(19)中华人民共和国国家知识产权局

(12)发明专利申请

(10)申请公布号 CN 108646983 A
(43)申请公布日 2018.10.12

(21)申请号 201810434004.9

(22)申请日 2018.05.08

(71)申请人 北京融链科技有限公司
地址 100000 北京市东城区东直门南大街11号中汇广场C座5层504室

(72)发明人 胡锴 郑涤非 孙雪慧 滕小俊

(74)专利代理机构 北京康信知识产权代理有限责任公司 11240
代理人 赵囡囡 董文倩

(51)Int.Cl.
G06F 3/06(2006.01)
G06Q 40/04(2012.01)

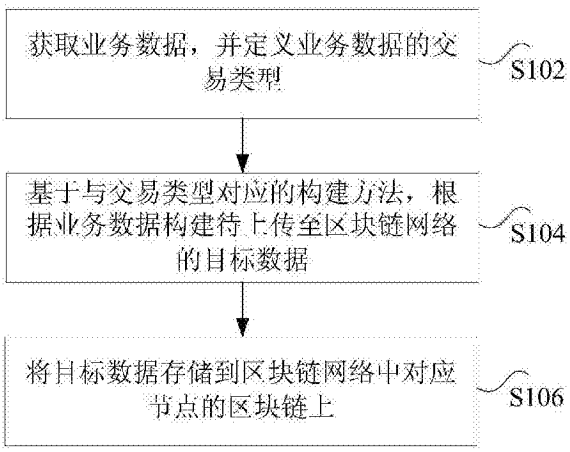
权利要求书2页 说明书7页 附图4页

(54)发明名称

在区块链上存储业务数据的处理方法和装置

(57)摘要

本发明公开了一种在区块链上存储业务数据的处理方法和装置。其中，该方法包括：获取业务数据，并定义业务数据的交易类型；基于与交易类型对应的构建方法，根据业务数据构建待上传至区块链网络的目标数据；将目标数据存储到区块链网络中对应节点的区块链上。本发明解决了现有技术中，由于区块链上记录的数据只有交易数据没有业务数据，当业务数据被篡改的情况下，无法确保信息安全的技术问题。



CN 108646983 A

1.一种在区块链上存储业务数据的处理方法，其特征在于，包括：

获取业务数据，并定义所述业务数据的交易类型；

基于与所述交易类型对应的构建方法，根据所述业务数据构建待上传至区块链网络的目标数据；

将所述目标数据存储到区块链网络中对应节点的区块链上。

2.根据权利要求1所述的方法，其特征在于，将所述目标数据存储到区块链网络中对应节点的区块链上，包括：

生成所述目标数据在所述区块链网络中的标识信息；

基于所述标识信息，对所述目标数据的合法性进行验证；

在验证所述目标数据合法的情况下，将所述目标数据存储到区块链网络中对应节点的区块链上。

3.根据权利要求2所述的方法，其特征在于，生成所述目标数据在所述区块链网络的标识信息，包括：

根据所述目标数据，生成对应的哈希值；

根据所述哈希值，生成所述目标数据在所述区块链网络中的标识信息。

4.根据权利要求3所述的方法，其特征在于，根据所述目标数据，生成对应的哈希值，包括：

对所述目标数据进行加密处理，得到加密后的数据，其中，所述加密处理包括如下至少之一：采用密钥加密、添加数字签名；

根据所述加密后的数据，生成对应的哈希值。

5.根据权利要求3所述的方法，其特征在于，根据所述哈希值，生成所述目标数据在所述区块链网络中的标识信息，包括：

将所述哈希值转换为对应的十六进制数值，将所述十六进制数值作为所述目标数据在所述区块链网络中的标识信息。

6.根据权利要求5所述的方法，其特征在于，在根据所述哈希值，生成所述目标数据在所述区块链网络中的标识信息之前，所述方法还包括：

对所述哈希值进行加密处理，其中，所述加密处理包括如下至少之一：采用密钥加密、添加数字签名。

7.根据权利要求2所述的方法，其特征在于，基于所述标识信息，对所述目标数据的合法性进行验证，包括：

对所述目标数据进行业务验证；

在所述目标数据通过业务验证的情况下，基于所述标识信息，对所述目标数据的合法性进行验证。

8.根据权利要求2所述的方法，其特征在于，在所述目标数据通过业务验证的情况下，基于所述标识信息，对所述目标数据的合法性进行验证，包括：

在所述目标数据通过业务验证的情况下，基于所述标识信息，判断目标区块链上是否存在所述目标数据；

在所述目标区块链上不存在所述目标数据的情况下，基于所述标识信息，对所述目标数据的合法性进行验证。

9.根据权利要求8所述的方法，其特征在于，将所述目标数据存储到区块链网络中对应节点的区块链上，包括：

如果所述目标数据被记载在所述目标区块链上，则所述区块链网络中其他节点将所述目标数据同步至对应的区块链上；

如果所述目标数据未被记载在所述目标区块链上，则所述目标区块链的节点将所述目标数据广播至所述区块链网络上的其他节点，其中，通过任意一个节点验证的目标数据被存储到对应的区块链上。

10.一种在区块链上存储业务数据的处理装置，其特征在于，包括：

获取单元，用于获取业务数据，并定义所述业务数据的交易类型；

构建单元，用于基于与所述交易类型对应的构建方法，根据所述业务数据构建待上传至区块链网络的目标数据；

存储单元，用于将所述目标数据存储到区块链网络中对应节点的区块链上。

在区块链上存储业务数据的处理方法和装置

技术领域

[0001] 本发明涉及互联网领域，具体而言，涉及一种在区块链上存储业务数据的处理方法和装置。

背景技术

[0002] 在互联网信息技术领域，一些业务数据通常都会通过一个中心服务器的数据库存储，但是一旦中心服务器受到攻击，那么数据很有可能就会被篡改或者丢失，造成的损失将是不可估量。比特币为了解决这一问题提出了区块链技术，但是，比特币只是将经济学概念中的交易数据写入了区块链，对于一些功能性的业务数据却并没有记录到区块链。因此针对这一现状，需要开发了一种将功能性数据写入区块链的方法。

[0003] 针对上述现有技术中，由于区块链上记录的数据只有交易数据没有业务数据，当业务数据被篡改的情况下，无法确保信息安全的问题，目前尚未提出有效的解决方案。

发明内容

[0004] 本发明实施例提供了一种在区块链上存储业务数据的处理方法和装置，以至少解决现有技术中，由于区块链上记录的数据只有交易数据没有业务数据，当业务数据被篡改的情况下，无法确保信息安全的技术问题。

[0005] 根据本发明实施例的一个方面，提供了一种业务数据的处理方法，包括：获取业务数据，并定义业务数据的交易类型；基于与交易类型对应的构建方法，根据业务数据构建待上传至区块链网络的目标数据；将目标数据存储到区块链网络中对应节点的区块链上。

[0006] 根据本发明实施例的另一方面，还提供了一种业务数据的处理装置，包括：获取单元，用于获取业务数据，并定义业务数据的交易类型；构建单元，用于基于与交易类型对应的构建方法，根据业务数据构建待上传至区块链网络的目标数据；存储单元，用于将目标数据存储到区块链网络中对应节点的区块链上。

[0007] 在本发明实施例中，通过获取业务数据，并定义业务数据的交易类型；基于与交易类型对应的构建方法，根据业务数据构建待上传至区块链网络的目标数据；将目标数据存储到区块链网络中对应节点的区块链上，达到了将业务数据存储到区块链以防止业务数据被篡改的目的，从而实现了提高业务数据的安全性的技术效果，进而解决了现有技术中，由于区块链上记录的数据只有交易数据没有业务数据，当业务数据被篡改的情况下，无法确保信息安全的技术问题。

附图说明

[0008] 此处所说明的附图用来提供对本发明的进一步理解，构成本申请的一部分，本发明的示意性实施例及其说明用于解释本发明，并不构成对本发明的不当限定。在附图中：

[0009] 图1是根据本发明实施例的一种在区块链上存储业务数据的处理方法流程图；

[0010] 图2是根据本发明实施例的一种可选的在区块链上存储业务数据的处理方法流程

图；

[0011] 图3是根据本发明实施例的一种可选的生成区块链数据的方法流程图；

[0012] 图4是根据本发明实施例的一种可选的在区块链上写入业务数据的方法流程图；以及

[0013] 图5是根据本发明实施例的一种在区块链上存储业务数据的处理装置示意图。

具体实施方式

[0014] 为了使本技术领域的人员更好地理解本发明方案，下面将结合本发明实施例中的附图，对本发明实施例中的技术方案进行清楚、完整地描述，显然，所描述的实施例仅仅是本发明一部分的实施例，而不是全部的实施例。基于本发明中的实施例，本领域普通技术人员在没有做出创造性劳动前提下所获得的所有其他实施例，都应当属于本发明保护的范围。

[0015] 需要说明的是，本发明的说明书和权利要求书及上述附图中的术语“第一”、“第二”等是用于区别类似的对象，而不必用于描述特定的顺序或先后次序。应该理解这样使用的数据在适当情况下可以互换，以便这里描述的本发明的实施例能够以除了在这里图示或描述的那些以外的顺序实施。此外，术语“包括”和“具有”以及他们的任何变形，意图在于覆盖不排他的包含，例如，包含了一系列步骤或单元的过程、方法、系统、产品或设备不必限于清楚地列出的那些步骤或单元，而是可包括没有清楚地列出的或对于这些过程、方法、产品或设备固有的其它步骤或单元。

[0016] 根据本发明实施例，提供了一种在区块链上存储业务数据的处理方法实施例，需要说明的是，在附图的流程图示出的步骤可以在诸如一组计算机可执行指令的计算机系统中执行，并且，虽然在流程图中示出了逻辑顺序，但是在某些情况下，可以以不同于此处的顺序执行所示出或描述的步骤。

[0017] 图1是根据本发明实施例的一种在区块链上存储业务数据的处理方法流程图，如图1所示，该方法包括如下步骤：

[0018] 步骤S102，获取业务数据，并定义业务数据的交易类型。

[0019] 具体地，上述业务数据可以是与交易关联的一些功能性业务数据，包括但不限于电量数据、用户数据(例如，注册、登录、访问、投票等)。这些业务数据可以扩展为一种交易，在区块链上记录。上述交易类型可以是预先定义的业务数据所属交易的类型，即不同的业务数据，其计算和交易方法可能均不相同，因而，在获取到业务数据后，至少要获取该业务数据的交易类型，以便根据该交易类型确定业务数据的计算或交易规则或方法。

[0020] 一种可选的实施例中，可以将功能性业务数据存储到数据库，并在配置文件中定义业务数据的交易类型。

[0021] 步骤S104，基于与交易类型对应的构建方法，根据业务数据构建待上传至区块链网络的目标数据。

[0022] 具体地，在根据获取到的业务数据确定该业务数据的类型后，可以基于该交易类型对应的构建方法，根据该业务数据构建对应的待上传至区块链网络的目标数据。

[0023] 作为一种可选的实施例，可以根据配置文件中定义的交易类型，设计业务数据的交易流程，具体地，构建共有的交易数据，同时根据不同类型交易调用相对应类的方法来处

理业务数据，在构建待上传至区块链网络的目标数据的时候，可以根据功能需求，调用功能性业务类的构造方法构建业务交易数据，并将功能性业务数据和主流程数据构建目标数据。

[0024] 步骤S106，将目标数据存储到区块链网络中对应节点的区块链上。

[0025] 具体地，在通过上述步骤S104构建待上传至区块链网络的目标数据后，将目标数据存储到区块链网络中对应节点的区块链上。

[0026] 由上可知，在本申请上述实施例中，在获取到任意一种业务的业务数据后，基于与该种交易类型对应的构建方法，根据获取到的业务数据构建待上传至区块链网络的目标数据，并将构建的目标数据存储到区块链网络中对应节点的区块链上，达到了将业务数据存储到区块链以防止业务数据被篡改的目的，从而实现了提高业务数据的安全性的技术效果，进而解决了现有技术中，由于区块链上记录的数据只有交易数据没有业务数据，当业务数据被篡改的情况下，无法确保信息安全的技术问题。

[0027] 需要说明的是，为了保证区块链上存储的数据的准确性，在将待上传至区块链网络的目标数据上传到区块链网络的时候，作为一种可选的实例，如图2所示，可以包括如下步骤：

[0028] 步骤S202，生成目标数据在区块链网络中的标识信息；

[0029] 步骤S204，基于标识信息，对目标数据的合法性进行验证；

[0030] 步骤S206，在验证目标数据合法的情况下，将目标数据存储到区块链网络中对应节点的区块链上。

[0031] 可选地，生成目标数据在区块链网络的标识信息，可以包括如下步骤：根据目标数据，生成对应的哈希值；根据哈希值，生成目标数据在区块链网络中的标识信息。

[0032] 可选地，根据目标数据，生成对应的哈希值，包括：对目标数据进行加密处理，得到加密后的数据，其中，加密处理包括如下至少之一：采用密钥加密、添加数字签名；根据加密后的数据，生成对应的哈希值。

[0033] 可选地，根据哈希值，生成目标数据在区块链网络中的标识信息，可以包括：将哈希值转换为对应的十六进制数值，将十六进制数值作为目标数据在区块链网络中的标识信息。

[0034] 可选地，在根据哈希值，生成目标数据在区块链网络中的标识信息之前，上述方法还可以包括：对哈希值进行加密处理，其中，加密处理包括如下至少之一：采用密钥加密、添加数字签名。

[0035] 一种可选的实施例中，上述标识信息可以是目标数据对应的交易ID，对目标数据添加间戳、签名、并基于哈希算法生成对应的交易ID，具体地，作为一种可选的实施方式，可以获取当前时间，并记录交易时间戳，引入Node.js的加解密模块Crypto模块进行加密，通过Ed25519组件签名认证，并对签名后的目标数据通过sha256哈希算法生成简单哈希值。可选地，还可以利用签名算法Ed25519对上述哈希值加上密钥进行签名。进一步地，还可以对生成的哈希值进行再一次加密，并对加密后的哈希值(二进制数)进行多进制(例如，16进制)处理，生成对应的交易ID。

[0036] 可选地，作为一种可选的实施例，基于标识信息，对目标数据的合法性进行验证，可以包括如下步骤：对目标数据进行业务验证；在目标数据通过业务验证的情况下，基于标

识信息，对目标数据的合法性进行验证。

[0037] 具体地，在对目标数据的合法性进行验证时，不仅要对目标数据的交易ID、签名、时间戳等信息进行验证，还要对目标数据的业务逻辑进行验证，例如，当业务数据为电量数据的情况下需要验证电量数据是否符合电量计算规则等。

[0038] 可选地，在目标数据通过业务验证的情况下，基于标识信息，对目标数据的合法性进行验证，可以包括：在目标数据通过业务验证的情况下，基于标识信息，判断目标区块链上是否存在目标数据；在目标区块链上不存在目标数据的情况下，基于标识信息，对目标数据的合法性进行验证。

[0039] 其中，作为一种可选的实施方式，将目标数据存储到区块链网络中对应节点的区块链上，可以包括如下步骤：如果目标数据被记载在目标区块链上，则区块链网络中其他节点将目标数据同步至对应的区块链上；如果目标数据未被记载在目标区块链上，则目标区块链的节点将目标数据广播至区块链网络上的其他节点，其中，通过任意一个节点验证的目标数据被存储到对应的区块链上。

[0040] 具体地，在对目标数据进行合法性验证后，未被区块链网络节点确认的目标数据需要通过P2P网络进行广播，广播出去之后可能会被任何一个节点经过验证之后记录进区块链；如果目标数据被区块链网络的某个节点写入到区块了，那么其他的节点就会将此区块同步过来(包括交易)，然后进行验证，并解决分叉问题。利用区块链技术进行同步，待其他节点验证成功后插入自己区块链数据库中。

[0041] 作为一种优选的实施例，图3是根据本发明实施例的一种可选的生成区块链数据的方法流程图，如图3所示，在构建待上传至区块链网络的目标数据后，可以为待上传至区块链的目标数据添加时间戳，并对添加时间戳后的目标数据进行加密，生成对应的哈希值，然后使用业务方提供的密钥对哈希值添加数字签名，并对添加数字签名的目标数据进行十六进制处理，得到目标数据的标识信息(例如，交易ID)，以便基于该标识信息上传到区块链网络。

[0042] 作为一种优选的实施例，图4是根据本发明实施例的一种可选的在区块链上写入业务数据的方法流程图，如图4所示，包括如下步骤：

[0043] (1)创建一个配置文件，定义交易类型，包括但不限于功能性交易和转账交易；

[0044] (2)将创建的或者采集的某些功能性业务数据存储到数据库以便后面在构建交易数据的时候查询；

[0045] (3)导入用户数据，包括用户密码(私钥)，地址等数据；

[0046] (4)利用前面的用户数据构建交易的公共数据，以供后面步骤的数字签名和验证等功能使用。

[0047] (5)在上步之后，通过判断交易类型调用相应交易类型的相应方法构建业务数据。

[0048] (6)将上两步构建的数据组合成一个完整的交易数据。

[0049] (7)对交易进行签名，以防止数据在传播过程中被篡改，在这里举例将电表数据写入到交易里面去。

[0050] (8)对交易做hash等一系列处理，生成一个交易ID，以便后面的验证。

[0051] (9)根据需求对交易做进一步的处理(例如，对电量数据的四舍五入、取整等处理操作)。

[0052] (10)再次验证交易的合法性,防止在处理过程中产生不合法的数据。

[0053] (11)再次验证功能性业务数据是否被篡改,防止在处理过程中发生改动。

[0054] (12)判断交易是否存在,如果存在,那么将不做后续处理。

[0055] (13)如果交易不存在,那么将验证交易的签名、时间戳等信息。

[0056] (14)此时系统的另外一个线程每隔16秒就会产生一个区块,并且会将未经确认的交易写入最后产生的区块。

[0057] (15)如果交易还未来及时被写入,那么交易将通过p2p网络广播出去,这样就实现了分布式的存储,防止单个节点被攻击之后数据丢失或者被篡改。

[0058] (16)广播出去之后可能会被任何一个节点经过验证之后记录进区块链。

[0059] (17)如果交易被写入到区块了,那么其他的节点就会将此区块同步过来(包括交易),然后进行验证,并解决分叉问题。

[0060] (18)验证通过之后将区块和交易保存到本地数据库。

[0061] 通过本申请上述实施例,每次全网升级的时候,可以根据需求在底层新增一些功能性交易类型,相比于智能合约,此方法的解析相对简单,管理成本低廉,针对性较强。

[0062] 根据本发明实施例,还提供了一种用于实现上述在区块链上存储业务数据的处理方法的装置实施例,图5是根据本发明实施例的一种在区块链上存储业务数据的处理装置示意图,如图5所示,该装置包括:获取单元501、构建单元503和存储单元505。

[0063] 其中,获取单元501,用于获取业务数据,并定义业务数据的交易类型;

[0064] 构建单元503,用于基于与交易类型对应的构建方法,根据业务数据构建待上传至区块链网络的目标数据;

[0065] 存储单元505,用于将目标数据存储到区块链网络中对应节点的区块链上。

[0066] 此处需要说明的是,上述获取单元501、构建单元503和存储单元505对应于方法实施例中的步骤S102至S106,上述模块与对应的步骤所实现的示例和应用场景相同,但不限于上述方法实施例所公开的内容。需要说明的是,上述模块作为装置的一部分可以在诸如一组计算机可执行指令的计算机系统中执行。

[0067] 由上可知,在本申请上述实施例中,在通过获取单元501获取到任意一种业务的业务数据后,通过构建单元503基于与该种交易类型对应的构建方法,根据获取到的业务数据构建待上传至区块链网络的目标数据,并通过存储单元505将构建的目标数据存储到区块链网络中对应节点的区块链上,达到了将业务数据存储到区块链以防止业务数据被篡改的目的,从而实现了提高业务数据的安全性的技术效果,进而解决了现有技术中,由于区块链上记录的数据只有交易数据没有业务数据,当业务数据被篡改的情况下,无法确保信息安全的技术问题。

[0068] 在一种可选的实例中,上述存储单元可以包括:生成模块,用于生成目标数据在区块链网络中的标识信息;验证模块,用于基于标识信息,对目标数据的合法性进行验证;存储模块,用于在验证目标数据合法的情况下,将目标数据存储到区块链网络中对应节点的区块链上。

[0069] 可选地,上述生成模块可以包括:第一生成子模块,用于根据目标数据,生成对应的哈希值;第二生成子模块,用于根据哈希值,生成目标数据在区块链网络中的标识信息。

[0070] 可选地,上述第一生成子模块还用于对目标数据进行加密处理,得到加密后的数

据，并根据加密后的数据，生成对应的哈希值，其中，加密处理包括如下至少之一：采用密钥加密、添加数字签名。

[0071] 可选地，上述第二生成子模块还用于将哈希值转换为对应的十六进制数值，将十六进制数值作为目标数据在区块链网络中的标识信息。

[0072] 在一种可选的实施例，上述装置还可以包括：加密模块，用于对哈希值进行加密处理，其中，加密处理包括如下至少之一：采用密钥加密、添加数字签名。

[0073] 在一种可选的实施例，上述验证模块还用于对目标数据进行业务验证，并在目标数据通过业务验证的情况下，基于标识信息，对目标数据的合法性进行验证。

[0074] 在一种可选的实施例，上述验证模块还用于在目标数据通过业务验证的情况下，基于标识信息，判断目标区块链上是否存在目标数据，并在目标区块链上不存在目标数据的情况下，基于标识信息，对目标数据的合法性进行验证。

[0075] 在一种可选的实施例，上述存储单元包括：同步模块，用于如果目标数据被记载在目标区块链上，则区块链网络中其他节点将目标数据同步至对应的区块链上；传播模块，用于如果目标数据未被记载在目标区块链上，则目标区块链的节点将目标数据广播至区块链网络上的其他节点，其中，通过任意一个节点验证的目标数据被存储到对应的区块链上。

[0076] 根据本发明实施例，还提供了一种存储介质，存储介质包括存储的程序，其中，程序执行上述方法实施例中任意一项的可选的或优选的在区块链上存储业务数据的处理方法。

[0077] 根据本发明实施例，还提供了一种处理器，其特征在于，处理器用于运行程序，其中，程序运行时执行上述方法实施例中任意一项的可选的或优选的在区块链上存储业务数据的处理方法。

[0078] 上述本发明实施例序号仅仅为了描述，不代表实施例的优劣。

[0079] 在本发明的上述实施例中，对各个实施例的描述都各有侧重，某个实施例中没有详述的部分，可以参见其他实施例的相关描述。

[0080] 在本申请所提供的几个实施例中，应该理解到，所揭露的技术内容，可通过其它的方式实现。其中，以上所描述的装置实施例仅仅是示意性的，例如所述单元的划分，可以为一种逻辑功能划分，实际实现时可以有另外的划分方式，例如多个单元或组件可以结合或者可以集成到另一个系统，或一些特征可以忽略，或不执行。另一点，所显示或讨论的相互之间的耦合或直接耦合或通信连接可以是通过一些接口，单元或模块的间接耦合或通信连接，可以是电性或其它的形式。

[0081] 所述作为分离部件说明的单元可以是或者也可以不是物理上分开的，作为单元显示的部件可以是或者也可以不是物理单元，即可以位于一个地方，或者也可以分布到多个单元上。可以根据实际的需要选择其中的部分或者全部单元来实现本实施例方案的目的。

[0082] 另外，在本发明各个实施例中的各功能单元可以集成在一个处理单元中，也可以是各个单元单独物理存在，也可以两个或两个以上单元集成在一个单元中。上述集成的单元既可以采用硬件的形式实现，也可以采用软件功能单元的形式实现。

[0083] 所述集成的单元如果以软件功能单元的形式实现并作为独立的产品销售或使用时，可以存储在一个计算机可读取存储介质中。基于这样的理解，本发明的技术方案本质上或者说对现有技术做出贡献的部分或者该技术方案的全部或部分可以以软件产品的形式

体现出来，该计算机软件产品存储在一个存储介质中，包括若干指令用以使得一台计算机设备(可为个人计算机、服务器或者网络设备等)执行本发明各个实施例所述方法的全部或部分步骤。而前述的存储介质包括：U盘、只读存储器(ROM，Read-Only Memory)、随机存取存储器(RAM，Random Access Memory)、移动硬盘、磁碟或者光盘等各种可以存储程序代码的介质。

[0084] 以上所述仅是本发明的优选实施方式，应当指出，对于本技术领域的普通技术人员来说，在不脱离本发明原理的前提下，还可以做出若干改进和润饰，这些改进和润饰也应视为本发明的保护范围。

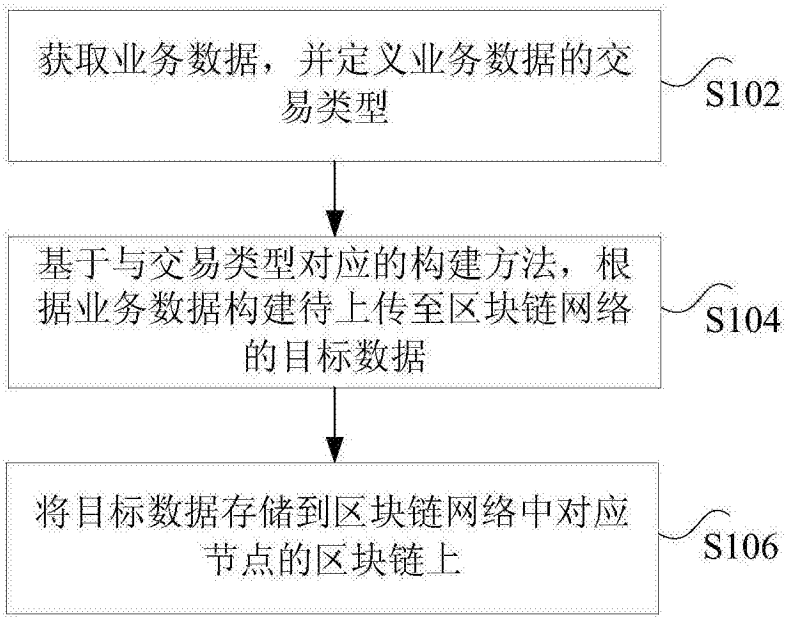

获取业务数据，并定义业务数据的交易类型
S102
基于与交易类型对应的构建方法，根据业务数据构建待上传至区块链网络的目标数据
S104
将目标数据存储到区块链网络中对应节点的区块链上
S106

图1

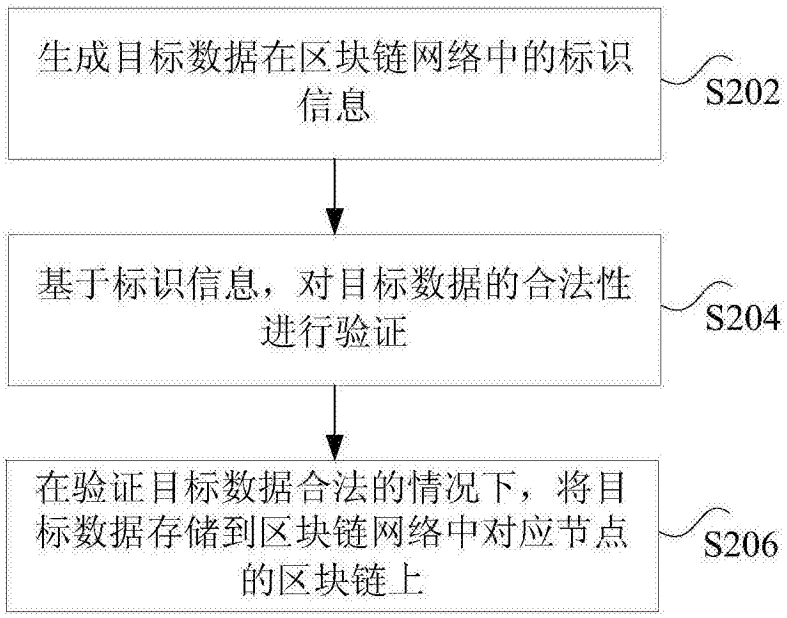

生成目标数据在区块链网络中的标识信息
S202
基于标识信息，对目标数据的合法性进行验证
S204
在验证目标数据合法的情况下，将目标数据存储到区块链网络中对应节点的区块链上
S206

图2

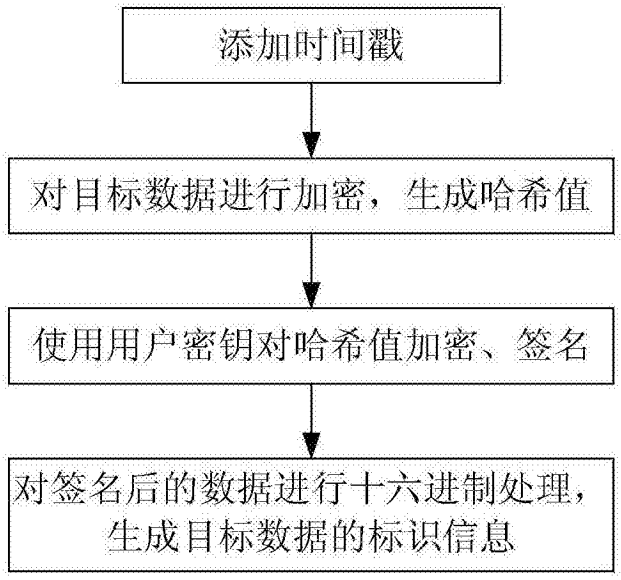

添加时间戳
对目标数据进行加密，生成哈希值
使用用户密钥对哈希值加密、签名
对签名后的数据进行十六进制处理，
生成目标数据的标识信息

图3

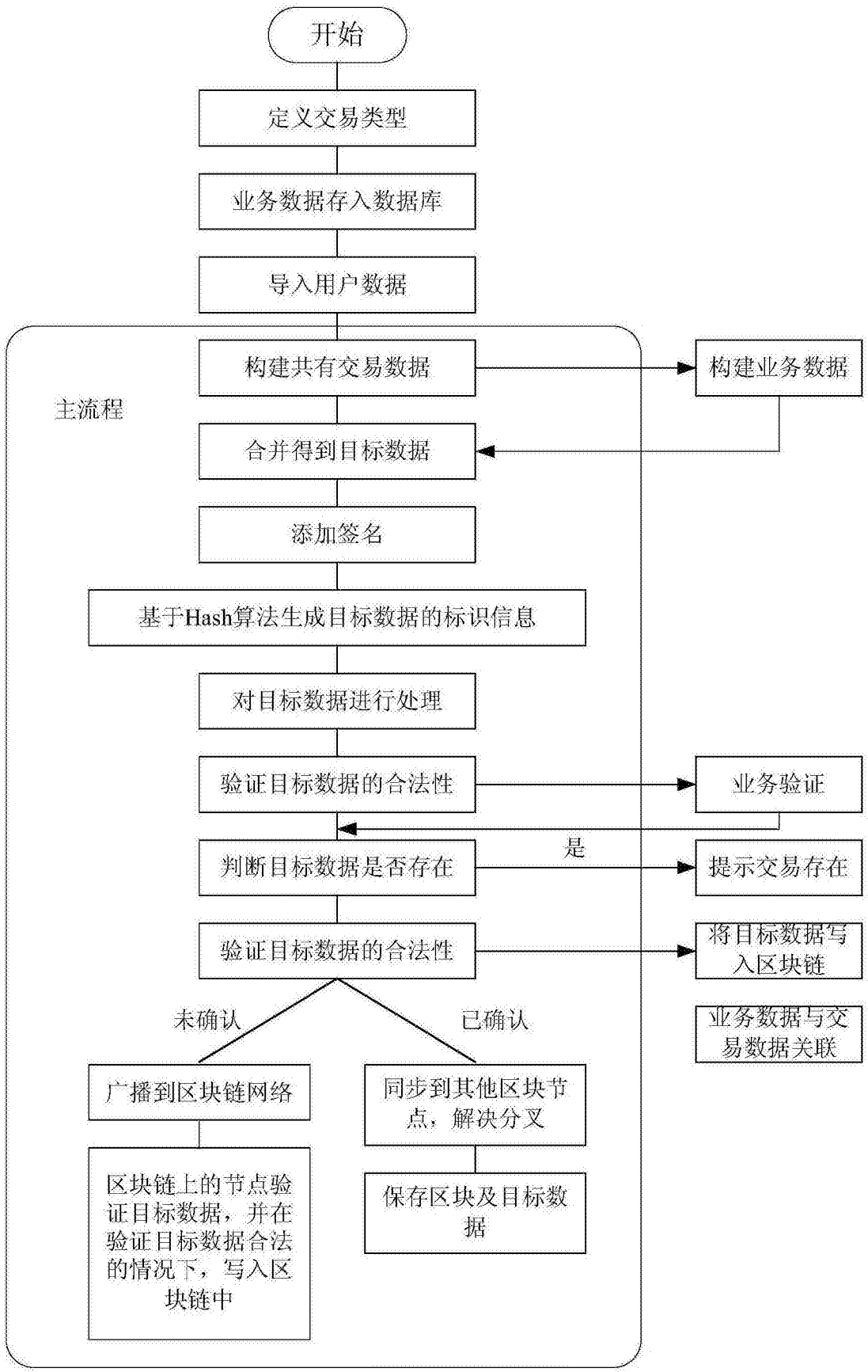

开始
定义交易类型
业务数据存入数据库
导入用户数据
主流程
构建共有交易数据
构建业务数据
合并得到目标数据
添加签名
基于Hash算法生成目标数据的标识信息
对目标数据进行处理
验证目标数据的合法性
业务验证
判断目标数据是否存在
是
提示交易存在
验证目标数据的合法性
将目标数据写入区块链
业务数据与交易数据关联
未确认
已确认
广播到区块链网络
同步到其他区块节点，解决分叉
区块链上的节点验证目标数据，并在验证目标数据合法的情况下，写入区块链中
保存区块及目标数据

图4

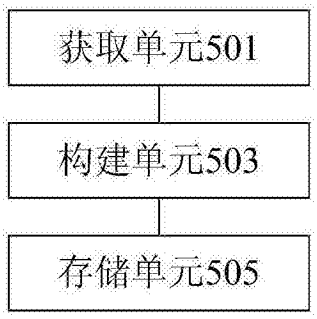


图5