

权利要求书

1、一种构建梅克尔树的方法，包括：

目标全节点针对目标区块中的每个交易存储位置，从该交易存储位置读取数据；所述目标全节点是区块链网络中的任一全节点，所述目标区块是所述目标全节点的区块链中的任一区块；

对从该交易存储位置读取的数据进行分析；

若确定从该交易存储位置读取的数据为交易，则对读取的交易进行哈希计算，得到交易哈希；

若确定从该交易存储位置读取的数据为隐匿化数据，则从所述隐匿化数据中提取交易哈希；其中，从所述隐匿化数据中提取的交易哈希，是该交易存储位置原本存储的交易的交易哈希，将该交易存储位置原本存储的交易替换成所述隐匿化数据的操作，是所述区块链网络中具有交易隐匿权限的节点指令各节点执行的；

基于所述目标区块中各交易存储位置分别对应的交易哈希，构建所述目标区块对应的梅克尔树。

2、如权利要求 1 所述的方法，将该交易存储位置存储的交易替换成所述隐匿化数据的操作如下：

获取该交易存储位置存储的交易的交易哈希；

将预设的前标记字符拼接到所述交易哈希的首部；

根据所述前标记字符与所述交易哈希拼接成的数据，确定隐匿化数据；

将该交易存储位置存储的交易替换成所述隐匿化数据。

3、如权利要求 2 所述的方法，根据所述前标记字符与所述交易哈希拼接成的数据，确定隐匿化数据，具体包括：

将预设的后标记字符拼接到所述交易哈希的尾部，并且，将备注信息拼接到所述后标记字符的尾部；

将所述前标记字符、所述交易哈希、所述后标记字符以及所述备注信息拼接成的数据确定为所述隐匿化数据。

4、如权利要求 2 或 3 所述的方法，对从该交易存储位置读取的数据进行分析，具体包括：

若从该交易存储位置读取的数据不包含所述前标记字符，则确定从该交易存储位置读取的数据为交易；

若从该交易存储位置读取的数据包含所述前标记字符，则确定从该交易存储位置读

取的数据为隐匿化数据。

5、如权利要求 2 所述的方法，从所述隐匿化数据中提取交易哈希，具体包括：

将所述隐匿化数据中位于所述前标记字符之后的数据确定为交易哈希并提取。

6、如权利要求 3 所述的方法，从所述隐匿化数据中提取交易哈希，具体包括：

5 将所述隐匿化数据中位于所述前标记字符与所述后标记字符之间的数据确定为交易哈希并提取。

7、一种简单支付验证方法，包括：

目标全节点接收验证请求；所述验证请求包含目标交易标识；所述目标全节点是区块链网络中的任一全节点；

10 根据所述验证请求，在自身的区块链中确定所述目标交易标识对应的交易所在的区块，并基于权利要求 1~6 任一项所述的方法构建所述区块对应的梅克尔树；

基于构建的梅克尔树，触发针对所述目标交易标识对应的交易的简单支付验证 SPV 流程。

8、如权利要求 7 所述的方法，针对写入区块链的任一交易，区块链网络中的各节点上预先记录有该交易的交易标识与区块链中该交易所在的交易存储位置之间的对应关系；

根据所述目标交易标识，在自身的区块链中确定所述目标交易标识对应的交易所在的区块，具体包括：

20 根据所述目标交易标识以及预先记录的交易标识与交易存储位置的对应关系，确定所述目标交易标识对应的交易存储位置，作为目标交易存储位置；

确定所述目标交易存储位置所属的区块，作为所述目标交易标识对应的交易所在的区块。

9、一种构建梅克尔树的装置，所述装置是区块链网络中的任一全节点，所述装置包括：

25 读取模块，针对目标区块中的每个交易存储位置，从该交易存储位置读取数据；所述目标区块是所述装置的区块链中的任一区块；

分析模块，对从该交易存储位置读取的数据进行分析；

交易哈希确定模块，若确定从该交易存储位置读取的数据为交易，则对读取的交易进行哈希计算，得到交易哈希；若确定从该交易存储位置读取的数据为隐匿化数据，则从所述隐匿化数据中提取交易哈希；其中，从所述隐匿化数据中提取的交易哈希，是该交易存储位置原本存储的交易的交易哈希；将该交易存储位置原本存储的交易替换成所

述隐匿化数据的操作,是所述区块链网络中具有交易隐匿权限的节点指令各节点执行的;

梅克尔树构建模块,基于所述目标区块中各交易存储位置分别对应的交易哈希,构建所述目标区块对应的梅克尔树。

10、如权利要求 9 所述的装置,将该交易存储位置存储的交易替换成所述隐匿化数据的操作如下:

获取该交易存储位置存储的交易的交易哈希;

将预设的前标记字符拼接所述交易哈希的首部;

根据所述前标记字符与所述交易哈希拼接成的数据,确定隐匿化数据;

将该交易存储位置存储的交易替换成所述隐匿化数据。

11、如权利要求 10 所述的装置,根据所述前标记字符与所述交易哈希拼接成的数据,确定隐匿化数据,具体包括:

将预设的后标记字符拼接所述交易哈希的尾部,并且,将备注信息拼接所述后标记字符的尾部;

15 据确定为所述隐匿化数据。

12、如权利要求 10 或 11 所述的装置,所述分析模块,若从该交易存储位置读取的数据不包含所述前标记字符,则确定从该交易存储位置读取的数据为交易;若从该交易存储位置读取的数据包含所述前标记字符,则确定从该交易存储位置读取的数据为隐匿化数据。

20 13、如权利要求 10 所述的装置,所述交易哈希确定模块,将所述隐匿化数据中位于所述前标记字符之后的数据确定为交易哈希并提取。

14、如权利要求 11 所述的装置,所述交易哈希确定模块,将所述隐匿化数据中位于所述前标记字符与所述后标记字符之间的数据确定为交易哈希并提取。

25 15、一种简单支付验证装置,所述装置是区块链网络中的任一全节点,所述装置包括:

接收模块,接收验证请求;所述验证请求包含目标交易标识;

确定构建模块,根据所述验证请求,在自身的区块链中确定所述目标交易标识对应的交易所在的区块,并基于权利要求 1~6 任一项所述的方法构建所述区块对应的梅克尔树;

30 触发模块,基于构建的梅克尔树,触发针对所述目标交易标识对应的交易的简单支付验证 SPV 流程。

16、如权利要求 15 所述的装置，针对写入区块链的任一交易，区块链网络中的各节点上预先记录有该交易的交易标识与区块链中该交易所在的交易存储位置之间的对应关系；

5 所述确定构建模块，根据所述目标交易标识以及预先记录的交易标识与交易存储位置的对应关系，确定所述目标交易标识对应的交易存储位置，作为目标交易存储位置；确定所述目标交易存储位置所属的区块，作为所述目标交易标识对应的交易所在的区块。

17、一种区块链系统，包括：由多个节点组成的区块链网络；

10 所述区块链网络中的任一全节点，针对目标区块中的每个交易存储位置，从该交易存储位置读取数据，所述目标区块是所述目标全节点的区块链中的任一区块；对从该交易存储位置读取的数据进行分析；若确定从该交易存储位置读取的数据为交易，则对读取的交易进行哈希计算，得到交易哈希；若确定从该交易存储位置读取的数据为隐匿化数据，则从所述隐匿化数据中提取交易哈希，其中，从所述隐匿化数据中提取的交易哈希，是该交易存储位置原本存储的交易的交易哈希；将该交易存储位置原本存储的交易替换成所述隐匿化数据的操作，是所述区块链网络中具有交易隐匿权限的节点指令各节点执行的；基于所述目标区块中各交易存储位置分别对应的交易哈希，构建所述目标区块对应的梅克尔树。

18、一种区块链系统，包括：由多个节点组成的区块链网络；

20 所述区块链网络中的任一全节点，接收验证请求，所述验证请求包含目标交易标识；根据所述验证请求，在自身的区块链中确定所述目标交易标识对应的交易所在的区块，并基于权利要求 1~6 任一项所述的方法构建所述区块对应的梅克尔树；基于构建的梅克尔树，触发针对所述目标交易标识对应的交易的简单支付验证 SPV 流程。

19、一种计算机设备，包括存储器、处理器及存储在存储器上并可在处理器上运行的计算机程序，其中，所述处理器执行所述程序时实现如权利要求 1~6 任一项所述的方法。

25 20、一种计算机设备，包括存储器、处理器及存储在存储器上并可在处理器上运行的计算机程序，其中，所述处理器执行所述程序时实现如权利要求 7 或 8 所述的方法。