(19)中华人民共和国国家知识产权局

(12)发明专利

(10)授权公告号 CN 107104977 B
(45)授权公告日 2020.07.31

(21)申请号 201710367410.3

(22)申请日 2017.05.23

(65)同一申请的已公布的文献号
申请公布号 CN 107104977 A

(43)申请公布日 2017.08.29

(73)专利权人 北京天德科技有限公司
地址 100089 北京市海淀区知春路113号1708-048

(72)发明人 邓恩艳

(51)Int.Cl.
H04L 29/06(2006.01)
H04L 9/08(2006.01)

(56)对比文件
CN 106100847 A,2016.11.09,
CN 101998392 A,2011.03.30,
CN 106549933 A,2017.03.29,
CN 106656784 A,2017.05.10,
US 2005172132 A1,2005.08.04,
US 2003172278 A1,2003.09.11,

审查员 李凯

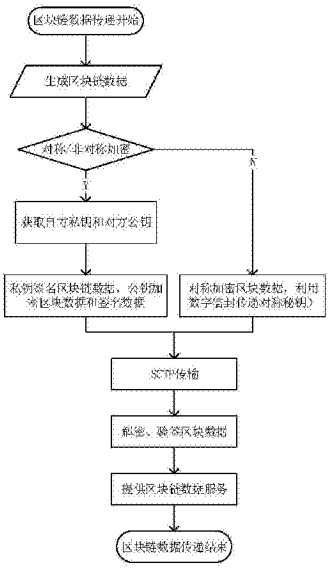
权利要求书2页 说明书4页 附图3页

(54)发明名称

一种基于SCTP协议的区块链数据安全传输方法

(57)摘要

本发明公开了一种基于SCTP协议的区块链数据安全传输方法，包括以下步骤：S1、应用层获取非对称加密的公私钥对、对称加密秘钥，并对区块链数据进行签名、加密；S2、传输层使用SCTP协议对数据包进行传递；S3、应用层获取非对称加密的公私钥对、对称加密秘钥，并对区块链数据进行解密、验签。本发明的有益效果在于，提供一种安全高速的区块链数据的传输方法。



CN 107104977 B

1.一种基于SCTP协议的区块链数据安全传输方法，其特征在于，包括以下步骤：

S1、应用层客户端获取非对称加密的公私钥对、对称加密秘钥，并对区块链数据进行签名、加密；

S2、传输层使用SCTP协议对数据进行传输：

S21：SCTP通过4次握手建立偶联；

S22：SCTP基于多宿主、多流、消息分帧协议技术传递加密后的区块链数据；

S23：SCTP平滑关闭本次传输套接字；

S24：如果有多次数据传输需求，重复S21-S23；

S3、应用层服务端获取非对称加密的公私钥对、对称加密秘钥，并对区块链数据进行解密、验签。

2.根据权利要求1所述的基于SCTP协议的区块链数据安全传输方法，其特征在于：所述步骤S1中对区块链数据签名和加密方式的实现方法之一具体包括以下步骤：

S11：采用非对称加密，获取自方私钥对区块链数据进行签名，从电子认证服务CA或其他密钥管理Key Management中获取对方公钥，对签名字符串和区块链数据进行公钥加密，得到加密数据P11。

3.根据权利要求2所述的基于SCTP协议的区块链数据安全传输方法，其特征在于：所述步骤S1中对区块链数据签名和加密方式的实现方法之二具体包括以下步骤：

S12：采用对称加密结合数字信封传递对称秘钥，获取自方私钥对区块链数据进行签名，从电子认证服务CA或其他密钥管理Key Management中获取对方公钥，对签名字符串和区块链数据进行对称加密，得到加密数据P12，使用对方公钥将对称秘钥进行加密，得到加密数据P13。

4.根据权利要求3所述的基于SCTP协议的区块链数据安全传输方法，其特征在于：使用S11的数据签名和加密方式实现S1步骤，则步骤S2中对区块链数据进行传输的步骤为：通过SCTP协议套接字接口Socket API将S11中的加密数据P11经过传输层SCTP协议递交给下层分组网络。

5.根据权利要求4所述的基于SCTP协议的区块链数据安全传输方法，其特征在于：使用S12的数据签名和加密方式实现S1步骤，则步骤S2中对区块链数据进行传输的步骤为：通过SCTP协议套接字接口Socket API将S12中的加密数据P12和加密数据P13经过传输层SCTP协议递交给下层分组网络。

6.根据权利要求5所述的基于SCTP协议的区块链数据安全传输方法，其特征在于：使用S11的数据签名和加密方式实现S1步骤，则所述步骤S3中对区块链数据解密和验签方式具体包括以下步骤：

S31：获取自方私钥对SCTP传递的加密区块链数据进行解密，从CA或其他Key Management中获取对方公钥，对签名字符串和区块链数据进行公钥验签。

7.根据权利要求6所述的基于SCTP协议的区块链数据安全传输方法，其特征在于：使用S12的数据签名和加密方式实现S1步骤，则所述步骤S3中对区块链数据解密和验签方式具体包括以下步骤：

S32：获取自方私钥将非对称加密的对称秘钥进行解密，利用对称秘钥对加密的区块链数据进行解密，从CA或其他Key Management中获取对方公钥，对区块链数据进行验签。

8.根据权利要求7所述的基于SCTP协议的区块链数据安全传输方法，其特征在于：所述数据安全传输方法适用于区块链共识节点之间的区块数据传输。

9.根据权利要求8所述的基于SCTP协议的区块链数据安全传输方法，其特征在于：所述数据安全传输方法适用于区块链共识节点与存储节点之间的区块数据传输。

10.根据权利要求9所述的基于SCTP协议的区块链数据安全传输方法，其特征在于：所述数据安全传输方法适用于区块链存储节点之间的区块数据传输。

一种基于SCTP协议的区块链数据安全传输方法

技术领域

[0001] 本发明涉及一种区块链数据传输的方法，尤其涉及一种使用SCTP协议对区块链数据进行安全传输的方法。

背景技术

[0002] 基于对等协议传输区块链数据是目前常用的区块链数据传输方式，目前对等网络大部分是建立在UDP或TCP协议基础之上。

[0003] 在区块链数据传输的对等网络环境中，计算机节点之间不依赖专用的集中服务器，每一个节点既能充当网络服务的请求者，又能对其它节点的请求提供服务，但这样的架构却存在数据安全性差、实时性差、数据冗余度大、不可预测、不可控等问题。

发明内容

[0004] 为了克服上述现有技术的不足，本发明提供了一种基于SCTP协议的区块链数据安全传输方法。

[0005] 本发明提供了一种基于SCTP协议的区块链数据安全传输方法，包括以下步骤：

[0006] S1、应用层客户端获取非对称加密的公私钥对、对称加密秘钥，并对区块链数据进行签名、加密；

[0007] S2、传输层使用SCTP协议对数据包进行传递；

[0008] S3、应用层服务端获取非对称加密的公私钥对、对称加密秘钥，并对区块链数据进行解密、验签。

[0009] 所述步骤S1中对区块链数据签名和加密方式具体可以使用S11或S12的实现方式，分别包括以下步骤：

[0010] S11：采用非对称加密，获取自方私钥对区块链数据进行签名，从电子认证服务CA或其他密钥管理Key Management中获取对方公钥，对签名字符串和区块链数据进行公钥加密，得到加密数据P11；

[0011] S12：采用对称加密结合数字信封传递对称秘钥，获取自方私钥对区块链数据进行签名，从电子认证服务CA或其他密钥管理Key Management中获取对方公钥，对签名字符串和区块链数据进行对称加密，得到加密数据P12，使用对方公钥将对称秘钥进行加密，得到加密数据P13。

[0012] 所述步骤S2中对区块链数据进行传输的步骤为：

[0013] S21：SCTP通过4次握手建立偶联；

[0014] S22：SCTP基于多宿主、多流、消息分帧协议技术传递加密后的区块链数据；

[0015] S23：SCTP平滑关闭本次传输套接字；

[0016] S24：如果有多次数据传输需求，重复S21-S23。

[0017] 进一步地，使用S11的数据签名和加密方式实现S1步骤，则步骤S2中对区块链数据进行传输的步骤为：通过SCTP协议套接字接口Socket API将S11中的加密数据P11经过传输

层SCTP协议递交给下层分组网络。

[0018] 进一步地，使用S12的数据签名和加密方式实现S1步骤，则步骤S2中对区块链数据进行传输的步骤为：通过SCTP协议套接字接口Socket API将S12中的加密数据P12和P13经过传输层SCTP协议递交给下层分组网络。

[0019] 使用S11的数据签名和加密方式实现S1步骤，则所述步骤S3中对区块链数据解密和验签方式具体包括以下步骤：

[0020] S31：获取自方私钥对SCTP传递的加密区块链数据进行解密，从电子认证服务CA或其他密钥管理Key Management中获取对方公钥，对签名字符串和区块链数据进行公钥验签。

[0021] 使用S12的数据签名和加密方式实现S1步骤，则所述步骤S3中对区块链数据解密和验签方式具体包括以下步骤：

[0022] S32：获取自方私钥将非对称加密的对称秘钥进行解密，利用对称秘钥对加密的区块链数据进行解密，从电子认证服务CA或其他密钥管理Key Management中获取对方公钥，对区块链数据进行验签。

[0023] 本发明具有以下优点和有益效果：本发明提供一种基于SCTP协议的区块链数据安全传输方法，这种区块链数据传输方法可以利用现有以太网组网结构提升区块链数据传输的安全性、实时性、降低网络传输的数据冗余等问题。

附图说明

[0024] 图1为本发明选取代表性非对称加密算法RSA为典型实施例1提供的一种基于SCTP协议的区块链数据安全传输方法的流程图。

[0025] 图2为本发明选取代表性非对称加密算法RSA和对称加密算法AES为典型实施例2提供的一种基于SCTP协议的区块链数据安全传输方法的流程图。

[0026] 图3为本发明提供的一种基于SCTP协议的区块链数据安全传输方法的整体业务流程图。

具体实施方式

[0027] 为了使本发明的目的、技术方案及优点更加清楚明白，以下结合附图及实施例，对本发明进行进一步详细说明。应当理解，此处所描述的具体实施例仅仅用以解释本发明，并不用于限定本发明。本实施例的附图中相同或相似的标号对应相同或相似的部件；在本发明的描述中，需要说明的是，除非另有说明，“多个”的含义是两个或两个以上；术语“上”、“下”、“左”、“右”、“内”、“外”、“前端”、“后端”、“头部”、“尾部”等指示的方位或位置关系为基于附图所示的方位或位置关系，仅是为了便于描述本发明和简化描述，而不是指示或暗示所指的装置或元件必须具有特定的方位、以特定的方位构造和操作，因此不能理解为对本发明的限制。此外，术语“第一”、“第二”、“第三”等仅用于描述目的，而不能理解为指示或暗示相对重要性。

[0028] 在本发明的描述中，还需要说明的是，除非另有明确的规定和限定，术语“安装”、“相连”、“连接”应做广义理解，例如，可以是固定连接，也可以是可拆卸连接，或一体地连接；可以是硬连接，也可以是软连接；可以是直接相连，也可以通过中间媒介间接相连。对于

本领域的普通技术人员而言，可视具体情况理解上述术语在本发明中的具体含义。

[0029] 下面结合附图1对本发明的实施例1进一步说明。

[0030] 如附图1所示：本发明选取代表性非对称加密算法RSA为典型实施例1提供的一种基于SCTP协议的区块链数据安全传输方法包括以下步骤：

[0031] S1、应用层获取RSA公私钥对并对区块链数据进行签名、加密；

[0032] S2、传输层使用SCTP协议对数据包进行传递；

[0033] S3、应用层获取RSA公私钥对并对区块链数据进行解密、验签。

[0034] 作为上述实施例的优选实施方式，步骤S1中，我们选择非对称加密算法RSA作为典型实施例，包括但不仅限于采用RSA，ECC，SM2等非对称加密算法。所述步骤S1中对区块链数据签名和加密方式具体包括以下步骤：

[0035] S11：采用RSA非对称加密，获取自方私钥，对区块链数据进行签名，从电子认证服务CA或其他密钥管理Key Management中获取对方RSA公钥，对签名字符串和区块链数据进行RSA公钥加密，得到加密数据P11。

[0036] 所述步骤S2中对区块链数据进行传输的步骤为：

[0037] S21：SCTP通过4次握手建立偶联；

[0038] S22：SCTP基于多宿主、多流、消息分帧协议技术传递加密后的区块链数据；

[0039] S23：SCTP平滑关闭本次传输套接字；

[0040] S24：如果有多次数据传输需求，重复S21-S23。

[0041] 所述步骤S3中对区块链数据解密和验签方式具体包括以下步骤：

[0042] S31：采用RSA非对称加密，获取自方私钥对SCTP传递的加密区块链数据进行解密，从电子认证服务CA或其他密钥管理Key Management中获取对方RSA公钥，对签名字符串和区块链数据进行公钥验签。

[0043] 下面结合附图2对本发明的实施例2进一步说明。

[0044] 如附图2所示：本发明选取代表性非对称加密算法RSA和对称加密算法AES为典型实施例2提供的一种基于SCTP协议的区块链数据安全传输方法包括以下步骤：

[0045] S1、应用层获取RSA公私钥对和AES秘钥并对区块链数据进行签名、加密；

[0046] S2、传输层使用SCTP协议对数据包进行传递；

[0047] S3、应用层获取RSA公私钥对和AES秘钥并对区块链数据进行解密、验签。

[0048] 作为上述实施例的优选实施方式，步骤S1中，我们选择非对称加密算法RSA和对称加密算法AES作为典型实施例2，包括但不仅限于采用RSA，ECC，SM2等非对称加密算法和AES、DES等对称加密算法构造的数字信封，所述步骤S1中对区块链数据签名和加密方式具体包括以下步骤：

[0049] S12：采用AES对称加密结合RSA数字信封传递对称秘钥，获取自方RSA私钥对区块链数据进行签名，从电子认证服务CA或其他密钥管理Key Management中获取对方RSA公钥，对签名字符串和区块链数据进行AES对称加密，得到加密数据P12，使用对方RSA公钥将AES对称秘钥进行加密，得到加密数据P13。

[0050] 所述步骤S2中对区块链数据进行传输的步骤为：

[0051] S21：SCTP通过4次握手建立偶联；

[0052] S22：SCTP基于多宿主、多流、消息分帧协议技术传递加密后的区块链数据；

[0053] S23:SCTP平滑关闭本次传输套接字;

[0054] S24:如果有多次数据传输需求,重复S21-S23。

[0055] 所述步骤S3中对区块链数据解密和验签方式具体包括以下与S1相对应的步骤:

[0056] S31:采用AES对称加密结合RSA数字信封传递AES对称秘钥,获取RSA自方私钥将RSA非对称加密的AES对称秘钥进行解密,利用AES对称秘钥对加密的区块链数据进行解密,从电子认证服务CA或其他密钥管理Key Management中获取对方RSA公钥,对区块链数据进行验签。

[0057] 最后说明的是:以上所述的2个实施例仅为本发明的较佳实施例而已,并不用以限制本发明,凡在本发明的精神和原则之内所作的任何修改、等同替换和改进等,均应包含在本发明的保护范围之内。

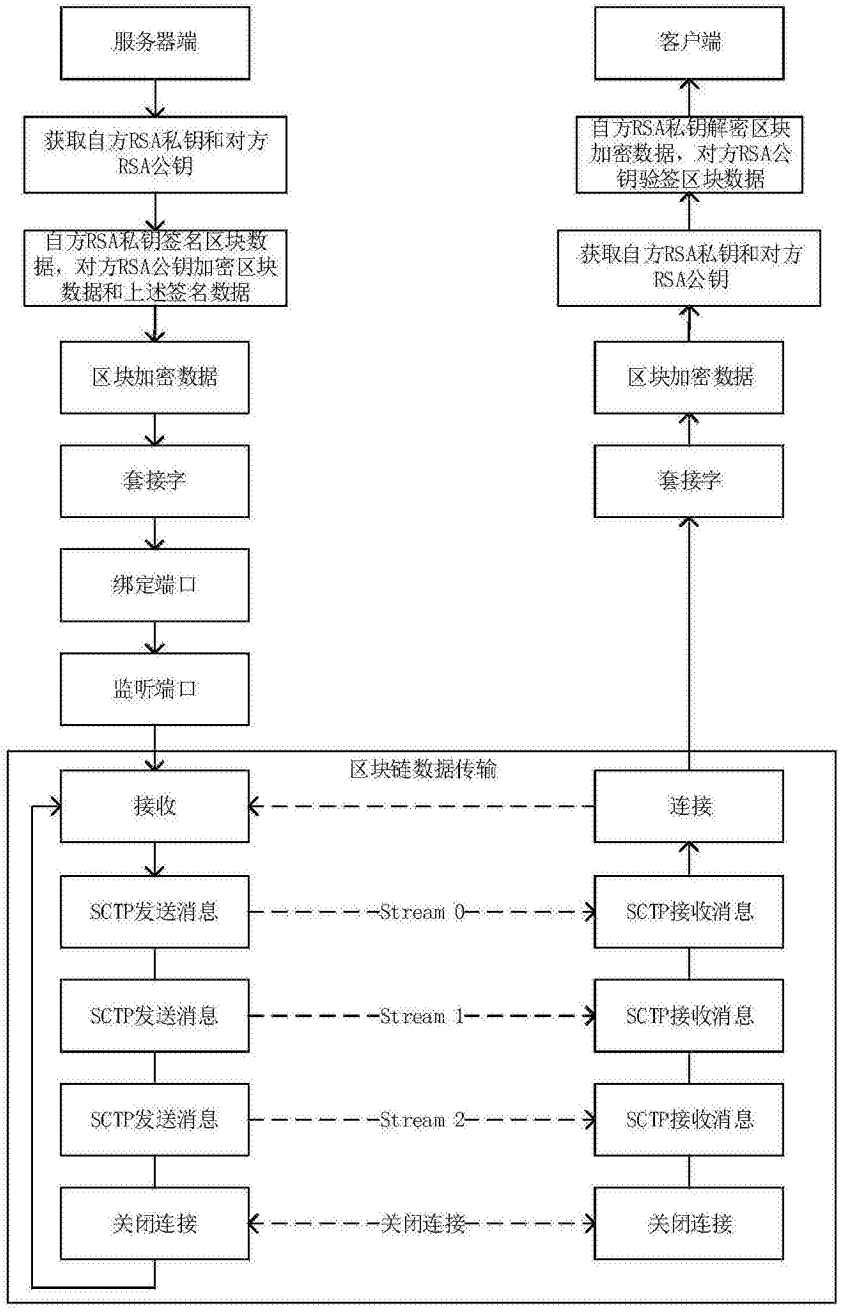

服务器端
获取自方RSA私钥和对方RSA公钥
自方RSA私钥签名区块数据，对方RSA公钥加密区块数据和上述签名数据
区块加密数据
套接字
绑定端口
监听端口
区块链数据传输
接收
SCTP发送消息
Stream 0
SCTP发送消息
Stream 1
SCTP发送消息
Stream 2
关闭连接
关闭连接
客户端
自方RSA私钥解密区块加密数据，对方RSA公钥验签区块数据
获取自方RSA私钥和对方RSA公钥
区块加密数据
套接字
连接
SCTP接收消息
SCTP接收消息
SCTP接收消息
关闭连接

图1

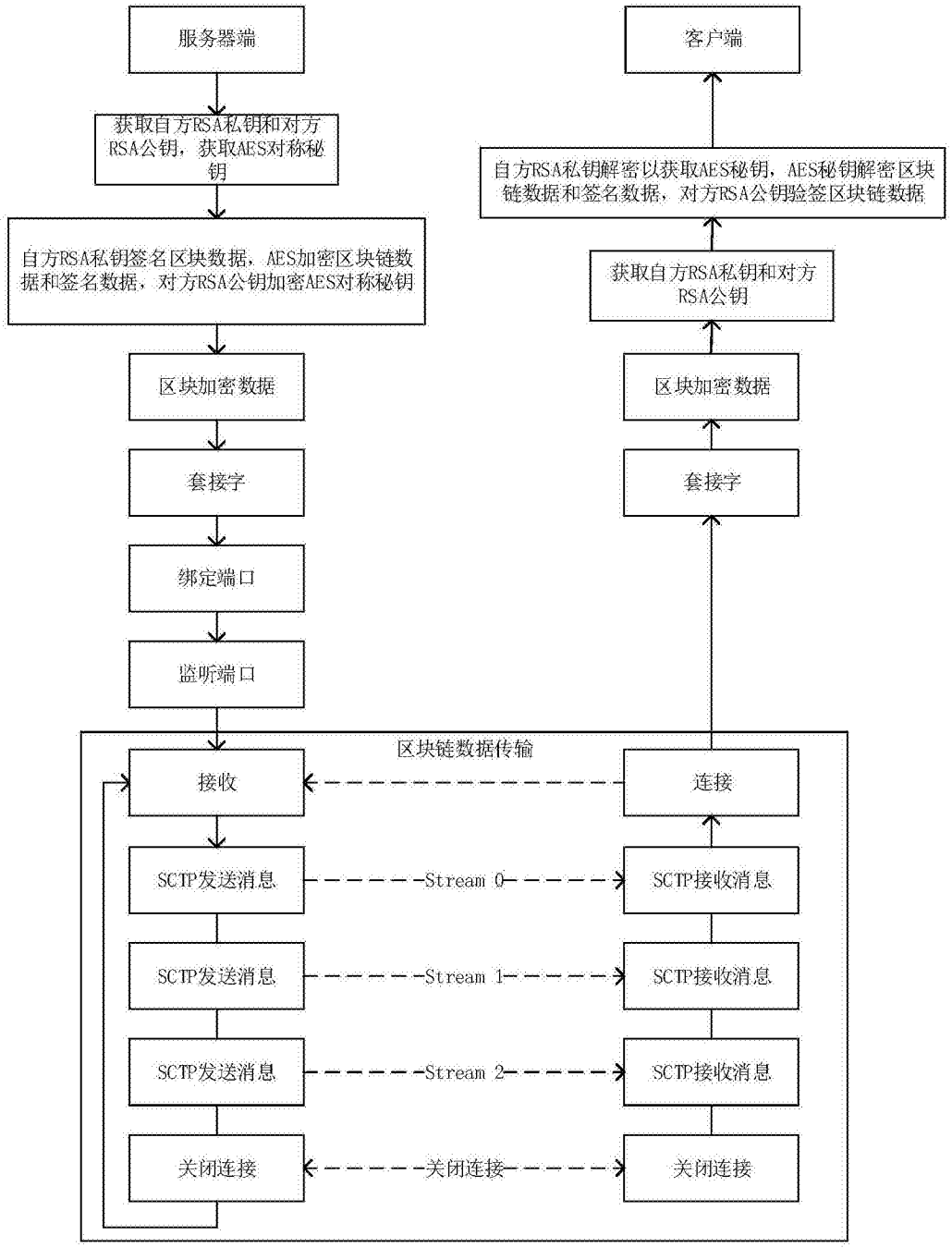

服务器端
获取自方RSA私钥和对方RSA公钥，获取AES对称秘钥
自方RSA私钥签名区块数据，AES加密区块链数据和签名数据，对方RSA公钥加密AES对称秘钥
区块加密数据
套接字
绑定端口
监听端口
客户端
自方RSA私钥解密以获取AES秘钥，AES秘钥解密区块链数据和签名数据，对方RSA公钥验签区块链数据
获取自方RSA私钥和对方RSA公钥
区块加密数据
套接字
区块链数据传输
接收
连接
SCTP发送消息
Stream 0
SCTP接收消息
SCTP发送消息
Stream 1
SCTP接收消息
SCTP发送消息
Stream 2
SCTP接收消息
关闭连接
关闭连接
关闭连接

图2

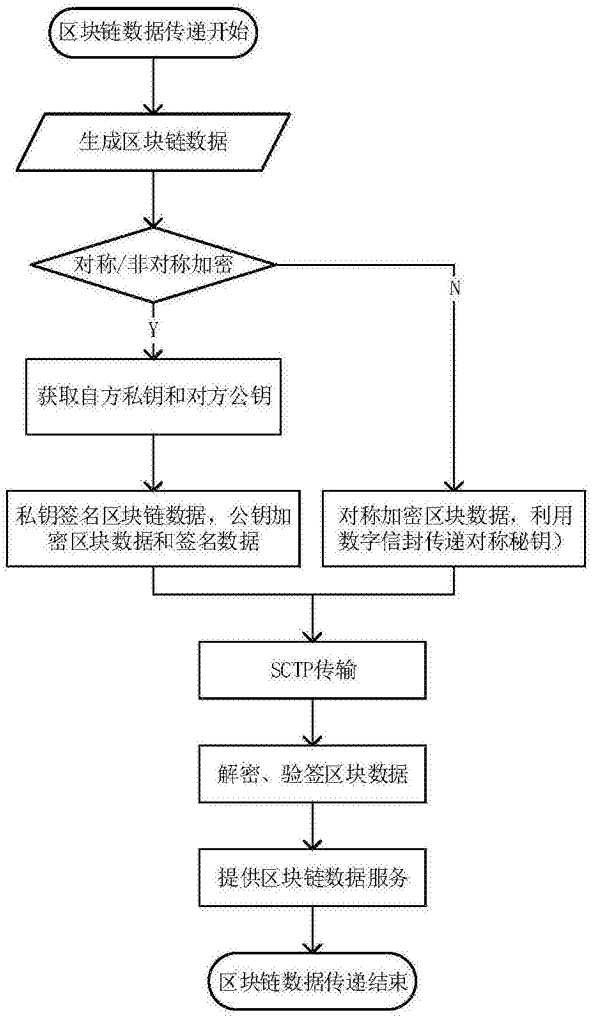

区块链数据传递开始
生成区块链数据
对称/非对称加密
N
Y
获取自方私钥和对方公钥
私钥签名区块链数据，公钥加密区块数据和签名数据
对称加密区块数据，利用数字信封传递对称秘钥）
SCTP传输
解密、验签区块数据
提供区块链数据服务
区块链数据传递结束

图3