(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 113508563 A
(43)申请公布日 2021.10.15

(21)申请号 202080018217.9

(22)申请日 2020.02.28

(30)优先权数据
62/812,615 2019.03.01 US

(85)PCT国际申请进入国家阶段日
2021.09.01

(86)PCT国际申请的申请数据
PCT/CA2020/050267 2020.02.28

(87)PCT国际申请的公布数据
WO2020/176975 EN 2020.09.10

(71)申请人 泽乌科技公司
地址 加拿大魁北克

(72)发明人 弗朗索瓦·杜马斯 钱玉明
帕特里夏·波佩特-福捷

(74)专利代理机构 北京集佳知识产权代理有限公司 11227
代理人 杜诚 姚文杰

(51)Int.Cl.
H04L 12/58(2006.01)
G06F 16/25(2006.01)
G06F 16/27(2006.01)
G06F 21/62(2006.01)
H04L 9/06(2006.01)
H04L 9/30(2006.01)

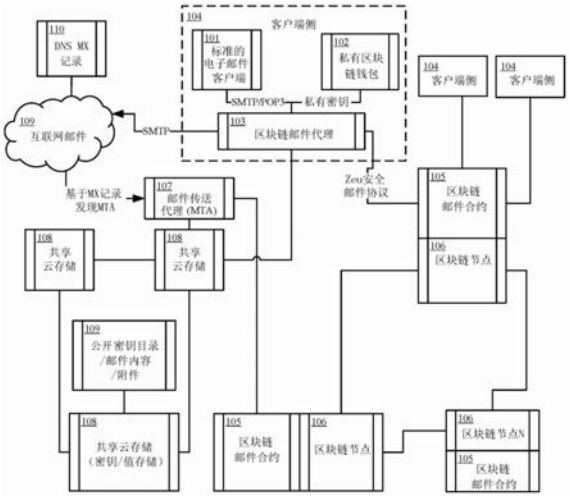
权利要求书2页 说明书11页 附图6页

(54)发明名称

基于区块链的安全电子邮件系统

(57)摘要

本专利描述了一种完整的区块链电子邮件系统，该系统支持内部和跨链的电子邮件以及可能与非区块链电子邮件系统的交互。通过这种方法，只要电子邮件的发送方或接收方是区块链邮箱，则电子邮件信息将被记录在区块链中以确保电子邮件的真实性。此外，当区块链邮箱交换消息时，电子邮件信息将被加密并存储在分布式存储中，其中只有接收方可以获取电子邮件的唯一的密码本和存储位置，从而确保电子邮件传输的安全性。



CN 113508563 A

1.一种区块链消息传送系统,包括:

第一区块链邮件代理,包括:

i)用于与第一区块链上的第一智能合约通信的第一接口;

ii)用于与共享存储进行通信的第二接口;

iii)用于接收从发送方到接收方的消息的传输请求的第三接口,

所述第一区块链邮件代理接收所述传输请求,确定所述接收方的邮箱在区块链中,并且在所述确定的情况下,进行如下操作:

加密所述消息的内容;

以存储索引将加密内容保存到所述共享存储;以及

创建所述第一智能合约的智能合约请求,

其中,所述第一智能合约生成交易记录并将所述交易记录保存在所述第一区块链中。

2.根据权利要求1所述的区块链消息传送系统,其中,所述消息是电子邮件。

3.根据权利要求2所述的区块链消息传送系统,其中,在验证所述接收方的邮箱在所述共享存储中的情况下,所述区块链邮件代理进行如下操作:

生成用于加密所述电子邮件的所述内容的密码本;以及

使用所述接收方的公开密钥对所述存储索引和所述密码本进行加密。

4.根据权利要求3所述的区块链消息传送系统,还包括第二区块链邮件代理,其中,所述第二区块链邮件代理在所述第一区块链生成与所述接收方相关联的所述交易记录的情况下,进行如下操作:

i)获取所述发送方的公开密钥;

ii)使用与所述接收方的所述公开密钥相对应的私有密钥对所述消息的所述内容进行解密来获取所述存储索引和所述密码本;

iii)使用所述存储索引信息从所述共享存储检索加密的所述电子邮件的所述内容;以及

iv)使用所述密码本解密所述内容以形成解密的电子邮件内容。

5.根据权利要求4所述的区块链消息传送系统,其中,所述第一区块链邮件代理和第二区块链邮件代理是相同的。

6.根据权利要求4所述的区块链消息传送系统,其中,所述第一区块链邮件代理和第二区块链邮件代理是不同的。

7.根据权利要求6所述的区块链消息传送系统,其中,所述接收方的邮箱在与所述第一区块链不同的第二区块链中。

8.根据权利要求4所述的区块链消息传送系统,其中,在所述接收方打开标准电子邮件客户端的情况下,所述标准电子邮件客户端与所述第二邮件代理通信以获取并呈现所述解密的电子邮件内容。

9.根据权利要求8所述的区块链消息传送系统,其中,所述电子邮件客户端使用标准的POP3协议获取所述解密的电子邮件内容。

10.根据权利要求4所述的区块链消息传送系统,其中,所述第二区块链邮件代理将所述解密的电子邮件内容存储在所述接收方的所述邮箱中。

11.根据权利要求4所述的区块链消息传送系统,其中,所述私有密钥在所述第一区块

链中的区块链钱包中。

12.根据权利要求6所述的区块链消息传送系统,还包括

a)第一邮件传输网关(MTA);

b)第二邮件传输网关(MTA);

其中,所述第二区块链邮件代理包括:

i)用于与所述第二区块链上的所述第二智能合约通信的第三接口;以及

ii)用于与所述共享存储进行通信的第四接口,以及

其中,所述第一MTA将所述密码本和所述存储索引发送至所述第二MTA,并且所述第二MTA将所述密码本和所述存储索引发送至所述接收方。

13.根据权利要求12所述的区块链消息传送系统,其中,第一MTA通过常规互联网电子邮件将所述密码本和所述存储索引发送至所述第二MTA。

14.根据权利要求1所述的区块链消息传送系统,其中所述传输请求针对复数N个接收方,并且其中所述第一智能合约生成N个交易记录并将所述N个交易记录中的每个交易记录保存在所述第一区块链中。

15.一种使用区块链的安全消息传送方法,包括:

a)接收从发送方到接收方的消息的传输请求,所述发送方在所述区块链上有发送方账户;

b)生成密码本;

c)使用所述密码本对所述消息的内容进行加密;

d)以存储索引将加密内容存储到共享存储;以及

e)用所述接收方的公开密钥对所述存储索引和所述密码本进行加密,使得只有具有与所述接收方的所述公开密钥相对应的私有密钥的所述接收方能够访问所述存储索引和密码本。

16.根据权利要求15所述的方法,还包括检查所述接收方的邮箱是否是在所述区块链中,如果所述接收方的邮箱在所述区块链中,则在所述区块链上执行智能合约以将对应于所述传输请求的传送的记录存储在所述区块链中,否则,发送包含加密的密码和存储索引的外部消息。

17.根据权利要求16所述的方法,还包括:在所述执行之前,确保所述发送方账户被授权发送消息。

18.根据权利要求17所述的方法,还包括:在所述执行之前,确保所述接收方账户在所述区块链上有至少第一预定数量的代币。

19.根据权利要求18所述的方法,其中,所述接收方在所述区块链上有接收方账户,所述方法还包括:在所述执行之前,确保所述接收方帐户在所述区块链上有至少第二预定数量的代币。

20.根据权利要求19所述的方法,还包括:确保所述接收方账户被授权接收消息。

21.根据权利要求20所述的方法,还包括检索所述记录。

22.根据权利要求21所述的方法,还包括删除所述记录。

基于区块链的安全电子邮件系统

技术领域

[0001] 本申请一般地涉及安全电子邮件系统，并且更具体地涉及基于区块链的安全电子邮件系统。

背景技术

[0002] 电子邮件并不像我们自己相信的那样安全。市场上可获得的电子邮件服务器、电子邮件客户端和网页邮件服务器存在安全漏洞。传统的电子邮件系统仅根据用户名和密码在电子邮件服务器上进行验证，而信息本身通常以明文存储在服务器上。因此，电子邮件服务中的漏洞可以被恶意行为者利用来获取邮箱中包含的敏感信息。

[0003] 对于传统的电子邮件系统，电子邮件从发送方到接收方的传送要通过两点之间的多台计算机。不仅用户可以访问电子邮件，而且诸如邮箱持有者、电子邮件服务提供者甚至网络提供者的许多其他方都可以访问电子邮件，并且可以在不通知用户的情况下修改电子邮件的内容。在目前的邮件传输过程中，内容数据以明文封装并暴露于通用端口，使得数据容易截获。可以通过监视网络、设备或软件来抓取电子邮件数据信息。

[0004] 除访问安全因素外，电子邮件系统的数据集中存储。电子邮件存储服务中的漏洞可能泄露重要的电子邮件信息或导致电子邮件被篡改。电子邮件服务的故障，无论是软件引起还是硬件引起的故障，同样可能导致重要电子邮件信息的丢失。在通过这些漏洞访问计算机后，入侵者可以容易地获取电子邮件地址以及相应的用户名、密码和电子邮件的内容。如果有电子邮件地址簿，则入侵者也可以获取那些人的联系方式。一些电子邮件客户端也存在漏洞。入侵者可以在特殊格式的电子邮件中注入木马程序。然后用户在打开电子邮件时执行木马程序，产生可能有危险的安全风险。

[0005] 鉴于上述漏洞，需要更安全的电子邮件系统。

发明内容

[0006] 根据本发明的一个方面，提供了一种包括第一区块链邮件代理的区块链消息传送系统，该第一区块链邮件代理包括：用于与第一区块链上的第一智能合约通信的第一接口；用于与共享存储通信的第二接口；以及用于接收从发送方到接收方的消息的传输请求的第三接口。第一区块链邮件代理接收传输请求，确定接收方的邮箱在区块链中，并且在确定的情况下，进行如下操作：加密消息的内容；以储存索引将加密的内容保存到共享存储；以及创建第一智能合约的智能合约请求。第一智能合约生成交易记录并将交易记录保存在第一区块链中。

[0007] 根据本发明的另一方面，提供了一种使用区块链的安全消息传送方法。该方法包括：接收从发送方到接收方的消息的传输请求，发送方在区块链上有发送方账户；生成密码本；使用密码本对消息的内容进行加密；以储存索引将加密的内容存储到共享存储；以及用接收方的公开密钥对存储索引和密码本进行加密，使得只有具有与接收方的公开密钥相对应的私有密钥的接收方可以访问存储索引和密码本。

附图说明

[0008] 附图仅通过示例的方式示出本发明的实施方式，在附图中，

[0009] 图1是简化的系统架构框图；

[0010] 图2是示出从同一区块链中的邮箱发送和接收电子邮件的简化图；

[0011] 图3是示出区块链邮件代理的内部逻辑的简化图；

[0012] 图4是示出邮件传送代理(MTA)的内部逻辑的简化图；

[0013] 图5是示出发送跨链的电子邮件的详细过程的简化图；以及

[0014] 图6是示出两种服务的简化图：一种用于发送电子邮件，而另一种用于检查电子邮件。

具体实施方式

[0015] 下面提供本发明的各种实施方式的描述。在本公开内容中，当在本文中结合术语“包括”使用“一(a)”或“一个(an)”时，可以是指“一个”，但是也与“一个或更多个”、“至少一个”以及“一个或大于一个”的意思一致。以单数形式表达的任何元件也包含其复数形式。以复数形式表达的任何元件也包含其单数形式。如本文中所使用的，术语“多个”是指大于一个，例如，两个或更多个、三个或更多个、四个或更多个等。诸如“顶部”、“底部”、“向上”、“向下”、“竖直地”和“横向地”的方向性术语仅用于提供相对参考的目的，并不旨在对任何物品在使用期间如何定位或者在组装中或相对于环境如何安装具有任何限制。

[0016] 术语“包括(comprising)”、“具有”、“包括(including)”和“包含”及其语法的变体是包括的或开放式的，并且不排除附加的、未列举的元件和/或方法步骤。当术语“基本上由……组成”在本文中与成分、用途或方法一起使用时，表示可以存在附加的元件、方法步骤或者附加的元件和方法步骤二者，但是这些附加物不实质上影响所列举的成分、方法或使用功能的方式。当术语“由……组成”在本文中与成分、使用或方法一起使用时，排除了附加元件和/或方法步骤的存在。

[0017] “区块链”是一种记录计算设备的公共或私有的对等式网络中的交易的防篡改的共享数字账本。账本保持为增长的加密哈希链块的连续链。

[0018] “节点”是区块链网络上的设备。该设备通常是具有与其上储存有处理器可读指令的处理器可读介质互连的处理器的计算机，该处理器可读介质包括存储器。

[0019] 另外，术语“第一”、“第二”、“第三”等仅用于描述性目的，并且不能被解释为指示或暗示相对重要性。

[0020] 在本发明的描述中，还应注意，术语“安装”、“链接”和“连接”应被解释为广义的，除非另有明确定义和限制。例如，可以是固定连接，或装配式连接，或一体式连接；要么硬连线要么软连线；可以直接连接，或通过中间体间接连接。对于技术人员，可以按照上下文理解本发明中上述术语的具体意思。

[0021] 在示出本发明的实施方式的附图中，相同或相似的附图标记与相同或相似的部分相对应。在本发明的说明书中，应当注意，“多个”的意思是指两个或更多个，除非另有说明；术语“上”、“下”、“左”、“右”、“内部”、“外部”、“前端”、“后端”、“头”、“尾”的方向或位置，附图中所示出的方向或位置关系仅是为了方便描述本发明和简化描述，而不是指示或暗示指示的装置或元件必须具有特定的方向并且在特定的方向上构造和操作，因此不能用作对本

发明的限制。

[0022] 区块链技术和电子邮件技术的结合可以有效地解决背景部分中发现的问题。区块链验证区块链电子邮件的发送方和接收方。该验证无法伪造。所有内容和附件用另一方的加密密钥加密，并存储在分布式存储服务上。第三方无法获取所有数据。万一数据被非法地检索，没有合适的密钥仍然无法解密相应的数据。所有电子邮件内容和附件被处理，由发送方签名以生成指纹信息，并且被存储在区块链中，这意味着发送方的公开密钥可以随时验证电子邮件的准确性。接收方使用他们的私有密钥解密数据并验证区块链上的数据指纹以确保数据没有被修改或伪造。这种完全分布式的去中心化电子邮件系统可以从根本上确保电子邮件的安全。

[0023] 在现实世界中，所有用户利用同一个区块链系统几乎是不可能。因此，存在彼此不交互的多个联盟链。然而，作为电子邮件系统，提供跨链的电子邮件互操作性，以及区块链电子邮件和与常规互联网电子邮件的通信是重要紧急的。本专利不涉及与普通邮箱交互时的信息安全问题，原因是普通邮箱以明文传输或存储；然而，我们仍然可以使用区块链特征来确保所有发送或接收的消息的真实性。此外，对于区块链到区块链邮箱，电子邮件传输将被端到端加密，并且只有经授权的接收方可以阅读邮件。

[0024] 本说明书描述了一种区块链电子邮件系统，该区块链电子邮件系统支持内部和跨链的电子邮件以及可能与非区块链电子邮件系统的交互。通过这种方法，只要电子邮件的发送方或接收方是区块链邮箱，则电子邮件信息将被记录在区块链中以确保电子邮件的真实性。此外，当区块链邮箱交换消息时，电子邮件信息将被加密并存储在分布式存储中；只有接收方可以获取电子邮件的唯一的密码本和存储位置，从而确保电子邮件传输的安全性。

[0025] 下面描述本发明的实施方式的示例性系统。图1描绘了本发明的实施方式的系统架构图。如所示出的，系统架构图包括以下组件。

[0026] 组件101是标准的电子邮件客户端。为了适应不同用户的使用习惯，例如作为电子邮件客户端插件提供了电子邮件服务，以通过安全邮件代理组件103经由内部协议或标准电子邮件协议来捕获电子邮件的内容。代理通过电子邮件内容中的特殊标签来识别区块链电子邮件。如果电子邮件是普通电子邮件，则电子邮件将通过传统邮件服务器；否则，电子邮件将被加密并且通过区块链电子邮件服务发送。可选地，本地邮件代理可以为本地电子邮件客户端提供POP 3和SMTP接口，因此任何第三方电子邮件客户端可以通过安全的本地电子邮件代理服务发送/接收电子邮件。为确保信息安全，安全邮件代理需要与标准电子邮件客户端在同一节点上运行，以防止不安全的邮件消息在网络上传输和保存。

[0027] 替选地，标准电子邮件客户端可以有插件，该插件与电子邮件客户端的用户界面(UI)交互以捕获电子邮件的内容。如果电子邮件被识别为区块链电子邮件，则该插件将充当安全的邮件代理并将安全的区块链电子邮件转换为明文电子邮件以显示在电子邮件客户端的UI上，或者将明文邮件加密为区块链电子邮件并且发送至区块链电子邮件服务以用于进一步处理。

[0028] 组件102是区块链钱包。区块链钱包的主要功能是存储用户的私有密钥和公开密钥。我们可以使用钱包将电子邮件帐户与区块链帐户进行关联。每个区块链电子邮件帐户设置公开密钥和私有密钥。公开密钥将被发布至共享云存储，并且任何人可以访问公开密

钥,而钱包充分地保护私有密钥。数据将通过使用钱包API(应用程序编程接口)被加密或解密。由于钱包存储了重要的区块链账户信息和私有密钥,为避免信息泄露,我们需要钱包运行在用户侧终端上以确保只有用户可以访问钱包。

[0029] 组件103是安全区块链本地电子邮件代理或插件。代理通过私有插件协议或者通过POP 3和SMTP接口与本地电子邮件客户端通信,并且将电子邮件发送/接收请求转换为区块链智能合约请求。通过在区块链中运行的智能合约发送和接收包含加密存储索引密钥和用于解密的共有密码的安全的区块链电子邮件消息。替选地,可以通过普通邮件服务器发送和接收加密邮件,同时使用插件或邮件代理来验证内容并加密/解密邮件。安全电子邮件代理在共享云存储上登记本地邮箱的公开密钥信息。接收方侧电子邮件代理监视区块链以检索消息。收到消息后,钱包中的私有密钥被用于解密并获取共享的专有密码本,并且在共享的云存储中使用索引数据以获取相应的加密电子邮件内容和附件。在检索电子邮件内容和附件后,电子邮件代理使用专有密码本对电子邮件内容进行解密并将其转发至本地电子邮件。当本地电子邮件客户端应用程序未启用时,代理还负责在本地缓存各种接收到的消息。

[0030] 组件104是客户端侧组件。为确保信息安全,将组件101、102、103部署在一起以形成客户端组件104。

[0031] 组件105是区块链电子邮件智能合约。智能合约用于在链中记录每封电子邮件的加密专有密码本和发送方的签名信息。针对智能合约,在区块链节点处完成共识,确保数据被存储且不可更改。由于存储在区块链中的密码本由接收方的公开密钥加密,并且主要的电子邮件内容和附件由专有密码本加密并存储在分布式云存储中,因此只有接收方可以正确地检索相应的电子邮件信息。没有其他人——甚至管理员——知道电子邮件信息存储在哪里,也不能拦截电子邮件的内容;因此没有办法解码电子邮件。对于所有发送或接收到互联网邮箱的电子邮件,只要一方是区块链邮箱,则电子邮件的签名信息也将留在区块链中以用于验证目的。

[0032] 组件106是区块链节点。组件106用于完成多节点共识和账户记录工作。本专利不限制具体区块链;任何可以支持智能合约的区块链系统都应该是适合的。此外,本专利适用于多个异构区块链系统来交换电子邮件。

[0033] 组件107是邮件传送代理(MTA)。组件107用于互联网电子邮件的接口网关。MX(邮件交换器)信息在域名服务器上注册,使得所有互联网电子邮件和其他跨链的区块链电子邮件被发送至节点进行处理。当MTA收到普通互联网电子邮件时,该MTA将用MTA私有密钥对电子邮件进行签名,根据接收方信息获取接收方的公开密钥,对内容进行加密,以及将加密的内容转发至区块链电子邮件。当MTA收到来自另一区块链的跨链电子邮件时,该MTA将基于接收方信息将消息直接发送至区块链邮箱。

[0034] 组件108是共享的云存储服务组件。组件108提供基本的密钥/值映射存储,以及以多副本分布式存储方式将数据分发至多个不同的节点以确保整个系统的效率和数据安全性。所有用户都可以公开访问存储系统。然而,当存储区块链电子邮件时,电子邮件信息是加密的且相应的密钥也是加密的,并且仅可由接收方访问。因此,第三方无法组合完整的电子邮件,也无法对其进行解密。

[0035] 组件109描述了在该实施方式中存储在共享云存储上的至少三种类型的数据。这

三种类型的数据包括:1)邮箱的相应的公开密钥信息,以及可公开访问的信息;2)加密的电子邮件消息内容,其由每封邮件的专有密钥使用;以及3)加密的大附件。对称加密算法用于用专有密码本对电子邮件内容进行加密。内容格式为MIME(多用途互联网邮件扩展类型)。因此,小附件可以与电子邮件正文一起加密,作为加密的电子邮件消息内容的一部分。加密的大附件类似地由使用对称加密算法的专有密码本进行加密。

[0036] 组件110是DNS(域名系统)服务组件。为了在域名的MX记录上填充MTA的IP(互联网协议)地址,所有寻址到该域名的电子邮件将被转发至指定的MTA。

[0037] 完整的电子邮件系统包括电子邮件客户端、电子邮件服务器和电子邮件传输通道。电子邮件本身通常包括发送方、接收方、标题、内容和多个附件。为了与现有的电子邮件系统集成,本发明的实施方式的系统示例的部署根据接收方的邮箱域名进行区分。接收方可以属于在同一区块链或在另一区块链中的本地邮箱。在其他实施方式中,接收方的邮箱也可以是外部互联网邮箱。

[0038] 电子邮件的发送和接收过程可以按照以下场景进行分类。

[0039] 电子邮件过程

[0040] 邮件投递过程

[0041] 场景1:从区块链邮箱到同一链中的区块链邮箱

[0042] 在该场景中,电子邮件客户端首先使用通用邮件协议将电子邮件发送至本地区块链电子邮件代理。本地代理确定电子邮件中多个接收方所属的域是否在本地区块链中有其邮箱。如果电子邮件中多个接收方所属的域在本地区块链中有其邮箱,则本地代理为该电子邮件生成唯一的密码本,并将加密的电子邮件正文和附件通过加密保存至共享存储,并且使用发送方的私有密钥对数据进行签名以防止被第三方非法篡改。本地电子邮件代理用区块链接收方的邮箱的公开密钥同时对共享存储索引信息和电子邮件专有密码本进行加密,将其推送至电子邮件合约以生成交易记录,将其保存在区块链上,并且完成共识。如果电子邮件中有N个接收方,则分别生成N条区块链记录,并且N个接收方的公开密钥用于加密密码本以及对共享存储上的电子邮件的信息进行索引。

[0043] 在实现该步骤后,至少一个电子邮件正文将被保留在共享存储中,并且电子邮件代理生成N(接收方的数目)个区块链记录并完成在链上的共识。

[0044] 场景2:从区块链邮箱到另一链中的区块链邮箱

[0045] 在该场景中,当发送电子邮件时,本地区块链电子邮件代理询问共享云存储以检查相应的接收方电子邮件地址是否为区块链邮箱。如果是区块链邮箱,本地区块链电子邮件代理首先生成专有密码本并用该密码本对电子邮件进行加密。加密的邮件内容和附件存储在共享云存储中。发送方的区块链电子邮件代理从共享云存储中获取接收方账户的公开密钥信息,并且使用公开密钥来加密专有密码本并通过常规互联网电子邮件将其发送至另一方的邮件传输网关(MTA)。收到区块链电子邮件后,另一方的MTA根据接收方信息将区块链电子邮件推送至另一方的区块链电子邮件合约。

[0046] 在该场景中,依靠由多个区块链共享的云存储服务从而交换跨链数据。由于数据是共享的,因此当接收代理接收电子邮件信息时,电子邮件正文数据必须已经存在并且只能被另一方的电子邮件解密;任何中间节点都无法知道电子邮件内容,这确保了数据安全性。

[0047] 场景3:从区块链邮箱到普通非加密互联网邮箱

[0048] 在该场景中,由于接收方是非加密互联网邮箱,因此信息安全的责任不取决于系统的示例性实施方式。然而,示例性系统计算发送电子邮件的内容和附件的指纹信息,并且使用发送方的私有密钥对指纹信息进行签名和验证。区块链邮箱代理将信息推送至区块链电子邮件智能合约,并且将相关信息保存到区块链,使得电子邮件的接收方根据签名的指纹信息验证电子邮件消息是否被篡改。这些电子邮件记录也可以用于合法目的。

[0049] 邮件接收方过程

[0050] 邮件接收方可以包括以下场景:

[0051] 场景4:从属于同一区块链的邮箱接收区块链电子邮件

[0052] 区块链电子邮件代理监视区块链上的新消息。当区块链为接收方的当前账户生成了电子邮件交易记录时,区块链电子邮件代理解析消息内容,获取发送方的公开密钥以验证签名,并且使用本地钱包中的私有密钥对消息正文进行解密以获取邮件存储索引和相应的专有密码本。区块链电子邮件代理使用电子邮件存储索引信息以从共享云存储服务下载相应的加密电子邮件内容和附件,并且使用专有密码本解密内容。解密的电子邮件将被临时存储在本地邮局。当用户打开标准的电子邮件客户端时,电子邮件客户端使用标准的POP3协议与本地电子邮件代理通信以获取解密的电子邮件和附件。这种方法使得用户的区块链邮箱体验与使用常规邮箱服务没有区别。

[0053] 场景5:从另一区块链上的邮箱接收跨链区块链电子邮件

[0054] 区块链电子邮件代理服务作为普通MX电子邮件服务注册到互联网域名,并且将区块链电子邮件代理的公开密钥和域名映射保存至共享云存储服务。当收到由另一区块链上的邮箱发送的跨链区块链电子邮件时,MTA首先从共享云存储服务中的公开密钥目录中获取发送方的公开密钥,验证电子邮件签名,然后将加密的专有密码本和存储索引信息推送至本地区块链电子邮件智能合约。当本地接收方收到相应的区块链电子邮件消息时,消息将被与场景1相同地处理。

[0055] 场景6:从常规互联网邮箱接收常规电子邮件

[0056] 从常规互联网邮箱发送的电子邮件是非加密的。为了使区块链邮箱能接收通过互联网发送的常规电子邮件,区块链MTA需要执行电子邮件转发工作:生成专有密码本,用该密码本对消息的内容和附件进行加密,将加密的电子邮件内容和附件保存至共享云存储服务,获取云存储索引以及根据接收方邮箱在云存储中搜索相应的接收方邮箱公开密钥,然后使用公开密钥对密码本和存储索引进行加密。专有密码本用电子邮件代理的私有密钥被加密和签名,然后被推送至区块链电子邮件合约以完成本地电子邮件转发。接收方的区块链邮箱客户端可以使用与场景1相同的过程来接收常规互联网邮件。

[0057] 示例:

[0058] 参照图2描述以下示例,图2描绘了示出从同一区块链中的邮箱发送和接收电子邮件的示意框图。

[0059] 用户A向用户B的邮箱发送区块链电子邮件;他们二者都在同一区块链上。

[0060] 在步骤201,用户A的电子邮件代理注册系统从钱包获取用户A的公开密钥并将其注册至共享存储。因此,同一链或不同链中的其他用户可以找到用户A的公开密钥。

[0061] 在步骤202,用户A的电子邮件客户端通过POP 3协议用本地电子邮件代理执行验

证。

[0062] 在步骤203,用户A撰写电子邮件,并且通过SMTP将其发送至本地电子邮件代理。

[0063] 在步骤204,用户A的本地电子邮件代理接收电子邮件发送请求并生成唯一的专有密码本。

[0064] 在步骤205,用户A的本地电子邮件代理使用该唯一的密码本基于对称加密方法对电子邮件内容和附件进行加密。

[0065] 在步骤206,用户A的本地电子邮件代理调用钱包,使用用户A的私有密钥对加密的电子邮件内容和附件进行签名,并且为该电子邮件生成签名。

[0066] 在步骤207,用户A的本地电子邮件代理将加密的邮件内容和附件使用索引密钥(日期时间+哈希(发送方+接收方+标题))或(日期时间+哈希(发送方+接收方+附件名))存储到共享云存储。

[0067] 在步骤208,用户A的本地电子邮件代理从共享存储检索用户B(接收方)的公开密钥,并且基于非对称加密使用用户B的公开密钥对专有密码本和云存储索引密钥进行加密。如果有不止一个接收方,本地邮件代理会为每个接收方加密多次。

[0068] 在步骤209,用户A的本地电子邮件代理调用电子邮件合约,将加密的专有密码本和云索引密钥推送至智能合约并将其存储在区块链中。

[0069] 在步骤210,电子邮件合约在区块链中执行共识操作并且将消息存储在区块链上。

[0070] 在步骤211,用户B的电子邮件代理继续监视区块链。当代理发现给用户B的消息时,其从区块链检索消息。

[0071] 在步骤212,用户B的电子邮件代理基于非对称加密方法使用用户B在钱包中的私有密钥对消息进行解密。

[0072] 在解密之后的步骤213,用户B的电子邮件代理检索电子邮件内容和附件的索引以及该电子邮件的密码本。用户B的电子邮件代理使用索引从共享存储检索加密的电子邮件内容和附件。

[0073] 在步骤214,用户B的电子邮件代理基于对称加密方法使用密码本对电子邮件内容和附件进行解密。

[0074] 在步骤215,用户B的电子邮件代理将解密的邮件内容和附件临时存储在本地存储中。

[0075] 在步骤216,用户B的电子邮件客户端使用POP3协议或插件从用户B的电子邮件代理检索邮件,并且将消息显示给用户B。

[0076] 共享云存储中的三种类型的数据

[0077] 以下三种类型的数据存储在共享云存储中。

[0078] 数据类型1:用户邮箱→邮箱的公开密钥映射

[0079] 一种示例性格式如下:

[0080] 字符串表示格式为XX@[domain.com]的作为唯一主密钥的用户的邮箱,其中XX是邮箱名称,并且domain.com是域名。

[0081] 字符串表示邮箱的公开密钥。对于不同的密钥系统,公开密钥的格式可以不同;建议以PEM(隐私增强型电子邮件)格式表示。

[0082] 数据类型2:邮件索引→加密的邮件内容映射

[0083] 字符串表示邮件索引。结构为日期时间+哈希(发送方+接收方+标题),这使得更容易按照日期分组,这便于云存储上的冷热数据交换。

[0084] 标准的MIME结构表示电子邮件的内容。在一个实施方式中,该结构可以是如可在https://www.w3.org/Protocols/rfc1341/7_2_Multipart.html在线获取的标题为“MIME(多用途互联网邮件扩展):用于指定和描述互联网消息正文的机制”的RFC 1341的第7.2节“The Multipart Content-Type”以及可在https://en.wikipedia.org/wiki/MIME在线获取的MIME的维基百科条目中所描述的。

[0085] 电子邮件标题、发送方(FROM)、接收方(TO)、抄送(CC)、密送(BCC)等未加密,但是邮件内容和附件通过AES(高级加密标准)以及其他对称加密算法进行加密,然后根据Base 64编码组合为字符串。

[0086] 数据类型3:附件索引→加密的附件数据

[0087] 为了降低获取邮件的成本,可以分别保存大附件和超大附件。

[0088] 附件索引格式为“邮件索引-附件ID”,其通过引用消息中的附件索引来添加大附件。

[0089] 电子邮件的附件和内容的加密方式是通过使用电子邮件的专有密码本进行加密,并通过区块链将专有密码本传输至接收方。

[0090] 区块链邮件代理的内部逻辑

[0091] 图3描绘了表示利用区块链邮件代理的过程的实施方式的内部逻辑的过程图,包括以下步骤。

[0092] 在e过程的步骤300,客户端发送电子邮件。

[0093] 在步骤301,邮件代理在本地缓存待处理电子邮件。

[0094] 在步骤302,过程用发送者的私有密钥对消息进行签名。

[0095] 在步骤303,过程询问共享云存储,检查电子邮件接收方是否注册有区块链邮箱。

[0096] 在步骤304,如果共享存储中注册了区块链邮箱,这意味着接收方为区块链邮箱,并且生成专有密码本。

[0097] 在步骤305,过程使用专有密码本加密消息内容和附件。

[0098] 在步骤306,过程将加密的邮件和附件存储到共享云存储。

[0099] 在步骤307,过程检查接收方是否在同一区块链中。

[0100] 在步骤308,过程询问接收方是否不在同一区块链中,用加密的专有密码本和存储索引构建输出消息。

[0101] 在步骤309,过程使用SMTP协议发送互联网电子邮件。

[0102] 在步骤310,过程将消息推送至电子邮件合约,将邮件签名信息、加密的专有密码本和存储索引信息保存在区块链中。

[0103] 在步骤311过程,如果电子邮件的接收方不是区块链邮箱,则过程构造明文消息,发送该消息并将该消息推送至仅包含电子邮件签名的电子邮件合约。

[0104] 邮件传送代理(MTA)的内部逻辑

[0105] 图4描绘了邮件传送代理(MTA)的内部逻辑,包括以下步骤。

[0106] 在过程的步骤400,MTA从互联网接收电子邮件。

[0107] 在步骤401,过程检查接收方的域。

[0108] 在过程的步骤402,如果域与当前注册的域不同,则这是垃圾邮件并被丢弃。

[0109] 在步骤403,过程询问电子邮件的发送方是否是区块链邮箱。

[0110] 在过程的步骤404,如果发送方不是区块链邮箱,则需要将常规的互联网电子邮件转换为区块链电子邮件,并且生成用于加密的共有密码本。

[0111] 在步骤405,过程用专有密码本对内容和附件进行加密,并且用MTA私有密钥对电子邮件进行签名。

[0112] 在步骤406,过程将加密的内容和附件存储到共享云存储。

[0113] 在步骤407,过程使用接收方的公开密钥对专有密码本和存储索引进行加密。

[0114] 在步骤408,过程调用电子邮件合约,将加密的专有密码本和存储索引作为消息推送至区块链电子邮件合约。

[0115] 跨链电子邮件

[0116] 参照图5描述了发送跨链电子邮件的详细示例过程,图5描绘了发送跨链的电子邮件所涉及的元件或步骤。这些包括邮件客户端500、区块链邮件代理501、节点502、区块链邮件代理503、诸如互联网的网络504、邮件传送代理(MTA)505、节点506、区块链邮件代理507、邮件客户端508、邮件服务器509、DNS节点510和共享云存储511。

[0117] 在一个示例性实施方式中,为了支持跨链区块链电子邮件,过程首先将MTA 505注册到DNS服务510的MX记录,使得在通过互联网协议发送电子邮件时可以找到相应的服务器。为了获取接收方邮箱的公开密钥信息,区块链电子邮件代理需要注册其自己的公开密钥和邮箱地址以映射到云端共享分布式存储。然后,发送方可以使用接收方密钥对数据进行加密,并且验证发送方的签名信息以确保内容正确且不会泄露给第三方。

[0118] 为了将跨链电子邮件内容从一个区块链系统传送至另一区块链系统,过程首先生成唯一的专有密码本,然后在发送方的区块链邮件代理501上用发送方的私有密钥对其进行签名。专有密码本用于使用对称加密算法对邮件内容和附件进行加密,并且加密的电子邮件数据被存储在可以被全局共享的分布式云存储511中。该实施方式中需要对外暴露分布式云存储的密钥值(K/V)访问接口。然后接收方邮箱的公开密钥被用于使用非对称加密算法对生成的专有密码本和云存储的索引位置进行加密。由于加密的数据只能通过接收方邮箱的私有密钥解密,因此限制了可能引起安全性问题的安全电子邮件的随意转发或者电子邮件内容的拦截。

[0119] 完成专有密码本加密后,过程构建常规的互联网电子邮件以将信息传送至新域名下的电子邮件服务——邮件传送代理505。然后MTA 505将消息内容转发至区块链系统节点506,完成区块链共识操作,并将消息记录到区块链账本中。当接收方客户端508的区块链电子邮件代理507检测到新邮件时,使用本地钱包中邮箱的私有密钥对邮件消息进行解密,获取专有密码本和云存储511的索引地址,以及检索云存储511中相应的地址。电子邮件内容和附件使用专有密码本进行解密以供接收方客户端508使用标准的邮件协议来检索和显示。

[0120] 区块链智能合约逻辑

[0121] 块数据存储格式

[0122]

消息id	发送方	接收方	共有密码	存储密钥	签名	日期时间
64位整型	账户	账户	字符串	字符串	字符串	64位整型

[0123] 发送方： 发送方的区块链账户

[0124] 接收方： 接收方的区块链账户

[0125] 共有密码： 加密的共有密码

[0126] 存储密钥： 加密的存储索引密钥

[0127] 签名： 邮件的签名

[0128] 日期时间： 发送时间

[0129] 如果电子邮件来自互联网，则“发送方”字段将被填充为MTA的帐户。如果电子邮件的接收方在当前链的外部，则“接收方”字段将被填充为空位。

[0130] 为避免垃圾邮件，除MTA之外的所有用户都需要根据接收方的数目支付一定数量的代币。

[0131] 图6描绘了包括发送和检查电子邮件的智能合约电子邮件服务的过程图。如所示出的，区块链电子邮件合约包括两项服务，一项用于发送电子邮件消息(步骤600-步骤605)，而一项用于检查电子邮件消息(步骤607-步骤612)。

[0132] 服务需要确保用户有足够的代币来发送电子邮件，并且电子邮件的发送方与消息的发送方一致并具有操作合约的权限。服务还需要确保消息的接收方只能获取发送至该账户的消息，而不能获取发送至其他人的任何消息。

[0133] 两项服务的具体过程如下：

[0134] 发送消息服务：

[0135] 在步骤600，调用过程传送电子邮件消息合约。

[0136] 在步骤601，过程检查发送方的验证并确保操作员与发送方的帐户相同并且具有发送电子邮件的权限。

[0137] 在步骤602，过程询问发送方的账户是否有足够的代币。账户需要向库支付一定数量的代币以支付电子邮件传送费用。

[0138] 在步骤603，如果发送方的账户在付款后有正数的代币，则过程调用代币传送合约。

[0139] 在步骤604，过程存储记录在区块链的未读消息表中的电子邮件。

[0140] 在步骤605，宣布交易成功。

[0141] 在步骤606，如果付款后发送方的账户有负数的代币，则交易将失败。检查消息服务：

[0142] 在步骤607，过程检查调用的消息。

[0143] 在步骤608，过程询问接收方账户是否具有接收消息的权限以及接收方是否与当前账户相同。

[0144] 在步骤609，过程询问链表是否包含未读消息。

[0145] 在步骤610，过程查找并检索当前帐户的未读消息。

[0146] 在步骤611，过程从未读消息表删除消息。

[0147] 在步骤612，交易结束。

[0148] 收到新消息后，智能合约将新消息封装到电子邮件代理中，该电子邮件代理以JSON(JavaScript对象表示法)格式传递给接收方。

[0149] 为便于接收消息，区块链电子邮件代理不断地监视区块链。当生成新的块时，区块链电子邮件代理检查链是否包含当前用户的未读消息。然后该区块链电子邮件代理通过调用智能合约的接收功能来检索消息。在合约中，只有根据接收方账户提供相应的验证密钥的客户端可以检索消息。

[0150] 已经仅通过示例的方式描述了本发明的实施方式，因此要理解，由所附权利要求限定的本发明不受上述示例性实施方式的描述中阐述的特定细节的限制，如在不脱离权利要求的范围的情况下，许多变体和置换是可以的。

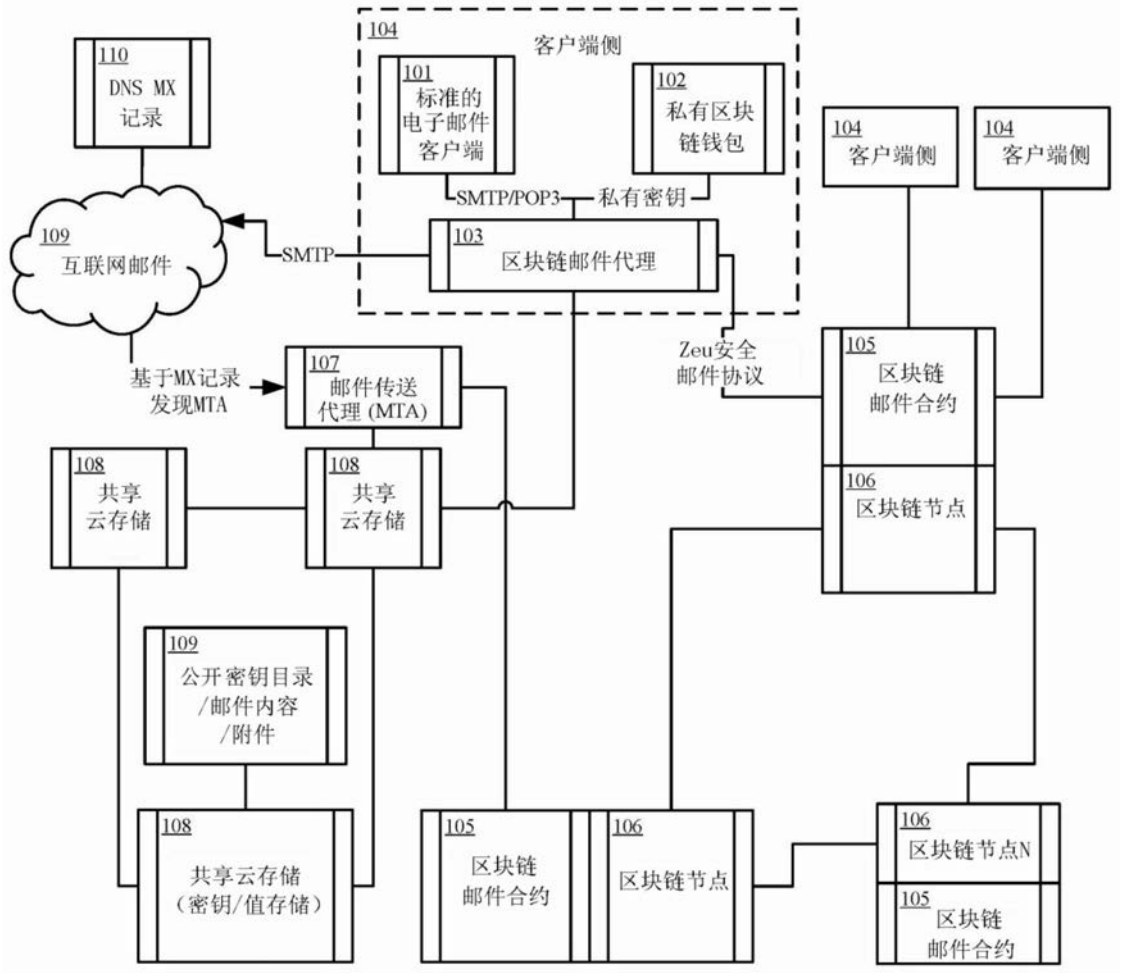

104
客户端侧
110
DNS MX
记录
101
标准的
电子邮件
客户端
102
私有区块
链钱包
104
客户端侧
104
客户端侧
SMTP/POP3
私有密钥
109
互联网邮件
SMTP
103
区块链邮件代理
Zeu安全
邮件协议
105
区块链
邮件合约
基于MX记录
发现MTA
107
邮件传送
代理 (MTA)
108
共享
云存储
108
共享
云存储
106
区块链节点
109
公开密钥目录
/邮件内容
/附件
108
共享云存储
（密钥/值存储）
105
区块链
邮件合约
106
区块链节点
106
区块链节点N
105
区块链
邮件合约

图1

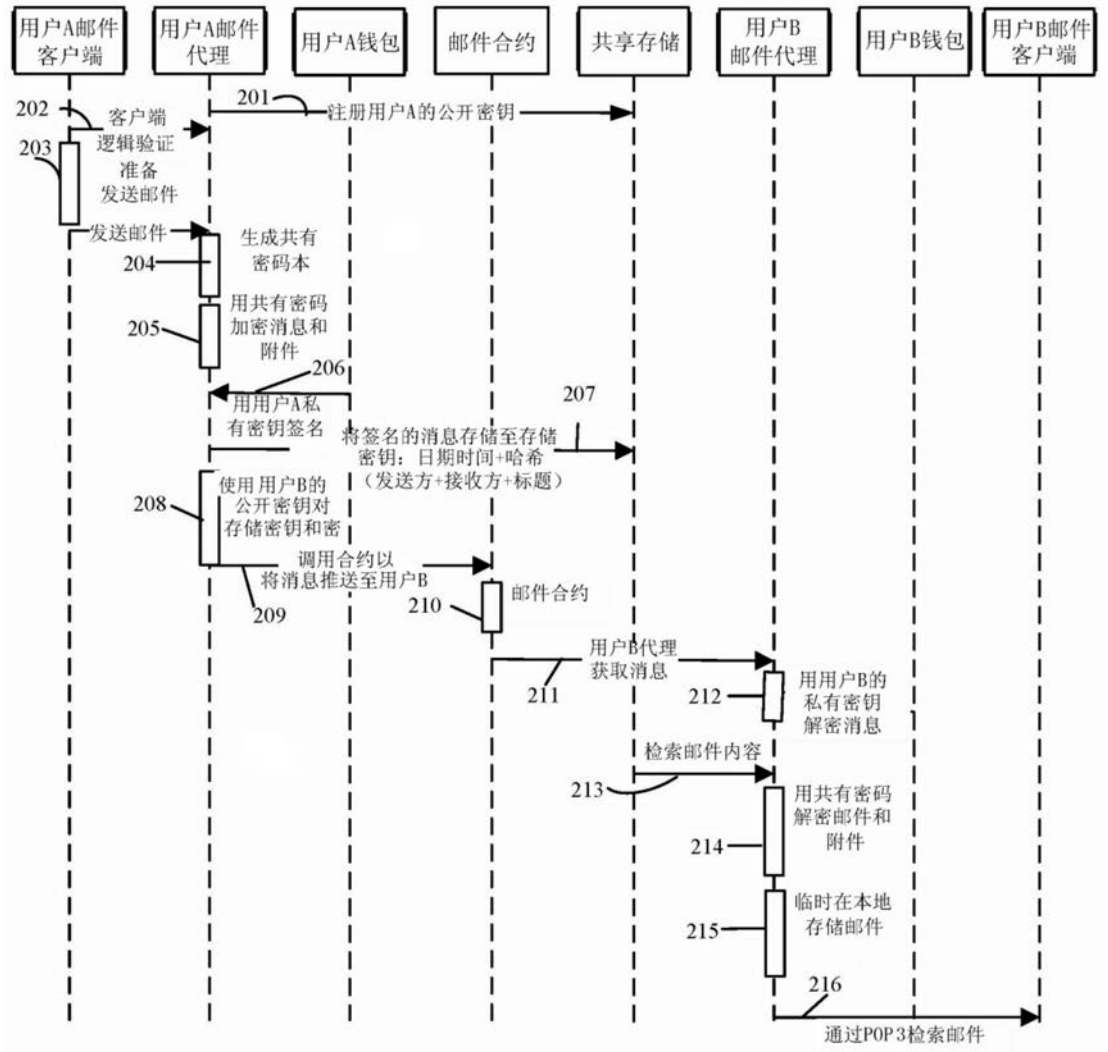

用户A邮件客户端
用户A邮件代理
用户A钱包
邮件合约
共享存储
用户B邮件代理
用户B钱包
用户B邮件客户端
201
注册用户A的公开密钥
202
客户端逻辑验证
203
准备发送邮件
发送邮件
生成共有密码本
204
用共有密码加密消息和附件
205
206
用用户A私有密钥签名
207
将签名的消息存储至存储密钥：日期时间+哈希（发送方+接收方+标题）
使用用户B的公开密钥对存储密钥和密
208
调用合约以将消息推送至用户B
209
210
邮件合约
用户B代理获取消息
211
212
用用户B的私有密钥解密消息
检索邮件内容
213
用共有密码解密邮件和附件
214
临时在本地存储邮件
215
216
通过POP3检索邮件

图2

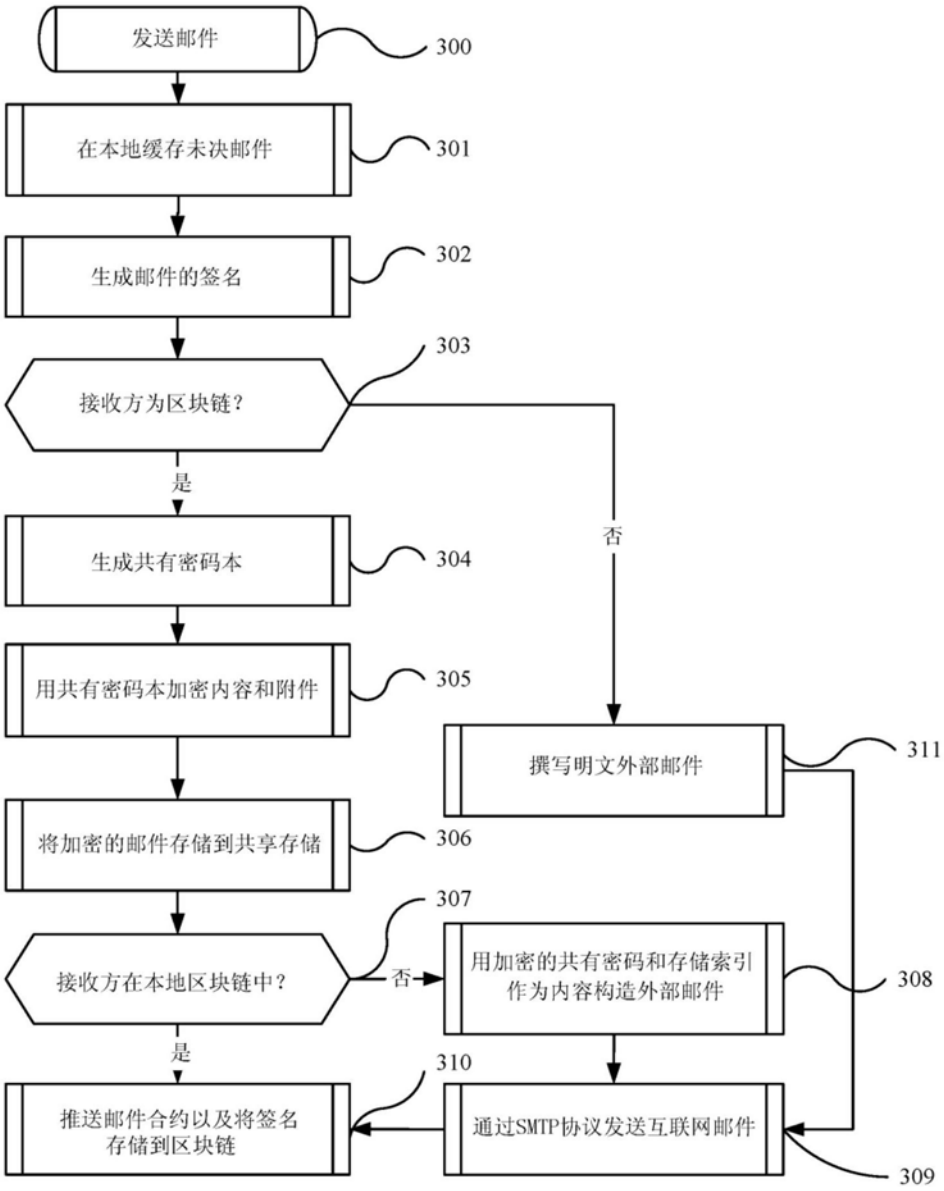

发送邮件
300
在本地缓存未决邮件
301
生成邮件的签名
302
接收方为区块链?
303
是
否
生成共有密码本
304
用共有密码本加密内容和附件
305
撰写明文外部邮件
311
将加密的邮件存储到共享存储
306
307
接收方在本地区块链中?
否
用加密的共有密码和存储索引作为内容构造外部邮件
308
是
310
推送邮件合约以及将签名存储到区块链
通过SMTP协议发送互联网邮件
309

图3

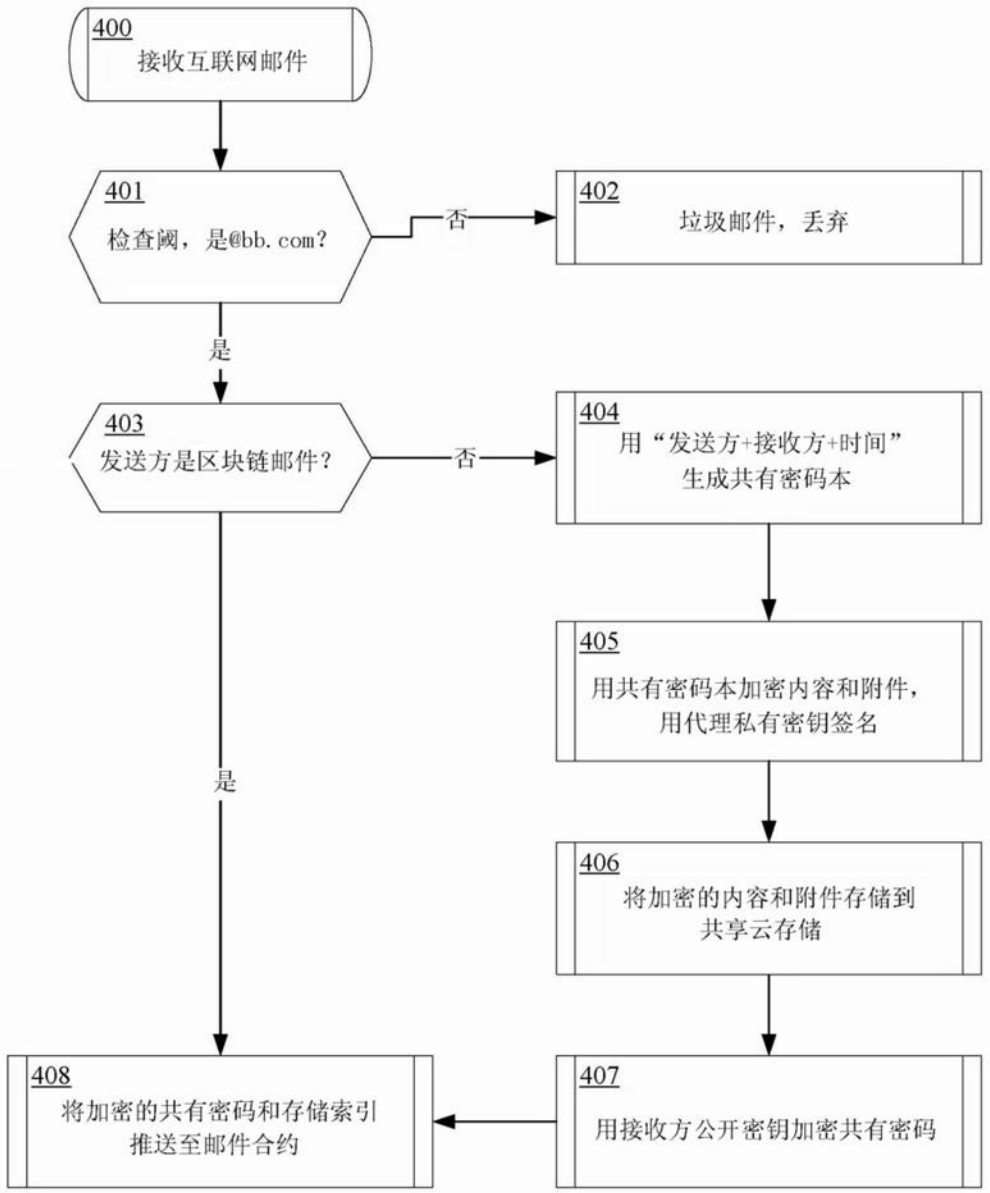

400
接收互联网邮件
401
检查阈，是@bb.com?
否
402
垃圾邮件，丢弃
是
403
发送方是区块链邮件？
否
404
用“发送方+接收方+时间”
生成共有密码本
405
用共有密码本加密内容和附件，
用代理私有密钥签名
406
将加密的内容和附件存储到
共享云存储
是
407
用接收方公开密钥加密共有密码
408
将加密的共有密码和存储索引
推送至邮件合约

图4

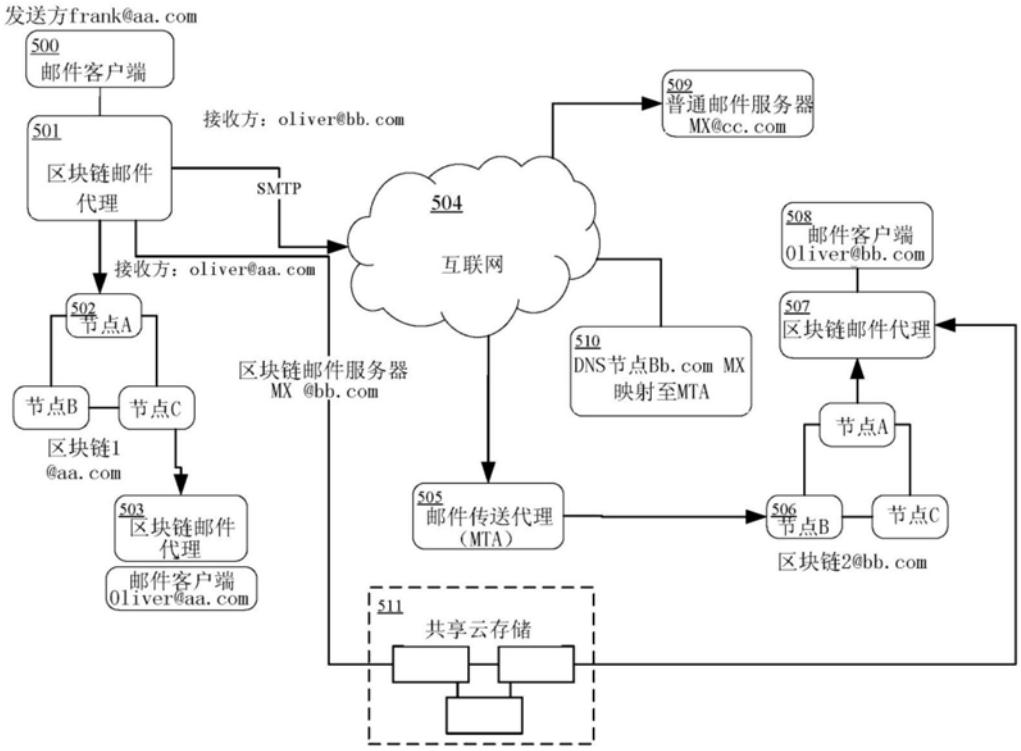

发送方frank@aa.com
500
邮件客户端
501
区块链邮件代理
接收方：oliver@bb.com
SMTP
接收方：oliver@aa.com
504
互联网
509
普通邮件服务器
MX@cc.com
508
邮件客户端
Oliver@bb.com
507
区块链邮件代理
502
节点A
节点B
节点C
区块链1
@aa.com
503
区块链邮件代理
邮件客户端
Oliver@aa.com
区块链邮件服务器
MX @bb.com
510
DNS节点Bb.com MX
映射至MTA
505
邮件传送代理
（MTA）
节点A
506
节点B
节点C
区块链2@bb.com
511
共享云存储

图5

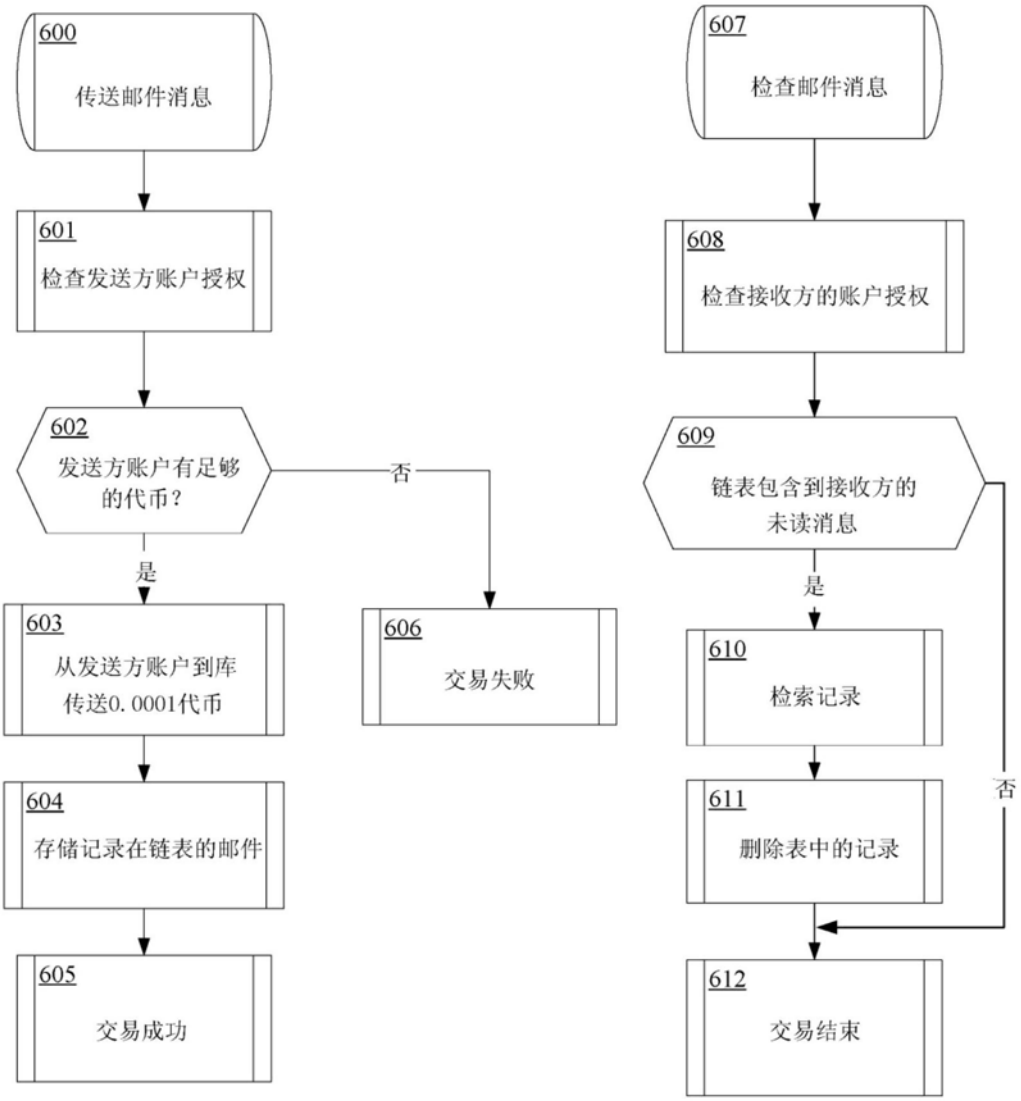

600
传送邮件消息
601
检查发送方账户授权
602
发送方账户有足够的代币？
否
是
603
从发送方账户到库传送0.0001代币
606
交易失败
604
存储记录在链表的邮件
605
交易成功
607
检查邮件消息
608
检查接收方的账户授权
609
链表包含到接收方的未读消息
是
否
610
检索记录
611
删除表中的记录
612
交易结束

图6