(19)中华人民共和国国家知识产权局

(12)发明专利

(10)授权公告号 CN 110071807 B
(45)授权公告日 2022.03.01

(21)申请号 201910225548.9
(22)申请日 2019.03.22
(65)同一申请的已公布的文献号
申请公布号 CN 110071807 A
(43)申请公布日 2019.07.30
(73)专利权人 湖南天河国云科技有限公司
地址 410000 湖南省长沙市长沙经济技术开发区星沙产业基地开元东路1318号综合楼308
(72)发明人 谭林 申涛 李旷 杨征 刘秀
(74)专利代理机构 长沙德恒三权知识产权代理事务所(普通合伙) 43229
代理人 徐仰贵
(51)Int.Cl.
H04L 9/32(2006.01)
H04L 9/40(2022.01)
H04L 67/104(2022.01)
(56)对比文件
CN 107592293 A,2018.01.16
CN 108182581 A,2018.06.19
CN 108512667 A,2018.09.07
CN 108512667 A,2018.09.07
US 2018082291 A1,2018.03.22
审查员 李文聪

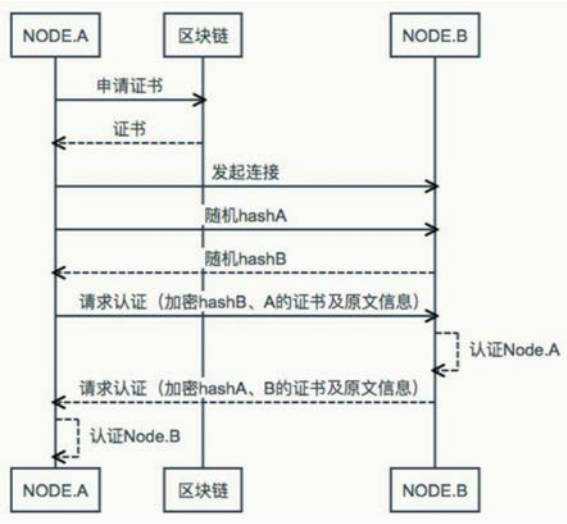
权利要求书1页 说明书3页 附图1页

(54)发明名称

区块链点对点节点认证方法、系统及计算机可读存储介质

(57)摘要

本发明公开了一种区块链点对点节点认证方法、系统及计算机可读存储介质，点对点节点认证方法包括证书签发流程和点对点认证流程；(一)证书签发流程：由区块链的节点向区块链提出申请，区块链进行审核后生成加密证书给提出申请的节点；(二)点对点认证流程：节点A与节点B基于随机码、证书进行互相认证。这种区块链点对点节点认证方法、系统及计算机可读存储介质易于实施，具有去中心化及使用灵活方便的优点。



CN 110071807 B

1.一种区块链点对点节点认证方法,其特征在于,包括证书签发流程和点对点认证流程;

(一)证书签发流程:

为需要进行认证的节点向区块链合约提出申请,区块链合约按照固定的流程进行审核后生成加密证书给提出申请的节点;节点在提出申请时,向区块链某一个固定账户进行转账产生交易ID,区块链合约需要通过这个交易ID来验证申请证书的节点确实提供了抵押资产;

(二)点对点认证流程:

节点A与节点B基于随机码、证书进行互相认证。

2.根据权利要求1所述的区块链点对点节点认证方法,其特征在于,证书签发流程的步骤如下:

(1)节点提供基本信息向区块链申请证书;

(2)区块链根据节点提供的基本信息进行哈希运算,然后用自己的私钥进行加密签名生成证书给节点。

3.根据权利要求1-2任一项所述的区块链点对点节点认证方法,其特征在于,点对点认证的具体流程如下:

(1)某节点A收到连接请求后,发送一个随机码到节点B,之后等待节点B回应;

(2)节点B提供证书以及申请证书时的原文信息,同时用自己的私钥对收到的随机码进行加密后回应节点A;

(3)节点A对节点B回应过来的证书进行校验:

对证书原文进行哈希运算,同时用区块链中心提供的公钥对证书进行解密,最后对比得到的哈希值是否匹配;

(4)节点A校验完B发送的证书后,即得到了B的证书对应的公钥,并用该公钥来解析出节点B发过来的加密后的随机码;

(5)节点A继续校验随机码是否和自己发过去的随机码匹配,若匹配,则完成节点A和节点B的验证。

4.一种基于区块链的点对点节点认证系统,其特征在于,包括:

区块链,用于对节点的认证请求进行验证并颁发证书;

区块链中的节点,具有以下模块:

(1)证书请求模块,用于向区块链申请证书;

(2)向另一个节点提出认证请求的模块:用于向另一个节点提出认证请求;

(3)验证模块:对另一个节点发出的认证资料进行校验,认证资料包括区块链签发的证书;

采用权利要求1-2任一项所述的区块链点对点节点认证方法实施证书签发和点对点认证。

5.一种计算机可读存储介质,其特征在于,所述存储介质上存储有计算机程序,当所述计算机程序被处理器执行时,能实现如权利要求1-2任一项所述的点对点节点认证方法实施证书签发和点对点认证。

区块链点对点节点认证方法、系统及计算机可读存储介质

技术领域

[0001] 本发明涉及一种区块链点对点节点认证方法、系统及计算机可读存储介质。

背景技术

[0002] 点对点技术为现阶段的热门技术，点对点：也叫P2P，P2P是英文peer to peer lending(或peer-to-peer)的缩写，意即个人对个人。本专利中点对点主要指的P2P网络中的两个服务之间。

[0003] 现在的点对点网络要么没有认证，要么是通过中心化的服务器进行证书签发。

[0004] 首先，现在的很多点对点网络并没有任何认证机制，即任何几点都可以随时进入到整个网络中来，如果这个点对点网络对节点要求严格，比如要求满足一定的性能和稳定性，则开放的点对点网络无法满足要求。

[0005] 其次传统的证书签发，例如WEB，都是通过中心化的机构进行的证书签发，这就存在中心化带来的风险，如可信任性，垄断性等。

[0006] 所以，本发明基于区块链，为点对点网络设计一种去中心化的认证机制，有效解决点对点网络中的节点认证机制，同时也避免了证书签发机构中心化的问题。

[0007] 因此，有必要设计一种新的区块链点对点节点认证方法、系统及计算机可读存储介质。

发明内容

[0008] 本发明所要解决的技术问题是提供一种区块链点对点节点认证方法、系统及计算机可读存储介质，该区块链点对点节点认证方法、系统及计算机可读存储介质易于实施。

[0009] 发明的技术解决方案如下：

[0010] 一种区块链点对点节点认证方法，其特征在于，包括证书签发流程和点对点认证流程；

[0011] (一)证书签发流程：

[0012] 为需要进行认证的节点向区块链合约提出申请，区块链合约按照固定的流程进行审核后生成加密证书给提出申请的节点；

[0013] (二)点对点认证流程：

[0014] 节点A与节点B基于随机码、证书进行互相认证。

[0015] 证书签发流程的步骤如下：

[0016] (1)节点提供基本信息向区块链申请证书；

[0017] (2)区块链根据节点提供的基本信息进行哈希运算，然后用自己的私钥进行加密签名生成证书给节点。

[0018] 节点在提出申请时，向区块链某一个固定账户进行转账产生交易ID，区块链合约需要通过这个交易ID来验证申请证书的节点确实提供了抵押资产。

[0019] 点对点认证的具体流程如下：

[0020] (1)某节点A收到连接请求后,发送一个随机码到节点B,之后等待节点B回应;

[0021] (2)节点B提供证书以及申请证书时的原文信息,同时用自己的私钥对收到的随机码进行加密后回应节点A;

[0022] (3)节点A对节点B回应过来的证书进行校验:

[0023] 对证书原文进行哈希运算,同时用区块链中心提供的公钥对证书进行解密,最后对比得到的哈希值是否匹配;

[0024] (4)节点A校验完B发送的证书后,即得到了B的证书对应的公钥,并用该公钥来解析出节点B发过来的加密后的随机码;

[0025] (5)节点A继续校验随机码是否和自己发过去的随机码匹配,若匹配,则完成节点A和节点B的验证。

[0026] 一种基于区块链的点对点节点认证系统,包括:

[0027] 区块链,用于对节点的认证请求进行验证并颁发证书;

[0028] 区块链中的节点,具有以下模块:

[0029] (1)证书请求模块,用于向区块链申请证书;

[0030] (2)向另一个节点提出认证请求的模块:用于向另一个节点提出认证请求;

[0031] (3)验证模块:对另一个节点发出的认证资料进行校验,认证资料包括区块链签发的证书;

[0032] 采用前述的区块链点对点节点认证方法实施证书签发和点对点认证。

[0033] 一种计算机可读存储介质,所述存储介质上存储有计算机程序,当所述计算机程序被处理器执行时,能实现前述的点对点节点认证方法实施证书签发和点对点认证。

[0034] 有益效果:

[0035] 本发明的区块链点对点节点认证方法、系统及计算机可读存储介质,采用基于区块链的证书签发、点对点认证方案,能为点对点网络带来以下效益:

[0036] 1、本发明能有效的封闭点对点网络,为封闭性网络提供扎实的基础支撑。

[0037] 2、本发明完成覆盖从证书签发到实际认证,能直接应用在需要进行节点认证的点对点网络环境中。

附图说明

[0038] 图1为区块链点对点节点认证方法、系统及计算机可读存储介质的流程图。

具体实施方式

[0039] 以下将结合附图和具体实施例对本发明做进一步详细说明:

[0040] 实施例1:

[0041] 如图1所示,本发明可以进行证书签发,并提供给点对点网络进行节点认证。

[0042] 首先,基于区块链的证书签发,主要是解决传统签发结构的中心化痛点,将签发流程和签发结果上链,形成公正、公开的证书记录。

[0043] 具体的签发流程有:

[0044] 1、节点抵押一定的资产来保证可提供服务的稳定性。

[0045] 2、节点提供基本信息向区块链申请证书。

[0046] 3、区块链对节点的抵押资产进行验证。

[0047] 4、区块链根据节点提供的基本信息进行哈希运算，然后用自己的私钥进行加密签名生成证书给节点。

[0048] 哈希运算的简介:Hash，一般翻译做散列、杂凑，或音译为哈希，是把任意长度的输入(又叫做预映射pre-image)通过散列算法变换成固定长度的输出，该输出就是散列值。这种转换是一种压缩映射，也就是，散列值的空间通常远小于输入的空间，不同的输入可能会散列成相同的输出，所以不可能从散列值来确定唯一的输入值。简单的说就是一种将任意长度的消息压缩到某一固定长度的消息摘要的函数。

[0049] 其次，点对点网络中的节点，在请求链接对方时，都立刻要求对方进行身份认证，这里的认证方向为双向，即互相验证对方的证书有效性。

[0050] 具体某一方的认证流程为：

[0051] 1、某节点A收到连接请求后，立刻发送一个随机码过去，接下来等待对方回应。

[0052] 2、对方节点B需要提供证书，以及申请证书时的原文信息，同时用自己的私钥对收到的随机码进行加密进行回应。

[0053] 3、节点A对B回应过来的证书进行校验:对证书原文进行哈希运算，同时用区块链中心提供的公钥对证书进行解密，最后对比得到的哈希值是否匹配。

[0054] 4、节点A校验完B发过来的证书后，即得到了B的证书对应的公钥，接下来用这个公钥去验证B发过来的加密后的随机码。

[0055] 5、节点A继续校验随机码是否和自己发过去的匹配。

[0056] 最后，结合证书签发和节点认证流程，组成完整的一套基于区块链的点对点节点认证方案。

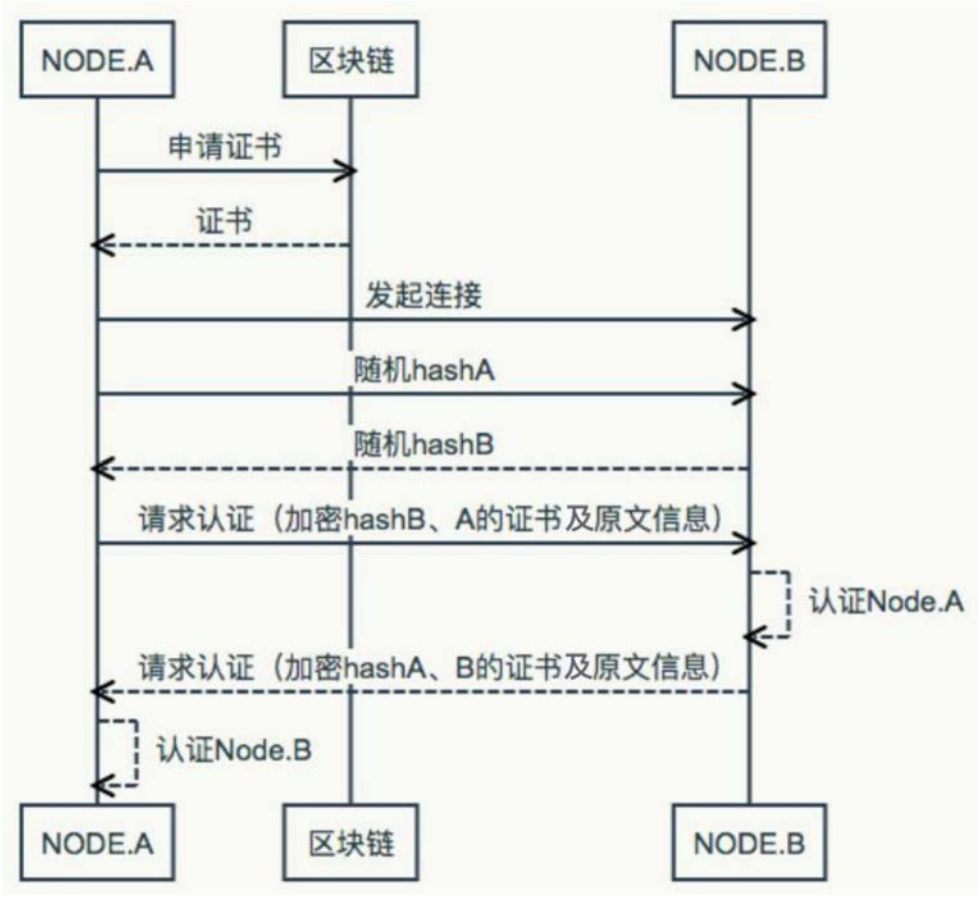

NODE.A
区块链
NODE.B
申请证书
证书
发起连接
随机hashA
随机hashB
请求认证（加密hashB、A的证书及原文信息）
认证Node.A
请求认证（加密hashA、B的证书及原文信息）
认证Node.B
NODE.A
区块链
NODE.B

图1