(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 110289946 A
(43)申请公布日 2019.09.27

(21)申请号 201910633225.3

(22)申请日 2019.07.12

(71)申请人 深圳市元征科技股份有限公司
地址 518000 广东省深圳市龙岗区坂田街道五和大道北4012元征工业园

(72)发明人 刘新 侯利朋

(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 郝传鑫 熊永强

(51)Int.Cl.
H04L 9/06(2006.01)
H04L 9/08(2006.01)
H04L 9/30(2006.01)

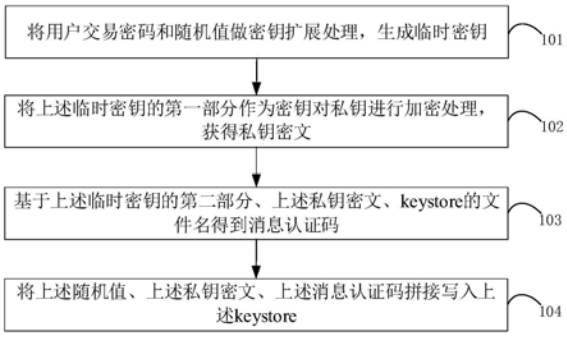
权利要求书2页 说明书9页 附图6页

(54)发明名称

一种区块链钱包本地化文件的生成方法及区块链节点设备

(57)摘要

一种区块链钱包本地化文件的生成方法及区块链节点设备。该方法包括:将用户交易密码和随机值做密钥扩展处理,生成临时密钥;将上述临时密钥的第一部分作为密钥对私钥进行加密处理,获得私钥密文;基于上述临时密钥的第二部分、上述私钥密文、keystore的文件名得到消息认证码;将上述随机值、上述私钥密文、上述消息认证码拼接写入上述keystore。实施本申请,可以优化keystore生成存储流程,大大减少了文件中的冗余信息,解决了keystore文件占用空间大的问题。



CN 110289946 A

1.一种区块链钱包本地化文件的生成方法,其特征在于,所述方法包括:

将用户交易密码和随机值做密钥扩展处理,生成临时密钥;

将所述临时密钥的第一部分作为密钥对私钥进行加密处理,获得私钥密文;

基于所述临时密钥的第二部分、所述私钥密文、keystore的文件名得到消息认证码;

将所述随机值、所述私钥密文、所述消息认证码拼接写入所述keystore。

2.根据权利要求1所述的方法,其特征在于,所述将用户交易密码和随机值做密钥扩展处理之前,还包括:

生成随机种子;

根据所述随机种子生成私钥和区块链钱包地址。

3.根据权利要求2所述的方法,其特征在于,所述将所述临时密钥的第一部分作为密钥对私钥进行加密处理,获得私钥密文,包括:

截取所述临时密钥的第一部分作为密钥,将所述随机值作为加密参数;

利用所述密钥与所述加密参数对所述私钥进行加密,获得私钥密文。

4.根据权利要求3所述的方法,其特征在于,所述基于所述临时密钥的第二部分、所述私钥密文、keystore的文件名得到消息认证码之前,还包括:

将所述keystore的生成时间与所述区块链钱包地址拼接后作为所述keystore的文件名。

5.根据权利要求1所述的方法,其特征在于,所述基于所述临时密钥的第二部分、所述私钥密文、keystore的文件名得到消息认证码,包括:

将所述临时密钥的第二部分、所述私钥密文、所述keystore的文件名进行拼接并加密运算,获得结果;

截取所述结果的目标部分作为消息认证码。

6.根据权利要求1至5任意一项所述的方法,其特征在于,所述将所述随机值、所述私钥密文、所述消息认证码拼接写入所述keystore,包括:

将所述随机值、所述私钥密文、所述消息认证码进行拼接,获得拼接结果;

对所述拼接结果添加标签,并以二进制方式写入所述keystore。

7.一种区块链节点设备,其特征在于,所述设备包括:

扩展单元,用于将用户交易密码和随机值做密钥扩展处理,生成临时密钥;

加密单元,用于将所述临时密钥的第一部分作为密钥对私钥进行加密处理,获得私钥密文;

第一拼接单元,用于基于所述临时密钥的第二部分、所述私钥密文、keystore的文件名得到消息认证码;

第二拼接单元,用于将所述随机值、所述私钥密文、所述消息认证码拼接写入所述keystore。

8.根据权利要求7所述的设备,其特征在于,

所述加密单元,具体用于截取所述临时密钥的第一部分作为密钥,将所述随机值作为加密参数;利用所述密钥与所述加密参数对所述私钥进行加密,获得私钥密文。

9.一种区块链节点设备,其特征在于,包括处理器、存储器和收发器;其中,所述存储器用于存储计算机程序,所述计算机程序包括程序指令,所述处理器被配置用于调用所述程

序指令，执行如权利要求1至6任一项所述的方法。

10.一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存储有计算机程序，所述计算机程序包括程序指令，所述程序指令当被处理器执行时，使所述处理器执行如权利要求1至6任一项所述的方法。

一种区块链钱包本地化文件的生成方法及区块链节点设备

技术领域

[0001] 本申请涉及区块链技术领域，尤其涉及一种区块链钱包本地化文件的生成方法及区块链节点设备。

背景技术

[0002] 随着区块链技术的发展，针对虚拟货币的区块链钱包应运而生。而区块链钱包的本地化文件keystore得到了越来越广泛的应用。

[0003] 现有的区块链系统中，单个keystore文件大小为491字节，占用大量存储空间。对于交易所等拥有大量区块链钱包的场景，存在过多的冗余信息，造成大量的存储空间浪费。

[0004] 本申请提出一种新的keystore生成存储方案，优化keystore生成，存储流程，解决keystore文件占用空间大的问题。

发明内容

[0005] 本申请提出一种区块链钱包本地化文件的生成方法及区块链节点设备，可以优化keystore生成存储流程，并采用TV格式(标签:数值)二进制存储数据，大大减少了文件中的冗余信息，解决了keystore文件占用空间大的问题。通过区块链钱包地址拼接世界标准时间作为文件名，可以在毫秒级控制区块链钱包的唯一性。通过对文件名和文件内容中的私钥密文作摘要，保证了文件名和文件内容的一致性，避免被非法篡改。

[0006] 第一方面，本申请提出一种区块链钱包本地化文件的生成方法，所述方法包括：

[0007] 将用户交易密码和随机值做密钥扩展处理，生成临时密钥；

[0008] 将所述临时密钥的第一部分作为密钥对私钥进行加密处理，获得私钥密文；

[0009] 基于所述临时密钥的第二部分、所述私钥密文、keystore的文件名得到消息认证码；

[0010] 将所述随机值、所述私钥密文、所述消息认证码拼接写入所述keystore。

[0011] 在一种可能的实现方式中，所述将用户交易密码和随机值做密钥扩展处理之前，所述方法还包括：

[0012] 生成随机种子；

[0013] 根据所述随机种子生成私钥和区块链钱包地址。

[0014] 在一种可能的实现方式中，所述将所述临时密钥的第一部分作为密钥对私钥进行加密处理，获得私钥密文，所述方法包括：

[0015] 截取所述临时密钥的第一部分作为密钥，将所述随机值作为加密参数；

[0016] 利用所述密钥与所述加密参数对所述私钥进行加密，获得私钥密文。

[0017] 在一种可能的实现方式中，所述基于所述临时密钥的第二部分、所述私钥密文、所述keystore的文件名得到消息认证码之前，所述方法还包括：

[0018] 将所述keystore的生成时间与所述区块链钱包地址拼接后作为所述keystore的文件名。

[0019] 在一种可能的实现方式中，所述基于所述临时密钥的第二部分、所述私钥密文、所述keystore的文件名得到消息认证码，所述方法包括：

[0020] 将所述临时密钥的第二部分、所述私钥密文、所述keystore的文件名进行拼接并加密运算，获得结果；

[0021] 截取所述结果的目标部分作为消息认证码。

[0022] 在一种可能的实现方式中，所述将所述随机值、所述私钥密文、所述消息认证码拼接写入所述keystore，所述方法包括：

[0023] 将所述随机值、所述私钥密文、所述消息认证码进行拼接，获得拼接结果；

[0024] 对所述拼接结果添加标签，并以二进制方式写入所述keystore。

[0025] 第二方面，本申请提出一种区块链节点设备，所述设备包括：

[0026] 扩展单元，用于将用户交易密码和随机值做密钥扩展处理，生成临时密钥；

[0027] 加密单元，用于将所述临时密钥的第一部分作为密钥对私钥进行加密处理，获得私钥密文；

[0028] 第一拼接单元，用于基于所述临时密钥的第二部分、所述私钥密文、所述keystore的文件名得到消息认证码；

[0029] 第二拼接单元，用于将所述随机值、所述私钥密文、所述消息认证码拼接写入所述keystore。

[0030] 在一种可能的实现方式中，所述设备还包括：

[0031] 第一生成单元，用于生成随机种子；

[0032] 第二生成单元，用于根据所述随机种子生成私钥和区块链钱包地址。

[0033] 在一种可能的实现方式中，所述加密单元，具体用于截取所述临时密钥的第一部分作为密钥，将所述随机值作为加密参数；利用所述密钥与所述加密参数对所述私钥进行加密，获得私钥密文。

[0034] 在一种可能的实现方式中，所述设备还包括：

[0035] 第三拼接单元，用于将所述keystore的生成时间与所述区块链钱包地址拼接后作为所述keystore的文件名。

[0036] 在一种可能的实现方式中，所述第一拼接单元，具体用于将所述临时密钥的第二部分、所述私钥密文、所述keystore的文件名进行拼接并加密运算，获得结果；截取所述结果的目标部分作为消息认证码。

[0037] 在一种可能的实现方式中，所述第二拼接单元，具体用于将所述随机值、所述私钥密文、所述消息认证码进行拼接，获得拼接结果；对所述拼接结果添加标签，并以二进制方式写入所述keystore。

[0038] 第三方面，本申请提出一种区块链节点设备，包括：处理器、存储器和收发器；其中，所述存储器用于存储计算机程序，所述计算机程序包括程序指令，所述处理器被配置用于调用所述程序指令，执行如第一方面所提出的方法。

[0039] 第四方面，本申请提出一种计算机可读存储介质，所述计算机可读存储介质存储有计算机程序，所述计算机程序包括程序指令，所述程序指令当被处理器执行时，使所述处理器执行所述第一方面所提出的方法。

[0040] 第五方面，本申请实施例提供了一种包含程序指令的计算机程序产品，当其在计

算机上运行时，使得计算机执行所述第一方面所提出的方法。

[0041] 实施本申请，可以优化keystore生成存储流程，并采用TV格式(标签:数值)二进制存储数据，大大减少了文件中的冗余信息，解决了keystore文件占用空间大的问题。通过区块链钱包地址拼接世界标准时间作为文件名，可以在毫秒级控制区块链钱包的唯一性。通过对文件名和文件内容中的私钥密文作摘要，保证了文件名和文件内容的一致性，避免被非法篡改。

附图说明

[0042] 为了更清楚地说明本申请实施例或背景技术中的技术方案，下面将对本申请实施例或背景技术中所需要使用的附图进行说明。

[0043] 图1是本申请提出的一种区块链钱包本地化文件的生成方法的流程图；

[0044] 图2是本申请提出的另一种区块链钱包本地化文件的生成方法的流程图；

[0045] 图3是本申请提出的一种区块链钱包本地化文件的生成方法的具体应用场景的流程图；

[0046] 图4是本申请提出的另一种区块链钱包本地化文件的生成方法的具体应用场景的流程图；

[0047] 图5是本申请提出的一种区块链节点设备的结构示意图；

[0048] 图6是本申请提出的另一种区块链节点设备的结构示意图。

具体实施方式

[0049] 本申请的说明书和权利要求书及上述附图中的术语“第一”、“第二”等是用于区别不同的对象，而不是用于描述特定顺序。此外，术语“包括”和“具有”以及它们任何变形，意图在于覆盖不排他的包含。例如包含了一系列步骤或单元的过程、方法、系统、产品或设备没有限定于已列出的步骤或单元，而是可选地还包括没有列出的步骤或单元，或可选地还包括对于这些过程、方法或设备固有的其他步骤或单元。

[0050] 现有的区块链系统中，单个keystore文件大小为491字节，占用大量存储空间。对于交易所等拥有大量区块链钱包的场景，存在过多的冗余信息，造成大量的存储空间浪费。

[0051] 本申请，可以优化keystore生成存储流程，并采用TV格式(标签:数值)二进制存储数据，大大减少了文件中的冗余信息，解决了keystore文件占用空间大的问题。

[0052] 图1是本申请提出的一种区块链钱包本地化文件的生成方法的流程图，应用于区块链节点设备，上述方法包括以下内容：

[0053] 101、将用户交易密码和随机值做密钥扩展处理，生成临时密钥。

[0054] 具体的，区块链节点设备接收用户发送的用户交易密码，用户交易密码是用户在进行交易时需输入的密码，是确认交易操作是用户本人操作的验证方法。用户交易密码的规则不做具体要求。随机值由区块链节点设备生成，随机值可以为128比特。密钥扩展处理可以采用scrypt算法。

[0055] 102、将上述临时密钥的第一部分作为密钥对私钥进行加密处理，获得私钥密文。

[0056] 具体的，将上述临时密钥的前半部分作为密钥，上述随机值作为加密参数，对私钥进行加密，获得私钥密文。

[0057] 103、基于上述临时密钥的第二部分、上述私钥密文、keystore的文件名得到消息认证码。

[0058] 具体的，上述临时密钥的第二部分为临时密钥的后半部分。将临时密钥的后半部分、私钥密文、keystore的文件名进行拼接，然后进行摘要运算，将运算结果的后4字节作为消息认证码。上述拼接顺序不做限制。消息认证码(message authentication code，MAC)，在密码学中是经过特定算法后产生的一小段信息，检查某段消息的完整性，以及作身份验证。它可以用来检查在消息传递过程中，其内容是否被更改过，不管更改的原因是来自意外或是蓄意攻击。同时可以作为消息来源的身份验证，确认消息的来源。上述加密算法可以采用sha3-256摘要算法，摘要算法的主要特征是加密过程不需要密钥，并且经过加密的数据无法被解密。keystore为区块链钱包的本地化文件。

[0059] 实施该步骤，使用摘要算法可以避免文件内容被非法篡改。

[0060] 104、将上述随机值、上述私钥密文、上述消息认证码拼接写入上述keystore。

[0061] 具体的，区块链节点设备将随机值、私钥密文、消息认证码拼接在一起，加上tag标签，以二进制的方式写入keystore文件。上述拼接顺序不做限制，优先按照上述所列顺序进行拼接。tag标签以字母R代表随机值，即字母R以后到下一个标签之前的数据为随机值；以字母C代表私钥密文，即字母C以后到下一个标签之前的数据为私钥密文；以字母M代表消息认证码，即字母M以后为消息认证码。tag标签有利于快速分辨不同含义的数据。

[0062] 现有区块链系统中，单个keystore文件大小为491字节。通过以上步骤生成的keystore，文件大小为55字节。

[0063] 实施本申请实施例，可以优化keystore生成存储流程，并采用TV格式(标签:数值)二进制存储数据，大大减少了文件中的冗余信息，解决了keystore文件占用空间大的问题。

[0064] 图2是本申请提出的另一种区块链钱包本地化文件的生成方法的流程图，应用于区块链节点设备，上述方法包括以下内容：

[0065] 201、生成随机种子。

[0066] 随机种子是一种以随机数作为对象的以真随机数(种子)为初始条件的随机数。一般计算机的随机数都是伪随机数，随机种子是以一个真随机数(种子)作为初始条件，然后用一定的算法不停迭代产生随机数。

[0067] 202、根据上述随机种子生成私钥和区块链钱包地址。

[0068] 具体的，私钥由随机种子通过算法运算后得到，过程如下：将随机种子通过SHA算法转化成256位的二进制数字，再验证选择的随机种子是否处于1到n-1之间(其中n是一个常数，略小于2^256)，如果运算结果小于n-1，则随机种子合适，否则需要重新选取随机种子，直至所选取的随机种子满足验证条件为止。不同的区块链钱包选取的随机种子位数可能不一样。

[0069] 私钥经过SECP256K1算法处理生成了公钥。SECP256K1是一种椭圆曲线算法，通过一个已知私钥时可以算出公钥，而公钥已知时却无法反向计算出私钥。上述公钥经过sha3-256算法处理后，截取后20字节作为区块链钱包地址。

[0070] 203、将用户交易密码和随机值做密钥扩展处理，生成临时密钥。

[0071] 具体的，用户交易密码是用户在进行交易时需输入的密码，是确认交易操作是用户本人操作的验证方法。用户交易密码的规则不做具体要求。随机值由区块链节点设备生

成,随机值可以为128比特。密钥扩展处理可以采用scrypt算法,固定参数为dklen:32,n:262144,p:1,r:8,dklen是输出的哈希值的长度,n是CPU/Memory开销值,r表示块大小,p表示并行度,此处固定参数由系统设置,不做具体要求,但是后续不允许修改。

[0072] 204、截取上述临时密钥的第一部分作为密钥,将上述随机值作为加密参数。

[0073] 具体的,为了对上述私钥进行加密,区块链节点设备截取上述临时密钥的前半部分作为密钥,将上述随机值作为加密参数。若结合具体的加密算法,例如AES-128-CTR加密算法,则该加密参数可以为初始化向量(initialisation vector,iv),该iv是AES-128-CTR加密算法需要的初始化向量。初始化向量可以让加密后的密文更难以被攻击者破解,保证了信息的安全性。

[0074] 205、利用上述密钥与上述加密参数对上述私钥进行加密,获得私钥密文。

[0075] 具体的,加密算法可以采用AES-128-CTR算法,利用该算法对上述私钥行加密,生成32字节的私钥密文。加密算法的种类可以进行替换,不做限制。根据加密算法的不同,生成的私钥密文的字节数有可能发生变化。

[0076] 206、将keystore的生成时间与上述区块链钱包地址拼接后作为上述keystore的文件名。

[0077] 具体的,keystore文件的命名规则为address4-UTCtime,其中UTCtime为当前时间,为了更方便的对时间进行统一管理,一般采用0时区的当前时间,时间可以精确到毫秒级。address为区块链钱包地址。

[0078] 举例来说,文件名可以如下:

[0079] be51108ffa60d68d1ca123bd8eb91f0dc756e45f-2019-03-18T07-33-08.245Z

[0080] 该步骤,通过区块链钱包地址拼接UTC时间作为文件名,可以在毫秒级控制钱包的唯一性。如果1毫秒内生成多个keystore文件,则可以用时间前面的数字对文件进行区分。

[0081] 207、将上述临时密钥的第二部分、上述私钥密文、上述keystore的文件名进行拼接并加密运算,获得结果。

[0082] 具体的,上述临时密钥的第二部分可以是该临时密钥的后半部分。加密算法可以是sha3-256摘要算法。摘要算法的主要特征是加密过程不需要密钥,并且经过加密的数据无法被解密。上述加密算法的种类不做限制,相较于sha3-256摘要算法,Md5算法安全性不足,Sha3-512算法运算速度较慢,所以本技术方案优先选择sha3-256摘要算法。

[0083] 上述拼接过程的拼接顺序不做限制,为了降低复杂度统一管理,采取如下顺序进行拼接:临时密钥的后半部分、私钥密文、keystore的文件名。

[0084] 208、截取上述结果的目标部分作为消息认证码。

[0085] 具体的,区块链节点设备截取上述结果的后4字节作为消息认证码。

[0086] 209、将上述随机值、上述私钥密文、上述消息认证码值进行拼接,获得拼接结果。

[0087] 具体的,上述拼接过程的拼接顺序不做限制,为了降低复杂度统一管理,采取如下顺序进行拼接:随机值、私钥密文、消息认证码。

[0088] 210、对上述拼接结果添加标签,并以二进制方式写入上述keystore。

[0089] 具体的,将上述拼接结果加上tag标签,以二进制的方式写入keystore文件。上述拼接顺序不做限制,优先按照随机值、私钥密文、消息认证码的顺序进行拼接。

[0090] tag标签以字母R代表随机值,即字母R以后到下一个标签之前的数据为随机值;以

字母C代表私钥密文,即字母C以后到下一个标签之前的数据为私钥密文;以字母M代表消息认证码,即字母M以后为消息认证码。tag标签有利于快速分辨不同含义的数据。

[0091] 数据组织格式如下:

[0092]

R	随机值RND	C	私钥密文	M	MAC值

[0093] 现有区块链系统中,单个keystore文件大小为491字节。通过以上步骤生成的keystore,文件大小为55字节。

[0094] 实施本申请实施例,可以优化keystore生成存储流程,并采用TV格式(标签:数值)二进制存储数据,大大减少了文件中的冗余信息,解决了keystore文件占用空间大的问题。通过区块链钱包地址拼接世界标准时间作为文件名,可以在毫秒级控制区块链钱包的唯一性。通过对文件名和文件内容中的私钥密文作摘要,保证了文件名和文件内容的一致性,避免被非法篡改。

[0095] 图3是本申请提出的另一种区块链钱包本地化文件的生成方法的具体应用场景的流程图,应用于区块链节点设备,上述方法包括以下内容:

[0096] 301、生成随机种子。

[0097] 举例来说,区块链节点设备生成512比特随机种子。

[0098] 302、根据上述随机种子生成私钥和区块链钱包地址。

[0099] 举例来说,区块链节点设备将上述512比特随机种子通过HMAC-SHA256算法运算形成私钥。将上述私钥经SECP256K1算法运算得到公钥。上述公钥经过sha3-256算法处理后,截取后20字节作为区块链钱包地址。

[0100] 303、将用户交易密码和随机值做密钥扩展处理,生成临时密钥。

[0101] 举例来说,区块链节点设备将用户交易密码与128比特随机值通过scrypt算法运算生成256比特临时私钥。scrypt算法的固定参数为dklen:32,n:262144,p:1,r:8,dklen是输出的哈希值的长度,n是CPU/Memory开销值,r表示块大小,p表示并行度,此处固定参数后续不允许修改。

[0102] 304、截取上述临时密钥的第一部分作为密钥,将上述随机值作为加密参数。

[0103] 举例来说,加密算法可以采用AES-128-CTR加密算法。区块链节点设备截取上述256比特临时密钥的前半部分128比特作为该算法的密钥,将上述128比特随机值作为该算法的加密参数,该加密参数可以为初始化向量iv,该iv是AES-128-CTR加密算法需要的初始化向量。AES-128-CTR加密算法是一种对称加密算法,在对称加密算法中,如果只有一个密钥来加密数据,则明文中的相同数据就会被加密成相同的密文,这样密文与明文就有完全相同的结构,容易被破解。如果加密过程中使用随机数产生的初始化向量,则可以让加密出来的密文结构与明文完全不同,使攻击者难以对密文进行破解。

[0104] 305、利用上述密钥与上述加密参数对上述私钥进行加密,获得私钥密文。

[0105] 举例来说,加密算法可以采用AES-128-CTR算法,利用该算法对上述私钥行加密,生成32字节的私钥密文。

[0106] 306、将keystore的生成时间与上述区块链钱包地址拼接后作为上述keystore的文件名。

[0107] 举例来说,keystore文件的命名规则为address4-UTCtime,其中UTCtime为0时区

的当前时间,时间可以精确到毫秒级。address为区块链钱包地址。

[0108] 举例来说,文件名可以如下:

[0109] be51108ffa60d68d1ca123bd8eb91f0dc756e45f-2019-03-18T07-33-08.245Z

[0110] 307、将上述临时密钥的第二部分、上述私钥密文、上述keystore的文件名进行拼接并加密运算,获得结果。

[0111] 举例来说,将上述临时密钥的后半部分128bit,32字节私钥密文,keystore文件名拼接并采用sha3-256摘要算法进行加密运算,获得结果。

[0112] 308、截取上述结果的目标部分作为消息认证码。

[0113] 举例来说,区块链节点设备截取上述结果的后4字节作为消息认证码。

[0114] 309、将上述随机值、上述私钥密文、上述消息认证码进行拼接,获得拼接结果。

[0115] 举例来说,区块链节点设备将上述随机值、32字节私钥密文、4字节的消息认证码进行拼接,获得拼接结果。

[0116] 310、对上述拼接结果添加标签,并以二进制方式写入上述keystore。

[0117] 举例来说,将拼接结果添加tag标签,并以二进制方式写入上述keystore。

[0118] tag标签以字母R代表随机值,即字母R以后到下一个标签之前的数据为随机值;以字母C代表私钥密文,即字母C以后到下一个标签之前的数据为私钥密文;以字母M代表消息认证码Mac,即字母M以后为消息认证码。tag标签有利于快速分辨不同含义的数据。

[0119] 数据组织格式如下:

[0120]

R	随机值RND	C	私钥密文	M	MAC

[0121] 现有区块链系统中,单个keystore文件大小为491字节。通过以上步骤生成的keystore,文件大小为55字节。

[0122] 为了更好地理解keystore生成方案,还可以参考图4所示的流程图。

[0123] 针对新的keystore生成存储方案,可以采用如下区块链钱包使用方法:接收用户输入的交易密码;读取keystore文件内容,其中R标签后16字节作为随机值RND,C标签后32字节为私钥密文,M标签后4字节为消息认证码;按照钱包生成流程中的介绍,对用户交易密码作密钥扩展处理生成临时密钥,结合私钥密文和文件名字符串生成新的消息认证码,比较与keystore生成过程中的消息认证码是否一致,若一致则进行后续步骤,若不一致则表示用户输入的交易密码不正确或文件被非法修改,流程结束;对私钥密文作AES-128-CTR解密运算(若keystore生成时采用了其他类型加密算法,则钱包使用时的解密算法也做对应调整),临时密钥前半部分为密钥,随机值RND作为iv值,得到用户私钥;使用用户私钥进行后续的钱包签名等操作。

[0124] 实施本申请实施例,可以优化keystore生成存储流程,并采用TV格式(标签:数值)二进制存储数据,大大减少了文件中的冗余信息,解决了keystore文件占用空间大的问题。通过区块链钱包地址拼接世界标准时间作为文件名,可以在毫秒级控制区块链钱包的唯一性。通过对文件名和文件内容中的私钥密文作摘要,保证了文件名和文件内容的一致性,避免被非法篡改。

[0125] 图5是本申请提出的一种区块链节点设备的结构示意图,上述设备包括:

[0126] 扩展单元501,用于将用户交易密码和随机值做密钥扩展处理,生成临时密钥;

[0127] 加密单元502,用于将上述临时密钥的第一部分作为密钥对私钥进行加密处理,获得私钥密文;

[0128] 第一拼接单元503,用于基于上述临时密钥的第二部分、上述私钥密文、上述keystore的文件名得到消息认证码;

[0129] 第二拼接单元504,用于将上述随机值、上述私钥密文、上述消息认证码拼接写入上述keystore。

[0130] 如图5所示,上述设备还包括:

[0131] 第一生成单元505,用于生成随机种子;

[0132] 第二生成单元506,用于根据上述随机种子生成私钥和区块链钱包地址。

[0133] 进一步的,上述加密单元502,具体用于截取上述临时密钥的第一部分作为密钥,将上述随机值作为加密参数;利用上述密钥与上述加密参数对上述私钥进行加密,获得私钥密文。

[0134] 进一步的,上述设备还包括:

[0135] 第三拼接单元507,用于将上述keystore的生成时间与上述区块链钱包地址拼接后作为上述keystore的文件名。

[0136] 进一步的,上述第一拼接单元503,具体用于将上述临时密钥的第二部分、上述私钥密文、上述keystore的文件名进行拼接并加密运算,获得结果;截取上述结果的目标部分作为消息认证码。

[0137] 进一步的,上述第二拼接单元504,具体用于将上述随机值、上述私钥密文、上述消息认证码进行拼接,获得拼接结果;对上述拼接结果添加标签,并以二进制方式写入上述keystore。

[0138] 可理解,图5所示的区块链节点设备的具体实现方式还可参考图1、图2、图3和图4所示的方法,这里不再一一详述。

[0139] 在本申请实施例中,扩展单元501将用户交易密码和随机值做密钥扩展处理,生成临时密钥;加密单元502将上述临时密钥的第一部分作为密钥对私钥进行加密处理,获得私钥密文;第一拼接单元503基于上述临时密钥的第二部分、上述私钥密文、上述keystore的文件名得到消息认证码;第二拼接单元504将上述随机值、上述私钥密文、上述消息认证码拼接写入上述keystore。可见,本申请实施例可以优化keystore生成存储流程,并采用TV格式(标签:数值)二进制存储数据,大大减少了文件中的冗余信息,解决了keystore文件占用空间大的问题。

[0140] 请参阅图6,图6是本申请实施例提供的一种区块链节点设备的结构示意图,该设备包括:至少一个处理器601,例如中央处理器(central processing unit,CPU),至少一个存储器602,至少一个收发器603和至少一个总线604。其中,上述总线604可以是一组并行的数据线,用于实现上述处理器601、上述存储器602和上述收发器603的相互连接;上述存储器602可以是高速随机存取存储器(random access memory,RAM),也可以是非易失性存储器(non-volatile memory),例如至少一个只读存储器(read only memory,ROM)。

[0141] 具体的,上述处理器601将用户交易密码和随机值做密钥扩展处理,生成临时密钥;上述处理器601将上述临时密钥的第一部分作为密钥对私钥进行加密处理,获得私钥密文;上述处理器601基于上述临时密钥的第二部分、上述私钥密文、上述keystore的文件名

得到消息认证码;上述处理器601将上述随机值、上述私钥密文、上述消息认证码拼接写入上述keystore。

[0142] 进一步的,上述处理器601生成随机种子;上述处理器601根据上述随机种子生成私钥和区块链钱包地址。

[0143] 进一步的,上述处理器601截取上述临时密钥的第一部分作为密钥,将上述随机值作为加密参数;上述处理器601利用上述密钥与上述加密参数对上述私钥进行加密,获得私钥密文。

[0144] 进一步的,上述处理器601将上述keystore的生成时间与上述区块链钱包地址拼接后作为上述keystore的文件名。

[0145] 进一步的,上述处理器601将上述临时密钥的第二部分、上述私钥密文、上述keystore的文件名进行拼接并加密运算,获得结果;上述处理器601截取上述结果的目标部分作为消息认证码。

[0146] 进一步的,上述处理器601将上述随机值、上述私钥密文、上述消息认证码进行拼接,获得拼接结果;上述处理器601对上述拼接结果添加标签,并以二进制方式写入上述keystore。

[0147] 具体的,上述存储器602中可以存储程序指令,上述处理器601可用于调用程序指令执行图1、图2、图3和图4所示的方法。

[0148] 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,该程序可以存储于计算机可读存储介质中,存储介质包括只读存储器(read only memory,ROM)、随机存储器(random access memory,RAM)、可编程只读存储器(programmable read only memory,PROM)、可擦除可编程只读存储器(erasable programmable read only memory,EPROM)、一次可编程只读存储器(one-time programmable read-only memory,OTPROM)、电子抹除式可复写只读存储器(electrically-erasable programmable read-only memory,EEPROM)、只读光盘(compact disc read-only memory,CD-ROM)或其他光盘存储器、磁盘存储器、磁带存储器、或者能够用于携带或存储数据的计算机可读的任何其他介质。

[0149] 以上对本申请实施例公开的一种区块链钱包本地化文件的生成方法及区块链节点设备进行了详细介绍,本文中应用了具体个例对本申请的原理及实施方式进行了阐述,以上实施例的说明只是用于帮助理解本申请的方法及其核心思想;同时,对于本领域的一般技术人员,依据本申请的思想,在具体实施方式及应用范围上均会有改变之处。综上所述,本说明书内容不应理解为对本申请的限制。

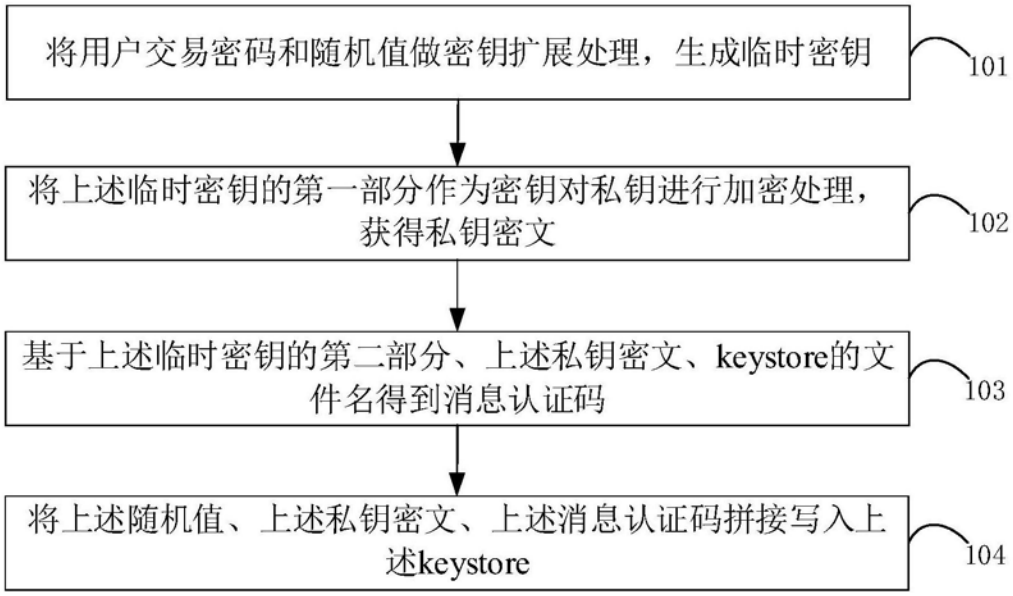

将用户交易密码和随机值做密钥扩展处理，生成临时密钥
101
将上述临时密钥的第一部分作为密钥对私钥进行加密处理，获得私钥密文
102
基于上述临时密钥的第二部分、上述私钥密文、keystore的文件名得到消息认证码
103
将上述随机值、上述私钥密文、上述消息认证码拼接写入上述keystore
104

图1


生成随机种子
201
根据上述随机种子生成私钥和区块链钱包地址
202
将用户交易密码和随机值做密钥扩展处理，生成临时密钥
203
截取上述临时密钥的第一部分作为密钥，将上述随机值作为加密参数
204
利用上述密钥与上述加密参数对上述私钥进行加密，获得私钥密文
205
将keystore的生成时间与上述区块链钱包地址拼接后作为上述keystore的文件名
206
将上述临时密钥的第二部分、上述私钥密文、上述keystore的文件名进行拼接并加密运算，获得结果
207
截取上述结果的目标部分作为消息认证码
208
将上述随机值、上述私钥密文、上述消息认证码值进行拼接，获得拼接结果
209
对上述拼接结果添加标签，并以二进制方式写入上述keystore
210

图2


生成随机种子
301
根据上述随机种子生成私钥和区块链钱包地址
302
将用户交易密码和随机值做密钥扩展处理，生成临时密钥
303
截取上述临时密钥的第一部分作为密钥，将上述随机值作为加密参数
304
利用上述密钥与上述加密参数对上述私钥进行加密，获得私钥密文
305
将keystore的生成时间与上述区块链钱包地址拼接后作为上述keystore的文件名
306
将上述临时密钥的第二部分、上述私钥密文、上述keystore的文件名进行拼接并加密运算，获得结果
307
截取上述结果的目标部分作为消息认证码
308
将上述随机值、上述私钥密文、上述消息认证码值进行拼接，获得拼接结果
309
对上述拼接结果添加标签，并以二进制方式写入上述keystore
310

图3

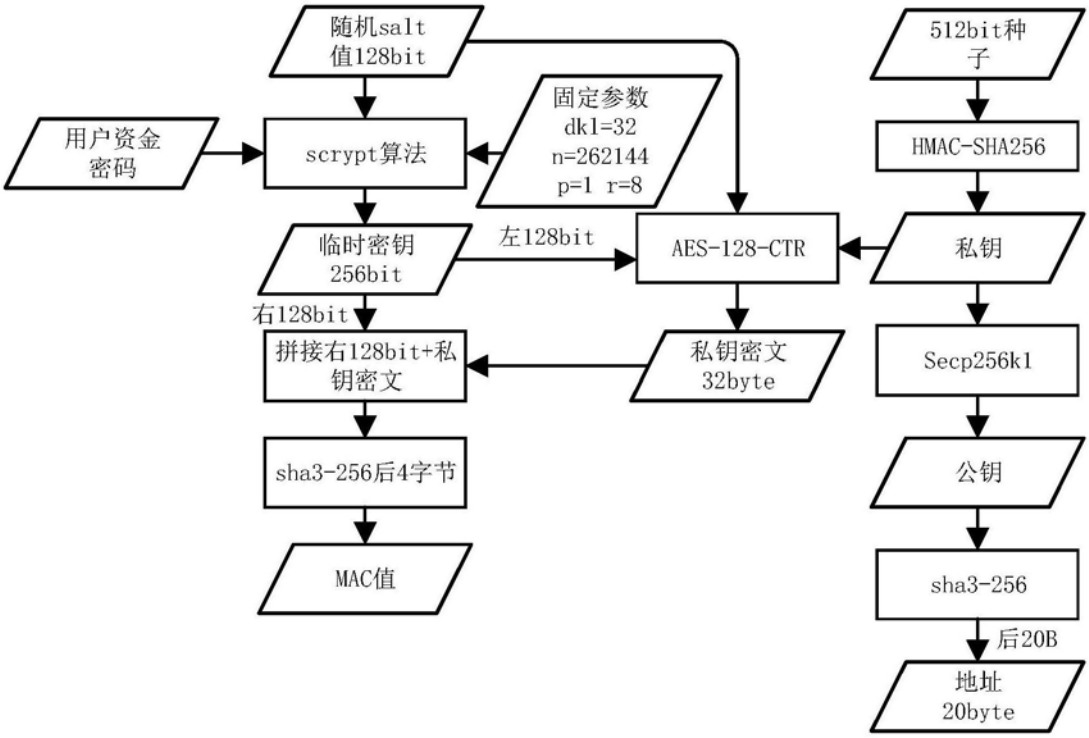

随机salt
值128bit
用户资金
密码
scrypt算法
固定参数
dk1=32
n=262144
p=1 r=8
临时密钥
256bit
左128bit
AES-128-CTR
右128bit
拼接右128bit+私
钥密文
私钥密文
32byte
sha3-256后4字节
MAC值
512bit种
子
HMAC-SHA256
私钥
Secp256k1
公钥
sha3-256
后20B
地址
20byte

图4

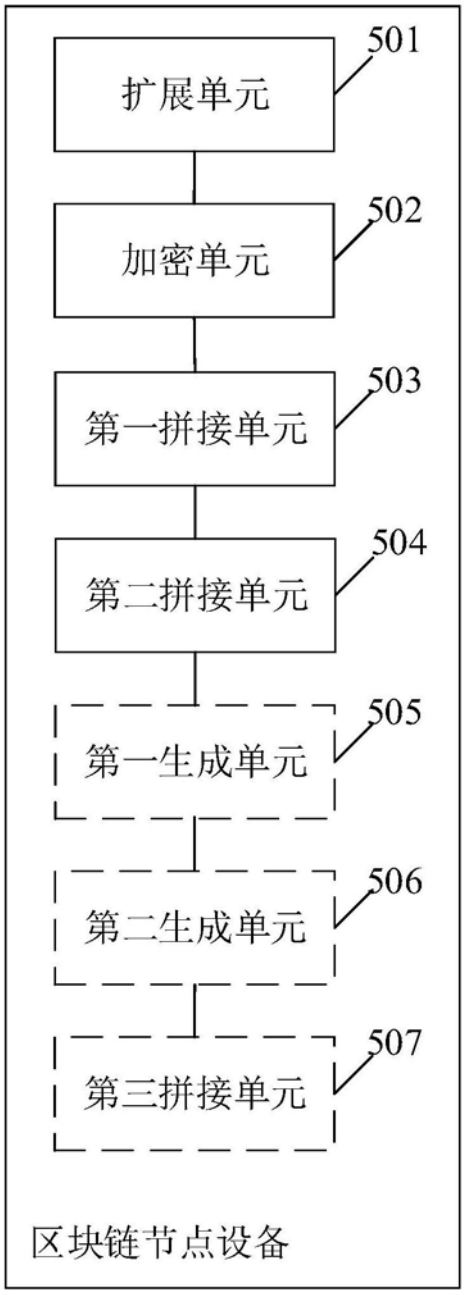

501
扩展单元
502
加密单元
503
第一拼接单元
504
第二拼接单元
505
第一生成单元
506
第二生成单元
507
第三拼接单元
区块链节点设备

图5

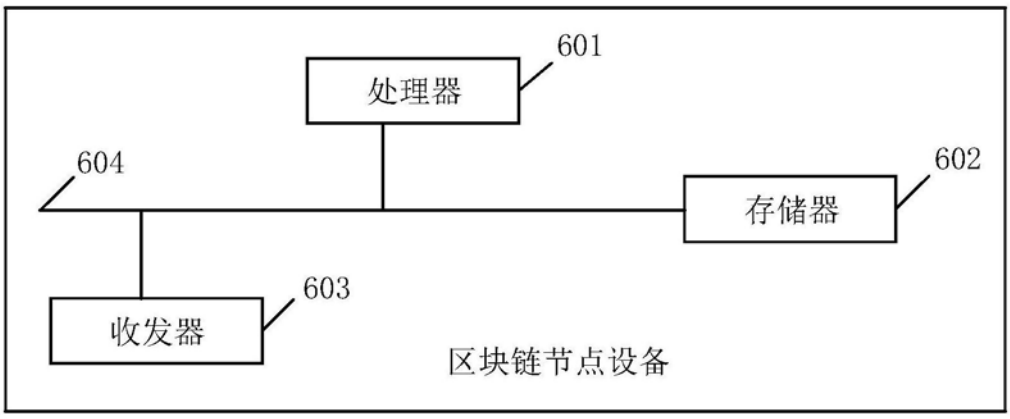


图6