(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 6 月 18 日 (18.06.2020)

WIPO | PCT

(10) 国际公布号
WO 2020/119380 A1

(51) 国际专利分类号:
H04L 9/32 (2006.01)

(21) 国际申请号: PCT/CN2019/118740

(22) 国际申请日: 2019 年 11 月 15 日 (15.11.2019)

(25) 申请语言: 中文

(26) 公布语言: 中文

(30) 优先权:
201811519173.9 2018年12月12日 (12.12.2018) CN

(71) 申请人: 阿里巴巴集团控股有限公司 (**ALIBABA GROUP HOLDING LIMITED**) [—/CN]; 开曼群岛大开曼资本大厦一座四层 847 号邮箱, Grand Cayman (KY)。

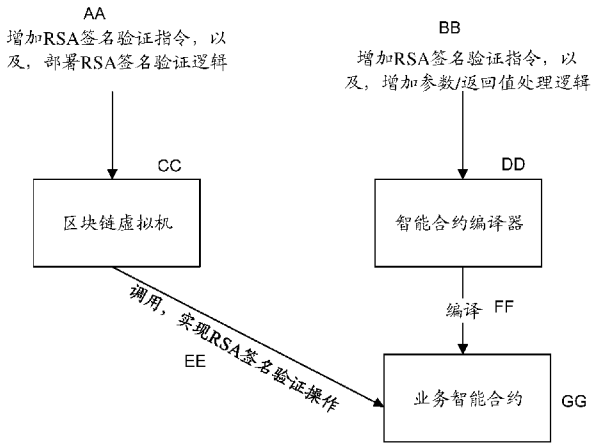
(72) 发明人: 谢桂鲁 (**XIE, Guilu**); 中国浙江省杭州市余杭区文一西路 969 号 3 号楼 5 楼阿里巴巴集团法务部, Zhejiang 311121 (CN)。 周知远 (**ZHOU, Zhiyuan**); 中国浙江省杭州市余杭区文一西路 969 号 3 号楼 5 楼阿里巴巴集团法务部, Zhejiang 311121 (CN)。

(74) 代理人: 北京博思佳知识产权代理有限公司 (**BEIJING BESTIPR INTELLECTUAL PROPERTY LAW CORPORATION**); 中国北京市海淀区上地三街 9 号嘉华大厦 B 座 409, Beijing 100085 (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:** SIGNATURE VERIFICATION METHOD AND SYSTEM BASED ON BLOCKCHAIN SMART CONTRACT

(54) 发明名称: 一种基于区块链智能合约的签名验证方法及系统



AA Add an RSA signature verification instruction, and deploy RSA signature verification logic
BB Add the RSA signature verification instruction, and add parameter/return value processing logic
CC Blockchain virtual machine
DD Smart contract compiler
EE Call to achieve an RSA signature verification operation
FF Compile
GG Service smart contract

图 8a

(57) **Abstract:** Disclosed are a signature verification method and system based on a blockchain smart contract. In embodiments of the specification, on one hand, an RSA signature verification instruction is defined and added into an instruction set of a blockchain virtual machine, and moreover, RSA signature verification logic corresponding to the RSA signature verification instruction is deployed in the blockchain virtual machine. On the other hand, the defined RSA signature verification instruction needs to be added to an instruction set of a smart contract compiler, so that the service smart contract compiled by the smart contract compiler contains the RSA signature verification instruction. In this way, if the service smart contract is deployed in a blockchain network, the user can simultaneously assign and call the service smart contract to execute the service initiation transaction when constructing the service initiation transaction.

WO 2020/119380 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))。

(57) 摘要：公开了一种基于区块链智能合约的签名验证方法及系统。在本说明书实施例中，一方面，定义RSA签名验证指令并添加到区块链虚拟机的指令集中，同时，在区块链虚拟机中部署对应于所述RSA签名验证指令的RSA签名验证逻辑。另一方面，还需要将定义的RSA签名验证指令添加到智能合约编译器的指令集中，使得经智能合约编译器编译的业务智能合约中包含RSA签名验证指令。这样一来，倘若将所述业务智能合约部署到区块链网络中，那么，用户在构建业务发起交易时，就可以同时指定调用所述业务智能合约执行该业务发起交易。

一种基于区块链智能合约的签名验证方法及系统

技术领域

[01] 本说明书实施例涉及信息技术领域，尤其涉及一种基于区块链智能合约的签名验证方法及系统。

背景技术

[02] 目前，通过在基于以太坊协议搭建的区块链网络中部署智能合约，可以满足各种各样的线上业务需求。

[03] 在实践中，对于有的业务需求，区块链网络中的各节点在通过以太坊虚拟机调用该业务需求对应的智能合约执行交易时，需要进行基于 RSA 算法的签名验证操作。其中，RSA 算法是 1977 年由罗纳德·李维斯特（Ron Rivest）、阿迪·萨莫尔（Adi Shamir）和伦纳德·阿德曼（Leonard Adleman），RSA 算法也因此得名。

[04] 但是，现有的以太坊虚拟机并不支持基于 RSA 算法的签名验证操作。

发明内容

[05] 为了解决现有的以太坊虚拟机不默认支持 RSA 签名验证操作的问题，本说明书实施例提供一种基于区块链智能合约的签名验证方法及系统，技术方案如下：

[06] 根据本说明书实施例的第 1 方面，提供一种基于区块链智能合约的签名验证方法，区块链虚拟机的指令集中包括 RSA 签名验证指令，并且，区块链虚拟机中部署有对应于所述 RSA 签名验证指令的 RSA 签名验证逻辑；

[07] 智能合约编译器的指令集中包括所述 RSA 签名验证指令，经所述智能合约编译器编译的业务智能合约中包含所述 RSA 签名验证指令；

[08] 区块链网络中部署有所述业务智能合约；

[09] 所述签名验证方法包括：

[10] 所述区块链网络中的节点获得业务发起交易并广播给其他节点；

[11] 针对所述区块链网络中的每个节点，该节点在执行所述业务发起交易时，通过区块链虚拟机，调用所述业务智能合约；

[12] 该节点通过区块链虚拟机，根据所述业务智能合约中的RSA签名验证指令，触发执行所述RSA签名验证逻辑，以对业务签名进行RSA签名验证操作。

[13] 根据本说明书实施例的第 2 方面，提供另一种基于区块链智能合约的签名验证方法，区块链虚拟机的指令集中包括 RSA 签名验证指令，并且，区块链虚拟机中部署有对应于所述RSA签名验证指令的 RSA 签名验证逻辑；

[14] 智能合约编译器的指令集中包括所述RSA签名验证指令，经所述智能合约编译器编译的业务智能合约中包含RSA签名验证智能合约的合约标识，所述RSA签名验证智能合约是预先部署于区块链网络中的智能合约；

[15] 区块链网络中部署有所述业务智能合约；

[16] 所述签名验证方法包括:

[17] 所述区块链网络中的节点获得业务发起交易并广播给其他节点；

[18] 针对所述区块链网络中的每个节点，该节点在执行所述业务发起交易时，通过区块链虚拟机，调用所述业务智能合约；

[19] 该节点通过区块链虚拟机，根据所述业务智能合约中的所述RSA签名验证智能合约的合约标识，调用所述RSA签名验证智能合约；

[20] 该节点通过区块链虚拟机，根据所述RSA签名验证智能合约中的RSA签名验证指令，触发执行所述RSA签名验证逻辑，以对业务签名进行RSA签名验证操作，以对业务签名进行RSA签名验证操作。

[21] 根据本说明书实施例的第 3 方面，提供一种区块链虚拟机，用于实现上述第 1 方面与第 2 方面的方法；

[22] 其中，智能合约编译器的指令集中包括所述RSA签名验证指令，经所述智能合约编译器编译的业务智能合约中包含所述RSA签名验证指令。

[23] 根据本说明书实施例的第 4 方面，提供一种智能合约编译器，用于实现上述第 1 方面的方法；

[24] 其中，智能合约编译器的指令集中包括所述RSA签名验证指令，经所述智能合约编译器编译的业务智能合约中包含所述RSA签名验证指令。

[25] 根据本说明书实施例的第 5 方面，提供一种智能合约编译器，用于实现上述第 2 方面的方法；

[26] 其中，智能合约编译器的指令集中包括所述 RSA 签名验证指令，经所述智能合约编译器编译的业务智能合约中包含 RSA 签名验证智能合约的合约标识，所述 RSA 签名验证智能合约是预先部署于区块链网络中的智能合约。

[27] 根据本说明书实施例的第 6 方面，提供一种区块链系统，包括区块链网络；

[28] 其中，区块链虚拟机的指令集中包括 RSA 签名验证指令，并且，区块链虚拟机中部署有对应于所述 RSA 签名验证指令的 RSA 签名验证逻辑；智能合约编译器的指令集中包括所述 RSA 签名验证指令，经所述智能合约编译器编译的业务智能合约中包含所述 RSA 签名验证指令；区块链网络中部署有所述业务智能合约；

[29] 所述区块链网络中的节点，获得业务发起交易并广播给其他节点；

[30] 所述区块链网络中的每个节点，在执行所述业务发起交易时，通过区块链虚拟机，调用所述业务智能合约；通过区块链虚拟机，根据所述业务智能合约中的 RSA 签名验证指令，触发执行所述 RSA 签名验证逻辑，以对业务签名进行 RSA 签名验证操作，以对业务签名进行 RSA 签名验证操作。

[31] 根据本说明书实施例的第 7 方面，提供另一种区块链系统，包括区块链网络；

[32] 其中，区块链虚拟机的指令集中包括 RSA 签名验证指令，并且，区块链虚拟机中部署有对应于所述 RSA 签名验证指令的 RSA 签名验证逻辑；智能合约编译器的指令集中包括所述RSA签名验证指令，经所述智能合约编译器编译的业务智能合约中包含RSA签名验证智能合约的合约标识，所述 RSA 签名验证智能合约是预先部署于区块链网络中的智能合约；区块链网络中部署有所述业务智能合约；

[33] 所述区块链网络中的节点，获得业务发起交易并广播给其他节点；

[34] 所述区块链网络中的每个节点，在执行所述业务发起交易时，通过区块链虚拟机，调用所述业务智能合约；通过区块链虚拟机，根据所述业务智能合约中的所述 RSA 签名验证智能合约的合约标识，调用所述 RSA 签名验证智能合约；通过区块链虚拟机，根据所述 RSA 签名验证智能合约中的 RSA 签名验证指令，触发执行所述 RSA 签名验证逻辑，以对业务签名进行 RSA 签名验证操作，以对业务签名进行 RSA 签名验证操作。

[35] 本说明书实施例所提供的技术方案，一方面，定义 RSA 签名验证指令并添加到区块链虚拟机的指令集中，同时，在区块链虚拟机中部署对应于所述 RSA 签名验证指令的 RSA 签名验证逻辑。另一方面，还需要将定义的 RSA 签名验证指令添加到智能合约编译器的指令集中，使得经智能合约编译器编译的业务智能合约中包含 RSA 签名验证

指令。

[36] 这样一来，倘若将所述业务智能合约部署到区块链网络中，那么，用户在构建业务发起交易时，就可以同时指定调用所述业务智能合约执行该业务发起交易，进而，虚拟机在执行该业务发起交易时，就会调用所述业务智能合约，并根据所述业务智能合约中的RSA签名验证指令，触发执行预先部署的RSA签名验证逻辑。

[37] 通过本说明书实施例，通过对区块链虚拟机与智能合约编译器的指令集进行扩展，使得区块链虚拟机可以默认支持RSA签名验证操作。

[38] 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，并不能限制本说明书实施例。

[39] 此外，本说明书实施例中的任一实施例并不需要达到上述的全部效果。

附图说明

[40] 为了更清楚地说明本说明书实施例或现有技术中的技术方案，下面将对实施例或现有技术描述中所需要使用的附图作简单地介绍，显而易见地，下面描述中的附图仅仅是本说明书实施例中记载的一些实施例，对于本领域普通技术人员来讲，还可以根据这些附图获得其他的附图。

[41] 图1是本说明书实施例提供的一种基于区块链智能合约的编码方法的流程示意图；

[42] 图2是本说明书实施例提供的另一种基于区块链智能合约的编码方法的流程示意图；

[43] 图3是本说明书实施例提供的一种基于区块链智能合约的解码方法的流程示意图；

[44] 图4是本说明书实施例提供的另一种基于区块链智能合约的解码方法的流程示意图；

[45] 图5a~b是本说明书实施例提供的BASE64编解码操作的部署示意图；

[46] 图6是本说明书实施例提供的一种基于区块链智能合约的签名验证方法的流程示意图；

[47] 图7是本说明书实施例提供的另一种基于区块链智能合约的签名验证方法的流程示意图；

[48] 图8a~b是本说明书实施例提供的RSA签名验证操作的部署示意图；

[49] 图 9 是本说明书实施例提供的一种基于区块链智能合约的数据处理方法的流程示意图;

[50] 图 10 是本说明书实施例提供的一种基于区块链智能合约的数据处理方法的流程示意图;

[51] 图 11a~b 是本说明书实施例提供的 JSON 处理操作的部署示意图;

[52] 图 12 是本说明书实施例提供的一种基于区块链智能合约的数据处理方法的流程示意图;

[53] 图 13 是本说明书实施例提供的一种基于区块链智能合约的数据处理方法的流程示意图;

[54] 图 14a~b 是本说明书实施例提供的处理操作的部署示意图;

[55] 图 15 是本说明书实施例提供的一种基于区块链智能合约的交易哈希获取方法的流程示意图;

[56] 图 16 是本说明书实施例提供的一种基于区块链智能合约的交易哈希获取方法的流程示意图;

[57] 图 17a~b 是本说明书实施例提供的交易哈希获取操作的部署示意图;

[58] 图 18 是本说明书实施例提供的一种基于区块链智能合约的转账方法的流程示意图;

[59] 图 19 是本说明书实施例提供的一种基于区块链智能合约的交易哈希获取方法的流程示意图;

[60] 图 20a~b 是本说明书实施例提供的转账交易的相关校验操作的部署示意图;

[61] 图 21 示出了本说明书实施例所提供的一种区块链系统的结构示意图;

[62] 图 22 是用于配置本说明书实施例方法的一种计算机设备的结构示意图。

具体实施方式

[63] 在本文中，区块链虚拟机，是指每个区块链节点在执行交易时所依赖的执行程序。区块链虚拟机为区块链交易提供了执行环境。

[64] 需要说明的是，区块链虚拟机不仅可以是以太坊协议中记载的以太坊虚拟机（Ethereum Virtual Machine，EVM），还可以是除以太坊协议之外的其他区块链协议中

所指的虚拟机。

[65] 在本文中，智能合约编译器，是指用于将使用编程语言（如 solidity 语言）编写的智能合约，编译成区块链虚拟机可以识别并执行的机器语言（如字节码、二进制码等）的程序。需要说明的是，部署于区块链网络中的智能合约，一般是指经过智能合约编译器编译后的智能合约，即字节码形式或二进制码形式的智能合约。

[66] 在以太坊协议或其他类似于以太坊协议的区块链协议中，区块链虚拟机在本地维护了若干组指令与操作之间的映射关系（如下表 1 所示），并且，区块链虚拟机本地还部署有表 1 中的每个操作的代码逻辑。指令 1~指令 N 都是区块链虚拟机所默认支持的指令，指令 1~指令 N 组成了区块链虚拟机的指令集。区块链虚拟机在调用智能合约时，如果从智能合约中读取到表 1 中的任一指令，就会触发执行该指令对应的操作的代码逻辑。需要说明的是，本文所述的指令一般是字节码形式或二进制码形式的。

指令 1	操作 1
指令 2	操作 2
指令 3	操作 3
……	……
指令 N	操作 N

表 1

[67] 因此，如果想让区块链虚拟机执行表 1 中的任一操作，就需要在区块链虚拟机所要调用智能合约中，预先写入该操作对应的指令。这意味着，智能合约编译器在预先对该智能合约进行编译时，能够将智能合约（使用编程语言编写的）中声明实现表 1 中任一操作的内容编译成对应的指令，以便区块链虚拟机可以识别。这就要求，智能合约编译器也需要默认支持表 1 中的指令 1~指令 N，指令 1~指令 N 组成了智能合约编译器的指令集。

[68] 总之，在以太坊协议或其他类似于以太坊协议的区块链协议中，一般是由区块链虚拟机、智能合约编译器以及智能合约协同实现特定的业务需求。

[69] 但是，现有的以太坊虚拟机在本地默认支持的操作是有限的，而业务需求是复杂多样的。例如，现有的以太坊虚拟机与以太坊的智能合约编译器并不默认支持如下操作，导致在现有的以太坊架构中，无法实现一些依赖于如下操作的业务需求：

[70] 1、基于 64 个可打印字符（BASE64）的编解码操作。

[71] 2、RSA 签名验证操作；其中，RSA 算法是 1977 年由罗纳德·李维斯特（Ron Rivest）、阿迪·萨莫尔（Adi Shamir）和伦纳德·阿德曼（Leonard Adleman），RSA 算法也因此得名。

[72] 3、对 JS 对象简谱（JavaScript Object Notation，JSON）数据的处理操作；其中，JSON 是一种常见的数据交换格式，JSON 数据是具有这种数据交换格式的数据。

[73] 4、对可扩展标记语言（eXtensible Markup Language，XML）数据的处理操作；其中，XML 是一种常见的数据交换格式，XML 数据是具有这种数据交换格式的数据。

[74] 5、获取当前执行的交易的交易哈希的操作。

[75] 6、对于一笔转账交易，在不暴露转账人的资产余额与转账金额的前提下，判断转账人的资产余额是否足够支付这笔转账交易的转账金额。

[76] 由于现有的以太坊虚拟机与以太坊的智能合约编译器不默认支持上述操作的问题，因此，在现有技术中，针对上述任一种操作，一般采用将实现该操作的代码逻辑直接写入智能合约的方式，使得以太坊虚拟机在执行交易时，调用智能合约来执行该操作的代码逻辑。也就是说，以太坊虚拟机虽然不默认支持上述操作，但是将上述操作的代码逻辑写入智能合约，并让以太坊虚拟机调用该智能合约，也可以实现以太坊虚拟机执行上述操作的目的。

[77] 但是，实践中，相比于以太坊虚拟机直接执行本地预先部署的代码逻辑，以太坊虚拟机执行智能合约中的代码逻辑的效率较低。

[78] 而本申请的核心思想在于，一方面，对区块链虚拟机的指令集进行扩展，增加上述操作对应的指令，同时在区块链虚拟机本地预先部署上述操作对应的代码逻辑，使得区块链虚拟机可以默认支持上述操作。另一方面，对智能合约编译器的指令集也进行扩展，增加上述操作对应的指令。其中，针对同一操作，为区块链虚拟机的指令集增加的对应于该操作的指令与为智能合约编译器的指令集增加的对应于该操作的指令应当一致。如表 2 所示。

指令 1	操作 1
指令 2	操作 2
指令 3	操作 3
BASE64 编码指令	BASE64 编码操作
……	……
指令 N	操作 N

表 2

[79] 如此，以上述的 BASE64 编码操作为例，可以在使用编程语言编写智能合约时，在智能合约中声明调用 BASE64 编码操作，智能合约编译器在对智能合约进行编译时，将这段声明编译成 BASE64 编码指令。该智能合约被部署到区块链网络中之后，用户在发起业务时，可以在业务发起交易中指定调用该智能合约，这样，区块链虚拟机在执行业务发起交易时，就会调用该智能合约，并当从该智能合约中读取到 BASE64 编码指令，触发在本地执行相应的 BASE64 编码逻辑，以实现 BASE64 编码操作。

[80] 为了使本领域技术人员更好地理解本说明书实施例中的技术方案，下面将结合本说明书实施例中的附图，对本说明书实施例中的技术方案进行详细地描述，显然，所描述的实施例仅仅是本说明书的一部分实施例，而不是全部的实施例。基于本说明书中的实施例，本领域普通技术人员所获得的所有其他实施例，都应当属于保护的范围。

[81] 以下结合附图，详细说明本说明书各实施例提供的技术方案。需要说明的是，由于以下的各实施例所基于的技术思想都是类似的，因此，下文的各实施例可互相参照理解。

实施例一

[82] 图 1 是本说明书实施例提供的一种基于区块链智能合约的编码方法的流程示意图，包括以下步骤:

[83] S100: 区块链网络中的节点获得业务发起交易并广播给其他节点。

[84] S102: 针对所述区块链网络中的每个节点，该节点在执行所述业务发起交易时，通过区块链虚拟机，调用所述业务智能合约。

[85] S104: 该节点通过区块链虚拟机，根据所述业务智能合约中的 BASE64 编码指令，触发执行所述 BASE64 编码逻辑，以对待编码数据进行编码操作。

[86] 在本实施例中，需要针对区块链网络进行预先配置，使得:

[87] 1）区块链虚拟机的指令集中包括BASE64编码指令，并且，区块链虚拟机中部署有对应于所述BASE64编码指令的BASE64编码逻辑。

[88] 2）智能合约编译器的指令集中包括所述BASE64编码指令，经所述智能合约编译器编译的业务智能合约中包含所述BASE64编码指令。

[89] 3）区块链网络中部署有所述业务智能合约。

[90] 所述业务智能合约是需要调用BASE64编码功能的业务所对应的智能合约。

[91] 在本说明的各实施例中，区块链网络包括多个节点。其中，从软件层面上看，节点是指用于实现区块链功能的区块链程序；从硬件层面上看，节点是指安装有区块链程序的用户设备。在实际应用中，每个节点可以对接至少一个客户端（或称钱包），区块链中的交易通常是客户端构建的。

[92] 在本说明的各实施例中所描述的交易（transaction），是指用户通过区块链的客户端创建，并需要最终发布至区块链的分布式数据库中的一笔数据。交易是区块链协议中所约定的一种数据结构，一笔数据要存入区块链，就需要被封装成交易。

[93] 区块链中的交易，存在狭义的交易以及广义的交易之分。狭义的交易是指用户向区块链发布的一笔价值转移；例如，在传统的比特币区块链网络中，交易可以是用户在区块链中发起的一笔转账。而广义的交易是指用户向区块链发布的一笔具有业务意图的业务数据；例如，运营方可以基于实际的业务需求搭建一个联盟链，依托于联盟链部署一些与价值转移无关的其它类型的在线业务（比如，租房业务、车辆调度业务、保险理赔业务、信用服务、医疗服务等），而在这类联盟链中，交易可以是用户在联盟链中发布的一笔具有业务意图的业务消息或者业务请求。

[94] 在区块链网络中，用户通常以交易的形式发起业务。具体地，节点需要获得业务发起交易如果上述的业务智能合约不是区块链网络中部署的唯一的智能合约，业务发起交易中还会注明所述业务智能合约的合约标识，以明确交易执行时所需要调用的智能合约。

[95] 其中，业务发起交易通常是用户通过客户端构建并发送给节点的。一般而言，区块链网络对接的客户端与各用户一一对应。

[96] 节点在将业务发起交易广播给其他节点之后，针对每个节点，该节点在接收到所述业务发起交易之后，需要通过区块链虚拟机调用所述业务智能合约来执行该业务发起交易。此处需要说明的是，在区块链网络中，每个节点上都部署有区块链虚拟机，节点

执行交易时，实际上是节点上部署的区块链虚拟机在执行交易。

[97] 在实施例一中，区块链虚拟机调用所述业务智能合约之后，会读取所述业务智能合约中的字节码或二进制码并执行，当读取到所述业务智能合约中的 BASE64 编码指令时，相当于明确了此时需要进行 BASE64 编码操作，因此，区块链虚拟机此时会触发执行预先部署于本地的 BASE64 编码逻辑，以对待编码数据进行编码操作。

[98] 在实际应用中，视具体的业务需求的不同，待编码数据可以是包含于所述业务发起交易中的，也可以包含于所述业务智能合约中的，还可以是区块链虚拟机在执行所述业务发起交易时产生的。

[99] 此外，各节点除了通过区块链虚拟机执行业务发起交易之外，还需要基于共识机制，将所述业务发起交易写入区块链。

[100] 另外需要说明的是，区块链虚拟机如果根据所述业务智能合约中的 BASE64 编码指令触发执行 BASE64 编码逻辑，那么，在执行过程中所采用的数据传递方式通常是栈传递（即一般会将 BASE64 编码后的数据写入栈中），但是，对于经过 BASE64 编码后的数据而言，其数据长度是不固定的，如果采用栈传递的方式，就要求针对各种可能当数据长度都预先设置相应的 BASE64 编码指令，实现起来较为复杂。

[101] 为此，以下的实施例二提供了另一种基于区块链智能合约的编码方法。

实施例二

[102] 图 2 是本说明书实施例提供的另一种基于区块链智能合约的编码方法的流程示意图，包括以下步骤：

[103] S200：区块链网络中的节点获得业务发起交易并广播给其他节点。

[104] S202：针对所述区块链网络中的每个节点，该节点在执行所述业务发起交易时，通过区块链虚拟机，调用所述业务智能合约。

[105] S204：该节点通过区块链虚拟机，根据所述业务智能合约中的所述 BASE64 编码智能合约的合约标识，调用所述 BASE64 编码智能合约。

[106] S206：该节点通过区块链虚拟机，根据所述 BASE64 编码智能合约中的，BASE64 编码指令，触发执行所述 BASE64 编码逻辑，以对待编码数据进行编码操作。

[107] 在本实施例中，需要针对区块链网络进行预先配置，使得：

[108] 1）区块链虚拟机的指令集中包括 BASE64 编码指令，并且，区块链虚拟机中部署

有对应于所述 BASE64 编码指令的 BASE64 编码逻辑。

[109] 2）智能合约编译器的指令集中包括所述 BASE64 编码指令，经所述智能合约编译器编译的业务智能合约中包含 BASE64 编码智能合约的合约标识，所述 BASE64 编码智能合约是预先部署于所述区块链网络中的智能合约。

[110] 3）区块链网络中部署有所述业务智能合约。

[111] 实施例二与实施例一的区别主要在于，在实施例二中，区块链虚拟机调用所述业务智能合约之后，当读取到所述 BASE64 编码智能合约的合约标识时，相当于明确了此时需要进一步调用所述 BASE64 编码智能合约。区块链虚拟机调用所述 BASE64 编码智能合约，也会读取所述 BASE64 编码智能合约中的字节码或二进制码，当读取到所述 BASE64 编码指令时，相当于明确了此时需要执行 BASE64 编码操作，因此，区块链虚拟机此时会触发执行预先部署于本地的 BASE64 编码逻辑，以对待编码数据进行编码操作。

[112] 也就是说，在实施例二中，智能合约编译器在编译业务智能合约时，如果发现业务智能合约中声明调用 BASE64 编码操作，则不会将这段声明编译 BASE64 编码指令，而是编译成所述 BASE64 编码智能合约的合约标识。这样，区块链虚拟机在调用业务智能合约时，会进一步调用所述 BASE64 编码智能合约。

[113] 在区块链技术领域，所述 BASE64 编码智能合约实际上是一种预编译合约，区块链虚拟机在调用并执行如 BASE64 编码智能合约这样的预编译合约时，并不会采用栈传递的方式进行参数传递，而是会采用内存传递的方式进行参数传递（支持不固定长度的数据读写）。

实施例三

[114] 图 3 是本说明书实施例提供的一种基于区块链智能合约的编码方法的流程示意图，包括以下步骤:

[115] S300: 区块链网络中的节点获得业务发起交易并广播给其他节点。

[116] S302: 针对所述区块链网络中的每个节点，该节点在执行所述业务发起交易时，通过区块链虚拟机，调用所述业务智能合约。

[117] S304: 该节点通过区块链虚拟机，根据所述业务智能合约中的 BASE64 解码指令，触发执行所述 BASE64 解码逻辑，以对待解码数据进行解码操作。

[118] 在本实施例中，需要针对区块链网络进行预先配置，使得:

[119] 1）区块链虚拟机的指令集中包括 BASE64 解码指令，并且，区块链虚拟机中部署有对应于所述 BASE64 解码指令的 BASE64 解码逻辑。

[120] 2）智能合约编译器的指令集中包括所述 BASE64 解码指令，经所述智能合约编译器编译的业务智能合约中包含所述 BASE64 解码指令。

[121] 3）区块链网络中部署有所述业务智能合约。

[122] 由于 BASE64 解码操作与 BASE64 编码操作是相对应的一组操作，因此，相关说明参见实施例一即可，不再赘述。

[123] 需要说明的是，在实际应用中，视具体的业务需求的不同，待解码数据可以是包含于所述业务发起交易中的，也可以包含于所述业务智能合约中的，还可以是区块链虚拟机在执行所述业务发起交易时产生的。

[124] 此外，在实施例三中，也存在前文所述的栈传递实现复杂的问题，为此，以下的实施例四提供了另一种基于区块链智能合约的解码方法。

实施例四

[125] 图 4 是本说明书实施例提供的另一种基于区块链智能合约的解码方法的流程示意图，包括以下步骤:

[126] S400: 区块链网络中的节点获得业务发起交易并广播给其他节点。

[127] S402: 针对所述区块链网络中的每个节点，该节点在执行所述业务发起交易时，通过区块链虚拟机，调用所述业务智能合约。

[128] S404: 该节点通过区块链虚拟机，根据所述业务智能合约中的所述 BASE64 解码智能合约的合约标识，调用所述 BASE64 解码智能合约。

[129] S406: 该节点通过区块链虚拟机，根据所述 BASE64 解码智能合约中的，BASE64 解码指令，触发执行所述 BASE64 解码逻辑，以对待解码数据进行解码操作。

[130] 在本实施例中，需要针对区块链网络进行预先配置，使得:

[131] 1）区块链虚拟机的指令集中包括 BASE64 解码指令，并且，区块链虚拟机中部署有对应于所述 BASE64 解码指令的 BASE64 解码逻辑。

[132] 2）智能合约编译器的指令集中包括所述 BASE64 解码指令，经所述智能合约编译

器编译的业务智能合约中包含 BASE64 解码智能合约的合约标识，所述 BASE64 解码智能合约是预先部署于所述区块链网络中的智能合约。

[133] 3）区块链网络中部署有所述业务智能合约。

[134] 实施例四与实施例三的区别主要在于，在实施例四中，区块链虚拟机调用所述业务智能合约之后，当读取到所述 BASE64 解码智能合约的合约标识时，相当于明确了此时需要进一步调用所述 BASE64 解码智能合约。区块链虚拟机调用所述 BASE64 解码智能合约，也会读取所述 BASE64 解码智能合约中的字节码或二进制码，当读取到所述 BASE64 解码指令时，相当于明确了此时需要执行 BASE64 解码操作，因此，区块链虚拟机此时会触发执行预先部署于本地的 BASE64 解码逻辑，以对待解码数据进行解码操作。

[135] 图 5a 是本说明书实施例提供的对应于实施例一与实施例三的 BASE64 编解码操作的部署示意图。如图 5a 所示，其一，为区块链虚拟机的指令集添加 BASE64 编码指令和/或 BASE64 解码指令，同时，在区块链虚拟机中部署 BASE64 编码逻辑和/或 BASE64 解码逻辑。其二，为智能合约编译器的指令集添加 BASE64 编码指令和/或 BASE64 解码指令。其三，将经过智能合约编译器编译的业务智能合约（包含 BASE64 编码指令和/或 BASE64 解码指令）部署于区块链网络中。

[136] 需要说明的是，在为智能合约编译器增加功能指令（包括本文中所述的各种指令）时，一般需要相应为智能合约编译器增加该功能指令对应的处理逻辑，（如参数/返回值处理逻辑），以便智能合约编译器将该功能指令对应的处理逻辑也写入业务智能合约。

[137] 对于实施例二与实施例四，图 5b 是本说明书实施例提供的对应于实施例二与实施例四的 BASE64 编解码操作的部署示意图。如图 5b 所示，其一，为区块链虚拟机的指令集添加 BASE64 编码指令和/或 BASE64 解码指令，同时，在区块链虚拟机中部署 BASE64 编码逻辑和/或 BASE64 解码逻辑。其二，为智能合约编译器的指令集添加 BASE64 编码指令和/或 BASE64 解码指令。其三，将经过智能合约编译器编译的业务智能合约（包含 BASE64 编码智能合约的合约标识与 BASE64 解码智能合约的合约标识）部署于区块链网络中。

实施例五

[138] 图 6 是本说明书实施例提供的一种基于区块链智能合约的签名验证方法的流程示意图，包括如下步骤：

[139] S600: 区块链网络中的节点获得业务发起交易并广播给其他节点。

[140] S602: 针对所述区块链网络中的每个节点，该节点在执行所述业务发起交易时，通过区块链虚拟机，调用所述业务智能合约。

[141] S604: 该节点通过区块链虚拟机,根据所述业务智能合约中的 RSA 签名验证指令，触发执行所述 RSA 签名验证逻辑，以对业务签名进行 RSA 签名验证操作。

[142] 在本实施例中，需要针对区块链网络进行预先配置，使得:

[143] 1）区块链虚拟机的指令集中包括 RSA 签名验证指令，并且，区块链虚拟机中部署有对应于所述 RSA 签名验证指令的 RSA 签名验证逻辑。

[144] 2）智能合约编译器的指令集中包括所述 RSA 签名验证指令，经所述智能合约编译器编译的业务智能合约中包含所述 RSA 签名验证指令。

[145] 3）区块链网络中部署有所述业务智能合约。

[146] 所述业务智能合约是需要调用 RSA 签名验证功能的业务所对应的智能合约。

[147] 在实施例一中，区块链虚拟机调用所述业务智能合约之后，会读取所述业务智能合约中的字节码或二进制码并执行，当读取到所述业务智能合约中的 RSA 签名验证指令时，相当于明确了此时需要进行 RSA 签名验证操作，因此，区块链虚拟机此时会触发执行预先部署于本地的 RSA 签名验证逻辑，以对业务签名进行签名验证操作。

[148] 在实际应用中，视具体的业务需求的不同，存在以下几种情况:

[149] 1）所述业务发起交易包含所述业务签名、所述业务签名对应的被签名数据以及用于验证所述业务签名的公钥。

[150] 2）所述业务发起交易包含所述业务签名、所述业务签名对应的被签名数据的摘要以及用于验证所述业务签名的公钥。

[151] 3）所述业务发起交易包含所述业务签名、所述业务签名对应的被签名数据，所述业务智能合约包含用于验证所述业务签名的公钥。

[152] 4）所述业务发起交易包含所述业务签名、所述业务签名对应的被签名数据的摘要，所述业务智能合约包含用于验证所述业务签名的公钥。

[153] 需要说明的是，区块链虚拟机如果根据所述业务智能合约中的 RSA 签名验证指令触发执行 RSA 签名验证逻辑，那么，在执行过程中所采用的数据传递方式通常是栈传

递。

[154] 此外，区块链虚拟机也可以使用内存传递的方式执行 RSA 签名验证逻辑（预编译合约的方式），即以下的实施例六。

实施例六

[155] 图 7 是本说明书实施例提供的一种基于区块链智能合约的签名验证方法的流程示意图，包括如下步骤：

[156] S700：区块链网络中的节点获得业务发起交易并广播给其他节点。

[157] S702：针对所述区块链网络中的每个节点，该节点在执行所述业务发起交易时，通过区块链虚拟机，调用所述业务智能合约。

[158] S704：该节点通过区块链虚拟机，根据所述业务智能合约中的所述 RSA 签名验证智能合约的合约标识，调用所述 RSA 签名验证智能合约。

[159] S706：该节点通过区块链虚拟机，根据所述 RSA 签名验证智能合约中的 RSA 签名验证指令，触发执行所述 RSA 签名验证逻辑，以对业务签名进行 RSA 签名验证操作，以对业务签名进行 RSA 签名验证操作。

[160] 在本实施例中，需要针对区块链网络进行预先配置，使得：

[161] 1）区块链虚拟机的指令集中包括 RSA 签名验证指令，并且，区块链虚拟机中部署有对应于所述 RSA 签名验证指令的 RSA 签名验证逻辑。

[162] 2）智能合约编译器的指令集中包括所述 RSA 签名验证指令，经所述智能合约编译器编译的业务智能合约中包含 RSA 签名验证智能合约的合约标识，所述 RSA 签名验证智能合约是预先部署于所述区块链网络中的智能合约。

[163] 3）区块链网络中部署有所述业务智能合约。

[164] 实施例六与实施例五的区别主要在于，在实施例六中，区块链虚拟机调用所述业务智能合约之后，当读取到所述 RSA 签名验证智能合约的合约标识时，相当于明确了此时需要进一步调用所述 RSA 签名验证智能合约。区块链虚拟机调用所述 RSA 签名验证智能合约，也会读取所述 RSA 签名验证智能合约中的字节码或二进制码，当读取到所述 RSA 签名验证指令时，相当于明确了此时需要执行 RSA 签名验证操作，因此，区块链虚拟机此时会触发执行预先部署于本地的 RSA 签名验证逻辑，以对业务签名进行 RSA 签名验证操作。

[165] 也就是说，在实施例六中，智能合约编译器在编译业务智能合约时，如果发现业务智能合约中声明调用 RSA 签名验证操作，则不会将这段声明编译为 RSA 签名验证指令，而是编译成所述 RSA 签名验证智能合约的合约标识。这样，区块链虚拟机在调用业务智能合约时，会进一步调用所述 RSA 签名验证智能合约。

[166] 图 8a 是本说明书实施例提供的对应于实施例五的 RSA 签名验证操作的部署示意图。如图 8a 所示，其一，为区块链虚拟机的指令集添加 RSA 签名验证指令，同时，在区块链虚拟机中部署 RSA 签名验证逻辑。其二，为智能合约编译器的指令集添加 RSA 签名验证指令。其三，将经过智能合约编译器编译的业务智能合约（包含 RSA 签名验证指令）部署于区块链网络中。

[167] 图 8b 是本说明书实施例提供的对应于实施例六的 RSA 签名验证操作的部署示意图。如图 8b 所示，其一，为区块链虚拟机的指令集添加 RSA 签名验证指令，同时，在区块链虚拟机中部署 RSA 签名验证逻辑。其二，为智能合约编译器的指令集添加 RSA 签名验证指令。其三，将经过智能合约编译器编译的业务智能合约（包含 RSA 签名验证智能合约的合约标识）部署于区块链网络中。

实施例七

[168] 图 9 是本说明书实施例提供的一种基于区块链智能合约的数据处理方法的流程示意图，包括如下步骤：

[169] S900：区块链网络中的节点获得业务发起交易并广播给其他节点。

[170] S902：针对所述区块链网络中的每个节点，该节点在执行所述业务发起交易时，通过区块链虚拟机，调用所述业务智能合约。

[171] S904：该节点通过区块链虚拟机，根据所述业务智能合约中的 JSON 处理指令，触发执行所述 JSON 处理逻辑，以对待处理数据进行 JSON 处理操作。

[172] 在本实施例中，需要针对区块链网络进行预先配置，使得：

[173] 1）区块链虚拟机的指令集中包括 JSON 处理指令，并且，区块链虚拟机中部署有对应于所述 JSON 处理指令的 JSON 处理逻辑。

[174] 2）智能合约编译器的指令集中包括所述 JSON 处理指令，经所述智能合约编译器编译的业务智能合约中包含所述 JSON 处理指令。

[175] 3）区块链网络中部署有所述业务智能合约。

[176] 所述业务智能合约是需要调用 JSON 处理功能的业务所对应的智能合约。JSON 处理具体包括 JSON 数据解析与 JSON 数据生成。

[177] 在实施例七中，区块链虚拟机调用所述业务智能合约之后，会读取所述业务智能合约中的字节码或二进制码并执行，当读取到所述业务智能合约中的 JSON 处理指令时，相当于明确了此时需要进行 JSON 处理操作，因此，区块链虚拟机此时会触发执行预先部署于本地的 JSON 处理逻辑，以对待处理数据进行 JSON 处理操作。

[178] 在实际应用中，视具体的业务需求的不同，所述待处理数据可以包含于所述业务发起交易中，也可以包含于所述业务智能合约中，还可以是区块链虚拟机执行所述业务发起交易时产生的。

[179] 另外需要说明的是，区块链虚拟机如果根据所述业务智能合约中的 JSON 处理指令触发执行 JSON 处理逻辑，那么，在执行过程中所采用的数据传递方式通常是栈传递（即一般会将 JSON 处理出的数据写入栈中），但是，对于 JSON 处理出的数据而言，其数据长度是不固定的，采用栈传递的方式往往会导致实现较为复杂。

[180] 为此，以下的实施例八提供了另一种基于区块链智能合约的数据处理方法（预编译合约的方式）。

实施例八

[181] 图 10 是本说明书实施例提供的一种基于区块链智能合约的数据处理方法的流程示意图，包括如下步骤：

[182] S1000：区块链网络中的节点获得业务发起交易并广播给其他节点。

[183] S1002：针对所述区块链网络中的每个节点，该节点在执行所述业务发起交易时，通过区块链虚拟机，调用所述业务智能合约。

[184] S1004：该节点通过区块链虚拟机，根据所述业务智能合约中的所述 JSON 处理智能合约的合约标识，调用所述 JSON 处理智能合约。

[185] S1006：该节点通过区块链虚拟机，根据所述 JSON 处理智能合约中的 JSON 处理指令，触发执行所述 JSON 处理逻辑，以对待处理数据进行 JSON 处理操作。

[186] 在本实施例中，需要针对区块链网络进行预先配置，使得：

[187] 1）区块链虚拟机的指令集中包括 JSON 处理指令，并且，区块链虚拟机中部署有对应于所述 JSON 处理指令的 JSON 处理逻辑。

[188] 2）智能合约编译器的指令集中包括所述 JSON 处理指令，经所述智能合约编译器编译的业务智能合约中包含 JSON 处理智能合约的合约标识，所述 JSON 处理智能合约是预先部署于所述区块链网络中的智能合约。

[189] 3）区块链网络中部署有所述业务智能合约。

[190] 实施例八与实施例七的区别主要在于，在实施例八中，区块链虚拟机调用所述业务智能合约之后，当读取到所述 JSON 处理智能合约的合约标识时，相当于明确了此时需要进一步调用所述JSON处理智能合约。区块链虚拟机调用所述JSON处理智能合约，也会读取所述 JSON 处理智能合约中的字节码或二进制码，当读取到所述 JSON 处理指令时，相当于明确了此时需要执行 JSON 处理操作，因此，区块链虚拟机此时会触发执行预先部署于本地的 JSON 处理逻辑，以对待处理数据进行 JSON 处理操作。

[191] 也就是说，在实施例八中，智能合约编译器在编译业务智能合约时，如果发现业务智能合约中声明调用 JSON 处理操作，则不会将这段声明编译为 JSON 处理指令，而是编译成所述 JSON 处理智能合约的合约标识。这样，区块链虚拟机在调用业务智能合约时，会进一步调用所述 JSON 处理智能合约。

[192] 图 11a 是本说明书实施例提供的对应于实施例七的 JSON 处理操作的部署示意图。如图 11a 所示，其一，为区块链虚拟机的指令集添加 JSON 处理指令，同时，在区块链虚拟机中部署 JSON 处理逻辑。其二，为智能合约编译器的指令集添加 JSON 处理指令。其三，将经过智能合约编译器编译的业务智能合约（包含 JSON 处理指令）部署于区块链网络中。

[193] 图 11b 是本说明书实施例提供的对应于实施例八的 JSON 处理操作的部署示意图。如图 11b 所示，其一，为区块链虚拟机的指令集添加 JSON 处理指令，同时，在区块链虚拟机中部署 JSON 处理逻辑。其二，为智能合约编译器的指令集添加 JSON 处理指令。其三，将经过智能合约编译器编译的业务智能合约（包含 JSON 处理智能合约的合约标识）部署于区块链网络中。

实施例九

[194] 图 12 是本说明书实施例提供的一种基于区块链智能合约的数据处理方法的流程示意图，包括如下步骤：

[195] S1200：区块链网络中的节点获得业务发起交易并广播给其他节点。

[196] S1202：针对所述区块链网络中的每个节点，该节点在执行所述业务发起交易时，

通过区块链虚拟机，调用所述业务智能合约。

[197] S1204：该节点通过区块链虚拟机，根据所述业务智能合约中的 XML 处理指令，触发执行所述 XML 处理逻辑，以对待处理数据进行 XML 处理操作。

[198] 在本实施例中，需要针对区块链网络进行预先配置，使得：

[199] 1）区块链虚拟机的指令集中包括 XML 处理指令，并且，区块链虚拟机中部署有对应于所述 XML 处理指令的 XML 处理逻辑。

[200] 2）智能合约编译器的指令集中包括所述 XML 处理指令，经所述智能合约编译器编译的业务智能合约中包含所述 XML 处理指令。

[201] 3）区块链网络中部署有所述业务智能合约。

[202] 所述业务智能合约是需要调用 XML 处理功能的业务所对应的智能合约。XML 处理具体包括 XML 数据解析与 XML 数据生成。

[203] 在实施例九中，区块链虚拟机调用所述业务智能合约之后，会读取所述业务智能合约中的字节码或二进制码并执行，当读取到所述业务智能合约中的 XML 处理指令时，相当于明确了此时需要进行 XML 处理操作，因此，区块链虚拟机此时会触发执行预先部署于本地的 XML 处理逻辑，以对待处理数据进行 XML 处理操作。

[204] 在实际应用中，视具体的业务需求的不同，所述待处理数据可以包含于所述业务发起交易中，也可以包含于所述业务智能合约中，还可以是区块链虚拟机执行所述业务发起交易时产生的。

[205] 另外需要说明的是，区块链虚拟机如果根据所述业务智能合约中的 XML 处理指令触发执行 XML 处理逻辑，那么，在执行过程中所采用的数据传递方式通常是栈传递（即一般会将 XML 处理出的数据写入栈中），但是，对于 XML 处理出的数据而言，其数据长度是不固定的，采用栈传递的方式往往会导致实现较为复杂。

[206] 为此，以下的实施例十提供了另一种基于区块链智能合约的数据处理方法（预编译合约的方式）。

实施例十

[207] 图 13 是本说明书实施例提供的一种基于区块链智能合约的数据处理方法的流程示意图，包括如下步骤：

[208] S1300：区块链网络中的节点获得业务发起交易并广播给其他节点。

[209] S1302：针对所述区块链网络中的每个节点，该节点在执行所述业务发起交易时，通过区块链虚拟机，调用所述业务智能合约。

[210] S1304：该节点通过区块链虚拟机，根据所述业务智能合约中的所述 XML 处理智能合约的合约标识，调用所述 XML 处理智能合约。

[211] S1306：该节点通过区块链虚拟机，根据所述 XML 处理智能合约中的 XML 处理指令，触发执行所述 XML 处理逻辑，以对待处理数据进行 XML 处理操作。

[212] 在本实施例中，需要针对区块链网络进行预先配置，使得：

[213] 1）区块链虚拟机的指令集中包括 XML 处理指令，并且，区块链虚拟机中部署有对应于所述 XML 处理指令的 XML 处理逻辑。

[214] 2）智能合约编译器的指令集中包括所述 XML 处理指令，经所述智能合约编译器编译的业务智能合约中包含 XML 处理智能合约的合约标识，所述 XML 处理智能合约是预先部署于所述区块链网络中的智能合约。

[215] 3）区块链网络中部署有所述业务智能合约。

[216] 实施例十与实施例九的区别主要在于，在实施例十中，区块链虚拟机调用所述业务智能合约之后，当读取到所述 XML 处理智能合约的合约标识时，相当于明确了此时需要进一步调用所述 XML 处理智能合约。区块链虚拟机调用所述 XML 处理智能合约，也会读取所述 XML 处理智能合约中的字节码或二进制码，当读取到所述 XML 处理指令时，相当于明确了此时需要执行 XML 处理操作，因此，区块链虚拟机此时会触发执行预先部署于本地的 XML 处理逻辑，以对待处理数据进行 XML 处理操作。

[217] 也就是说，在实施例十中，智能合约编译器在编译业务智能合约时，如果发现业务智能合约中声明调用 XML 处理操作，则不会将这段声明编译为 XML 处理指令，而是编译成所述 XML 处理智能合约的合约标识。这样，区块链虚拟机在调用业务智能合约时，会进一步调用所述 XML 处理智能合约。

[218] 图 14a 是本说明书实施例提供的对应于实施例九的 XML 处理操作的部署示意图。如图 14a 所示，其一，为区块链虚拟机的指令集添加 XML 处理指令，同时，在区块链虚拟机中部署 XML 处理逻辑。其二，为智能合约编译器的指令集添加 XML 处理指令。其三，将经过智能合约编译器编译的业务智能合约（包含 XML 处理指令）部署于区块链网络中。

[219] 图 14b 是本说明书实施例提供的对应于实施例十的 XML 处理操作的部署示意图。如图 14b 所示，其一，为区块链虚拟机的指令集添加 XML 处理指令，同时，在区块链虚拟机中部署 XML 处理逻辑。其二，为智能合约编译器的指令集添加 XML 处理指令。其三，将经过智能合约编译器编译的业务智能合约（包含 XML 处理智能合约的合约标识）部署于区块链网络中。

实施例十一

[220] 图 15 是本说明书实施例提供的一种基于区块链智能合约的交易哈希获取方法的流程示意图，包括如下步骤:

[221] S1500: 区块链网络中的节点获得业务发起交易并广播给其他节点。

[222] S1502: 针对所述区块链网络中的每个节点，该节点在执行所述业务发起交易时，通过区块链虚拟机，调用所述业务智能合约。

[223] S1504: 该节点通过区块链虚拟机，根据所述业务智能合约中的交易哈希获取指令，触发执行所述交易哈希获取逻辑，以获取所述业务发起交易的交易哈希。

[224] 在本实施例中，需要针对区块链网络进行预先配置，使得:

[225] 1）区块链虚拟机的指令集中包括交易哈希获取指令，并且，区块链虚拟机中部署有对应于所述交易哈希获取指令的交易哈希获取逻辑。

[226] 2）智能合约编译器的指令集中包括所述交易哈希获取指令，经所述智能合约编译器编译的业务智能合约中包含所述交易哈希获取指令。

[227] 3）区块链网络中部署有所述业务智能合约。

[228] 所述业务智能合约是需要调用交易哈希获取功能的业务所对应的智能合约。

[229] 在实施例十一中，区块链虚拟机调用所述业务智能合约之后，会读取所述业务智能合约中的字节码或二进制码并执行，当读取到所述业务智能合约中的交易哈希获取指令时，相当于明确了此时需要进行交易哈希获取操作，因此，区块链虚拟机此时会触发执行预先部署于本地的交易哈希获取逻辑，以对待处理数据进行交易哈希获取操作。

[230] 在实际应用中，针对所述区块链网络中的每个节点，该节点在调用所述业务智能合约之前，初始化区块链虚拟机的上下文，并将所述业务发起交易的交易哈希写入所述上下文中。

[231] 如此，在步骤 S1504 中，具体地，该节点通过区块链虚拟机，根据所述业务智能

合约中的交易哈希获取指令，触发执行所述交易哈希获取逻辑，以从所述上下文中获取所述业务发起交易的交易哈希。

[232] 另外需要说明的是，区块链虚拟机如果根据所述业务智能合约中的交易哈希获取指令触发执行交易哈希获取逻辑，那么，在执行过程中所采用的数据传递方式通常是栈传递。以下的实施例十二提供了另一种基于区块链智能合约的交易哈希获取方法（预编译合约的方式）。

实施例十二

[233] 图 16 是本说明书实施例提供的一种基于区块链智能合约的交易哈希获取方法的流程示意图，包括如下步骤：

[234] S1600：区块链网络中的节点获得业务发起交易并广播给其他节点。

[235] S1602：针对所述区块链网络中的每个节点，该节点在执行所述业务发起交易时，通过区块链虚拟机，调用所述业务智能合约。

[236] S1604：该节点通过区块链虚拟机，根据所述业务智能合约中的所述交易哈希获取智能合约的合约标识，调用所述交易哈希获取智能合约。

[237] S1606：该节点通过区块链虚拟机，根据所述交易哈希获取智能合约中的交易哈希获取指令，触发执行所述交易哈希获取逻辑，以获取所述业务发起交易的交易哈希。

[238] 在本实施例中，需要针对区块链网络进行预先配置，使得：

[239] 1）区块链虚拟机的指令集中包括交易哈希获取指令，并且，区块链虚拟机中部署有对应于所述交易哈希获取指令的交易哈希获取逻辑。

[240] 2）智能合约编译器的指令集中包括所述交易哈希获取指令，经所述智能合约编译器编译的业务智能合约中包含交易哈希获取智能合约的合约标识，所述交易哈希获取智能合约是预先部署于所述区块链网络中的智能合约。

[241] 3）区块链网络中部署所述业务智能合约。

[242] 实施例十二与实施例十一的区别主要在于，在实施例十二中，区块链虚拟机调用所述业务智能合约之后，当读取到所述交易哈希获取智能合约的合约标识时，相当于明确了此时需要进一步调用所述交易哈希获取智能合约。区块链虚拟机调用所述交易哈希获取智能合约，也会读取所述交易哈希获取智能合约中的字节码或二进制码，当读取到所述交易哈希获取指令时，相当于明确了此时需要执行交易哈希获取操作，因此，区块

链虚拟机此时会触发执行预先部署于本地的交易哈希获取逻辑，以获取所述业务发起交易的交易哈希。

[243] 也就是说，在实施例十二中，智能合约编译器在编译业务智能合约时，如果发现业务智能合约中声明调用交易哈希获取操作，则不会将这段声明编译为交易哈希获取指令，而是编译成所述交易哈希获取智能合约的合约标识。这样，区块链虚拟机在调用业务智能合约时，会进一步调用所述交易哈希获取智能合约。

[244] 在实际应用中，针对所述区块链网络中的每个节点，该节点在调用所述业务智能合约之前，初始化区块链虚拟机的上下文，并将所述业务发起交易的交易哈希写入所述上下文中。

[245] 如此，在步骤 S1606 中，具体地，该节点通过区块链虚拟机，根据所述交易哈希获取智能合约中的交易哈希获取指令，触发执行所述交易哈希获取逻辑，以从所述上下文中获取所述业务发起交易的交易哈希。

[246] 图 17a 是本说明书实施例提供的对应于实施例十一的交易哈希获取操作的部署示意图。如图 17a 所示，其一，为区块链虚拟机的指令集添加交易哈希获取指令，同时，在区块链虚拟机中部署交易哈希获取逻辑。其二，为智能合约编译器的指令集添加交易哈希获取指令。其三，将经过智能合约编译器编译的业务智能合约（包含交易哈希获取指令）部署于区块链网络中。

[247] 图 17b 是本说明书实施例提供的对应于实施例十二的交易哈希获取操作的部署示意图。如图 17b 所示，其一，为区块链虚拟机的指令集添加交易哈希获取指令，同时，在区块链虚拟机中部署交易哈希获取逻辑。其二，为智能合约编译器的指令集添加交易哈希获取指令。其三，将经过智能合约编译器编译的业务智能合约（包含交易哈希获取智能合约的合约标识）部署于区块链网络中。

实施例十三

[248] 图 18 是本说明书实施例提供的一种基于区块链智能合约的转账方法的流程示意图，包括如下步骤：

[249] S1800：区块链网络中的节点通过转账外部账户获得转账交易并广播给其他节点。

[250] 即节点接收客户端（登录了转账外部账户）构建并发送的转账交易。

[251] S1802：针对所述区块链网络中的每个节点，该节点在执行所述转账交易时，通过

区块链虚拟机，调用所述业务智能合约并根据所述业务智能合约中的出入校验指令，触发执行所述出入校验逻辑。

[252] S1804：若校验结果为是，则该节点通过区块链虚拟机，执行所述业务智能合约中的用户资产表修改逻辑。

[253] 在以太坊架构中，各外部账户与各用户一一对应，两个用户之间的转账行为实际上就是两个外部账户之间的转账行为。

[254] 假设外部账户 A 想要向外部账户 B 转账，那么，外部账户 A 首先会构建包含转账金额与外部账户 B 的账户地址的转账交易，随后，该转账交易会被广播给区块链网络中的各节点。各节点对转账交易进行验证通过后，执行转账交易，将转账金额写入外部账户 B。

[255] 需要说明的是，各节点对转账交易的验证事项一般包括验证外部账户 A 的余额是否充足，即外部账户 A 的余额是否大于或等于转账金额，若是，则验证通过。这意味着，在现有的以太坊架构中，如果要进行转账，那么转账人的账户余额以及转账金额都会暴露给区块链网络中的各节点。

[256] 在实施例十三中，实际上给出了一种业务需求，即针对区块链网络中的节点之间的一笔转账交易，在不暴露转账用户的资产余额以及转账金额的前提下，判断转账用户的资产余额是否足够支付转账金额。

[257] 为了满足这种业务需求，本申请采用了一种新的转账模型，不再使用区块链网络中的外部账户中的余额进行转账和收账，而是创建业务智能合约，在业务智能合约中重新搭建一个用户的资产体系。在这个资产体系中，不再有资产余额概念，每个用户拥有的资产相当于是一种虚拟物，用户花出一个资产，这个资产就会消失。

[258] 具体地，在区块链网络中部署所述业务智能合约，所述业务智能合约对应有用户资产表，所述用户资产表用于记录每个外部账户（与每个用户一一对应）对应的资产，针对任一资产，该资产为包含加密金额的数据，该加密金额是对该资产的金额进行加密后得到的。

[259] 下表 3 示列性地给出了所述用户资产表。

外部账户 1	资产 1、资产 2
外部账户 2	资产 3、资产 4、资产 5
外部账户 3	资产 6

表 3

[260] 例如，外部账户 1 向外部账户 2 转账 120 元，假设资产 1 的金额为 100 元，资产 2 的金额为 50 元，那么外部账户 1 需要花销掉自己的资产 1 与资产 2，随后，资产 1 与资产 2 消失，产生了资产 7（金额为 120 元）与资产 8（金额为 30 元），外部账户 1 得到资产 8，外部账户 2 得到资产 7。可见，资产 1+资产 2 实际上是这笔转账的输入，资产 7+资产 8 实际上是这笔转账的输出。经过这笔转账后，表 3 会更新为如下所示的表 4。

外部账户 1	资产 8
外部账户 2	资产 3、资产 4、资产 5、资产 7
外部账户 3	资产 6

表 4

[261] 如此，在本申请中，针对一笔转账交易，将验证余额的问题转化成了验证输入输出是否平衡的问题。由于每个资产的金额实际上是加密的，因为不会暴露给区块链虚拟机，这意味着，要求区块链虚拟机在执行转账交易时，采用同态加密算法（如 Pedersen Commitment 算法），校验输入的资产与输出的资产是否相等，如果校验结果为是，就意味着这笔转账交易是可行的（相当于说明了转账人的余额充足）。

[262] 对于具体地实施方式，在本实施例十三中，需要针对区块链网络进行预先配置，使得:

[263] 1）区块链虚拟机的指令集中包括出入校验指令，并且，区块链虚拟机中部署有对应于所述交易哈希获取指令的出入校验逻辑。

[264] 其中，所述出入校验逻辑包括：针对任一转账交易，采用同态加密算法，校验该转账交易指定的转账资产的金额与该转账交易指定的找零资产的金额之和，是否等于该转账交易指定的各花销资产的金额之和。

[265] 还需要说明的是，所述转账交易实际上就是前文所述的业务发起交易，只不过此处的业务具体为加密转账业务。

[266] 2）智能合约编译器的指令集中包括所述出入校验指令，经所述智能合约编译器编

译的业务智能合约中包含所述出入校验指令。

[267] 3）区块链网络中部署有所述业务智能合约。

[268] 所述业务智能合约是用于实现隐藏转账金额和资产余额的转账功能的智能合约。

[269] 在步骤 S1800 中，节点实际上是指转账用户对应的节点。转账外部账户实际上是指转账用户所控制的外部账户。

[270] 节点通过转账外部账户获得转账交易，实际上是转账用户登录客户端（或称“钱包”），构建转账交易并发送给节点。

[271] 所述转账交易中包括转账资产、找零资产和至少一个花销资产。其中，所述至少一个花销资产实际上就是输入到这笔转账的资产，转账资产与找零资产实际上就是这笔转账输出的资产。

[272] 在实施例十三中，区块链虚拟机调用所述业务智能合约之后，会读取所述业务智能合约中的字节码或二进制码并执行，当读取到所述业务智能合约中的出入校验指令时，相当于明确了此时需要进行出入校验操作，因此，区块链虚拟机此时会触发执行预先部署于本地的出入校验逻辑，以便采用同态加密算法，校验所述转账资产的金额与所述找零资产的金额之和是否等于各花销资产的金额之和。

[273] 如果校验结果为是，则说明这笔转账交易是可行的。进而，区块链虚拟机需要执行这笔转账交易，即根据转账交易修改用户资产表。修改用户资产表的用户资产表修改逻辑实际上是预先写入到业务智能合约中的。用户资产表修改逻辑为，解除所述转账外部账户与各花销资产的对应关系，建立所述转账外部账户与所述找零资产的对应关系，并建立收账外部账户与所述转账资产的对应关系。

[274] 此外，在实际应用中，为了防止出现如下情况：某些恶意用户在发起转账交易时，将转账交易中包含的转账资产的实际金额设置为负数，以转账的方式偷取他人的资产；以及，用户在发起转账交易操作失误，将转账交易中包含的找零资产的实际金额设置为负数，导致用户实际转出的资产的金额大于转账资产的金额，可以采用零知识证明的方法，在转账资产的实际金额与找零资产的实际金额都不可见的情况下，校验转账资产的实际金额与找零资产的实际金额是否皆落入指定数值范围，如（$0,2^{64}$]。如果校验结果为是，就排除了以上情况发生的可能性。

[275] 具体地，在实施例十三中，可以进一步针对区块链网络进行预先配置，使得：

[276] 4）区块链虚拟机的指令集中还包括金额校验指令，并且，区块链虚拟机中还部署有对应于所述金额校验指令的金额校验逻辑。

[277] 5）所述智能合约编译器的指令集中还包括所述金额校验指令，经所述智能合约编译器编译的业务智能合约中还包含所述金额校验指令。

[278] 基于此，用户发起的转账交易中还需要包括用于实现零知识证明的证明相关数据（如 Bullet Proof、Borromean 环签名等）。

[279] 区块链虚拟机在读取到所述业务智能合约中的金额校验指令时，会触发执行本地预先部署的金额校验逻辑，即根据所述证明相关数据，校验所述转账资产的金额与所述找零资产的金额是否皆落入指定数值范围。

[280] 另外，在实施例十三中，业务智能合约中还可以包含花销资产校验逻辑，使得区块链虚拟机在执行业务智能合约时，还可以根据所述用户资产表，校验所述转账外部账户对应的资产中是否包括各花销资产。如果校验结果为是，说明转账用户所要使用的花销资产是自己拥有的资产。

[281] 此外，针对任一资产，该资产的数据结构还可以包括表征该资产已花销或未花销的第一状态参数。业务智能合约中还可以包括第一状态参数相关逻辑，以便区块链虚拟机在执行业务智能合约时，针对转账交易中的每个花销资产，该花销资产包括的第一状态参数，校验该花销资产是否未花销。并且，所述第一状态参数相关逻辑还包括：如果最终针对所述转账交易的全部校验的结果皆为是，那么，对该花销资产包括的第一状态参数进行修改，使得修改后的该第一状态参数表征该花销资产已花销。如果最终针对所述转账交易的全部校验的结果中有任一结果为否，则转账交易会失败，各花销资产并没有被花销出去，自然没必要对第一状态参数进行修改。

[282] 还有，针对任一资产，该资产的数据结构还可以包括表征该资产存在或不存在的第二状态参数。业务智能合约中还可以包括第二状态参数相关逻辑，以便区块链虚拟机在执行业务智能合约时，针对所述转账交易中的每个花销资产，根据该花销资产包括的第二状态参数，校验该花销资产是否存在。这样，可以有效防止恶意用户虚构并不存在的资产并使用虚构的资产来进行转账。

[283] 另外需要说明的是，区块链虚拟机如果根据所述业务智能合约中的出入校验指令与金额校验指令触发执行出入校验逻辑与金额校验逻辑，那么，在执行过程中所采用的数据传递方式通常是栈传递。以下的实施例十四提供了另一种基于区块链智能合约的转

账方法（预编译合约的方式）。

实施例十四

[284] 图 19 是本说明书实施例提供的一种基于区块链智能合约的交易哈希获取方法的流程示意图，包括如下步骤：

[285] S1900：区块链网络中的节点通过转账外部账户获得转账交易并广播给其他节点。

[286] S1902：针对所述区块链网络中的每个节点，该节点在执行所述转账交易时，通过区块链虚拟机，调用所述业务智能合约，并根据所述业务智能合约中的所述出入校验智能合约的合约标识，调用所述出入校验智能合约。

[287] S1904：该节点根据所述出入校验智能合约中的出入校验指令，触发执行所述出入校验逻辑。

[288] S1906：若校验结果为是，则该节点通过区块链虚拟机，执行所述业务智能合约中的用户资产表修改逻辑。

[289] 在实施例十四中，需要针对区块链网络进行预先配置，使得：

[290] 1）区块链虚拟机的指令集中包括交易哈希获取指令，并且，区块链虚拟机中部署有对应于所述交易哈希获取指令的交易哈希获取逻辑。

[291] 2）智能合约编译器的指令集中包括所述出入校验指令，经所述智能合约编译器编译的业务智能合约中包含出入校验智能合约的合约标识，所述出入校验智能合约是预先部署于所述区块链网络中的智能合约。

[292] 3）区块链网络中部署有所述业务智能合约。

[293] 实施例十四与实施例十三的区别主要在于，在实施例十四中，区块链虚拟机调用所述业务智能合约之后，当读取到所述出入校验智能合约的合约标识时，相当于明确了此时需要进一步调用所述出入校验智能合约。区块链虚拟机调用所述出入校验智能合约，也会读取所述出入校验智能合约中的字节码或二进制码，当读取到所述出入校验指令时，相当于明确了此时需要执行出入校验操作，因此，区块链虚拟机此时会触发执行预先部署于本地的出入校验逻辑。

[294] 也就是说，在实施例十四中，智能合约编译器在编译业务智能合约时，如果发现业务智能合约中声明调用出入校验操作，则不会将这段声明编译为出入校验指令，而是编译成所述所述出入校验智能合约的合约标识。这样，区块链虚拟机在调用业务智能合

约时，会进一步调用所述出入校验智能合约。

[295] 进一步地，在实施例十四中，需要针对区块链网络进行预先配置，使得：

[296] 4）区块链虚拟机的指令集中还包括金额校验指令，并且，区块链虚拟机中还部署有对应于所述金额校验指令的金额校验逻辑。

[297] 5）所述智能合约编译器的指令集中还包括所述金额校验指令，经所述智能合约编译器编译的业务智能合约中还包含所述金额校验智能合约的合约标识，所述金额校验智能合约是预先部署于所述区块链网络中的智能合约。

[298] 如此，在实施例十四中，针对所述区块链网络中的每个节点，该节点通过区块链虚拟机，根据所述业务智能合约中的所述金额校验智能合约的合约标识，调用所述金额校验智能合约；该节点根据所述金额校验智能合约中的金额校验指令，触发执行所述金额校验逻辑，以便根据所述证明相关数据，校验所述转账资产的金额与所述找零资产的金额是否皆落入指定数值范围。

[299] 此外需要说明的是，在实施例十四中，执行的校验事项与实施例十三中的一致，只不过，对于出入校验与金额校验，是通过调用预编译合约（即出入校验智能合约与金额校验智能合约）的方式进行的。

[300] 在实施例十三与实施例十四中，针对转账交易进行的校验事项有多个时，当全部校验结果都为是时，区块链虚拟机才会执行用户资产表修改逻辑。

[301] 图 20a 是本说明书实施例提供的对应于实施例十三的转账交易的相关校验操作的部署示意图。如图 20a 所示，其一，为区块链虚拟机的指令集添加出入校验指令与金额校验指令，同时，在区块链虚拟机中部署出入校验逻辑与金额校验逻辑。其二，为智能合约编译器的指令集添加出入校验指令与金额校验指令。其三，将经过智能合约编译器编译的业务智能合约（包含出入校验指令与金额校验指令）部署于区块链网络中。

[302] 图 20b 是本说明书实施例提供的对应于实施例十四的转账交易的相关校验操作的部署示意图。如图 20b 所示，其一，为区块链虚拟机的指令集添加出入校验指令与金额校验指令，同时，在区块链虚拟机中部署出入校验逻辑与金额校验逻辑。其二，为智能合约编译器的指令集添加出入校验指令与金额校验指令。其三，将经过智能合约编译器编译的业务智能合约（包含出入校验智能合约的合约标识与金额校验智能合约的合约标识）部署于区块链网络中。

[303] 以上，是分别对实施例一至实施例十四的解释说明。实际上，在实际应用中，业

务发起交易具体可以是转账交易，而为了实现转账交易，可能不仅需要进行相关校验（如实施例十三中提及的各项校验），还需要进行 BASE54 编码操作、BASE54 解码操作、RSA 签名验证操作、JSON 处理操作、XML 处理操作、交易哈希获取操作中的一种或多种。

[304] 也就是说，可以将上述的 BASE64 编码方法、BASE64 解码方法、RSA 签名验证方法、JSON 处理方法、XML 处理方法以及交易哈希获取方法中的一种或多种应用于实施例十三或实施例十四中的转账方法中，此时，前文所述业务发起交易就是转账交易。

[305] 此外需要说明的是，在本说明书的各实施例中，如果业务智能合约不是所述区块链网络中唯一的智能合约，那么，业务发起交易（以及转账交易）中还需要包含业务智能合约的合约标识，以便区块链虚拟机根据所述业务发起交易（以及转账交易）中包括的合约标识，调用对应的业务智能合约。

[306] 还有，对于本说明书中的各实施例，所述区块链虚拟机的指令集中还包括至少一个以太坊指令，以太坊指令是以太坊虚拟机的指令集中的指令；针对所述区块链虚拟机的指令集中包括的每个以太坊指令，所述区块链虚拟机中部署有对应于该以太坊指令的相关逻辑。所述智能合约编译器的指令集中还包括至少一个以太坊指令，以太坊指令是以太坊虚拟机的指令集中的指令。也就是说，本申请中的区块链虚拟机可以是在以太坊虚拟机的基础上扩展得到的，本申请中的智能合约编译器可以是在以太坊的智能合约编译器的基础上扩展得到的。

[307] 本说明书提供的一种区块链系统，包括区块链网络；

[308] 其中，区块链虚拟机的指令集中包括出入校验指令，并且，区块链虚拟机中部署有对应于所述出入校验指令的出入校验逻辑；智能合约编译器的指令集中包括所述出入校验指令，经所述智能合约编译器编译的业务智能合约中包含所述出入校验指令；区块链网络中部署有所述业务智能合约，所述业务智能合约对应有用户资产表，所述用户资产表用于记录每个外部账户对应的资产，针对任一资产，该资产为包含加密金额的数据，该加密金额是对该资产的金额进行加密后得到的；

[309] 所述区块链网络中的节点，通过转账外部账户获得转账交易并广播给其他节点；所述转账交易包括转账资产、找零资产和至少一个花销资产；

[310] 所述区块链网络中的每个节点，在执行所述转账交易时，通过区块链虚拟机，调用所述业务智能合约并根据所述业务智能合约中的出入校验指令，触发执行所述出入校

验逻辑，以便采用同态加密算法，校验所述转账资产的金额与所述找零资产的金额之和是否等于各花销资产的金额之和；若校验结果为是，则通过区块链虚拟机，执行所述业务智能合约中的用户资产表修改逻辑，以便解除所述转账外部账户与各花销资产的对应关系，建立所述转账外部账户与所述找零资产的对应关系，并建立收账外部账户与所述转账资产的对应关系。

[311] 本说明书提供的一种区块链系统，包括区块链网络；

[312] 其中，区块链虚拟机的指令集中包括出入校验指令，并且，区块链虚拟机中部署有对应于所述出入校验指令的出入校验逻辑；智能合约编译器的指令集中包括所述出入校验指令，经所述智能合约编译器编译的业务智能合约中包含出入校验智能合约的合约标识，所述出入校验智能合约是预先部署于所述区块链网络中的智能合约；区块链网络中部署有所述业务智能合约，所述业务智能合约对应有用户资产表，所述用户资产表用于记录每个外部账户对应的资产，针对任一资产，该资产为包含加密金额的数据，该加密金额是对该资产的金额进行加密后得到的；

[313] 所述区块链网络中的节点，通过转账外部账户获得转账交易并广播给其他节点；所述转账交易包括转账资产、找零资产和至少一个花销资产；

[314] 所述区块链网络中的每个节点，在执行所述转账交易时，通过区块链虚拟机，调用所述业务智能合约，并根据所述业务智能合约中的所述出入校验智能合约的合约标识，调用所述出入校验智能合约；根据所述出入校验智能合约中的出入校验指令，触发执行所述出入校验逻辑，以便采用同态加密算法，校验所述转账资产的金额与所述找零资产的金额之和是否等于各花销资产的金额之和；若校验结果为是，则通过区块链虚拟机，执行所述业务智能合约中的用户资产表修改逻辑，以便解除所述转账外部账户与各花销资产的对应关系，建立所述转账外部账户与所述找零资产的对应关系，并建立收账外部账户与所述转账资产的对应关系。

[315] 本说明书提供的一种区块链系统，包括区块链网络；

[316] 其中，区块链虚拟机的指令集中包括 BASE64 编码指令，并且，区块链虚拟机中部署有对应于所述 BASE64 编码指令的 BASE64 编码逻辑；智能合约编译器的指令集中包括所述 BASE64 编码指令，经所述智能合约编译器编译的业务智能合约中包含所述 BASE64 编码指令；区块链网络中部署有所述业务智能合约；

[317] 所述区块链网络中的节点，获得业务发起交易并广播给其他节点；

[318] 所述区块链网络中的每个节点，在执行所述业务发起交易时，通过区块链虚拟机，调用所述业务智能合约；通过区块链虚拟机，根据所述业务智能合约中的 BASE64 编码指令，触发执行所述 BASE64 编码逻辑，以对待编码数据进行编码操作。

[319] 本说明书提供的一种区块链系统，包括区块链网络；

[320] 其中，区块链虚拟机的指令集中包括 BASE64 编码指令，并且，区块链虚拟机中部署有对应于所述 BASE64 编码指令的 BASE64 编码逻辑；智能合约编译器的指令集中包括所述 BASE64 编码指令，经所述智能合约编译器编译的业务智能合约中包含 BASE64 编码智能合约的合约标识，所述 BASE64 编码智能合约是预先部署于所述区块链网络中的智能合约；所述区块链网络中部署有所述业务智能合约；

[321] 所述区块链网络中的节点，获得业务发起交易并广播给其他节点；

[322] 所述区块链网络中的每个节点，在执行所述业务发起交易时，通过区块链虚拟机，调用所述业务智能合约；通过区块链虚拟机，根据所述业务智能合约中的所述 BASE64 编码智能合约的合约标识，调用所述 BASE64 编码智能合约；通过区块链虚拟机，根据所述 BASE64 编码智能合约中的，BASE64 编码指令，触发执行所述 BASE64 编码逻辑，以对待编码数据进行编码操作。

[323] 本说明书提供的一种区块链系统，包括区块链网络；

[324] 其中，区块链虚拟机的指令集中包括 BASE64 解码指令，并且，区块链虚拟机中部署有对应于所述 BASE64 解码指令的 BASE64 解码逻辑；智能合约编译器的指令集中包括所述 BASE64 解码指令，经所述智能合约编译器编译的业务智能合约中包含所述 BASE64 解码指令；区块链网络中部署有所述业务智能合约；

[325] 所述区块链网络中的节点，获得业务发起交易并广播给其他节点；

[326] 所述区块链网络中的每个节点，在执行所述业务发起交易时，通过区块链虚拟机，调用所述业务智能合约；通过区块链虚拟机，根据所述业务智能合约中的 BASE64 解码指令，触发执行所述 BASE64 解码逻辑，以对待解码数据进行解码操作。

[327] 本说明书提供的一种区块链系统，包括区块链网络；

[328] 其中，区块链虚拟机的指令集中包括 BASE64 解码指令，并且，区块链虚拟机中部署有对应于所述 BASE64 解码指令的 BASE64 解码逻辑；智能合约编译器的指令集中包括所述 BASE64 解码指令，经所述智能合约编译器编译的业务智能合约中包含

BASE64 解码智能合约的合约标识，所述 BASE64 解码智能合约是预先部署于所述区块链网络中的智能合约；所述区块链网络中部署有所述业务智能合约；

[329] 所述区块链网络中的节点，获得业务发起交易并广播给其他节点；

[330] 所述区块链网络中的每个节点，该节点在执行所述业务发起交易时，通过区块链虚拟机，调用所述业务智能合约；通过区块链虚拟机，根据所述业务智能合约中的所述 BASE64 解码智能合约的合约标识，调用所述 BASE64 解码智能合约；通过区块链虚拟机，根据所述 BASE64 解码智能合约中的，BASE64 解码指令，触发执行所述 BASE64 解码逻辑，以对待解码数据进行解码操作。

[331] 本说明书提供的一种区块链系统，包括区块链网络；

[332] 其中，区块链虚拟机的指令集中包括 RSA 签名验证指令，并且，区块链虚拟机中部署有对应于所述 RSA 签名验证指令的 RSA 签名验证逻辑；智能合约编译器的指令集中包括所述 RSA 签名验证指令，经所述智能合约编译器编译的业务智能合约中包含所述 RSA 签名验证指令；区块链网络中部署有所述业务智能合约；

[333] 所述区块链网络中的节点，获得业务发起交易并广播给其他节点；

[334] 所述区块链网络中的每个节点，在执行所述业务发起交易时，通过区块链虚拟机，调用所述业务智能合约；通过区块链虚拟机，根据所述业务智能合约中的 RSA 签名验证指令，触发执行所述 RSA 签名验证逻辑，以对业务签名进行 RSA 签名验证操作，以对业务签名进行 RSA 签名验证操作。

[335] 本说明书提供的一种区块链系统，包括区块链网络；

[336] 其中，区块链虚拟机的指令集中包括 RSA 签名验证指令，并且，区块链虚拟机中部署有对应于所述 RSA 签名验证指令的 RSA 签名验证逻辑；智能合约编译器的指令集中包括所述 RSA 签名验证指令，经所述智能合约编译器编译的业务智能合约中包含所述 RSA 签名验证智能合约的合约标识，所述 RSA 签名验证智能合约是预先部署于所述区块链网络中的智能合约；区块链网络中部署有所述业务智能合约；

[337] 所述区块链网络中的节点，获得业务发起交易并广播给其他节点；

[338] 所述区块链网络中的每个节点，在执行所述业务发起交易时，通过区块链虚拟机，调用所述业务智能合约；通过区块链虚拟机，根据所述业务智能合约中的所述 RSA 签名验证智能合约的合约标识，调用所述 RSA 签名验证智能合约；通过区块链虚拟机，

根据所述 RSA 签名验证智能合约中的 RSA 签名验证指令，触发执行所述 RSA 签名验证逻辑，以对业务签名进行 RSA 签名验证操作，以对业务签名进行 RSA 签名验证操作。

[339] 本说明书提供的一种区块链系统，包括区块链网络；

[340] 其中，区块链虚拟机的指令集中包括 JSON 处理指令，并且，区块链虚拟机中部署有对应于所述 JSON 处理指令的 JSON 处理逻辑；智能合约编译器的指令集中包括所述 JSON 处理指令，经所述智能合约编译器编译的业务智能合约中包含所述 JSON 处理指令；区块链网络中部署有所述业务智能合约；

[341] 所述区块链网络中的节点，获得业务发起交易并广播给其他节点；

[342] 所述区块链网络中的每个节点，在执行所述业务发起交易时，通过区块链虚拟机，调用所述业务智能合约；通过区块链虚拟机，根据所述业务智能合约中的 JSON 处理指令，触发执行所述 JSON 处理逻辑，以对待处理数据进行 JSON 处理操作。

[343] 本说明书提供的一种区块链系统，包括区块链网络；

[344] 其中，区块链虚拟机的指令集中包括 JSON 处理指令，并且，区块链虚拟机中部署有对应于所述 JSON 处理指令的 JSON 处理逻辑；智能合约编译器的指令集中包括所述 JSON 处理指令，经所述智能合约编译器编译的业务智能合约中包含 JSON 处理智能合约的合约标识，所述 JSON 处理智能合约是预先部署于所述区块链网络中的智能合约；区块链网络中部署有所述 JSON 处理智能合约与所述业务智能合约；

[345] 所述区块链网络中的节点，获得业务发起交易并广播给其他节点；

[346] 所述区块链网络中的每个节点，在执行所述业务发起交易时，通过区块链虚拟机，调用所述业务智能合约；通过区块链虚拟机，根据所述业务智能合约中的所述 JSON 处理智能合约的合约标识，调用所述 JSON 处理智能合约；通过区块链虚拟机，根据所述 JSON 处理智能合约中的 JSON 处理指令，触发执行所述 JSON 处理逻辑，以对待处理数据进行 JSON 处理操作。

[347] 本说明书提供的一种区块链系统，包括区块链网络；

[348] 其中，区块链虚拟机的指令集中包括 XML 处理指令，并且，区块链虚拟机中部署有对应于所述 XML 处理指令的 XML 处理逻辑；智能合约编译器的指令集中包括所述 XML 处理指令，经所述智能合约编译器编译的业务智能合约中包含所述 XML 处理指令；区块链网络中部署有所述业务智能合约；

[349] 所述区块链网络中的节点，获得业务发起交易并广播给其他节点；

[350] 所述区块链网络中的每个节点，在执行所述业务发起交易时，通过区块链虚拟机，调用所述业务智能合约；通过区块链虚拟机，根据所述业务智能合约中的 XML 处理指令，触发执行所述 XML 处理逻辑，以对待处理数据进行 XML 处理操作。

[351] 本说明书提供的一种区块链系统，包括区块链网络；

[352] 其中，区块链虚拟机的指令集中包括 XML 处理指令，并且，区块链虚拟机中部署有对应于所述 XML 处理指令的 XML 处理逻辑；智能合约编译器的指令集中包括所述 XML 处理指令，经所述智能合约编译器编译的业务智能合约中包含 XML 处理智能合约的合约标识，所述 XML 处理智能合约是预先部署于所述区块链网络中的智能合约；区块链网络中部署有所述 XML 处理智能合约与所述业务智能合约；

[353] 所述区块链网络中的节点，获得业务发起交易并广播给其他节点；

[354] 所述区块链网络中的每个节点，在执行所述业务发起交易时，通过区块链虚拟机，调用所述业务智能合约；通过区块链虚拟机，根据所述业务智能合约中的所述 XML 处理智能合约的合约标识，调用所述 XML 处理智能合约；通过区块链虚拟机，根据所述 XML 处理智能合约中的 XML 处理指令，触发执行所述 XML 处理逻辑，以对待处理数据进行 XML 处理操作。

[355] 本说明书提供的一种区块链系统，包括区块链网络；

[356] 其中，区块链虚拟机的指令集中包括交易哈希获取指令，并且，区块链虚拟机中部署有对应于所述交易哈希获取指令的交易哈希获取逻辑；智能合约编译器的指令集中包括所述交易哈希获取指令，经所述智能合约编译器编译的业务智能合约中包含所述交易哈希获取指令；区块链网络中部署有所述业务智能合约；

[357] 所述区块链网络中的节点，获得业务发起交易并广播给其他节点；

[358] 所述区块链网络中的每个节点，在执行所述业务发起交易时，通过区块链虚拟机，调用所述业务智能合约；通过区块链虚拟机，根据所述业务智能合约中的交易哈希获取指令，触发执行所述交易哈希获取逻辑，以获取所述业务发起交易的交易哈希。

[359] 本说明书提供的一种区块链系统，包括区块链网络；

[360] 其中，区块链虚拟机的指令集中包括交易哈希获取指令，并且，区块链虚拟机中部署有对应于所述交易哈希获取指令的交易哈希获取逻辑；智能合约编译器的指令集中

包括所述交易哈希获取指令，经所述智能合约编译器编译的业务智能合约中包含交易哈希获取智能合约的合约标识，所述交易哈希获取智能合约是预先部署于所述区块链网络中的智能合约；区块链网络中部署有所述交易哈希获取智能合约与所述业务智能合约；

[361] 所述区块链网络中的节点，获得业务发起交易并广播给其他节点；

[362] 所述区块链网络中的每个节点，在执行所述业务发起交易时，通过区块链虚拟机，调用所述业务智能合约；通过区块链虚拟机，根据所述业务智能合约中的所述交易哈希获取智能合约的合约标识，调用所述交易哈希获取智能合约；通过区块链虚拟机，根据所述交易哈希获取智能合约中的交易哈希获取指令，触发执行所述交易哈希获取逻辑，以获取所述业务发起交易的交易哈希。

[363] 图 21 示出了本说明书实施例所提供的一种区块链系统的结构示意图。

[364] 本说明书还提供一种计算机设备，其至少包括存储器、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，其中，处理器执行所述程序时实现本文各实施例的方法以及各实施例中至少两个实施例组合后的方法的功能。

[365] 图 22 示出了本说明书实施例所提供的一种更为具体的计算设备硬件结构示意图，该设备可以包括：处理器 2210、存储器 2220、输入/输出接口 2230、通信接口 2240 和总线 2250。其中处理器 2210、存储器 2220、输入/输出接口 2230 和通信接口 2240 通过总线 2250 实现彼此之间在设备内部的通信连接。

[366] 处理器 2210 可以采用通用的 CPU（Central Processing Unit，中央处理器）、微处理器、应用专用集成电路（Application Specific Integrated Circuit，ASIC）、或者一个或多个集成电路等方式实现，用于执行相关程序，以实现本说明书实施例所提供的技术方案。

[367] 存储器 2220 可以采用 ROM（Read Only Memory，只读存储器）、RAM（Random Access Memory，随机存取存储器）、静态存储设备，动态存储设备等形式实现。存储器 2220 可以存储操作系统和其他应用程序，在通过软件或者固件来实现本说明书实施例所提供的技术方案时，相关的程序代码保存在存储器 2220 中，并由处理器 2210 来调用执行。

[368] 输入/输出接口 2230 用于连接输入/输出模块，以实现信息输入及输出。输入输出/模块可以作为组件配置在设备中（图中未示出），也可以外接于设备以提供相应功能。其中输入设备可以包括键盘、鼠标、触摸屏、麦克风、各类传感器等，输出设备可以包

括显示器、扬声器、振动器、指示灯等。

[369] 通信接口 2240 用于连接通信模块（图中未示出），以实现本设备与其他设备的通信交互。其中通信模块可以通过有线方式（例如 USB、网线等）实现通信，也可以通过无线方式（例如移动网络、WIFI、蓝牙等）实现通信。

[370] 总线 2250 包括一通路，在设备的各个组件（例如处理器 2210 存储器 2220、输入/输出接口 2230 和通信接口 2240）之间传输信息。

[371] 需要说明的是，尽管上述设备仅示出了处理器 2210、存储器 2220、输入/输出接口 2230、通信接口 2240 以及总线 2250，但是在具体实施过程中，该设备还可以包括实现正常运行所必需的其他组件。此外，本领域的技术人员可以理解的是，上述设备中也可以仅包含实现本说明书实施例方案所必需的组件，而不必包含图中所示的全部组件。

[372] 本说明书实施例还提供一种计算机可读存储介质，其上存储有计算机程序，该程序被处理器执行时实现本文各实施例的方法以及各实施例中至少两个实施例组合后的方法的功能。

[373] 计算机可读介质包括永久性和非永久性、可移动和非可移动媒体可以由任何方法或技术来实现信息存储。信息可以是计算机可读指令、数据结构、程序的模块或其他数据。计算机的存储介质的例子包括，但不限于相变内存（PRAM）、静态随机存取存储器（SRAM）、动态随机存取存储器（DRAM）、其他类型的随机存取存储器（RAM）、只读存储器（ROM）、电可擦除可编程只读存储器（EEPROM）、快闪记忆体或其他内存技术、只读光盘只读存储器（CD-ROM）、数字多功能光盘（DVD）或其他光学存储、磁盒式磁带，磁带磁磁盘存储或其他磁性存储设备或任何其他非传输介质，可用于存储可以被计算设备访问的信息。按照本文中的界定，计算机可读介质不包括暂存电脑可读媒体（transitory media），如调制的数据信号和载波。

[374] 通过以上的实施方式的描述可知，本领域的技术人员可以清楚地了解到本说明书实施例可借助软件加必需的通用硬件平台的方式来实现。基于这样的理解，本说明书实施例的技术方案本质上或者说对现有技术做出贡献的部分可以以软件产品的形式体现出来，该计算机软件产品可以存储在存储介质中，如 ROM/RAM、磁碟、光盘等，包括若干指令用以使得一台计算机设备（可以是个人计算机，服务器，或者网络设备等）执行本说明书实施例各个实施例或者实施例的某些部分所述的方法。

[375] 上述实施例阐明的系统、方法、模块或单元，具体可以由计算机芯片或实体实现，

或者由具有某种功能的产品来实现。一种典型的实现设备为计算机，计算机的具体形式可以是个人计算机、膝上型计算机、蜂窝电话、相机电话、智能电话、个人数字助理、媒体播放器、导航设备、电子邮件收发设备、游戏控制台、平板计算机、可穿戴设备或者这些设备中的任意几种设备的组合。

[376] 本说明书中的各个实施例均采用递进的方式描述，各个实施例之间相同相似的部分互相参见即可，每个实施例重点说明的都是与其他实施例的不同之处。尤其，对于装置和设备实施例而言，由于其基本相似于方法实施例，所以描述得比较简单，相关之处参见方法实施例的部分说明即可。以上所描述的方法实施例仅仅是示意性的，其中所述作为分离部件说明的模块可以是或者也可以不是物理上分开的，在实施本说明书实施例方案时可以把各模块的功能在同一个或多个软件和/或硬件中实现。也可以根据实际的需要选择其中的部分或者全部模块来实现本实施例方案的目的。本领域普通技术人员在不付出创造性劳动的情况下，即可以理解并实施。

[377] 以上所述仅是本说明书实施例的具体实施方式，应当指出，对于本技术领域的普通技术人员来说，在不脱离本说明书实施例原理的前提下，还可以做出若干改进和润饰，这些改进和润饰也应视为本说明书实施例的保护范围。

权利要求书

1、一种基于区块链智能合约的签名验证方法，区块链虚拟机的指令集中包括 RSA 签名验证指令，并且，区块链虚拟机中部署有对应于所述 RSA 签名验证指令的 RSA 签名验证逻辑；

智能合约编译器的指令集中包括所述 RSA 签名验证指令，经所述智能合约编译器编译的业务智能合约中包含所述 RSA 签名验证指令；

区块链网络中部署有所述业务智能合约；

所述签名验证方法包括：

所述区块链网络中的节点获得业务发起交易并广播给其他节点；

针对所述区块链网络中的每个节点，该节点在执行所述业务发起交易时，通过区块链虚拟机，调用所述业务智能合约；

该节点通过区块链虚拟机，根据所述业务智能合约中的 RSA 签名验证指令，触发执行所述 RSA 签名验证逻辑，以对业务签名进行 RSA 签名验证操作。

2、如权利要求 1 所述的方法，所述业务发起交易包含所述业务签名、所述业务签名对应的被签名数据以及用于验证所述业务签名的公钥；或，

所述业务发起交易包含所述业务签名、所述业务签名对应的被签名数据的摘要以及用于验证所述业务签名的公钥；或，

所述业务发起交易包含所述业务签名、所述业务签名对应的被签名数据，所述业务智能合约包含用于验证所述业务签名的公钥；或，

所述业务发起交易包含所述业务签名、所述业务签名对应的被签名数据的摘要，所述业务智能合约包含用于验证所述业务签名的公钥。

3、一种基于区块链智能合约的签名验证方法，区块链虚拟机的指令集中包括 RSA 签名验证指令，并且，区块链虚拟机中部署有对应于所述 RSA 签名验证指令的 RSA 签名验证逻辑；

智能合约编译器的指令集中包括所述 RSA 签名验证指令，经所述智能合约编译器编译的业务智能合约中包含 RSA 签名验证智能合约的合约标识，所述 RSA 签名验证智能合约是预先部署于区块链网络中的智能合约；

区块链网络中部署有所述业务智能合约；

所述签名验证方法包括：

所述区块链网络中的节点获得业务发起交易并广播给其他节点；

针对所述区块链网络中的每个节点，该节点在执行所述业务发起交易时，通过区块

链虚拟机，调用所述业务智能合约；

该节点通过区块链虚拟机，根据所述业务智能合约中的所述 RSA 签名验证智能合约的合约标识，调用所述 RSA 签名验证智能合约；

该节点通过区块链虚拟机，根据所述 RSA 签名验证智能合约中的 RSA 签名验证指令，触发执行所述 RSA 签名验证逻辑，以对业务签名进行 RSA 签名验证操作，以对业务签名进行 RSA 签名验证操作。

4、一种区块链虚拟机，用于实现权利要求 1~3 任一项所述的方法，其中，

智能合约编译器的指令集中包括所述 RSA 签名验证指令，经所述智能合约编译器编译的业务智能合约中包含所述 RSA 签名验证指令。

5、如权利要求 4 所述的区块链虚拟机，所述区块链虚拟机的指令集中还包括至少一个以太坊指令，以太坊指令是以太坊虚拟机的指令集中的指令；

针对所述区块链虚拟机的指令集中包括的每个以太坊指令，所述区块链虚拟机中部署有对应于该以太坊指令的相关逻辑。

6、一种智能合约编译器，用于实现权利要求 1 所述的方法，其中，

智能合约编译器的指令集中包括所述 RSA 签名验证指令，经所述智能合约编译器编译的业务智能合约中包含所述 RSA 签名验证指令。

7、如权利要求 6 所述的智能合约编译器，所述智能合约编译器的指令集中还包括至少一个以太坊指令，以太坊指令是以太坊虚拟机的指令集中的指令。

8、一种智能合约编译器，用于实现权利要求 3 所述的方法，其中，

智能合约编译器的指令集中包括所述 RSA 签名验证指令，经所述智能合约编译器编译的业务智能合约中包含 RSA 签名验证智能合约的合约标识，所述 RSA 签名验证智能合约是预先部署于区块链网络中的智能合约。

9、一种区块链系统，包括区块链网络，其中，

区块链虚拟机的指令集中包括 RSA 签名验证指令，并且，区块链虚拟机中部署有对应于所述 RSA 签名验证指令的 RSA 签名验证逻辑；智能合约编译器的指令集中包括所述 RSA 签名验证指令，经所述智能合约编译器编译的业务智能合约中包含所述 RSA 签名验证指令；区块链网络中部署有所述业务智能合约；

所述区块链网络中的节点，获得业务发起交易并广播给其他节点；

所述区块链网络中的每个节点，在执行所述业务发起交易时，通过区块链虚拟机，调用所述业务智能合约；通过区块链虚拟机，根据所述业务智能合约中的 RSA 签名验证指令，触发执行所述 RSA 签名验证逻辑，以对业务签名进行 RSA 签名验证操作，以

对业务签名进行RSA签名验证操作。

10、一种区块链系统，包括区块链网络，其中，

区块链虚拟机的指令集中包括 RSA 签名验证指令，并且，区块链虚拟机中部署有对应于所述RSA签名验证指令的 RSA 签名验证逻辑；智能合约编译器的指令集中包括所述RSA签名验证指令，经所述智能合约编译器编译的业务智能合约中包含RSA签名验证智能合约的合约标识，所述 RSA 签名验证智能合约是预先部署于区块链网络中的智能合约；区块链网络中部署有所述业务智能合约；

所述区块链网络中的节点，获得业务发起交易并广播给其他节点；

所述区块链网络中的每个节点，在执行所述业务发起交易时，通过区块链虚拟机，调用所述业务智能合约；通过区块链虚拟机，根据所述业务智能合约中的所述 RSA 签名验证智能合约的合约标识，调用所述 RSA 签名验证智能合约；通过区块链虚拟机，根据所述 RSA 签名验证智能合约中的 RSA 签名验证指令，触发执行所述 RSA 签名验证逻辑，以对业务签名进行RSA签名验证操作，以对业务签名进行RSA签名验证操作。

11、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，其中，所述处理器执行所述程序时实现如权利要求 1~3 任一项所述的方法。

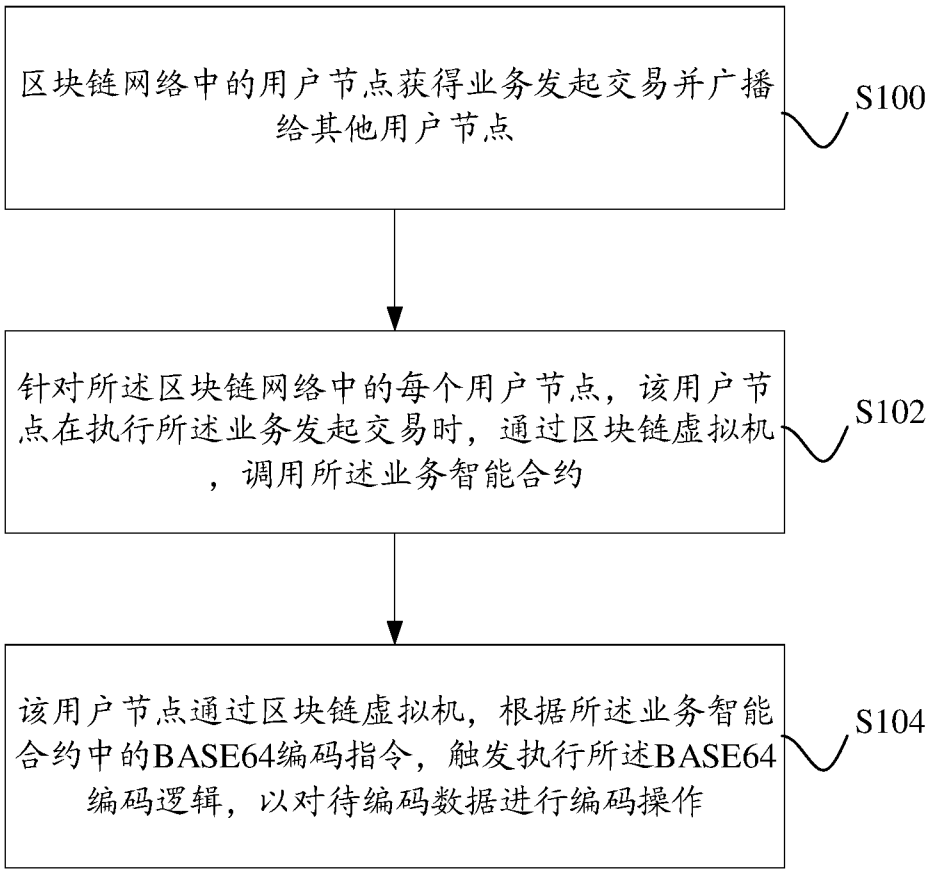

区块链网络中的用户节点获得业务发起交易并广播给其他用户节点
S100
针对所述区块链网络中的每个用户节点，该用户节点在执行所述业务发起交易时，通过区块链虚拟机，调用所述业务智能合约
S102
该用户节点通过区块链虚拟机，根据所述业务智能合约中的BASE64编码指令，触发执行所述BASE64编码逻辑，以对待编码数据进行编码操作
S104

图 1

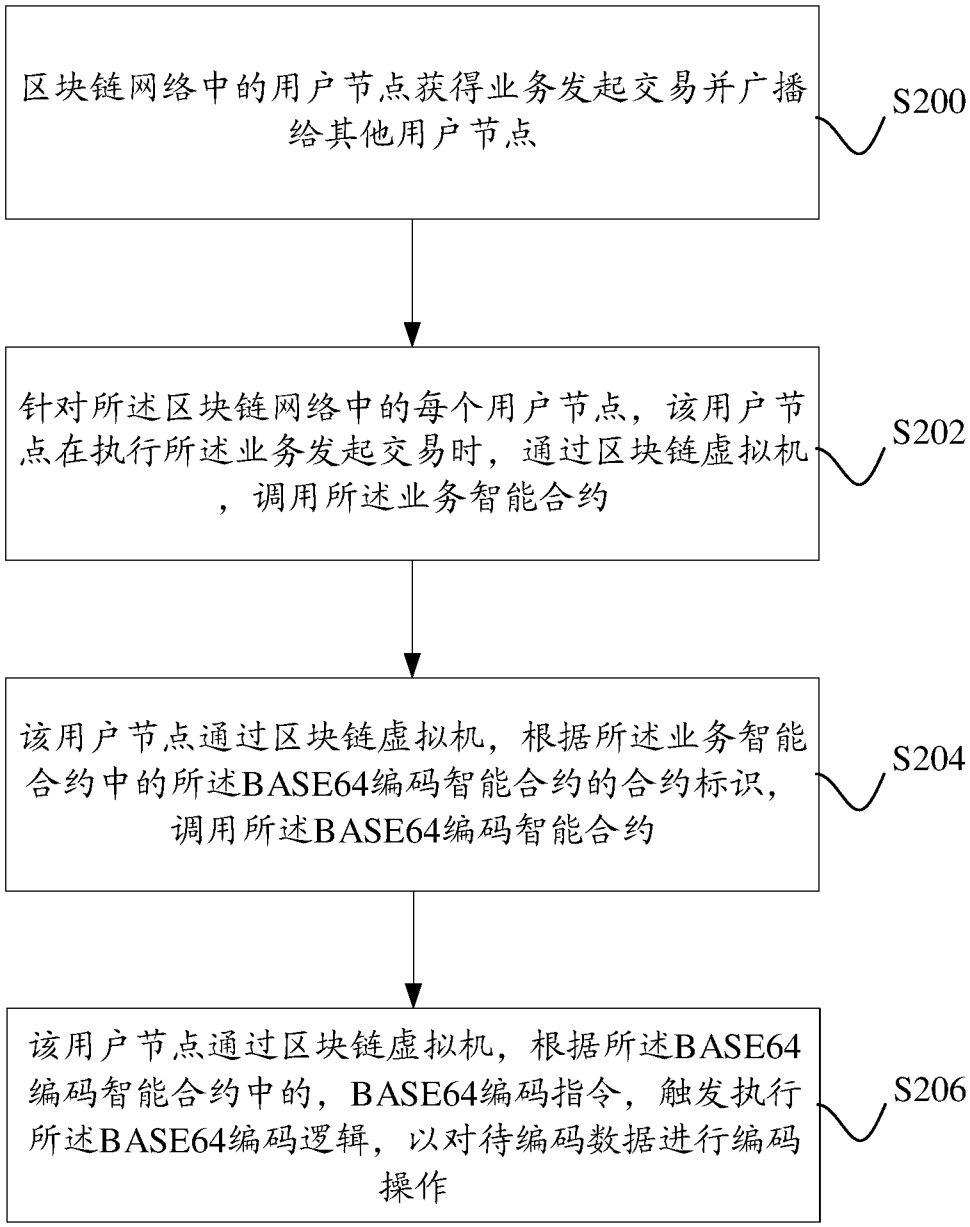

区块链网络中的用户节点获得业务发起交易并广播给其他用户节点
S200
针对所述区块链网络中的每个用户节点，该用户节点在执行所述业务发起交易时，通过区块链虚拟机，调用所述业务智能合约
S202
该用户节点通过区块链虚拟机，根据所述业务智能合约中的所述BASE64编码智能合约的合约标识，调用所述BASE64编码智能合约
S204
该用户节点通过区块链虚拟机，根据所述BASE64编码智能合约中的，BASE64编码指令，触发执行所述BASE64编码逻辑，以对待编码数据进行编码操作
S206

图 2

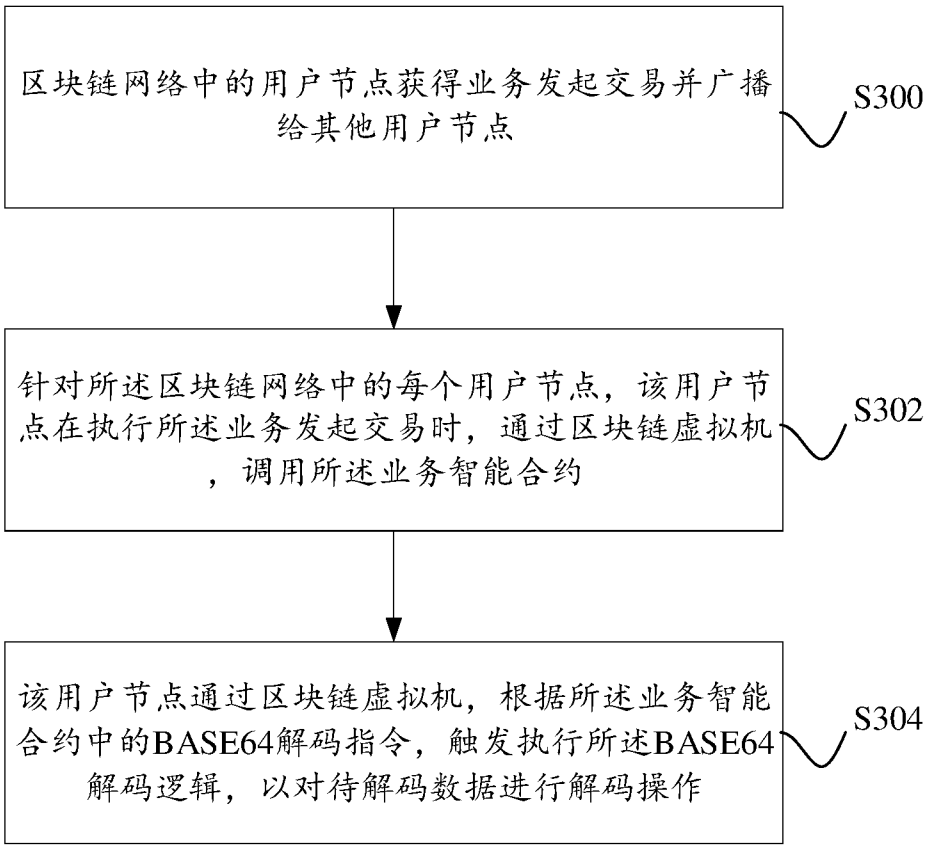

区块链网络中的用户节点获得业务发起交易并广播给其他用户节点
S300
针对所述区块链网络中的每个用户节点，该用户节点在执行所述业务发起交易时，通过区块链虚拟机，调用所述业务智能合约
S302
该用户节点通过区块链虚拟机，根据所述业务智能合约中的BASE64解码指令，触发执行所述BASE64解码逻辑，以对待解码数据进行解码操作
S304

图 3

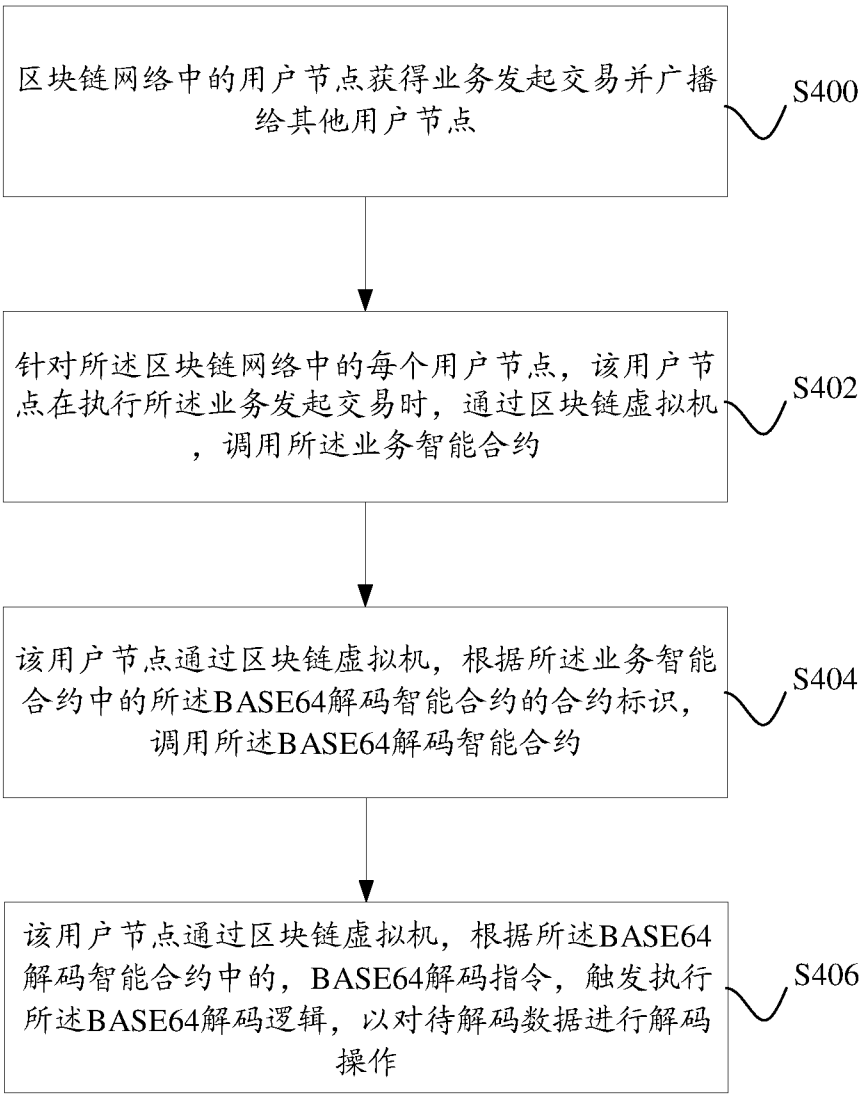

区块链网络中的用户节点获得业务发起交易并广播给其他用户节点
S400
针对所述区块链网络中的每个用户节点，该用户节点在执行所述业务发起交易时，通过区块链虚拟机，调用所述业务智能合约
S402
该用户节点通过区块链虚拟机，根据所述业务智能合约中的所述BASE64解码智能合约的合约标识，调用所述BASE64解码智能合约
S404
该用户节点通过区块链虚拟机，根据所述BASE64解码智能合约中的，BASE64解码指令，触发执行所述BASE64解码逻辑，以对待解码数据进行解码操作
S406

图 4

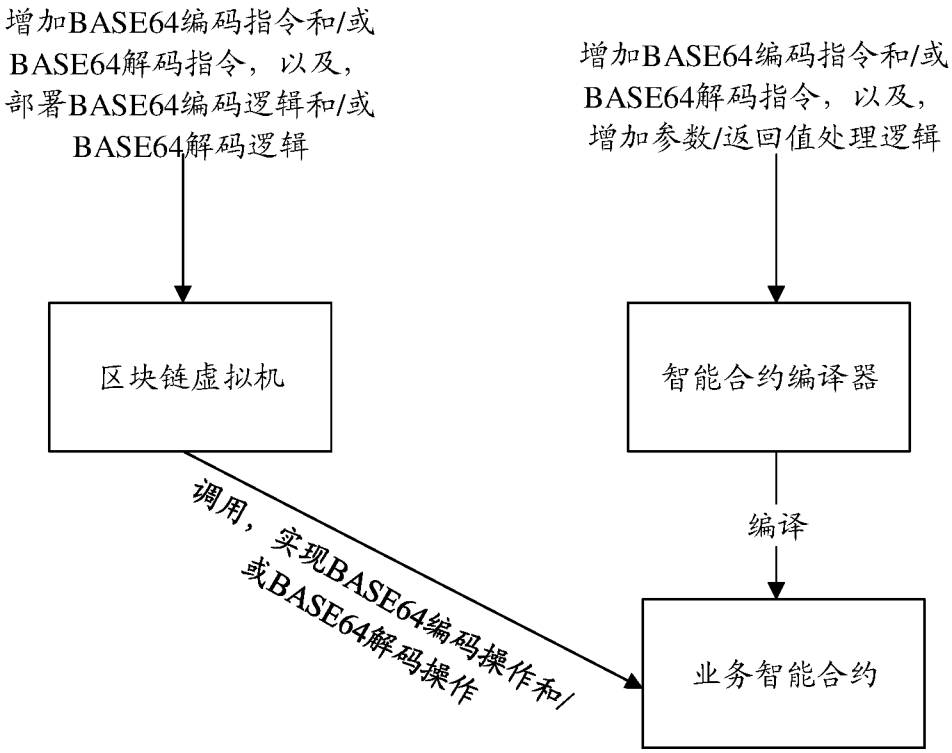

增加BASE64编码指令和/或
BASE64解码指令，以及，
部署BASE64编码逻辑和/或
BASE64解码逻辑
增加BASE64编码指令和/或
BASE64解码指令，以及，
增加参数/返回值处理逻辑
区块链虚拟机
智能合约编译器
调用，实现BASE64编码操作和/
或BASE64解码操作
编译
业务智能合约

图 5a

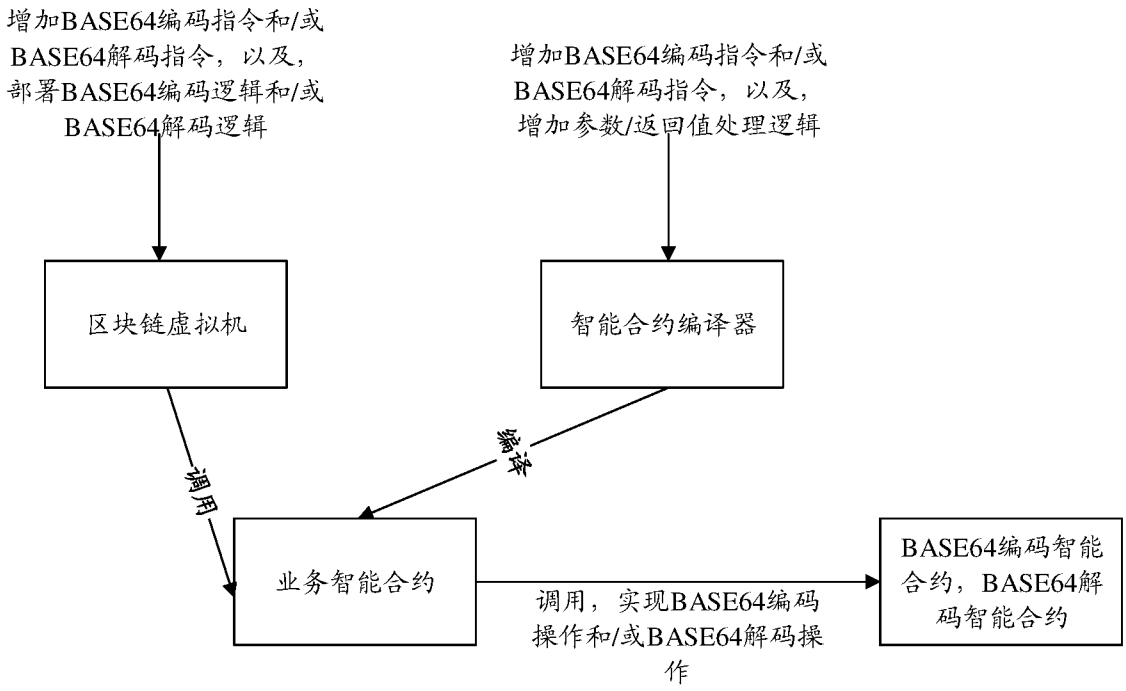

增加BASE64编码指令和/或
BASE64解码指令，以及，
部署BASE64编码逻辑和/或
BASE64解码逻辑
增加BASE64编码指令和/或
BASE64解码指令，以及，
增加参数/返回值处理逻辑
区块链虚拟机
智能合约编译器
调用
编译
业务智能合约
调用，实现BASE64编码
操作和/或BASE64解码操
作
BASE64编码智能
合约，BASE64解
码智能合约

图 5b

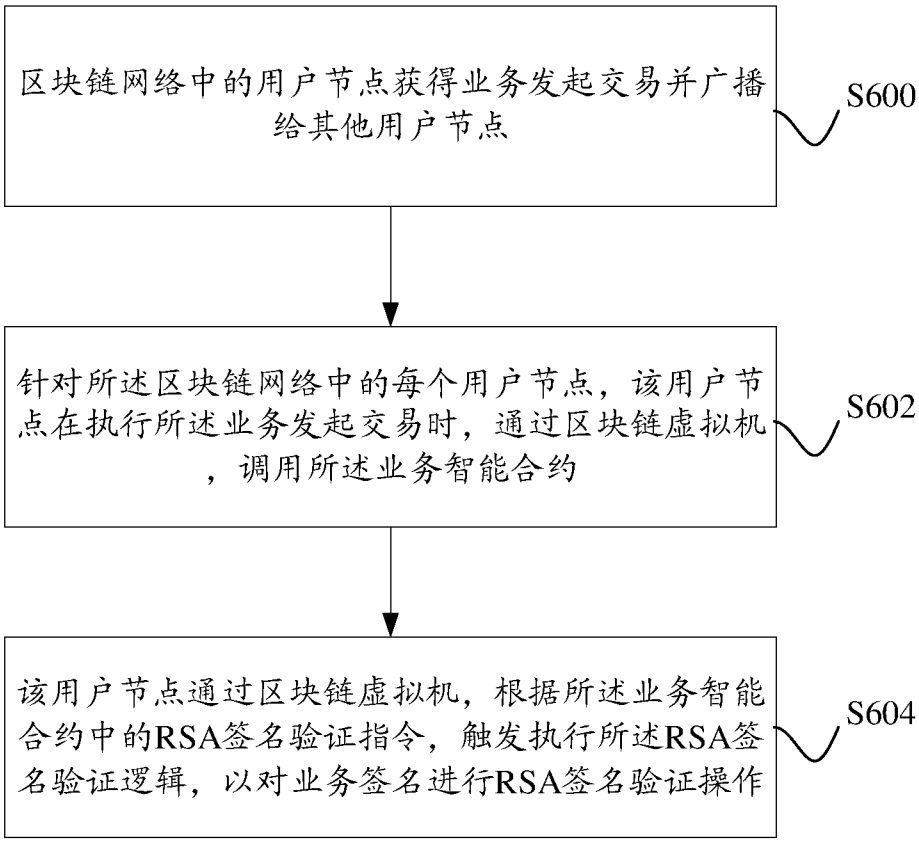

区块链网络中的用户节点获得业务发起交易并广播给其他用户节点
S600
针对所述区块链网络中的每个用户节点，该用户节点在执行所述业务发起交易时，通过区块链虚拟机，调用所述业务智能合约
S602
该用户节点通过区块链虚拟机，根据所述业务智能合约中的RSA签名验证指令，触发执行所述RSA签名验证逻辑，以对业务签名进行RSA签名验证操作
S604

图 6

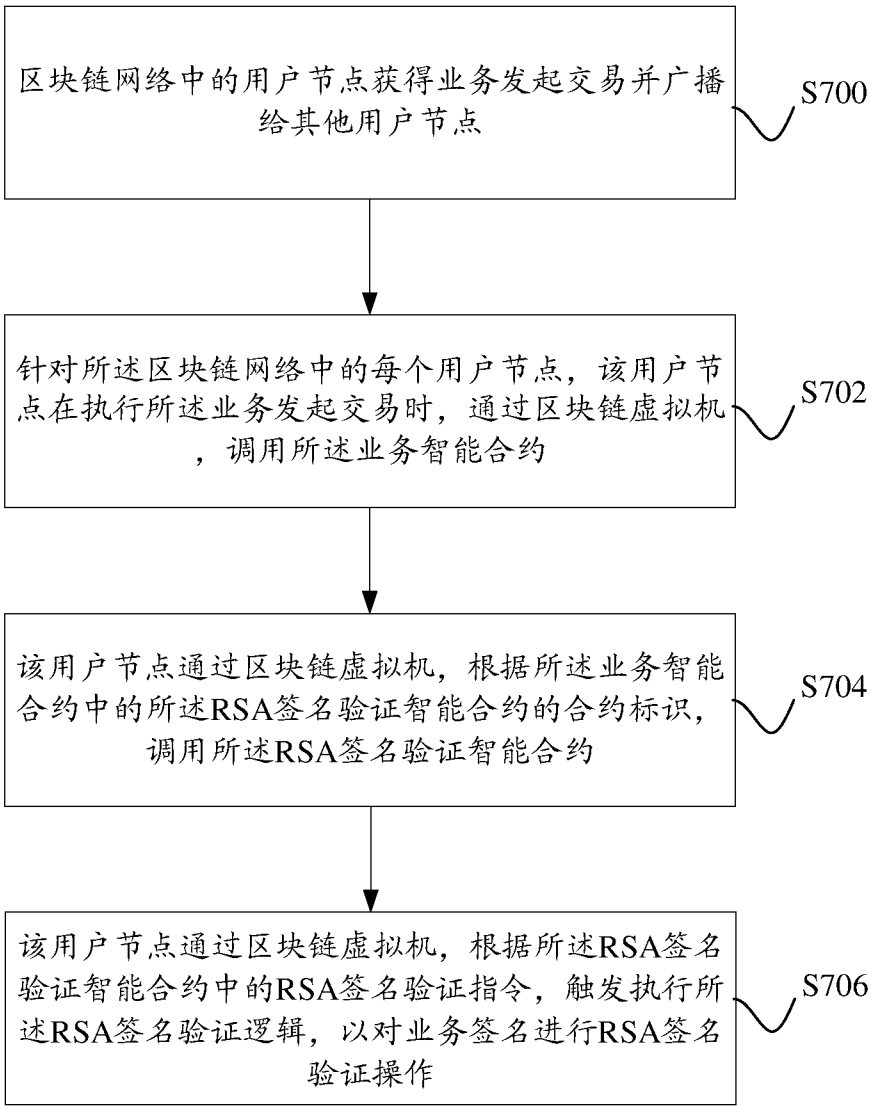

区块链网络中的用户节点获得业务发起交易并广播给其他用户节点
S700
针对所述区块链网络中的每个用户节点，该用户节点在执行所述业务发起交易时，通过区块链虚拟机，调用所述业务智能合约
S702
该用户节点通过区块链虚拟机，根据所述业务智能合约中的所述RSA签名验证智能合约的合约标识，调用所述RSA签名验证智能合约
S704
该用户节点通过区块链虚拟机，根据所述RSA签名验证智能合约中的RSA签名验证指令，触发执行所述RSA签名验证逻辑，以对业务签名进行RSA签名验证操作
S706

图 7

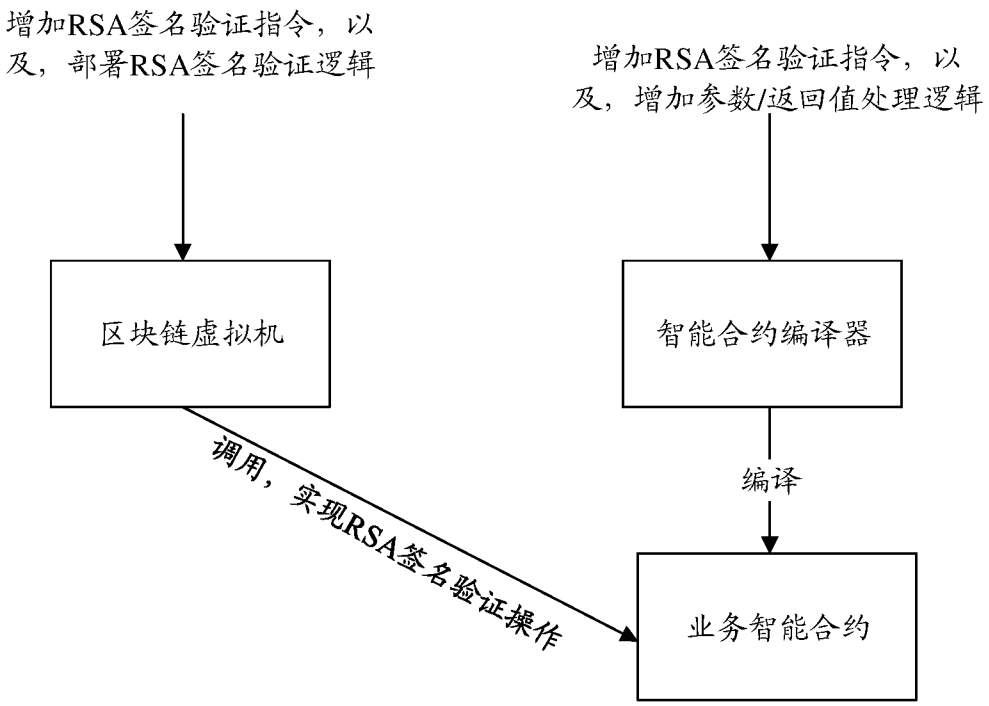

增加RSA签名验证指令，以及，部署RSA签名验证逻辑
增加RSA签名验证指令，以及，增加参数/返回值处理逻辑
区块链虚拟机
智能合约编译器
调用，实现RSA签名验证操作
编译
业务智能合约

图 8a

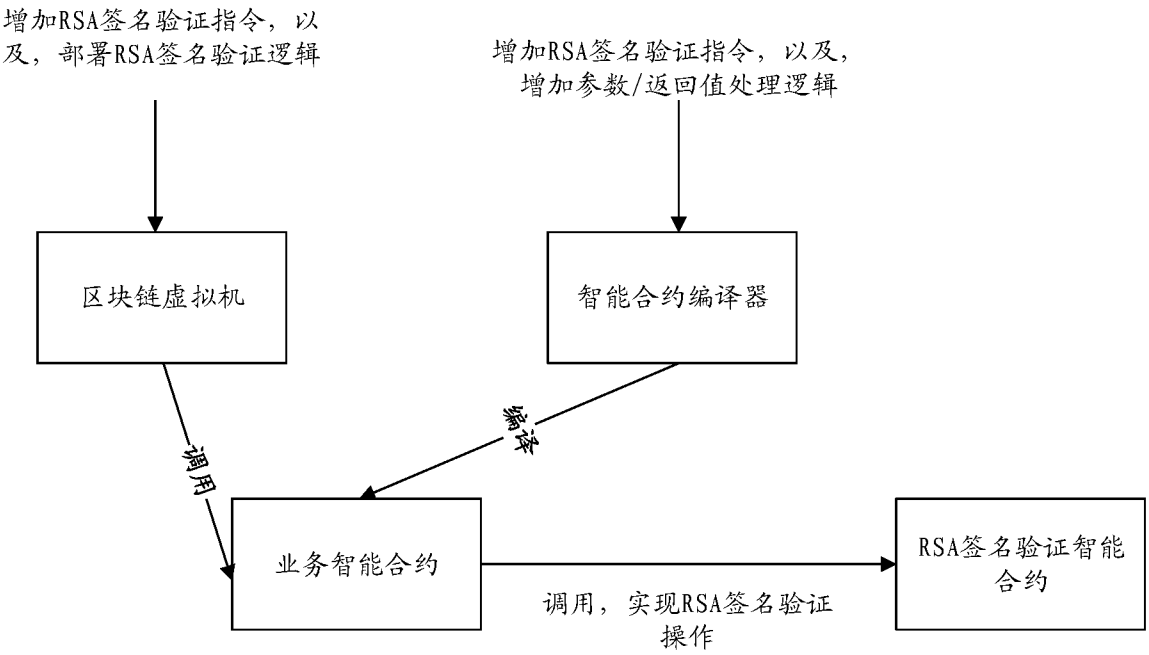

增加RSA签名验证指令，以及，部署RSA签名验证逻辑
增加RSA签名验证指令，以及，增加参数/返回值处理逻辑
区块链虚拟机
智能合约编译器
调用
编译
业务智能合约
调用，实现RSA签名验证操作
RSA签名验证智能合约

图 8b

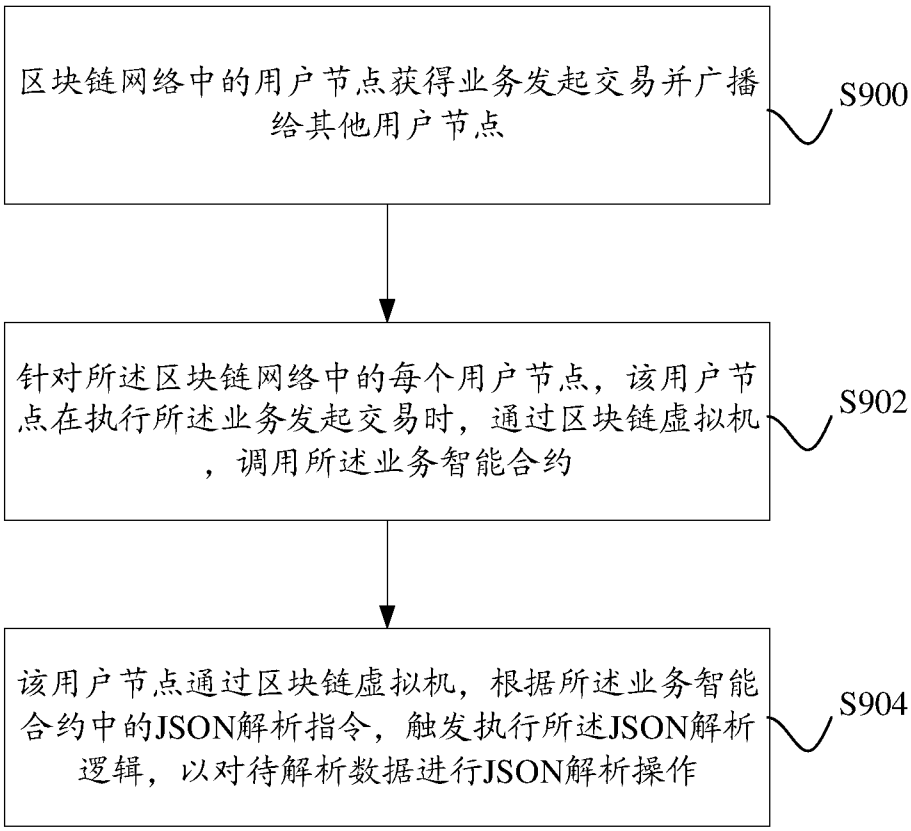

区块链网络中的用户节点获得业务发起交易并广播给其他用户节点
S900
针对所述区块链网络中的每个用户节点，该用户节点在执行所述业务发起交易时，通过区块链虚拟机，调用所述业务智能合约
S902
该用户节点通过区块链虚拟机，根据所述业务智能合约中的JSON解析指令，触发执行所述JSON解析逻辑，以对待解析数据进行JSON解析操作
S904

图 9

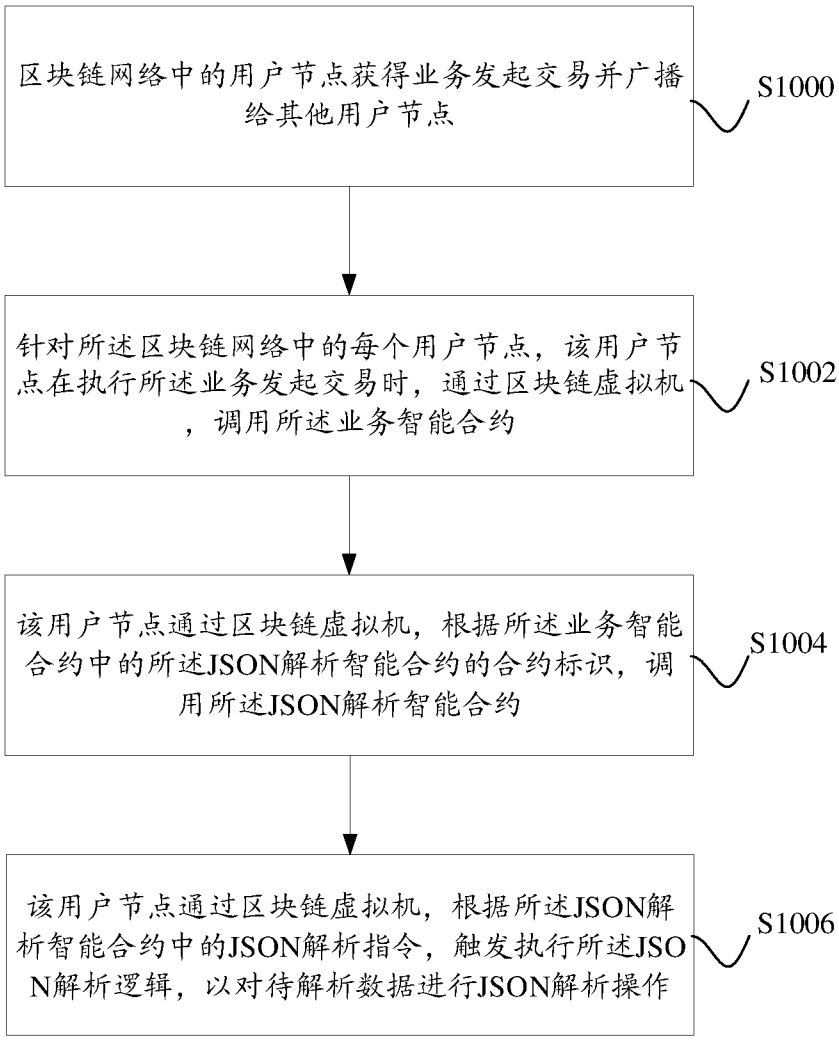

区块链网络中的用户节点获得业务发起交易并广播给其他用户节点
S1000
针对所述区块链网络中的每个用户节点，该用户节点在执行所述业务发起交易时，通过区块链虚拟机，调用所述业务智能合约
S1002
该用户节点通过区块链虚拟机，根据所述业务智能合约中的所述JSON解析智能合约的合约标识，调用所述JSON解析智能合约
S1004
该用户节点通过区块链虚拟机，根据所述JSON解析智能合约中的JSON解析指令，触发执行所述JSON解析逻辑，以对待解析数据进行JSON解析操作
S1006

图 10

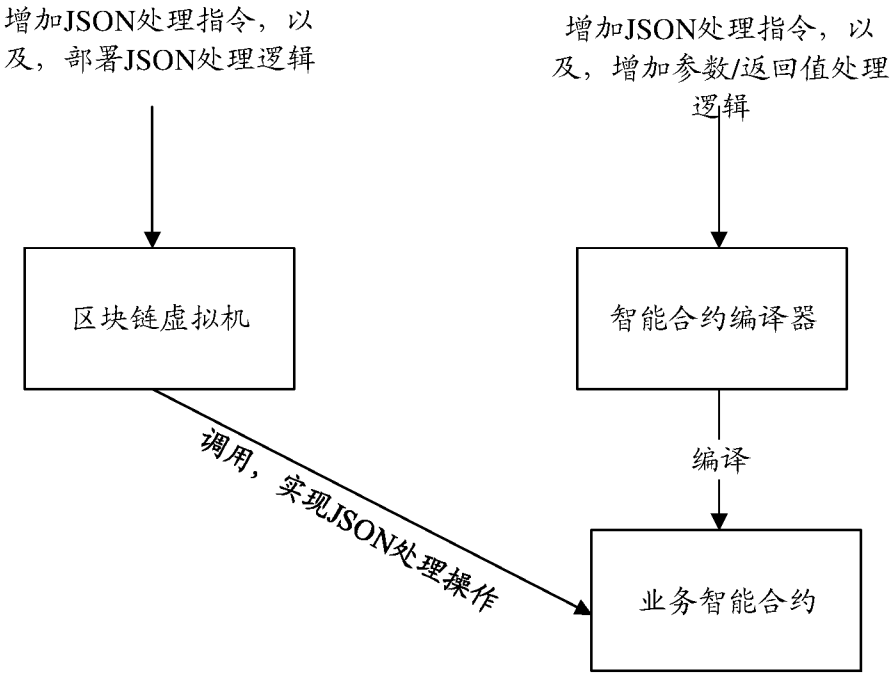

增加JSON处理指令，以及，部署JSON处理逻辑
增加JSON处理指令，以及，增加参数/返回值处理逻辑
区块链虚拟机
智能合约编译器
调用，实现JSON处理操作
编译
业务智能合约

图 11a

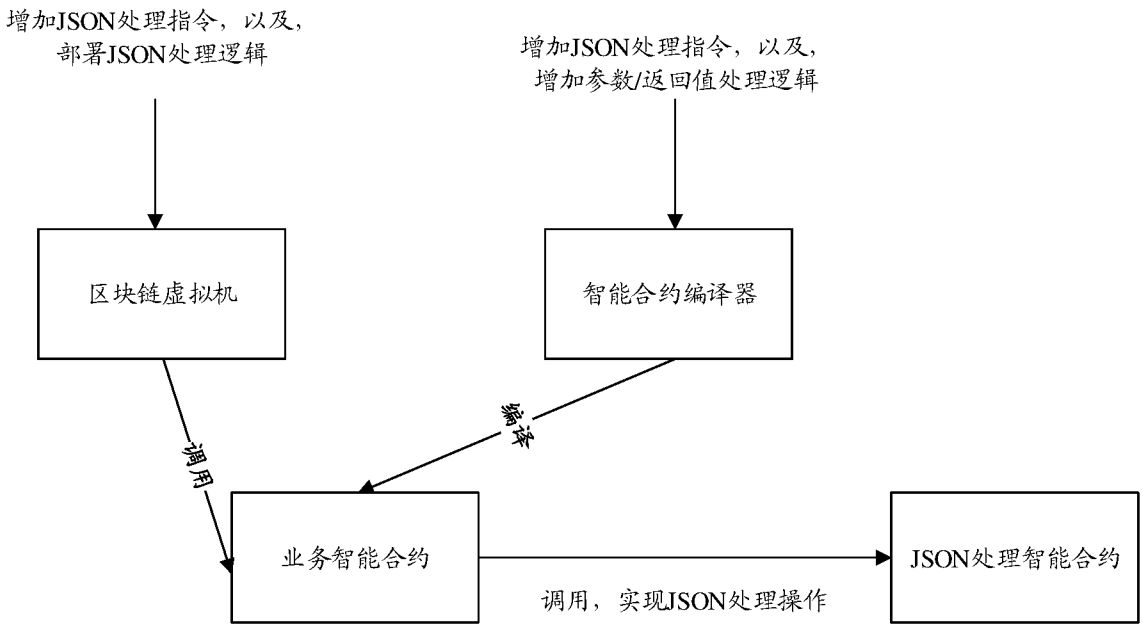

增加JSON处理指令，以及，部署JSON处理逻辑
增加JSON处理指令，以及，增加参数/返回值处理逻辑
区块链虚拟机
智能合约编译器
调用
编译
业务智能合约
JSON处理智能合约
调用，实现JSON处理操作

图 11b

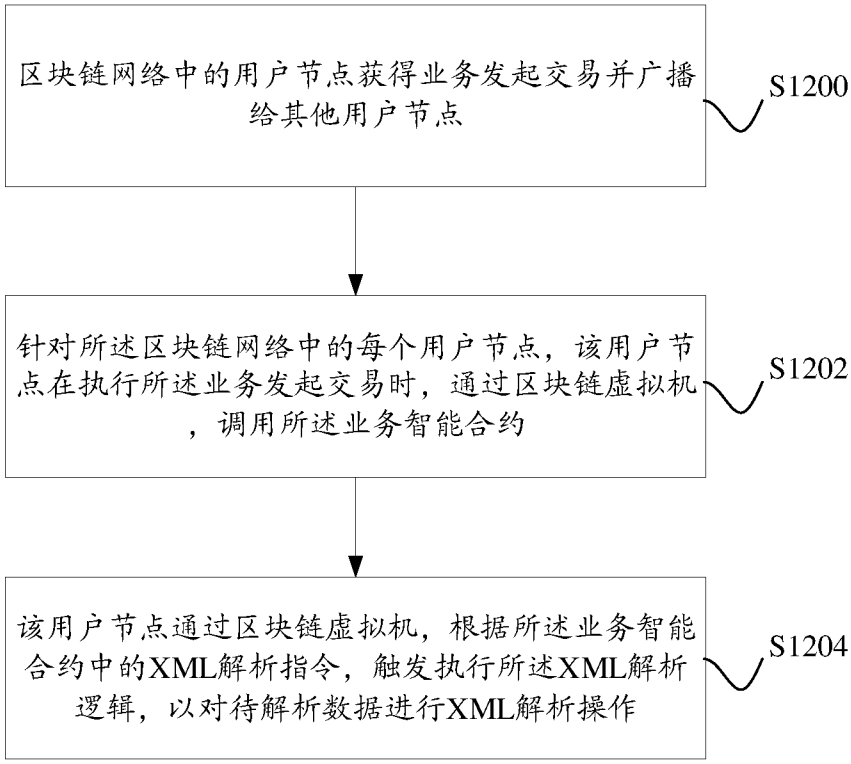

区块链网络中的用户节点获得业务发起交易并广播给其他用户节点
S1200
针对所述区块链网络中的每个用户节点，该用户节点在执行所述业务发起交易时，通过区块链虚拟机，调用所述业务智能合约
S1202
该用户节点通过区块链虚拟机，根据所述业务智能合约中的XML解析指令，触发执行所述XML解析逻辑，以对待解析数据进行XML解析操作
S1204

图 12

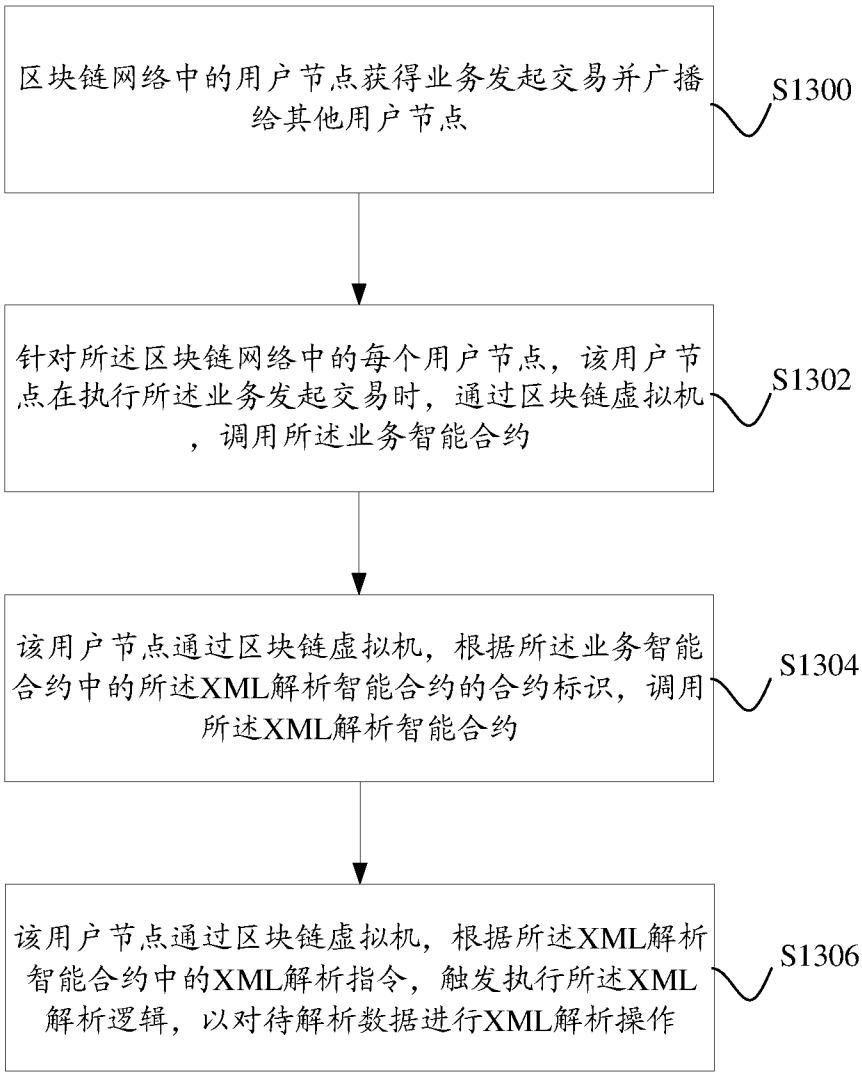

区块链网络中的用户节点获得业务发起交易并广播给其他用户节点
S1300
针对所述区块链网络中的每个用户节点，该用户节点在执行所述业务发起交易时，通过区块链虚拟机，调用所述业务智能合约
S1302
该用户节点通过区块链虚拟机，根据所述业务智能合约中的所述XML解析智能合约的合约标识，调用所述XML解析智能合约
S1304
该用户节点通过区块链虚拟机，根据所述XML解析智能合约中的XML解析指令，触发执行所述XML解析逻辑，以对待解析数据进行XML解析操作
S1306

图 13

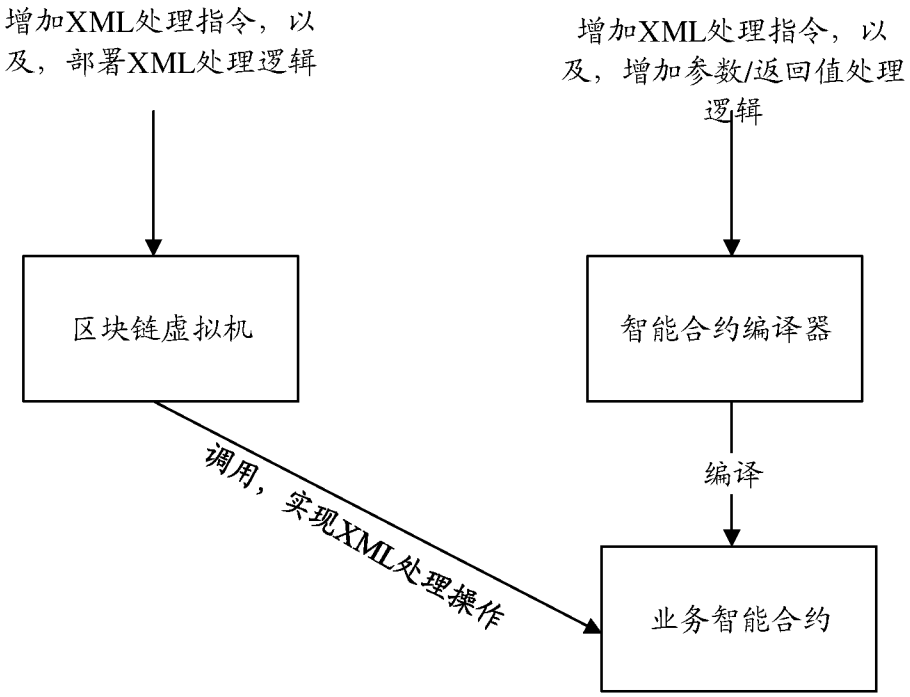

增加XML处理指令，以及，部署XML处理逻辑
增加XML处理指令，以及，增加参数/返回值处理逻辑
区块链虚拟机
智能合约编译器
调用，实现XML处理操作
编译
业务智能合约

图 14a

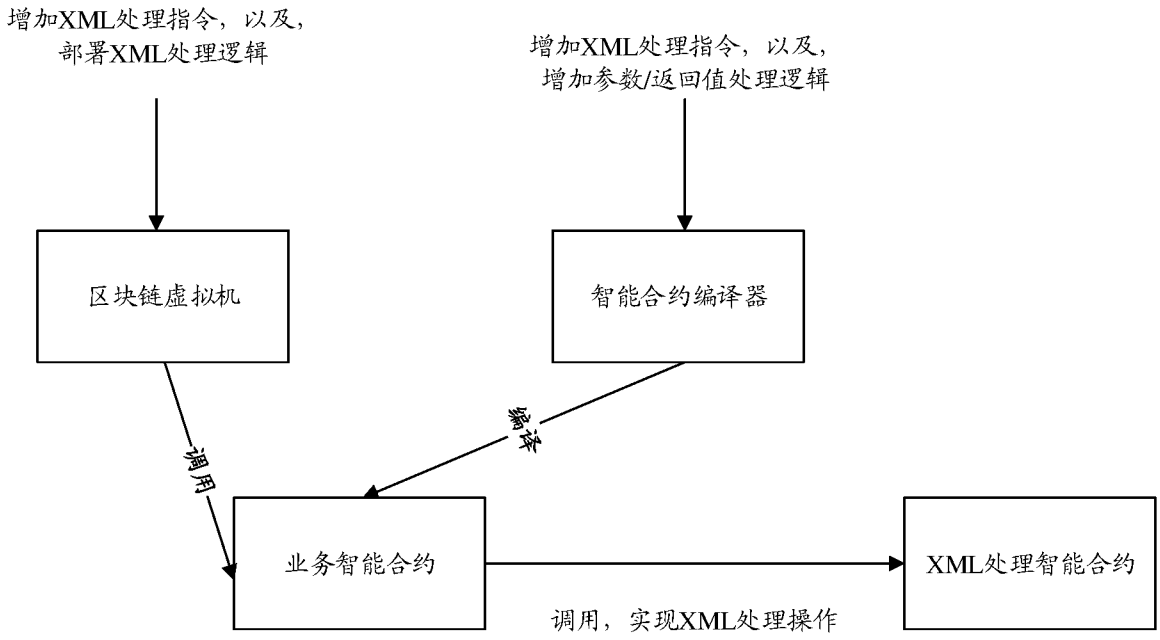

增加XML处理指令，以及，部署XML处理逻辑
增加XML处理指令，以及，增加参数/返回值处理逻辑
区块链虚拟机
智能合约编译器
调用
编译
业务智能合约
XML处理智能合约
调用，实现XML处理操作

图 14b

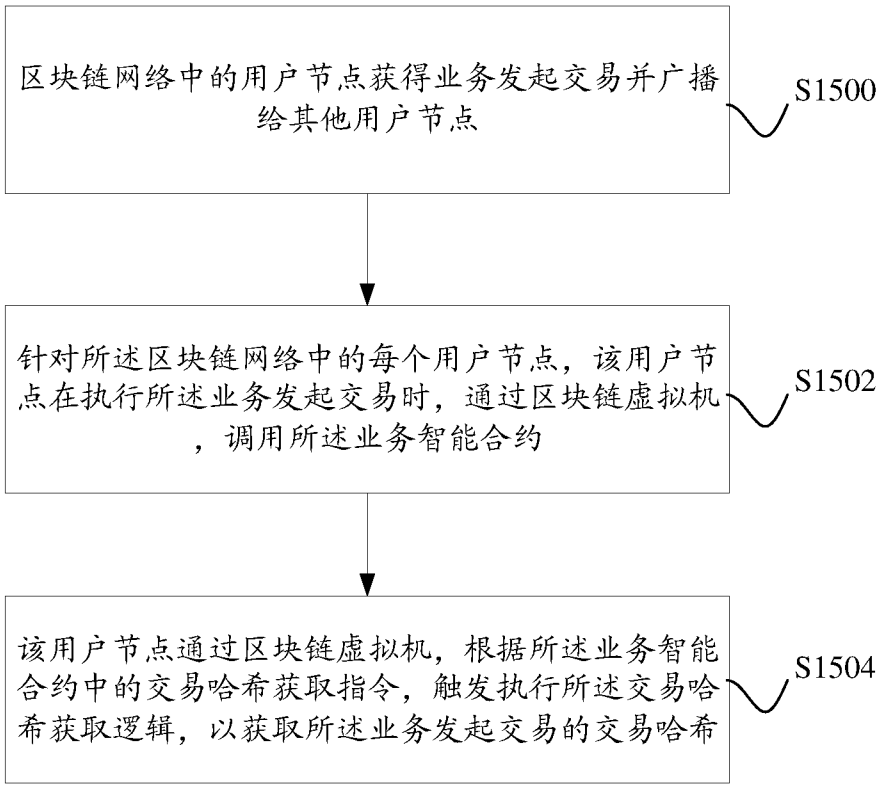

区块链网络中的用户节点获得业务发起交易并广播给其他用户节点
S1500
针对所述区块链网络中的每个用户节点，该用户节点在执行所述业务发起交易时，通过区块链虚拟机，调用所述业务智能合约
S1502
该用户节点通过区块链虚拟机，根据所述业务智能合约中的交易哈希获取指令，触发执行所述交易哈希获取逻辑，以获取所述业务发起交易的交易哈希
S1504

图 15

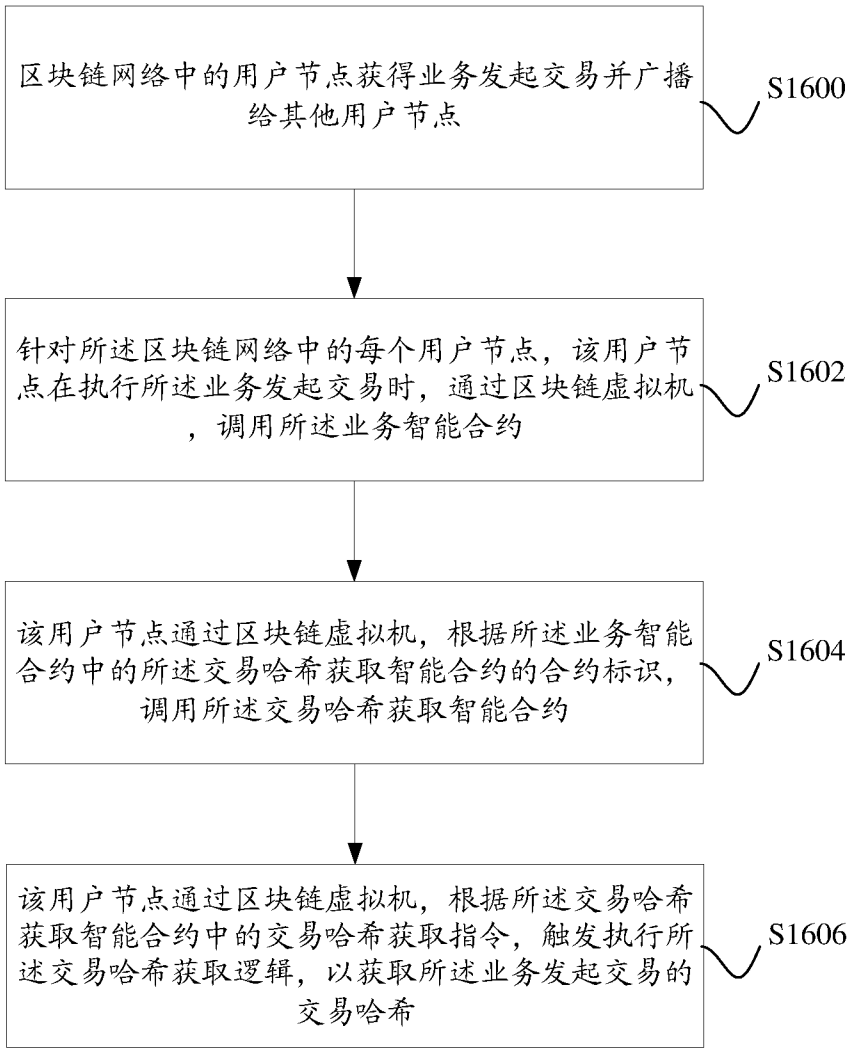

区块链网络中的用户节点获得业务发起交易并广播给其他用户节点
S1600
针对所述区块链网络中的每个用户节点，该用户节点在执行所述业务发起交易时，通过区块链虚拟机，调用所述业务智能合约
S1602
该用户节点通过区块链虚拟机，根据所述业务智能合约中的所述交易哈希获取智能合约的合约标识，调用所述交易哈希获取智能合约
S1604
该用户节点通过区块链虚拟机，根据所述交易哈希获取智能合约中的交易哈希获取指令，触发执行所述交易哈希获取逻辑，以获取所述业务发起交易的交易哈希
S1606

图 16

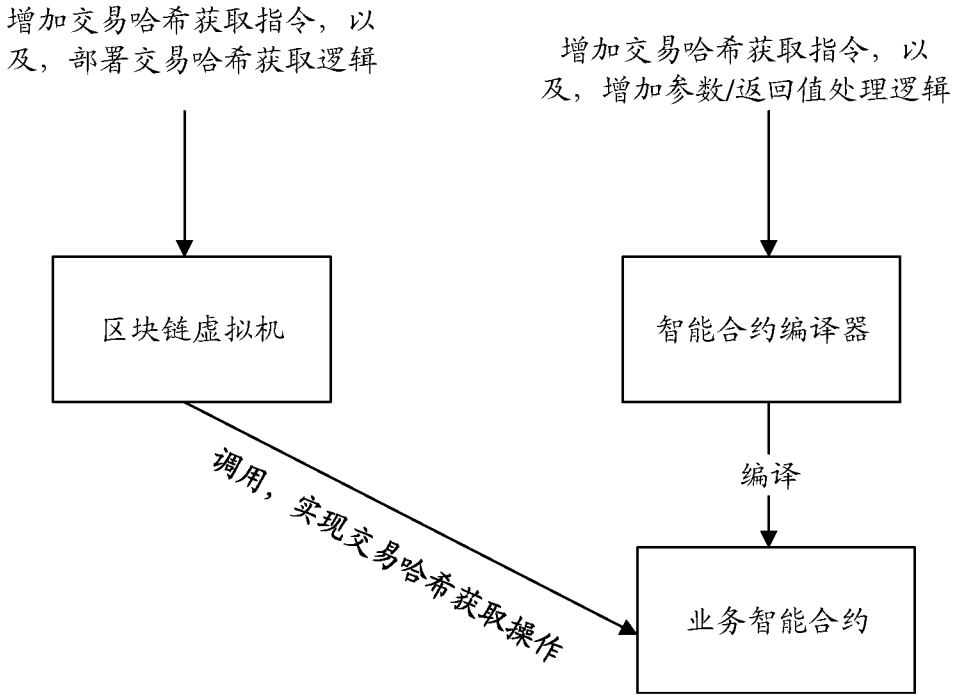

增加交易哈希获取指令，以及，部署交易哈希获取逻辑
增加交易哈希获取指令，以及，增加参数/返回值处理逻辑
区块链虚拟机
智能合约编译器
调用，实现交易哈希获取操作
编译
业务智能合约

图 17a

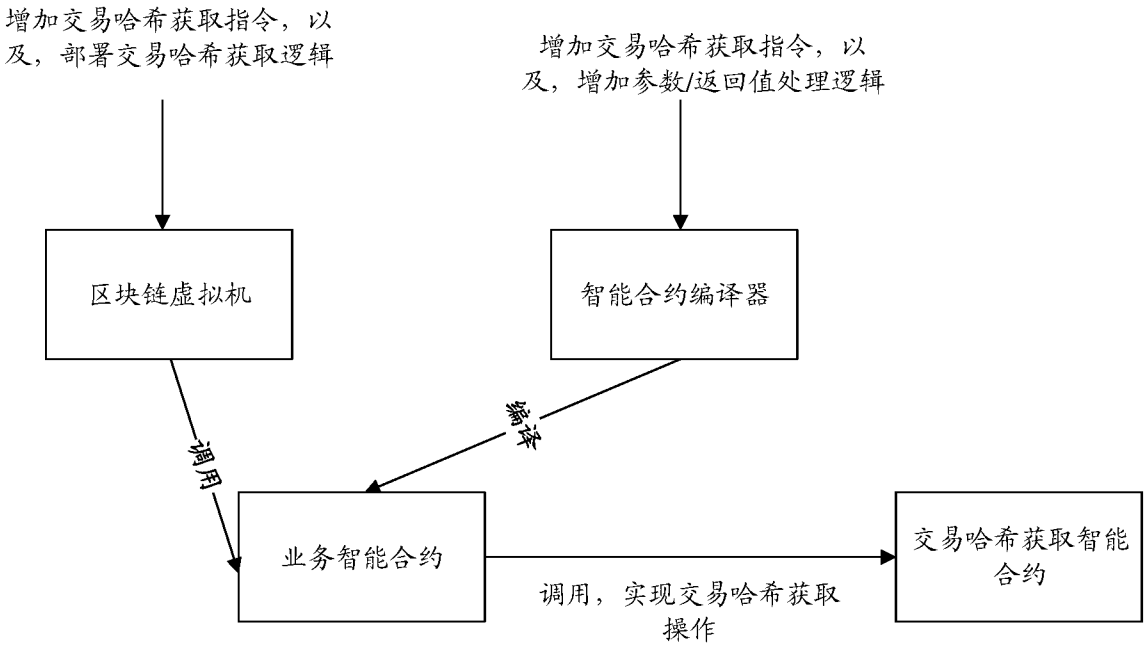

增加交易哈希获取指令，以及，部署交易哈希获取逻辑
增加交易哈希获取指令，以及，增加参数/返回值处理逻辑
区块链虚拟机
智能合约编译器
调用
编译
业务智能合约
交易哈希获取智能合约
调用，实现交易哈希获取操作

图 17b

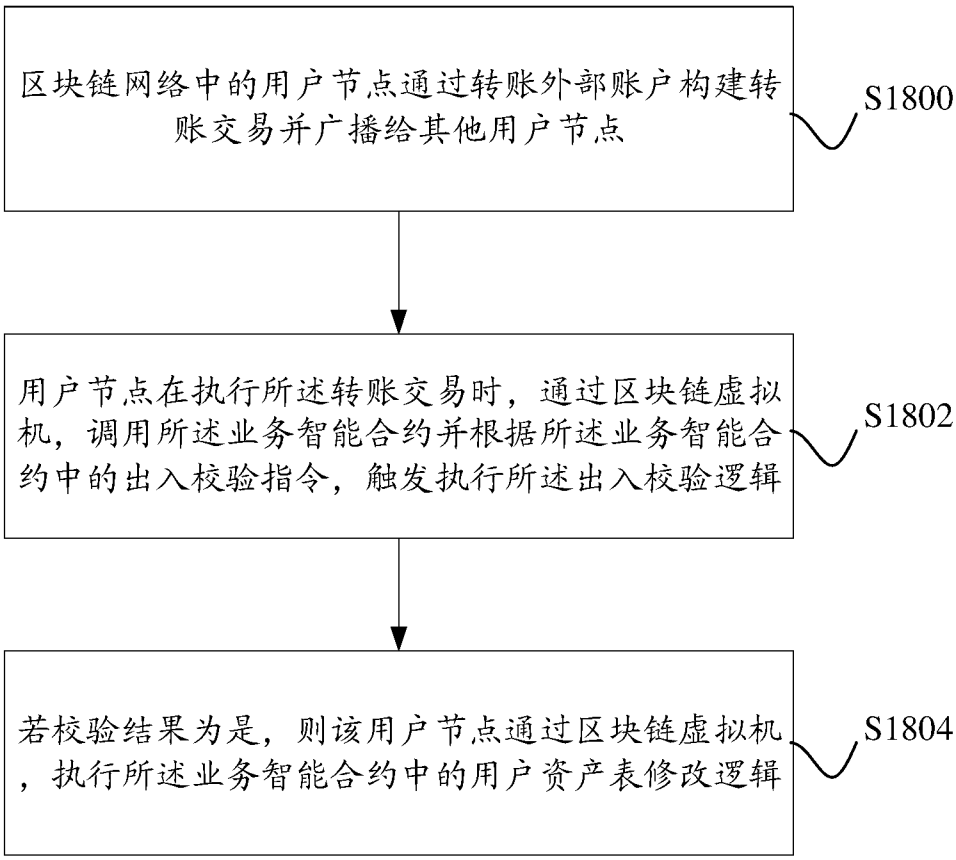

区块链网络中的用户节点通过转账外部账户构建转账交易并广播给其他用户节点
S1800
用户节点在执行所述转账交易时，通过区块链虚拟机，调用所述业务智能合约并根据所述业务智能合约中的出入校验指令，触发执行所述出入校验逻辑
S1802
若校验结果为是，则该用户节点通过区块链虚拟机，执行所述业务智能合约中的用户资产表修改逻辑
S1804

图 18

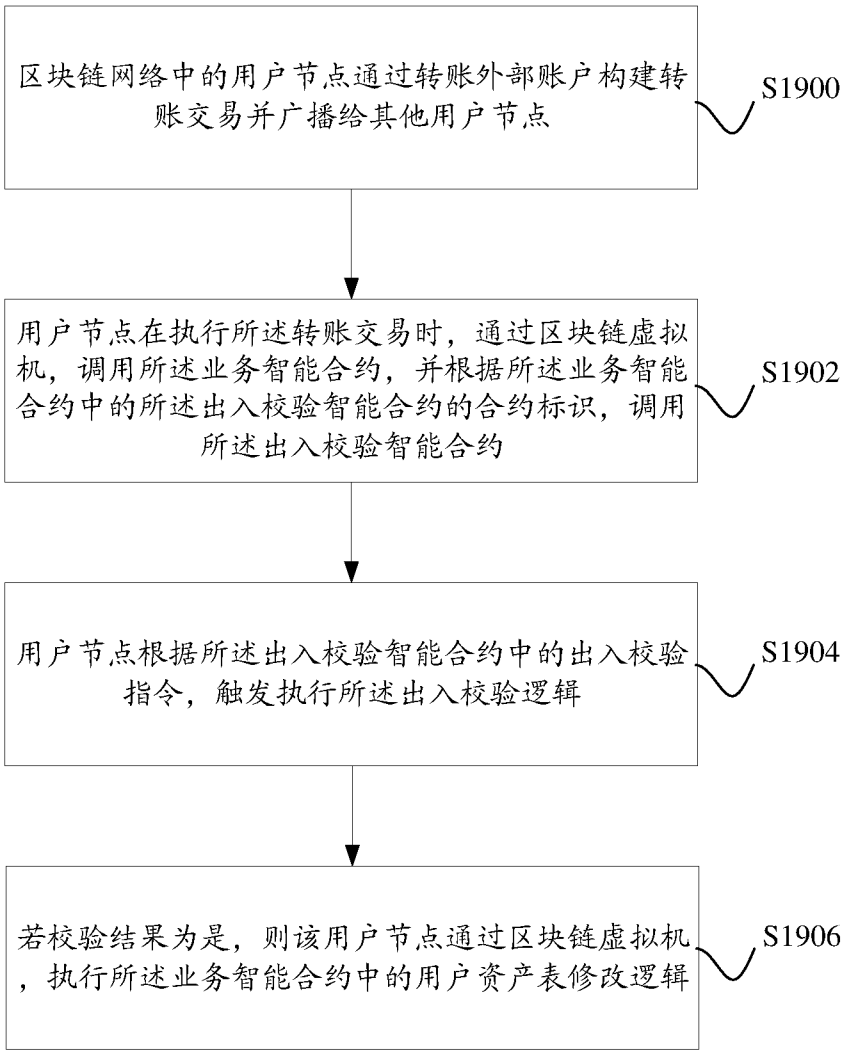

区块链网络中的用户节点通过转账外部账户构建转账交易并广播给其他用户节点
S1900
用户节点在执行所述转账交易时，通过区块链虚拟机，调用所述业务智能合约，并根据所述业务智能合约中的所述出入校验智能合约的合约标识，调用所述出入校验智能合约
S1902
用户节点根据所述出入校验智能合约中的出入校验指令，触发执行所述出入校验逻辑
S1904
若校验结果为是，则该用户节点通过区块链虚拟机，执行所述业务智能合约中的用户资产表修改逻辑
S1906

图 19

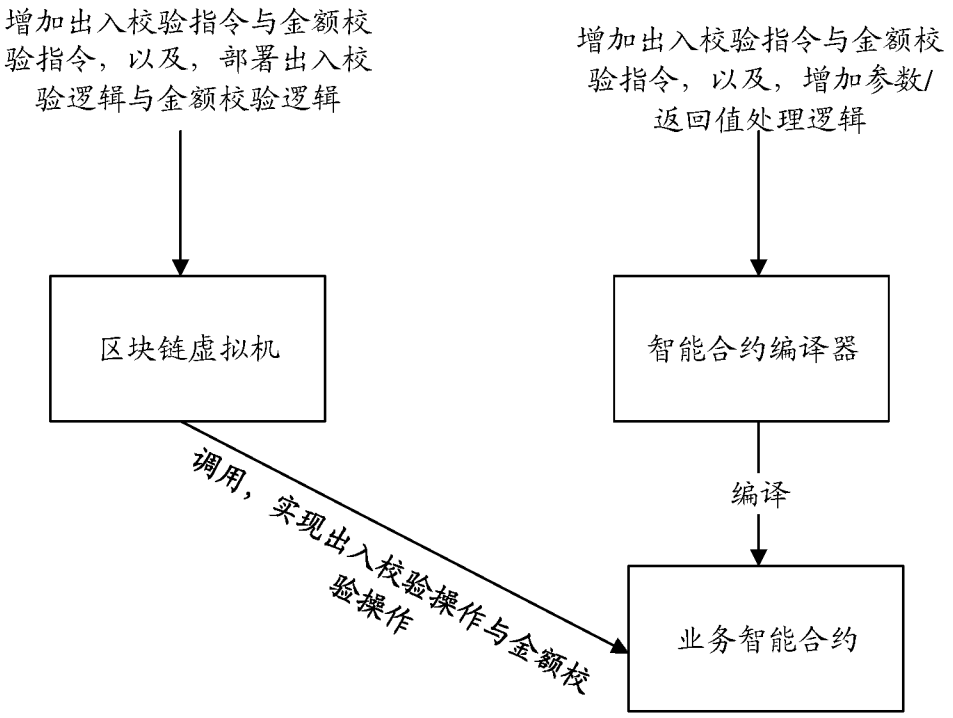

增加出入校验指令与金额校验指令，以及，部署出入校验逻辑与金额校验逻辑
增加出入校验指令与金额校验指令，以及，增加参数/返回值处理逻辑
区块链虚拟机
智能合约编译器
调用，实现出入校验操作与金额校验操作
编译
业务智能合约

图 20a

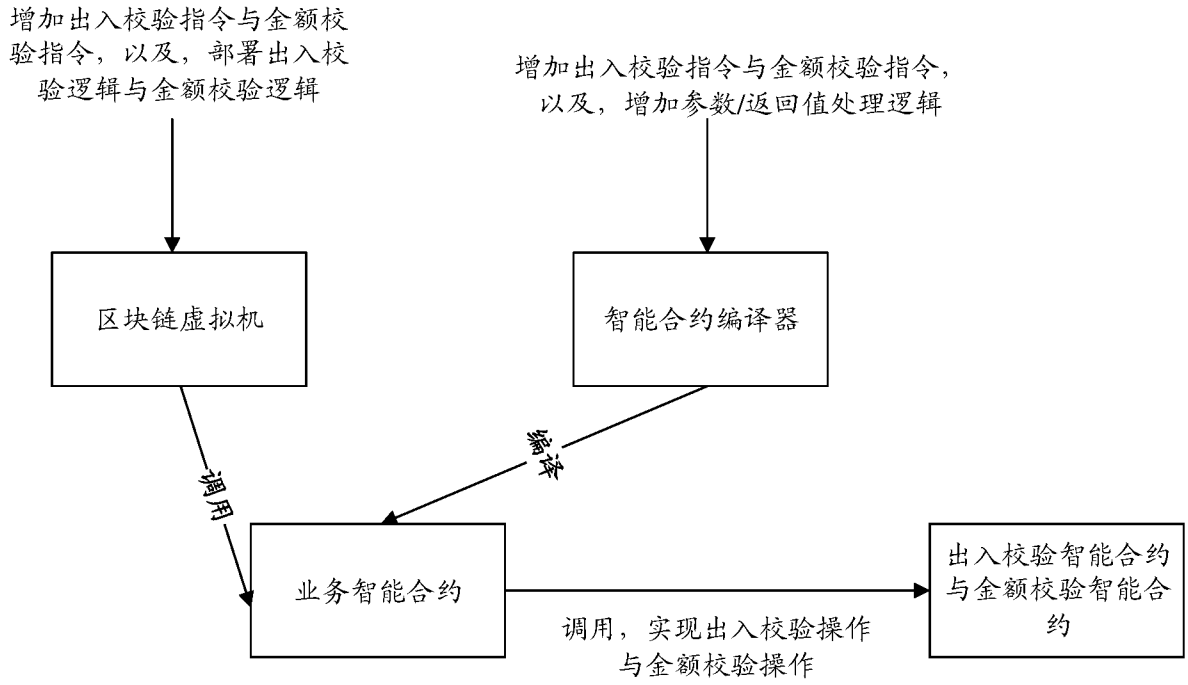

增加出入校验指令与金额校验指令，以及，部署出入校验逻辑与金额校验逻辑
增加出入校验指令与金额校验指令，以及，增加参数/返回值处理逻辑
区块链虚拟机
智能合约编译器
调用
编译
业务智能合约
调用，实现出入校验操作与金额校验操作
出入校验智能合约与金额校验智能合约

图 20b

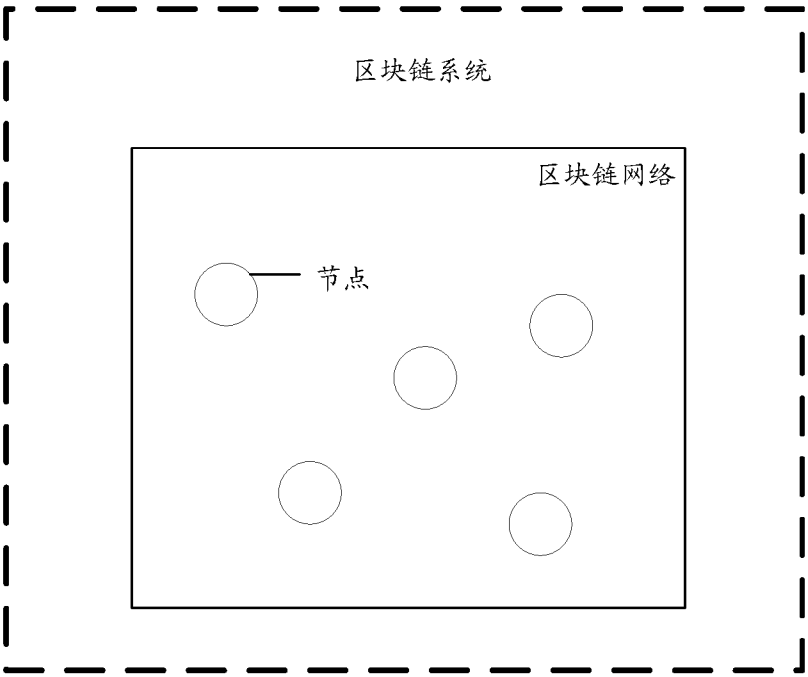


图 21

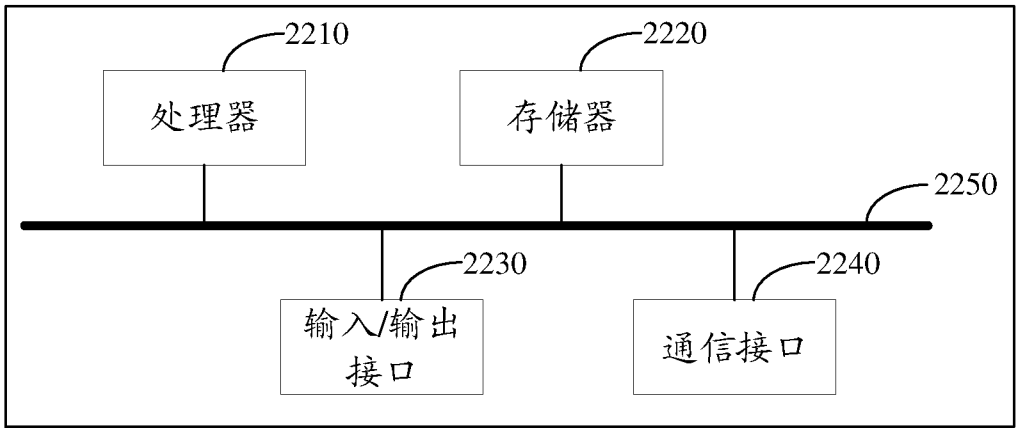


图 22

INTERNATIONAL SEARCH REPORT

International application No.
PCT/CN2019/118740

A. CLASSIFICATION OF SUBJECT MATTER

H04L 9/32(2006.01)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)

H04L

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)

CNABS; CNTXT; DWPI; VEN; CNKI: 区块链, 智能, 合约, 合同, 签名, 认证, block chain, intelligent, smart, contract, verify, signature, authenticate, RSA

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	CN 108833115 A (SUN YAT-SEN UNIVERSITY) 16 November 2018 (2018-11-16) the abstract, and description, paragraphs [0076]-[0103]	1-11
A	CN 107423565 A (SUN YAT-SEN UNIVERSITY) 01 December 2017 (2017-12-01) entire document	1-11
A	US 2013198853 A1 (MCKEEN, FRANCIS X. et al.) 01 August 2013 (2013-08-01) entire document	1-11
PX	CN 110048846 A (ALIBABA GROUP HOLDING LIMITED) 23 July 2019 (2019-07-23) claims 1-11	1-11

☐ 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
21 January 2020	**01 February 2020**

Name and mailing address of the ISA/CN	Authorized officer
China National Intellectual Property Administration (ISA/CN) **No. 6, Xitucheng Road, Jimenqiao Haidian District, Beijing 100088** **China**	
Facsimile No. **(86-10)62019451**	Telephone No.

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/CN2019/118740

Patent document cited in search report	Publication date (day/month/year)	Patent family member(s)	Publication date (day/month/year)
CN 108833115 A	16 November 2018	None	
CN 107423565 A	01 December 2017	None	
US 2013198853 A1	01 August 2013	US 2019087586 A1	21 March 2019
		US 2013159726 A1	20 June 2013
		US 10102380 B2	16 October 2018
		US 9087200 B2	21 July 2015
CN 110048846 A	23 July 2019	None	

国际检索报告

国际申请号
PCT/CN2019/118740

A. 主题的分类

H04L 9/32(2006.01)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)

H04L

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）)

CNABS; CNTXT; DWPI; VEN; CNKI：区块链，智能，合约，合同，签名，认证，block chain, intelligent, smart, contract, verify, signature, authenticate, RSA

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 108833115 A (中山大学) 2018年 11月 16日 (2018-11-16) 摘要，说明书第[0076]-[0103]段	1-11
A	CN 107423565 A (中山大学) 2017年 12月 1日 (2017-12-01) 全文	1-11
A	US 2013198853 A1 (MCKEEN FRANCIS X等) 2013年 8月 1日 (2013-08-01) 全文	1-11
PX	CN 110048846 A (阿里巴巴集团控股有限公司) 2019年 7月 23日 (2019-07-23) 权利要求 1-11	1-11

☐ 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
2020年 1月 21日	2020年 2月 1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 白坦 电话号码 86-(010)-62411245

国际检索报告
关于同族专利的信息

国际申请号
PCT/CN2019/118740

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	108833115	A	2018年 11月 16日	无			
CN	107423565	A	2017年 12月 1日	无			
US	2013198853	A1	2013年 8月 1日	US	2019087586	A1	2019年 3月 21日
				US	2013159726	A1	2013年 6月 20日
				US	10102380	B2	2018年 10月 16日
				US	9087200	B2	2015年 7月 21日
CN	110048846	A	2019年 7月 23日	无			