(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 111552991 A
(43)申请公布日 2020.08.18

(21)申请号 202010356265.0

(22)申请日 2020.04.29

(71)申请人 支付宝实验室(新加坡)有限公司
地址 新加坡珊顿大道8号安盛大厦45-01号

(72)发明人 鲁泽增 魏玮 王林青 陈春伟

(74)专利代理机构 北京博思佳知识产权代理有限公司 11415
代理人 田雅

(51)Int.Cl.
G06F 21/64(2013.01)
G06Q 40/04(2012.01)

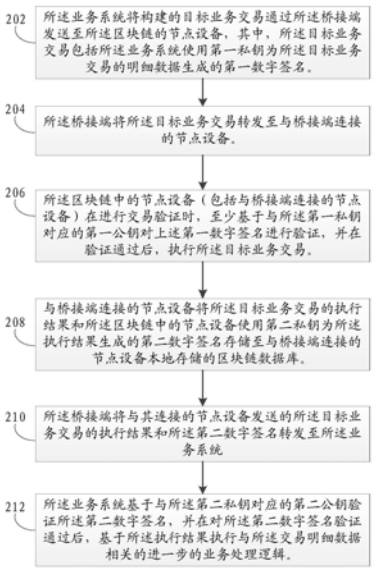
权利要求书5页 说明书15页 附图3页

(54)发明名称

一种区块链交易方法及装置

(57)摘要

本说明书提供了一种区块链交易方法和装置,包括:业务系统将构建的目标业务交易通过所述桥接端发送至所述区块链的节点设备,所述目标业务交易包括所述业务系统使用第一私钥为所述目标业务交易的明细数据生成的第一数字签名;以使所述节点设备在进行交易验证时,至少基于与所述第一私钥对应的第一公钥对所述第一数字签名进行验证,在验证通过后,执行所述目标业务交易,并将所述目标业务交易的执行结果和所述区块链中的节点设备使用第二私钥为所述执行结果生成的第二数字签名存储至所述节点设备本地存储的区块链数据库。



CN 111552991 A

1.一种区块链交易方法,应用于业务系统;所述业务系统通过桥接端与区块链的节点设备连接;所述方法包括:

所述业务系统将构建的目标业务交易通过所述桥接端发送至所述区块链的节点设备,其中,所述目标业务交易包括所述业务系统使用第一私钥为所述目标业务交易的明细数据生成的第一数字签名;以使所述节点设备在进行交易验证时,至少基于与所述第一私钥对应的第一公钥对所述第一数字签名进行验证,在验证通过后,执行所述目标业务交易,并将所述目标业务交易的执行结果和所述区块链中的节点设备使用第二私钥为所述执行结果生成的第二数字签名存储至所述节点设备本地存储的区块链数据库;

通过所述桥接端从所述节点设备获取所述目标业务交易的执行结果和所述第二数字签名;

基于与所述第二私钥对应的第二公钥验证所述第二数字签名,并在对所述第二数字签名验证通过后,基于所述执行结果执行与所述交易明细数据相关的进一步的业务处理逻辑。

2.根据权利要求1所述的方法,所述第二数字签名包括:所述区块链的节点设备使用持有的第二私钥、为收录所述目标业务交易的目标区块的区块头中存储的状态数据库的认证根生成的数字签名。

3.根据权利要求2所述的方法,所述状态数据库为基于与所述目标区块中存储的交易对应的状态数据构建的默克尔树;所述认证根为所述默克尔树的root hash。

4.根据权利要求2或3所述的方法,所述第二数字签名由所述区块链的记账节点设备使用其持有的第二私钥生成,所述第二数字签名被保存在所述区块链存储的目标区块的区块头。

5.根据权利要求2或3所述的方法,所述第二数字签名由所述节点设备使用其持有的第二私钥生成,所述第二数字签名被保存在所述节点设备本地存储的所述目标区块的区块头。

6.根据权利要求1所述的方法,所述第二数字签名包括:所述节点设备使用持有的第二私钥为所述目标业务交易的执行结果生成的数字签名。

7.根据权利要求6所述的方法,所述第二数字签名和所述执行结果,或者,所述第二数字签名和所述执行结果的哈希摘要,被存储在所述桥接端连接的节点设备本地存储的所述目标区块的区块头。

8.根据权利要求7所述的方法,所述通过所述桥接端从所述节点设备获取所述目标业务交易的执行结果和所述第二数字签名,包括:

通过所述桥接端从所述节点设备拉取所述目标区块,以获取所述执行结果和所述第二数字签名;或者,

通过所述桥接端从所述节点设备拉取所述目标区块,以获取所述执行结果的哈希摘要和所述第二数字签名;并通过所述桥接端基于所述目标业务交易的检索标识,从所述节点设备获取所述目标业务交易的执行结果。

9.根据权利要求6所述的方法,所述第二数字签名和所述执行结果被存储在所述桥接端连接的节点设备本地存储的所述区块链的状态数据库中。

10.根据权利要求1所述的方法,所述第一私钥被保存在所述业务系统搭载的硬件安全

模块HSM中。

11.根据权利要求1所述的方法,所述目标业务交易为转账交易;所述交易明细数据为区块链转账数据;

所述执行与所述交易明细数据相关的进一步业务处理逻辑,包括:

执行与所述区块链转账数据相关的汇款操作;或者,

执行与所述区块链转账数据相关的退款操作。

12.一种区块链交易方法,应用于区块链的节点设备;业务系统通过桥接端与所述区块链的节点设备连接;所述方法包括:

与所述桥接端连接的节点设备通过所述桥接端获取所述业务系统构建的目标业务交易,其中,所述目标业务交易包括所述业务系统使用第一私钥为所述目标业务交易的明细数据生成的第一数字签名;

对所述目标业务交易进行交易验证,所述交易验证至少包括基于与所述第一私钥对应的第一公钥对所述第一数字签名进行验证;

在验证通过后,执行所述目标业务交易,并将所述目标业务交易的执行结果和所述区块链中的节点设备使用第二私钥为所述执行结果生成的第二数字签名存储至所述节点设备本地存储的区块链数据库;

通过所述桥接端向所述业务系统发送所述执行结果和所述第二数字签名,以使所述业务系统基于与所述第二私钥对应的第二公钥验证所述第二数字签名,并在对所述第二数字签名验证通过后,基于所述执行结果执行与所述交易明细数据相关的进一步的业务处理逻辑。

13.根据权利要求12所述的方法,所述第二数字签名包括:所述区块链的节点设备使用持有的第二私钥、为收录所述目标业务交易的目标区块的区块头中存储的状态数据库的认证根生成的数字签名。

14.根据权利要求13所述的方法,所述状态数据库为基于与所述目标区块中存储的交易对应的状态数据构建的默克尔树;所述认证根为所述默克尔树的root hash。

15.根据权利要求13或14所述的方法,所述第二数字签名由所述区块链的记账节点设备使用其持有的第二私钥生成,所述第二数字签名被保存在所述区块链存储的目标区块的区块头。

16.根据权利要求13或14所述的方法,所述第二数字签名由所述节点设备使用其持有的第二私钥生成,所述第二数字签名被保存在所述节点设备本地存储的所述目标区块的区块头。

17.根据权利要求12所述的方法,所述第二数字签名包括:所述节点设备使用持有的第二私钥为所述目标业务交易的执行结果生成的数字签名。

18.根据权利要求17所述的方法,所述第二数字签名和所述执行结果,或者,所述第二数字签名和所述执行结果的哈希摘要被存储在所述节点设备本地存储的所述目标区块的区块头。

19.根据权利要求18所述的方法,所述通过所述桥接端向所述业务系统发送所述执行结果和所述第二数字签名,包括:

向所述桥接端发送所述目标区块,以使所述业务系统通过所述桥接端获取所述目标区

块包括的所述执行结果和所述第二数字签名;或者,

向所述桥接端发送所述目标区块,以使所述业务系统通过所述桥接端获取所述目标区块包括的所述执行结果的哈希摘要和所述第二数字签名;并基于所述桥接端发送的所述目标业务交易的检索标识,向所述桥接端发送所述执行结果,以使所述业务系统通过所述桥接端获取所述执行结果。

20.根据权利要求17所述的方法,所述第二数字签名和所述执行结果被存储在被存储在所述桥接端连接的节点设备本地存储的所述区块链的状态数据库中。

21.根据权利要求12所述的方法,所述第一私钥被保存在所述业务系统搭载的硬件安全模块HSM中。

22.根据权利要求12所述的方法,所述目标业务交易为转账交易;所述交易明细数据为区块链转账数据;

所述执行与所述交易明细数据相关的进一步业务处理逻辑,包括:

执行与所述区块链转账数据相关的汇款操作;或者,

执行与所述区块链转账数据相关的退款操作。

23.一种区块链交易装置,应用于业务系统;所述业务系统通过桥接端与区块链的节点设备连接;所述装置包括:

发送单元,将构建的目标业务交易通过所述桥接端发送至所述区块链的节点设备,其中,所述目标业务交易包括所述业务系统使用第一私钥为所述目标业务交易的明细数据生成的第一数字签名;以使所述节点设备在进行交易验证时,至少基于与所述第一私钥对应的第一公钥对所述第一数字签名进行验证,在验证通过后,执行所述目标业务交易,并将所述目标业务交易的执行结果和所述区块链中的节点设备使用第二私钥为所述执行结果生成的第二数字签名存储至所述节点设备本地存储的区块链数据库;

获取单元,通过所述桥接端从所述节点设备获取所述目标业务交易的执行结果和所述第二数字签名;

验证单元,基于与所述第二私钥对应的第二公钥验证所述第二数字签名;

执行单元,基于所述执行结果执行与所述交易明细数据相关的进一步的业务处理逻辑。

24.根据权利要求23所述的装置,所述第二数字签名为:所述区块链的节点设备使用持有的第二私钥、为收录所述目标业务交易的目标区块的区块头中存储的状态数据库的认证根生成的数字签名。

25.根据权利要求24所述的装置,所述状态数据库为基于与所述目标区块中存储的交易对应的状态数据构建的默克尔树;所述认证根为所述默克尔树的root hash。

26.根据权利要求24或25所述的装置,所述第二数字签名由所述区块链的记账节点设备使用其持有的第二私钥生成,所述第二数字签名被保存在所述区块链存储的目标区块的区块头。

27.根据权利要求24或25所述的装置,所述第二数字签名由所述节点设备使用其持有的第二私钥生成,所述第二数字签名被保存在所述节点设备本地存储的所述目标区块的区块头。

28.根据权利要求23所述的装置,所述第二数字签名包括:所述节点设备使用持有的第

二私钥为所述目标业务交易的执行结果生成的数字签名。

29.根据权利要求28所述的装置，所述第二数字签名和所述执行结果，或者，所述第二数字签名和所述执行结果的哈希摘要，被存储在所述桥接端连接的节点设备本地存储的所述目标区块的区块头。

30.根据权利要求29所述的装置，所述获取单元，进一步用于：

通过所述桥接端从所述节点设备拉取所述目标区块，以获取所述执行结果和所述第二数字签名；或者，

通过所述桥接端从所述节点设备拉取所述目标区块，以获取所述执行结果的哈希摘要和所述第二数字签名；并通过所述桥接端基于所述目标业务交易的检索标识，从所述节点设备获取所述目标业务交易的执行结果。

31.根据权利要求28所述的方法，所述第二数字签名和所述执行结果被存储在所述桥接端连接的节点设备本地存储的所述区块链的状态数据库中。

32.一种区块链交易装置，应用于区块链的节点设备；业务系统通过桥接端与所述区块链的节点设备连接；所述装置包括：

获取单元，与所述桥接端连接的节点设备通过所述桥接端获取所述业务系统构建的目标业务交易，其中，所述目标业务交易包括所述业务系统使用第一私钥为所述目标业务交易的明细数据生成的第一数字签名；

验证单元，对所述目标业务交易进行交易验证，所述交易验证至少包括基于与所述第一私钥对应的第一公钥对所述第一数字签名进行验证；

执行单元，执行所述目标业务交易；

存储单元，将所述目标业务交易的执行结果和所述区块链中的节点设备使用第二私钥为所述执行结果生成的第二数字签名存储至所述节点设备本地存储的区块链数据库；

发送单元，通过所述桥接端向所述业务系统发送所述执行结果和所述第二数字签名，以使所述业务系统基于与所述第二私钥对应的第二公钥验证所述第二数字签名，并在对所述第二数字签名验证通过后，基于所述执行结果执行与所述交易明细数据相关的进一步的业务处理逻辑。

33.根据权利要求32所述的装置，所述第二数字签名包括：所述区块链的节点设备使用持有的第二私钥、为收录所述目标业务交易的目标区块的区块头中存储的状态数据库的认证根生成的数字签名。

34.根据权利要求33所述的装置，所述状态数据库为基于与所述目标区块中存储的交易对应的状态数据构建的默克尔树；所述认证根为所述默克尔树的root hash。

35.根据权利要求33或34所述的装置，所述第二数字签名由所述区块链的记账节点设备使用其持有的第二私钥生成，所述第二数字签名被保存在所述区块链存储的目标区块的区块头。

36.根据权利要求33或34所述的装置，所述第二数字签名由所述节点设备使用其持有的第二私钥生成，所述第二数字签名被保存在所述节点设备本地存储的所述目标区块的区块头。

37.根据权利要求32所述的装置，所述第二数字签名包括：所述节点设备使用持有的第二私钥为所述目标业务交易的执行结果生成的数字签名。

38.根据权利要求37所述的装置,所述第二数字签名和所述执行结果,或者,所述第二数字签名和所述执行结果的哈希摘要被存储在所述节点设备本地存储的所述目标区块的区块头。

39.根据权利要求38所述的装置,所述发送单元,进一步用于:

向所述桥接端发送所述目标区块,以使所述业务系统通过所述桥接端获取所述目标区块包括的所述执行结果和所述第二数字签名;或者,

向所述桥接端发送所述目标区块,以使所述业务系统通过所述桥接端获取所述目标区块包括的所述执行结果的哈希摘要和所述第二数字签名;并基于所述桥接端发送的所述目标业务交易的检索标识,向所述桥接端发送所述执行结果,以使所述业务系统通过所述桥接端获取所述执行结果。

40.根据权利要求37所述的装置,所述第二数字签名和所述执行结果被存储在被存储在所述桥接端连接的节点设备本地存储的所述区块链的状态数据库中。

41.一种计算机设备,包括:存储器和处理器;所述存储器上存储有可由所述处理器运行的计算机程序;所述处理器运行所述计算机程序时,执行如权利要求1至11任意一项所述的方法。

42.一种计算机设备,包括:存储器和处理器;所述存储器上存储有可由所述处理器运行的计算机程序;所述处理器运行所述计算机程序时,执行如权利要求12至22任意一项所述的方法。

一种区块链交易方法及装置

技术领域

[0001] 本说明书一个或多个实施方式涉及区块链技术领域，尤其涉及一种区块链交易方法和装置。

背景技术

[0002] 区块链技术，也被称之为分布式账本技术，是一种由若干台计算设备共同参与“记账”，共同维护一份完整的分布式数据库的新兴技术。由于区块链技术具有去中心化、公开透明、每台计算设备可以参与数据库记录、并且各计算设备之间可以快速的进行数据同步的特性，使得区块链技术已在众多的领域中广泛的进行应用。

[0003] 随着区块链技术的发展，越来越多的业务系统提出了接入区块链网络的需求，然而将业务系统服务器与区块链网络直接对接会带来数据安全的风险，尤其是当区块链网络为公有区块链网络时，不仅对业务系统服务器有着更高的硬件需求，而且对业务系统服务器有着较大的隐私破坏风险。

发明内容

[0004] 有鉴于此，本说明书一个或多个实施方式提供了一种区块链交易方法、装置及计算机设备。

[0005] 根据本说明书一个或多个实施方式的第一方面，提出了应用于业务系统；所述业务系统通过桥接端与区块链的节点设备连接；所述方法包括：

[0006] 所述业务系统将构建的目标业务交易通过所述桥接端发送至所述区块链的节点设备，其中，所述目标业务交易包括所述业务系统使用第一私钥为所述目标业务交易的明细数据生成的第一数字签名；以使所述节点设备在进行交易验证时，至少基于与所述第一私钥对应的第一公钥对所述第一数字签名进行验证，在验证通过后，执行所述目标业务交易，并将所述目标业务交易的执行结果和所述区块链中的节点设备使用第二私钥为所述执行结果生成的第二数字签名存储至所述节点设备本地存储的区块链数据库；

[0007] 通过所述桥接端从所述节点设备获取所述目标业务交易的执行结果和所述第二数字签名；

[0008] 基于与所述第二私钥对应的第二公钥验证所述第二数字签名，并在对所述第二数字签名验证通过后，基于所述执行结果执行与所述交易明细数据相关的进一步的业务处理逻辑。

[0009] 根据本说明书一个或多个实施方式的第二方面，提出了一种区块链交易方法，应用于区块链的节点设备；业务系统通过桥接端与所述区块链的节点设备连接；所述方法包括：

[0010] 与所述桥接端连接的节点设备通过所述桥接端获取所述业务系统构建的目标业务交易，其中，所述目标业务交易包括所述业务系统使用第一私钥为所述目标业务交易的明细数据生成的第一数字签名；

[0011] 对所述目标业务交易进行交易验证，所述交易验证至少包括基于与所述第一私钥对应的第一公钥对所述第一数字签名进行验证；

[0012] 在验证通过后，执行所述目标业务交易，并将所述目标业务交易的执行结果和所述区块链中的节点设备使用第二私钥为所述执行结果生成的第二数字签名存储至所述节点设备本地存储的区块链数据库；

[0013] 通过所述桥接端向所述业务系统发送所述执行结果和所述第二数字签名，以使所述业务系统基于与所述第二私钥对应的第二公钥验证所述第二数字签名，并在对所述第二数字签名验证通过后，基于所述执行结果执行与所述交易明细数据相关的进一步的业务处理逻辑。

[0014] 根据本说明书一个或多个实施方式的第三方面，提出了、一种区块链交易装置，应用于业务系统；所述业务系统通过桥接端与区块链的节点设备连接；所述装置包括：

[0015] 发送单元，将构建的目标业务交易通过所述桥接端发送至所述区块链的节点设备，其中，所述目标业务交易包括所述业务系统使用第一私钥为所述目标业务交易的明细数据生成的第一数字签名；以使所述节点设备在进行交易验证时，至少基于与所述第一私钥对应的第一公钥对所述第一数字签名进行验证，在验证通过后，执行所述目标业务交易，并将所述目标业务交易的执行结果和所述区块链中的节点设备使用第二私钥为所述执行结果生成的第二数字签名存储至所述节点设备本地存储的区块链数据库；

[0016] 通过所述桥接端从所述节点设备获取所述目标业务交易的执行结果和所述第二数字签名；

[0017] 基于与所述第二私钥对应的第二公钥验证所述第二数字签名，并在对所述第二数字签名验证通过后，基于所述执行结果执行与所述交易明细数据相关的进一步的业务处理逻辑。

[0018] 根据本说明书一个或多个实施方式的第四方面，提出了一种区块链交易装置，应用于区块链的节点设备；业务系统通过桥接端与所述区块链的节点设备连接；所述装置包括：

[0019] 获取单元，与所述桥接端连接的节点设备通过所述桥接端获取所述业务系统构建的目标业务交易，其中，所述目标业务交易包括所述业务系统使用第一私钥为所述目标业务交易的明细数据生成的第一数字签名；

[0020] 验证单元，对所述目标业务交易进行交易验证，所述交易验证至少包括基于与所述第一私钥对应的第一公钥对所述第一数字签名进行验证；

[0021] 执行单元，执行所述目标业务交易；

[0022] 存储单元，将所述目标业务交易的执行结果和所述区块链中的节点设备使用第二私钥为所述执行结果生成的第二数字签名存储至所述节点设备本地存储的区块链数据库；

[0023] 发送单元，通过所述桥接端向所述业务系统发送所述执行结果和所述第二数字签名，以使所述业务系统基于与所述第二私钥对应的第二公钥验证所述第二数字签名，并在对所述第二数字签名验证通过后，基于所述执行结果执行与所述交易明细数据相关的进一步的业务处理逻辑。

[0024] 根据本说明书一个或多个实施方式的第五方面，提出了一种计算机设备，包括：存储器和处理器；所述存储器上存储有可由所述处理器运行的计算机程序；所述处理器运行

所述计算机程序时，执行业务系统所执行的区块链交易方法。

[0025] 根据本说明书一个或多个实施方式的第六方面，提出了一种计算机设备，包括：存储器和处理器；所述存储器上存储有可由所述处理器运行的计算机程序；所述处理器运行所述计算机程序时，执行与桥接端连接的节点设备所执行的区块链交易方法。

[0026] 本说明书各个实施方式提供的区块链交易方法、装置和计算机设备，在业务系统与区块链节点设备之间设置了桥接端，由桥接端负责向区块链网络转发业务系统构建的交易和向业务系统转发区块链上的交易执行结果。为了防止桥接端作恶，上述业务系统构建的交易包含了业务系统所作的第一数字签名，且与桥接端连接的区块链节点设备在其收录上述交易的区块内包含了区块链的节点设备所作的第二数字签名，通过数字签名验证技术，从而有效降低了桥接端作恶而造成的数据安全风险，提高了业务系统的数据安全性。

附图说明

[0027] 图1是一示例性实施方式提供的通过包括业务系统、桥接端和区块链网络的系统来实施区块链交易的示意图；

[0028] 图2是一示例性实施方式提供的区块链交易方法的流程示意图；

[0029] 图3是一示例性实施方式提供的应用于业务系统的区块链交易装置的示意图；

[0030] 图4是一示例性实施方式提供的应用于区块链节点设备端的区块链交易装置的示意图；

[0031] 图5是运行本说明书所提供的区块链交易装置实施方式的一种硬件结构图。

具体实施方式

[0032] 这里将详细地对示例性实施方式进行说明，其示例表示在附图中。下面的描述涉及附图时，除非另有表示，不同附图中的相同数字表示相同或相似的要素。以下示例性实施方式中所描述的实施方式并不代表与本说明书一个或多个实施方式相一致的所有实施方式。相反，它们仅是与如所附权利要求书中所详述的、本说明书一个或多个实施方式的一些方面相一致的装置和方法的例子。

[0033] 需要说明的是：在其他实施方式中并不一定按照本说明书示出和描述的顺序来执行相应方法的步骤。在一些其他实施方式中，其方法所包括的步骤可以比本说明书所描述的更多或更少。此外，本说明书中所描述的单个步骤，在其他实施方式中可能被分解为多个步骤进行描述；而本说明书中所描述的多个步骤，在其他实施方式中也可能被合并为单个步骤进行描述。

[0034] 随着区块链支持的应用业务日渐成熟，越来越多的业务系统需要接入区块链网络，以向区块链上发送转账交易、存证交易、或智能合约调用交易，并获得上述交易在区块链上的执行结果。如果将业务系统与区块链网络的节点设备直接连接，为了业务系统的安全，除业务逻辑外，还需要在业务系统部署网络通信、证书交换、密钥安全及隐私保护等复杂逻辑，业务系统直接接入区块链的成本较高。

[0035] 鉴于以上的问题，本说明书的一个或多个实施方式提供了一种区块链交易方法，用于业务系统向区块链网络发布交易、且接收交易的执行结果；上述业务系统通过桥接端与区块链的节点设备连接。

[0036] 图1是一示例性实施方式提供的通过包括业务系统、桥接端和区块链网络的系统来实施区块链交易的示意图；

[0037] 本说明书一个或多个实施方式所述的业务系统可包括一个或多个部署有业务处理逻辑的业务系统服务器，还可以包括与业务系统服务器连接的、负责网络通信、或密钥计算等其他功能的硬件模块(如HSM硬件安全模块)或独立设备。

[0038] 本说明书一个或多个实施方式所收到桥接端，是连接业务系统与区块链的任一节点设备的独立设备，或者是被设置于所述业务系统内部的硬件模块，使得业务系统通过该硬件模块与区块链的节点设备连接，还可以是被设置于区块链节点设备内部的硬件模块，在此不作限定。

[0039] 具体地，上述业务系统可设置其信任的区块链节点设备，并要求桥接端与上述信任的区块链节点设备通信连接以进行业务交易的执行。

[0040] 本说明书一个或多个实施方式所述的区块链或区块链网络，具体可指一个各节点设备通过共识机制达成的、具有分布式数据存储结构的P2P网络系统，该区块链内的账本数据分布在时间上相连的一个个“区块(block)”之内，后一区块可包含前一区块的数据摘要，且根据具体的共识机制(如POW、POS、DPOS或PBFT等)的不同，达成全部或部分节点的数据全备份。

[0041] 本领域的技术人员熟知，由于区块链网络系统在相应共识机制下运行，已收录至区块链数据库内的数据很难被任意的节点篡改，例如采用Pow共识的区块链，至少需要全网51％算力的攻击才有可能篡改已有数据，因此区块链系统有着其他中心化数据库系统所无法比拟的保证数据安全、防攻击篡改的特性。

[0042] 对于物理世界产生的真实数据，可以将其构建成区块链所支持的标准的交易(transaction)格式，然后发布、并广播至区块链的节点设备中，由区块链中的节点设备对收到的交易进行共识处理，并在达成共识后，由区块链中作为记账节点的节点设备，将这笔交易打包进区块，在区块链中进行持久化存证。

[0043] 无论区块链采用哪种共识算法，记账节点均可以将接收到的交易打包以生成最新区块，并将生成的最新区块或者该最新区块的区块头发送至其它节点设备进行共识验证。如果其它节点设备接收到最新区块或者该最新区块的区块头后，经验证没有问题，可以将该最新区块追加到原有的区块链末尾，从而完成区块链的记账过程。其它节点验证记账节点发来的新的区块或区块头的过程中，也可以执行该区块中的包含的交易。

[0044] 对于大多数区块链模型，通常都会使用Merkle树；或者，基于Merkle树的数据结构，来存储和维护数据。以以太坊为例，以太坊使用了MPT树(一种Merkle树变种)，作为数据组织形式，用来组织和管理账户状态、交易信息等重要数据。

[0045] 以太坊针对区块链中需要存储和维护的数据，设计了三棵MPT树，分别是MPT状态树、MPT交易树和MPT收据树。其中，除了以上三棵MPT树以外，实际上还存在一棵基于合约账户的存储内容构建的Storage树。

[0046] MPT状态树，是由区块链中所有账户的账户状态(state)数据组织成的MPT树；MPT交易树，是由区块链中的交易(transaction)数据组织成的MPT树；MPT收据树，是区块中的交易在执行完毕后生成的与每笔交易对应的交易(receipt)收据组织成的MPT树。以上示出的MPT状态树、MPT交易树和MPT收据树的根节点的hash值，最终都会被添加至对应区块的区

块头中。

[0047] 其中,MPT交易树和MPT收据树均与区块相对应,即每一个区块都有自己的MPT交易树和MPT收据树。而MPT状态树是一个全局的MPT树,并不与某一个特定的区块相对应,而是涵盖了区块链中所有账户的账户状态数据。

[0048] 对于组织成的MPT交易树、MPT收据树和MPT状态树,最终都会在采用多级数据存储结构的Key-Value型数据库(比如,LevelDB)中进行存储。对交易的执行方法,可依据交易的类型和内容而具体设定。例如,当交易为转账交易时,区块链的节点设备在收到记账节点发来的新区块后,可依据转账交易所包含的转账值,在本地保存的区块链用户账户状态数据库中,从转账交易的汇出方账户转出与转账值对应的金额,并在接收方用户加入与转账至对应的金额,且该交易的执行结果会以交易日志的形式被保存在节点设备本地状态数据库的收据树(receipt MPT)中。

[0049] 当交易为业务数据存证交易时,区块链的节点设备在收到记账节点发来的新区块后,可将包含上述业务数据存证交易的新区块保存在本地维护的区块链账本数据库(区块block)中,且该交易的执行结果会以交易日志的形式被保存在节点设备本地状态数据库的收据树(receipt MPT)中;

[0050] 当交易为智能合约调用交易时,区块链的节点设备在收到记账节点发来的新区块后,可在本地虚拟机上执行上述交易调用的智能合约逻辑,除了将该交易的执行结果以交易日志的形式被保存在节点设备本地状态数据库的收据树(receipt MPT)中之外,还可以将智能合约逻辑的执行结果保存在与该智能合约对应的区块链状态数据存储空间中。

[0051] 需要说明的是,区块链每产生一个最新区块,则在该最新区块中的交易被执行之后,区块链中这些被执行交易的相关账户(可以是外部账户也可以是合约账户)的账户状态,通常也会随之发生变化;

[0052] 例如,当区块中的一笔“转账交易”执行完毕后,与该“转账交易”相关的转出方账户和转入方账户的余额(即这些账户的Balance字段的字段值),通常也会随之发生变化。

[0053] 而节点设备在区块链产生的最新区块中的交易执行完毕后,由于当前区块链中的账户状态发生了变化,因此节点设备需要根据区块链中所有账户当前的账户状态数据,来构建MPT状态树,用于维护区块链中所有账户的最新状态。

[0054] 也即,每当区块链中产生一个最新区块,并且该最新区块中的交易执行完毕后,导致区块链中的账户状态发生了变化,节点设备都需要基于区块链中所有账户最新的账户状态数据,重新构建一棵MPT状态树。换句话说,区块链中每一个区块,都有一个与之对应的MPT状态树;该MPT状态树,维护了在该区块中的交易在执行完毕后,区块链中所有账户最新的账户状态。

[0055] 区块链一般被划分为三种类型:公有链(Public Blockchain),私有链(Private Blockchain)和联盟链(Consortium Blockchain)。此外,还可以有上述多种类型的结合,比如私有链+联盟链、联盟链+公有链等。

[0056] 其中,去中心化程度最高的是公有链。公有链以比特币、以太坊为代表,加入公有链的参与者(也可称为区块链中的节点)可以读取链上的数据记录、参与交易、以及竞争新区块的记账权等。而且,各节点可自由加入或者退出网络,并进行相关操作。

[0057] 私有链则相反,该网络的写入权限由某个组织或者机构控制,数据读取权限受组

织规定。简单来说，私有链可以为一个弱中心化系统，其对节点具有严格限制且节点数量较少。这种类型的区块链更适合于特定机构内部使用。

[0058] 联盟链则是介于公有链以及私有链之间的区块链，可实现“部分去中心化”。联盟链中各个节点通常有与之相对应的实体机构或者组织；节点通过授权加入网络并组成利益相关联盟，共同维护区块链运行。

[0059] 可以预期，本说明书所提供的实施方式能够在任何合适类型的区块链网络中实现。

[0060] 如图2所示，本说明书提供的一个或多个实施方式所提供的区块链交易方法，包括：

[0061] 步骤202，所述业务系统将构建的目标业务交易通过所述桥接端发送至所述区块链的节点设备，其中，所述目标业务交易包括所述业务系统使用第一私钥为所述目标业务交易的明细数据生成的第一数字签名。

[0062] 业务系统可基于业务需要构建目标业务交易，该目标业务交易可包含与业务处理相关的明细数据，和业务系统使用持有的第一私钥为上述明细数据生成的第一数字签名。具体地，上述第一数字签名可针对上述明细数据的原文、或上述明细数据的哈希摘要等衍生数据而做出。

[0063] 为进一步地提高密钥安全性，上述第一私钥被保存在业务系统搭载的硬件安全模块HSM中。硬件安全模块HSM是用于保护和管理业务系统所使用的密钥，并同时提供相关密钥运算操作(如数字签名操作)的计算机硬件设备，例如，业务系统可使用包括上述明细数据的指令，调用HSM执行基于其存储的第一私钥对上述明细数据生成第一数字签名的密钥运算服务，并从HSM中直接获取上述第一数字签名。进一步地，业务系统可以将上述明细数据和第一数字签名按照交易的格式封装成目标业务交易，再将该目标业务交易发送到桥接端。

[0064] 步骤204，所述桥接端将所述目标业务交易转发至与桥接端连接的节点设备。

[0065] 在本实施方式中，上述桥接端可以与上述区块链网络中的一个或多个节点设备连接，并将上述目标业务交易转发至一个或多个节点设备中；获得上述目标业务交易的节点设备可继续在区块链网络中广播转发上述目标业务交易。

[0066] 步骤206，所述区块链中的节点设备(包括与桥接端连接的节点设备)在进行交易验证时，至少基于与所述第一私钥对应的第一公钥对上述第一数字签名进行验证，并在验证通过后，执行所述目标业务交易。

[0067] 与上述桥接端对应的一个或多个节点设备，或者区块链中的节点设备，可保存有与业务系统持有的第一私钥对应的第一公钥。在实现时，业务系统可在申请加入上述区块链网络时，或者，在上述连接有桥接端的业务系统与上述一个或多个节点设备进行初始化连接时，将上述业务系统持有的第一私钥对应的第一公钥，通过上述桥接端转发、或者通过业务系统与上述一个或多个节点设备直接通信的方式，将上述第一公钥传输给上述一个或多个节点设备，或者所述区块链中的节点设备。本说明书并不限定区块链的节点设备获取上述第一公钥的具体方式。

[0068] 而且，为了进一步保证业务系统的安全性，业务系统还可定期更新上述第一私钥-第一公钥对，并将更新后的第一公钥传输至区块链的节点设备中。

[0069] 步骤208，与桥接端连接的节点设备将所述目标业务交易的执行结果和所述区块链中的节点设备使用第二私钥为所述执行结果生成的第二数字签名存储至与桥接端连接的节点设备本地存储的区块链数据库。

[0070] 在一示出的实施方式中，所述第二数字签名为所述区块链的节点设备使用持有的第二私钥、为收录所述目标业务交易的目标区块的区块头中存储的状态数据库的认证根生成的数字签名。

[0071] 区块链的节点设备接收共识验证后的目标区块后，可执行目标区块中收录的交易，并将交易的执行结果、即交易执行完毕后的状态数据存储在区块链状态数据库中。本实施方式所述的认证根，是由该目标区块中所有交易对应的状态数据衍生生成的、或者所有交易的执行结果数据衍生生成的、可为目标区块内的任一交易的执行结果数据进行认证验证的数值，该数值可保存在目标区块的区块头内。

[0072] 例如，以太坊针对区块链中需要存储和维护的数据，设计了三棵MPT树，分别是MPT状态树、MPT交易树和MPT收据树。其中，除了以上三棵MPT树以外，实际上还存在一棵基于合约账户的存储内容构建的Storage树。

[0073] MPT状态树，是由区块链中所有账户的账户状态(state)数据组织成的MPT树；MPT交易树，是由区块链中的交易(transaction)数据组织成的MPT树；MPT收据树，是区块中的交易在执行完毕后生成的与每笔交易对应的交易日志收据(receipt)组织成的MPT树，上述交易日志收据包含交易的执行结果。以上示出的MPT状态树、MPT交易树和MPT收据树的根节点的hash值，最终都会被添加至对应区块的区块头中。此时，上述实施方式所述的状态数据库为基于与所述目标区块中存储的交易对应的状态数据构建的默克尔树(MPT状态树或者MPT状态树)；所述认证根为所述默克尔树(MPT状态树或者MPT状态树)的root hash。

[0074] 当然，本实施方式并未将上述区块链限定为以太坊架构，本领域技术人员可至少为目标业务交易的执行结果、或目标业务交易执行后的状态数据设计特定衍生规则而得到的认证根，并将该认证根收录于目标区块的区块头中，以基于该认证根实现对目标业务交易的验证。

[0075] 本实施方式未限定对上述目标区块的区块头中的认证根生成数字签名的节点设备的角色，也未限定对上述目标区块的区块头中的认证根生成数字签名的存储位置。

[0076] 在一示出的实施方式中，上述第二数字签名是由所述区块链的记账节点设备使用其持有的第二私钥生成，所述第二数字签名被保存在所述区块链存储的目标区块的区块头。

[0077] 区块链的记账节点在接收到上述目标业务交易后，在将上述目标业务交易打包至目标区块时，使用记账节点持有的第二私钥、为目标区块的区块头中的认证根生成第二数字签名，并将该第二数字签名也收录于目标区块的区块头中。记账节点将包含上述第二数字签名的目标区块广播至区块链网络中的节点设备以进行共识验证。上述区块链的记账节点的选举方式、新生区块中包括的交易的收录方式、及对新生区块的共识验证的具体方式内容也基于区块链共识机制的不同而不同，在此不作限定。

[0078] 当上述目标区块通过区块链网络中节点设备的共识验证(包括上述一实施方式所述的对第一数字签名的验证)，区块链中的节点设备可执行上述目标区块链中包含的交易，并将包含上述记账节点作出的第二数字签名的目标区块存储在该节点设备本地保存的区

块链数据库中。

[0079] 在又一示出的实施方式中，上述第二数字签名由与桥接端连接的节点设备使用其持有的第二私钥生成，所述第二数字签名被保存在与桥接端连接的节点设备本地存储的所述目标区块的区块头。

[0080] 在本实施方式中，区块链的记账节点在接收到上述目标业务交易后，可将上述目标业务交易打包至目标区块，再将该目标区块广播至区块链网络中的节点设备以进行共识验证。上述区块链的记账节点的选举方式、新生区块中包括的交易的收录方式、及对新生区块的共识验证的具体方式内容也基于区块链共识机制的不同而不同，在此不作限定。

[0081] 上述与桥接端连接的一个或多个节点设备，在收到包括上述目标业务交易的目标区块后，即可通过执行上述目标区块收录的每个交易，在本地存储的区块链状态数据库中存储上述每个交易的执行结果、更新每个交易对应的状态数据；当与桥接端连接的一个或多个节点设备在其本地存储上述目标区块时，可使用自身持有的第二私钥、为上述目标区块的区块头中的认证根生成第二数字签名，并将该第二数字签名保存在该节点设备本地存储的目标区块的区块头。

[0082] 值得注意的是，本实施方式中所述的、由与桥接端连接的节点设备基于其持有的第二私钥对目标区块的区块头中的认证根所作的第二数字签名，仅仅是为了防止桥接端作恶、以方便该业务系统对目标业务交易的执行结果进行验证，由与桥接端连接的节点设备保存在其本地存储的目标区块的区块头中的，区块链中的其他节点设备接收到上述记账节点广播的目标区块中并未包含上述第二数字签名。

[0083] 在又一示出的实施方式中，在与桥接端连接的节点设备执行上述目标业务交易后，可使用该节点设备其持有的第二私钥、为上述目标业务交易的执行结果生成第二数字签名。

[0084] 以基于以太坊架构的账户型区块链为例，当目标业务交易为转账交易时，区块链的节点设备在收到记账节点发来的目标区块后，可依据转账交易所包含的转账值，在本地保存的区块链状态数据库中，从转账交易的汇出方账户转出与转账值对应的金额，并在接收方用户加入与转账至对应的金额，且该交易的执行结果会以交易日志的形式被保存在节点设备本地状态数据库的收据树(receipt MPT)中。

[0085] 当目标业务交易为业务数据存证交易时，区块链的节点设备在收到记账节点发来的目标区块后，可将该交易的执行结果会以交易日志的形式被保存在节点设备本地维护的区块链状态数据库的收据树(receipt MPT)中。

[0086] 当目标业务交易为智能合约调用交易时，区块链的节点设备在收到记账节点发来的目标区块后，可在本地虚拟机上执行上述交易调用的智能合约逻辑，除了将该交易的执行结果以交易日志的形式被保存在节点设备本地状态数据库的收据树(receipt MPT)中之外，还可以将智能合约逻辑的执行结果保存在与该智能合约对应的账户存储空间(storage MPT)中。

[0087] 通过执行上述目标业务交易，上述目标业务交易的执行结果即被保存在节点设备本地存储的区块链状态数据库中。在本实施方式中，为了防止在向业务系统通知目标业务交易的执行结果时桥接端作恶，与上述桥接端连接的一个或多个节点设备可在对上述目标业务交易验证通过、收录包含目标业务交易的目标区块时，执行所述目标业务交易，并使用

持有的第二私钥对该目标业务交易的执行结果生成第二数字签名。

[0088] 具体地，上述与桥接端连接的节点设备可对上述目标业务交易的执行结果明文进行数字签名运算，以得到上述第二数字签名；或者，对于一些目标业务交易，其执行结果可占用较大的容量，此时上述节点设备也可对上述执行结果的验证数据，例如，上述执行结果的哈希摘要进行数字签名运算，以得到上述第二数字签名。

[0089] 类似的，本实施方式中所述的、由与桥接端连接的节点设备基于其持有的第二私钥对目标业务交易的执行结果所作的第二数字签名，仅仅是为了防止桥接端作恶、以方便该业务系统对目标业务交易的执行结果进行验证，由与桥接端连接的节点设备保存在其本地存储的区块链数据库中的，区块链中的其他节点设备由于没有与上述业务系统的通信需求，而无需对上述目标业务交易的执行结果进行数字签名、也无需在其本地存储的区块链数据库中保存上述数字签名。

[0090] 在本实施方式中，并不限定上述第二数字签名在与上述桥接端连接的节点设备本地的区块链数据库中的具体存储位置。由于为方便桥接端或业务系统验证目标业务交易确实已被收录至目标区块，节点设备可通过向桥接端发送整个目标区块的方式，向桥接端或业务系统通知上述目标业务交易被区块链收录，为了进一步地方便通知，减少节点设备与桥接端的信息交互步骤，上述节点设备可将上述执行结果和第二数字签名、或者上述执行结果的验证数据(如执行结果的哈希摘要)和第二数字签名存储在目标区块中，例如，目标区块的区块头中，以通过桥接端从该节点设备直接拉取目标区块的方式，获取到上述执行结果和第二数字签名。

[0091] 或者，为方便与桥接端连接的节点设备查询上述执行结果和为上述执行结果生成的第二数字签名，上述第二数字签名可被该节点设备与执行结果对应保存在状态数据库中，例如，将上述第二数字签名和执行结果对应保存在上述目标区块对应的收据树中，或者将上述第二数字签名和执行结果对应保存在目标业务交易所调用的智能合约的账户存储空间，等等。

[0092] 步骤210，所述桥接端将与其连接的节点设备发送的所述目标业务交易的执行结果和所述第二数字签名转发至所述业务系统。

[0093] 与桥接端连接的节点设备可从其本地存储的区块链数据库中，获取上述执行结果和第二数字签名，再将上述执行结果和第二数字签名发送至桥接端，以使桥接端可将上述执行结果和第二数字签名转发至业务系统。

[0094] 在一示出的实施方式中，当上述第二数字签名是区块链的记账节点为收录目标业务交易的目标区块的区块头中存储的状态数据库的认证根所生成的，或者，当上述第二数字签名是与桥接端连接的节点设备为上述认证根所生成的，业务系统除了验证所述第二数字签名是所述记账节点设备、或者与桥接端连接的节点设备为上述区块头中包含的认证根生成的，还需验证上述目标业务交易的执行结果与上述区块头中包含的认证根的认证对应关系，亦即验证上述执行结果是否确实被收录于与所述目标区块对应的区块链状态数据库。

[0095] 此时，上述与桥接端连接的节点设备还需向桥接端发送与目标区块对应的状态数据，上述状态数据可包括，基于与所述目标区块中存储的交易对应的状态数据构建的默克尔树(如MPT状态树或MPT收据树)，上述默克尔树包含上述目标业务交易的执行结果，以使

桥接端将上述状态数据转发至业务系统，由业务系统基于包含上述执行结果的状态数据是否可衍生得到上述认证根，如果可以得到，即证明所述目标业务交易的执行结果确实被收录于与所述目标区块对应的区块链状态数据库。

[0096] 值得注意的是，上述业务系统可在其本地保存区块链中节点设备、或与该桥接端对接的节点设备所对应的公钥，以方便对上述第二数字签名进行验证。

[0097] 在又一示出的实施方式中，所述第二数字签名是与桥接端连接的节点设备使用所述第二私钥对所述执行结果的原文而做出的，与桥接端连接的节点设备可将上述执行结果和所述第二数字签名保存在其本地存储的目标区块的区块头内。所述桥接端可定时监听与其连接的节点设备以获取节点设备存储的目标区块，或者上述节点设备在将上述执行结果和第二数字签名保存在目标区块后，向桥接端发送目标业务交易被收录的通知，该通知可包括目标区块的区块高度和所述目标业务交易的检索标识，以方便上述桥接端从所述节点设备拉取所述目标区块，并基于上述检索标识查验上述目标业务交易被收录于所述目标区块。

[0098] 在又一示出的实施方式中，上述第二数字签名是与所述桥接端连接的节点设备使用所述第二私钥对所述执行结果的哈希摘要而做出的，所述执行结果的哈希摘要和所述第二数字签名被保存在该节点设备本地存储的所述目标区块的区块头。上述节点设备在将上述执行结果的哈希值和第二数字签名保存在目标区块的区块头后，可向桥接端发送目标业务交易被收录的通知，该通知可包括目标区块的区块高度和所述目标业务交易的检索标识(例如目标业务交易的TXID或交易序列号)，以方便上述桥接端从所述节点设备拉取所述目标区块，并基于该检索标识向上述节点设备问询目标业务交易的执行结果；上述节点设备基于上述检索标识，在其本地维护的区块链状态数据库中查询到与上述目标业务交易对应的执行结果，并将上述执行结果返回至桥接端，以使所述桥接端将上述执行结果转发至业务系统。

[0099] 在又一示出的实施方式中，上述第二数字签名是与所述桥接端连接的节点设备使用所述第二私钥对所述执行结果的原文、或所述执行结果的哈希摘要而做出的，且所述第二数字签名与所述执行结果被对应保存在该节点设备本地存储的区块链状态数据库中。该节点设备可直接从其本地存储的区块链状态数据库中获取所述执行结果的原文和所述第二数字签名，并将上述执行结果的原文和所述第二数字签名由桥接端转发至业务系统。

[0100] 步骤212，所述业务系统基于与所述第二私钥对应的第二公钥验证所述第二数字签名，并在对所述第二数字签名验证通过后，基于所述执行结果执行与所述交易明细数据相关的进一步的业务处理逻辑。

[0101] 上述业务系统可在其本地维护其信任的区块链节点设备(例如上述记账节点)、或与桥接端连接的节点设备的公钥列表，在收到上述桥接端转发的所述执行结果和第二数字签名后，上述业务系统可从上述公钥列表中获取与上述节点设备持有的第二私钥对应的第二公钥，并基于该第二公钥对上述第二数字签名进行验证。

[0102] 当上述第二数字签名是基于目标区块的区块头所包括的认证根所生成时，除了对上述第二数字签名进行验证，业务系统还需基于桥接端所转发的区块链的状态数据库数据，例如与目标区块基于与所述目标区块中存储的交易对应的状态数据构建的默克尔树(MPT收据树或MPT状态树)，或目标业务交易所调用的智能合约的账户空间所存储的状态数

据树，来验证所述认证根与执行结果的认证对应关系。业务系统可对包含目标业务交易的目标区块内的所有交易的执行结果的值执行默克尔树根生成计算，以验证其计算所得的默克尔树的树根与上述区块头中的认证根是否一致；上述两根值一致时，即代表上述执行结果可由上述认证根认证，且上述执行结果被收录在可生成上述认证根的区块链状态数据库中。

[0103] 当上述第二数字签名是与桥接端连接的节点设备使用第二私钥至少对执行结果的哈希摘要所作出时，除了对上述第二数字签名进行验证，所述业务系统还需验证所述执行结果的哈希摘要与所述执行结果是否匹配。

[0104] 在对第二数字签名的验证通过，或者且对所述执行结果与认证根的认证对应关系验证通过，或者且对所述执行结果的哈希摘要与执行结果的原文一致验证通过后，执行与所述交易明细数据相关的业务处理逻辑。

[0105] 在一示出的实施方式中，上述交易明细数据包括区块链转账数据，上述目标业务交易为转账交易，当上述转账交易被收录到区块链的目标区块后，节点设备可依据转账交易所包含的转账值，在本地保存的区块链用户账户状态数据库中，从转账交易的汇出方账户转出与转账值对应的金额，并在接收方用户加入与转账至对应的金额。值得注意的是，上述区块链的用户账户余额值及转账值对应的是区块链上流通的虚拟货币(Token)，该虚拟货币可以仅仅作为与链下的实际资产对应的货币符号，在链上进行资产流通过程的存证。

[0106] 当上述转账交易在区块链上被执行成功后，业务系统需在链外执行与上述区块链转账数据相关的汇款操作，例如由上述业务系统向其用户发起实际的银行汇款操作，或通知与上述转账交易相关的汇出方执行汇款操作，或通知上述转账交易相关的接收方查收汇款是否到账，等等。

[0107] 当上述转账交易的执行结果显示转账失败时，业务系统需在链外执行与上述区块链转账数据相关的退款操作，例如由上述业务系统向其用户发起实际的银行账户退款操作，或通知与上述转账交易相关的汇出方执行退款操作，或通知上述转账交易相关的接收方查收退款是否到账，等等。

[0108] 由上述一个或多个实施方式所提供的区块链交易方法，在业务系统与区块链网络的节点设备之间设置了桥接端，由桥接端负责向区块链网络转发业务系统构建的交易和向业务服务端转发区块链上的交易执行结果。为了防止桥接端作恶，上述业务系统构建的交易包含了业务系统基于业务数据所作的第一数字签名，且与桥接端连接的区块链节点设备在其收录上述交易的区块内包含了区块链的节点设备基于交易执行结果所作的第二数字签名，使业务系统对桥接端的信任转化为对区块链中的节点设备的信任；通过数字签名验证技术，有效降低了桥接端作恶而造成的数据安全风险，从而既降低了业务系统接入区块链的成本，又提高了业务系统的数据安全性。

[0109] 与上述流程实现对应，本说明书的实施方式还提供了一种区块链交易装置30和40。装置30和40可以通过软件实现，也可以通过硬件或者软硬件结合的方式实现。以软件实现为例，作为逻辑意义上的装置，是通过所在设备的CPU(Central Process Unit，中央处理器)将对应的计算机程序指令读取到内存中运行形成的。从硬件层面而言，除了图5所示的CPU、内存以及存储器之外，上述装置所在的设备通常还包括用于进行无线信号收发的芯片等其他硬件，和/或用于实现网络通信功能的板卡等其他硬件。

[0110] 如图3所示，本说明书还提供了一种区块链交易装置30，应用于业务系统；所述业务系统通过桥接端与区块链的节点设备连接；所述装置30包括：

[0111] 发送单元302，将构建的目标业务交易通过所述桥接端发送至所述区块链的节点设备，其中，所述目标业务交易包括所述业务系统使用第一私钥为所述目标业务交易的明细数据生成的第一数字签名；以使所述节点设备在进行交易验证时，至少基于与所述第一私钥对应的第一公钥对所述第一数字签名进行验证，在验证通过后，执行所述目标业务交易，并将所述目标业务交易的执行结果和所述区块链中的节点设备使用第二私钥为所述执行结果生成的第二数字签名存储至所述节点设备本地存储的区块链数据库；

[0112] 获取单元304，通过所述桥接端从所述节点设备获取所述目标业务交易的执行结果和所述第二数字签名；

[0113] 验证单元306，基于与所述第二私钥对应的第二公钥验证所述第二数字签名；

[0114] 执行单元308，基于所述执行结果执行与所述交易明细数据相关的进一步的业务处理逻辑。

[0115] 在又一示出的实施方式中，所述第二数字签名为：所述区块链的节点设备使用持有的第二私钥、为收录所述目标业务交易的目标区块的区块头中存储的状态数据库的认证根生成的数字签名。

[0116] 在又一示出的实施方式中，所述状态数据库为基于与所述目标区块中存储的交易对应的状态数据构建的默克尔树；所述认证根为所述默克尔树的root hash。

[0117] 在又一示出的实施方式中，所述第二数字签名由所述区块链的记账节点设备使用其持有的第二私钥生成，所述第二数字签名被保存在所述区块链存储的目标区块的区块头。

[0118] 在又一示出的实施方式中，所述第二数字签名由所述节点设备使用其持有的第二私钥生成，所述第二数字签名被保存在所述节点设备本地存储的所述目标区块的区块头。

[0119] 在又一示出的实施方式中，所述第二数字签名包括：所述节点设备使用持有的第二私钥为所述目标业务交易的执行结果生成的数字签名。

[0120] 在又一示出的实施方式中，所述第二数字签名和所述执行结果，或者，所述第二数字签名和所述执行结果的哈希摘要，被存储在所述桥接端连接的节点设备本地存储的所述目标区块的区块头。

[0121] 在又一示出的实施方式中，所述获取单元304，进一步用于：

[0122] 通过所述桥接端从所述节点设备拉取所述目标区块，以获取所述执行结果和所述第二数字签名；或者，

[0123] 通过所述桥接端从所述节点设备拉取所述目标区块，以获取所述执行结果的哈希摘要和所述第二数字签名；并通过所述桥接端基于所述目标业务交易的检索标识，从所述节点设备获取所述目标业务交易的执行结果。

[0124] 在又一示出的实施方式中，所述第二数字签名和所述执行结果被存储在所述桥接端连接的节点设备本地存储的所述区块链的状态数据库中。

[0125] 如图4所示，本说明书还提供了一种区块链交易装置40，应用于区块链的节点设备；业务系统通过桥接端与所述区块链的节点设备连接；所述装置40包括：

[0126] 获取单元402，与所述桥接端连接的节点设备通过所述桥接端获取所述业务系统

构建的目标业务交易，其中，所述目标业务交易包括所述业务系统使用第一私钥为所述目标业务交易的明细数据生成的第一数字签名；

[0127] 验证单元404，对所述目标业务交易进行交易验证，所述交易验证至少包括基于与所述第一私钥对应的第一公钥对所述第一数字签名进行验证；

[0128] 执行单元406，执行所述目标业务交易；

[0129] 存储单元408，将所述目标业务交易的执行结果和所述区块链中的节点设备使用第二私钥为所述执行结果生成的第二数字签名存储至所述节点设备本地存储的区块链数据库；

[0130] 发送单元410，通过所述桥接端向所述业务系统发送所述执行结果和所述第二数字签名，以使所述业务系统基于与所述第二私钥对应的第二公钥验证所述第二数字签名，并在对所述第二数字签名验证通过后，基于所述执行结果执行与所述交易明细数据相关的进一步的业务处理逻辑。

[0131] 在又一示出的实施方式中，所述第二数字签名包括：所述区块链的节点设备使用持有的第二私钥、为收录所述目标业务交易的目标区块的区块头中存储的状态数据库的认证根生成的数字签名。

[0132] 在又一示出的实施方式中，所述状态数据库为基于与所述目标区块中存储的交易对应的状态数据构建的默克尔树；所述认证根为所述默克尔树的root hash。

[0133] 在又一示出的实施方式中，所述第二数字签名由所述区块链的记账节点设备使用其持有的第二私钥生成，所述第二数字签名被保存在所述区块链存储的目标区块的区块头。

[0134] 在又一示出的实施方式中，所述第二数字签名由所述节点设备使用其持有的第二私钥生成，所述第二数字签名被保存在所述节点设备本地存储的所述目标区块的区块头。

[0135] 在又一示出的实施方式中，所述第二数字签名包括：所述节点设备使用持有的第二私钥为所述目标业务交易的执行结果生成的数字签名。

[0136] 在又一示出的实施方式中，所述第二数字签名和所述执行结果，或者，所述第二数字签名和所述执行结果的哈希摘要被存储在所述节点设备本地存储的所述目标区块的区块头。

[0137] 在又一示出的实施方式中，所述发送单元410，进一步用于：

[0138] 向所述桥接端发送所述目标区块，以使所述业务系统通过所述桥接端获取所述目标区块包括的所述执行结果和所述第二数字签名；或者，

[0139] 向所述桥接端发送所述目标区块，以使所述业务系统通过所述桥接端获取所述目标区块包括的所述执行结果的哈希摘要和所述第二数字签名；并基于所述桥接端发送的所述目标业务交易的检索标识，向所述桥接端发送所述执行结果，以使所述业务系统通过所述桥接端获取所述执行结果。

[0140] 在又一示出的实施方式中，所述第二数字签名和所述执行结果被存储在被存储在所述桥接端连接的节点设备本地存储的所述区块链的状态数据库中。

[0141] 上述装置30、40中各个单元的功能和作用的实现过程具体详见上述业务系统、区块链的节点设备端所执行的区块链交易方法中对应步骤的实现过程，相关之处参见方法实施方式的部分说明即可，在此不再赘述。

[0142] 以上所描述的装置实施方式仅仅是示意性的，其中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模块，即可以位于一个地方，或者也可以分布到多个网络模块上。可以根据实际的需要选择其中的部分或者全部单元或模块来实现本说明书方案的目的。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。

[0143] 上述实施方式阐明的装置、单元、模块，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。

[0144] 与上述方法实施方式相对应，本说明书的实施方式还提供了一种计算机设备，如图5所示，该计算机设备包括存储器和处理器。其中，存储器上存储有能够由处理器运行的计算机程序；处理器在运行存储的计算机程序时，执行本说明书实施方式中业务系统所执行的区块链交易方法的各个步骤。对上述业务系统所执行的区块链交易方法的各个步骤的详细描述请参见之前的内容，不再重复。

[0145] 与上述方法实施方式相对应，本说明书的实施方式还提供了一种计算机设备，如图5所示，该计算机设备包括存储器和处理器。其中，存储器上存储有能够由处理器运行的计算机程序；处理器在运行存储的计算机程序时，执行本说明书实施方式中区块链的节点设备所执行的区块链交易方法的各个步骤。对上述区块链的节点设备所执行的区块链交易方法的各个步骤的详细描述请参见之前的内容，不再重复。

[0146] 以上所述仅为本说明书的较佳实施方式而已，并不用以限制本说明书，凡在本说明书的精神和原则之内，所做的任何修改、等同替换、改进等，均应包含在本说明书保护的范围之内。

[0147] 在一个典型的配置中，计算设备包括一个或多个处理器(CPU)、输入/输出接口、网络接口和内存。

[0148] 内存可能包括计算机可读介质中的非永久性存储器，随机存取存储器(RAM)和/或非易失性内存等形式，如只读存储器(ROM)或闪存(flash RAM)。内存是计算机可读介质的示例。

[0149] 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。

[0150] 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。

[0151] 还需要说明的是，术语“包括”、“包含”或者其任何其他变体意在涵盖非排他性的包含，从而使得包括一系列要素的过程、方法、商品或者设备不仅包括那些要素，而且还包

括没有明确列出的其他要素，或者是还包括为这种过程、方法、商品或者设备所固有的要素。在没有更多限制的情况下，由语句“包括一个……”限定的要素，并不排除在包括所述要素的过程、方法、商品或者设备中还存在另外的相同要素。

[0152] 本领域技术人员应明白，本说明书的实施方式可提供为方法、系统或计算机程序产品。因此，本说明书的实施方式可采用完全硬件实施方式、完全软件实施方式或结合软件和硬件方面的实施方式的形式。而且，本说明书的实施方式可采用在一个或多个其中包含有计算机可用程序代码的计算机可用存储介质(包括但不限于磁盘存储器、CD-ROM、光学存储器等)上实施的计算机程序产品的形式。

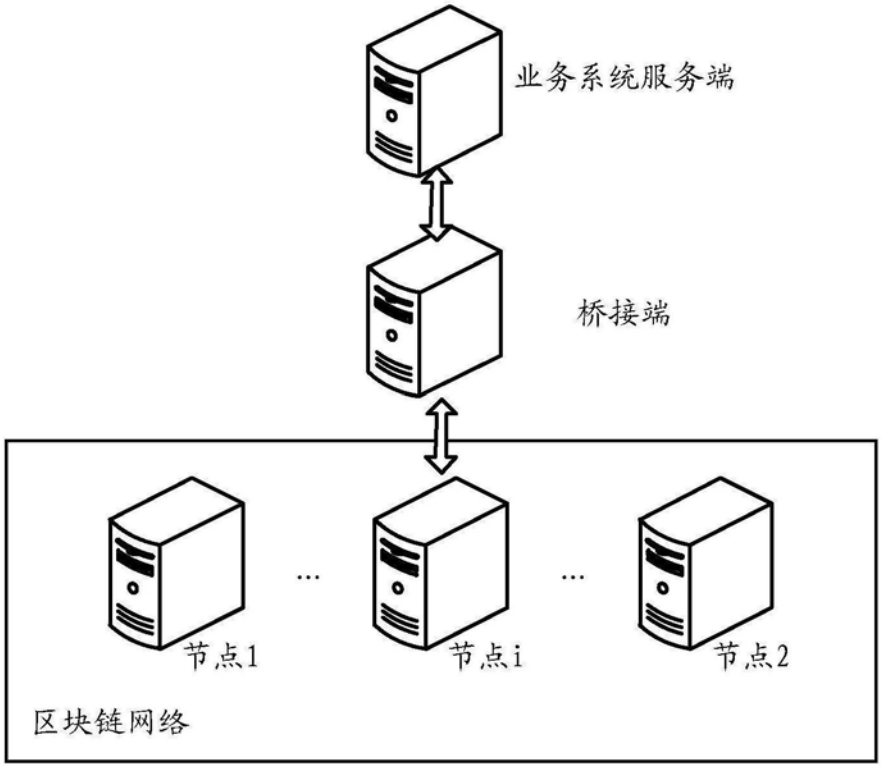


图1

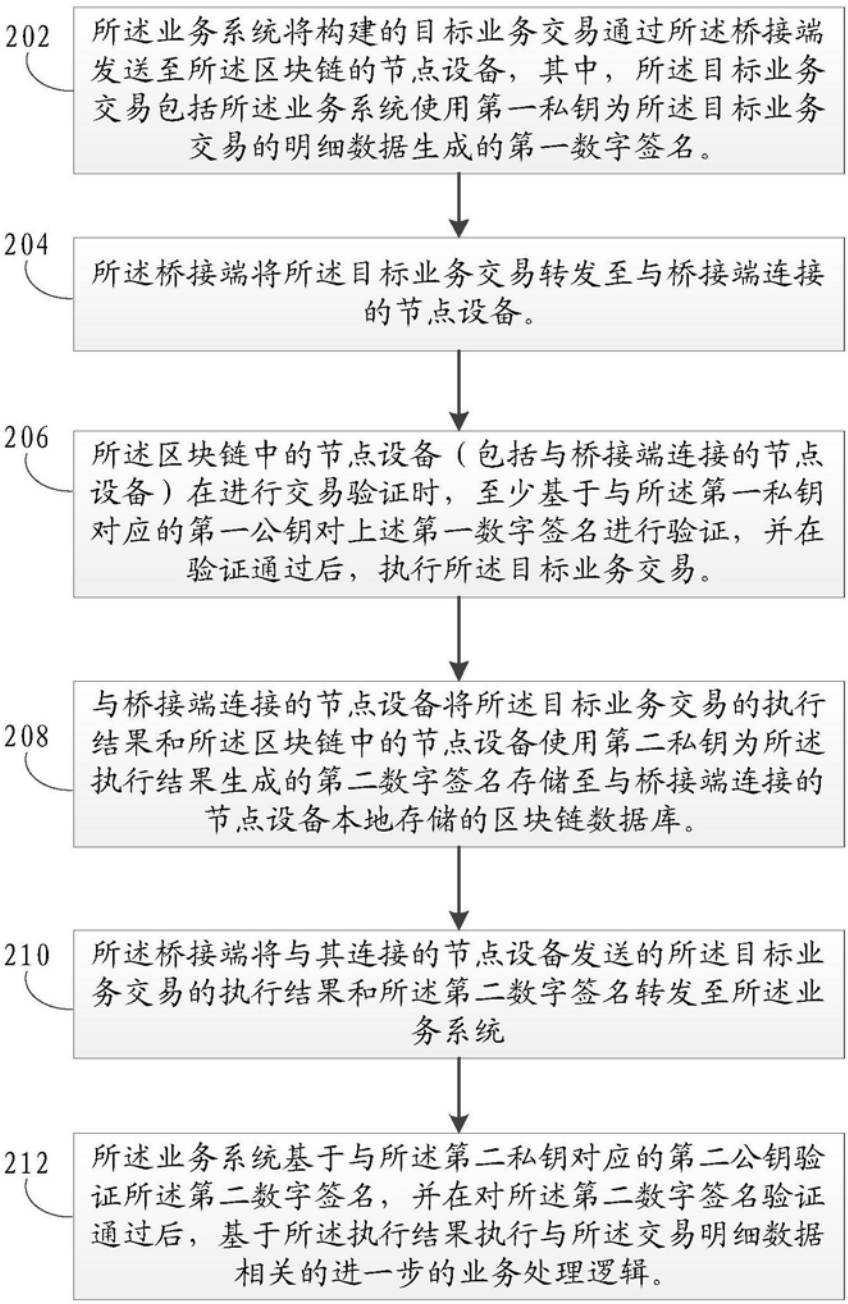

202
所述业务系统将构建的目标业务交易通过所述桥接端发送至所述区块链的节点设备，其中，所述目标业务交易包括所述业务系统使用第一私钥为所述目标业务交易的明细数据生成的第一数字签名。
204
所述桥接端将所述目标业务交易转发至与桥接端连接的节点设备。
206
所述区块链中的节点设备（包括与桥接端连接的节点设备）在进行交易验证时，至少基于与所述第一私钥对应的第一公钥对上述第一数字签名进行验证，并在验证通过后，执行所述目标业务交易。
208
与桥接端连接的节点设备将所述目标业务交易的执行结果和所述区块链中的节点设备使用第二私钥为所述执行结果生成的第二数字签名存储至与桥接端连接的节点设备本地存储的区块链数据库。
210
所述桥接端将与其连接的节点设备发送的所述目标业务交易的执行结果和所述第二数字签名转发至所述业务系统
212
所述业务系统基于与所述第二私钥对应的第二公钥验证所述第二数字签名，并在对所述第二数字签名验证通过后，基于所述执行结果执行与所述交易明细数据相关的进一步的业务处理逻辑。

图2

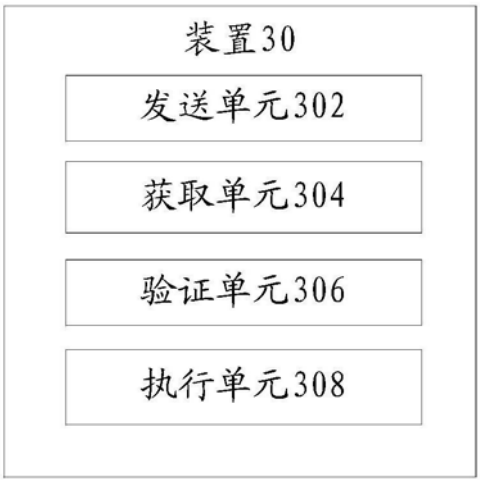

装置30
发送单元302
获取单元304
验证单元306
执行单元308

图3

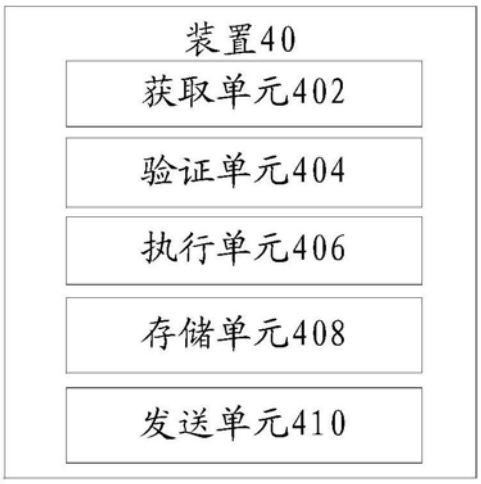

装置40
获取单元402
验证单元404
执行单元406
存储单元408
发送单元410

图4

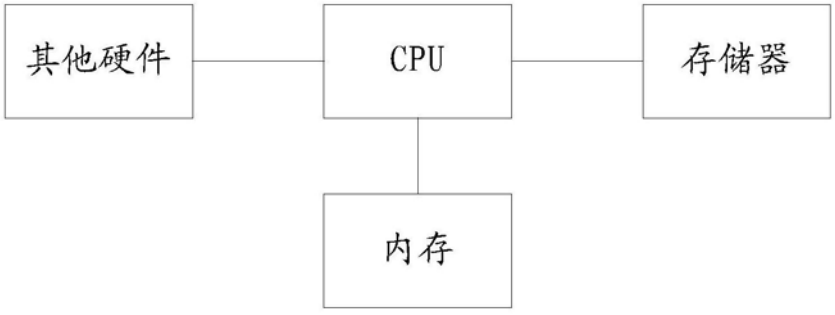

其他硬件
CPU
存储器
内存

图5