(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 106506146 A
(43)申请公布日 2017.03.15

(21)申请号 201610949992.1

(22)申请日 2016.10.26

(71)申请人 北京瑞卓喜投科技发展有限公司
地址 100026 北京市朝阳区东方梅地亚中心C座1908室

(72)发明人 钟峰 谭智勇 宋承根 王子龙 张勇

(74)专利代理机构 北京鼎佳达知识产权代理事务所(普通合伙) 11348
代理人 王伟锋 刘铁生

(51)Int.Cl.
H04L 9/08(2006.01)
H04L 9/32(2006.01)
H04L 29/06(2006.01)

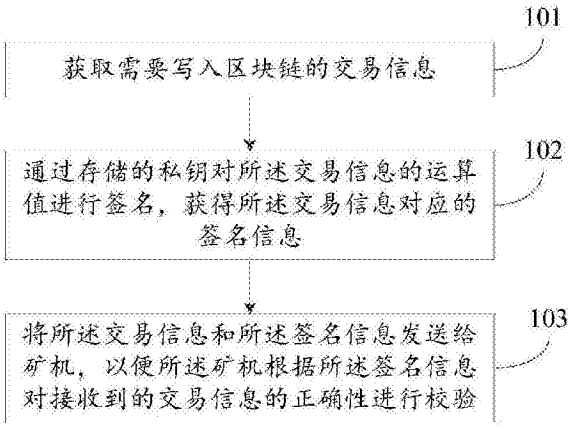
权利要求书3页 说明书11页 附图4页

(54)发明名称

基于区块链技术的交易信息校验方法、装置及系统

(57)摘要

本发明公开了一种基于区块链技术的交易信息校验方法、装置及系统，涉及互联网技术领域，能够对需要写入区块链的交易信息的正确性进行校验，从而防止将被篡改的交易信息写入区块链中。本发明的方法主要包括：获取需要写入区块链的交易信息，所述交易信息由客户端发起的交易操作生成；通过存储的私钥对所述交易信息的运算值进行签名，获得所述交易信息对应的签名信息，所述交易信息的运算值根据预设算法进行运算而得；将所述交易信息和所述签名信息发送给矿机，以便所述矿机根据所述签名信息对接收到的交易信息的正确性进行校验。本发明主要适用于利用区块链存储交易信息的场景中。



CN 106506146 A

1.一种基于区块链技术的交易信息校验方法，所述方法应用于客户平台，其特征在于，所述方法包括：

获取需要写入区块链的交易信息，所述交易信息由客户端发起的交易操作生成；

通过存储的私钥对所述交易信息的运算值进行签名，获得所述交易信息对应的签名信息，所述交易信息的运算值根据预设算法进行运算而得；

将所述交易信息和所述签名信息发送给矿机，以便所述矿机根据所述签名信息对接收到的交易信息的正确性进行校验。

2.根据权利要求1所述的方法，其特征在于，所述方法还包括：

接收所述矿机发送的重发指令；

根据所述重发指令，向所述矿机重新发送所述交易信息和所述签名信息。

3.根据权利要求1所述的方法，其特征在于，在将所述交易信息和所述签名信息发送给矿机之前，所述方法还包括：

向所述矿机发送携带所述客户平台的身份标识信息的身份验证请求；

所述将所述交易信息和所述签名信息发送给矿机包括：

若接收到所述矿机发送的身份验证成功响应消息，则将所述交易信息和所述签名信息发送给所述矿机。

4.根据权利要求1至3中任一项所述的方法，其特征在于，所述客户平台存储的私钥为发起交易操作的客户端发送的私钥，或者为所述客户平台的私钥。

5.一种基于区块链技术的交易信息校验方法，所述方法应用于矿机，其特征在于，所述方法包括：

接收客户平台发送的交易信息和所述交易信息对应的签名信息，所述交易信息由客户端发起的交易操作生成，所述签名信息是通过所述客户平台存储的私钥对所述交易信息的运算值进行签名得到的，所述交易信息的运算值根据预设算法进行运算而得；

根据所述预设算法对接收到的交易信息进行运算，获得所述交易信息的运算值；

根据所述交易信息的运算值、所述签名信息以及所述私钥对应的公钥进行验签；

若验签成功，则确定接收到的交易信息正确，并将包括所述交易信息的新区块写入区块链中。

6.根据权利要求5所述的方法，其特征在于，所述方法还包括：

若验签失败，则删除所述交易信息以及所述签名信息，并输出用于提示接收到的交易信息存在异常的提示信息。

7.根据权利要求5所述的方法，其特征在于，所述方法还包括：

若验签失败，则向所述客户平台发送重发指令，以便所述客户平台根据所述重发指令重新发送交易信息以及所述交易信息对应的签名信息。

8.根据权利要求5所述的方法，其特征在于，所述根据所述交易信息的运算值、所述签名信息以及所述私钥对应的公钥进行验签包括：

利用所述公钥对所述签名信息进行解密，获得解密后的运算值；

将所述交易信息的运算值与所述解密后的运算值进行比较；

若两者相同，则确定验签成功；

若两者不同，则确定验签失败。

9.根据权利要求5所述的方法，其特征在于，在接收客户平台发送的交易信息和所述交易信息对应的签名信息之前，所述方法还包括：

接收所述客户平台发送的身份验证请求，所述身份验证请求中携带有所述客户平台的身份标识信息；

若确认保存有所述客户平台的身份标识信息，则向所述客户平台发送身份验证成功响应消息；

所述接收客户平台发送的交易信息和所述交易信息对应的签名信息包括：

接收所述客户平台根据所述身份验证成功响应消息发送的交易信息和所述交易信息对应的签名信息。

10.根据权利要求5至9中任一项所述的方法，其特征在于，所述客户平台存储的私钥为发起交易操作的客户端发送的私钥，或者为所述客户平台的私钥。

11.一种基于区块链技术的交易信息校验装置，所述装置应用于客户平台，其特征在于，所述装置包括：

获取单元，用于获取需要写入区块链的交易信息，所述交易信息由客户端发起的交易操作生成；

签名单元，用于通过存储的私钥对所述获取单元获取的所述交易信息的运算值进行签名，获得所述交易信息对应的签名信息，所述交易信息的运算值根据预设算法进行运算而得；

发送单元，用于将所述获取单元获取的所述交易信息和所述签名单元获取的所述签名信息发送给矿机，以便所述矿机根据所述签名信息对接收到的交易信息的正确性进行校验。

12.根据权利要求11所述的装置，其特征在于，所述装置还包括：

接收单元，用于接收所述矿机发送的重发指令；

所述发送单元还用于根据所述接收单元接收的所述重发指令，向所述矿机重新发送所述交易信息和所述签名信息。

13.根据权利要求11所述的装置，其特征在于，所述发送单元还用于在将所述交易信息和所述签名信息发送给矿机之前，向所述矿机发送携带所述客户平台的身份标识信息的身份验证请求；

所述发送单元还用于当接收到所述矿机发送的身份验证成功响应消息时，将所述交易信息和所述签名信息发送给所述矿机。

14.根据权利要求11至13中任一项所述的装置，其特征在于，所述客户平台存储的私钥为发起交易操作的客户端发送的私钥，或者为所述客户平台的私钥。

15.一种基于区块链技术的交易信息校验装置，所述装置应用于矿机，其特征在于，所述装置包括：

接收单元，用于接收客户平台发送的交易信息和所述交易信息对应的签名信息，所述交易信息由客户端发起的交易操作生成，所述签名信息是通过所述客户平台存储的私钥对所述交易信息的运算值进行签名得到的，所述交易信息的运算值根据预设算法进行运算而得；

运算单元，用于根据所述预设算法对所述接收单元接收到的交易信息进行运算，获得

所述交易信息的运算值；

验签单元，用于根据所述运算单元获得的所述交易信息的运算值、所述接收单元接收的所述签名信息以及所述私钥对应的公钥进行验签；

写入单元，用于当所述验签单元验签成功时，确定接收到的交易信息正确，并将包括所述交易信息的新区块写入区块链中。

16.根据权利要求15所述的装置，其特征在于，所述装置还包括：

删除单元，用于当所述验签单元验签失败时，删除所述交易信息以及所述签名信息；

输出单元，用于输出用于提示接收到的交易信息存在异常的提示信息。

17.根据权利要求15所述的装置，其特征在于，所述装置还包括：

第一发送单元，用于当所述验签单元验签失败时，向所述客户平台发送重发指令，以便所述客户平台根据所述重发指令重新发送交易信息以及所述交易信息对应的签名信息。

18.根据权利要求15所述的装置，其特征在于，所述验签单元包括：

解密模块，用于利用所述公钥对所述签名信息进行解密，获得解密后的运算值；

比较模块，用于将所述交易信息的运算值与所述解密模块解密后的运算值进行比较；

确定模块，用于当所述比较模块的比较结果为两者相同时，确定验签成功；当所述比较模块的比较结果为两者不同时，确定验签失败。

19.根据权利要求15所述的装置，其特征在于，所述接收单元还用于在接收客户平台发送的交易信息和所述交易信息对应的签名信息之前，接收所述客户平台发送的身份验证请求，所述身份验证请求中携带有所述客户平台的身份标识信息；

所述装置还包括：

第二发送单元，用于当确认保存有所述客户平台的身份标识信息时，向所述客户平台发送身份验证成功响应消息；

所述接收单元还用于接收所述客户平台根据所述身份验证成功响应消息发送的交易信息和所述交易信息对应的签名信息。

20.根据权利要求15至19中任一项所述的装置，其特征在于，所述客户平台存储的私钥为发起交易操作的客户端发送的私钥，或者为所述客户平台的私钥。

21.一种基于区块链技术的交易信息校验系统，其特征在于，所述系统包括客户平台和矿机；其中，所述客户平台包括如权利要求11至14中任一项所述的装置；所述矿机包括如权利要求15至20中任一项所述的装置。

基于区块链技术的交易信息校验方法、装置及系统

技术领域

[0001] 本发明涉及互联网技术领域，特别是涉及一种基于区块链技术的交易信息校验方法、装置及系统。

背景技术

[0002] 随着信息技术的不断发展，互联网的应用也越来越普及，例如，用户可以通过互联网进行网上交易。在通过互联网进行网上交易时，每一笔网上交易一般对应一条或多条交易信息，而交易信息可以反映出用户的交易行为。因此，如何对交易信息进行保存十分关键。

[0003] 在区块链技术中，客户平台生成的交易信息是由具有写入权限的矿机代理写入区块链中实现保存的。具体的，当某客户平台需要将交易信息写入区块链中时，先将该交易信息发送给矿机，然后由该矿机将接收到的交易信息写入区块链中，最后再将写入区块链中的新区块同步至点对点网络中的各个客户平台。

[0004] 然而，交易信息在从客户平台传输至矿机的过程中，可能会被其他设备截获进行篡改，因此若将篡改的交易信息写入区块链中，则会造成写入区块链中的交易信息的可靠性和准确性降低。

发明内容

[0005] 有鉴于此，本发明提供一种基于区块链技术的交易信息校验方法、装置及系统，能够对需要写入区块链的交易信息的正确性进行校验，从而防止将被篡改的交易信息写入区块链中。

[0006] 本发明的目的是采用以下技术方案来实现的：

[0007] 第一方面，本发明提供了一种基于区块链技术的交易信息校验方法，所述方法应用于客户平台，所述方法包括：

[0008] 获取需要写入区块链的交易信息，所述交易信息由客户端发起的交易操作生成；

[0009] 通过存储的私钥对所述交易信息的运算值进行签名，获得所述交易信息对应的签名信息，所述交易信息的运算值根据预设算法进行运算而得；

[0010] 将所述交易信息和所述签名信息发送给矿机，以便所述矿机根据所述签名信息对接收到的交易信息的正确性进行校验。

[0011] 结合第一方面，在第一方面的第一种可能的实现方式中，所述方法还包括：

[0012] 接收所述矿机发送的重发指令；

[0013] 根据所述重发指令，向所述矿机重新发送所述交易信息和所述签名信息。

[0014] 结合第一方面，在第一方面的第二种可能的实现方式中，在将所述交易信息和所述签名信息发送给矿机之前，所述方法还包括：

[0015] 向所述矿机发送携带所述客户平台的身份标识信息的身份验证请求；

[0016] 所述将所述交易信息和所述签名信息发送给矿机包括：

[0017] 若接收到所述矿机发送的身份验证成功响应消息，则将所述交易信息和所述签名信息发送给所述矿机。

[0018] 结合第一方面或者第一方面的第一种或第二种可能的实现方式，在第一方面的第三种可能的实现方式中，所述客户平台存储的私钥为发起交易操作的客户端发送的私钥，或者为所述客户平台的私钥。

[0019] 第二方面，本发明提供了一种基于区块链技术的交易信息校验方法，所述方法应用于矿机，所述方法包括：

[0020] 接收客户平台发送的交易信息和所述交易信息对应的签名信息，所述交易信息由客户端发起的交易操作生成，所述签名信息是通过所述客户平台存储的私钥对所述交易信息的运算值进行签名得到的，所述交易信息的运算值根据预设算法进行运算而得；

[0021] 根据所述预设算法对接收到的交易信息进行运算，获得所述交易信息的运算值；

[0022] 根据所述交易信息的运算值、所述签名信息以及所述私钥对应的公钥进行验签；

[0023] 若验签成功，则确定接收到的交易信息正确，并将包括所述交易信息的新区块写入区块链中。

[0024] 结合第二方面，在第二方面的第一种可能的实现方式中，所述方法还包括：

[0025] 若验签失败，则删除所述交易信息以及所述签名信息，并输出用于提示接收到的交易信息存在异常的提示信息。

[0026] 结合第二方面，在第二方面的第二种可能的实现方式中，所述方法还包括：

[0027] 若验签失败，则向所述客户平台发送重发指令，以便所述客户平台根据所述重发指令重新发送交易信息以及所述交易信息对应的签名信息。

[0028] 结合第二方面，在第二方面的第三种可能的实现方式中，所述根据所述交易信息的运算值、所述签名信息以及所述私钥对应的公钥进行验签包括：

[0029] 利用所述公钥对所述签名信息进行解密，获得解密后的运算值；

[0030] 将所述交易信息的运算值与所述解密后的运算值进行比较；

[0031] 若两者相同，则确定验签成功；

[0032] 若两者不同，则确定验签失败。

[0033] 结合第二方面，在第二方面的第四种可能的实现方式中，在接收客户平台发送的交易信息和所述交易信息对应的签名信息之前，所述方法还包括：

[0034] 接收所述客户平台发送的身份验证请求，所述身份验证请求中携带有所述客户平台的身份标识信息；

[0035] 若确认保存有所述客户平台的身份标识信息，则向所述客户平台发送身份验证成功响应消息；

[0036] 所述接收客户平台发送的交易信息和所述交易信息对应的签名信息包括：

[0037] 接收所述客户平台根据所述身份验证成功响应消息发送的交易信息和所述交易信息对应的签名信息。

[0038] 结合第二方面或者第二方面的第一种至第四种任一项可能的实现方式，在第二方面的第五种可能的实现方式中，所述客户平台存储的私钥为发起交易操作的客户端发送的私钥，或者为所述客户平台的私钥。

[0039] 第三方面，本发明提供了一种基于区块链技术的交易信息校验装置，所述装置应

用于客户平台，所述装置包括：

[0040] 获取单元，用于获取需要写入区块链的交易信息，所述交易信息由客户端发起的交易操作生成；

[0041] 签名单元，用于通过存储的私钥对所述获取单元获取的所述交易信息的运算值进行签名，获得所述交易信息对应的签名信息，所述交易信息的运算值根据预设算法进行运算而得；

[0042] 发送单元，用于将所述获取单元获取的所述交易信息和所述签名单元获取的所述签名信息发送给矿机，以便所述矿机根据所述签名信息对接收到的交易信息的正确性进行校验。

[0043] 结合第三方面，在第三方面的第一种可能的实现方式中，所述装置还包括：

[0044] 接收单元，用于接收所述矿机发送的重发指令；

[0045] 所述发送单元还用于根据所述接收单元接收的所述重发指令，向所述矿机重新发送所述交易信息和所述签名信息。

[0046] 结合第三方面，在第三方面的第二种可能的实现方式中，所述发送单元还用于在将所述交易信息和所述签名信息发送给矿机之前，向所述矿机发送携带所述客户平台的身份标识信息的身份验证请求；

[0047] 所述发送单元还用于当接收到所述矿机发送的身份验证成功响应消息时，将所述交易信息和所述签名信息发送给矿机。

[0048] 结合第三方面获得第三方面的第一种或者第二种可能的实现方式，在第三方面的第三种可能的实现方式中，所述客户平台存储的私钥为发起交易操作的客户端发送的私钥，或者为所述客户平台的私钥。

[0049] 第四方面，本发明提供了一种基于区块链技术的交易信息校验装置，所述装置应用于矿机，所述装置包括：

[0050] 接收单元，用于接收客户平台发送的交易信息和所述交易信息对应的签名信息，所述交易信息由客户端发起的交易操作生成，所述签名信息是通过所述客户平台存储的私钥对所述交易信息的运算值进行签名得到的，所述交易信息的运算值根据预设算法进行运算而得；

[0051] 运算单元，用于根据所述预设算法对所述接收单元接收到的交易信息进行运算，获得所述交易信息的运算值；

[0052] 验签单元，用于根据所述运算单元获得的所述交易信息的运算值、所述接收单元接收的所述签名信息以及所述私钥对应的公钥进行验签；

[0053] 写入单元，用于当所述验签单元验签成功时，确定接收到的交易信息正确，并将包括所述交易信息的新区块写入区块链中。

[0054] 结合第四方面，在第四方面的第一种可能的实现方式中，所述装置还包括：

[0055] 删除单元，用于当所述验签单元验签失败时，删除所述交易信息以及

[0056] 所述签名信息；

[0057] 输出单元，用于输出用于提示接收到的交易信息存在异常的提示信息。

[0058] 结合第四方面，在第四方面的第二种可能的实现方式中，所述装置还包括：

[0059] 第一发送单元，用于当所述验签单元验签失败时，向所述客户平台发送重发指令，

以便所述客户平台根据所述重发指令重新发送交易信息以及所述交易信息对应的签名信息。

[0060] 结合第四方面，在第四方面的第三种可能的实现方式中，所述验签单元包括：

[0061] 解密模块，用于利用所述公钥对所述签名信息进行解密，获得解密后的运算值；

[0062] 比较模块，用于将所述交易信息的运算值与所述解密模块解密后的运算值进行比较；

[0063] 确定模块，用于当所述比较模块的比较结果为两者相同时，确定验签成功；当所述比较模块的比较结果为两者不同时，确定验签失败。

[0064] 结合第四方面，在第四方面的第四种可能的实现方式中，所述接收单元还用于在接收客户平台发送的交易信息和所述交易信息对应的签名信息之前，接收所述客户平台发送的身份验证请求，所述身份验证请求中携带有所述客户平台的身份标识信息；

[0065] 所述装置还包括：

[0066] 第二发送单元，用于当确认保存有所述客户平台的身份标识信息时，向所述客户平台发送身份验证成功响应消息；

[0067] 所述接收单元还用于接收所述客户平台根据所述身份验证成功响应消息发送的交易信息和所述交易信息对应的签名信息。

[0068] 结合第四方面或者第四方面的第一种至第四种可能的实现方式，在第四方面的第五种可能的实现方式中，所述客户平台存储的私钥为发起交易操作的客户端发送的私钥，或者为所述客户平台的私钥。

[0069] 第五方面，本发明提供了一种基于区块链技术的交易信息校验系统，所述系统包括客户平台和矿机；其中，所述客户平台包括如第三方面或者第三方面的第一种至第三种任一项可能实现方式所述的装置；所述矿机包括如如第四方面或者第四方面的第一种至第五种任一项可能实现方式所述的装置。

[0070] 借由上述技术方案，本发明提供的基于区块链技术的交易信息校验方法、装置及系统，能够在客户平台获得交易信息后，不仅将该交易信息发送给矿机，还会为该交易信息配置无法篡改的签名信息，并将签名信息也发送给矿机，从而使得矿机在接收到交易信息和交易信息对应的签名信息后，不直接将交易信息写入区块链中，而是先利用交易信息对应的签名信息对接收到的交易信息的正确性进行校验，当确定接收到的交易信息正确后，才将交易信息写入区块链中，进而可以防止将被篡改的交易信息写入区块链中，由此提高了矿机向区块链中写入的交易信息的可靠性和准确性。

[0071] 上述说明仅是本发明技术方案的概述，为了能够更清楚了解本发明的技术手段，而可依照说明书的内容予以实施，并且为了让本发明的上述和其它目的、特征和优点能够更明显易懂，以下特举本发明的具体实施方式。

附图说明

[0072] 通过阅读下文优选实施方式的详细描述，各种其他的优点和益处对于本领域普通技术人员将变得清楚明了。附图仅用于示出优选实施方式的目的，而并不认为是对本发明的限制。而且在整个附图中，用相同的参考符号表示相同的部件。在附图中：

[0073] 图1示出了本发明实施例提供的一种基于区块链技术的交易信息校验方法的流程

图；

[0074] 图2示出了本发明实施例提供的另一种基于区块链技术的交易信息校验方法的流程图；

[0075] 图3示出了本发明实施例提供的一种区块链交易信息校验的场景示意图；

[0076] 图4示出了本发明实施例提供的一种基于区块链技术的交易信息校验装置的组成框图；

[0077] 图5示出了本发明实施例提供的另一种基于区块链技术的交易信息校验装置的组成框图；

[0078] 图6示出了本发明实施例提供的另一种基于区块链技术的交易信息校验装置的组成框图；

[0079] 图7示出了本发明实施例提供的另一种基于区块链技术的交易信息校验装置的组成框图；

[0080] 图8示出了本发明实施例提供的一种基于区块链技术的交易信息校验系统的示意图。

具体实施方式

[0081] 下面将参照附图更详细地描述本公开的示例性实施例。虽然附图中显示了本公开的示例性实施例，然而应当理解，可以以各种形式实现本公开而不应被这里阐述的实施例所限制。相反，提供这些实施例是为了能够更透彻地理解本公开，并且能够将本公开的范围完整的传达给本领域的技术人员。

[0082] 本发明实施例提供了一种基于区块链技术的交易信息校验方法，所述方法主要应用于客户平台，如图1所示，所述方法主要包括：

[0083] 101、获取需要写入区块链的交易信息；

[0084] 其中，交易信息是由客户端发起的交易操作生成的交易完整记录，主要包括用户ID(Identity，身份标识号码)、项目ID、交易金额、交易时间、客户平台ID等信息。例如，用户基于客户端对项目1投资100元时，客户端会将当前用户的用户ID、项目1的ID以及交易金额100发送给与之对应的服务器(即客户平台)，客户平台接收到这些信息后，会生成对应的、包括用户ID、项目1ID、100元、交易时间、客户平台ID的完整交易记录。另外，交易信息的具体表现形式可以为记录条，也可以为其他形式，本发明实施例对此不做限定。

[0085] 102、通过存储的私钥对所述交易信息的运算值进行签名，获得所述交易信息对应的签名信息；

[0086] 其中，交易信息的运算值根据预设算法进行运算而得；预设算法可以为哈希算法，也可以为其他算法；相应地，运算值可以为哈希值，也可以为其他数值。另外，签名信息具体可以根据需求配置在交易信息的不同位置，例如，可以将签名信息配置在交易信息的头部、尾部等，本发明实施例不做限定。

[0087] 需要说明的是，客户平台存储的私钥可以为发起交易操作的客户端发送的私钥，也可以为客户平台的私钥，具体可以根据具体应用而定，本发明实施例对此不进行限制。例如，当客户平台所服务的用户较少时，可以直接使用客户平台的私钥作为签名时所需的私钥；当客户平台所服务的用户较多时，为了保证用户交易信息的安全性，可以使用用户基于

客户端设置的私钥作为签名时所需的私钥。

[0088] 103、将所述交易信息和所述签名信息发送给矿机，以便所述矿机根据所述签名信息对接收到的交易信息的正确性进行校验。

[0089] 在获得交易信息和交易信息对应的签名信息后，可以将交易信息和签名信息发送给矿机，以使得矿机在接收到交易信息和签名信息后，先利用签名信息对接收到的交易信息的正确性进行校验，当确定接收到的交易信息正确时，才将交易信息写入区块链中，否则不将其写入区块链中。其中，区块链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过去一段预定时间内所有的交易信息，用于验证其信息的有效性和生成下一个区块。

[0090] 本发明实施例提供的基于区块链技术的交易信息校验方法，能够在客户平台获得交易信息后，不仅将该交易信息发送给矿机，还会为该交易信息配置无法篡改的签名信息，并将签名信息也发送给矿机，从而使得矿机在接收到交易信息和交易信息对应的签名信息后，不直接将交易信息写入区块链中，而是先利用交易信息对应的签名信息对接收到的交易信息的正确性进行校验，当确定接收到的交易信息正确后，才将交易信息写入区块链中，进而可以防止将被篡改的交易信息写入区块链中，由此提高了矿机向区块链中写入的交易信息的可靠性和准确性。

[0091] 进一步的，为了在矿机确定接收到的交易信息错误的情况下，继续获得正确的交易信息，可以在确定接收到的交易信息错误后，向客户平台发送重发指令，以使得客户平台在接收到矿机发送的重发指令后，可以根据该重发指令重新发送交易信息和交易信息对应的签名信息。

[0092] 进一步的，矿机为了防止非法客户平台与其进行交互，可以先对将要与其进行交互的客户平台进行身份合法性验证，当确定其身份合法时，才与其进行交互。

[0093] 具体的，在将所述交易信息和所述签名信息发送给矿机之前，客户平台可以向所述矿机发送携带所述客户平台的身份标识信息的身份验证请求，当接收到所述矿机发送的身份验证成功响应消息时，将所述交易信息和所述签名信息发送给矿机。其中，身份标识信息用于唯一标识客户平台的身份，具体可以为客户平台名、端口IP地址等，本发明实施例不做限定。

[0094] 此外，矿机中还存储有预先注册的用户ID，在接收到客户平台发送的交易信息和签名信息后，可以从交易信息中获取用户ID，然后判断该用户ID是否为预先注册的用户ID，由此来验证用户身份的合法性，并且当确定该用户ID合法时，才继续利用签名信息对交易信息的正确性进行校验。

[0095] 进一步的，依据图1所示的方法，本发明的另一个实施例还提供了一种基于区块链技术的交易信息校验方法，所述方法主要应用于矿机，如图2所示，所述方法主要包括：

[0096] 201、接收客户平台发送的交易信息和所述交易信息对应的签名信息；

[0097] 其中，交易信息由客户端发起的交易操作生成，且关于交易信息的具体内容详见上述步骤101的详细描述，在此不再赘述。

[0098] 签名信息是通过客户平台存储的私钥对交易信息的运算值进行签名得到的。其中，客户平台存储的私钥可以为发起交易操作的客户端发送的私钥，也可以为客户平台的私钥。交易信息的运算值根据预设算法进行运算而得；预设算法可以为哈希算法，也可以为

其他算法，在此不做限定。

[0099] 202、根据所述预设算法对接收到的交易信息进行运算，获得所述交易信息的运算值；

[0100] 其中，当所述预设算法为哈希算法时，本步骤具体为：根据哈希算法对接收到的交易信息进行运算，获得该交易信息的哈希值。

[0101] 203、根据所述交易信息的运算值、所述签名信息以及所述私钥对应的公钥进行验签；

[0102] 具体的，矿机先利用所述公钥对所述签名信息进行解密，获得解密后的运算值；然后将所述交易信息的运算值与所述解密后的运算值进行比较；若两者相同，则确定验签成功；若两者不同，则确定验签失败。其中，矿机中存储有各个客户平台存储的私钥所对应的公钥。

[0103] 当预设算法为哈希算法时，本步骤具体可以为：先利用客户平台签名时所使用的私钥对应的公钥对接收到的签名信息进行解密，获得解密后的哈希值；然后将接收到的交易信息的哈希值与解密后的哈希值进行比较；若这两个哈希值相同，则确定验签成功；若这两个哈希值不相同，则确定验签失败。

[0104] 204、若验签成功，则确定接收到的交易信息正确，并将包括所述交易信息的新区块写入区块链中。

[0105] 当验签成功时，矿机可以确定接收到的交易信息与客户平台发送给矿机的交易信息相同，从而确定接收到的交易信息正确，并可以将包括交易信息的新区块写入区块链中；当验签失败时，可以确定接收到的交易信息与客户平台发送给矿机的交易信息不相同，从而确定接收到的交易信息错误，不将包括将该交易信息的新区块写入区块链中。

[0106] 需要说明的是，新区块中除了包括交易信息外，还可以包括签名信息、时间戳、上一区块的运算值(如哈希值)等信息。其中，若将交易信息对应的签名信息也写入区块链中，则可以在矿机将新区块发送给点对点网络中的各个客户平台后，各个客户平台可以根据签名信息对新区块中的交易信息的正确性进行校验，以判断矿机在将交易信息写入区块链时是否对交易信息进行篡改。

[0107] 本发明实施例提供的基于区块链技术的交易信息校验方法，能够在客户平台获得交易信息后，不仅将该交易信息发送给矿机，还会为该交易信息配置无法篡改的签名信息，并将签名信息也发送给矿机，从而使得矿机在接收到交易信息和交易信息对应的签名信息后，不直接将交易信息写入区块链中，而是先利用交易信息对应的签名信息对接收到的交易信息的正确性进行校验，当确定接收到的交易信息正确后，才将交易信息写入区块链中，进而可以防止将被篡改的交易信息写入区块链中，由此提高了矿机向区块链中写入的交易信息的可靠性和准确性。

[0108] 进一步的，为了防止错误的交易信息占用矿机的存储空间，在确定验签失败后，可以将接收到的交易信息和签名信息删除。为了提示矿机的管理员及时获知矿机接收到的交易信息存在异常，还可以输出用于提示接收到的交易信息存在异常的提示信息。为了在确定验签失败的情况下，继续获得正确的交易信息，可以在确定验签失败后，向客户平台发送重发指令，以便客户平台根据该重发指令重新发送交易信息以及该交易信息对应的签名信息。

[0109] 进一步的，为了防止非法客户平台与矿机进行交互，从而导致非法交易信息写入区块链，矿机可以先对客户平台的身份进行验证，当确定其身份合法时，再接收其发送的的交易信息和签名信息。

[0110] 具体的，在接收客户平台发送的交易信息和所述交易信息对应的签名信息之前，矿机可以先接收所述客户平台发送的身份验证请求，所述身份验证请求中携带有所述客户平台的身份标识信息；若确认保存有所述客户平台的身份标识信息，则向所述客户平台发送身份验证成功响应消息，并接收所述客户平台根据所述身份验证成功响应消息发送的交易信息和所述交易信息对应的签名信息。

[0111] 通过上述实施例可知，以哈希算法进行运算为例，在实现区块链交易信息正确性校验的过程中，涉及的签名和验签过程可以如图3所示。具体的，当客户平台生成交易信息后，可以利用哈希算法对该交易信息进行哈希运算，获得哈希值，然后利用存储的私钥对该哈希值进行签名，获得交易信息对应的签名信息，并将交易信息和签名信息发送给矿机；矿机接收到客户平台发送的交易信息和签名信息后，先利用哈希算法对接收到的交易信息进行哈希运算获得哈希值，然后根据客户平台进行签名时所使用的私钥所对应的公钥、接收到的交易信息的哈希值以及签名信息进行验签操作，以确定接收到的交易信息是否正确，并且在确定正确时，才将包括交易信息和签名信息的区块n与区块n-1进行连接，从而使得交易信息和签名信息写入区块链中。

[0112] 进一步的，依据图1所示的方法，本发明的另一个实施例还提供了一种一种基于区块链技术的交易信息校验装置，所述装置应用于客户平台，如图4所示，所述装置主要包括：

[0113] 获取单元31，用于获取需要写入区块链的交易信息，所述交易信息由客户端发起的交易操作生成；

[0114] 签名单元32，用于通过存储的私钥对所述获取单元31获取的所述交易信息的运算值进行签名，获得所述交易信息对应的签名信息，所述交易信息的运算值根据预设算法进行运算而得；

[0115] 发送单元33，用于将所述获取单元31获取的所述交易信息和所述签名单元获取的所述签名信息发送给矿机，以便所述矿机根据所述签名信息对接收到的交易信息的正确性进行校验。

[0116] 进一步的，如图5所示，所述装置还包括：

[0117] 接收单元34，用于接收所述矿机发送的重发指令；

[0118] 所述发送单元33还用于根据所述接收单元34接收的所述重发指令，向所述矿机重新发送所述交易信息和所述签名信息。

[0119] 进一步的，所述发送单元33还用于在将所述交易信息和所述签名信息发送给矿机之前，向所述矿机发送携带所述客户平台的身份标识信息的身份验证请求；

[0120] 所述发送单元33还用于当接收到所述矿机发送的身份验证成功响应消息时，将所述交易信息和所述签名信息发送给矿机。

[0121] 进一步的，所述客户平台存储的私钥为发起交易操作的客户端发送的私钥，或者为所述客户平台的私钥。

[0122] 本发明实施例提供的基于区块链技术的交易信息校验装置，能够在客户平台获得交易信息后，不仅将该交易信息发送给矿机，还会为该交易信息配置无法篡改的签名信息，

并将签名信息也发送给矿机，从而使得矿机在接收到交易信息和交易信息对应的签名信息后，不直接将交易信息写入区块链中，而是先利用交易信息对应的签名信息对接收到的交易信息的正确性进行校验，当确定接收到的交易信息正确后，才将交易信息写入区块链中，进而可以防止将被篡改的交易信息写入区块链中，由此提高了矿机向区块链中写入的交易信息的可靠性和准确性。

[0123] 进一步的，依据图2所示的方法，本发明的另一个实施例还提供了一种基于区块链技术的交易信息校验装置，所述装置主要应用于矿机，如图6所示，所述装置包括：

[0124] 接收单元41，用于接收客户平台发送的交易信息和所述交易信息对应的签名信息，所述交易信息由客户端发起的交易操作生成，所述签名信息是通过所述客户平台存储的私钥对所述交易信息的运算值进行签名得到的，所述交易信息的运算值根据预设算法进行运算而得；

[0125] 运算单元42，用于根据所述预设算法对所述接收单元41接收到的交易信息进行运算，获得所述交易信息的运算值；

[0126] 验签单元43，用于根据所述运算单元42获得的所述交易信息的运算值、所述接收单元接收的所述签名信息以及所述私钥对应的公钥进行验签；

[0127] 写入单元44，用于当所述验签单元43验签成功时，确定接收到的交易信息正确，并将包括所述交易信息的新区块写入区块链中。

[0128] 进一步的，如图7所示，所述装置还包括：

[0129] 删除单元45，用于当所述验签单元43验签失败时，删除所述交易信息以及所述签名信息；

[0130] 输出单元46，用于输出用于提示接收到的交易信息存在异常的提示信息。

[0131] 进一步的，如图7所示，所述装置还包括：

[0132] 第一发送单元47，用于当所述验签单元43验签失败时，向所述客户平台发送重发指令，以便所述客户平台根据所述重发指令重新发送交易信息以及所述交易信息对应的签名信息。

[0133] 进一步的，如图7所示，所述验签单元43包括：

[0134] 解密模块431，用于利用所述公钥对所述签名信息进行解密，获得解密后的运算值；

[0135] 比较模块432，用于将所述交易信息的运算值与所述解密模块解密后的运算值进行比较；

[0136] 确定模块433，用于当所述比较模块432的比较结果为两者相同时，确定验签成功；当所述比较模块432的比较结果为两者不同时，确定验签失败。

[0137] 进一步的，所述接收单元41还用于在接收客户平台发送的交易信息和所述交易信息对应的签名信息之前，接收所述客户平台发送的身份验证请求，所述身份验证请求中携带有所述客户平台的身份标识信息；

[0138] 如图7所示，所述装置还包括：

[0139] 第二发送单元48，用于当确认保存有所述客户平台的身份标识信息时，向所述客户平台发送身份验证成功响应消息；

[0140] 所述接收单元41还用于接收所述客户平台根据所述身份验证成功响应消息发送

的交易信息和所述交易信息对应的签名信息。

[0141] 进一步的，如图7所示，所述客户平台存储的私钥为发起交易操作的客户端发送的私钥，或者为所述客户平台的私钥。

[0142] 本发明实施例提供的基于区块链技术的交易信息校验装置，能够在客户平台获得交易信息后，不仅将该交易信息发送给矿机，还会为该交易信息配置无法篡改的签名信息，并将签名信息也发送给矿机，从而使得矿机在接收到交易信息和交易信息对应的签名信息后，不直接将交易信息写入区块链中，而是先利用交易信息对应的签名信息对接收到的交易信息的正确性进行校验，当确定接收到的交易信息正确后，才将交易信息写入区块链中，进而可以防止将被篡改的交易信息写入区块链中，由此提高了矿机向区块链中写入的交易信息的可靠性和准确性。

[0143] 进一步的，依据上述装置实施例，本发明的另一个实施例还提供了一种基于区块链技术的交易信息校验系统，如图8所示，所述系统包括客户平台51和矿机52；其中，所述客户平台51包括如图4或5所示的装置；所述矿机52包括如图6或7所示的装置。

[0144] 本发明实施例提供的基于区块链技术的交易信息校验系统，能够在客户平台获得交易信息后，不仅将该交易信息发送给矿机，还会为该交易信息配置无法篡改的签名信息，并将签名信息也发送给矿机，从而使得矿机在接收到交易信息和交易信息对应的签名信息后，不直接将交易信息写入区块链中，而是先利用交易信息对应的签名信息对接收到的交易信息的正确性进行校验，当确定接收到的交易信息正确后，才将交易信息写入区块链中，进而可以防止将被篡改的交易信息写入区块链中，由此提高了矿机向区块链中写入的交易信息的可靠性和准确性。

[0145] 在上述实施例中，对各个实施例的描述都各有侧重，某个实施例中没有详述的部分，可以参见其他实施例的相关描述。

[0146] 可以理解的是，上述方法及装置中的相关特征可以相互参考。另外，上述实施例中的“第一”、“第二”等是用于区分各实施例，而并不代表各实施例的优劣。

[0147] 所属领域的技术人员可以清楚地了解到，为描述的方便和简洁，上述描述的系统，装置和单元的具体工作过程，可以参考前述方法实施例中的对应过程，在此不再赘述。

[0148] 在此提供的算法和显示不与任何特定计算机、虚拟系统或者其它设备固有相关。各种通用系统也可以与基于在此的示教一起使用。根据上面的描述，构造这类系统所要求的结构是显而易见的。此外，本发明也不针对任何特定编程语言。应当明白，可以利用各种编程语言实现在此描述的本发明的内容，并且上面对特定语言所做的描述是为了披露本发明的最佳实施方式。

[0149] 在此处所提供的说明书中，说明了大量具体细节。然而，能够理解，本发明的实施例可以在没有这些具体细节的情况下实践。在一些实例中，并未详细示出公知的方法、结构和技术，以便不模糊对本说明书的理解。

[0150] 类似地，应当理解，为了精简本公开并帮助理解各个发明方面中的一个或多个，在上面对本发明的示例性实施例的描述中，本发明的各个特征有时被一起分组到单个实施例、图、或者对其的描述中。然而，并不应将该公开的方法解释成反映如下意图：即所要求保护的本发明要求比在每个权利要求中所明确记载的特征更多的特征。更确切地说，如下面的权利要求书所反映的那样，发明方面在于少于前面公开的单个实施例的所有特征。因此，

遵循具体实施方式的权利要求书由此明确地并入该具体实施方式，其中每个权利要求本身都作为本发明的单独实施例。

[0151] 本领域那些技术人员可以理解，可以对实施例中的设备中的模块进行自适应性地改变并且把它们设置在与该实施例不同的一个或多个设备中。可以把实施例中的模块或单元或组件组合成一个模块或单元或组件，以及此外可以把它们分成多个子模块或子单元或子组件。除了这样的特征和/或过程或者单元中的至少一些是相互排斥之外，可以采用任何组合对本说明书(包括伴随的权利要求、摘要和附图)中公开的所有特征以及如此公开的任何方法或者设备的所有过程或单元进行组合。除非另外明确陈述，本说明书(包括伴随的权利要求、摘要和附图)中公开的每个特征可以由提供相同、等同或相似目的的替代特征来代替。

[0152] 此外，本领域的技术人员能够理解，尽管在此所述的一些实施例包括其它实施例中所包括的某些特征而不是其它特征，但是不同实施例的特征的组合意味着处于本发明的范围之内并且形成不同的实施例。例如，在下面的权利要求书中，所要求保护的实施例的任意之一都可以以任意的组合方式来使用。

[0153] 本发明的各个部件实施例可以以硬件实现，或者以在一个或者多个处理器上运行的软件模块实现，或者以它们的组合实现。本领域的技术人员应当理解，可以在实践中使用微处理器或者数字信号处理器(DSP)来实现根据本发明实施例的基于区块链技术的交易信息校验方法、装置及系统中的一些或者全部部件的一些或者全部功能。本发明还可以实现为用于执行这里所描述的方法的一部分或者全部的设备或者装置程序(例如，计算机程序和计算机程序产品)。这样的实现本发明的程序可以存储在计算机可读介质上，或者可以具有一个或者多个信号的形式。这样的信号可以从因特网网站上下载得到，或者在载体信号上提供，或者以任何其他形式提供。

[0154] 应该注意的是上述实施例对本发明进行说明而不是对本发明进行限制，并且本领域技术人员在不脱离所附权利要求的范围的情况下可设计出替换实施例。在权利要求中，不应将位于括号之间的任何参考符号构造成对权利要求的限制。单词“包含”不排除存在未列在权利要求中的元件或步骤。位于元件之前的单词“一”或“一个”不排除存在多个这样的元件。本发明可以借助于包括有若干不同元件的硬件以及借助于适当编程的计算机来实现。在列举了若干装置的单元权利要求中，这些装置中的若干个可以是通过同一个硬件项来具体体现。单词第一、第二、以及第三等的使用不表示任何顺序。可将这些单词解释为名称。

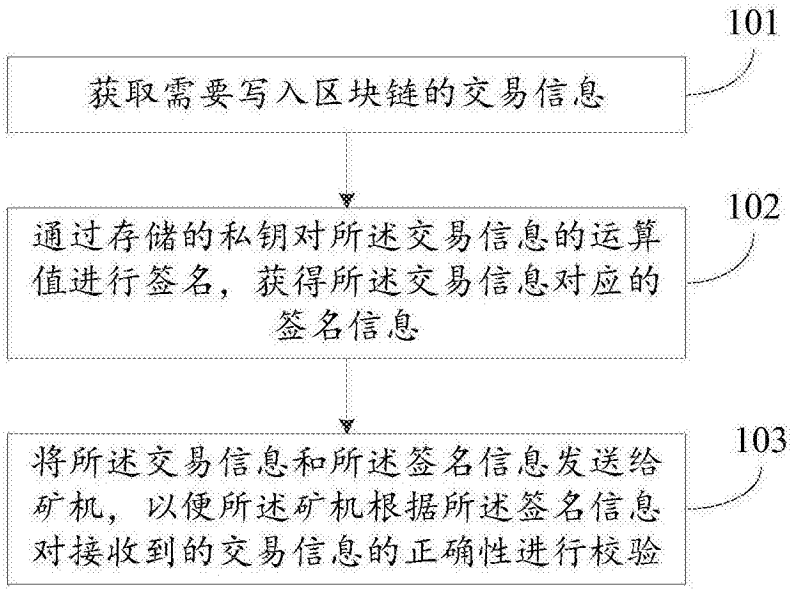

101
获取需要写入区块链的交易信息
102
通过存储的私钥对所述交易信息的运算值进行签名，获得所述交易信息对应的签名信息
103
将所述交易信息和所述签名信息发送给矿机，以便所述矿机根据所述签名信息对接收到的交易信息的正确性进行校验

图1

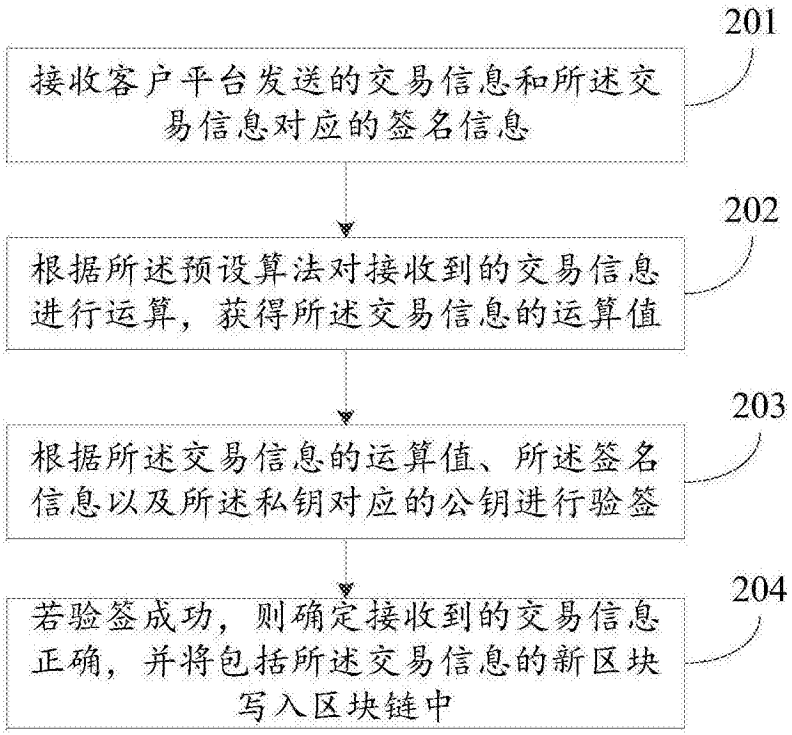

201
接收客户平台发送的交易信息和所述交易信息对应的签名信息
202
根据所述预设算法对接收到的交易信息进行运算，获得所述交易信息的运算值
203
根据所述交易信息的运算值、所述签名信息以及所述私钥对应的公钥进行验签
204
若验签成功，则确定接收到的交易信息正确，并将包括所述交易信息的新区块写入区块链中

图2

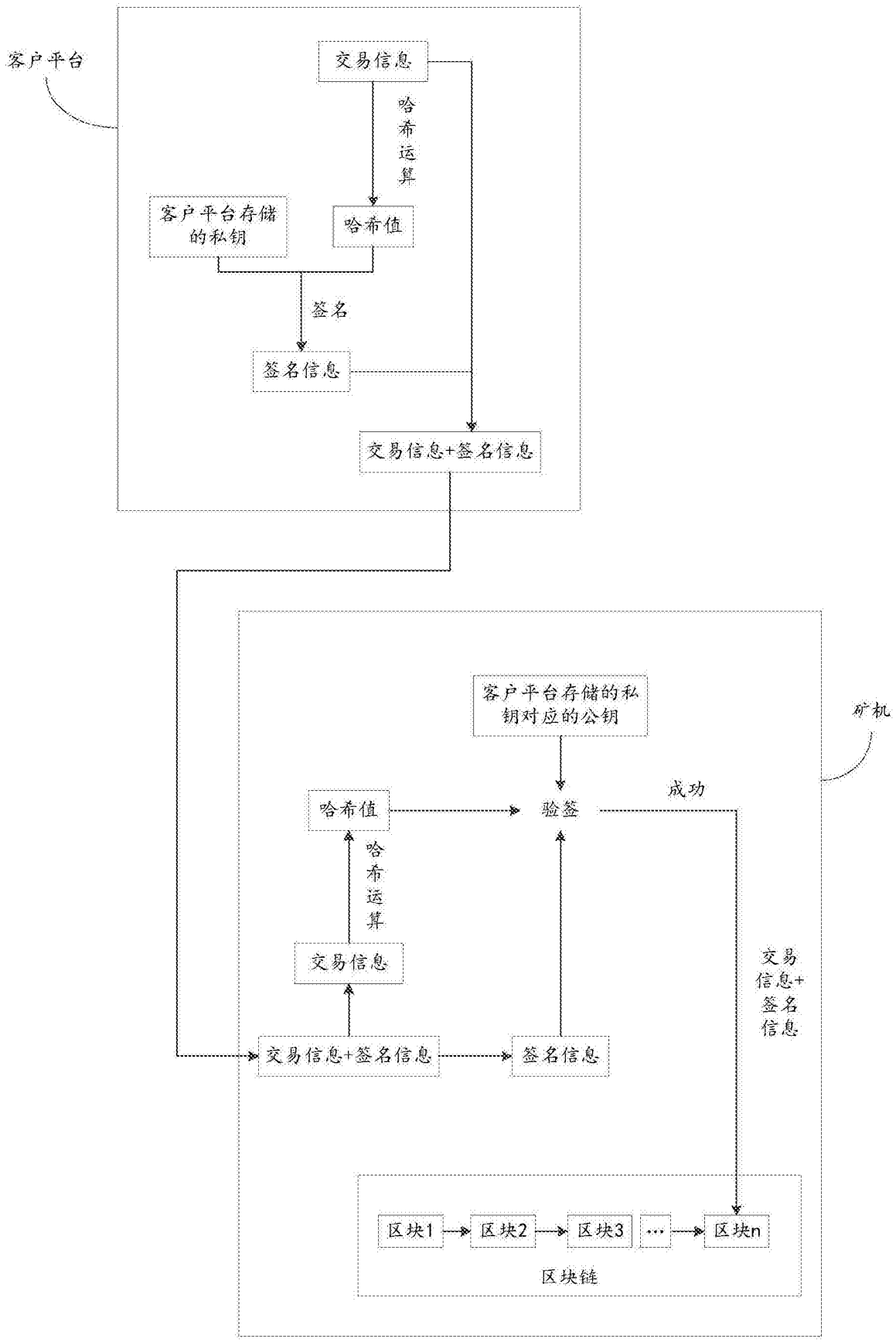

客户平台
交易信息
哈希运算
客户平台存储的私钥
哈希值
签名
签名信息
交易信息+签名信息
矿机
客户平台存储的私钥对应的公钥
哈希值
验签
成功
哈希运算
交易信息
交易信息+签名信息
交易信息+签名信息
签名信息
区块1
区块2
区块3
…
区块n
区块链

图3

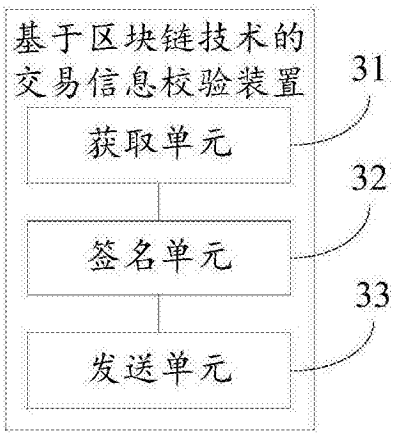

基于区块链技术的交易信息校验装置
31
获取单元
32
签名单元
33
发送单元

图4

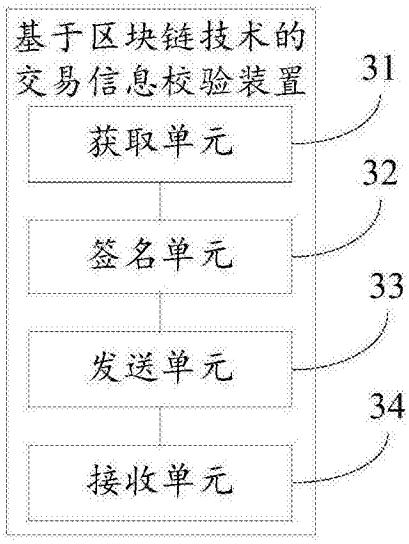

基于区块链技术的交易信息校验装置
31
获取单元
32
签名单元
33
发送单元
34
接收单元

图5

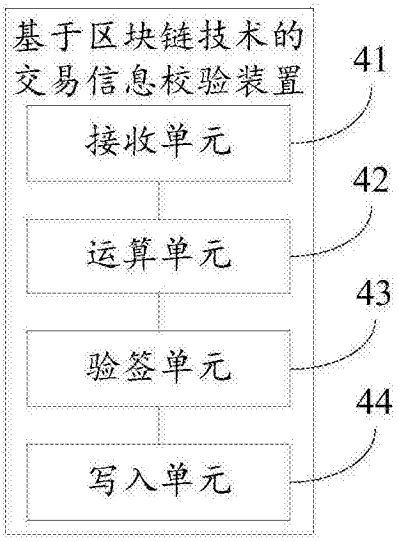

基于区块链技术的交易信息校验装置
41
接收单元
42
运算单元
43
验签单元
44
写入单元

图6

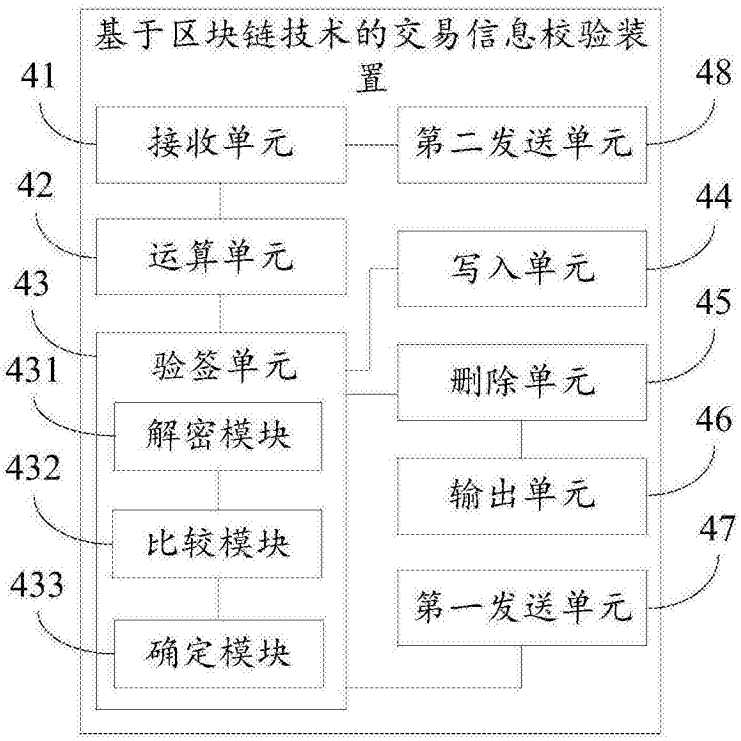

基于区块链技术的交易信息校验装置
41
接收单元
48
第二发送单元
42
运算单元
44
写入单元
43
验签单元
45
删除单元
431
解密模块
46
输出单元
432
比较模块
47
第一发送单元
433
确定模块

图7

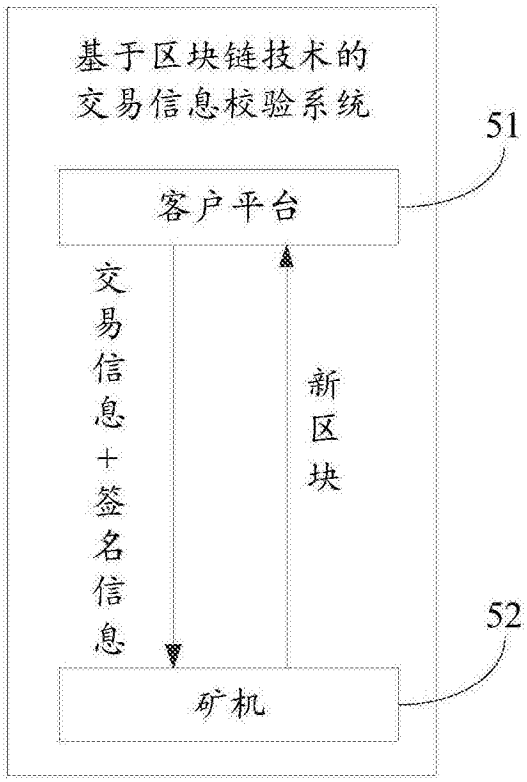


图8