

权利要求书

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:
 - 5 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;
 - 10 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, - 15 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;
 - 20 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, - 25 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;
 - 30 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。

- 5 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

- 10 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。

- 15 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:

- 20 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。

- 25 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。

- 30 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;

- 5 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;

- 10 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:

- 15 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,

- 20 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:

- 25 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:

- 30 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;

5 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:

10 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。

15 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;

20 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:

25 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;

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;

30 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。