(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 108009811 A
(43)申请公布日 2018.05.08

(21)申请号 201711237256.4

(22)申请日 2017.11.30

(71)申请人 中国人民解放军国防科技大学
地址 410073 湖南省长沙市开福区砚瓦池正街47号
申请人 上海优刻得信息科技有限公司

(72)发明人 史佩昌 杨识澜 王怀民 刘惠 岳喜坤 季昕华 邱模炯 刘畅 刘源 司照凯

(74)专利代理机构 湖南兆弘专利事务所(普通合伙) 43008
代理人 谭武艺

(51)Int.Cl.
G06Q 20/08(2012.01)
G06Q 20/22(2012.01)
G06Q 20/40(2012.01)
H04L 29/08(2006.01)

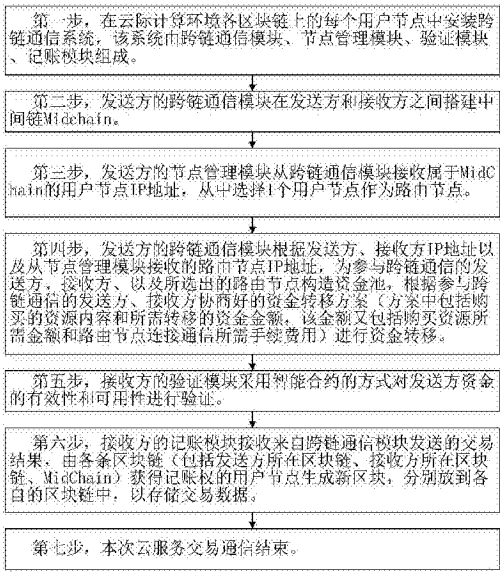
权利要求书4页 说明书11页 附图4页

(54)发明名称

一种面向云际计算环境价值交换的跨链通信方法

(57)摘要

本发明公开了一种面向云际计算环境价值交换的跨链通信方法,目的是保证价值交换过程的安全可靠和高效。技术方案是在各区块链上的每个用户节点中安装由跨链通信模块、节点管理模块、验证模块、记账模块组成的跨链通信系统,建立中间链,从中间链上选择路由节点,由路由节点完成链与链之间的价值转移和沟通交流;发送方的跨链通信模块为发送方、接收方、路由节点构造资金池,根据资金转移方案进行资金转移,接收方的验证模块采用智能合约的方式对发送方资金的有效性和可用性进行验证;接收方的记账模块广播交易结果,发送方、接收方、MidChain生成新区块以存储交易数据。采用本发明可保证价值交换过程的安全可靠和高效,实现链与链之间的无缝跨链通信。



CN 108009811 A

1.一种面向云际计算环境价值交换的跨链通信方法,其特征在于包括以下步骤:

第一步,在云际计算环境各区块链上的每个用户节点中安装跨链通信系统,该系统由跨链通信模块、节点管理模块、验证模块、记账模块组成;区块链上的用户节点或属于某条区块链的用户节点是指将该条区块链上所有区块同步到本地服务器的用户终端,包括云服务消费者和云服务提供商;

跨链通信模块与发送方即交易发送方、接收方即交易接收方、节点管理模块、验证模块、记账模块相连,负责搭建中间链、构造路由节点资金池,同时负责发送方、接收方、路由节点之间的通信并进行资金转移;它根据发送方发送的请求,确定发送方地址和接收方地址,根据这两个地址构建出连接发送方与接收方的中间链,将中间链上的所有用户节点IP地址送给节点管理模块;跨链通信模块从节点管理模块接收路由节点IP地址,根据路由节点结果进行通信连接并进行云服务交易,同时将交易中涉及的资金发送给验证模块;跨链通信模块从验证模块接收交易验收结果,根据交易验收结果继续执行交易或终止;跨链通信模块完成交易后,将交易信息发送给记账模块;

节点管理模块与跨链通信模块相连,从跨链通信模块接收中间链上的用户节点IP地址,从中间链上的用户节点中选择参与跨链通信的路由节点,将路由节点IP地址发送给跨链通信模块;

验证模块与跨链通信模块相连,从跨链通信模块接收交易资金,负责验证交易资金的有效性和可用性,并将交易验证结果返回给跨链通信模块;

记账模块与跨链通信模块、发送方、接收方相连,从跨链通信模块接收交易信息,负责为交易产生账本并同步给发送方和接收方所在链的所有用户节点;

第二步,发送方的跨链通信模块在发送方和接收方之间搭建中间链,方法如下:

2.1发送方的跨链通信模块根据发送方地址StartAddr和接收方地址EndAddr,构建中间链MidChain,方法为:

2.1.1将中间链数据结构确定为区块链,区块中的交易信息包括的内容为:交易记录索引号、发送方地址、接收方地址、交易资源内容、交易转移金额、生成交易的时间戳;交易记录索引号是对区块链中第i个区块中记载的每一笔交易记录按时间顺序进行的编号,用于资金验证和交易完成后查看交易信息;发送方地址指发起交易的用户节点的IP地址;接收方地址指接收交易的用户节点的IP地址;交易资源内容指云服务交易中,云服务提供商向云服务消费者提供的云服务资源;交易转移金额指云服务交易中,云服务消费者购买云服务提供商提供的资源所需的金额;生成交易的时间戳指一串表示交易生成时间的字符序列;i为正整数;

2.1.2初始化中间链的第一个区块;

2.1.3创建属于MidChain的用户节点,方法为:分别在发送方所在区块链、接收方所在区块链中任意选择至少5个不同的用户节点服务器来同步MidChain上的区块信息,并将同步了的服务器地址记录为用户节点的IP地址;

2.1.4发送方的跨链通信模块将中间链上的所有用户节点IP地址发送给发送方的节点管理模块;

第三步,发送方的节点管理模块从跨链通信模块接收属于MidChain的用户节点IP地址,从中选择1个用户节点作为路由节点,方法是:

3.1采用PoW共识算法来确定候选节点范围；

3.2从采用PoW共识算法选择出的候选节点中，对它们连接交易双方通信所需的手续费高低进行排序，选择手续费最低的候选节点作为MidChain上的路由节点，简称路由节点；

3.3发送方的节点管理模块将路由节点IP地址发送给发送方的跨链通信模块；

第四步，发送方的跨链通信模块根据发送方、接收方IP地址以及从节点管理模块接收的路由节点IP地址，为参与跨链通信的发送方、接收方、以及所选出的路由节点构造资金池，根据参与跨链通信的发送方、接收方协商好的资金转移方案进行资金转移，具体步骤如下：

4.1为参与跨链通信的发送方、接收方以及路由节点这三方建立独立的资金池，即用形如(节点IP地址，预存资金金额)的键值对来表示节点及其对应的预存资金金额；

4.2发送方、接收方以及路由节点这三方都预存一部分资金到资金池中，即给这三方的(节点IP地址，预存资金金额)分别赋三者的IP地址和相应的预存资金值；

4.3发送方将资金转移方案广播给路由节点和接收方，路由节点及接收方收到广播出的资金转移方案，核对资金转移方案内容是否正确，若正确，则接收方将确认结果发送给路由节点，路由节点收集好确认结果后签名，将附上签名的资金转移方案返回给发送方，同时，路由节点和接收方将交易中涉及的资金发送给自己的验证模块，转第五步；若不正确，则接收方将错误信息发送给路由节点，路由节点收集好错误信息并附上自己的签名，将错误信息发送至发送方，发送方检查修改资金转移方案后，再次广播出来，转4.3步；所述资金转移方案内容包括资金转移金额和路由节点手续费，所述确认结果是认为方案内容正确无误的结果，所述确认结果包括路由节点自身的确认结果，所述错误信息包括路由节点自己发现的错误信息；

第五步，接收方的验证模块采用智能合约的方式对发送方资金的有效性和可用性进行验证，验证的具体方法是：

5.1在智能合约即部署在验证模块中的一段自动执行判断动作的程序中输入资金的判断条件：判断资金来源是否有效，即发送方是否有足够的资金进行转移；

5.2遍历发送方所属区块链的每一个区块，查询发送方的交易信息即交易转移金额和交易资源内容，判断发送方是否存在足够资金用于本次交易，即发送方的转入资金总额减去转出资金总额是否大于本次交易需要转出的资金数额，若不存在足够资金，说明验证失败，资金转移方案作废，交易双方协调下一步操作，根据协调结果，或转4.3步，或转第七步终止本次交易；若存在足够资金，则说明验证成功，将验证成功的结果返回给发送方的跨链通信模块，转5.3步；

5.3发送方的跨链通信模块根据资金转移方案中涉及的交易转移金额重新分配资金池中的资金，即将发送方的(节点IP地址，预存资金金额)改为(节点IP地址，现有资金金额)完成资金转移，(现有资金金额＝预存资金金额-交易转移金额)，并将交易信息发送给记账模块；

第六步，接收方的记账模块接收来自跨链通信模块发送的交易信息，由发送方所在区块链、接收方所在区块链、MidChain获得记账权的用户节点生成新区块，分别放到各自的区块链中，方法是：

6.1记账模块将交易信息进行哈希运算后，广播给发送方和接收方所在区块链、以及中

间链上的每个用户节点；

6.2发送方所在链、接收所在链以及中间链上的所有用户节点争夺记账权，方法是采用PoW共识算法进行算力竞争，选出算力最强的1个用户节点；每条区块链最终有一个用户节点获得记账权，并在该用户节点所属区块链上生成一个新的区块，并将区块大小、交易计数器、区块头、交易信息一同放入新生成的区块中；

6.3发送方和接收方所在区块链以及中间链上的各用户节点将新生成的区块同步下载到各自的本地账本；

第七步，本次云服务交易通信结束。

2.如权利要求1所述的一种面向云际计算环境价值交换的跨链通信方法，其特征在于2.1.2步所述初始化中间链的第一个区块的方法是：

2.1.2.1将区块大小确定为整个区块所占字节大小；

2.1.2.2将交易计数器初始化为0；

2.1.2.3初始化中间链第一个区块的区块头：

2.1.2.3.1将区块ID初始化为001；

2.1.2.3.2将随机数初始化为0；

2.1.2.3.3将上一区块哈希值初始化为0；

2.1.2.3.4将难度值初始化为0；

2.1.2.3.5将生成区块的时间戳确定为该区块生成时刻的时间；

2.1.2.3.6将Merkle根哈希值初始化为0；

2.1.2.4初始化区块中的交易信息：

2.1.2.4.1将交易记录索引号初始化为Mid-1-1；

2.1.2.4.2将交易资源内容初始化为空；

2.1.2.4.3将交易转移金额初始化为0；

2.1.2.4.4将发送方地址确定为StartAddr；

2.1.2.4.5将接收方地址确定为EndAddr；

2.1.2.4.6将生成交易的时间戳初始化为0。

3.如权利要求1所述的一种面向云际计算环境价值交换的跨链通信方法，其特征在于3.1步所述采用PoW共识算法来确定候选节点范围的方法是：采用PoW共识算法进行算力竞争，选择算力最强的前五个用户节点作为侯选节点，所述算力最强是指用户节点通过运算最快得到一个随机数，使得该随机数与区块头内6个数据使用Merkle Proof方法合并在一起之后得到的数满足难度值设定，难度值＝最大目标值÷当前目标值，最大目标值为固定的哈希值，当前目标值为当前区块即最新生成的这个区块的区块头哈希值。

4.如权利要求3所述的一种面向云际计算环境价值交换的跨链通信方法，其特征在于所述最大目标值为为0x00000000FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF。

5.如权利要求1所述的一种面向云际计算环境价值交换的跨链通信方法，其特征在于6.2步所述将区块大小、交易计数器、区块头、交易信息一同放入新生成的区块中的方法是：

6.2.1区块大小确定为整个区块所占的字节大小；

6.2.2交易计数器确定为该区块中所包含的交易次数；

6.2.3区块头中所包含的6个数据分别赋值：

6.2.3.1区块ID为00i，i为区块序号，随着区块的增加，i的值按n+1，n+2，n+3，…的规律递增，n为获得记账权的用户节点所属区块链原有区块数，n为正整数；

6.2.3.2随机数即为获得记账权的用户节点在争夺记账权时运算获得的随机数值；

6.2.3.3上一区块哈希值为上一个区块的哈希值；

6.2.3.4难度值通过公式难度值＝最大目标值÷当前目标值确定；

6.2.3.5生成区块的时间戳确定为该区块生成时刻的时间；

6.2.3.6 Merkle根哈希为交易信息通过Merkle Proof方法合并得到的哈希值；

6.2.4交易信息所包含的6个数据分别赋值：

6.2.4.1将交易记录索引号赋值为Mid-(i-1)；

6.2.4.2将交易资源内容确定为具体交易的资源内容；

6.2.4.3将交易转移金额确定为具体交易所转移的金额数目；

6.2.4.4将发送方地址确定为StartAddr；

6.2.4.5将接收方地址确定为EndAddr；

6.2.4.6将生成交易的时间戳确定为交易生成时刻的时间。

6.如权利要求1所述的一种面向云际计算环境价值交换的跨链通信方法，其特征在于6.1步所述哈希运算是一种将目标文本转换成具有相同长度的杂凑字符串的算法，采用SHA-256哈希算法。

7.如权利要求1所述的一种面向云际计算环境价值交换的跨链通信方法，其特征在于所述发送方为购买资源并支付金额的一方，所述接收方为提供资源并接受金额的一方。

一种面向云际计算环境价值交换的跨链通信方法

技术领域

[0001] 本发明涉及区块链以及分布式云计算领域，具体涉及一种利用区块链作为基础技术支撑，跨链进行价值交换的通信方法。

背景技术

[0002] 区块链的概念在08年中本聪的《Bitcoin:A Peer-to-Peer Electronic Cash System》(即《比特币：一种点对点的电子现金系统》)一文中，作为比特币的底层技术被提出。为了实现一种点对点的去中心化可信记账系统，中本聪将比特币的每次交易信息分别放入一个区块(即一个用于存放交易数据哈希值和时间戳的块结构)中，每个区块再按照时间戳顺序连成一条链，称为区块链。某条区块链上的用户节点(也可称属于某条区块链的用户节点)是指将该条区块链上所有区块同步到本地服务器的用户终端，在云际计算环境中，特指云服务消费者和云服务提供商。一条区块链上有多个用户节点，所有用户节点都具备广播功能、验证功能、分配资金池中的资金、资金转移功能。此外，由于区块链本身就可看作一本分布式帐本，所以将每个用户节点同步到本地服务器的整条区块链称作本地账本，随着新区块的生成，本地账本也要同步进行更新。这样通过区块链的形式，中本聪完美地实现了对等网络下的去中心化可信记账系统。如图2所示，区块链由多个区块(规定第一个区块叫做创世块)按照生成交易的时间戳顺序连成。每个区块由区块头和其他三个数据域组成。区块头包含6个数据域，分别为：区块ID、随机数、上一区块哈希值、生成区块的时间戳、Merkle根哈希值、难度值。区块ID是对每一个区块的编号，用于验证模块和交易完成后查看交易信息；随机数是和交易信息做哈希运算的一个数字(哈希运算是一个把任意长度的数据映射成固定长度数据的运算，比特币中使用到的是SHA-256哈希算法，来源于美国国家标准与技术研究院发布的《安全散列标准》)，用于用户节点依据PoW共识机制争夺记账权；上一区块哈希值是指与所属区块相连的上一个区块的各数据域信息合并进行哈希运算所得到的值，第一个区块的上一区块哈希值为0；生成区块的时间戳指一串表示区块生成时间的字符序列；Merkle根哈希值是将交易信息里面的各条交易信息通过Merkle Proof方法(Nakamoto S.Bitcoin:Apeer-to-peer electronic cash system[J].2008，即《比特币：一种点对点的电子现金系统》第4页第22-31行)合并而成；难度值是用户争夺记账权时计算哈希值的难度系数。区块中的另外三个数据域分别为：区块大小、交易计数器、交易信息。区块大小是用字节数表示的区块的大小；交易计数器是该区块中记录的交易数量；交易信息是对每条交易记录的信息，由用户节点根据具体的交易进行记录。之后，受到比特币的灵感启示，越来越多致力于区块链基础设施发展的企业涌入行业市场，极具代表性的包括Blockstream、Ripple以及Ethereum等。

[0003] 借鉴比特币的思想，以太坊尝试在比特币协议之上构建一个总体上完全无需信任基础的智能合约平台。它是一个创新的可编程的区块链平台，允许任何人在平台中建立和使用通过区块链技术运行的去中心化应用。相比于比特币区块链，纯粹是一个关于交易信息的列表，以太坊区块链以账户为基础单元，它跟踪每个账户的状态，所有以太坊区块链上

的状态转换都是账户之间价值和信息的转移。账户分为外部账户和合约账户，外部账户由用户通过私钥控制，合约账户则是由合约编码——即智能合约——来控制。

[0004] 关于智能合约，早在1994年，密码学家尼克萨博(Nick Szabo)就在自己的网站中提出了智能合约的概念，但一直不能应用于现实。直到中本聪的比特币被提出之后，才得以继续发展。智能合约是一段可自动执行的计算机程序(如《Ethereum White Paper:ANEXT GENERATION SMART CONTRACT&DECENTRALIZED APPLICATION PLATFORM》，即《以太坊：下一代智能合约和去中心化应用平台》，第13页16行-第17页24行，介绍了以太坊中智能合约的概念、怎么编写以及如何使用。文中讲到：“Smart contracts,cryptographic"boxes"that contain value and only unlock it if certain conditions are met”，说明智能合约是一个包含有价值，且仅当满足某些特定条件时才可被解锁的加密盒子，即一段自动执行判断动作的程序)，在程序中输入用于判断动作执行与否的条件，当一个预先编好的条件被触发时，智能合约执行相应的合同条款。将它部署到区块链上，可实现对交易流程和交易数据的自动操控，进而也可通过执行这段程序实现与现实资产的交互。

[0005] 如果说区块链解决了交易通道不可信问题的话，那么共识机制则是解决了区块链如何在分布式场景下达成一致性的问题。具有代表性的共识算法有PBFT(Practical Byzantine Fault Tolerance，实用拜占庭容错算法)、PoW(Proof of Work，工作量证明)共识算法(Nakamoto S.Bitcoin:Apeer-to-peer electronic cashsystem[J].2008，即《比特币：一种点对点的电子现金系统》第4页第1-22行)、PoS(Proof of Stake，股权证明)共识算法等。PBFT是在拜占庭将军问题场景下产生的一种基于消息传递的共识算法。异步网络环境下PBFT算法所能允许的最大容错数为(n-1)/3(n为总节点数)。PBFT算法经过预准备、准备、执行三个阶段达成一致性，而这三阶段均有可能因为失败而重复进行。基于工作量证明的PoW共识算法主要用于区块的记账权争夺中。一个区块的哈希值(即将该区块中的交易记录通过哈希加密运算所得的结果，交易记录由一串数字表示)由N个前导零构成，零的个数取决于网络的难度值。要得到合理的哈希值需要经过大量尝试计算，计算时间取决于机器的哈希运算速度。区块链上的用户基于算力来争夺记账权，从而获得比特币收益，这一操作也被称为挖矿。由于寻找到正确的哈希值是一个概率事件，当节点拥有占全网m%的算力时，该节点即有m%的概率找到区块的哈希值，m为实数。但是，PoW资源浪费度极高，且最终运算并没有实际用途。PoS是基于权益的证明算法，它认为区块链上的记录和证明应该由那些在链上具有经济利益的人来维护和保障。通过要求证明人提供一定数量加密货币的所有权而非进行难度极高的工作量证明，PoS从根本上摆脱了PoW的算力浪费。

[0006] 现有的多云服务提供商，例如Inter-Cloud、SuperCloud、Multi-Cloud、FedeartedCloud等，主要侧重于为满足云服务消费者的需求而进行资源的整合，但其缺乏参与者共享协作的平台与机制支撑以及云服务提供商之间合作共赢的服务模式。

[0007] 云际计算(Joint Cloud Computing)是为满足未来云计算的需求，适应云计算的未来发展而提出的可解决现有研究困境的支撑技术，它是以云服务提供商之间开放协作为基础，多云资源深度融合，支持云提供者之间自助协作和利益交换的多云联合，方便开发者通过“软件定义”方式定制云服务、创造云价值的新一代云计算模式。在云际计算场景中，云际链与其它类型的区块链(用户链、业务链)共存，单条区块链内存在价值交换的需求，同时，随着云计算的多样变化和发展，链与链之间的价值交换需求也日益增加。

[0008] 在互联网全球化的发展趋势下，单一区块链结构越来越难以满足多样的交易服务的需求。为了应对复杂多变的云计算交易服务挑战，一些公司提出了跨链进行交易的概念。具有代表性的包括Blockstream公司提出的侧链技术(Sidechain)、Ripple公司提出的跨链协议Interledger等。Blockstream公司提出的侧链是一条用于实现比特币在多个区块链间转移的链。资金转移时，需要等待一个确认期和一个竞赛期。确认期是指资金在转移到侧链之前，需要在资金发送方所处的链上被锁定一段时间，以便能生成足够多的工作量来抵抗攻击。而竞赛期则是用于防止重组时出现双花攻击。这两段时期都分别需要等待1-2天的时间锁定资金。由于花费了过多时间用于处理资金验证，造成了侧链技术的效率低下，并不能满足正常交易的需求。

[0009] Ripple公司提出的Interledger协议是一种用于跨支付系统之间支付的协议。若交易双方处于不同的支付系统，彼此之间是没有直接的交易通道来完成交易的。针对这种情况，Interledger协议提出，在交易资金的发送方(Sender)和接收方(Receiver)之间加入中间件(Connectors)来连接，通过这样的方式，在不同的支付系统之间建立一条可直接交易的通道，同时，通过第三方资金托管平台(Escrow)来实现交易准备时对资金的托管和控制，但Escrow本身具有的巨大敞口风险使得Interledger协议的安全性存在置疑。

[0010] 因此，要实现跨链进行交易或通信，还存在着以下这些技术问题：

[0011] 1.安全性问题。基于数字货币进行链间通信需要对通信双方的权益进行保障，即保证交易货币有效可用；交易记录真实可追溯；恶意攻击的可能性低。因此，需要完善的机制来维护交易的可追溯性和稳定运行，目前技术往往通过第三方(如Interledger中的Escrow)对交易进行监督和维护，由于第三方机构本身具有一定的安全隐患(可能存在欺诈行为)，所以整个价值交换过程的安全并不能得到保证。

[0012] 2.效率问题。要保证安全性，则需要耗费大量时间用于货币验证(包括验证货币的来源是否有效以及货币是否可用)和确帐(确认交易并记录)。目前技术大多耗费大量时间用于验证资金的有效性(如侧链在一次价值转移中，花费了2-4天时间用于锁定资金)，大大降低了价值交换的效率。

发明内容

[0013] 本发明要解决的技术问题是提供一种面向云际计算环境价值交换的跨链通信方法，保证价值交换过程的安全可靠和高效，促进任意两条链之间的交易和沟通交流，实现链与链之间的无缝跨链通信。

[0014] 本发明的技术方案是为了促进链间价值交换，特别是针对某些没有直接连接通道的链而提供跨链通信方案。在云际计算环境中，存在一条称为云际链的区块链，它与其它类型的区块链(包括提供云计算服务的业务链，以及使用云计算服务的用户链)都存在跨链通信的需求。根据Ripple(瑞波)公司提出的Interledger协议(《AProtocol for Interledger Payments》，即《Interledger白皮书》)建立中间件连接不同支付系统的思想，本发明建立连接云际链和任意一条链之间(如图4所示，以业务链A为例)的中间链，通过中间链进行跨链通信进而实现价值交换；同时，采用智能合约的方式对价值交换过程中的资金有效性进行验证，保障交易过程的安全性。本发明采用的区块链与图2所示数据结构相同，对区块中的交易信息域的内容做了规定。每条交易信息包括的内容为：交易记录索引号、发送方地址、

接收方地址、交易资源内容、交易转移金额、生成交易的时间戳。交易记录索引号是对区块链中第i个区块中记载的每一笔交易记录按时间顺序进行的编号，用于资金验证和交易完成后查看交易信息，i为正整数；发送方地址指发起交易的用户节点的IP地址；接收方地址指接收交易的用户节点的IP地址；交易资源内容指云服务交易中，云服务提供商向云服务消费者提供的云服务资源；交易转移金额指云服务交易中，云服务消费者购买云服务提供商提供的资源所需的金额；生成交易的时间戳指一串表示交易生成时间的字符序列。

[0015] 本发明包括以下步骤：

[0016] 第一步，在云际计算环境各区块链上的每个用户节点中安装跨链通信系统，该系统由跨链通信模块、节点管理模块、验证模块、记账模块组成。

[0017] 跨链通信模块与发送方(即交易发送方，本发明默认交易发送方为购买资源并支付金额的一方)、接收方(即交易接收方，本发明默认交易接收方为提供资源并接受金额的一方)、节点管理模块、验证模块、记账模块相连，负责搭建中间链、构造路由节点资金池，同时负责发送方、接收方、路由节点之间的通信并进行资金转移。它根据发送方发送的请求，确定发送方地址和接收方地址，根据这两个地址构建出连接发送方与接收方的中间链，将中间链上的所有用户节点IP地址送给节点管理模块；跨链通信模块从节点管理模块接收路由节点IP地址，根据路由节点结果进行通信连接并进行云服务交易，同时将交易中涉及的资金发送给验证模块；跨链通信模块从验证模块接收交易验收结果，根据交易验收结果继续执行交易或终止；跨链通信模块完成交易后，将交易信息发送给记账模块。

[0018] 节点管理模块与跨链通信模块相连，从跨链通信模块接收中间链上的用户节点IP地址，从中间链上的用户节点中选择参与跨链通信的路由节点，将路由节点IP地址发送给跨链通信模块；

[0019] 验证模块与跨链通信模块相连，从跨链通信模块接收交易资金，负责验证交易资金的有效性和可用性，并将交易验证结果返回给跨链通信模块；

[0020] 记账模块与跨链通信模块、发送方、接收方相连，从跨链通信模块接收交易信息，负责为交易产生账本并同步给发送方和接收方所在链的所有用户节点。

[0021] 第二步，发送方的跨链通信模块在发送方和接收方之间搭建中间链。方法如下：

[0022] 2.1发送方的跨链通信模块根据发送方地址-StartAddr和接收方地址EndAddr，构建中间链，构建的中间链用MidChain表示。方法为：

[0023] 2.1.1将中间链数据结构确定为区块链。

[0024] 2.1.2初始化中间链的第一个区块：

[0025] 2.1.2.1将区块大小确定为整个区块所占字节大小；

[0026] 2.1.2.2将交易计数器初始化为0；

[0027] 2.1.2.3初始化中间链第一个区块的区块头：

[0028] 2.1.2.3.1将区块ID初始化为001；

[0029] 2.1.2.3.2将随机数初始化为0；

[0030] 2.1.2.3.3将上一区块哈希值初始化为0；

[0031] 2.1.2.3.4将难度值初始化为0；

[0032] 2.1.2.3.5将生成区块的时间戳确定为该区块生成时刻的时间；

[0033] 2.1.2.3.6将Merkle根哈希值初始化为0；

[0034] 2.1.2.4初始化区块中的交易信息：

[0035] 2.1.2.4.1将交易记录索引号初始化为Mid-1-1(并以Mid-1-2,Mid-1-3,Mid-1-4的形式依次增长)；

[0036] 2.1.2.4.2将交易资源内容初始化为空；

[0037] 2.1.2.4.3将交易转移金额初始化为0；

[0038] 2.1.2.4.4将发送方地址确定为StartAddr；

[0039] 2.1.2.4.5将接收方地址确定为EndAddr；

[0040] 2.1.2.4.6将生成交易的时间戳初始化为0；

[0041] 2.1.3创建属于MidChain的用户节点,方法为:分别在发送方所在区块链、接收方所在区块链中任意选择至少5个不同的用户节点服务器来同步MidChain上的区块信息,并将同步了的服务器地址记录为用户节点的IP地址。

[0042] 2.1.4发送方的跨链通信模块将中间链上的所有用户节点IP地址发送给发送方的节点管理模块。

[0043] 第三步,发送方的节点管理模块从跨链通信模块接收属于MidChain的用户节点IP地址,从中选择1个用户节点作为路由节点,方法是：

[0044] 3.1采用PoW共识算法来确定候选节点范围,方法是:采用PoW共识算法进行算力竞争,选择算力最强的前五个用户节点作为侯选节点,所述算力最强是指用户节点通过运算最快得到一个随机数,使得该随机数与区块头内6个数据使用Merkle Proof方法合并在一起之后得到的数满足难度值设定,难度值＝最大目标值÷当前目标值(最大目标值为固定的哈希值,一般设为0x00000000FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF;当前目标值为当前区块(即最新生成的这个区块)的区块头哈希值)。

[0045] 3.2由于使用路由节点连接通信需要手续费(路由节点作为跨链通信的中间连接节点,为发送方和接收方连接通信是要收取费用的,具体手续费金额由路由节点自定),因此,从采用PoW共识算法选择出的五个候选节点中,对它们连接交易双方通信所需的手续费高低进行排序,选择手续费最低的候选节点作为MidChain上的路由节点,简称路由节点。

[0046] 3.3发送方的节点管理模块将路由节点IP地址发送给发送方的跨链通信模块。

[0047] 第四步,发送方的跨链通信模块根据发送方、接收方IP地址以及从节点管理模块接收的路由节点IP地址,为参与跨链通信的发送方、接收方、以及所选出的路由节点构造资金池,根据参与跨链通信的发送方、接收方协商好的资金转移方案(方案中包括购买的资源内容和所需转移的资金金额,该金额又包括购买资源所需金额和路由节点连接通信所需手续费用)进行资金转移。具体步骤如下：

[0048] 4.1为参与跨链通信的发送方、接收方以及路由节点这三方建立独立的资金池,即用形如(节点IP地址,预存资金金额)的键值对来表示节点及其对应的预存资金金额；

[0049] 4.2发送方、接收方以及路由节点这三方都预存一部分资金到资金池中,即给这三方的(节点IP地址,预存资金金额)分别赋三者的IP地址和相应的预存资金值。

[0050] 4.3发送方将资金转移方案广播给路由节点和接收方,路由节点及接收方收到广播出的资金转移方案,核对资金转移方案内容(资金转移金额和路由节点手续费)是否正确,若正确,则接收方将确认结果(即认为方案内容正确无误)发送给路由节点,路由节点收集好确认结果(包括自己的确认结果)后签名,将附上签名的资金转移方案返回给发送方,

同时，路由节点和接收方将交易中涉及的资金发送给自己的验证模块，转第五步；若不正确，则接收方将错误信息发送给路由节点，路由节点收集好错误信息(包括自己发现的错误信息)并附上自己的签名，将错误信息发送至发送方，发送方检查修改资金转移方案后，再次广播出来，转4.3步。

[0051] 第五步，接收方的验证模块采用智能合约的方式对发送方资金的有效性和可用性进行验证。验证的具体方法是：

[0052] 5.1在智能合约(即部署在验证模块中的一段自动执行判断动作的程序)中输入资金的判断条件：判断资金来源是否有效，即发送方是否有足够的资金进行转移。

[0053] 5.2遍历发送方所属区块链的每一个区块，查询发送方的交易信息(即交易转移金额和交易资源内容)，判断发送方是否存在足够资金用于本次交易(即发送方的转入资金总额减去转出资金总额是否大于本次交易需要转出的资金数额)，若不存在足够资金，说明验证失败，资金转移方案作废，交易双方协调下一步操作，根据协调结果，或转4.3步，由发送方重新生成资金转移方案并再次广播；或转第七步终止本次交易；若存在足够资金，则说明验证成功，将验证成功的结果返回给发送方的跨链通信模块，转5.3步；

[0054] 5.3发送方的跨链通信模块根据资金转移方案中涉及的交易转移金额重新分配资金池中的资金，即将发送方的(节点IP地址，预存资金金额)改为(节点IP地址，现有资金金额)完成资金转移，(现有资金金额＝预存资金金额-交易转移金额)，并将交易信息发送给记账模块。

[0055] 第六步，接收方的记账模块接收5.3步中来自跨链通信模块发送的交易信息，由各条区块链(包括发送方所在区块链、接收方所在区块链、MidChain)获得记账权的用户节点生成新区块，分别放到各自的区块链中，以存储交易信息，方法是：

[0056] 6.1记账模块将交易信息(包括交易记录索引号、交易资源内容、交易转移金额、发送方地址、接收方地址以及生成交易的时间戳)进行哈希运算(一种将目标文本转换成具有相同长度的杂凑字符串的算法，采用美国国家标准与技术研究院发布的《安全散列标准》中的SHA-256哈希算法)后，广播给发送方和接收方所在区块链、以及中间链上的每个用户节点。

[0057] 6.2各用户节点(包括发送方所在链、接收所在链以及中间链上的所有用户节点)争夺记账权，方法是采用PoW共识算法进行算力竞争，选出算力最强的1个用户节点。每条区块链最终有一个用户节点获得记账权，并在该用户节点所属区块链上生成一个新的区块，并将区块大小、交易计数器、区块头、以及交易信息一同放入新生成的区块中。区块中各内容赋值如下：

[0058] 6.2.1区块大小确定为整个区块所占的字节大小；

[0059] 6.2.2交易计数器确定为该区块中所包含的交易次数；

[0060] 6.2.3区块头中所包含的6个数据分别赋值：

[0061] 6.2.3.1区块ID为00i(i为区块序号，随着区块的增加，i的值按n+1,n+2,n+3,…的规律递增，n为获得记账权的用户节点所属区块链原有区块数，n为正整数)；

[0062] 6.2.3.2随机数即为获得记账权的用户节点在争夺记账权时运算获得的随机数值；

[0063] 6.2.3.3上一区块哈希值为上一个区块的哈希值；

[0064] 6.2.3.4难度值通过公式难度值＝最大目标值÷当前目标值确定；

[0065] 6.2.3.5生成区块的时间戳确定为该区块生成时刻的时间；

[0066] 6.2.3.6Merkle根哈希为交易信息通过Merkle Proof方法合并得到的哈希值；

[0067] 6.2.4交易信息所包含的6个数据分别赋值：

[0068] 6.2.4.1将交易记录索引号赋值为Mid-(i-1)；

[0069] 6.2.4.2将交易资源内容确定为具体交易的资源内容(字符串形式)；

[0070] 6.2.4.3将交易转移金额确定为具体交易所转移的金额数目；

[0071] 6.2.4.4将发送方地址确定为StartAddr；

[0072] 6.2.4.5将接收方地址确定为EndAddr；

[0073] 6.2.4.6将生成交易的时间戳确定为交易生成时刻的时间；

[0074] 6.3发送方和接收方所在区块链以及中间链上的各用户节点将新生成的区块同步下载到各自的本地账本。

[0075] 第七步，本次云服务交易通信结束。

[0076] 采用本发明可以达到以下技术效果：

[0077] 1.由于记账模块将交易信息记录在每个用户节点的本地账本中，规避了只由交易双方记账所带来的交易信息可追溯性差的问题，同时也避免了第三方托管系统资金敞口风险大的问题。

[0078] 2.由于第五步采用智能合约的方式，与现有的资金验证方式相比，效率得到提高。例如，侧链技术中通过两个等待期的资金锁定来完成验证，两个等待期总共花费2-4天的时间，这样一来，严重影响了交易进程。而采用智能合约的方式，针对资金是否有效(即该资金上一笔的交易记录是否存在)、是否可用(即该资金是否已被使用)预先设置规则，自动完成资金验证，减少了不必要的等待时间，加快了确账速度，交易的高效和有序得到保证。

[0079] 3.第四步中采用建立资金池的方式，根据资金分配方案所描述的转移对象和金额来重新分配双方资金池中的资金数额，通过这样的方式，与将具体货币进行直接转移相比，安全性有所提高。同时，此种方式也适用于多次小型交易，直接修改资金金额，减少了不必要的时间延迟，效率更高。

附图说明

[0080] 图1是云际计算环境中链与链之间跨链通信的场景图。

[0081] 图2是本发明区块链的数据结构图。

[0082] 图3是本发明第一步构建的面向云际计算环境的跨链通信系统逻辑结构图；

[0083] 图4是本发明构建的中间链连接发送方与接收方并进行通信的场景图。

[0084] 图5是本发明整体流程图。

具体实施方式

[0085] 图1是背景技术中云际计算环境中链与链之间跨链通信的场景图。在云际计算环境中，存在着各种类别的区块链(区块链的数据结构如图2所示)，包括沟通各种链联接协作的云际链，提供云计算服务的业务链A、业务链B，以及购买使用云计算服务的用户链C、用户链D。处于不同链上的用户节点(包括CSP(云服务提供商)、和CSC(云服务消费者))都存在着

交易的需求。针对这种跨链的情况，需要通信的两条链之间搭建一条中间链来连接。

[0086] 图2是本发明区块链的数据结构图。本发明对区块中的交易信息域的内容做了规定。每条交易信息包括的内容为：交易记录索引号、发送方地址、接收方地址、交易资源内容、交易转移金额、生成交易的时间戳。区块中的其它信息和背景技术中描述的现有区块链完全相同。

[0087] 图3是本发明第一步构建的面向云际计算环境的跨链通信系统逻辑结构图。跨链通信模块与发送方(即交易发送方，本发明默认交易发送方为购买资源并支付金额的一方)、接收方(即交易接收方，本发明默认交易接收方为提供资源并接受金额的一方)、节点管理模块、验证模块、记账模块相连，负责搭建中间链、构造路由节点资金池，同时负责发送方、接收方、路由节点之间的通信并进行资金转移。它根据发送方发送的请求，确定发送方地址和接收方地址，根据这两个地址构建出连接发送方与接收方的中间链，将中间链上的所有用户节点IP地址送给节点管理模块；跨链通信模块从节点管理模块接收路由节点IP地址，根据路由节点结果进行通信连接并进行云服务交易，同时将交易中涉及的资金发送给验证模块；跨链通信模块从验证模块接收交易验收结果，根据交易验收结果继续执行交易或终止；跨链通信模块完成交易后，将交易信息发送给记账模块。

[0088] 节点管理模块与跨链通信模块相连，从跨链通信模块接收中间链上的用户节点IP地址，从中间链上的用户节点中选择参与跨链通信的路由节点，将路由节点IP地址发送给跨链通信模块；

[0089] 验证模块与跨链通信模块相连，从跨链通信模块接收交易资金，负责验证交易资金的有效性和可用性，并将交易验证结果返回给跨链通信模块；

[0090] 记账模块与跨链通信模块、发送方、接收方相连，从跨链通信模块接收交易信息，负责为交易产生账本并同步给发送方和接收方所在链的所有用户节点。

[0091] 图4是本发明构建的中间链联接发送方和接收方并进行通信的场景图。假设云际链与业务链A之间存在通信的需求，但不存在直接的联接通道，于是在两链之间搭建中间链，Node2是中间链的路由节点，发送方、接收方和中间链的路由节点都配有一个资金池。

[0092] 图5是本发明的整体流程图。本发明具体步骤如下：

[0093] 第一步，在云际计算环境各区块链上的每个用户节点中安装跨链通信系统，该系统如图3所示，由跨链通信模块、节点管理模块、验证模块、记账模块组成。

[0094] 第二步，发送方的跨链通信模块在发送方和接收方之间搭建中间链。方法如下：

[0095] 2.1发送方的跨链通信模块根据发送方地址-StartAddr和接收方地址EndAddr，构建中间链，构建的中间链用MidChain表示。方法为：

[0096] 2.1.1将中间链数据结构确定为区块链。

[0097] 2.1.2初始化中间链的第一个区块：

[0098] 2.1.2.1将区块大小确定为整个区块所占字节大小；

[0099] 2.1.2.2将交易计数器初始化为0；

[0100] 2.1.2.3初始化中间链第一个区块的区块头：

[0101] 2.1.2.3.1将区块ID初始化为001；

[0102] 2.1.2.3.2将随机数初始化为0；

[0103] 2.1.2.3.3将上一区块哈希值初始化为0；

[0104] 2.1.2.3.4将难度值初始化为0；

[0105] 2.1.2.3.5将生成区块的时间戳确定为该区块生成时刻的时间；

[0106] 2.1.2.3.6将Merkle根哈希值初始化为0；

[0107] 2.1.2.4初始化区块中的交易信息：

[0108] 2.1.2.4.1将交易记录索引号初始化为Mid-1-1(并以Mid-1-2,Mid-1-3,Mid-1-4的形式依次增长)；

[0109] 2.1.2.4.2将交易资源内容初始化为空；

[0110] 2.1.2.4.3将交易转移金额初始化为0；

[0111] 2.1.2.4.4将发送方地址确定为StartAddr；

[0112] 2.1.2.4.5将接收方地址确定为EndAddr；

[0113] 2.1.2.4.6将生成交易的时间戳初始化为0；

[0114] 2.1.3创建属于MidChain的用户节点，方法为：分别在发送方所在区块链、接收方所在区块链中任意选择至少5个不同的用户节点服务器来同步MidChain上的区块信息，并将同步了的服务器地址记录为用户节点的IP地址。

[0115] 2.1.4发送方的跨链通信模块将中间链上的所有用户节点IP地址发送给发送方的节点管理模块。

[0116] 第三步，发送方的节点管理模块从跨链通信模块接收属于MidChain的用户节点IP地址，从中选择1个用户节点作为路由节点，方法是：

[0117] 3.1采用PoW共识算法来确定候选节点范围，方法是：采用PoW共识算法进行算力竞争，选择算力最强的前五个用户节点作为侯选节点，所述算力最强是指用户节点通过运算最快得到一个随机数，使得该随机数与区块头内6个数据使用Merkle Proof方法合并在一起之后得到的数满足难度值设定，难度值＝最大目标值÷当前目标值(最大目标值为固定的哈希值，一般设为0x00000000FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF；当前目标值为当前区块(即最新生成的这个区块)的区块头哈希值)。

[0118] 3.2由于使用路由节点连接通信需要手续费(路由节点作为跨链通信的中间连接节点，为发送方和接收方连接通信是要收取费用的，具体手续费金额由路由节点自定)，因此，从采用PoW共识算法选择出的五个候选节点中，对它们连接交易双方通信所需的手续费高低进行排序，选择手续费最低的候选节点作为MidChain上的路由节点，简称路由节点。

[0119] 3.3发送方的节点管理模块将路由节点IP地址发送给发送方的跨链通信模块。

[0120] 第四步，发送方的跨链通信模块根据发送方、接收方IP地址以及从节点管理模块接收的路由节点IP地址，为参与跨链通信的发送方、接收方、以及所选出的路由节点构造资金池，根据参与跨链通信的发送方、接收方协商好的资金转移方案进行资金转移。具体步骤如下：

[0121] 4.1为参与跨链通信的发送方、接收方以及路由节点这三方建立独立的资金池，即用形如(节点IP地址，预存资金金额)的键值对来表示节点及其对应的预存资金金额；

[0122] 4.2发送方、接收方以及路由节点这三方都预存一部分资金到资金池中，即给这三方的(节点IP地址，预存资金金额)分别赋三者的IP地址和相应的预存资金值。

[0123] 4.3发送方将资金转移方案广播给路由节点和接收方，路由节点及接收方收到广播出的资金转移方案，核对资金转移方案内容是否正确，若正确，则接收方将确认结果(即

认为方案内容正确无误)发送给路由节点,路由节点收集好确认结果(包括自己的确认结果)后签名,将附上签名的资金转移方案返回给发送方,同时,路由节点和接收方将交易中涉及的资金发送给自己的验证模块,转第五步;若不正确,则接收方将错误信息发送给路由节点,路由节点收集好错误信息(包括自己发现的错误信息)并附上自己的签名,将错误信息发送至发送方,发送方检查修改资金转移方案后,再次广播出来,转4.3步。

[0124] 第五步,接收方的验证模块采用智能合约的方式对发送方资金的有效性和可用性进行验证。验证的具体方法是:

[0125] 5.1在智能合约中输入资金的判断条件:判断资金来源是否有效,即发送方是否有足够的资金进行转移。

[0126] 5.2遍历发送方所属区块链的每一个区块,查询发送方的交易信息(即交易转移金额和交易资源内容),判断发送方是否存在足够资金用于本次交易(即发送方的转入资金总额减去转出资金总额是否大于本次交易需要转出的资金数额),若不存在足够资金,说明验证失败,资金转移方案作废,交易双方协调下一步操作,根据协调结果,或转4.3步,由发送方重新生成资金转移方案并再次广播;或转第七步终止本次交易;若存在足够资金,则说明验证成功,将验证成功的结果返回给发送方的跨链通信模块,转5.3步;

[0127] 5.3发送方的跨链通信模块根据资金转移方案中涉及的交易转移金额重新分配资金池中的资金,即将发送方的(节点IP地址,预存资金金额)改为(节点IP地址,现有资金金额)完成资金转移,现有资金金额=预存资金金额-交易转移金额,并将交易信息发送给记账模块。

[0128] 第六步,接收方的记账模块接收5.3步中来自跨链通信模块发送的交易信息,由各条区块链(包括发送方所在区块链、接收方所在区块链、MidChain)获得记账权的用户节点生成新区块,分别放到各自的区块链中,以存储交易信息,方法是:

[0129] 6.1记账模块将交易信息进行哈希运算(一种将目标文本转换成具有相同长度的杂凑字符串的算法,采用美国国家标准与技术研究院发布的《安全散列标准》中的SHA-256哈希算法)后,广播给发送方和接收方所在区块链、以及中间链上的每个用户节点。

[0130] 6.2各用户节点(包括发送方所在链、接收所在链以及中间链上的所有用户节点)争夺记账权,方法是采用PoW共识算法进行算力竞争,选出算力最强的1个用户节点。每条区块链最终有一个用户节点获得记账权,并在该用户节点所属区块链上生成一个新的区块,并将区块大小、交易计数器、区块头、以及交易信息一同放入新生成的区块中。区块中各内容赋值如下:

[0131] 6.2.1区块大小确定为整个区块所占的字节大小;

[0132] 6.2.2交易计数器确定为该区块中所包含的交易次数;

[0133] 6.2.3区块头中所包含的6个数据分别赋值:

[0134] 6.2.3.1区块ID为00i(i为区块序号,随着区块的增加,i的值按n+1,n+2,n+3,…的规律递增,n为获得记账权的用户节点所属区块链原有区块数,n为正整数);

[0135] 6.2.3.2随机数即为获得记账权的用户节点在争夺记账权时运算获得的随机数值;

[0136] 6.2.3.3上一区块哈希值为上一个区块的哈希值;

[0137] 6.2.3.4难度值通过公式难度值=最大目标值÷当前目标值确定;

[0138] 6.2.3.5生成区块的时间戳确定为该区块生成时刻的时间；

[0139] 6.2.3.6Merkle根哈希为交易信息通过Merkle Proof方法合并得到的哈希值；

[0140] 6.2.4交易信息所包含的6个数据分别赋值：

[0141] 6.2.4.1将交易记录索引号赋值为Mid-(i-1)；

[0142] 6.2.4.2将交易资源内容确定为具体交易的资源内容；

[0143] 6.2.4.3将交易转移金额确定为具体交易所转移的金额数目；

[0144] 6.2.4.4将发送方地址确定为StartAddr；

[0145] 6.2.4.5将接收方地址确定为EndAddr；

[0146] 6.2.4.6将生成交易的时间戳确定为交易生成时刻的时间；

[0147] 6.3发送方和接收方所在区块链以及中间链上的各用户节点将新生成的区块同步下载到各自的本地账本。

[0148] 第七步，本次云服务交易通信结束。

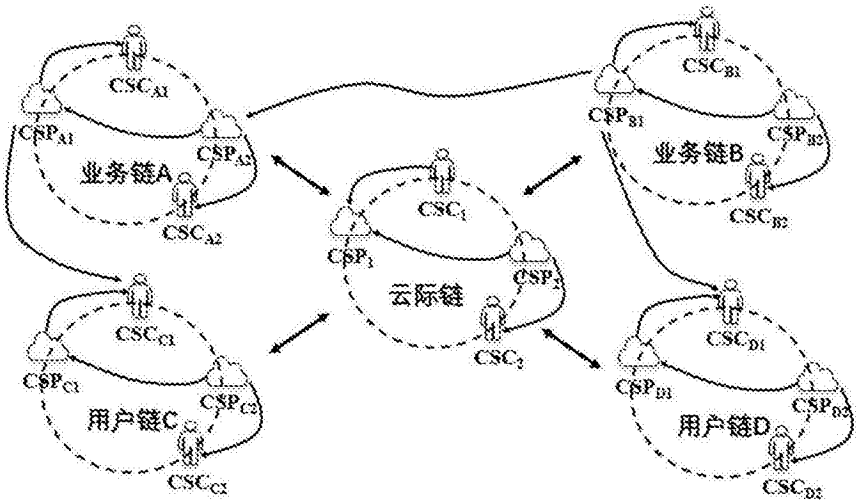

CSC_A1
CSP_A1
CSP_A2
业务链A
CSC_A2
CSC_B1
CSP_B1
CSP_B2
业务链B
CSC_B2
CSC_1
CSP_1
CSP_2
云际链
CSC_2
CSC_C1
CSP_C1
CSP_C2
用户链C
CSC_C2
CSC_D1
CSP_D1
CSP_D2
用户链D
CSC_D2

图1

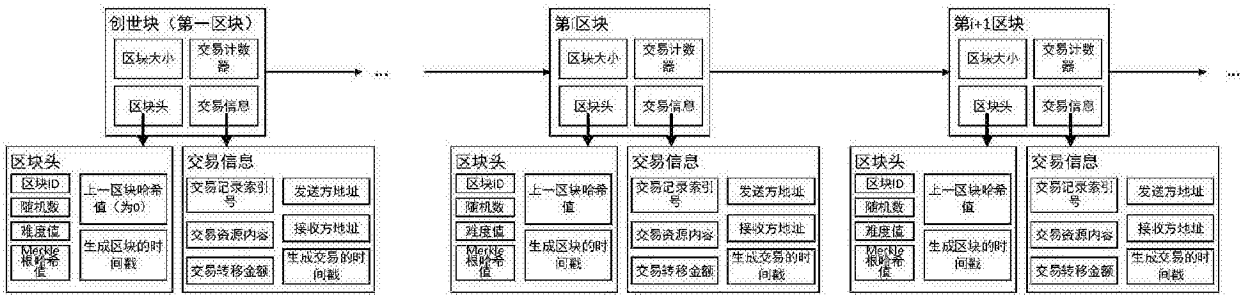

创世块（第一区块）
区块大小
交易计数器
区块头
交易信息
区块头
区块ID
随机数
难度值
Merkle根哈希值
上一区块哈希值（为0）
生成区块的时间戳
交易信息
交易记录索引号
交易资源内容
交易转移金额
发送方地址
接收方地址
生成交易的时间戳
...
第i区块
第i+1区块

图2

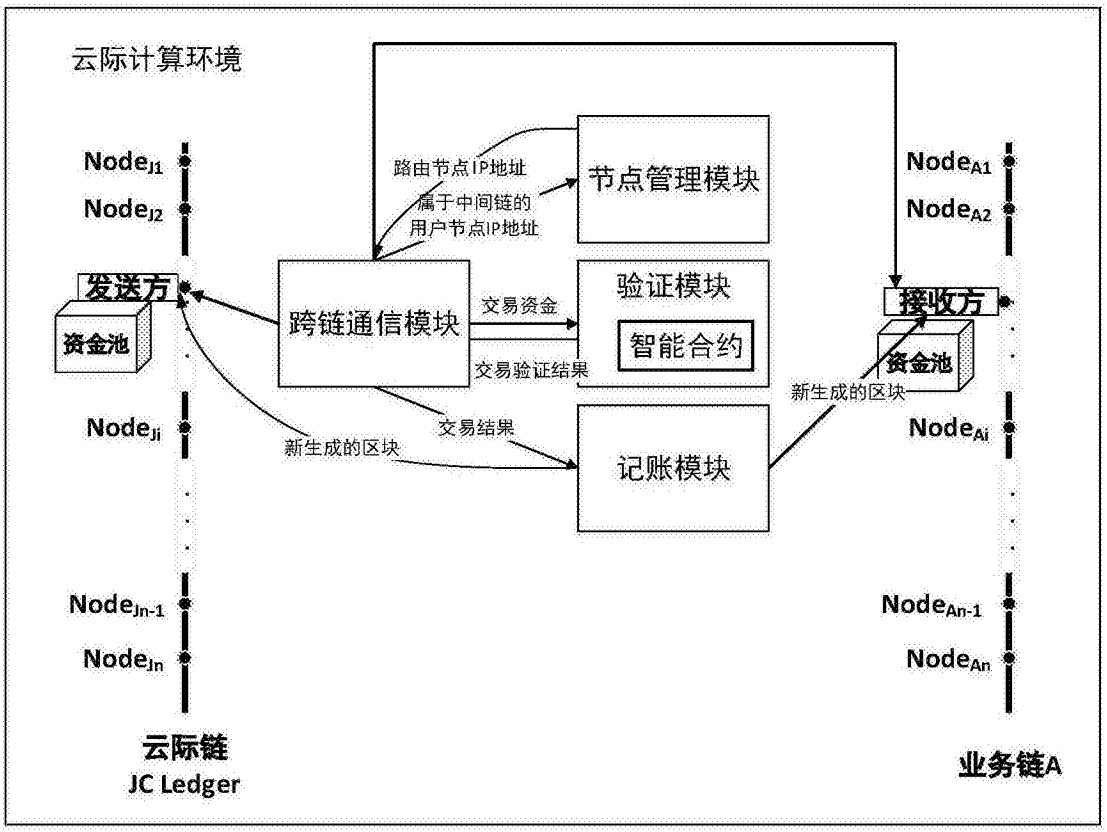

云际计算环境
$Node_{J1}$
$Node_{J2}$
发送方
资金池
$Node_{Ji}$
$Node_{Jn-1}$
$Node_{Jn}$
云际链
JC Ledger
路由节点IP地址
属于中间链的
用户节点IP地址
节点管理模块
跨链通信模块
交易资金
验证模块
智能合约
交易验证结果
交易结果
新生成的区块
记账模块
新生成的区块
$Node_{A1}$
$Node_{A2}$
接收方
资金池
$Node_{Ai}$
$Node_{An-1}$
$Node_{An}$
业务链A

图3

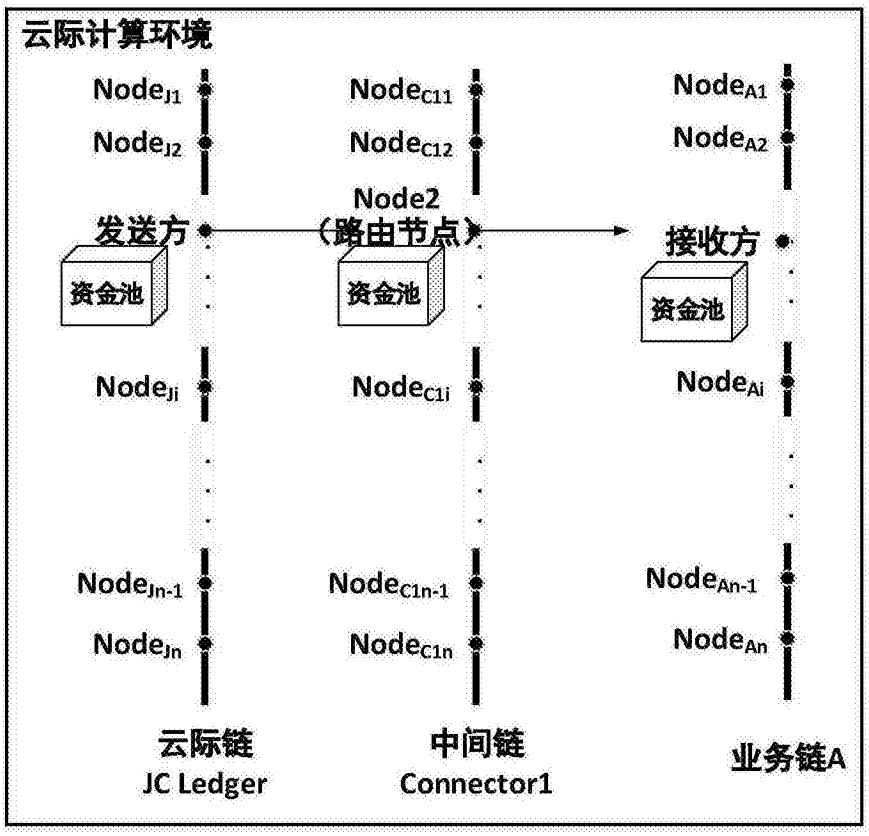

云际计算环境
NodeJ1
NodeJ2
发送方
资金池
NodeJi
NodeJn-1
NodeJn
云际链
JC Ledger
NodeC11
NodeC12
Node2
（路由节点）
资金池
NodeC1i
NodeC1n-1
NodeC1n
中间链
Connector1
NodeA1
NodeA2
接收方
资金池
NodeAi
NodeAn-1
NodeAn
业务链A

图4

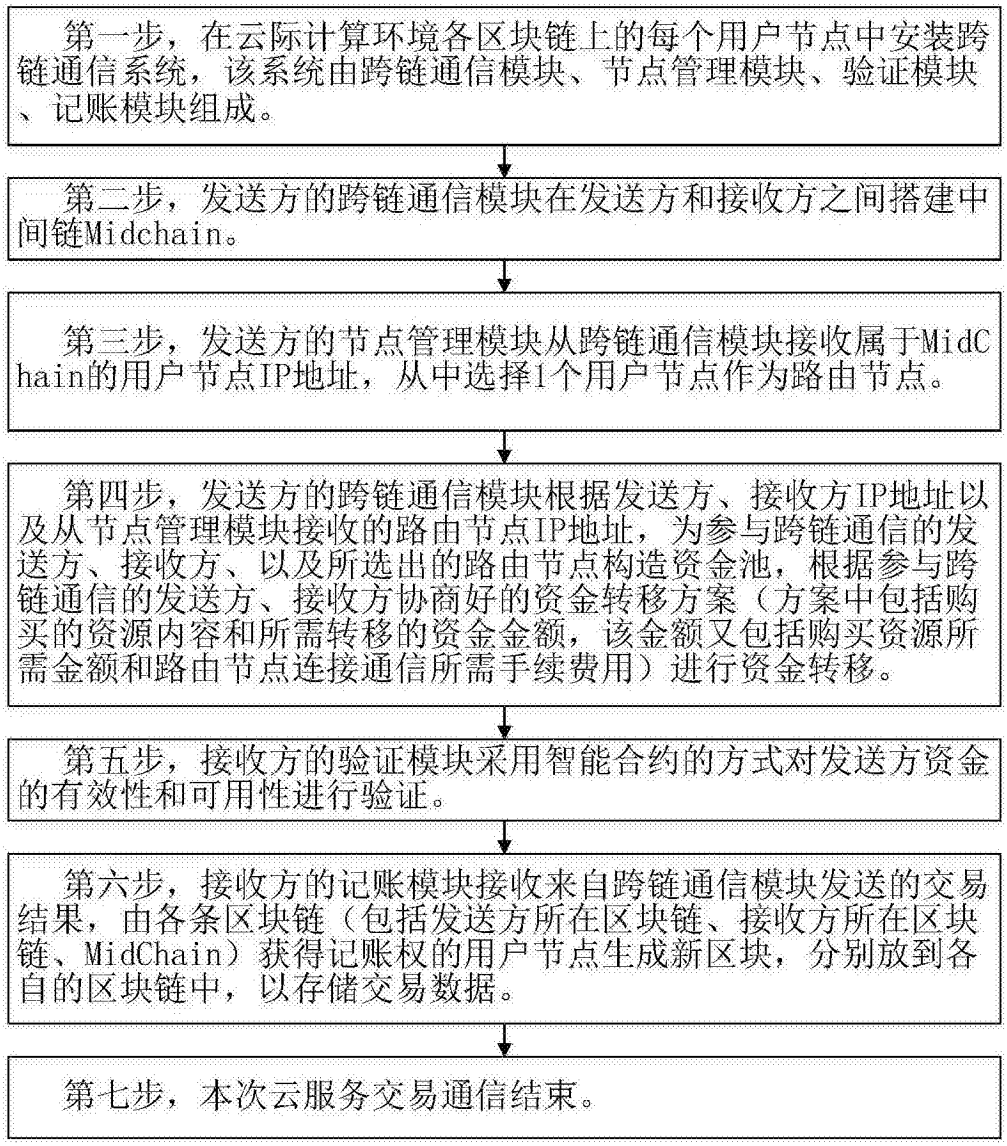

第一步，在云际计算环境各区块链上的每个用户节点中安装跨链通信系统，该系统由跨链通信模块、节点管理模块、验证模块、记账模块组成。
第二步，发送方的跨链通信模块在发送方和接收方之间搭建中间链Midchain。
第三步，发送方的节点管理模块从跨链通信模块接收属于MidChain的用户节点IP地址，从中选择1个用户节点作为路由节点。
第四步，发送方的跨链通信模块根据发送方、接收方IP地址以及从节点管理模块接收的路由节点IP地址，为参与跨链通信的发送方、接收方、以及所选出的路由节点构造资金池，根据参与跨链通信的发送方、接收方协商好的资金转移方案（方案中包括购买的资源内容和所需转移的资金金额，该金额又包括购买资源所需金额和路由节点连接通信所需手续费用）进行资金转移。
第五步，接收方的验证模块采用智能合约的方式对发送方资金的有效性和可用性进行验证。
第六步，接收方的记账模块接收来自跨链通信模块发送的交易结果，由各条区块链（包括发送方所在区块链、接收方所在区块链、MidChain）获得记账权的用户节点生成新区块，分别放到各自的区块链中，以存储交易数据。
第七步，本次云服务交易通信结束。

图5