(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 109345386 B
(45)授权公告日 2020.04.14

(21)申请号 201811015599.0

(22)申请日 2018.08.31

(65)同一申请的已公布的文献号
申请公布号 CN 109345386 A

(43)申请公布日 2019.02.15

(73)专利权人 阿里巴巴集团控股有限公司
地址 英属开曼群岛大开曼资本大厦一座四层847号邮箱

(72)发明人 邓福喜

(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 林祥

(51)Int.Cl.
G06Q 40/04(2012.01)

(56)对比文件
CN 106603198 A,2017.04.26,说明书第16-23段.
CN 105741095 A,2016.07.06,说明书第5-20段.
US 2017344987 A1,2017.11.30,全文.
黄秋波等.一种改进PBFT算法作为以太坊共识机制的研究与实现.《计算机应用与软件》.2017,第34卷(第10期),第1-5章节.

审查员 于雷

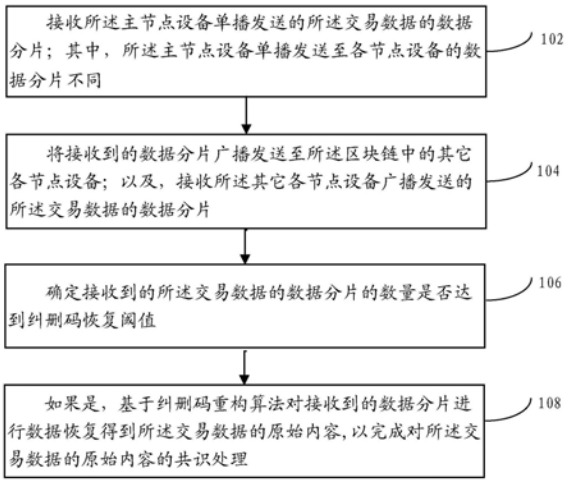
权利要求书4页 说明书17页 附图3页

(54)发明名称

基于区块链的交易共识处理方法及装置、电子设备

(57)摘要

一种基于区块链的交易共识处理方法,所述区块链中的节点设备至少包括一主节点设备以及若干从节点设备;其中,所述主节点设备基于纠删码算法将提议的交易数据分割为指定数量的数据分片,包括:接收所述主节点设备单播发送的所述交易数据的数据分片;其中,所述主节点设备单播发送至各节点设备的数据分片不同;将接收到的数据分片广播发送至所述区块链中的其它各节点设备;以及,接收所述其它各节点设备广播发送的所述交易数据的数据分片;确定接收到的所述交易数据的数据分片的数量是否达到纠删码恢复阈值;如果是,基于纠删码重构算法对接收到的数据分片进行数据恢复得到所述交易数据的原始内容,以完成对所述交易数据的原始内容的共识处理。



CN 109345386 B

1.一种基于区块链的交易共识处理方法,所述区块链中的节点设备至少包括一主节点设备以及若干从节点设备;其中,所述主节点设备基于纠删码算法将提议的交易数据分割为指定数量的数据分片,所述方法包括:

接收所述主节点设备单播发送的所述交易数据的数据分片;其中,所述主节点设备单播发送至各节点设备的数据分片不同;

将接收到的数据分片广播发送至所述区块链中的其它各节点设备;以及,接收所述其它各节点设备广播发送的所述交易数据的数据分片;

确定接收到的所述交易数据的数据分片的数量是否达到纠删码恢复阈值;

如果是,基于纠删码重构算法对接收到的数据分片进行数据恢复得到所述交易数据的原始内容,以完成对所述交易数据的原始内容的共识处理。

2.根据权利要求1所述的方法,所述方法还包括:

确定本节点设备是否被选举为所述主节点设备;

如果是,基于所述纠删码算法将提议的交易数据分割为指定数量的数据分片;以及,

将所述指定数量的数据分片分别单播发送至其它各节点设备。

3.根据权利要求1所述的方法,所述区块链搭载的共识算法为pbft算法;

所述接收所述主节点设备单播发送的所述交易数据的数据分片,包括:

接收所述主节点设备单播发送的Pre-Prepare消息;其中,所述Pre-Prepare消息中包括所述交易数据的数据分片;

获取并保存所述Pre-Prepare消息中的数据分片。

4.根据权利要求3所述的方法,所述将接收到的数据分片广播发送至所述区块链中的其它各节点设备,包括:

向所述区块链中的其它各节点设备广播发送Prepare消息;其中,所述Prepare消息包括接收到的所述数据分片,以使所述其它各节点设备在接收到所述Prepare消息时,获取并保存所述Prepare消息中的数据分片。

5.根据权利要求1或2所述的方法,所述基于所述纠删码算法将提议的交易数据分割为指定数量的数据分片,包括:

基于预设的压缩算法对提议的所述交易数据进行压缩处理;

基于所述纠删码算法将压缩处理后的所述交易数据分割为指定数量的数据分片;

所述基于纠删码重构算法对接收到的数据分片进行数据恢复得到所述交易数据的原始内容,包括:

基于纠删码重构算法对接收到的数据分片进行数据恢复得到压缩后的所述交易数据;

基于与所述压缩算法对应的解压缩算法,对恢复出的所述交易数据进行解压缩处理,以得到所述交易数据的原始内容。

6.根据权利要求1或2所述的方法,基于所述纠删码算法将提议的交易数据分割为指定数量的数据分片,包括:

基于预设的加密算法以及加密密钥对提议的交易数据进行加密处理;

基于所述纠删码算法将加密处理后的所述交易数据分割为指定数量的数据分片;

所述基于纠删码重构算法对接收到的数据分片进行数据恢复得到所述交易数据的原始内容,包括:

基于纠删码重构算法对接收到的数据分片进行数据恢复得到加密后的所述交易数据；

基于与所述加密算法对应的解密算法，以及与所述加密密钥对应的解密密钥，对恢复出的所述交易数据进行解密处理，以得到所述交易数据的原始内容。

7.根据权利要求6所述的方法，所述加密算法为门限加密算法；所述解密算法为与门限加密算法对应的门限解密算法；所述解密密钥被分割为指定数量的子密钥；其中，各子密钥由各节点设备分别持有；

基于与所述加密算法对应的解密算法，以及与所述加密密钥对应的解密密钥，对恢复出的所述交易数据进行解密处理，包括：

收集所述其它各节点设备持有的子密钥；

确定收集到的子密钥的数量是否达到预设的解密门限阈值；

如果是，基于收集到的子密钥重构所述解密密钥，并基于与所述门限加密算法对应的门限解密算法，以及所述解密密钥，对恢复出的所述交易数据进行解密处理。

8.根据权利要求1所述的方法，所述主节点提议的交易数据，为所述主节点设备当前共识周期内由各用户客户端广播发送的待共识交易构建的交易列表；所述指定数量为所述区块链中的节点设备的总数量。

9.根据权利要求1所述的方法，所述区块链为联盟链。

10.一种基于区块链的交易共识处理装置，所述区块链中的节点设备至少包括一主节点设备以及若干从节点设备；其中，所述主节点设备基于纠删码算法将提议的交易数据分割为指定数量的数据分片，所述装置包括：

接收模块，接收所述主节点设备单播发送的所述交易数据的数据分片；其中，所述主节点设备单播发送至各节点设备的数据分片不同；

发送模块，将接收到的数据分片广播发送至所述区块链中的其它各节点设备；以及，接收所述其它各节点设备广播发送的所述交易数据的数据分片；

确定模块，确定接收到的所述交易数据的数据分片的数量是否达到纠删码恢复阈值；

恢复模块，如果是，基于纠删码重构算法对接收到的数据分片进行数据恢复得到所述交易数据的原始内容，以完成对所述交易数据的原始内容的共识处理。

11.根据权利要求10所述的装置，所述装置还包括：

分割模块，确定本节点设备是否被选举为所述主节点设备；如果是，基于所述纠删码算法将提议的交易数据分割为指定数量的数据分片；

所述发送模块进一步：

将所述指定数量的数据分片分别单播发送至其它各节点设备。

12.根据权利要求10所述的装置，所述区块链搭载的共识算法为pbft算法；

所述接收模块：

接收所述主节点设备单播发送的Pre-Prepare消息；其中，所述Pre-Prepare消息中包括所述交易数据的数据分片；

获取并保存所述Pre-Prepare消息中的数据分片。

13.根据权利要求12所述的装置，所述发送模块：

向所述区块链中的其它各节点设备广播发送Prepare消息；其中，所述Prepare消息包括接收到的所述数据分片，以使所述其它各节点设备在接收到所述Prepare消息时，获取并

保存所述Prepare消息中的数据分片。

14.根据权利要求11所述的装置,所述分割模块:

基于预设的压缩算法对提议的所述交易数据进行压缩处理;

基于所述纠删码算法将压缩处理后的所述交易数据分割为指定数量的数据分片;

所述恢复模块:

基于纠删码重构算法对接收到的数据分片进行数据恢复得到压缩后的所述交易数据;

基于与所述压缩算法对应的解压缩算法,对恢复出的所述交易数据进行解压缩处理,以得到所述交易数据的原始内容。

15.根据权利要求11所述的装置,所述分割模块:

基于预设的加密算法以及加密密钥对提议的交易数据进行加密处理;

基于所述纠删码算法将加密处理后的所述交易数据分割为指定数量的数据分片;

所述恢复模块:

基于纠删码重构算法对接收到的数据分片进行数据恢复得到加密后的所述交易数据;

基于与所述加密算法对应的解密算法,以及与所述加密密钥对应的解密密钥,对恢复出的所述交易数据进行解密处理,以得到所述交易数据的原始内容。

16.根据权利要求15所述的装置,所述加密算法为门限加密算法;所述解密算法为与门限加密算法对应的门限解密算法;所述解密密钥被分割为指定数量的子密钥;其中,各子密钥由各节点设备分别持有;

所述恢复模块进一步:

收集所述其它各节点设备持有的子密钥;

确定收集到的子密钥的数量是否达到预设的解密门限阈值;

如果是,基于收集到的子密钥重构所述解密密钥,并基于与所述门限加密算法对应的门限解密算法,以及所述解密密钥,对恢复出的所述交易数据进行解密处理。

17.根据权利要求10所述的装置,所述主节点提议的交易数据,为所述主节点设备当前共识周期内由各用户客户端广播发送的待共识交易构建的交易列表;所述指定数量为所述区块链中的节点设备的总数量。

18.根据权利要求10所述的装置,所述区块链为联盟链。

19.一种电子设备,包括:

处理器;

用于存储机器可执行指令的存储器;

其中,通过读取并执行所述存储器存储的与基于区块链的交易共识处理的控制逻辑对应的机器可执行指令,所述处理器被促使:

接收主节点设备单播发送的所述交易数据的数据分片;其中,所述区块链中的节点设备至少包括一主节点设备以及若干从节点设备;所述主节点设备基于纠删码算法将提议的交易数据分割为指定数量的数据分片所述主节点设备单播发送至各节点设备的数据分片不同;

将接收到的数据分片广播发送至所述区块链中的其它各节点设备;以及,接收所述其它各节点设备广播发送的所述交易数据的数据分片;

确定接收到的所述交易数据的数据分片的数量是否达到纠删码恢复阈值;

如果是,基于纠删码重构算法对接收到的数据分片进行数据恢复得到所述交易数据的原始内容,以完成对所述交易数据的原始内容的共识处理。

基于区块链的交易共识处理方法及装置、电子设备

技术领域

[0001] 本说明书一个或多个实施例涉及区块链技术领域，尤其涉及一种基于区块链的交易共识处理方法及装置、电子设备。

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

发明内容

[0003] 本说明书提出一种基于区块链的交易共识处理方法，所述区块链中的节点设备至少包括一主节点设备以及若干从节点设备；其中，所述主节点设备基于纠删码算法将提议的交易数据分割为指定数量的数据分片，所述方法包括：

[0004] 接收所述主节点设备单播发送的所述交易数据的数据分片；其中，所述主节点设备单播发送至各节点设备的数据分片不同；

[0005] 将接收到的数据分片广播发送至所述区块链中的其它各节点设备；以及，接收所述其它各节点设备广播发送的所述交易数据的数据分片；

[0006] 确定接收到的所述交易数据的数据分片的数量是否达到纠删码恢复阈值；

[0007] 如果是，基于纠删码重构算法对接收到的数据分片进行数据恢复得到所述交易数据的原始内容，以完成对所述交易数据的原始内容的共识处理。

[0008] 可选的，所述方法还包括：

[0009] 确定本节点设备是否被选举为所述主节点设备；

[0010] 如果是，基于所述纠删码算法将提议的交易数据分割为指定数量的数据分片；以及，

[0011] 将所述指定数量的数据分片分别单播发送至其它各节点设备。

[0012] 可选的，所述区块链搭载的共识算法为pbft算法；

[0013] 所述接收所述主节点设备单播发送的所述交易数据的数据分片，包括：

[0014] 接收所述主节点设备单播发送的Pre-Prepare消息；其中，所述Pre-Prepare消息中包括所述交易数据的数据分片；

[0015] 获取并保存所述Pre-Prepare消息中的数据分片。

[0016] 可选的，所述将接收到的数据分片广播发送至所述区块链中的其它各节点设备，包括：

[0017] 向所述区块链中的其它各节点设备广播发送Prepare消息；其中，所述Prepare消息包括接收到的所述数据分片，以使所述其它各节点设备在接收到所述Prepare消息时，获取并保存所述Prepare消息中的数据分片。

[0018] 可选的，所述基于所述纠删码算法将提议的交易数据分割为指定数量的数据分片，包括：

[0019] 基于预设的压缩算法对提议的所述交易数据进行压缩处理；

[0020] 基于所述纠删码算法将压缩处理后的所述交易数据分割为指定数量的数据分片。

[0021] 所述基于纠删码重构算法对接收到的数据分片进行数据恢复得到所述交易数据的原始内容，包括：

[0022] 基于纠删码重构算法对接收到的数据分片进行数据恢复得到压缩后的所述交易数据；

[0023] 基于与所述压缩算法对应的解压缩算法，对恢复出的所述交易数据进行解压缩处理，以得到所述交易数据的原始内容。

[0024] 可选的，所述基于所述纠删码算法将提议的交易数据分割为指定数量的数据分片，包括：

[0025] 基于预设的加密算法以及加密密钥对提议的交易数据进行加密处理；

[0026] 基于所述纠删码算法将加密处理后的所述交易数据分割为指定数量的数据分片。

[0027] 所述基于纠删码重构算法对接收到的数据分片进行数据恢复得到所述交易数据的原始内容，包括：

[0028] 基于基于纠删码重构算法对接收到的数据分片进行数据恢复得到加密后的所述交易数据；

[0029] 基于与所述加密算法对应的解密算法，以及与所述加密密钥对应的解密密钥，对恢复出的所述交易数据进行解密处理，以得到所述交易数据的原始内容。

[0030] 可选的，所述加密算法为门限加密算法；所述解密算法为与门限加密算法对应的门限解密算法；所述解密密钥被分割为指定数量的子密钥；其中，各子密钥由各节点设备分别持有；

[0031] 所述基于与所述加密算法对应的解密算法，以及与所述加密密钥对应的解密密钥，对恢复出的所述交易数据进行解密处理，包括：

[0032] 收集所述其它各节点设备持有的子密钥；

[0033] 确定收集到的子密钥的数量是否达到预设的解密门限阈值；

[0034] 如果是，基于收集到的子密钥重构所述解密密钥，并基于与所述门限加密算法对应的门限解密算法，以及所述解密密钥，对恢复出的所述交易数据进行解密处理。

[0035] 可选的，所述主节点提议的交易数据，为所述主节点设备当前共识周期内由各用户客户端广播发送的待共识交易构建的交易列表；所述指定数量为所述区块链中的节点设备的总数量。

[0036] 可选的，所述区块链为联盟链。

[0037] 本说明书还提出一种基于区块链的交易共识处理装置，所述区块链中的节点设备至少包括一主节点设备以及若干从节点设备；其中，所述主节点设备基于纠删码算法将提议的交易数据分割为指定数量的数据分片，所述装置包括：

[0038] 接收模块，接收所述主节点设备单播发送的所述交易数据的数据分片；其中，所述主节点设备单播发送至各节点设备的数据分片不同；

[0039] 发送模块，将接收到的数据分片广播发送至所述区块链中的其它各节点设备；以

及,接收所述其它各节点设备广播发送的所述交易数据的数据分片;

[0040] 确定模块,确定接收到的所述交易数据的数据分片的数量是否达到纠删码恢复阈值;

[0041] 恢复模块,如果是,基于纠删码重构算法对接收到的数据分片进行数据恢复得到所述交易数据的原始内容,以完成对所述交易数据的原始内容的共识处理。

[0042] 可选的,所述装置还包括:

[0043] 分割模块,确定本节点设备是否被选举为所述主节点设备;如果是,基于所述纠删码算法将提议的交易数据分割为指定数量的数据分片;

[0044] 所述发送模块进一步:

[0045] 将所述指定数量的数据分片分别单播发送至其它各节点设备。

[0046] 可选的,所述区块链搭载的共识算法为pbft算法;

[0047] 所述接收模块:

[0048] 接收所述主节点设备单播发送的Pre-Prepare消息;其中,所述Pre-Prepare消息中包括所述交易数据的数据分片;

[0049] 获取并保存所述Pre-Prepare消息中的数据分片。

[0050] 可选的,所述发送模块:

[0051] 向所述区块链中的其它各节点设备广播发送Prepare消息;其中,所述Prepare消息包括接收到的所述数据分片,以使所述其它各节点设备在接收到所述Prepare消息时,获取并保存所述Prepare消息中的数据分片。

[0052] 可选的,所述分割模块:

[0053] 基于预设的压缩算法对提议的所述交易数据进行压缩处理;

[0054] 基于所述纠删码算法将压缩处理后的所述交易数据分割为指定数量的数据分片。

[0055] 所述恢复模块:

[0056] 基于纠删码重构算法对接收到的数据分片进行数据恢复得到压缩后的所述交易数据;

[0057] 基于与所述压缩算法对应的解压缩算法,对恢复出的所述交易数据进行解压缩处理,以得到所述交易数据的原始内容。

[0058] 可选的,所述分割模块:

[0059] 基于预设的加密算法以及加密密钥对提议的交易数据进行加密处理;

[0060] 基于所述纠删码算法将加密处理后的所述交易数据分割为指定数量的数据分片。

[0061] 所述恢复模块:

[0062] 基于基于纠删码重构算法对接收到的数据分片进行数据恢复得到加密后的所述交易数据;

[0063] 基于与所述加密算法对应的解密算法,以及与所述加密密钥对应的解密密钥,对恢复出的所述交易数据进行解密处理,以得到所述交易数据的原始内容。

[0064] 可选的,所述加密算法为门限加密算法;所述解密算法为与门限加密算法对应的门限解密算法;所述解密密钥被分割为指定数量的子密钥;其中,各子密钥由各节点设备分别持有;

[0065] 所述恢复模块进一步:

[0066] 收集所述其它各节点设备持有的子密钥；

[0067] 确定收集到的子密钥的数量是否达到预设的解密门限阈值；

[0068] 如果是，基于收集到的子密钥重构所述解密密钥，并基于与所述门限加密算法对应的门限解密算法，以及所述解密密钥，对恢复出的所述交易数据进行解密处理。

[0069] 可选的，所述主节点提议的交易数据，为所述主节点设备当前共识周期内由各用户客户端广播发送的待共识交易构建的交易列表；所述指定数量为所述区块链中的节点设备的总数量。

[0070] 可选的，所述区块链为联盟链。

[0071] 本说明书还提出一种电子设备，包括：

[0072] 处理器；

[0073] 用于存储机器可执行指令的存储器；

[0074] 其中，通过读取并执行所述存储器存储的与基于区块链的交易共识处理的控制逻辑对应的机器可执行指令，所述处理器被促使：

[0075] 接收所述主节点设备单播发送的所述交易数据的数据分片；其中，所述区块链中的节点设备至少包括一主节点设备以及若干从节点设备；所述主节点设备基于纠删码算法将提议的交易数据分割为指定数量的数据分片所述主节点设备单播发送至各节点设备的数据分片不同；

[0076] 将接收到的数据分片广播发送至所述区块链中的其它各节点设备；以及，接收所述其它各节点设备广播发送的所述交易数据的数据分片；

[0077] 确定接收到的所述交易数据的数据分片的数量是否达到纠删码恢复阈值；

[0078] 如果是，基于纠删码重构算法对接收到的数据分片进行数据恢复得到所述交易数据的原始内容，以完成对所述交易数据的原始内容的共识处理。

[0079] 通过以上技术方案，由于主节点设备在向各从节点设备提议待共识的交易数据时，基于纠删码算法对待共识的交易数据进行分片之后再进行传播：

[0080] 一方面，使得主节点设备在向各从节点设备提议交易数据时，可以不再需要将完整的交易数据向各从节点设备进行广播发送，而是采用向各从节点设备单播发送数据分片即可，因此可以显著的降低向参与共识的节点设备扩散传播需要共识的交易数据时所消耗的数据传输带宽，可以在短时间内将待共识的交易数据传播至各从节点设备来完成共识，从而可以提升共识处理效率；

[0081] 另一方面，由于主节点设备向各从节点设备单播发送的仅仅是上述交易数据的数据分片，对于主节点设备而言，无法获知该数据分片所属的完整交易的完整内容，因此可以有效避免主节点设备向其它参与共识的节点设备有选择性的单播一些特定的交易，对一些特定的交易进行有选择性的共识，从而可以保障共识的公正性，反正主节点通过有选择性共识来进行“作恶”。

附图说明

[0082] 图1是一示例性实施例提供的一种基于区块链的交易共识处理方法的流程图。

[0083] 图2是一示例性实施例提供的一种优化后的pbft算法三个阶段的交互示意图。

[0084] 图3是一示例性实施例提供的一种电子设备的结构示意图。

[0085] 图4是一示例性实施例提供的一种基于区块链的交易共识处理装置的框图。

具体实施方式

[0086] 本说明书中，旨在提出一种在区块链的共识处理过程中，引入纠删码算法对待共识的交易数据进行分片后进行传播扩散，来降低在向参与共识的节点设备传播需要共识的交易数据时所消耗的数据传输带宽，提升共识效率的技术方案。

[0087] 在实现时，在区块链的每一轮共识开始之前，可以在区块链中的各节点设备中选举出一台主节点设备(比如，每一轮共识都重新选举出一主节点设备，其它节点设备作为从节点设备)，由主节点设备向发起交易共识，并负责基于共识通过的交易数据为区块链创建最新的区块。

[0088] 主节点设备在发起一轮交易共识时，首先可以基于纠删码算法将提议的待共识的交易数据，分割为指定数量的数据分片，然后将分割的数据分片分别单播发送至其它各节点设备；其中，主节点设备单播发送至各节点设备的数据分片不同；

[0089] 其次，各从节点设备在收到主节点设备单播发送的上述交易数据的数据分片时，可以将接收到的数据分片继续广播发送至区块链中的其它各节点设备；以及，还可以收集由其它各节点设备广播发送的数据分片。

[0090] 最后，对于区块链中的任意一台节点设备(包括主节点设备和从节点设备)而言，可以确定收集到的上述交易数据的数据分片的数量，是否达到了在采用上述纠删码算法对上述交易数据进行分割时定义的纠删码恢复阈值；如果是，表明当前收集到的数据分片的数量，已经足够恢复出上述交易数据的原始内容，此时可以基于纠删码重构算法对已经收集到的数据分片进行数据恢复，得到上述交易数据的原始内容，然后完成对上述交易数据的原始内容的共识处理。

[0091] 通过以上技术方案，由于主节点设备在向各从节点设备提议待共识的交易数据时，基于纠删码算法对待共识的交易数据进行分片之后再进行传播：

[0092] 一方面，使得主节点设备在向各从节点设备提议交易数据时，可以不再需要将完整的交易数据向各从节点设备进行广播发送，而是采用向各从节点设备单播发送数据分片即可，因此可以显著的降低向参与共识的节点设备扩散传播需要共识的交易数据时所消耗的数据传输带宽，可以在短时间内将待共识的交易数据传播至各从节点设备来完成共识，从而可以提升共识处理效率；

[0093] 另一方面，由于主节点设备向各从节点设备单播发送的仅仅是上述交易数据的数据分片，对于主节点设备而言，无法获知该数据分片所属的完整交易的完整内容，因此可以有效避免主节点设备向其它参与共识的节点设备有选择性的单播一些特定的交易，对一些特定的交易进行有选择性的共识，从而可以保障共识的公正性，反正主节点通过有选择性共识来进行“作恶”。

[0094] 下面通过具体实施例并结合具体的应用场景对本说明书进行描述。

[0095] 请参考图1，图1是本说明书一实施例提供的一种基于区块链的交易共识处理方法，应用于区块链中的任一节点设备；其中，所述区块链中的节点设备至少包括一主节点设备以及若干从节点设备，所述主节点设备基于纠删码算法将提议的交易数据分割为指定数量的数据分片，执行以下步骤：

[0096] 步骤102，接收所述主节点设备单播发送的所述交易数据的数据分片；其中，所述主节点设备单播发送至各节点设备的数据分片不同；

[0097] 步骤104，将接收到的数据分片广播发送至所述区块链中的其它各节点设备；以及，接收所述其它各节点设备广播发送的所述交易数据的数据分片；

[0098] 步骤106，确定接收到的所述交易数据的数据分片的数量是否达到纠删码恢复阈值；

[0099] 步骤108，如果是，基于纠删码重构算法对接收到的数据分片进行数据恢复得到所述交易数据的原始内容，以完成对所述交易数据的原始内容的共识处理。

[0100] 在本说明书所描述的区块链，具体可以包括私有链、共有链以及联盟链等，在本说明书中不进行特别限定。

[0101] 例如，在一个场景中，上述区块链具体可以是由第三方支付平台的服务器、境内银行服务器、境外银行服务器、以及若干用户节点设备作为成员设备组成的一个联盟链。该联盟链的运营方可以依托于该联盟链，来在线部署诸如基于联盟链的跨境转账、资产转移等在线业务。

[0102] 在本说明书中所描述的交易，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。

[0103] 其中，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。

[0104] 需要说明的是，上述区块链搭载的共识算法，在本说明书中不进行特别限定；在实际应用中，具体可以采用拜占庭容错(Byzantine Fault Tolerance)系列算法作为共识算法，也可以采用非拜占庭容错系列算法作为共识算法。

[0105] 其中，所谓拜占庭容错算法，是指在由若干个节点设备组成的分布式网络中，需要考虑拜占庭节点(即作恶节点)的分布式容错算法；例如，pbft算法；如果采用拜占庭容错算法在区块链网络中进行共识处理时，会认为区块链中同时存储作恶节点和故障节点。而相应的，所谓非拜占庭容错算法，是指在由若干个节点设备组成的分布式网络中，不考虑拜占庭节点的分布式容错算法；例如，raft算法等等；如果采用非拜占庭容错算法在区块链网络中进行共识处理时，会认为区块链中不存在作恶节点，而只存在故障节点。

[0106] 在本说明书中所描述的由主节点设备提议的交易数据，具体是指由主节点设备收集到的，由用户客户端通过接入的节点设备提交的待共识交易；例如，在一种实现方式中，用户客户端可以通过接入的节点设备将用户发起的交易在区块链中进行广播发送。

[0107] 其中，在实际应用中，主节点设备可以针对单笔交易发起共识，也可以针对构建的一个交易列表来发起共识。

[0108] 例如，在一种实施方式中，用户客户端可以将用户提交的交易在区块链网络中进行广播。而主节点设备可以收集各个用户客户端，在本轮的共识时间段内，在区块链网络中

广播发送的待共识交易，然后基于收集到的待共识交易创建交易列表，将该交易列表作为提议的交易数据向其它各节点设备传播。

[0109] 以下以上述区块链为联盟链，以及该联盟链采用pbft算法作为共识算法，对主节点设备提议的交易列表进行共识处理为例进行说明。

[0110] 在本说明书中，可以在pbft算法现有的预准备(pre-prepare)、准备(prepare)、和确认(commit)等三个阶段的基础之上，引入纠删码算法，对pbft算法的pre-prepare和prepare阶段现有的交易数据传播扩散机制进行优化改进，以降低主节点设备与从节点设备之间进行共识交互时的数据传输带宽，提升共识处理效率。

[0111] 请参见图2，图2为本说明书示出的一种优化后的pbft算法三个阶段的交互示意图。

[0112] 如图2所示，在联盟链的每一轮共识开始之前，首先可以在联盟链中的各节点设备中选举出一台主节点设备；

[0113] 例如，基于Pbft算法，在联盟链的每一轮共识开始之前，可以基于以下的公式，为本轮公式计算出一个主节点设备：

[0114] $P = v \bmod R$

[0115] 其中，表示计算出的本轮共识的主节点编号；v表示联盟链当前的视图编号；试图编号通常是一个连续编号的整数，表示联盟链已经成功完成共识的轮数；比如，在成功完成一轮共识，选举出的主节点设备向联盟链成功写入一个新的区块之后，可以将试图编号自动加1。R表示联盟链中的节点设备的总数量。

[0116] 各个节点设备可以分别执行以上计算，并将计算出的主节点编号与本设备的编号进行匹配，来确定本设备是否被选举为主节点设备。

[0117] 一方面，如果一节点设备确定本设备未被选举为主节点设备，则可以将收到的由客户端提交的交易向联盟链中的各个节点设备进行广播发送。

[0118] 另一方面，如果一节点设备确定本设备被选举为主节点设备，则可以收集各个用户客户端在本轮的共识时间段内广播发送的交易，并基于收集到的交易，来创建交易列表。此时，创建的交易列表即为主节点设备提议的需要进行共识处理的交易数据。

[0119] 进一步的，主节点设备可以基于纠删码算法，对提议的交易列表进行分片处理，将上述交易列表分割为指定数量的数据分片。

[0120] 需要说明的是，对上述交易列表进行分割得到的数据分片的数量，可以与联盟链中的节点设备总数一致；例如，假设联盟链中有N台节点设备，那么可以将上述交易列表也分割成为N个数据分片。

[0121] 其中，基于纠删码算法对上述交易列表进行分割的具体过程，在本说明书中不再进行详细描述，本领域技术人员在将本说明书记载的技术方案付诸实现时，可以参考相关技术中的记载；

[0122] 例如，基于纠删码算法，假设将上述交易列表分割为N个数据分片，在这N个数据分片将会包含K个数据块，和M个校验块。M表示上述N个数据分片中可以容忍发生错误的数据分片的个数。K表示恢复出原始的交易列表至少所需的数据分片的个数(即行数纠删码恢复阈值)。即通过上述N个数据分片中的任意K个数据分片，通过纠删码重构算法(即纠删码算法的逆向算法)都可以恢复出上述交易列表的原始内容。

[0123] 当主节点设备基于纠删码算法对上述交易列表完成分割，可以通过向各从节点设备发送Pre-Prepare消息，将分割得到的数据分片分别发送至其它各节点设备；其中，在本说明书中，主节点设备发送至各从节点设备的数据分片需要保持不同。

[0124] 基于现有的pbft协议，主节点设备通过可以将完整的交易列表携带在Pre-Prepare消息中，然后将该Pre-Prepare消息在联盟链中的各个节点设备中进行广播发送，将完整的交易列表传播至联盟链中需要参与交易共识的从节点设备。

[0125] 然而，基于pbft协议现有的交易数据传播机制，由于Pre-Prepare消息中需要携带完整的交易列表，广播发送Pre-Prepare消息就会产生大量的数据副本；比如，需要基于联盟链中节点设备的总数量N，将Pre-Prepare消息复制N份，然后进行广播发送；因此，pbft协议在交易数据的传播阶段，会大量占用联盟链的网络带宽，对联盟链网络的带宽性能上具有较高的要求；一旦联盟链网络的带宽性能不足，会导致无法在短时间内将需要共识的交易列表扩散传播至其它参与共识的从节点设备。

[0126] 基于此，在本说明书中，可以对pbft算法的pre-prepare和prepare阶段现有的交易数据传播机制进行优化改进：

[0127] 一方面，主节点设备向各从节点设备发送Pre-Prepare消息中，可以不再携带完整的交易列表，而是仅携带上述交易列表的一个数据分片。

[0128] 另一方面，主节点设备向其它各从节点设备扩散Pre-Prepare消息的方式，可以由广播发送Pre-Prepare消息的方式，修改为向各从节点设备单播发送Pre-Prepare消息；例如，可以针对各个从节点设备分别构建Pre-Prepare消息，在Pre-Prepare消息中携带彼此互不相同的数据分片，然后逐一将构建的Pre-Prepare消息依次发送至各从节点设备，以确保各从节点设备能够收到不同的数据分片。

[0129] 请继续参见图2，收到上述Pre-Prepare消息的从节点设备，首先可以遵循pbft算法的规定，对收到的Pre-Prepare消息进行验证，以确定是否接受收到的Pre-Prepare消息。

[0130] 其中，在本说明书中，对收到的Pre-Prepare消息进行验证，即为对收到的Pre-Prepare消息中携带的内容进行验证的过程，具体的验证过程，在本说明书中不再进行详述；

[0131] 例如，遵循pbft算法的规定，在Pre-Prepare消息中，可以携带待共识的交易数据(本说明书中为数据分片)、视图编号v、待共识的交易数据的摘要(在本说明书中为数据分片的摘要)、数字签名等信息。相应的，在本说明书中老年个，在对Pre-Prepare消息进行验证时，具体可以执行以下的验证过程：

[0132] 1)验证视图编号V与本地记录的试图编号是否一致；

[0133] 2)对Pre-Prepare消息中的数字签名进行验证；

[0134] 3)对Pre-Prepare消息中携带的数据分片进行有效性验证；

[0135] 例如，在实现时，主节点设备可以基于所有数据分片构建一颗默克尔树，并在Pre-Prepare消息中携带默克尔树的各分支节点的hash值。而节点设备在对接收到的Pre-Prepare消息中携带的数据分片进行验证时，可以重新计算该Pre-Prepare消息中携带的数据分片的hash值，基于该hash值以及Pre-Prepare消息中携带的上述默克尔树的各分支节点的hash值，来重构默克尔树；然后，可以通过比较重构的默克尔树的树根对应的hash，来对该数据分片进行验证；如果重构的默克尔树的树根对应的hash没有发生变化，则认为该

数据分片通过有效性验证;反之,可以认为该Pre-Prepare消息中携带的为无效的数据分片,此时可以丢弃该数据分片。

[0136] 当然,在实际应用中,上述Pre-Prepare消息中所携带的内容,也可以基于实际需求进行扩展;例如,在一个例子中,上述Pre-Prepare消息中还可以携带共识高度h。上述共识高度h与试图编号v在功能上类似,通常是一个连续编号的整数,表示联盟链已经共识过的轮数(并非指示成功共识的轮数)。比如,在一轮共识的过程中,如果主节点设备发生故障,通常会触发试图切换,重新选举主节点设备,在这种情况下,可以立即将共识高度h加一,而由于本轮尚未共识成功,对于试图编号V而言,则并不加一,仍然保留原来的试图编号V。

[0137] 在这种情况下,在对Pre-Prepare消息进行验证时,在以上列举出的验证过程的基础上,还可以进一步执行以下示出的验证:

[0138] 4)验证共识高度h与本地记录的共识高度h是否一致。

[0139] 请继续参见图2,当收到上述Pre-Prepare消息的节点设备,在执行以上列举出的验证过程后,如果验证通过,表示该节点设备接受上述Pre-Prepare消息,此时该节点设备可以获取并保存该Pre-Prepare消息中携带的数据分片,并进入pbft协议的Prepare阶段,向联盟链中的其它各个节点设备广播发送一条用于对上述Pre-Prepare消息进行确认的Prepare消息;其中,上述Prepare消息中携带的内容格式,可以与上述Pre-Prepare消息保持一致。

[0140] 基于现有的pbft协议,节点设备向联盟链的其它各个节点设备广播的Prepare消息中,通常仅携带诸如视图编号v、待共识的交易数据的摘要等数据,在本说明书中,可以对Prepare消息的格式进行进一步扩展,各节点设备也可以将主节点设备通过Pre-Prepare消息单播发送的数据分片,也携带在上述Prepare消息中。

[0141] 一方面,各节点设备可以将携带数据分片的Prepare消息,在联盟链中的其它各个节点设备中进行广播发送,以将接收到的由主节点设备单播发送的数据分片,进一步扩散传播至联盟链中的其它各节点设备。

[0142] 另一方面,各节点设备也可以接收由其它各从节点设备广播发送的Prepare消息,对收到Prepare消息进行验证,以确定是否接受收到的Prepare消息。其中,对收到Prepare消息进行验证的具体过程,可以参考对Pre-Prepare消息进行验证的具体过程,在本说明书中不再进行赘述。

[0143] 如果验证通过,表示该节点设备接受收到的Prepare消息:

[0144] 一方面,该节点设备可以获取并保存该Prepare消息中携带的数据分片;

[0145] 另一方面,该节点设备还可以进一步确定接收到的由其它各节点设备广播发送的Prepare消息的数量,是否达到2f+1个(包括自身广播的Prepare消息在内)。

[0146] 其中,f表示pbft算法能够容错的错误节点的数量;f的具体取值,可以通过公式N=3f+1换算的得到;N表示联盟链中的节点设备的总数量。

[0147] 如果收到的Prepare消息的数量达到2f+1个,此时该节点设备可以进入pbft协议的commit阶段,该节点设备可以向联盟链中的其它各个节点设备广播发送一条commit消息,继续完成对上述交易列表的原始内容的共识处理过程。

[0148] 在本说明书中,联盟链中的节点设备在向联盟链中的其它各个节点设备广播发送

commit消息之后，也可以接收由其它各节点设备广播发送的commit消息消息，对收到commit消息进行验证，以确定是否接受收到的commit消息。

[0149] 其中，在本说明书中，上述commit消息中携带的内容格式，可以与Pre-Prepare消息和Prepare消息保持一致。但需要强调的是，在Pre-Prepare消息和Prepare消息中，携带的待共识的交易数据的摘要，为上述交易列表的数据摘要，而在commit阶段，由于节点设备已经恢复出完整的交易列表，因此在commit消息中可以携带恢复出的完整的交易列表的摘要。

[0150] 其中，对收到commit消息进行验证的具体过程，可以参考对Pre-Prepare消息进行验证的具体过程，在本说明书中不再进行赘述。

[0151] 如果验证通过，表示该节点设备接受收到的commit消息，该节点设备还可以进一步确定接收到的由其它各节点设备广播发送的commit消息的数量，是否达到2f+1个(包括自身广播的commit消息在内)。

[0152] 如果收到的commit消息的数量达到2f+1个，此时该节点设备可以进一步确定收集到的数据分片，是否达到了纠删码算法支持的纠删码恢复阈值；如果是，该节点设备可以立即基于纠删码重构算法，对已经收集到的数据分片进行数据恢复计算，还原出上述交易列表的原始内容。

[0153] 其中，基于纠删码重构算法，对已经收集到的数据分片进行数据恢复计算的具体计算过程，在本说明书中不再进行详述，本领域技术人员在将本说明书的技术方案付诸实现时，可以参考相关技术中的记载。

[0154] 其中，在示出的一种实施方式中，由于一旦上述纠删码恢复阈值的具体取值大于2f+1，会导致从节点设备在commit阶段，没有足够的数据分片来恢复出需要共识的上述交易列表的原始内容，因此在本说明书中，上述纠删码算法支持的纠删码恢复阈值的具体取值大小，需要小于或者等于上述2f+1；例如，可以恰好等于2f+1。

[0155] 通过这种方式，使得主节点设备在基于纠删码算法对上述交易列表进行分割时，可以参考pbft算法支持的错误节点的容错数量f，来控制最终分割得到的数据分片的数量，从而可以在确保在commit阶段，有足够的数据分片恢复出需要共识的上述交易列表的原始内容的前提下，尽可能的将上述交易列表分割为足够小的数据分片。

[0156] 在本说明书中，主节点设备在对上述交易列表进行分割之前，还可以基于支持的相关算法对上述交易列表进行预处理。

[0157] 在示出的一种实施方式中，主节点设备对上述交易列表进行分割之前，还可以对上述交易列表进行压缩预处理，基于支持的压缩算法对上述交易列表进行压缩处理。

[0158] 其中，上述主节点设备所采用的压缩算法，在本说明书中不进行特别限定。

[0159] 当完成针对上述交易列表的压缩处理之后，此时主节点设备再基于上述纠删码算法对压缩处理后的上述交易列表进行分割，将压缩处理后的上述交易列表分割成为指定数量的数据分片。

[0160] 相应的，在pbft协议的Prepare阶段，由于各节点设备传播扩散的数据分片，为基于压缩处理后的交易列表进行分割得到的数据分片，因此节点设备在基于纠删码重构算法，对收集到的数据分片进行数据恢复后，得到的也只是压缩处理后的交易列表。

[0161] 在这种情况下，节点设备在完成以上数据恢复计算后，可以基于与上述压缩算法

对应的解压缩算法，对恢复出的压缩后的交易列表进行解压缩处理，来解压缩出上述交易列表的原始内容，然后继续执行commit阶段的共识处理过程，具体的实施细节不再赘述。

[0162] 通过这种方式，由于主节点设备在对上述交易列表进行分割之前，预先对主节点设备进行了压缩处理，因此可以有效减低压缩后的数据分片的大小，从而能够最大程度的降低主节点设备与从节点设备之间进行共识交互时的数据传输带宽。

[0163] 在示出的另一种实施方式中，主节点设备对上述交易列表进行分割之前，还可以对上述交易列表进行加密预处理，基于预设的加密算法以及加密密钥对对上述交易列表进行加密处理。

[0164] 其中，上述主节点设备所采用的加密算法，在本说明书中不进行特别限定；例如，在实际应用中，可以是对称加密算法，也可以是非对称加密算法。

[0165] 当完成针对上述交易列表的加密处理之后，此时主节点设备再基于上述纠删码算法对加密处理后的上述交易列表进行分割，将加密处理后的上述交易列表分割成为指定数量的数据分片。

[0166] 相应的，在pbft协议的Prepare阶段，由于各节点设备传播扩散的数据分片，为基于加密处理后的交易列表进行分割得到的数据分片，因此节点设备在基于纠删码重构算法，对收集到的数据分片进行数据恢复后，得到的也只是加密处理后的交易列表。

[0167] 在这种情况下，节点设备在完成以上数据恢复计算后，可以基于与上述加密算法对应的解密算法，以及与上述加密密钥对应的解密密钥，对恢复出的压缩后的交易列表进行解密处理，来解密出上述交易列表的原始内容，然后继续执行commit阶段的共识处理过程，具体的实施细节不再赘述。

[0168] 其中，在示出的一种实施方式中，上述加密算法具体可以是门限加密算法。而上述解密算法具体可以是与门限加密算法对应的门限解密算法。

[0169] 在这种场景下，解密密钥具体可以被分割为指定数量的子密钥，并将各子密钥由各节点设备分别持有。

[0170] 需要说明的是，对上述解密密钥进行分割得到的子密钥的数量，可以与联盟链中的节点设备总数一致；例如，假设联盟链中有N台节点设备，那么可以将上述解密密钥也分割成为N个子密钥，由联盟链中的N台节点设备分别持有。

[0171] 在这种情况下，节点设备还可以收集其它各节点设备持有的子密钥，并确定收集到的子密钥的数量是否达到预设的解密门限阈值；比如，密钥门限阈值为N时，表明需要N个节点设备基于持有的子密钥(也即上述解密密钥的部分片段)，来共同对加密后的数据进行解密。

[0172] 其中，节点设备收集其它各节点设备持有的子密钥的具体方式，在本说明书中不进行特别限定；

[0173] 例如，仍以联盟链采用的共识算法为pbft算法为例，节点设备可以在与其它节点设备交互的commit消息中，携带自身持有的子密钥；当然，在实际应用中，各节点设备也可以通过单独定义一个用于传播持有的子密钥的交互消息，利用该交互消息将自身持有的子密钥同步到其它节点设备。

[0174] 如果节点设备设备收集到的子密钥的数量达到预设的解密门限阈值，表明该节点设备已经具有足够的分片来重构解密密钥，此时该节点设备可以基于收集到的子密钥对解

密密钥进行重构处理，以恢复出原始的解密密钥，然后基于门限解密算法以及恢复出的原始的解密密钥，对恢复出的加密处理后的交易列表进行解密处理，来解密出上述交易列表的原始内容。

[0175] 其中，基于收集到的子密钥对解密密钥进行重构的具体过程，在本说明书中不再进行详细描述，本领域技术人员在将本说明书的技术方案付诸实现时，可以参考相关技术中的记载；

[0176] 例如，在对解密密钥进行分割、以及基于收集到的子密钥对解密密钥进行恢复，仍然可以采用纠删码技术来实现，具体过程不再赘述。

[0177] 通过这种方式，由于主节点设备在对上述交易列表进行分割之前，预先对主节点设备进行了加密处理，因此可以有效的提升主节点设备在向各节点设备发送数据分片时的数据安全，使得一些非法的节点设备即便收集到足够的数据分片恢复出上述交易列表，也无法查看到交易列表的原始内容，从而可以提升主节点设备与从节点设备之间进行共识交互时的数据安全。

[0178] 需要补充说明的是，在以上实施例中，以利用pbft算法的pre-prepare和prepare阶段现有的交易数据传播扩散机制，将待共识的交易列表传播扩散至各个参与共识的节点设备为例进行了详细说明。

[0179] 需要强调的是，在实际应用中，在需要将待共识的交易列表传播扩散至各个参与共识的节点设备时，除了利用联盟链搭载的共识算法中已有的传播扩散机制来完成交易列表传播扩散以外，也可以通过定义单独的传播扩散协议来完成相同的功能；

[0180] 例如，仍然以联盟链采用的共识算法为pbft算法为例，主节点设备与从节点设备之间在启动pbft算法规定的三个阶段的共识交互之前，主节点设备可以通过定义的传播扩散协议，与从节点设备进行共识交互，提前将需要共识的交易列表传播扩散至各个从节点设备。也即，节点设备可以通过定义的传播扩散协议，提前将需要共识的交易列表扩散传播到各个参与共识的节点设备之后，再启动pbft算法规定的三个阶段的共识交互，完成对该交易列表的共识处理。

[0181] 在这种情况下，pbft算法的pre-prepare和prepare阶段现有的交易数据传播扩散机制则不再不需要执行以上实施例中描述的优化过程；比如，pre-prepare消息和prepare消息中，可以不再携带完整的交易列表，或者是交易列表的数据分片，而是直接携带上述交易列表的摘要值即可。

[0182] 另外，以上实施例中，仅以联盟链采用pbft算法作为共识算法为例进行了说明，显然在实际应用中，本说明书中的技术方案也可以等同应用在联盟链采用的其它形式的共识算法之中。

[0183] 也即，以上步骤102-106示出的传播扩散逻辑，除了可以应用在pbft算法的共识交互过程之中，也可以应用在注入raft等其它类似的共识算法之中，其具体的实施细节，在本说明书中不再进行详述，本领域技术人员在将本说明书的技术方案付诸实现时，可以参考以上实施例中的记载。

[0184] 通过以上各实施例可见，由于主节点设备在向各从节点设备提议待共识的交易数据时，可以基于纠删码算法对待共识的交易数据进行分片之后再进行传播：

[0185] 一方面，使得主节点设备在向各从节点设备提议交易数据时，可以不再需要将完

整的交易数据向各从节点设备进行广播发送，而是采用向各从节点设备单播发送数据分片即可，因此可以显著的降低向参与共识的节点设备扩散传播需要共识的交易数据时所消耗的数据传输带宽，可以在短时间内将待共识的交易数据传播至各从节点设备来完成共识，从而可以提升共识处理效率；

[0186] 另一方面，由于主节点设备向各从节点设备单播发送的仅仅是上述交易数据的数据分片，对于主节点设备而言，无法获知该数据分片所属的完整交易的完整内容，因此可以有效避免主节点设备向其它参与共识的节点设备有选择性的单播一些特定的交易，对一些特定的交易进行有选择性的共识，从而可以保障共识的公正性，反正主节点通过有选择性共识来进行“作恶”。

[0187] 与上述方法实施例相对应，本说明书还提供了一种基于区块链的交易共识处理装置的实施例。本说明书的基于区块链的交易共识处理装置的实施例可以应用在电子设备上。装置实施例可以通过软件实现，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，作为一个逻辑意义上的装置，是通过其所在电子设备的处理器将非易失性存储器中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，如图3所示，为本说明书的基于区块链的交易共识处理装置所在电子设备的一种硬件结构图，除了图3所示的处理器、内存、网络接口、以及非易失性存储器之外，实施例中装置所在的电子设备通常根据该电子设备的实际功能，还可以包括其他硬件，对此不再赘述。

[0188] 图4是本说明书一示例性实施例示出的一种基于区块链的交易共识处理装置的框图。

[0189] 请参考图4，所述基于区块链的交易共识处理装置40可以应用在前述图3所示的电子设备中，包括有：接收模块401、发送模块402、确定模块403和恢复模块404。

[0190] 接收模块401，接收所述主节点设备单播发送的所述交易数据的数据分片；其中，所述区块链中的节点设备至少包括一主节点设备以及若干从节点设备；所述主节点设备基于纠删码算法将提议的交易数据分割为指定数量的数据分片所述主节点设备单播发送至各节点设备的数据分片不同；

[0191] 发送模块402，将接收到的数据分片广播发送至所述区块链中的其它各节点设备；以及，接收所述其它各节点设备广播发送的所述交易数据的数据分片；

[0192] 确定模块403，确定接收到的所述交易数据的数据分片的数量是否达到纠删码恢复阈值；

[0193] 恢复模块404，如果是，基于纠删码重构算法对接收到的数据分片进行数据恢复得到所述交易数据的原始内容，以完成对所述交易数据的原始内容的共识处理。

[0194] 在本实施例中，所述装置40还包括：

[0195] 分割模块405，确定本节点设备是否被选举为所述主节点设备；如果是，基于所述纠删码算法将提议的交易数据分割为指定数量的数据分片；

[0196] 所述发送模块402进一步：

[0197] 将所述指定数量的数据分片分别单播发送至其它各节点设备。

[0198] 在本实施例中，所述区块链搭载的共识算法为pbft算法；

[0199] 所述接收模块401：

[0200] 接收所述主节点设备单播发送的Pre-Prepare消息；其中，所述Pre-Prepare消息

中包括所述交易数据的数据分片；

[0201] 获取并保存所述Pre-Prepare消息中的数据分片。

[0202] 在本实施例中，所述发送模块402：

[0203] 向所述区块链中的其它各节点设备广播发送Prepare消息；其中，所述Prepare消息包括接收到的所述数据分片，以使所述其它各节点设备在接收到所述Prepare消息时，获取并保存所述Prepare消息中的数据分片。

[0204] 在本实施例中，所述分割模块405：

[0205] 基于预设的压缩算法对提议的所述交易数据进行压缩处理；

[0206] 基于所述纠删码算法将压缩处理后的所述交易数据分割为指定数量的数据分片。

[0207] 所述恢复模块404：

[0208] 基于纠删码重构算法对接收到的数据分片进行数据恢复得到压缩后的所述交易数据；

[0209] 基于与所述压缩算法对应的解压缩算法，对恢复出的所述交易数据进行解压缩处理，以得到所述交易数据的原始内容。

[0210] 在本实施例中，所述分割模块405：

[0211] 基于预设的加密算法以及加密密钥对提议的交易数据进行加密处理；

[0212] 基于所述纠删码算法将加密处理后的所述交易数据分割为指定数量的数据分片。

[0213] 所述恢复模块404：

[0214] 基于基于纠删码重构算法对接收到的数据分片进行数据恢复得到加密后的所述交易数据；

[0215] 基于与所述加密算法对应的解密算法，以及与所述加密密钥对应的解密密钥，对恢复出的所述交易数据进行解密处理，以得到所述交易数据的原始内容。

[0216] 在本实施例中，所述加密算法为门限加密算法；所述解密算法为与门限加密算法对应的门限解密算法；所述解密密钥被分割为指定数量的子密钥；其中，各子密钥由各节点设备分别持有；

[0217] 所述恢复模块404进一步：

[0218] 收集所述其它各节点设备持有的子密钥；

[0219] 确定收集到的子密钥的数量是否达到预设的解密门限阈值；

[0220] 如果是，基于收集到的子密钥重构所述解密密钥，并基于与所述门限加密算法对应的门限解密算法，以及所述解密密钥，对恢复出的所述交易数据进行解密处理。

[0221] 在本实施例中，所述主节点提议的交易数据，为所述主节点设备当前共识周期内由各用户客户端广播发送的待共识交易构建的交易列表；所述指定数量为所述区块链中的节点设备的总数量。

[0222] 在本实施例中，所述区块链为联盟链。

[0223] 上述装置中各个模块的功能和作用的实现过程具体详见上述方法中对应步骤的实现过程，在此不再赘述。

[0224] 对于装置实施例而言，由于其基本对应于方法实施例，所以相关之处参见方法实施例的部分说明即可。以上所描述的装置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，作为模块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。

[0225] 上述实施例阐明的系统、装置、模块或模块,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。

[0226] 与上述方法实施例相对应,本说明书还提供了一种电子设备的实施例。该电子设备包括:处理器以及用于存储机器可执行指令的存储器;其中,处理器和存储器通常通过内部总线相互连接。在其他可能的实现方式中,所述设备还可能包括外部接口,以能够与其他设备或者部件进行通信。

[0227] 在本实施例中,通过读取并执行所述存储器存储的与基于区块链的交易共识处理的控制逻辑对应的机器可执行指令,所述处理器被促使:

[0228] 接收所述主节点设备单播发送的所述交易数据的数据分片;其中,所述区块链中的节点设备至少包括一主节点设备以及若干从节点设备;所述主节点设备基于纠删码算法将提议的交易数据分割为指定数量的数据分片所述主节点设备单播发送至各节点设备的数据分片不同;

[0229] 将接收到的数据分片广播发送至所述区块链中的其它各节点设备;以及,接收所述其它各节点设备广播发送的所述交易数据的数据分片;

[0230] 确定接收到的所述交易数据的数据分片的数量是否达到纠删码恢复阈值;

[0231] 如果是,基于纠删码重构算法对接收到的数据分片进行数据恢复得到所述交易数据的原始内容,以完成对所述交易数据的原始内容的共识处理。

[0232] 在本实施例中,通过读取并执行所述存储器存储的与基于区块链的交易共识处理的控制逻辑对应的机器可执行指令,所述处理器被促使:

[0233] 确定本节点设备是否被选举为所述主节点设备;

[0234] 如果是,基于所述纠删码算法将提议的交易数据分割为指定数量的数据分片;以及,

[0235] 将所述指定数量的数据分片分别单播发送至其它各节点设备。

[0236] 在本实施例中,所述区块链搭载的共识算法为pbft算法;

[0237] 通过读取并执行所述存储器存储的与基于区块链的交易共识处理的控制逻辑对应的机器可执行指令,所述处理器被促使:

[0238] 接收所述主节点设备单播发送的Pre-Prepare消息;其中,所述Pre-Prepare消息中包括所述交易数据的数据分片;

[0239] 获取并保存所述Pre-Prepare消息中的数据分片。

[0240] 在本实施例中,通过读取并执行所述存储器存储的与基于区块链的交易共识处理的控制逻辑对应的机器可执行指令,所述处理器被促使:

[0241] 向所述区块链中的其它各节点设备广播发送Prepare消息;其中,所述Prepare消息包括接收到的所述数据分片,以使所述其它各节点设备在接收到所述Prepare消息时,获

取并保存所述Prepare消息中的数据分片。

[0242] 在本实施例中，通过读取并执行所述存储器存储的与基于区块链的交易共识处理的控制逻辑对应的机器可执行指令，所述处理器被促使：

[0243] 基于预设的压缩算法对提议的所述交易数据进行压缩处理；

[0244] 基于所述纠删码算法将压缩处理后的所述交易数据分割为指定数量的数据分片。

[0245] 在本实施例中，通过读取并执行所述存储器存储的与基于区块链的交易共识处理的控制逻辑对应的机器可执行指令，所述处理器被促使：

[0246] 基于纠删码重构算法对接收到的数据分片进行数据恢复得到压缩后的所述交易数据；

[0247] 基于与所述压缩算法对应的解压缩算法，对恢复出的所述交易数据进行解压缩处理，以得到所述交易数据的原始内容。

[0248] 在本实施例中，通过读取并执行所述存储器存储的与基于区块链的交易共识处理的控制逻辑对应的机器可执行指令，所述处理器被促使：

[0249] 基于预设的加密算法以及加密密钥对提议的交易数据进行加密处理；

[0250] 基于所述纠删码算法将加密处理后的所述交易数据分割为指定数量的数据分片。

[0251] 在本实施例中，通过读取并执行所述存储器存储的与基于区块链的交易共识处理的控制逻辑对应的机器可执行指令，所述处理器被促使：

[0252] 基于基于纠删码重构算法对接收到的数据分片进行数据恢复得到加密后的所述交易数据；

[0253] 基于与所述加密算法对应的解密算法，以及与所述加密密钥对应的解密密钥，对恢复出的所述交易数据进行解密处理，以得到所述交易数据的原始内容。

[0254] 在本实施例中，所述加密算法为门限加密算法；所述解密算法为与门限加密算法对应的门限解密算法；所述解密密钥被分割为指定数量的子密钥；其中，各子密钥由各节点设备分别持有；

[0255] 通过读取并执行所述存储器存储的与基于区块链的交易共识处理的控制逻辑对应的机器可执行指令，所述处理器被促使：

[0256] 收集所述其它各节点设备持有的子密钥；

[0257] 确定收集到的子密钥的数量是否达到预设的解密门限阈值；

[0258] 如果是，基于收集到的子密钥重构所述解密密钥，并基于与所述门限加密算法对应的门限解密算法，以及所述解密密钥，对恢复出的所述交易数据进行解密处理。

[0259] 本领域技术人员在考虑说明书及实践这里公开的发明后，将容易想到本说明书的其它实施方案。本说明书旨在涵盖本说明书的任何变型、用途或者适应性变化，这些变型、用途或者适应性变化遵循本说明书的一般性原理并包括本说明书未公开的本技术领域中的公知常识或惯用技术手段。说明书和实施例仅被视为示例性的，本说明书的真正范围和精神由下面的权利要求指出。

[0260] 应当理解的是，本说明书并不局限于上面已经描述并在附图中示出的精确结构，并且可以在不脱离其范围进行各种修改和改变。本说明书的范围仅由所附的权利要求来限制。

[0261] 以上所述仅为本说明书的较佳实施例而已，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。

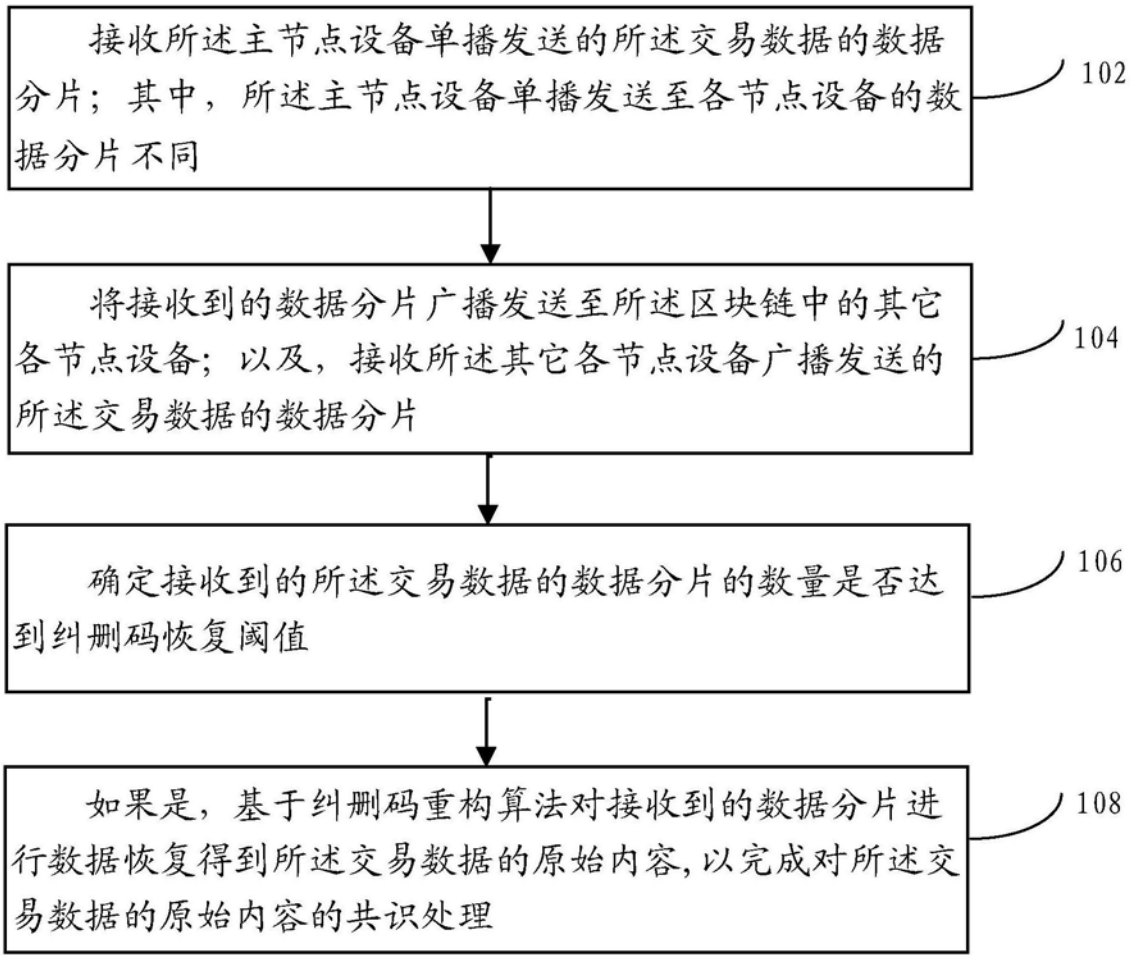

接收所述主节点设备单播发送的所述交易数据的数据分片；其中，所述主节点设备单播发送至各节点设备的数据分片不同
102
将接收到的数据分片广播发送至所述区块链中的其它各节点设备；以及，接收所述其它各节点设备广播发送的所述交易数据的数据分片
104
确定接收到的所述交易数据的数据分片的数量是否达到纠删码恢复阈值
106
如果是，基于纠删码重构算法对接收到的数据分片进行数据恢复得到所述交易数据的原始内容，以完成对所述交易数据的原始内容的共识处理
108

图1

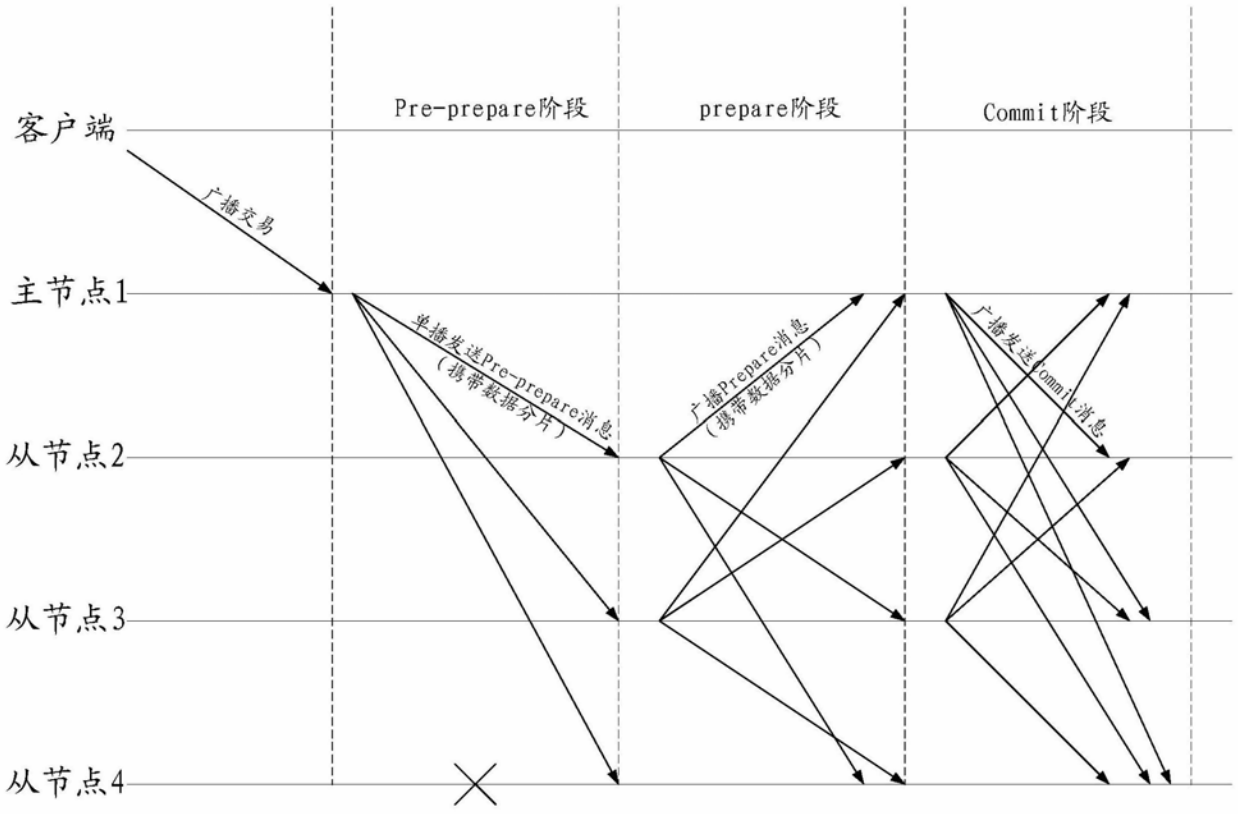

客户端
Pre-prepare阶段
prepare阶段
Commit阶段
广播交易
主节点1
单播发送Pre-prepare消息
（携带数据分片）
广播Prepare消息
（携带数据分片）
广播发送Commit消息
从节点2
从节点3
从节点4

图2

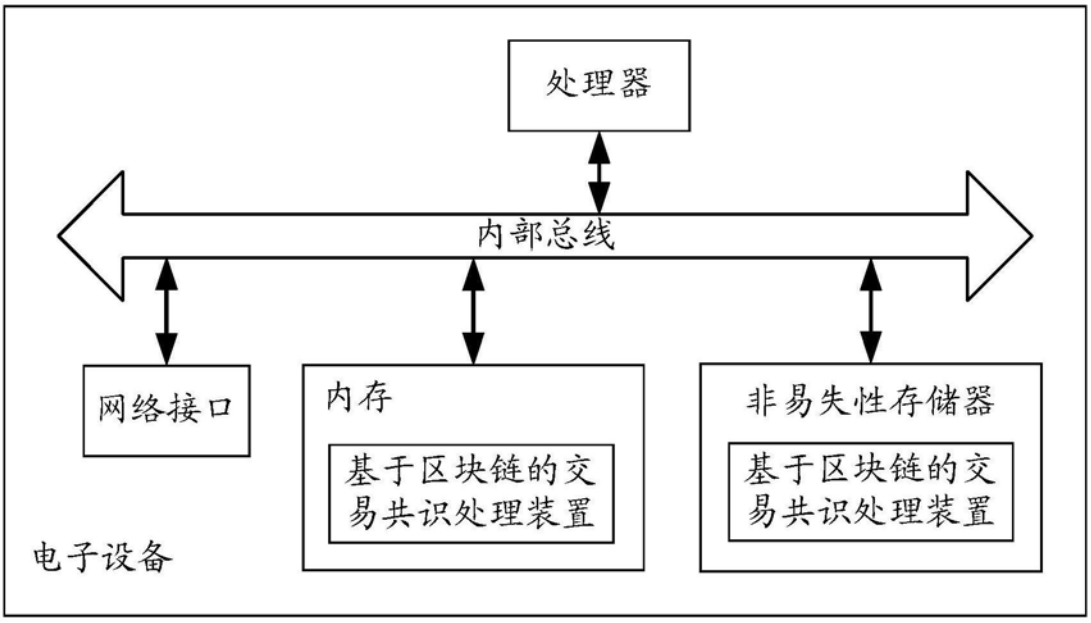

处理器
内部总线
网络接口
内存
基于区块链的交易共识处理装置
非易失性存储器
基于区块链的交易共识处理装置
电子设备

图3

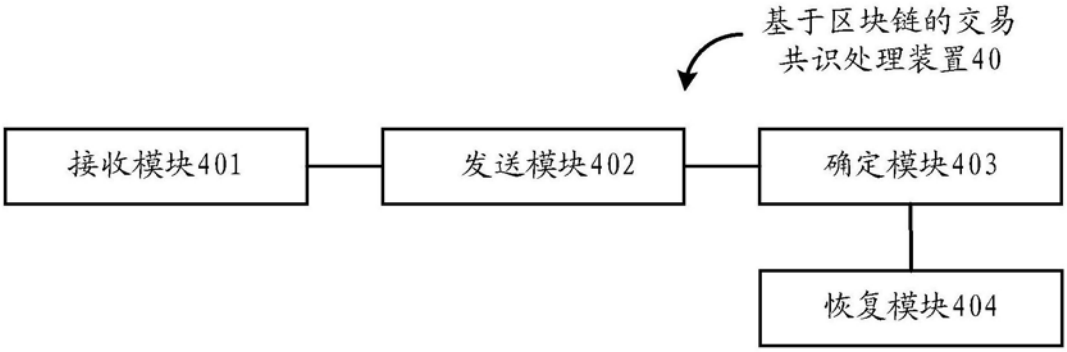


图4