造块者节点的地址，交易数额 value1 表示向造块者节点发放的手续费。

第二交易输出数据 Txout2 的接收方地址 s +PubKeyHash 为智能合约 A 的地址，交易数额 value2 表示在智能合约中存储的交易数额。

第三交易输出数据 Txout3 的接收方地址 n +PubKeyHash 为客户端的地址，交易数额 value3 表示向客户端找零的数额，value3 = value – value1 – value2。

可以看到，在执行智能合约 A 后，造块者将 Txout 拆分为三个款项。第一个款项作为运行智能合约 A 所需收取的费用，从而归造块者所有。第二个款项为按智能合约执行指令所示，将款项存储于智能合约中，或是发给指令执行结果的地址。第三个款项为多余的金额，该金额将被退回给客户端。

基于上述分析可知，本公开实施例具有以下有益效果：第一，实现了在UTXO体系下图灵完备的智能合约功能；第二，无需将智能合约状态记录在区块链上，极大地节省了区块链传输带宽与存储空间。

图 4 示意性示出了根据本公开的实施例的区块链的数据处理装置的框图。

如图 4 所示，区块链的数据处理装置 400 适配于区块链的未花费交易输出体系，区块链的数据处理装置 400 应用于区块链节点，包括接收模块 410 和管理模块 420。

接收模块 410 用于接收客户端发送的第一交易数据，所述第一交易数据包括交易输入数据和交易输出数据。所述交易输出数据包括：类别标识、交易数额、接收方地址和附加信息，其中，所述类别标识用于表征所述第一交易数据是否与智能合约关联，所述附加信息用于在所述第一交易数据与智能合约关联时表征所述智能合约运行所需的信息。

管理模块 420 用于当所述第一交易数据与智能合约关联时，与其他区块链节点经过共识验证将所述第一交易数据存入区块链中，并基于所述交易输出数据将相应的智能合约状态存入各自对应的本地数据库中。

其中可选地，所述类别标识和所述接收方地址在所述交易输出数据的数据结构中占据同一区域；或者，所述类别标识和所述接收方地址在所述交易输出数据的数据结构中占据不同的区域。

在本公开的一个实施例中，当所述第一交易数据为发布智能合约的交易数据时，所述类别标识表征第一交易数据与智能合约关联，所述交易数额为第一数值，所述第一数值大于零，所述接收方地址为所述智能合约的地址，所述附加信息包括所述智能合约的代码。管理模块 420 与其他区块链节点经过共识验证将所述第一交易数据存入区块链中，并基于所述交易输出数据将相应的智能合约状态存入各自对应的本地数据库中包括：管理模块 420 用于将所述第一交易数据打包至新的区块并发送至其他区块链节点，使得各区块链节点经过共识验证将所述新的区块加入区块链时基于所述附加信息初始化所述智能合约，将初始化后的状态存入各自对应的本地数据库中。

在本公开的另一个实施例中，当所述第一交易数据为触发智能合约的交易数据时，所述类别标识表征第一交易数据与智能合约关联，所述交易数额为第二数值，所述接收方地址为所述智能合约的地址，所述附加信息包括所述智能合约的执行指令。管理模块 420 与其他区块链节点经过共识验证将所述第一交易数据存入区块链中，并基于所述交易输出数据将相应的智能合约状态存入各自对应的本地数据库中包括：管理模块 420 用于将所述第一交易数据打包至新的区块并发送至其他区块链节点，使得各区块链节点经过共识验证将所述新的区块加入区块链时基于所述附加信息运行所述智能合约，将运行后的状态存入各自对应的本地数据库中。

具体地，作为一个可选的实施例，管理模块 420 基于所述附加信息初始化所述智能合约包括：管理模块 420 用于基于所述智能合约的代码使用虚拟机初始化所述智能合约。并且/或者，管理模块 420 基于所述附加信息运行所述智能合约包括：管理模块 420 用于基于所述智能合约的执行指令使用虚拟机运行所述智能合约。

图 5 示意性示出了根据本公开的另一实施例的区块链的数据处理装置的框图。

如图 5 所示，区块链的数据处理装置 500 应用于区块链节点，包括接收模块 410、管理模块 420、初始找零模块 430、和辅助管理模块 440。

其中接收模块 410 和管理模块 420 在上文中已经说明，重复的部分不再赘述。

初始找零模块 430 用于在基于所述附加信息初始化所述智能合约和/或运行所述智能合约之后，构造初始找零数据，所述初始找零数据的交易输入数据为所述第一交易数据的交易输入数据，所述初始找零数据的交易输出数据的接收方地址为所述客户端的地址，所述初始找零数据的交易输出数据的交易数额为初始找零数值，所述初始找零数值等于所述交易输入数据的实际交易数额减去所述第一数值和/或所述第二数值后的余额；将所述初始找零数据发送至其他区块链节点，使得各区块链节点经过共识验证将所述初始找零数据存入区块链中。

辅助管理模块 440 用于在基于所述附加信息运行所述智能合约之后，构造第二交易数据，所述第二交易数据包括交易输入数据和交易输出数据，所述第二交易数据的交易输入数据为所述第一交易数据的交易输出数据，所述第二交易数据包括第一交易输出数据，所述第一交易输出数据的接收方地址为本节点

的地址，所述第一交易输出数据的交易数额为第三数值；将所述第二交易数据发送至其他区块链节点，使得各区块链节点经过共识验证将所述第二交易数据存入区块链中。

进一步地，作为一个可选的实施例，所述第二交易数据还包括第二交易输出数据，所述第二交易输出数据的接收方地址为运行所述智能合约后的结果所指示的地址，所述第二交易输出数据的交易数额为第四数值，所述第四数值表征运行所述智能合约后的结果所指示的数额。

进一步地，作为另一个可选的实施例，所述第二交易数据还包括第三交易输出数据，所述第二交易输出数据的接收方地址为客户端的地址，所述第二交易输出数据的交易数额为第五数值，所述第五数值等于第二数值减去第三数值和第四数值后的余额。

需要说明的是，装置部分实施例中各模块/单元/子单元等的实施方式、解决的技术问题、实现的功能、以及达到的技术效果分别与方法部分实施例中各对应的步骤的实施方式、解决的技术问题、实现的功能、以及达到的技术效果相同或类似，在此不再赘述。

根据本公开的实施例的模块、子模块、单元、子单元中的任意多个、或其中任意多个的至少部分功能可以在一个模块中实现。根据本公开实施例的模块、子模块、单元、子单元中的任意一个或多个可以被拆分成多个模块来实现。根据本公开实施例的模块、子模块、单元、子单元中的任意一个或多个可以至少被部分地实现为硬件电路，例如现场可编程门阵列（FPGA）、可编程逻辑阵列（PLA）、片上系统、基板上的系统、封装上的系统、专用集成电路（ASIC），或可以通过对电路进行集成或封装的任何其他的合理方式的硬件或固件来实现，或以软件、硬件以及固件三种实现方式中任意一种或以其中任意几种的适当组合来实现。或者，根据本公开实施例的模块、子模块、单元、子单元中的一个或多个可以至少被部分地实现为计算机程序模块，当该计算机程序模块被运行时，可以执行相应的功能。

例如，接收模块 410、管理模块 420、初始找零模块 430、和辅助管理模块 440 中的任意多个可以合并在一个模块中实现，或者其中的任意一个模块可以被拆分成多个模块。或者，这些模块中的一个或多个模块的至少部分功能可以与其他模块的至少部分功能相结合，并在一个模块中实现。根据本公开的实施例，接收模块 410、管理模块 420、初始找零模块 430、和辅助管理模块 440 中的至

少一个可以至少被部分地实现为硬件电路，例如现场可编程门阵列（FPGA）、可编程逻辑阵列（PLA）、片上系统、基板上的系统、封装上的系统、专用集成电路（ASIC），或可以通过对电路进行集成或封装的任何其他的合理方式等硬件或固件来实现，或以软件、硬件以及固件三种实现方式中任意一种或以其中任意几种的适当组合来实现。或者，接收模块 410、管理模块 420、初始找零模块 430、和辅助管理模块 440 中的至少一个可以至少被部分地实现为计算机程序模块，当该计算机程序模块被运行时，可以执行相应的功能。

图 6 示意性示出了根据本公开实施例的适于实现上文描述的方法的计算机设备的框图。图 6 示出的计算机设备仅仅是一个示例，不应对本公开实施例的功能和使用范围带来任何限制。

如图 6 所示，根据本公开实施例的计算机设备 600 包括处理器 601，其可以根据存储在只读存储器（ROM）602 中的程序或者从存储部分 608 加载到随机访问存储器（RAM）603 中的程序而执行各种适当的动作和处理。处理器 601 例如可以包括通用微处理器（例如 CPU）、指令集处理器和/或相关芯片组和/或专用微处理器（例如，专用集成电路（ASIC）），等等。处理器 601 还可以包括用于缓存用途的板载存储器。处理器 601 可以包括用于执行根据本公开实施例的方法流程的不同动作的单一处理单元或者是多个处理单元。

在 RAM 603 中，存储有设备 600 操作所需的各种程序和数据。处理器 601、ROM 602 以及 RAM 603 通过总线 604 彼此相连。处理器 601 通过执行 ROM 602 和/或 RAM 603 中的程序来执行根据本公开实施例的方法流程的各种操作。需要注意，所述程序也可以存储在除 ROM 602 和 RAM 603 以外的一个或多个存储器中。处理器 601 也可以通过执行存储在所述一个或多个存储器中的程序来执行根据本公开实施例的方法流程的各种操作。

根据本公开的实施例，设备 600 还可以包括输入/输出（I/O）接口 605，输入/输出（I/O）接口 605 也连接至总线 604。设备 600 还可以包括连接至 I/O 接口 605 的以下部件中的一项或多项：包括键盘、鼠标等的输入部分 606；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 607；包括硬盘等的存储部分 608；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 609。通信部分 609 经由诸如因特网的网络执行通信处理。驱动器 610 也根据需要连接至 I/O 接口 605。可拆卸介质 611，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 610 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 608。

根据本公开的实施例，根据本公开实施例的方法流程可以被实现为计算机软件程序。例如，本公开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 609 从网络上被下载和安装，和/或从可拆卸介质 611 被安装。在该计算机程序被处理器 601 执行时，执行本公开实施例的系统中限定的上述功能。根据本公开的实施例，上文描述的系统、设备、装置、模块、单元等可以通过计算机程序模块来实现。

本公开还提供了一种计算机可读存储介质，该计算机可读存储介质可以是上述实施例中描述的设备/装置/系统中所包含的；也可以是单独存在，而未装配入该设备/装置/系统中。上述计算机可读存储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执行时，实现根据本公开实施例的方法。

根据本公开的实施例，计算机可读存储介质可以是非易失性的计算机可读存储介质，例如可以包括但不限于：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）、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。在本公开中，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。例如，根据本公开的实施例，计算机可读存储介质可以包括上文描述的 ROM 602 和/或 RAM 603 和/或 ROM 602 和 RAM 603 以外的一个或多个存储器。

附图中的流程图和框图，图示了按照本公开各种实施例的系统、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。本领域技术人员可以理解，本公开的各个实

施例和/或权利要求中记载的特征可以进行多种组合和/或结合，即使这样的组合或结合没有明确记载于本公开中。特别地，在不脱离本公开精神和教导的情况下，本公开的各个实施例和/或权利要求中记载的特征可以进行多种组合和/或结合。所有这些组合和/或结合均落入本公开的范围。

以上对本公开的实施例进行了描述。但是，这些实施例仅仅是为了说明的目的，而并非为了限制本公开的范围。尽管在以上分别描述了各实施例，但是这并不意味着各个实施例中的措施不能有利地结合使用。本公开的范围由所附权利要求及其等同物限定。不脱离本公开的范围，本领域技术人员可以做出多种替代和修改，这些替代和修改都应落在本公开的范围之内。

权利要求

1. 一种区块链的数据处理方法，适配于区块链的未花费交易输出体系，所述方法应用于区块链节点，包括：

接收客户端发送的第一交易数据，所述第一交易数据包括交易输入数据和交易输出数据；

所述交易输出数据包括：类别标识、交易数额、接收方地址和附加信息，其中，所述类别标识用于表征所述第一交易数据是否与智能合约关联，所述附加信息用于在所述第一交易数据与智能合约关联时表征所述智能合约运行所需的信息；

当所述第一交易数据与智能合约关联时，与其他区块链节点经过共识验证将所述第一交易数据存入区块链中，并基于所述交易输出数据将相应的智能合约状态存入各自对应的本地数据库中。

2. 根据权利要求 1 所述的方法，其中：

当所述第一交易数据为发布智能合约的交易数据时，所述类别标识表征第一交易数据与智能合约关联，所述交易数额为第一数值，所述第一数值大于零，所述接收方地址为所述智能合约的地址，所述附加信息包括所述智能合约的代码；

所述与其他区块链节点经过共识验证将所述第一交易数据存入区块链中，并基于所述交易输出数据将相应的智能合约状态存入各自对应的本地数据库中包括：

将所述第一交易数据打包至新的区块并发送至其他区块链节点，使得各区块链节点经过共识验证将所述新的区块加入区块链时基于所述附加信息初始化所述智能合约，将初始化后的状态存入各自对应的本地数据库中。

3. 根据权利要求 2 所述的方法，还包括：

在基于所述附加信息初始化所述智能合约之后，构造初始找零数据，所述初始找零数据的交易输入数据为所述第一交易数据的交易输入数据，所述初始找零数据的交易输出数据的接收方地址为所述客户端的地址，所述初始找零数据的交易输出数据的交易数额为初始找零数值，所述初始找零数值等于所述交易输入数据的实际交易数额减去所述第一数值后的余额；

将所述初始找零数据发送至其他区块链节点，使得各区块链节点经过共识验证将所述初始找零数据存入区块链中。

4. 根据权利要求 1 或 2 所述的方法，其中：

当所述第一交易数据为触发智能合约的交易数据时，所述类别标识表征第一交易数据与智能合约关联，所述交易数额为第二数值，所述接收方地址为所述智能合约的地址，所述附加信息包括所述智能合约的执行指令；

所述与其他区块链节点经过共识验证将所述第一交易数据存入区块链中，并基于所述交易输出数据将相应的智能合约状态存入各自对应的本地数据库中包括：

将所述第一交易数据打包至新的区块并发送至其他区块链节点，使得各区块链节点经过共识验证将所述新的区块加入区块链时基于所述附加信息运行所述智能合约，将运行后的状态存入各自对应的本地数据库中。

5. 根据权利要求 4 所述的方法，还包括：

在基于所述附加信息运行所述智能合约之后，构造第二交易数据，所述第二交易数据包括交易输入数据和交易输出数据，所述第二交易数据的交易输入数据为所述第一交易数据的交易输出数据，所述第二交易数据包括第一交易输出数据，所述第一交易输出数据的接收方地址为本节点的地址，所述第一交易输出数据的交易数额为第三数值；

将所述第二交易数据发送至其他区块链节点，使得各区块链节点经过共识验证将所述第二交易数据存入区块链中。

6. 根据权利要求 5 所述的方法，其中，所述第二交易数据还包括第二交易输出数据，所述第二交易输出数据的接收方地址为运行所述智能合约后的结果所指示的地址，所述第二交易输出数据的交易数额为第四数值，所述第四数值表征运行所述智能合约后的结果所指示的数额。

7. 根据权利要求 6 所述的方法，其中，所述第二交易数据还包括第三交易输出数据，所述第三交易输出数据的接收方地址为客户端的地址，所述第三交易输出数据的交易数额为第五数值，所述第五数值等于第二数值减去第三数值和第四数值后的余额。

8. 根据权利要求 4 所述的方法，其中：

所述基于所述附加信息初始化所述智能合约包括：基于所述智能合约的代码使用虚拟机初始化所述智能合约；并且/或者

所述基于所述附加信息运行所述智能合约包括：基于所述智能合约的执行指令使用虚拟机运行所述智能合约。

9. 根据权利要求 1 所述的方法，其中：

所述类别标识和所述接收方地址在所述交易输出数据的数据结构中占据同一区域；或者

所述类别标识和所述接收方地址在所述交易输出数据的数据结构中占据不同的区域。

10. 一种区块链的数据处理装置，适配于区块链的未花费交易输出体系，所述装置应用于区块链节点，包括：

接收模块，用于接收客户端发送的第一交易数据，所述第一交易数据包括交易输入数据和交易输出数据；所述交易输出数据包括：类别标识、交易数额、接收方地址和附加信息，其中，所述类别标识用于表征所述第一交易数据是否与智能合约关联，所述附加信息用于在所述第一交易数据与智能合约关联时表征所述智能合约运行所需的信息；

管理模块，用于当所述第一交易数据与智能合约关联时，与其他区块链节点经过共识验证将所述第一交易数据存入区块链中，并基于所述交易输出数据将相应的智能合约状态存入各自对应的本地数据库中。

11. 根据权利要求 10 所述的装置，其中：

当所述第一交易数据为发布智能合约的交易数据时，所述类别标识表征第一交易数据与智能合约关联，所述交易数额为第一数值，所述第一数值大于零，所述接收方地址为所述智能合约的地址，所述附加信息包括所述智能合约的代码；

所述管理模块与其他区块链节点经过共识验证将所述第一交易数据存入区块链中，并基于所述交易输出数据将相应的智能合约状态存入各自对应的本地数据库中包括：

所述管理模块，用于将所述第一交易数据打包至新的区块并发送至其他区块链节点，使得各区块链节点经过共识验证将所述新的区块加入区块链时基于所述附加信息初始化所述智能合约，将初始化后的状态存入各自对应的本地数据库中。

12. 根据权利要求 11 所述的装置，还包括：

初始找零模块，用于在基于所述附加信息初始化所述智能合约之后，构造初始找零数据，所述初始找零数据的交易输入数据为所述第一交易数据的交易输入数据，所述初始找零数据的交易输出数据的接收方地址为所述客户端的地址，所述初始找零数据的交易输出数据的交易数额为初始找零数值，所述初始找零数值等于所述交易输入数据的实际交易数额减去所述第一数值后的余额；将所述初始找零数据发送至其他区块链节点，使得各区块链节点经过共识验证将所述初始找零数据存入区块链中。

13. 根据权利要求 10 或 11 所述的装置，其中：

当所述第一交易数据为触发智能合约的交易数据时，所述类别标识表征第一交易数据与智能合约关联，所述交易数额为第二数值，所述接收方地址为所述智能合约的地址，所述附加信息包括所述智能合约的执行指令；

所述管理模块与其他区块链节点经过共识验证将所述第一交易数据存入区块链中，并基于所述交易输出数据将相应的智能合约状态存入各自对应的本地数据库中包括：

所述管理模块，用于将所述第一交易数据打包至新的区块并发送至其他区块链节点，使得各区块链节点经过共识验证将所述新的区块加入区块链时基于所述附加信息运行所述智能合约，将运行后的状态存入各自对应的本地数据库中。

14. 根据权利要求 13 所述的装置，还包括：

辅助管理模块，用于在基于所述附加信息运行所述智能合约之后，构造第二交易数据，所述第二交易数据包括交易输入数据和交易输出数据，所述第二交易数据的交易输入数据为所述第一交易数据的交易输出数据，所述第二交易数据包括第一交易输出数据，所述第一交易输出数据的接收方地址为本节点的地址，所述第一交易输出数据的交易数额为第三数值；将所述第二交易数据发送至其他区块链节点，使得各区块链节点经过共识验证将所述第二交易数据存入区块链中。

15. 根据权利要求 14 所述的装置，其中，所述第二交易数据还包括第二交易输出数据，所述第二交易输出数据的接收方地址为运行所述智能合约后的结果所指示的地址，所述第二交易输出数据的交易数额为第四数值，所述第四数值表征运行所述智能合约后的结果所指示的数额。

16. 根据权利要求 15 所述的装置，其中，所述第二交易数据还包括第三交易输出数据，所述第三交易输出数据的接收方地址为客户端的地址，所述第三交易输出数据的交易数额为第五数值，所述第五数值等于第二数值减去第三数值和第四数值后的余额。

17. 根据权利要求 13 所述的装置，其中：

所述管理模块基于所述附加信息初始化所述智能合约包括：所述管理模块，用于基于所述智能合约的代码使用虚拟机初始化所述智能合约；并且/或者

所述管理模块基于所述附加信息运行所述智能合约包括：所述管理模块，用于基于所述智能合约的执行指令使用虚拟机运行所述智能合约。

18. 根据权利要求 10 所述的装置，其中：

所述类别标识和所述接收方地址在所述交易输出数据的数据结构中占据同一区域；或者

所述类别标识和所述接收方地址在所述交易输出数据的数据结构中占据不同的区域。

19. 一种计算机设备，包括存储器、处理器及存储在存储器上并可在处理器上运行的计算机程序，所述处理器执行所述程序时，实现如权利要求 1~9 中任一项所述的区块链的数据处理方法。

20. 一种计算机可读存储介质，其上存储有可执行指令，该指令被处理器执行时使处理器执行如权利要求 1~9 中任一项所述的区块链的数据处理方法。

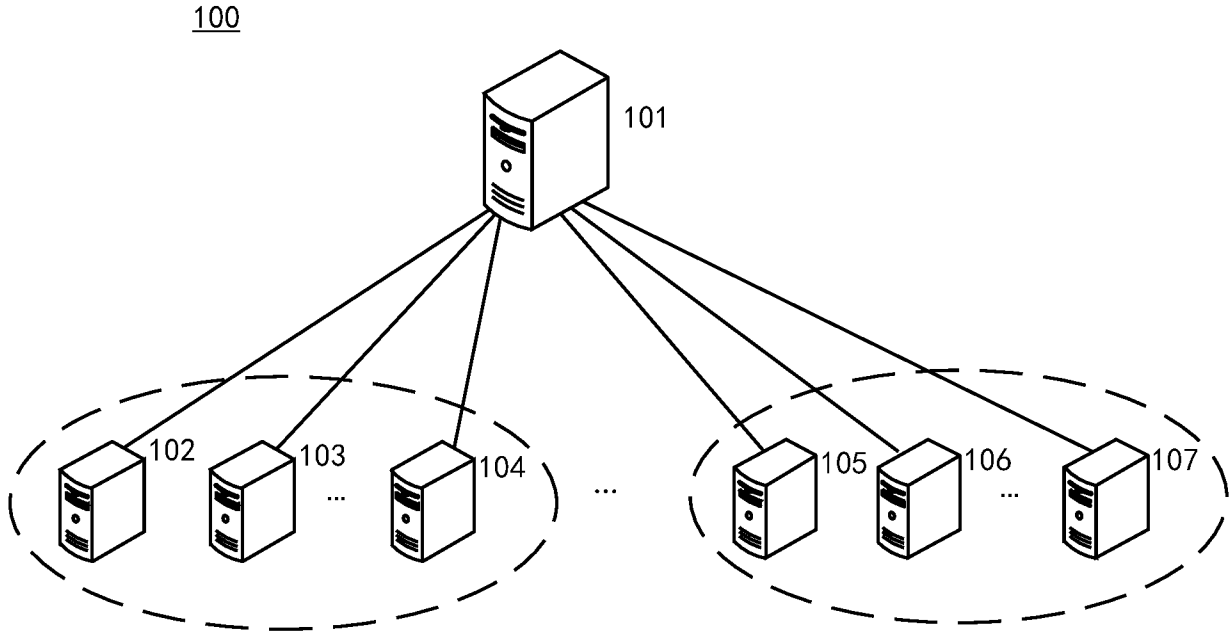
100
101
102
103
104
105
106
107

图 1

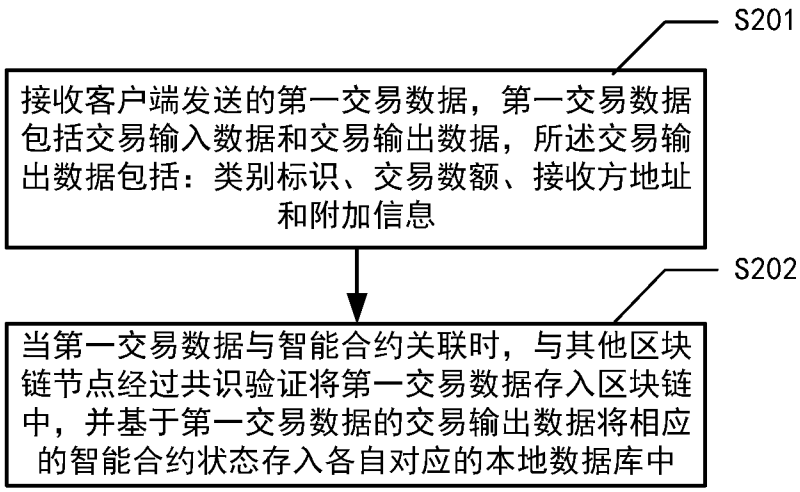
S201
接收客户端发送的第一交易数据，第一交易数据包括交易输入数据和交易输出数据，所述交易输出数据包括：类别标识、交易数额、接收方地址和附加信息
S202
当第一交易数据与智能合约关联时，与其他区块链节点经过共识验证将第一交易数据存入区块链中，并基于第一交易数据的交易输出数据将相应的智能合约状态存入各自对应的本地数据库中

图 2

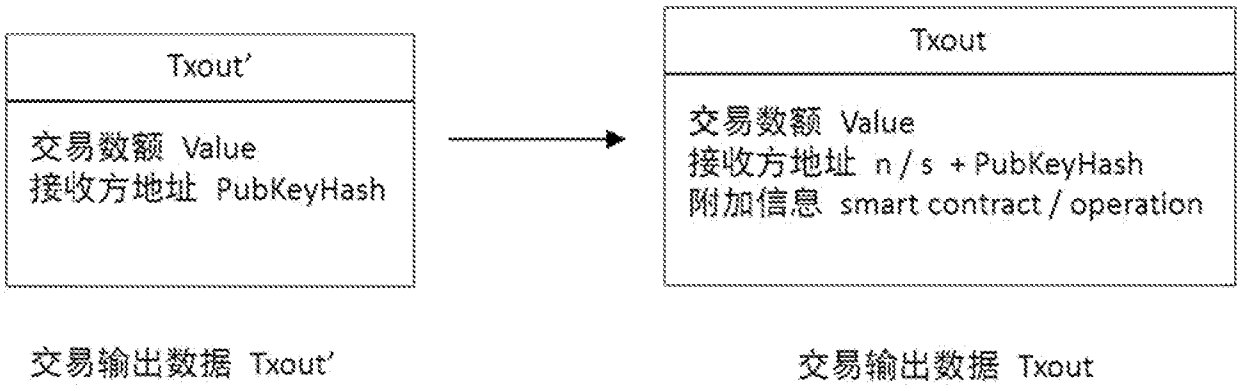
Txout'
交易数额 Value
接收方地址 PubKeyHash
Txout
交易数额 Value
接收方地址 n / s + PubKeyHash
附加信息 smart contract / operation
交易输出数据 Txout'
交易输出数据 Txout

图 3A

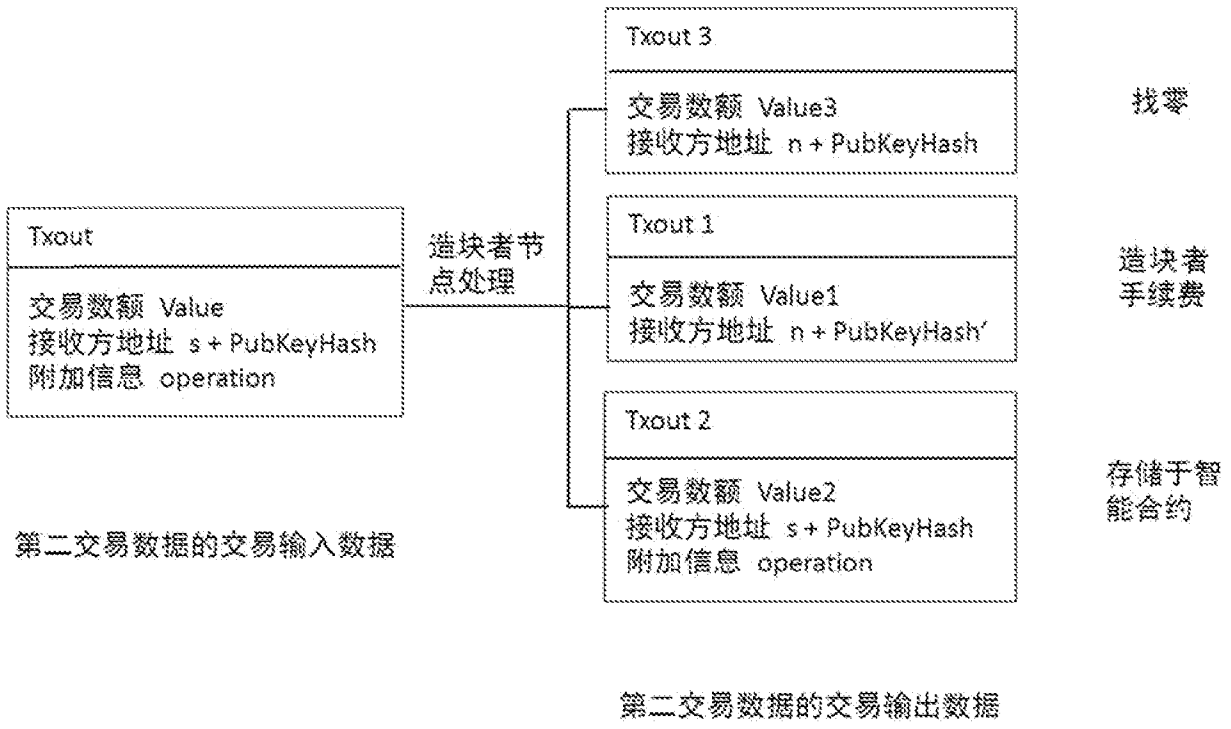
Txout
交易数额 Value
接收方地址 s + PubKeyHash
附加信息 operation
第二交易数据的交易输入数据
造块者节点处理
Txout 3
交易数额 Value3
接收方地址 n + PubKeyHash
找零
Txout 1
交易数额 Value1
接收方地址 n + PubKeyHash'
造块者手续费
Txout 2
交易数额 Value2
接收方地址 s + PubKeyHash
附加信息 operation
存储于智能合约
第二交易数据的交易输出数据

图 3B

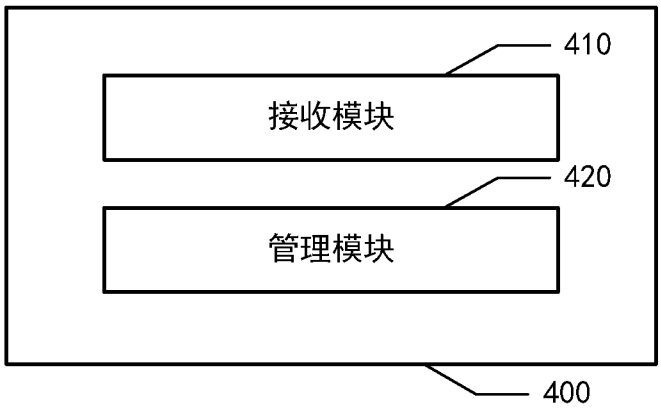
410
接收模块
420
管理模块
400

图 4

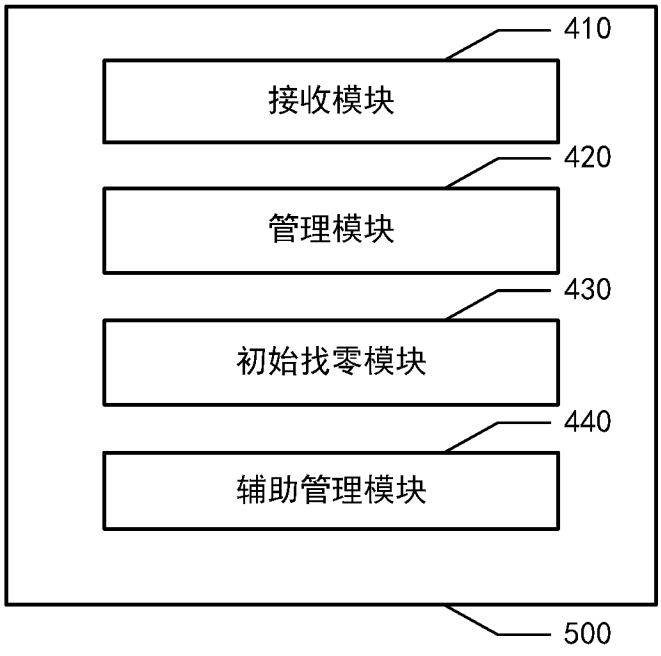
410
接收模块
420
管理模块
430
初始找零模块
440
辅助管理模块
500

图 5

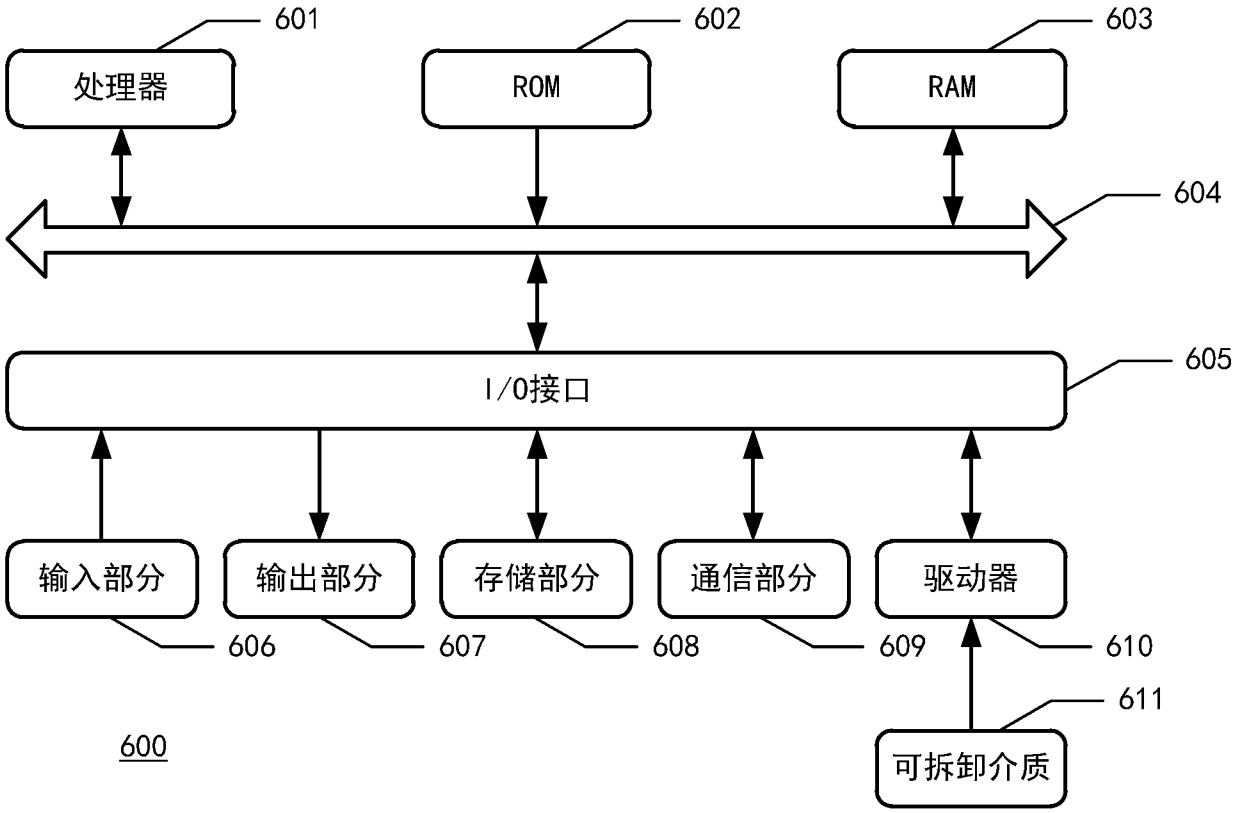
601
602
603
处理器
ROM
RAM
604
I/O接口
605
输入部分
输出部分
存储部分
通信部分
驱动器
606
607
608
609
610
611
600
可拆卸介质

图 6

INTERNATIONAL SEARCH REPORT

International application No.
PCT/CN2018/124368

A. CLASSIFICATION OF SUBJECT MATTER

G06Q 20/08(2012.01)i

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

G06Q

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

CNPAT, WPI, EPODOC, CNKI, IEEE: 区块链, 智能合约, 交易, 输入, 输出, 标识, 地址, 附加, 代码, 关联, 共识验证, 金额, 余额, block chain, agreement, business, input, output, id+, signature, address, code, associat+, money, balance

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	CN 108960797 A (BAIDU ONLINE NETWORK TECHNOLOGY (BEIJING) CO., LTD.) 07 December 2018 (2018-12-07) description, paragraphs [0053]-[0091], [0118]-[0120] and [0229]-[0239], and figures 2 and 9	1-20
A	CN 109034814 A (BAIDU ONLINE NETWORK TECHNOLOGY (BEIJING) CO., LTD.) 18 December 2018 (2018-12-18) entire document	1-20
A	CN 109040029 A (SHANGHAI DIANRONG INFORMATION TECHNOLOGY CO., LTD.) 18 December 2018 (2018-12-18) entire document	1-20
A	CN 108647966 A (SHENZHEN RONGXUN TECHNOLOGY CO., LTD.) 12 October 2018 (2018-10-12) entire document	1-20
A	US 2018181768 A1 (BULL SAS) 28 June 2018 (2018-06-28) entire document	1-20

☐ Further documents are listed in the continuation of Box C. ☑ See patent family annex.

* Special categories of cited documents:
"A" document defining the general state of the art which is not considered to be of particular relevance
"E" earlier application or patent but published on or after the international filing date
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
"O" document referring to an oral disclosure, use, exhibition or other means
"P" document published prior to the international filing date but later than the priority date claimed
"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
29 August 2019	**26 September 2019**
Name and mailing address of the ISA/CN **China National Intellectual Property Administration (ISA/CN)** **No. 6, Xitucheng Road, Jimenqiao Haidian District, Beijing 100088** **China** Facsimile No. **(86-10)62019451**	Authorized officer Telephone No.

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/CN2018/124368

Patent document cited in search report	Publication date (day/month/year)	Patent family member(s)	Publication date (day/month/year)
CN 108960797 A	07 December 2018	None	
CN 109034814 A	18 December 2018	None	
CN 109040029 A	18 December 2018	None	
CN 108647966 A	12 October 2018	None	
US 2018181768 A1	28 June 2018	BR 102017028033 A2	02 January 2019
		EP 3343425 A1	04 July 2018
		FR 3061330 A1	29 June 2018
		US 2019171830 A1	06 June 2019
		CN 108256858 A	06 July 2018

国际检索报告

国际申请号
PCT/CN2018/124368

A. 主题的分类

G06Q 20/08(2012.01)i

按照国际专利分类(IPC)或者同时按照国家分类和IPC两种分类

B. 检索领域

检索的最低限度文献(标明分类系统和分类号)

G06Q

包含在检索领域中的除最低限度文献以外的检索文献

在国际检索时查阅的电子数据库(数据库的名称，和使用的检索词（如使用））

CNPAT, WPI, EPODOC, CNKI, IEEE：区块链，智能合约，交易，输入，输出，标识，地址，附加，代码，关联，共识验证，金额，余额，block chain, agreement, business, input, output, id+, signature, address, code, associat+, money, balance

C. 相关文件

类 型*	引用文件，必要时，指明相关段落	相关的权利要求
X	CN 108960797 A (百度在线网络技术北京有限公司) 2018年 12月 7日 (2018-12-07) 说明书第[0053]-[0091]、[0118]-[0120]、[0229]-[0239]段，附图2、9	1-20
A	CN 109034814 A (百度在线网络技术北京有限公司) 2018年 12月 18日 (2018-12-18) 全文	1-20
A	CN 109040029 A (上海点融信息科技有限责任公司) 2018年 12月 18日 (2018-12-18) 全文	1-20
A	CN 108647966 A (深圳市融讯科技有限公司) 2018年 10月 12日 (2018-10-12) 全文	1-20
A	US 2018181768 A1 (BULL SAS) 2018年 6月 28日 (2018-06-28) 全文	1-20

☐ 其余文件在C栏的续页中列出。

☑ 见同族专利附件。

* 引用文件的具体类型：

“A” 认为不特别相关的表示了现有技术一般状态的文件

“E” 在国际申请日的当天或之后公布的在先申请或专利

“L” 可能对优先权要求构成怀疑的文件，或为确定另一篇引用文件的公布日而引用的或者因其他特殊理由而引用的文件（如具体说明的）

“O” 涉及口头公开、使用、展览或其他方式公开的文件

“P” 公布日先于国际申请日但迟于所要求的优先权日的文件

“T” 在申请日或优先权日之后公布，与申请不相抵触，但为了理解发明之理论或原理的在后文件

“X” 特别相关的文件，单独考虑该文件，认定要求保护的发明不是新颖的或不具有创造性

“Y” 特别相关的文件，当该文件与另一篇或者多篇该类文件结合并且这种结合对于本领域技术人员为显而易见时，要求保护的发明不具有创造性

“&” 同族专利的文件

国际检索实际完成的日期	国际检索报告邮寄日期
2019年 8月 29日	2019年 9月 26日
ISA/CN的名称和邮寄地址 中国国家知识产权局(ISA/CN) 中国北京市海淀区蓟门桥西土城路6号 100088 传真号 (86-10)62019451	受权官员 周亚楠 电话号码 86-(10)-53961530

表 PCT/ISA/210 (第2页) (2015年1月)

国际检索报告
关于同族专利的信息

国际申请号
PCT/CN2018/124368

检索报告引用的专利文件			公布日 (年/月/日)	同族专利			公布日 (年/月/日)
CN	108960797	A	2018年 12月 7日	无			
CN	109034814	A	2018年 12月 18日	无			
CN	109040029	A	2018年 12月 18日	无			
CN	108647966	A	2018年 10月 12日	无			
US	2018181768	A1	2018年 6月 28日	BR	102017028033	A2	2019年 1月 2日
				EP	3343425	A1	2018年 7月 4日
				FR	3061330	A1	2018年 6月 29日
				US	2019171830	A1	2019年 6月 6日
				CN	108256858	A	2018年 7月 6日