(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 112527912 B
(45)授权公告日 2021.06.01

(21)申请号 202110175960.1

(22)申请日 2021.02.07

(65)同一申请的已公布的文献号
申请公布号 CN 112527912 A

(43)申请公布日 2021.03.19

(73)专利权人 腾讯科技(深圳)有限公司
地址 518057 广东省深圳市南山区高新区科技中一路腾讯大厦35层

(72)发明人 温伟力

(74)专利代理机构 广州三环专利商标代理有限公司 44202
代理人 熊永强 杜维

(51)Int.Cl.
G06F 16/27(2019.01)
G06F 16/23(2019.01)
G06F 21/60(2013.01)
G06F 21/64(2013.01)
G06Q 40/04(2012.01)

(56)对比文件
CN 112053153 A,2020.12.08
CN 107908979 A,2018.04.13
CN 109493204 A,2019.03.19
CN 111327426 A,2020.06.23
CN 109150536 A,2019.01.04
US 2020/0007314 A1,2020.01.02

审查员 徐军

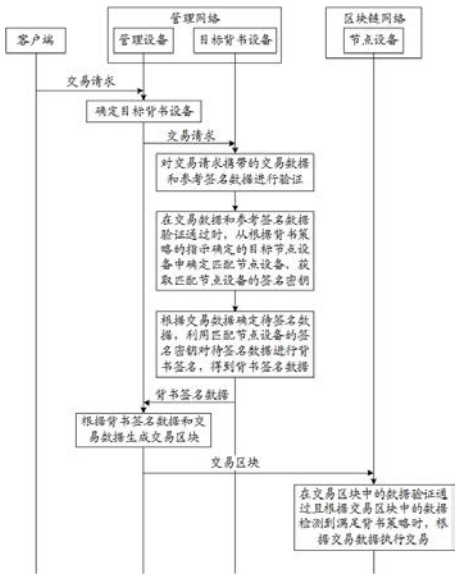
权利要求书4页 说明书17页 附图5页

(54)发明名称

基于区块链网络的数据处理方法、装置及计算机设备

(57)摘要

一种基于区块链网络的数据处理方法、装置及计算机设备，其中方法包括：管理设备获取携带交易数据和参考签名数据的交易请求，确定目标背书设备，并将交易请求发送给目标背书设备；目标背书设备在交易数据和参考签名数据验证通过时，确定匹配节点设备，并获取匹配节点设备的签名密钥，根据交易数据确定待签名数据，并利用匹配节点设备的签名密钥对待签名数据进行背书签名，得到背书签名数据，以及将背书签名数据发送给管理设备；管理设备根据背书签名数据和交易数据生成交易区块。通过本申请实施例可以有效节省共识所需的时间，从而提高整个网络的交易性能。



CN 112527912 B

1.一种基于区块链网络的数据处理方法,其特征在于,所述区块链网络包含于数据处理网络中,所述区块链网络包括多个节点设备,所述数据处理网络还包括管理网络,所述管理网络包括管理设备以及一个或者多个背书设备,所述管理网络中的背书设备存储有所述多个节点设备中至少部分节点设备的签名密钥,所述方法由目标背书设备执行,所述目标背书设备是所述管理设备根据背书策略的指示以及记录的各个背书设备存储节点设备签名密钥的情况,从所述一个或者多个背书设备中确定的,包括:

获取交易请求,所述交易请求携带交易数据和所述交易数据对应的参考签名数据;所述交易请求是所述管理设备在检测到客户端具备发起所述交易请求的权限时发送给所述目标背书设备的;

对所述交易数据和所述参考签名数据进行验证;

在所述交易数据和所述参考签名数据验证通过时,从根据背书策略的指示从所述多个节点设备中确定的目标节点设备中确定匹配节点设备,并获取所述目标背书设备存储的所述匹配节点设备的签名密钥;

根据所述交易数据确定待签名数据,并利用所述匹配节点设备的签名密钥对所述待签名数据进行背书签名,得到背书签名数据;

将所述背书签名数据发送给所述管理设备,以使得所述管理设备根据所述背书签名数据和所述交易数据生成交易区块。

2.如权利要求1所述的方法,其特征在于,所述管理网络中的各个背书设备存储有所述多个节点设备中部分节点设备的签名密钥,且各个背书设备存储不同节点设备的签名密钥,所述获取交易请求,包括:

接收所述管理设备发送的客户端的交易请求;

其中,所述管理设备在接收到所述客户端发送的交易请求之后,根据所述背书策略的指示从所述多个节点设备中确定目标节点设备,并将所述交易请求发送给存储有所述目标节点设备的签名密钥的目标背书设备。

3.如权利要求1所述的方法,其特征在于,所述管理网络中的各个背书设备均存储有所述多个节点设备中各个节点设备的签名密钥,所述获取交易请求,包括:

接收所述管理设备发送的客户端的交易请求;

其中,所述管理设备在接收到所述客户端发送的交易请求之后,根据各个背书设备的当前状态参数从所述一个或者多个背书设备中确定响应所述交易请求的目标背书设备,并将所述交易请求发送给所述目标背书设备。

4.如权利要求1-3任一项所述的方法,其特征在于,所述根据所述交易数据确定待签名数据,包括:

根据所述交易数据模拟执行交易,得到模拟交易结果;

根据所述模拟交易结果确定所述交易请求对应的表决结果,并将所述表决结果作为待签名数据。

5.如权利要求1-3任一项所述的方法,其特征在于,所述参考签名数据是利用秘钥对中的私钥对所述交易数据进行签名得到的,所述方法还包括:

获取所述秘钥对中的公钥,并利用所述秘钥对中的公钥对所述参考签名数据进行解签,得到解签数据;

若所述解签数据与所述交易数据相匹配，则检测所述交易数据是否具备执行性；

若所述交易数据具备执行性，则确定所述交易数据和所述参考签名数据校验通过。

6.一种基于区块链网络的数据处理方法，其特征在于，所述区块链网络包含于数据处理网络中，所述区块链网络包括多个节点设备，所述数据处理网络还包括管理网络，所述管理网络包括管理设备以及一个或者多个背书设备，所述管理网络中的背书设备存储有所述多个节点设备中至少部分节点设备的签名密钥，所述方法由所述管理设备执行，包括：

获取交易请求，所述交易请求携带交易数据和所述交易数据对应的参考签名数据；

在检测到客户端具备发起所述交易请求的权限时，从所述管理网络包括的一个或者多个背书设备中确定目标背书设备；

将所述交易请求发送给所述目标背书设备，以使得所述目标背书设备对所述交易数据和所述参考签名数据进行验证，在所述交易数据和所述参考签名数据验证通过时，从根据背书策略的指示从所述多个节点设备中确定的目标节点设备中确定匹配节点设备，并获取所述目标背书设备存储的所述匹配节点设备的签名密钥，根据所述交易数据确定待签名数据，并利用所述匹配节点设备的签名密钥对所述待签名数据进行背书签名，得到背书签名数据；其中，所述目标背书设备是所述管理设备根据背书策略的指示以及记录的各个背书设备存储节点设备签名密钥的情况，从所述一个或者多个背书设备中确定的；

接收所述目标背书设备发送的所述背书签名数据，并根据所述背书签名数据和所述交易数据生成交易区块。

7.如权利要求6所述的方法，其特征在于，所述管理网络中的各个背书设备存储有所述多个节点设备中部分节点设备的签名密钥，且各个背书设备存储不同节点设备的签名密钥，所述从所述管理网络包括的一个或者多个背书设备中确定目标背书设备，包括：

根据背书策略的指示从所述多个节点设备中确定目标节点设备；

从所述管理网络包括的一个或者多个背书设备中确定存储有所述目标节点设备的签名密钥的背书设备，并将所述存储有所述目标节点设备的签名密钥的背书设备确定为目标背书设备。

8.如权利要求6所述的方法，其特征在于，所述管理网络中的各个背书设备均存储有所述多个节点设备中各个节点设备的签名密钥，所述从所述管理网络包括的一个或者多个背书设备中确定目标背书设备，包括：

获取所述管理网络中各个背书设备的当前状态参数；

根据所述各个背书设备的当前状态参数从所述管理网络包括的一个或者多个背书设备中确定响应所述交易请求的背书设备，并将所述响应所述交易请求的背书设备确定为目标背书设备。

9.如权利要求6-8任一项所述的方法，其特征在于，所述方法还包括：

将所述交易区块广播给所述区块链网络中的节点设备，以使得所述区块链网络中的节点设备在所述交易区块中的数据验证通过且根据所述交易区块中的数据检测到满足背书策略时，根据所述交易数据执行交易。

10.一种基于区块链网络的数据处理装置，其特征在于，所述区块链网络包含于数据处理网络中，所述区块链网络包括多个节点设备，所述数据处理网络还包括管理网络，所述管理网络包括管理设备以及一个或者多个背书设备，所述管理网络中的背书设备存储有所述

多个节点设备中至少部分节点设备的签名密钥，所述装置对应于目标背书设备，所述目标背书设备是所述管理设备根据背书策略的指示以及记录的各个背书设备存储节点设备签名密钥的情况，从所述一个或者多个背书设备中确定的，包括：

获取单元，用于获取交易请求，所述交易请求携带交易数据和所述交易数据对应的参考签名数据；所述交易请求是所述管理设备在检测到客户端具备发起所述交易请求的权限时发送给所述目标背书设备的；

处理单元，用于对所述交易数据和所述参考签名数据进行验证；

所述处理单元，还用于在所述交易数据和所述参考签名数据验证通过时，从根据背书策略的指示从所述多个节点设备中确定的目标节点设备中确定匹配节点设备，并获取所述目标背书设备存储的所述匹配节点设备的签名密钥；

所述处理单元，还用于根据所述交易数据确定待签名数据，并利用所述匹配节点设备的签名密钥对所述待签名数据进行背书签名，得到背书签名数据；

收发单元，用于将所述背书签名数据发送给所述管理设备，以使得所述管理设备根据所述背书签名数据和所述交易数据生成交易区块。

11.一种基于区块链网络的数据处理装置，其特征在于，所述区块链网络包含于数据处理网络中，所述区块链网络包括多个节点设备，所述数据处理网络还包括管理网络，所述管理网络包括管理设备以及一个或者多个背书设备，所述管理网络中的背书设备存储有所述多个节点设备中至少部分节点设备的签名密钥，所述装置对应于所述管理设备，包括：

获取单元，用于获取交易请求，所述交易请求携带交易数据和所述交易数据对应的参考签名数据；

处理单元，用于在检测到客户端具备发起所述交易请求的权限时，从所述管理网络包括的一个或者多个背书设备中确定目标背书设备；

收发单元，用于将所述交易请求发送给所述目标背书设备，以使得所述目标背书设备对所述交易数据和所述参考签名数据进行验证，在所述交易数据和所述参考签名数据验证通过时，从根据背书策略的指示从所述多个节点设备中确定的目标节点设备中确定匹配节点设备，并获取所述目标背书设备存储的所述匹配节点设备的签名密钥，根据所述交易数据确定待签名数据，并利用所述匹配节点设备的签名密钥对所述待签名数据进行背书签名，得到背书签名数据；其中，所述目标背书设备是所述管理设备根据背书策略的指示以及记录的各个背书设备存储节点设备签名密钥的情况，从所述一个或者多个背书设备中确定的；

所述收发单元，还用于接收所述目标背书设备发送的所述背书签名数据；

所述处理单元，还用于根据所述背书签名数据和所述交易数据生成交易区块。

12.一种计算机设备，其特征在于，包括：处理器、通信接口和存储器，所述处理器、所述通信接口和所述存储器相互连接，其中，所述存储器存储有可执行程序代码，所述处理器用于调用所述可执行程序代码，执行如权利要求1-5中任一项所述的基于区块链网络的数据处理方法，或者执行如权利要求6-9中任一项所述的基于区块链网络的数据处理方法。

13.一种计算机可读存储介质，其特征在于，所述计算机可读存储介质中存储有计算机程序，当其在计算机上运行时，使得计算机执行如权利要求1-5中任一项所述的基于区块链网络的数据处理方法，或者执行如权利要求6-9中任一项所述的基于区块链网络的数据处

理方法。

基于区块链网络的数据处理方法、装置及计算机设备

技术领域

[0001] 本申请涉及区块链技术领域，尤其涉及一种基于区块链网络的数据处理方法、装置及计算机设备。

背景技术

[0002] 随着科技时代的到来和移动互联网的发展，网络变革的步伐也愈来愈快，实现同一领域或多个领域的信息融合，为客户提供全方位信息化方案的过程亦面临着体系结构的改进、支撑重心转移等新的挑战。因此，区块链技术作为分布式账本的一种特定实现，凭借其存储和管理数据的天然优势，逐渐成为各个领域存储数据和交易数据的首选方式。

[0003] 区块链网络的交易流程对交易性能有很大的影响，通常情况下，区块链网络中的每笔交易都需要通过共识后才能被各个节点执行或者上链。为保证共识结果的准确性，通常区块链网络中的大多数节点都被设置为共识节点，均需要参与到每一次共识过程，这导致共识过程耗时长，交易性能低效。因此，如何提高区块链网络的交易性能是有待解决的问题。

发明内容

[0004] 本申请实施例提供了一种基于区块链网络的数据处理方法、装置及计算机设备，可以有效节省共识所需的时间，从而提高整个网络的交易性能。

[0005] 一方面，本申请实施例提供了一种基于区块链网络的数据处理方法，所述区块链网络包含于数据处理网络中，所述区块链网络包括多个节点设备，所述数据处理网络还包括管理网络，所述管理网络包括管理设备以及一个或者多个背书设备，所述方法包括：

[0006] 获取交易请求，所述交易请求携带交易数据和所述交易数据对应的参考签名数据；对所述交易数据和所述参考签名数据进行验证；在所述交易数据和所述参考签名数据验证通过时，从根据背书策略的指示从所述多个节点设备中确定的目标节点设备中确定匹配节点设备，并获取所述匹配节点设备的签名密钥；根据所述交易数据确定待签名数据，并利用所述匹配节点设备的签名密钥对所述待签名数据进行背书签名，得到背书签名数据；将所述背书签名数据发送给所述管理设备，以使得所述管理设备根据所述背书签名数据和所述交易数据生成交易区块。

[0007] 一方面，本申请实施例提供了另一种基于区块链网络的数据处理方法，所述区块链网络包含于数据处理网络中，所述区块链网络包括多个节点设备，所述数据处理网络还包括管理网络，所述管理网络包括管理设备以及一个或者多个背书设备，所述方法包括：

[0008] 获取交易请求，所述交易请求携带交易数据和所述交易数据对应的参考签名数据；从所述管理网络包括的一个或者多个背书设备中确定目标背书设备；将所述交易请求发送给所述目标背书设备，以使得所述目标背书设备根据所述交易数据和所述参考签名数据得到背书签名数据；接收所述目标背书设备发送的所述背书签名数据，并根据所述背书签名数据和所述交易数据生成交易区块。

[0009] 一方面，本申请实施例提供了一种基于区块链网络的数据处理装置，所述区块链网络包含于数据处理网络中，所述区块链网络包括多个节点设备，所述数据处理网络还包括管理网络，所述管理网络包括管理设备以及一个或者多个背书设备，所述装置包括：

[0010] 获取单元，用于获取交易请求，所述交易请求携带交易数据和所述交易数据对应的参考签名数据；

[0011] 处理单元，用于对所述交易数据和所述参考签名数据进行验证；

[0012] 所述处理单元，还用于在所述交易数据和所述参考签名数据验证通过时，从根据背书策略的指示从所述多个节点设备中确定的目标节点设备中确定匹配节点设备，并获取所述匹配节点设备的签名密钥；

[0013] 所述处理单元，还用于根据所述交易数据确定待签名数据，并利用所述匹配节点设备的签名密钥对所述待签名数据进行背书签名，得到背书签名数据；

[0014] 收发单元，用于将所述背书签名数据发送给所述管理设备，以使得所述管理设备根据所述背书签名数据和所述交易数据生成交易区块。

[0015] 在一实施例中，所述管理网络中的背书设备存储有所述多个节点设备中至少部分节点设备的签名密钥。

[0016] 在一实施例中，所述管理网络中的各个背书设备存储有所述多个节点设备中部分节点设备的签名密钥，且各个背书设备存储不同节点设备的签名密钥，所述获取单元，具体用于：触发所述收发单元接收所述管理设备发送的客户端的交易请求；其中，所述管理设备在接收到所述客户端发送的交易请求之后，根据所述背书策略的指示从所述多个节点设备中确定目标节点设备，并将所述交易请求发送给存储有所述目标节点设备的签名密钥的目标背书设备。

[0017] 在一实施例中，所述管理网络中的各个背书设备均存储有所述多个节点设备中各个节点设备的签名密钥，所述获取单元，具体用于：触发所述收发单元接收所述管理设备发送的客户端的交易请求；其中，所述管理设备在接收到所述客户端发送的交易请求之后，根据各个背书设备的当前状态参数从所述一个或者多个背书设备中确定响应所述交易请求的目标背书设备，并将所述交易请求发送给所述目标背书设备。

[0018] 在一实施例中，所述处理单元根据所述交易数据确定待签名数据时，具体用于：根据所述交易数据模拟执行交易，得到模拟交易结果；根据所述模拟交易结果确定所述交易请求对应的表决结果，并将所述表决结果作为待签名数据。

[0019] 在一实施例中，所述参考签名数据是利用秘钥对中的私钥对所述交易数据进行签名得到的，所述获取单元，还用于获取所述秘钥对中的公钥；所述处理单元，还用于：利用所述秘钥对中的公钥对所述参考签名数据进行解签，得到解签数据；若所述解签数据与所述交易数据相匹配，则检测所述交易数据是否具备执行性；若所述交易数据具备执行性，则确定所述交易数据和所述参考签名数据校验通过。

[0020] 一方面，本申请实施例提供了另一种基于区块链网络的数据处理装置，所述区块链网络包含于数据处理网络中，所述区块链网络包括多个节点设备，所述数据处理网络还包括管理网络，所述管理网络包括管理设备以及一个或者多个背书设备，所述装置包括：

[0021] 获取单元，用于获取交易请求，所述交易请求携带交易数据和所述交易数据对应的参考签名数据；

[0022] 处理单元，用于从所述管理网络包括的一个或者多个背书设备中确定目标背书设备；

[0023] 收发单元，用于将所述交易请求发送给所述目标背书设备，以使得所述目标背书设备根据所述交易数据和所述参考签名数据得到背书签名数据；

[0024] 所述收发单元，还用于接收所述目标背书设备发送的所述背书签名数据；

[0025] 所述处理单元，还用于根据所述背书签名数据和所述交易数据生成交易区块。

[0026] 在一实施例中，所述管理网络中的背书设备存储有所述多个节点设备中至少部分节点设备的签名密钥。

[0027] 在一实施例中，所述管理网络中的各个背书设备存储有所述多个节点设备中部分节点设备的签名密钥，且各个背书设备存储不同节点设备的签名密钥，所述处理单元具体用于：根据背书策略的指示从所述多个节点设备中确定目标节点设备；从所述管理网络包括的一个或者多个背书设备中确定存储有所述目标节点设备的签名密钥的背书设备，并将所述存储有所述目标节点设备的签名密钥的背书设备确定为目标背书设备。

[0028] 在一实施例中，所述管理网络中的各个背书设备均存储有所述多个节点设备中各个节点设备的签名密钥，所述获取单元，还用于获取所述管理网络中各个背书设备的当前状态参数；所述处理单元具体用于：根据所述各个背书设备的当前状态参数从所述管理网络包括的一个或者多个背书设备中确定响应所述交易请求的背书设备，并将所述响应所述交易请求的背书设备确定为目标背书设备。

[0029] 在一实施例中，所述处理单元还用于：触发所述收发单元将所述交易区块广播给所述区块链网络中的节点设备，以使得所述区块链网络中的节点设备在所述交易区块中的数据验证通过且根据所述交易区块中的数据检测到满足所述背书策略时，根据所述交易数据执行交易。

[0030] 一方面，本申请实施例提供了一种计算机设备，包括：处理器、通信接口和存储器，所述处理器、所述通信接口和所述存储器相互连接，其中，所述存储器存储有可执行程序代码，所述处理器用于调用所述可执行程序代码，执行本申请实施例提供的基于区块链网络的数据处理方法。

[0031] 相应地，本申请实施例还提供了一种计算机可读存储介质，所述计算机可读存储介质中存储有计算机程序，当其在计算机上运行时，使得计算机执行本申请实施例提供的基于区块链网络的数据处理方法。

[0032] 相应地，本申请实施例还提供了一种计算机程序产品或计算机程序，所述计算机程序产品或计算机程序包括计算机指令，所述计算机指令存储在计算机可读存储介质中。计算机设备的处理器从所述计算机可读存储介质读取所述计算机指令，处理器执行所述计算机指令，使得所述计算机设备执行上述方法。

[0033] 本申请实施例中，在数据处理网络中设置管理网络，由管理网络中的背书设备对交易请求中的数据进行验证，并在数据验证通过之后，按照背书策略的指示利用相应节点设备的签名密钥，对根据交易数据确定的待签名数据进行背书签名，得到背书签名数据。采用此方式，可以由管理网络集中高效的完成数据验证和背书签名操作，即完成共识操作，无需区块链网络中的节点参与交易的共识，这样可以有效节省共识所需的时间，提高交易流程的处理效率，从而提高整个网络的交易性能。

附图说明

[0034] 为了更清楚地说明本申请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申请的一些实施例，对于本领域普通技术人员来讲，在不付出创造性劳动的前提下，还可以根据这些附图获得其他的附图。

[0035] 图1a是本申请实施例提供的一种数据处理网络的架构示意图；

[0036] 图1b是本申请实施例提供的另一种数据处理网络的架构示意图；

[0037] 图2是本申请实施例提供的一种数据处理方法的流程示意图；

[0038] 图3示出了本申请实施例中背书设备与节点设备之间的一种对应关系；

[0039] 图4示出了Fabric区块链的交易流程；

[0040] 图5示出了本申请实施例提供的区块链跨域节点治理方案的一种架构；

[0041] 图6示出了本申请实施例提供的区块链跨域节点治理方案的另一种架构；

[0042] 图7是本申请实施例提供的一种数据处理装置的结构示意图；

[0043] 图8是本申请实施例提供的一种计算机设备的结构示意图。

具体实施方式

[0044] 下面将结合本申请实施例中的附图，对本申请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申请一部分实施例，而不是全部的实施例。基于本申请中的实施例，本领域普通技术人员在没有作出创造性劳动前提下所获得的所有其他实施例，都属于本申请保护的范围。

[0045] 为更好的理解本申请实施例，下面先对本申请实施例所涉及的一些术语进行介绍。

[0046] 区块链(Blockchain)：一种去中心化的分布式账本数据库，用分布式数据库识别、传播和记载信息的智能化对等网络，也称为价值互联网。利用共识机制，密码学等保证数据传输和查询的准确性，它的特性包括不可篡改、可溯源，等等。区块链是分布式数据存储、点对点传输、共识机制、加密算法等计算机技术的新型应用模式。区块链本质上是一个去中心化的数据库，是一串使用密码学方法相关联产生的数据块，每一个数据块中包含了一批次网络交易的信息，用于验证其信息的有效性(防伪)和生成下一个区块。

[0047] 通常情况下，区块链可以包括区块链底层平台、平台产品服务层以及应用服务层。区块链底层平台可以包括用户管理、基础服务、智能合约以及运营监控等处理模块。其中，用户管理模块负责所有区块链参与者的身份信息管理，包括维护公私钥生成(账户管理)、密钥管理以及用户真实身份和区块链地址对应关系维护(权限管理)等，并且在授权的情况下，监管和审计某些真实身份的交易情况，提供风险控制的规则配置(风控审计)；基础服务模块部署在所有区块链节点设备上，用来验证业务请求的有效性，并对有效请求完成共识后记录到存储上，对于一个新的业务请求，基础服务先对接口适配解析和鉴权处理(接口适配)，然后通过共识算法将业务信息加密(共识管理)，在加密之后完整一致的传输至共享账本上(网络通信)，并进行记录存储；智能合约模块负责合约的注册发行以及合约触发和合约执行，开发人员可以通过某种编程语言定义合约逻辑，发布到区块链上(合约注册)，根据合约条款的逻辑，调用密钥或者其它的事件触发执行，完成合约逻辑，同时还提供对合约升

级注销的功能;运营监控模块主要负责产品发布过程中的部署、配置的修改、合约设置、云适配以及产品运行中的实时状态的可视化输出,例如:告警、监控网络情况、监控节点设备健康状态等。

[0048] 平台产品服务层提供典型应用的基本能力和实现框架,开发人员可以基于这些基本能力,叠加业务的特性,完成业务逻辑的区块链实现。应用服务层提供基于区块链方案的应用服务给业务参与方进行使用。

[0049] 可信计算:可信计算(Trusted Computing,TC)是一项由可信计算组(或者说可信计算集群,前称为TCPA)推动和开发的技术。可信计算是在计算和通信系统中广泛使用基于硬件安全模块支持下的可信计算平台,以提高系统整体的安全性。签注密钥是一个特定位数(如2048位)的RSA公共和私有密钥对,它在计算机设备出厂时随机生成并且不能改变。这个私有密钥保存在计算机设备中,而公共密钥可以用来认证及加密发送给计算机设备的敏感数据。

[0050] 跨域:这里不是单指跨地域,而是泛指同一个区块链网络中,节点没有部署在同一个集群内,节点间需要通过跨域访问。这里的跨域可以是跨集群,跨地域等。

[0051] 联盟链:只针对某个特定群体的成员和有限的第三方,其内部指定多个预选节点为记账人,每个块的生成由所有的预选节点共同决定。

[0052] 背书机制:在区块链(如联盟链中的Hyperledger Fabric区块链)中,有一些节点承担背书任务,可以使用背书策略来定义哪些节点需要执行交易。在区块链交易方面有一种新颖的思路,将智能合约的执行与账本的更新分开以提高交易吞吐量,支持更细粒度的隐私控制,实现更灵活强大的智能合约。而这些特性得以实现的一个关键因素就是在交易加入账本之前进行显式地交易背书。在区块链中背书可以理解为承担背书任务的节点为区块链交易进行交易信息验证,对验证通过的交易声明此交易合法的过程和机制。承担背书任务的节点必须通过有效证书的预期信息的有效签名来证明其合法性。

[0053] 背书策略(endorsement policy):可以理解为是对交易进行背书必须满足的条件,即要得到背书成功的结论,必须满足背书策略中给出的条件。区块链节点有预先指定的背书策略集,这些背书的条件判断在链码(Chaincode)中实现,所有的交易都必须依据背书策略进行交易,因为只有经过背书处理的交易才是合法、被认可的交易。因此背书策略也可以说就是用来指导被选中的节点如何决策交易是否正确的条件。

[0054] 一些背书策略样例如下:节点A、B、C和F都需要对类型为T的交易进行背书;通道中的大部分节点必须对类型为U的交易进行背书;A、B、C、D、E、F、G中的至少3个节点必须对类型为V的交易进行背书。

[0055] 区块链网络的交易流程对交易性能有很大的影响,通常情况下,区块链网络中的每笔交易都需要通过共识后才能被各个节点执行或者上链。为保证共识结果的准确性,通常区块链网络中的大多数节点(或者称之为节点设备)都被设置为共识节点,均需要参与到每一次共识过程,这导致共识过程耗时长,交易性能低效。基于此,本申请实施例提供了一种基于区块链网络的数据处理方法,以有效节省共识所需的时间,从而提高整个网络的交易性能。

[0056] 本申请实施例提供的数据处理方法基于区块链技术。在可行的实施例中,本申请实施例提供的数据处理方法还基于云技术(Cloud technology)。云技术是基于云计算商业

模式应用的网络技术、信息技术、整合技术、管理平台技术、应用技术等的总称，可以组成资源池，按需所用，灵活便利；而本申请实施例提供的数据处理方法主要涉及云技术中的云存储(Cloud storage)和云数据库(Cloud Database)，等等。

[0057] 本申请实施例提供的数据处理方法应用于数据处理网络中，该数据处理网络如图1a或者图1b所示，包括：客户端10、管理网络11和区块链网络12。管理网络11包括管理设备以及一个或者多个背书设备，区块链网络12包括多个节点设备。在一实施例中，如图1a所示，客户端10可既不包含于管理网络11中，也不包含于区块链网络12中。在另一实施例中，如图1b所示，客户端10可包含于区块链网络12中。

[0058] 在一实施例中，如图1a或者图1b所示，管理网络11与区块链网络12可以是两个不同的网络，即管理网络11独立于区块链网络12存在。在另一实施例中，管理网络也可以包含于区块链网络中，此时，管理网络中的管理设备和背书设备可以是区块链网络中的节点设备，也可以是区块链网络中除节点设备之外的普通计算机设备。

[0059] 管理网络可以是基于云技术实现的，具体可以是基于腾讯云或者阿里云等实现的。在可行的实施例中，背书设备可以是加密机，可以是物理的加密机，也可以是虚拟的加密机。当背书设备为虚拟的加密机时，虚拟加密机需要承载在计算机设备上。当管理网络中包括管理设备以及一个背书设备时，背书设备可以是管理设备的一部分，即背书设备设置于管理设备中。

[0060] 管理网络中的设备(背书设备和/或管理设备)基于可信计算，并托管区块链网络中至少部分节点设备的签名密钥，可以是存储区块链网络中每一个节点设备的签名密钥，也可以是存储区块链网络中部分节点设备的签名密钥，该部分节点设备为背书策略指示的可能用于承担背书任务的所有节点设备。在一实施例中，签名密钥可以是节点设备的密钥对中的私钥。密钥对可以是采用RSA加密算法计算得出的，包括私钥和公钥，通常私钥用于签名，公钥用于解签。管理网络中的背书设备可以取代区块链网络中的节点设备来提供数据验证(包括验签、校验交易数据等)和背书签名等服务，管理网络中的管理设备可以取代区块链网络中的节点设备来提供区块生成等服务。其中，背书签名就是一个共识过程。

[0061] 本申请实施例中，客户端、管理设备、背书设备和节点设备可以是服务器或者终端。服务器可以是独立的物理服务器，也可以是多个物理服务器构成的服务器集群或者分布式系统，还可以是提供云服务、云数据库、云计算、云函数、云存储、网络服务、云通信、中间件服务、域名服务、安全服务、CDN、以及大数据和人工智能平台等基础云计算服务的云服务器。终端可以是智能手机、平板电脑、笔记本电脑、台式计算机、智能音箱、智能手表等，但并不局限于此。客户端、管理设备、背书设备和节点设备之间可以通过有线或无线通信方式进行直接或间接地连接，本申请在此不做限制。

[0062] 本申请实施例提供的数据处理方法，通过在数据处理网络中设置管理网络，由管理网络中的背书设备对客户端的交易请求中的数据进行验证，并在数据验证通过之后，按照背书策略的指示利用相应节点设备的签名密钥，对根据交易数据确定的待签名数据进行背书签名，得到背书签名数据，从而可以由管理网络集中高效的完成数据验证和背书签名操作，即完成共识操作，无需区块链网络中的节点参与交易的共识，这样可以有效节省共识所需的时间，提高交易流程的处理效率，达到提高整个网络的交易性能的效果。

[0063] 请参阅图2，为本申请实施例提供的一种基于区块链网络的数据处理方法的流程

示意图。本申请实施例中所描述的基于区块链网络的数据处理方法应用于图1a或者图1b所示的数据处理网络中，包括但不限于如下步骤：

[0064] S201、客户端向管理网络中的管理设备发送交易请求，该交易请求携带交易数据和交易数据对应的参考签名数据。

[0065] 在一实施例中，参考签名数据可以是客户端利用其秘钥对中的私钥对交易数据进行签名得到的。密钥对可以是采用RSA加密算法计算得出的，包括私钥和公钥，通常私钥用于签名，公钥用于解签。

[0066] S202、管理设备获取客户端的交易请求，并从管理网络包括的一个或者多个背书设备中确定目标背书设备。

[0067] 针对节点设备的签名密钥的不同存储情况，可以采用如下二种方式来确定目标背书设备。

[0068] 方式一：

[0069] 管理网络中的各个背书设备存储有区块链网络中部分节点设备的签名密钥，且各个背书设备存储不同节点设备的签名密钥。管理网络中的背书设备存储的所有签名密钥对应的节点设备可以是区块链网络中的所有节点设备，也可以是区块链网络中的部分节点设备，该部分节点设备为背书策略指示的可能用于承担背书任务的所有节点设备。

[0070] 如图3所示，管理网络中的各个背书设备存储有区块链网络中一个或者多个节点设备的签名密钥。例如，背书设备1存储区块链网络中编号为1-X的X个节点设备的签名密钥，背书设备4存储区块链网络中编号为Z+1的节点设备的签名密钥。

[0071] 在可行的实施方式中，区块链网络中的多个节点设备部署在不同的集群中。例如，如图3所示，编号为1至X的节点设备部署在一个集群中，而编号为X+1至Y的节点设备部署在另一个集群中。管理网络中的背书设备存储区块链网络中属于同一个集群中的一个或者多个节点设备的签名密钥。

[0072] 管理设备接收到客户端发送的交易请求之后，根据背书策略的指示从区块链网络中包括的多个节点设备中确定目标节点设备，该目标节点设备为一个或者多个。确定出的目标节点设备为背书策略指示的针对当前交易需要承担背书任务的节点设备。例如，客户端发起的是类型为T的交易，按照预设的背书策略的指示，需要区块链网络中的节点设备A、B、C和F对类型为T的交易进行背书，则将区块链网络中的节点设备A、B、C和F确定为目标节点设备。

[0073] 进一步的，管理设备根据记录的各个背书设备存储节点设备签名密钥的情况，以及确定出的目标节点设备，从管理网络包括的一个或者多个背书设备中确定存储有目标节点设备的签名密钥的背书设备，并将存储有目标节点设备的签名密钥的背书设备确定为目标背书设备。确定出的目标背书设备为一个或者多个，其存储的所有签名密钥中包含每一个目标节点设备的签名密钥。管理设备在向目标背书设备发送客户端的交易请求时，可以一并发送目标节点设备的信息(如节点编号等)，可以是发送目标背书设备存储有相应签名密钥的目标节点设备的信息。

[0074] 方式二：

[0075] 管理网络中的各个背书设备均存储有区块链网络中各个节点设备的签名密钥，或者，管理网络中的各个背书设备均存储有区块链网络中相同部分节点设备的签名密钥，该

部分节点设备为背书策略指示的可能用于承担背书任务的所有节点设备。

[0076] 管理设备接收到客户端发送的交易请求之后，获取管理网络中各个背书设备的当前状态参数，该状态参数包括用于指示网络状况的参数、用于指示负载状况的参数，等等。根据各个背书设备的当前状态参数从管理网络包括的一个或者多个背书设备中确定用于响应该交易请求的目标背书设备，可以是将当前网络状况好且负载小的背书设备确定为用于响应该交易请求的目标背书设备。确定出的目标背书设备为一个或者多个。

[0077] 在可行的实施方式中，可以预先设置每一个背书设备的选取顺序，并按照该选取顺序从管理网络包括的一个或者多个背书设备中，选取当前用于提供背书服务的一个或者多个目标背书设备。例如，设置的背书设备的选取顺序为(背书设备1)→(背书设备2和3)→(背书设备4和5)。若上一次提供背书服务的是背书设备1，则这一次应选取背书设备2和3提供背书服务。

[0078] 在可行的实施方式中，当确定出的目标背书设备为多个时，管理设备可以对应设置每一个背书设备所承担的背书任务。例如，按照背书策略的指示针对当前交易需要目标节点设备1-10承担背书任务，如果这一次选取的是背书设备2和3提供背书服务，则可以设置背书设备2承担目标节点设备1-3对应的背书任务，设置背书设备3承担目标节点设备4-10对应的背书任务。管理设备在向目标背书设备发送客户端的交易请求时，可以一并发送目标背书设备对应的背书任务指示信息，该背书任务指示信息用于指示目标背书设备需要承担哪些目标节点设备对应的背书任务。

[0079] 在一实施例中，该交易请求还携带客户端的设备标识，管理设备接收到客户端发送的交易请求之后，先确定客户端是否具备发起交易请求的权限，包括检测客户端的设备标识是否在预设白名单中，若在，则确定客户端具备发起交易请求的权限，反之，则确定客户端不具备发起交易请求的权限。若客户端具备发起交易请求的权限，则从管理网络包括的一个或者多个背书设备中确定目标背书设备。若客户端不具备发起交易请求的权限，则直接拒绝客户端的交易请求。

[0080] S203、管理设备将客户端的交易请求发送给目标背书设备。

[0081] S204、目标背书设备获取客户端的交易请求，并对交易请求携带的交易数据和参考签名数据进行验证。

[0082] 在一实施例中，若参考签名数据是利用客户端的秘钥对中的私钥对交易数据进行签名得到的，则目标背书设备获取客户端的秘钥对中的公钥，并利用该公钥对参考签名数据进行解签，得到解签数据；若解签数据与交易数据相匹配，则表明交易数据未被篡改，并进一步检测交易数据是否具备执行性，包括检测交易数据所对应的交易是否合法，是否已经被执行过，等等，若合法且未被执行过，则可以确定具备执行性；若交易数据具备执行性，则确定交易请求中的交易数据和所述参考签名数据校验通过。

[0083] 在可行的实施方式中，客户端的公钥可以携带在交易请求中，也可以存储在各个背书设备中，还可以存储在管理设备中。当客户端的公钥存储在管理设备中时，目标背书设备可以主动从管理设备获取客户端的公钥，也可以由管理设备在向目标节点设备发送客户端的交易请求时一并发送给目标背书设备。

[0084] S205、在交易数据和参考签名数据验证通过时，目标背书设备从根据背书策略的指示从区块链网络包括的多个节点设备中确定的目标节点设备中确定匹配节点设备，并获

取匹配节点设备的签名密钥。

[0085] 本申请实施例中，在交易数据和参考签名数据验证通过时，目标背书设备确定其需要承担哪些目标节点设备对应的背书任务，即确定匹配节点设备，匹配节点设备为一个或者多个，其包括在背书策略指示的针对当前交易需要承担背书任务的一个或者多个目标节点设备中。

[0086] 针对步骤S202中的方式一所指示的情况，匹配节点设备为该一个或者多个目标节点设备中目标背书设备存储有相应签名密钥的目标节点设备。目标背书设备可以先根据背书策略的指示从区块链网络中包括的多个节点设备中，确定针对当前交易需要承担背书任务的一个或者多个目标节点设备；然后从该一个或者多个目标节点设备中确定存储有相应签名密钥的匹配节点设备。在另一实施方式中，若接收到管理设备发送的目标背书设备存储有相应签名密钥的目标节点设备的信息时，直接将该信息所指示的目标节点设备确定为匹配节点设备。

[0087] 针对步骤S202中的方式二所指示的情况，匹配节点设备为该一个或者多个目标节点设备中目标背书设备所需承担相应背书任务的目标节点设备。

[0088] 在确定出匹配节点设备之后，获取匹配节点设备的签名密钥。在一实施例中，签名密钥可以是节点设备的密钥对中的私钥。密钥对可以是采用RSA加密算法计算得出的，包括私钥和公钥，通常私钥用于签名，公钥用于解签。

[0089] S206、目标背书设备根据交易数据确定待签名数据，并利用匹配节点设备的签名密钥对待签名数据进行背书签名，得到背书签名数据。

[0090] 在一实施例中，目标背书设备根据交易数据模拟执行交易，得到模拟交易结果；根据模拟交易结果确定交易请求对应的表决结果，例如，如果模拟交易结果指示交易可以正确执行，则生成同意的表决结果。进一步地，将确定的表决结果作为待签名数据，并利用各匹配节点设备的签名密钥分别对该待签名数据进行签名，得到各签名密钥分别对应的背书签名数据。

[0091] S207、目标背书设备将背书签名数据发送给管理设备。

[0092] S208、管理设备接收目标背书设备发送的背书签名数据，并根据背书签名数据和交易数据生成交易区块。

[0093] 本申请实施例中，管理设备接收各个目标背书设备发送的一个或者多个背书签名数据，并在接收到各个目标背书设备发送的背书签名数据之后，根据接收到的背书签名数据和交易数据生成交易区块。

[0094] 在一实施例中，管理设备在接收到目标背书设备发送的背书签名数据之后，先对背书签名数据进行验证(即验签)，并在各个背书签名数据验证通过之后，生成交易区块。若存在验证未通过的背书签名数据，则指示相应背书设备(可以是原先的背书设备，也可以是新指定一个背书设备)重新进行相应的背书签名操作。对背书签名数据进行验证的方式可参考后续描述。

[0095] 在一实施例中，管理设备可以将生成的交易区块添加到其存储的区块链上，以进行存证。在另一实施例中，管理设备可以根据客户端的交易请求以及该交易区块生成存证区块，并将生成的存证区块添加到其存储的区块链上，以进行存证。

[0096] S209、管理设备将交易区块广播给区块链网络中的节点设备。

[0097] S210、区块链网络中的节点设备在交易区块中的数据验证通过且根据交易区块中的数据检测到满足背书策略时，根据交易数据执行交易。

[0098] 本申请实施例中，区块链网络中的节点设备在接收到管理设备广播的交易区块之后，从该交易区块中提取交易数据以及提取各个背书签名数据，并对交易数据和背书签名数据进行验证。对交易数据进行验证包括验证字段的正确性以及交易的合法性。

[0099] 对签名数据进行验证的方式可以为：根据背书策略的指示从区块链网络中包括的多个节点设备中，确定针对交易数据所对应交易需要承担背书任务的各个目标节点设备。获取各个目标节点设备的解签密钥。在一实施例中，区块链网络中的各个节点设备均存储背书策略指示的可能用于承担背书任务的所有节点设备的解签密钥，此时则可以直接从本地获取各个目标节点设备的解签密钥。在另一实施例中，背书策略指示的可能用于承担背书任务的所有节点设备的解签密钥，或者区块链网络中所有节点设备的解签密钥可以存储在云端数据库中，此时则需要从云端数据库获取各个目标节点设备的解签密钥。解签密钥和签名密钥构成密钥对，签名密钥可以是密钥对中的私钥，解签密钥可以是密钥对中的公钥；密钥对可以是采用RSA加密算法计算得出的。进一步的，利用各个目标节点设备的解签密钥分别对各个背书签名数据进行解签，并基于解签成功后的解签数据对各个背书签名数据进行验证。

[0100] 若利用各个目标节点设备的解签密钥能够对各个背书签名数据成功解签，且任意一个目标节点设备的解签密钥与至少一个背书签名数据所使用的签名密钥相匹配，且解签结果指示全部表决结果或者大多数(如超过2/3)的表决结果同意执行交易数据所对应的交易，则确定满足背书策略。

[0101] 当交易区块中的数据验证通过且根据交易区块中的数据检测到满足背书策略时，区块链网络中的节点设备则根据交易数据执行交易。在执行交易之后，可以将得到交易结果计入账本中(或者说根据交易结果生成区块，并将区块上链)。在一实施例中，区块链网络中的节点设备也可以将接收到的交易区块添加到其存储的区块链上，以进行存证。

[0102] 需要说明的是，目标背书设备在得到背书签名数据时，可以利用匹配节点设备的签名密钥对待签名数据(如交易请求对应的表决结果)和交易数据进行背书签名，得到背书签名数据。目标背书设备在将背书签名数据发送给管理设备时，可以一并发送待签名数据。管理设备生成交易区块时，可以根据背书签名数据、交易数据和待签名数据生成交易区块。在生成背书签名数据和交易区块的过程中添加的上述数据，可作用于后续的数据验证。另外，如果是由管理网络中的管理设备托管区块链网络中至少部分节点设备的签名密钥，则管理设备在向目标背书设备发送交易请求时，可以一并发送目标背书设备对应的匹配节点设备的签名密钥，以使得目标背书设备执行相应的背书任务。

[0103] 本申请实施例中，管理设备和背书设备采用的是可信计算，利用管理网络中的背书设备取代区块链网络中的节点设备来提供数据验证和背书签名等服务，即利用背书设备完成共识操作，利用管理网络中的管理设备取代区块链网络中的节点设备来提供区块生成等服务，这样可以由管理网络集中高效的完成交易共识和区块生成，无需区块链网络中的节点参与交易的共识以及区块的生成，相对目前的需要区块链网络中绝大多数节点参与共识的方式，本方案可以有效节省共识所需的时间，从而提高交易流程的处理效率，达到提高整个网络的交易性能的效果。

[0104] 本申请实施例提供的数据处理方法是一种区块链跨域节点治理方案。目前，很多服务商都提供了区块链的PaaS(Platform as a Service，平台即服务)平台服务或跟区块链相关的各种解决方案，部署形式大都是将同一个区块链网络中的所有节点部署在一起，这样可以很大程度上提升区块链网络的交易性能。但为了体现真正的去中心化，区块链节点跨域分布式部署，或者部署到不同的客户环境，在未来将会是一种常态，节点间通过公网通讯，整个网络的交易性能将面对巨大的挑战。

[0105] 目前针对区块链跨域节点的治理还没有一个统一的方案，常见的是在区块链节点中划分出一部分节点作为共识节点，由这些共识节点提供共识服务和打包区块。但这只能在一定程度上提升交易性能，在交易并发量较高的时候，也存在性能瓶颈，因为交易需要收集节点签名，同时通用性较差，无法在大多数区块链引擎中使用。

[0106] 区块链的交易流程对交易的性能有很大的影响，一般情况下，每笔交易都需要通过共识才能被各个节点执行。公链中提供了很多中共识算法，如PoW、PoS等。一般情况下，公链中所有节点都是共识节点，均需要参与到共识过程中，所以交易性能非常低效。而诸如企业间一般使用联盟链，联盟链一般会将共识服务抽离出来，从而在一定程度上提升交易性能。本申请实施例提供的区块链跨域节点治理方案主要针对联盟链。

[0107] 请参见图4，示出了Fabric区块链的交易流程。其中，Orderer节点用于提供区块打包服务。Pee节点用于执行交易，记录账本；可以是背书节点(Endorser)或提交节点(Committer)。提供证书服务的可以是CA(证书颁发机构，Certificate Authority)，可针对客户端生成相应的秘钥。交易流程主要包括如下步骤：

[0108] 客户端向背书节点发送交易提议(或者说交易请求)，背书节点接收到提议之后，校验提议签名，并检测是否满足channel(通道)ACL(访问控制列表)，包括检查客户端是否可以在当前channel进行操作，等等。如果提议签名校验通过且检测到满足channel ACL，则模拟执行交易并对结果(可以是根据交易模拟执行的结果所生成的表决结果)签名。背书节点向客户端返回结果签名。客户端接收背书节点返回的结果签名，并对结果签名进行校验；比对多个背书节点的回复结果，并检测是否收集了足够的结果签名。客户端如果收集了足够的结果签名，且大多数背书节点的回复结果表示同意执行交易，则向Orderer节点发送交易数据，可以是将交易数据发送给背书节点，由背书节点转发给Orderer节点。Orderer节点对交易进行排序，构造交易区块，并将交易区块发送给提交节点。提交节点针对交易区块检查交易结构和签名，检查交易是否满足背书策略；如果交易结构和签名检查通过，且检查到交易满足背书策略，则执行交易区块中的合法交易，并更新账本状态。提交节点在处理交易区块的过程中，可以向背书节点同步关于交易区块的处理数据。

[0109] 上述交易流程中，客户端所执行的步骤具体可以是客户端配置的APP(应用程序)或者SDK(软件开发工具包)执行的。从Fabric区块链的交易流程中可以看出，从客户端发送交易提议到最后Peer节点执行交易，中间存在多次签名验签的操作，而这也是每笔交易最耗时的地方。其中，背书签名就是一个共识过程，只有收集到足够多的背书签名，交易才能正常执行。如果背书节点(Endorser)分布式跨域部署，节点间通过公网通讯，针对每笔交易收集背书签名时，公网的网络稳定性，带宽等都会影响整体交易的性能。

[0110] 请参见图5，示出了本申请实施例提供的区块链跨域节点治理方案的一种架构。本申请实施提供的区块链跨域节点治理方案，结合可信计算，规划出一块可信计算区域(相当

于前文所述的管理网络)，将区块链网络中的各个节点的私钥(或者说签名密钥)托管到可信计算区域，在可信计算区域中完成交易的共识签名(即背书签名)操作，然后在可信计算区域中打包出块，分发给区块链网络中的各个节点，节点收到区块后，只需验证区块并执行区块中的合法交易即可。可信计算保证了节点私钥的安全性与数据的可靠性，在可信计算区域，有与节点对应的服务(如图5所示的P1-P4)，托管对应节点的私钥，并提供签名服务。如图5所示，P1-P4分别拖管Peer1-Peer4的私钥，并提供相应的背书签名服务。图5中的P1-P4相当于前文所述的背书设备，可以是加密机。这样，交易的背书签名就可以在可信计算区域集中完成，从而减少网络中请求的分发，加快交易流程的处理速率。

[0111] 请参见图6，示出了本申请实施例提供的区块链跨域节点治理方案的另一种架构。本申请实施提供的区块链跨域节点治理方案的具体交易流程如下：首先客户端通过CA注册证书(即获取到相应密钥)后，向可信计算区域发送交易请求。可信计算区域收到交易请求后，校验交易请求中携带的交易签名；在签名校验通过后，按照背书策略的指示使用托管的相应节点的私钥对交易背书签名；在收集到足够多的背书签名后，打包交易，生成交易区块，并将交易区块分发给Peer节点。Peer节点收到交易区块后，检查交易结构和背书签名，以及检查交易是否满足背书策略；在交易结构和背书签名检查通过且交易满足背书策略时，执行区块中的合法交易，并更新账本状态。需要说明的是，上述交易流程中的各步骤的具体实现方式可参考前文实施例中的描述，另外，上述交易流程仅指出了一些主要步骤，针对不同的区块链引擎，在交易流程上会有一些区别，但主要思想都是将共识签名(即背书签名)操作集中处理，由可信计算区域托管节点的私钥，并完成交易共识。

[0112] 本申请实施例，结合可信计算，将区块链网络中的各个节点的签名密钥托管到可信计算区域，由可信计算区域提供数据验证和背书签名服务，以及提供区块生成服务，而区块链网络中的各个节点只负责记录账本，这种模式在保证信息安全可靠的同时，可以提高背书签名(即共识)效率，从而加快交易的处理流程，极大提高整个网络的交易性能，并且通用性较好，可以在所有区块链引擎中复用。

[0113] 请参阅图7，为本申请实施例提供的一种基于区块链网络的数据处理装置的结构示意图。所述区块链网络包含于数据处理网络中，所述区块链网络包括多个节点设备，所述数据处理网络还包括管理网络，所述管理网络包括管理设备以及一个或者多个背书设备，所述数据处理网络的架构可参阅图1a或者图1b。所述装置包括：获取单元701、处理单元702和收发单元703。

[0114] 在一实施例中，本申请实施例中所描述的数据处理装置，对应于前文所述的目标背书设备，此时各单元所实现的功能如下：

[0115] 获取单元701，用于获取交易请求，所述交易请求携带交易数据和所述交易数据对应的参考签名数据；

[0116] 处理单元702，用于对所述交易数据和所述参考签名数据进行验证；

[0117] 所述处理单元，还用于在所述交易数据和所述参考签名数据验证通过时，从根据背书策略的指示从所述多个节点设备中确定的目标节点设备中确定匹配节点设备，并获取所述匹配节点设备的签名密钥；

[0118] 所述处理单元702，还用于根据所述交易数据确定待签名数据，并利用所述匹配节点设备的签名密钥对所述待签名数据进行背书签名，得到背书签名数据；

[0119] 收发单元703，用于将所述背书签名数据发送给所述管理设备，以使得所述管理设备根据所述背书签名数据和所述交易数据生成交易区块。

[0120] 在一实施方式中，所述管理网络中的背书设备存储有所述多个节点设备中至少部分节点设备的签名密钥。

[0121] 在一实施方式中，所述管理网络中的各个背书设备存储有所述多个节点设备中部分节点设备的签名密钥，且各个背书设备存储不同节点设备的签名密钥，所述获取单元701，具体用于：触发所述收发单元703接收所述管理设备发送的客户端的交易请求；其中，所述管理设备在接收到所述客户端发送的交易请求之后，根据所述背书策略的指示从所述多个节点设备中确定目标节点设备，并将所述交易请求发送给存储有所述目标节点设备的签名密钥的目标背书设备。

[0122] 在一实施方式中，所述管理网络中的各个背书设备均存储有所述多个节点设备中各个节点设备的签名密钥，所述获取单元701，具体用于：触发所述收发单元703接收所述管理设备发送的客户端的交易请求；其中，所述管理设备在接收到所述客户端发送的交易请求之后，根据各个背书设备的当前状态参数从所述一个或者多个背书设备中确定响应所述交易请求的目标背书设备，并将所述交易请求发送给所述目标背书设备。

[0123] 在一实施方式中，所述处理单元702根据所述交易数据确定待签名数据时，具体用于：根据所述交易数据模拟执行交易，得到模拟交易结果；根据所述模拟交易结果确定所述交易请求对应的表决结果，并将所述表决结果作为待签名数据。

[0124] 在一实施方式中，所述参考签名数据是利用秘钥对中的私钥对所述交易数据进行签名得到的，所述获取单元701，还用于获取所述秘钥对中的公钥；所述处理单元702，还用于：利用所述秘钥对中的公钥对所述参考签名数据进行解签，得到解签数据；若所述解签数据与所述交易数据相匹配，则检测所述交易数据是否具备执行性；若所述交易数据具备执行性，则确定所述交易数据和所述参考签名数据校验通过。

[0125] 可以理解的是，本申请实施例提供的数据处理装置的各功能单元的功能可根据上述方法实施例中目标节点设备所对应的方法具体实现，其具体实现过程可以参照上述方法实施例的相关描述，此处不再赘述。

[0126] 在另一实施例中，本申请实施例中所描述的数据处理装置，对应于前文所述的管理设备，此时各单元所实现的功能如下：

[0127] 获取单元701，用于获取交易请求，所述交易请求携带交易数据和所述交易数据对应的参考签名数据；

[0128] 处理单元702，用于从所述管理网络包括的一个或者多个背书设备中确定目标背书设备；

[0129] 收发单元703，用于将所述交易请求发送给所述目标背书设备，以使得所述目标背书设备根据所述交易数据和所述参考签名数据得到背书签名数据；

[0130] 所述收发单元703，还用于接收所述目标背书设备发送的所述背书签名数据；

[0131] 所述处理单元702，还用于根据所述背书签名数据和所述交易数据生成交易区块。

[0132] 在一实施方式中，所述管理网络中的背书设备存储有所述多个节点设备中至少部分节点设备的签名密钥。

[0133] 在一实施方式中，所述管理网络中的各个背书设备存储有所述多个节点设备中部

分节点设备的签名密钥,且各个背书设备存储不同节点设备的签名密钥,所述处理单元702具体用于:根据背书策略的指示从所述多个节点设备中确定目标节点设备;从所述管理网络包括的一个或者多个背书设备中确定存储有所述目标节点设备的签名密钥的背书设备,并将所述存储有所述目标节点设备的签名密钥的背书设备确定为目标背书设备。

[0134] 在一实施方式中,所述管理网络中的各个背书设备均存储有所述多个节点设备中各个节点设备的签名密钥,所述装置还包括获取单元701,用于获取所述管理网络中各个背书设备的当前状态参数;所述处理单元702具体用于:根据所述各个背书设备的当前状态参数从所述管理网络包括的一个或者多个背书设备中确定响应所述交易请求的背书设备,并将所述响应所述交易请求的背书设备确定为目标背书设备。

[0135] 在一实施方式中,所述处理单元702还用于:触发所述收发单元703将所述交易区块广播给所述区块链网络中的节点设备,以使得所述区块链网络中的节点设备在所述交易区块中的数据验证通过且根据所述交易区块中的数据检测到满足所述背书策略时,根据所述交易数据执行交易。

[0136] 可以理解的是,本申请实施例提供的数据处理装置的各功能单元的功能可根据上述方法实施例中管理设备所对应的方法具体实现,其具体实现过程可以参照上述方法实施例的相关描述,此处不再赘述。

[0137] 本申请实施例中,在数据处理网络中设置管理网络,由管理网络中的背书设备对交易请求中的数据进行验证,并在数据验证通过之后,按照背书策略的指示利用相应节点设备的签名密钥,对根据交易数据确定的待签名数据进行背书签名,得到背书签名数据。采用此方式,可以由管理网络集中高效的完成数据验证和背书签名操作,即完成共识操作,无需区块链网络中的节点参与交易的共识,这样可以有效节省共识所需的时间,提高交易流程的处理效率,从而提高整个网络的交易性能。

[0138] 请参阅图8,为本申请实施例提供的一种计算机设备的结构示意图。本申请实施例中所描述的计算机设备包括:处理器801、通信接口802及存储器803。其中,处理器801、通信接口802及存储器803可通过总线或其他方式连接,本申请实施例以通过总线连接为例。

[0139] 其中,处理器801(或称CPU(Central Processing Unit,中央处理器))是计算机设备的计算核心以及控制核心,其可以解析计算机设备内的各类指令以及处理计算机设备的各类数据,例如:CPU可以用于解析用户向计算机设备所发送的开关机指令,并控制计算机设备进行开关机操作;再如:CPU可以在计算机设备内部结构之间传输各类交互数据,等等。通信接口802可选的可以包括标准的有线接口、无线接口(如Wi-Fi、移动通信接口等),受处理器801的控制用于收发数据。存储器803(Memory)是计算机设备中的记忆设备,用于存放程序和数据。可以理解的是,此处的存储器803既可以包括计算机设备的内置存储器,当然也可以包括计算机设备所支持的扩展存储器。存储器803提供存储空间,该存储空间存储了计算机设备的操作系统,可包括但不限于:Android系统、iOS系统、Windows Phone系统等等,本申请对此并不作限定。

[0140] 在本申请实施例中,本申请实施例中所描述的计算机设备,对应于前文所述的目标背书设备或者管理设备,是基于区块链网络实现的,所述区块链网络包含于数据处理网络中,所述区块链网络包括多个节点设备,所述数据处理网络还包括管理网络,所述管理网络包括管理设备以及一个或者多个背书设备,所述数据处理网络的架构可参阅图1a或者图

1b。

[0141] 在一实施例中，本申请实施例中所描述的计算机设备，对应于前文所述的目标背书设备，此时处理器801通过运行存储器803中的可执行程序代码，执行如下操作：

[0142] 获取交易请求，所述交易请求携带交易数据和所述交易数据对应的参考签名数据；对所述交易数据和所述参考签名数据进行验证；在所述交易数据和所述参考签名数据验证通过时，从根据背书策略的指示从所述多个节点设备中确定的目标节点设备中确定匹配节点设备，并获取所述匹配节点设备的签名密钥；根据所述交易数据确定待签名数据，并利用所述匹配节点设备的签名密钥对所述待签名数据进行背书签名，得到背书签名数据；通过通信接口802将所述背书签名数据发送给所述管理设备，以使得所述管理设备根据所述背书签名数据和所述交易数据生成交易区块。

[0143] 在一实施方式中，所述管理网络中的背书设备存储有所述多个节点设备中至少部分节点设备的签名密钥。

[0144] 在一实施方式中，所述管理网络中的各个背书设备存储有所述多个节点设备中部分节点设备的签名密钥，且各个背书设备存储不同节点设备的签名密钥，所述处理器801获取交易请求时，具体用于：通过通信接口802接收所述管理设备发送的客户端的交易请求；其中，所述管理设备在接收到所述客户端发送的交易请求之后，根据所述背书策略的指示从所述多个节点设备中确定目标节点设备，并将所述交易请求发送给存储有所述目标节点设备的签名密钥的目标背书设备。

[0145] 在一实施方式中，所述管理网络中的各个背书设备均存储有所述多个节点设备中各个节点设备的签名密钥，所述处理器801获取交易请求时，具体用于：通过通信接口802接收所述管理设备发送的客户端的交易请求；其中，所述管理设备在接收到所述客户端发送的交易请求之后，根据各个背书设备的当前状态参数从所述一个或者多个背书设备中确定响应所述交易请求的目标背书设备，并将所述交易请求发送给所述目标背书设备。

[0146] 在一实施方式中，所述处理器801根据所述交易数据确定待签名数据时，具体用于：根据所述交易数据模拟执行交易，得到模拟交易结果；根据所述模拟交易结果确定所述交易请求对应的表决结果，并将所述表决结果作为待签名数据。

[0147] 在一实施方式中，所述参考签名数据是利用秘钥对中的私钥对所述交易数据进行签名得到的，所述处理器801还用于：获取所述秘钥对中的公钥，并利用所述秘钥对中的公钥对所述参考签名数据进行解签，得到解签数据；若所述解签数据与所述交易数据相匹配，则检测所述交易数据是否具备执行性；若所述交易数据具备执行性，则确定所述交易数据和所述参考签名数据校验通过。

[0148] 具体实现中，本申请实施例中所描述的处理器801、通信接口802及存储器803可执行本申请实施例提供的一种基于区块链网络的数据处理方法中所描述的目标背书设备的实现方式，也可执行本申请实施例提供的一种基于区块链网络的数据处理装置中所描述的对应于目标背书设备的实现方式，在此不再赘述。

[0149] 在另一实施例中，本申请实施例中所描述的计算机设备，对应于前文所述的管理设备，此时处理器801通过运行存储器803中的可执行程序代码，执行如下操作：

[0150] 获取交易请求，所述交易请求携带交易数据和所述交易数据对应的参考签名数据；从所述管理网络包括的一个或者多个背书设备中确定目标背书设备；通过通信接口802

将所述交易请求发送给所述目标背书设备，以使得所述目标背书设备根据所述交易数据和所述参考签名数据得到背书签名数据；通过通信接口802接收所述目标背书设备发送的所述背书签名数据，并根据所述背书签名数据和所述交易数据生成交易区块。

[0151] 在一实施方式中，所述管理网络中的背书设备存储有所述多个节点设备中至少部分节点设备的签名密钥。

[0152] 在一实施方式中，所述管理网络中的各个背书设备存储有所述多个节点设备中部分节点设备的签名密钥，且各个背书设备存储不同节点设备的签名密钥，所述处理器801从所述管理网络包括的一个或者多个背书设备中确定目标背书设备时，具体用于：根据背书策略的指示从所述多个节点设备中确定目标节点设备；从所述管理网络包括的一个或者多个背书设备中确定存储有所述目标节点设备的签名密钥的背书设备，并将所述存储有所述目标节点设备的签名密钥的背书设备确定为目标背书设备。

[0153] 在一实施方式中，所述管理网络中的各个背书设备均存储有所述多个节点设备中各个节点设备的签名密钥，所述处理器801从所述管理网络包括的一个或者多个背书设备中确定目标背书设备时，具体用于：获取所述管理网络中各个背书设备的当前状态参数；根据所述各个背书设备的当前状态参数从所述管理网络包括的一个或者多个背书设备中确定响应所述交易请求的背书设备，并将所述响应所述交易请求的背书设备确定为目标背书设备。

[0154] 在一实施方式中，所述处理器801还用于：通过通信接口802将所述交易区块广播给所述区块链网络中的节点设备，以使得所述区块链网络中的节点设备在所述交易区块中的数据验证通过且根据所述交易区块中的数据检测到满足背书策略时，根据所述交易数据执行交易。

[0155] 具体实现中，本申请实施例中所描述的处理器801、通信接口802及存储器803可执行本申请实施例提供的一种基于区块链网络的数据处理方法中所描述的管理舍内的实现方式，也可执行本申请实施例提供的一种基于区块链网络的数据处理装置中所描述的对应于管理设备的实现方式，在此不再赘述。

[0156] 本申请实施例中，在数据处理网络中设置管理网络，由管理网络中的背书设备对交易请求中的数据进行验证，并在数据验证通过之后，按照背书策略的指示利用相应节点设备的签名密钥，对根据交易数据确定的待签名数据进行背书签名，得到背书签名数据。采用此方式，可以由管理网络集中高效的完成数据验证和背书签名操作，即完成共识操作，无需区块链网络中的节点参与交易的共识，这样可以有效节省共识所需的时间，提高交易流程的处理效率，从而提高整个网络的交易性能。

[0157] 本申请实施例还提供了一种计算机可读存储介质，所述计算机可读存储介质中存储有计算机程序，当其在计算机上运行时，使得计算机执行如本申请实施例所述的基于区块链网络的数据处理方法。其具体实现方式可参考前文描述，此处不再赘述。

[0158] 本申请实施例还提供了一种计算机程序产品或计算机程序，所述计算机程序产品或计算机程序包括计算机指令，所述计算机指令存储在计算机可读存储介质中。计算机设备的处理器从所述计算机可读存储介质读取所述计算机指令，处理器执行所述计算机指令，使得所述计算机设备执行如本申请实施例所述的基于区块链网络的数据处理方法。其具体实现方式可参考前文描述，此处不再赘述。

[0159] 需要说明的是，对于前述的各个方法实施例，为了简单描述，故将其都表述为一系列的动作组合，但是本领域技术人员应该知悉，本申请并不受所描述的动作顺序的限制，因为依据本申请，某一些步骤可以采用其他顺序或者同时进行。其次，本领域技术人员也应该知悉，说明书中所描述的实施例均属于优选实施例，所涉及的动作和模块并不一定是本申请所必须的。

[0160] 本领域普通技术人员可以理解上述实施例的各种方法中的全部或部分步骤是可以通过程序来指令相关的硬件来完成，该程序可以存储于一计算机可读存储介质中，存储介质可以包括：闪存盘、只读存储器(Read-Only Memory ，ROM)、随机存取器(Random Access Memory，RAM)、磁盘或光盘等。

[0161] 以上所揭露的仅为本申请部分实施例而已，当然不能以此来限定本申请之权利范围，因此依本申请权利要求所作的等同变化，仍属本申请所涵盖的范围。

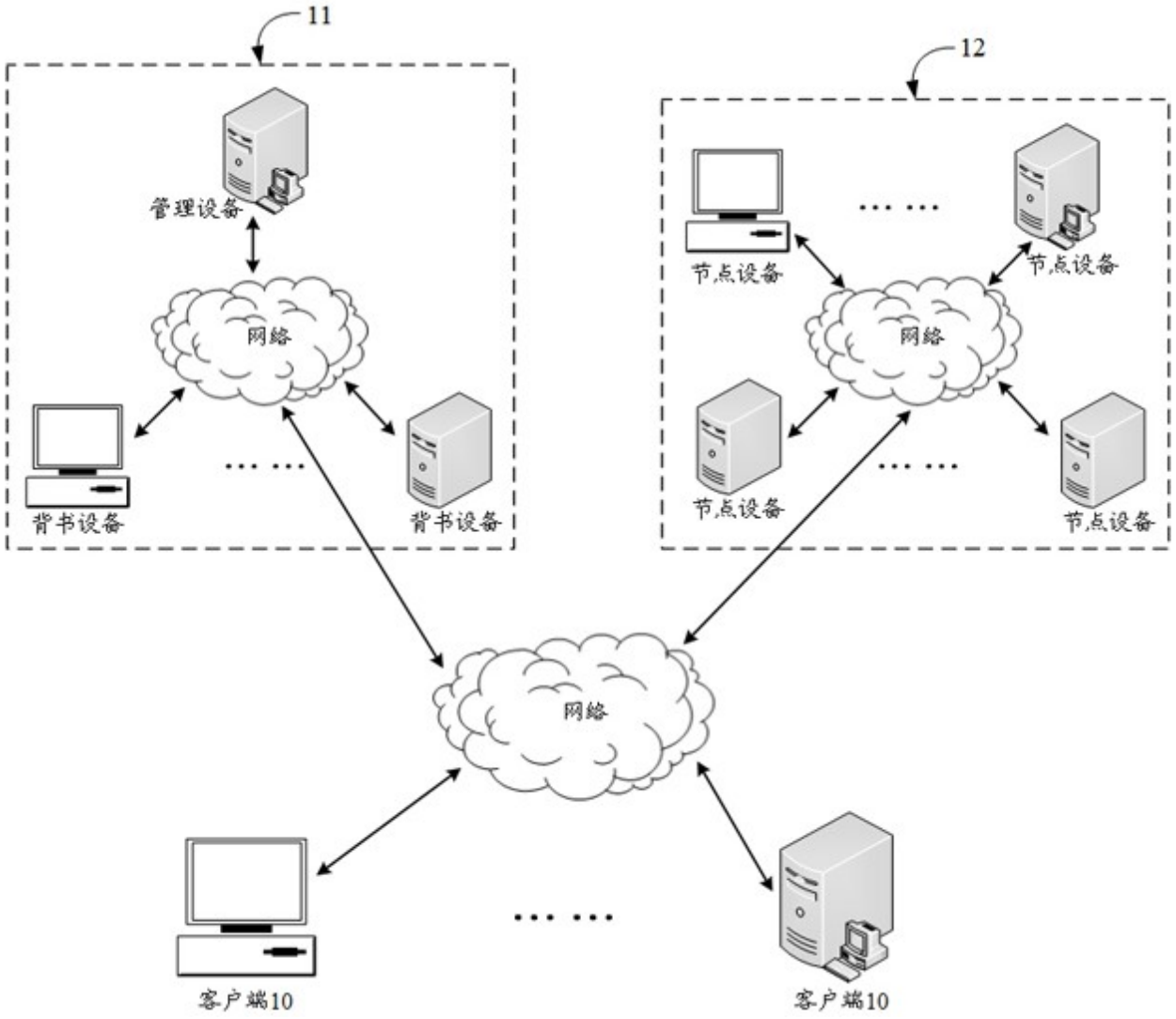


图 1a

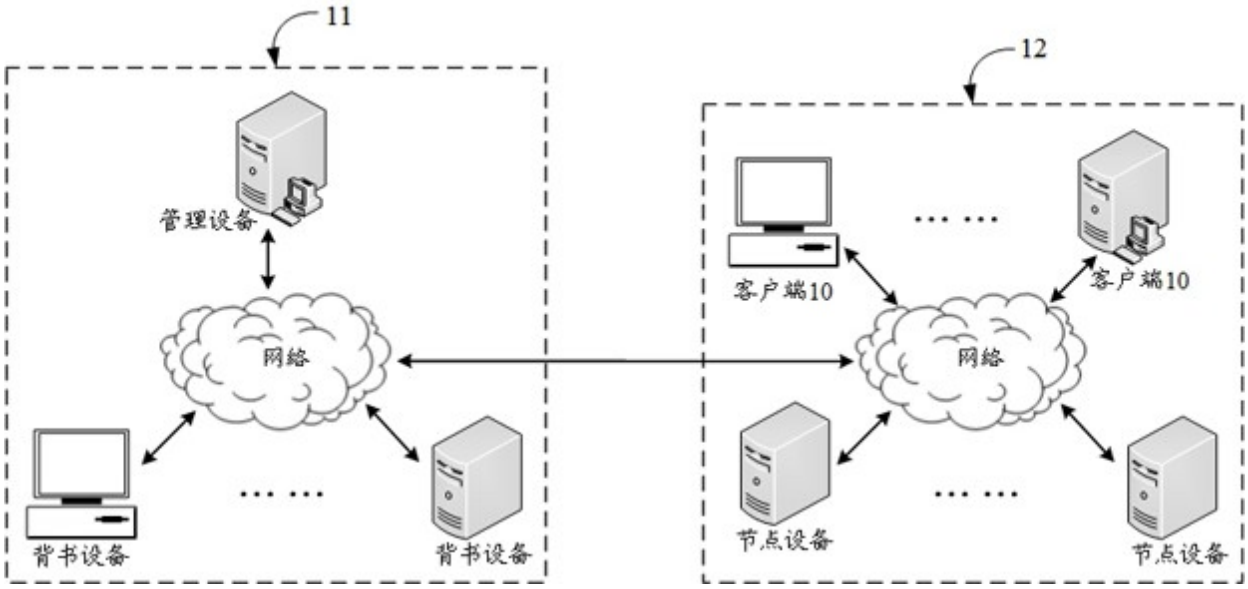


图 1b

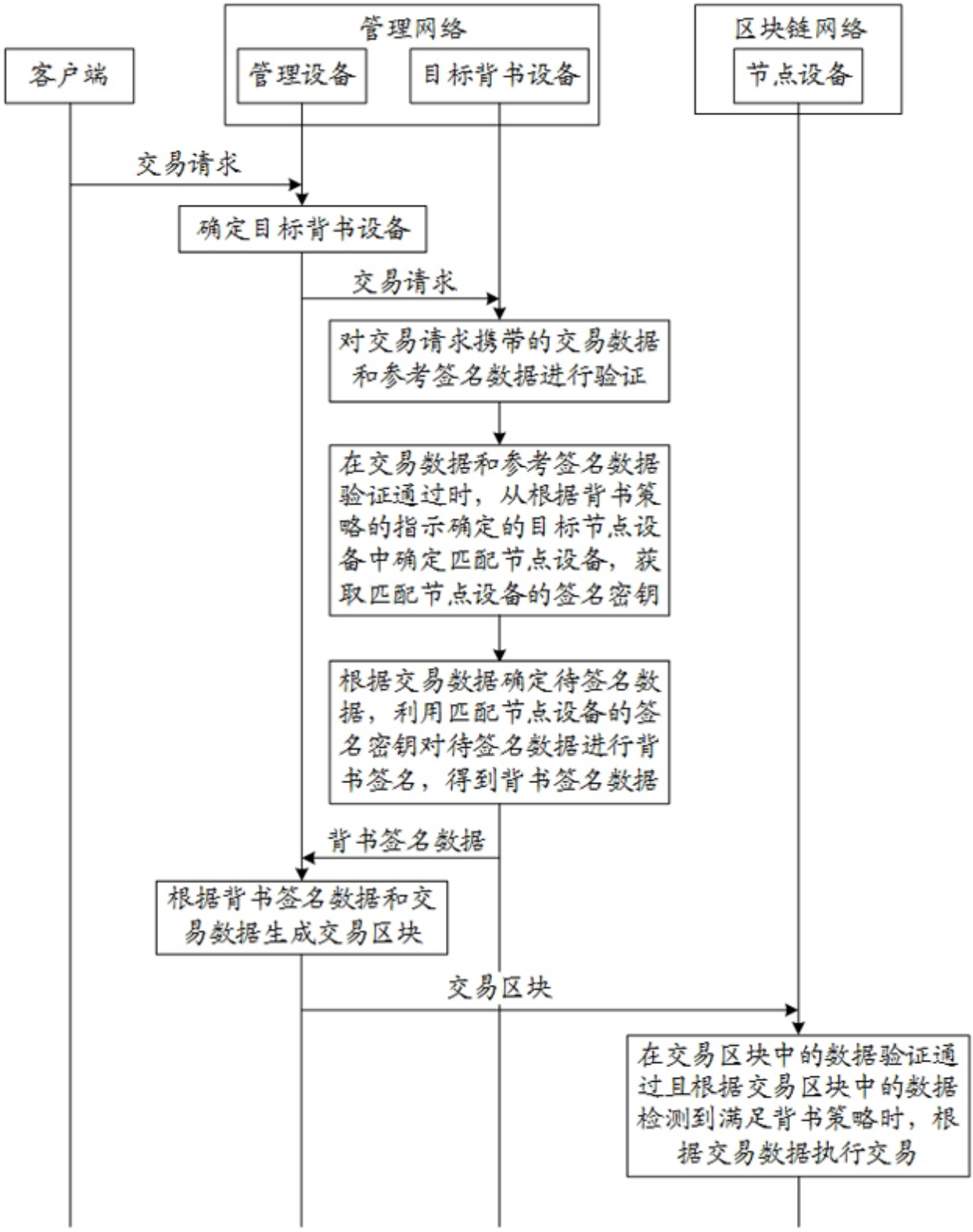

管理网络
客户端
管理设备
目标背书设备
区块链网络
节点设备
交易请求
确定目标背书设备
交易请求
对交易请求携带的交易数据和参考签名数据进行验证
在交易数据和参考签名数据验证通过时，从根据背书策略的指示确定的目标节点设备中确定匹配节点设备，获取匹配节点设备的签名密钥
根据交易数据确定待签名数据，利用匹配节点设备的签名密钥对待签名数据进行背书签名，得到背书签名数据
背书签名数据
根据背书签名数据和交易数据生成交易区块
交易区块
在交易区块中的数据验证通过且根据交易区块中的数据检测到满足背书策略时，根据交易数据执行交易

图2

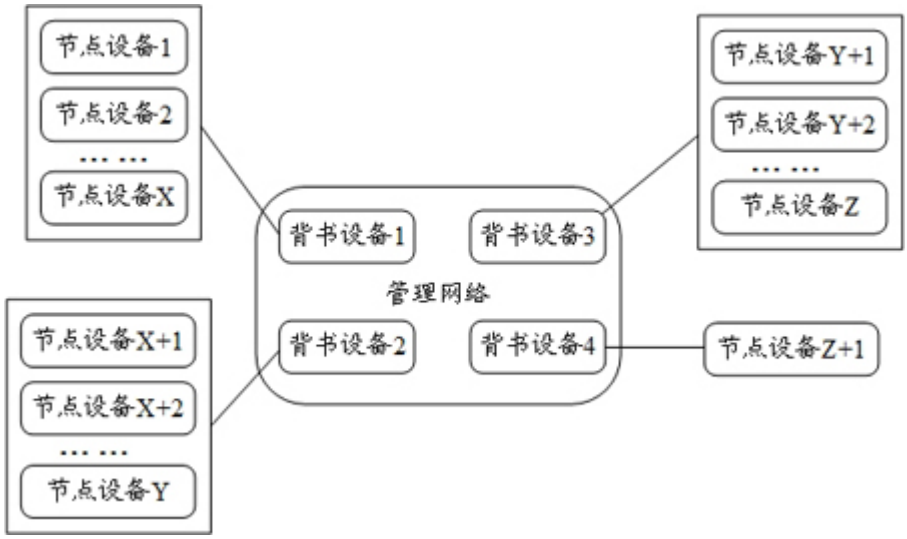

节点设备1
节点设备2
… …
节点设备X
节点设备Y+1
节点设备Y+2
… …
节点设备Z
背书设备1
背书设备3
管理网络
背书设备2
背书设备4
节点设备Z+1
节点设备X+1
节点设备X+2
… …
节点设备Y

图 3

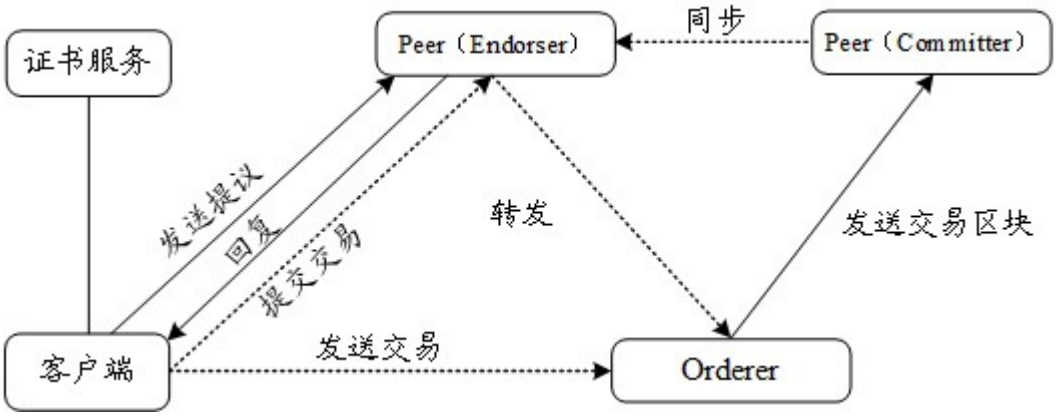

证书服务
Peer（Endorser）
同步
Peer（Committer）
发送提议
回复
提交交易
转发
发送交易区块
客户端
发送交易
Orderer

图 4

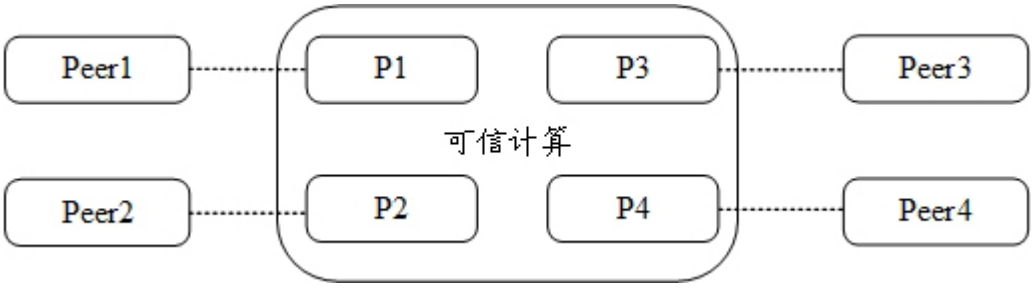

Peer1
P1
P3
Peer3
可信计算
Peer2
P2
P4
Peer4

图 5

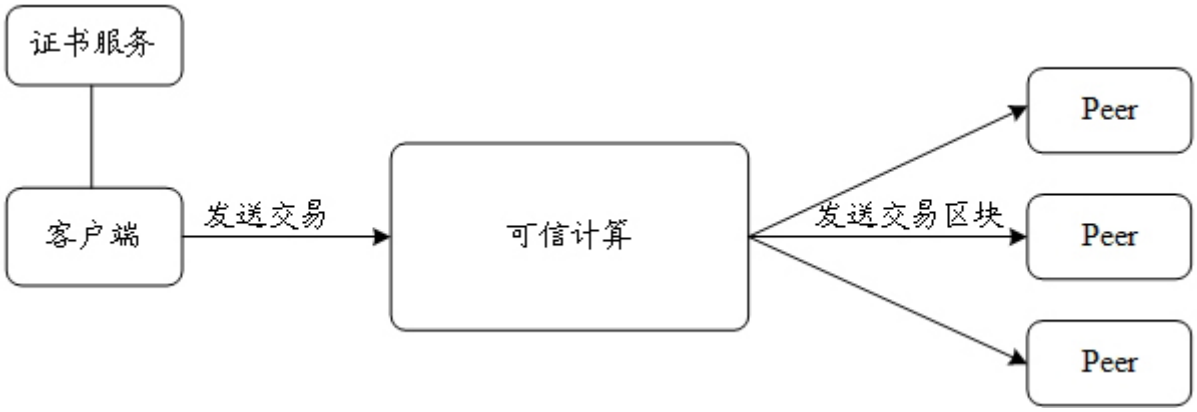

证书服务
客户端
发送交易
可信计算
发送交易区块
Peer
Peer
Peer

图 6

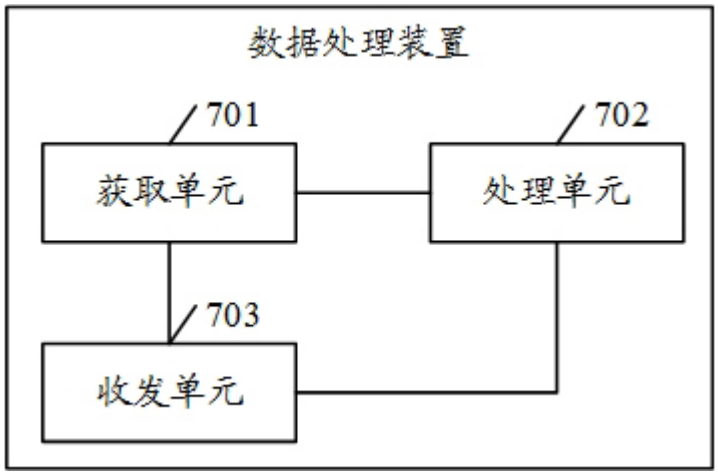

数据处理装置
701
获取单元
702
处理单元
703
收发单元

图 7

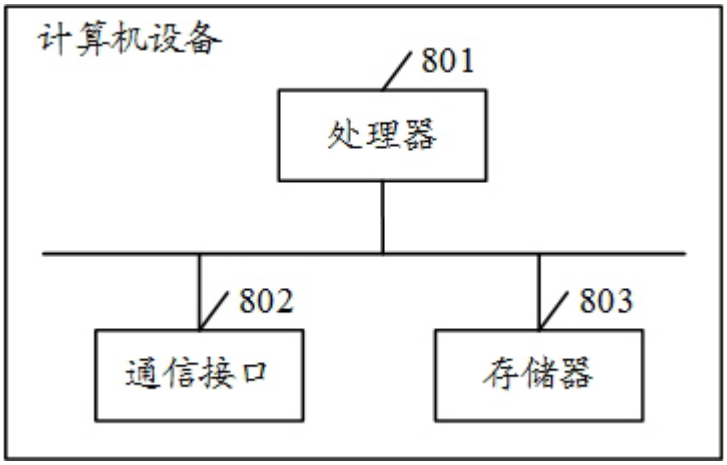

计算机设备
801
处理器
802
通信接口
803
存储器

图 8