一种双链式跨链交易的区块链互联网模型的核心算法

申请号：201710493422.0
申请日：2017-06-24

申请(专利权)人　北京天德科技有限公司
地址　100089 北京市海淀区知春路113号1708-048
发明(设计)人　邓恩艳

主分类号　G06Q20/38(2012.01)I
分类号　G06Q20/38(2012.01)I G06Q40/04(2012.01)I
公开(公告)号　107248076A
公开(公告)日　2017-10-13
专利代理机构
代理人

(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 107248076 A
(43)申请公布日 2017.10.13

(21)申请号 201710493422.0

(22)申请日 2017.06.24

(71)申请人 北京天德科技有限公司
地址 100089 北京市海淀区知春路113号1708-048

(72)发明人 邓恩艳

(51)Int.Cl.
G06Q 20/38(2012.01)
G06Q 40/04(2012.01)

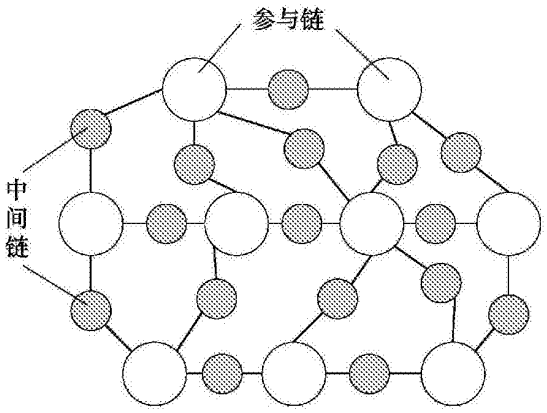
权利要求书5页 说明书22页 附图7页

(54)发明名称

一种双链式跨链交易的区块链互联网模型的核心算法

(57)摘要

本发明开发了一种双链式跨链交易的区块链互联网模型(金丝猴模型)的核心算法,该模型不同于传统的中心化架构,为完全分布式、多链网络架构。因为是全分布式的架构,所以比现有的架构更加容易扩展、延伸、容错。每条链维护自己的一致性,链与链之间的一致性不需要由中心组织来管理,而可以一个完全分布式的机制来维持,打破以前中心化的区块链互联网(以下简称链网)模型的限制,所有的链在这个模型上都可以并行运行,提高交易效率与网络运行速度。该模型是一种新的金融市场架构,具有可扩展性,金融单位可随时容易的加入或者离开该网络,支持大规模网络与高交易量。该模型包括参与链、中间链,无论是参与链还是中间链都可以是一家或一组金融机构。中间链为双链结构,交易记录与余额账户分离,实现跨链交易。本发明为链与链之间交易的核心算法,特别是中间链协助两个或以上的参与链相互交易的协议算法,无需一个中心机制而维持整个网络的一致性。



CN 107248076 A

1.一种双链式跨链交易的区块链互联网模型的核心算法，其特征在于：该模型如图1所示，包含以下组成部分：

(1)参与链(Participant Blockchain,PPC)，代表一个或多个金融机构或金融单位，可包含由一至多个节点；

(2)中间链(Inter-chain Blockchain,ICC)，代表一个中间机构，其本身也是一个金融机构，也可以起到CCP(Central Counterparty,中央对手方)的作用，可通过TBC(Trading Blockchain,交易区块链)与参与链进行交易；

(3)每两条参与链之间可连有一条或多条中间链，每条中间链可连接两条至多条参与链，并由中间链完成两条或多条参与链之间的交易，其包含两种交易模式，以适用于不同的需求(即时完成交易，或非实时但高效交易)；

(3a)实时交易(real-time transaction)：两条至多条参与链可通过一条中间链进行实时交易，中间链即时的执行每一条交易；

(3b)多边净额结算(multilateral netting)：每条中间链在每个结算周期结束时进行多边净额结算，一起处理多笔待定交易(tentative transaction)，起到CCP的作用，减少交易次数，提高交易效率；

(4)若干多个金融机构以参与链与中间链的形式构成了一个分布式网络，每条链维护自己的一致性，链与链之间的一致性不需要中央组织来管理，得以并行运行，提高交易效率与网络运行速度；新的金融单位可随时容易的加入或离开网络，具有可扩展性，支持大规模网络与高交易量。

2.根据权利要求1所述的一种双链式跨链交易的区块链互联网模型的核心算法，其特征在于：所述组成部分(1)，该链网包含若干多参与链，每一条参与链代表一个或多个金融单位，可包含若干多节点，每一个节点储存了该金融单位的全部信息；参与链的全部或部分节点具有投票权(全部节点及部分节点可参与投票这两种情况均适用于本专利)，各个节点之间采用并发拜占庭容错协议(CBFT,Concurrent Byzantine Fault Tolerance)、或实用拜占庭容错协议(PBFT,Practical Byzantine Fault Tolerance)、或其它拜占庭(Byzantine)共识协议、或数据库事物性一致性的算法(如使用数据库事物性一致性的算法，则不能查证说谎的节点，以至于是一个弱化的一致性算法)，来保证各个节点之间信息的一致性与难窜改性，保证了每条参与链自身的一致性。

3.根据权利要求1所述的一种双链式跨链交易的区块链互联网模型的核心算法，其特征在于：所述组成部分(2)，该链网包含若干多中间链，每一条中间链包含一个ABC(Account Blockchain,账户区块链)及两个至多个TBC(Trading Blockchian,交易区块链)，示意图见图3(两条参与链通过TBC-ABC-TBC结构相连)，图4(2个TBC)，图5(3个TBC)与图6(4个TBC)。ABC负责储存并维护账户信息，而TBC则负责执行交易。每一个ABC及TBC包含若干多个节点，其全部或部分节点具有投票权(全部节点及部分节点可参与投票这两种情况均适用于本专利)，各个节点之间采用拜占庭容错协议(或弱化的数据库事物协议)来保证各个节点之间信息的一致性与难窜改性，保证了每一条ABC链及每一条TBC自身的一致性。该ABC、TBC双链模型已由北京天德科技有限公司申请过专利，并已经实施。该中间链有两种存储模式：

(1)物理及逻辑隔离：每条TBC链及ABC链存储于不同的服务器，进行共识时每条TBC链及ABC链分别进行自己的共识，如图15所示，该模式可保证每条链之间的相互独立；

(2)逻辑隔离:每条TBC链及ABC链存储于同一个服务器的不同存储区域,但进行共识时每条TBC链及ABC链仍分别进行自己的共识,如图16所示,该模式也可保证每条链之间的相互独立,并比模式(1)更易进行链与链之间的信息传递。

4.根据权利要求1所述的一种双链式跨链交易的区块链互联网模型的核心算法,其特征在于:所述组成部分(3),在该链网中,每两条参与链之间可连有一条至多条中间链,每条中间链间可连接两条至多条参与链,并由中间链完成两条或多条参与链之间的交易,该链网可以实现两种不同的交易模式,以满足即时完成交易,及非实时但高效交易这两种不同的需求:

(1)实时交易:两条至多条参与链可通过一条中间链进行实时交易,中间链即时的执行每一条交易,实现实时清结算;

(2)多边净额结算:每条中间链在每个结算周期(一小时或一天等)结束时进行多边净额结算,一起处理多笔待定交易(tentative transaction),减少清结算的次数,提高交易效率,因为一次清结算可以解决大批的交易,但是这种方法无法实现实时清结算。

5.根据权利要求4所述的一种双链式跨链交易的区块链互联网模型的核心算法,其特征在于:对于(1)实时交易,此种交易模式的核心过程如图7与图11所示。该交易模式包含以下过程(以下为步骤的高阶层描述,详细描述见《说明书》中《具体实施方式》中的算法描述与伪代码),其流程如图8与图12所示。

(1):参与链1(PPC1)向中间链1(ICC1)发起交易;

下面的过程(2)分为两种模式:

模式(I),见图7:

(2)中间链1(ICC1)向参与链2(PPC2)发送交易请求;

若过程(1)的交易发起成功,过程(2)执行完毕后,将该交易状态标记为待定(tentative);

模式(II),见图11:

下面过程(2a)与过程(2b)同时执行;

(2a)中间链1(ICC1)向参与链1(PPC1)返回该交易请求成功与否的信息;

(2b)中间链1(ICC1)向参与链2(PPC2)发送交易请求;

若过程(1)的交易发起成功,过程(2a)与过程(2b)执行完毕后,将该交易状态标记为待定(tentative);

上述模式(II)中执行完毕(2a)后,参与链1(PPC1)即可进行其它操作,实现无阻塞的运行。

(3):参与链2(PPC2)向中间链1(ICC1)发送该交易请求是否成功被参与链2(PPC2)接受的消息,如果是,向中间链1(ICC1)发送该参与链2(PPC2)能够接受该交易的证明;

下面过程(4a)与过程(4b)同时执行;

(4a):中间链1(ICC1)向参与链1(PPC1)告知该交易满足执行条件,可以执行;

(4b):中间链1(ICC1)向参与链2(PPC2)告知该交易满足执行条件,可以执行;

两条参与链收到中间链1(ICC1)的消息后,立即执行该中间链1(ICC1)与参与链1(PPC1)及该中间链1(ICC1)与参与链2(PPC2)的待定交易,直至全部执行成功为止,即完成交易(commit)。

6.根据权利要求4所述的一种双链式跨链交易的区块链互联网模型的核心算法，其特征在于：对于第(2)种交易模式，多边净额结算，此种交易模式的核心过程如图9与图13所示。该交易模式包含以下步骤(以下为步骤的高阶层描述，详细描述见《说明书》中《具体实施方式》中的算法描述与伪代码)，其流程如图10与图14所示。

(1)参与链1(PPC1)向中间链1(ICC1)发起交易；

下面的过程(2)分为两种模式：

模式(I)，见图9：

(2)中间链1(ICC1)向参与链2(PPC2)发送交易请求；

若该交易发起成功，过程(2)执行完毕后，将该交易状态标记为预待定(pre-tentative)；

模式(II)，见图13：

下面过程(2a)与过程(2b)同时执行；

(2a)中间链1(ICC1)向参与链1(PPC1)返回该交易请求成功与否的信息；

(2b)中间链1(ICC1)向参与链2(PPC2)发送交易请求；

若该交易发起成功，过程(2a)与过程(2b)执行完毕后，将该交易状态标记为预待定(pre-tentative)；

上述模式(II)中执行完毕(2a)后，参与链1(PPC1)即可进行其它操作，实现无阻塞的运行。

(3)参与链2(PPC2)向中间链1(ICC1)发送该交易请求是否成功被参与链2(PPC2)接受的消息，如果是，向中间链1(ICC1)发送该参与链2(PPC2)能够接受该交易的证明；

若该请求被成功接受，将该交易状态标记为待定(tentative)；

下面过程(4a)与过程(4b)同时执行；

(4a)中间链1(ICC1)向参与链1(PPC1)告知该交易满足执行条件，可以执行；

(4b)中间链1(ICC1)向参与链2(PPC2)告知该交易满足执行条件，可以执行；

该交易等待该结算周期结束时，执行过程(5)；

(5)此时该结算周期结束，停止所有的即将开始或正在初始化的交易及待定交易，完成正在执行的交易，并由中间链1(ICC1)对所有该结算周期之内的被标记为待定(tentative)的交易进行多边净额结算，进入完成交易(commit)阶段。

7.根据权利要求4所述的一种双链式跨链交易的区块链互联网模型的核心算法，其特征在于：一条中间链由ABC与TBC与两条参与链进行交易的示意图见图2。对于过程(1)至(4)，对其交易过程及过程中ABC及TBC的作用的描述如下：当一条中间链在与一条参与链进行交易时，可以利用TBC与参与链的一个或者多个节点相连，由TBC负责处理该参与链与中间链的交易，在每条中间链中，有一个ABC，负责储存与维护账户信息，ABC与各个TBC相连，每个TBC与一个与该中间链相连的参与链相连，负责进行交易；每当一个TBC向ABC发送信息前，或当ABC向TBC发送信息前，该TBC或ABC都将首先自己进行共识；当该ABC或TBC收到信息(如请求等)后，都将首先由各个节点进行共识；当一个TBC向参与链发送信息前，也需首先进行共识；当一个TBC收到来自参与链的信息时，也需先进行共识。只有当每次的共识通过后，才能运行。

8.根据权利要求4所述的一种实时的双链式跨链交易的区块链互联网模型的核心算

法，其特征在于：当一条链向另一条链传递信息时，其传递模式为散装传递，一条链的每一个节点分别向另一条链的每一个节点传递信息，以防止某个或某几个节点作弊而影响整个传输过程的正确性。例如，当参与链1(PPC1)向TBC1发送请求时，若参与链1(PPC1)共有m个节点，分别为P1，P2，…，Pm，TBC1共有n个节点，分别为T1，T2，…，Tn，则由Pi(i＝1，2，…，n)分别向T1，T2，…，Tn发送请求，所有节点总共发送m＊n次请求。

9.根据权利要求4所述的一种双链式跨链交易的区块链互联网模型的核心算法，其特征在于：以下为对两条参与链，参与链1(PPC1)与参与链2(PPC2)通过中间链进行交易，对于过程(1)至(4)的每一个步骤的简要描述，详细描述见《说明书》中《具体实施方式》中的算法描述与伪代码。在交易过程中，每当一条链要向另一条链发送信息(如交易请求、交易成功信息等)前，都需要自己首先进行共识，决定是否执行该信息的指令；每当一条链收到了另一条链的信息时，都需要首先进行验证与共识，以决定是否接受或执行该信息，在算法描述与伪代码中省略了部分共识过程(省略部分可根据以前发布的专利技术解决：一种基于区块链技术的DVP结算方法(CN 106504085 A)、一种将交易信息和账户信息分别存储的区块链(CN 106503992 A)，本专利不再重复讨论)，保留了重要的共识过程。

(1)参与链1(PPC1)向中间链1(ICC1)发起交易：

(1.1)参与链1(PPC1)(金融机构)发起交易：参与链经过内部的投票(CBFT或PBFT等拜占庭容错共识协议或数据库事物协议)决定是否发起交易，若是，参与链1(PPC1)对该交易信息进行加密认证(使用数字签名等)，选定本次交易中在即将使用的TBC1(该TBC1在中间链内并与参与链1(PPC1)相连)，并将进行了加密认证的交易信息发送给该TBC1；若否，向参与链1(PPC1)返回错误信息，并将该过程标记为失败(failure)；

(1.2)中间机构验证信息：TBC1收到交易信息，并向ABC发送请求，ABC收到请求后，对交易信息进行验证(使用数字签名等)，若验证成功，则将该参与链的账户信息传给ABC；若验证失败，则返回错误信息，并将前面步骤均标记为失败(failure)；

(1.3)TBC1待定交易：TBC1中的各个节点对该交易进行投票与建块，并将该交易为待定(pending)状态。

下面的过程(2)分为两种模式：

模式(I)：

(2)中间链1(ICC1)向参与链2(PPC2)发送交易请求：

(2.1)中间链(ICC1)传递交易：中间链(ICC1)经过内部的投票(CBFT或PBFT等拜占庭容错共识协议或数据库事物协议)决定是否向参与链2(PPC2)传递交易，若是，则中间链(ICC1)对该交易进行加密认证(使用数字签名等)，并选定本次交易中将要使用的TBC2(该TBC2在中间链内并与参与链2(PPC2)相连)，并将进行了加密认证的交易信息发送给该TBC2；若否，则返回错误信息，并将前面步骤均标记为失败(failure)；

(2.2)参与链2(PPC2)验证信息：TBC2向参与链2(PPC2)发送对已经过加密认证的交易的验证请求，参与链2(PPC2)对该请求的交易进行验证(使用数字签名等)，若验证通过，则参与链2(PPC2)则进行内部投票决定是否接受该交易；若验证失败，则返回失败信息，并将前面步骤均标记为失败(failure)。

模式(II)：

(2a)中间链1(ICC1)向参与链1(PPC1)返回待定交易成功与否的信息：

若待定交易状态(pending)设定成功,则向参与链1(PPC1)返回待定交易成功的信息,TBC1则等待执行(pending);若交易失败,则向参与链1(PPC1)返回交易失败的信息,并将前面步骤均标记为失败(failure)。

(2b)与(2a)同时进行,同模式(I)中的过程(2)。

(3)参与链2(PPC2)向中间链1(ICC1)发送该交易请求是否成功被参与链2(PPC2)接受的消息,如果是,向中间链1(ICC1)发送该参与链2(PPC2)能够接受该交易的证明:

(3.1)若参与链2(PPC2)投票成功,同意接受该交易,则向中间链1(ICC1)返回成功信息,并进行(3.2);否则,则向中间链1(ICC1)返回失败信息,并将前面步骤均标记为失败(failure);

(3.2)参与链2(PPC2)向中间链1(ICC1)发送该参与链2(PPC2)能够接受该交易的证明,如参与链2(PPC2)有足量相关资源以完成此交易,并将TBC2待定执行与参与链2(PPC2)的交易设为待定(pending)状态。

(4)中间链验证参与链2(PPC2)返回的信息,并决定该交易是否满足执行条件,若是,则进行(4a)与(4b);若否,则进行投票决定是否取消待定交易,并将前面步骤均标记为失败(failure)。

(4a)中间链1(ICC1)向参与链1(PPC1)告知该交易满足执行条件,可以执行;

(4b)中间链1(ICC1)向参与链2(PPC2)告知该交易满足执行条件,可以执行。

一种双链式跨链交易的区块链互联网模型的核心算法

技术领域

[0001] 本发明涉及针对金融体系的区块链互联网技术领域，特别是采用分布式的区块链互联网结构。

背景技术

[0002] 区块链((Blockchain,BC)是分布式数据库系统，也可理解为由多个节点共同维护的分布式账簿技术(Distributed Ledger Technology,DLT)，其特点是不易篡改、很难伪造、可追溯。区块链互联网(Internet of Blockchians)是一种基于区块链搭建的价值网络，须具有高性能，安全性，隐私性，可扩展性，互通性，可更改性，容错性，可管理性及完备性

[0003] 现有的区块链互联网，如宇宙网(Cosmos)，多为中心化的结构，其中间链是一个中心机构，于是中间链的计算及通讯链易成为区块链互联网的瓶颈。另外，其每一条链都需要维持自己的一致性，而中间链也需要动态维持与每一条参与链之间的一致性，进而一条跨链交易需要多条参与链与中间链共同维持，使得区块链的运行速度减慢。

发明内容

[0004] 为了克服上述现有的应用于金融系统的链网(如Cosmos等)效率较慢的问题，本发明提供了一种双链式跨链交易的区块链互联网模型的核心算法，可以实现并行运算，提高系统的运行效率与交易速度，同时保证系统一致性。

[0005] 本发明所采用的技术方案是一种双链式跨链交易的区块链互联网模型的核心算法，其特征在于该模型如图1所示，包含以下组成部分：

[0006] (1)参与链(Participant Blockchain,PPC)，代表一个或多个金融机构或金融单位，可包含由一至多个节点；

[0007] (2)中间链(Inter-chain Blockchain,ICC)，代表一个中间机构，其本身也是一个金融机构，也可以起到CCP(Central Counterparty，中央对手方)的作用，可通过TBC(Trading Blockchain,交易区块链)与参与链进行交易；

[0008] (3)每两条参与链之间可连有一条或多条中间链，每条中间链可连接两条至多条参与链，并由中间链完成两条或多条参与链之间的交易，其包含两种交易模式，以适用于不同的需求(即时完成交易，或非实时但高效交易)：

[0009] (3a)实时交易(real-time transaction)：两条至多条参与链可通过一条中间链进行实时交易，中间链即时的执行每一条交易；

[0010] (3b)多边净额结算(multilateral netting)：每条中间链在每个结算周期结束时进行多边净额结算，一起处理多笔待定交易(tentative transaction)，起到CCP的作用，减少交易次数，提高交易效率；

[0011] (4)若干多个金融机构以参与链与中间链的形式构成了一个分布式网络，每条链维护自己的一致性，链与链之间的一致性不需要中央组织来管理，得以并行运行，提高交易

效率与网络运行速度;新的金融单位可随时容易的加入或离开网络,具有可扩展性,支持大规模网络与高交易量。

[0012] 优选的,对于组成部分(1),该链网包含若干多参与链,每一条参与链代表一个或多个金融单位,可包含若干多节点,每一个节点储存了该金融单位的全部信息;参与链的全部或部分节点具有投票权(全部节点及部分节点可参与投票这两种情况均适用于本专利),各个节点之间采用并发拜占庭容错协议(CBFT,Concurrent Byzantine Fault Tolerance)、或实用拜占庭容错协议(PBFT,Practical Byzantine Fault Tolerance)、或其它拜占庭(Byzantine)共识协议、或数据库事物性一致性的算法(如使用数据库事物性一致性的算法,则不能查证说谎的节点,以至于是一个弱化的一致性算法),来保证各个节点之间信息的一致性与难窜改性,保证了每条参与链自身的一致性。

[0013] 优选的,对于组成部分(2),该链网包含若干多中间链,每一条中间链包含一个ABC(Account Blockchain,账户区块链)及两个至多个TBC(Trading Blockchian,交易区块链),示意图见图3(两条参与链通过TBC-ABC-TBC结构相连),图4(2个TBC),图5(3个TBC)与图6(4个TBC)。ABC负责储存并维护账户信息,而TBC则负责执行交易。每一个ABC及TBC包含若干多个节点,其全部或部分节点具有投票权(全部节点及部分节点可参与投票这两种情况均适用于本专利),各个节点之间采用拜占庭容错协议(或弱化的数据库事物协议)来保证各个节点之间信息的一致性与难窜改性,保证了每一条ABC链及每一条TBC自身的一致性。该ABC、TBC双链模型已由北京天德科技有限公司申请过专利,并已经实施:一种基于区块链技术的DVP结算方法(CN 106504085 A)、一种将交易信息和账户信息分别存储的区块链(CN 106503992 A)。该中间链有两种存储模式:

[0014] (1)物理及逻辑隔离:每条TBC链及ABC链存储于不同的服务器,进行共识时每条TBC链及ABC链分别进行自己的共识,如图15所示,该模式可保证每条链之间的相互独立;

[0015] (2)逻辑隔离:每条TBC链及ABC链存储于同一个服务器的不同存储区域,但进行共识时每条TBC链及ABC链仍分别进行自己的共识,如图16所示,该模式也可保证每条链之间的相互独立,并比模式(1)更易进行链与链之间的信息传递。

[0016] 优选的,对于组成部分(3),在该链网中,每两条参与链之间可连有一条至多条中间链,每条中间链间可连接两条至多条参与链,并由中间链完成两条或多条参与链之间的交易,该链网可以实现两种不同的交易模式,以满足即时完成交易,及非实时但高效交易这两种不同的需求:

[0017] (1)实时交易:两条至多条参与链可通过一条中间链进行实时交易,中间链即时的执行每一条交易,实现实时清结算;

[0018] (2)多边净额结算:每条中间链在每个结算周期(一小时或一天等)结束时进行多边净额结算,一起处理多笔待定交易(tentative transaction),减少清结算的次数,提高交易效率,因为一次清结算可以解决大批的交易,但是这种方法无法实现实时清结算。

[0019] 优选的,对于(1)实时交易,此种交易模式的核心过程如图7与图11所示。该交易模式包含以下过程(以下为步骤的高阶层描述,详细描述见《说明书》中《具体实施方式》中的算法描述与伪代码),其流程如图8与图12所示。

[0020] (1)参与链1(PPC1)向中间链1(ICC1)发起交易;

[0021] 下面的过程(2)分为两种模式:

[0022] 模式(I)，见图7：

[0023] (2)中间链1(ICC1)向参与链2(PPC2)发送交易请求；

[0024] 若过程(1)的交易发起成功，过程(2)执行完毕后，将该交易状态标记为待定(tentative)；

[0025] 模式(II)，见图11：

[0026] 下面过程(2a)与过程(2b)同时执行；

[0027] (2a)中间链1(ICC1)向参与链1(PPC1)返回该交易请求成功与否的信息；

[0028] (2b)中间链1(ICC1)向参与链2(PPC2)发送交易请求；

[0029] 若过程(1)的交易发起成功，过程(2a)与过程(2b)执行完毕后，将该交易状态标记为待定(tentative)；

[0030] 上述模式(II)中执行完毕(2a)后，参与链1(PPC1)即可进行其它操作，实现无阻塞的运行。

[0031] (3)参与链2(PPC2)向中间链1(ICC1)发送该交易请求是否成功被参与链2(PPC2)接受的消息，如果是，向中间链1(ICC1)发送该参与链2(PPC2)能够接受该交易的证明；

[0032] 下面过程(4a)与过程(4b)同时执行；

[0033] (4a)中间链1(ICC1)向参与链1(PPC1)告知该交易满足执行条件，可以执行；

[0034] (4b)中间链1(ICC1)向参与链2(PPC2)告知该交易满足执行条件，可以执行；

[0035] 两条参与链收到中间链1(ICC1)的消息后，立即执行该中间链1(ICC1)与参与链1(PPC1)及该中间链1(ICC1)与参与链2(PPC2)的待定交易，直至全部执行成功为止，即完成交易(commit)。

[0036] 优选的，对于第(2)种交易模式，多边净额结算，此种交易模式的核心过程如图9与图13所示。该交易模式包含以下过程(以下为步骤的高阶层描述，详细描述见《说明书》中《具体实施方式》中的算法描述与伪代码)，其流程如图10与图14所示。

[0037] (1)参与链1(PPC1)向中间链1(ICC1)发起交易；

[0038] 下面的过程(2)分为两种模式：

[0039] 模式(I)，见图9：

[0040] (2)中间链1(ICC1)向参与链2(PPC2)发送交易请求；

[0041] 若该交易发起成功，过程(2)执行完毕后，将该交易状态标记为预待定(pre-tentative)；

[0042] 模式(II)，见图13：

[0043] 下面过程(2a)与过程(2b)同时执行；

[0044] (2a)中间链1(ICC1)向参与链1(PPC1)返回该交易请求成功与否的信息；

[0045] (2b)中间链1(ICC1)向参与链2(PPC2)发送交易请求；

[0046] 若该交易发起成功，过程(2a)与过程(2b)执行完毕后，将该交易状态标记为预待定(pre-tentative)；

[0047] 上述模式(II)中执行完毕(2a)后，参与链1(PPC1)即可进行其它操作，实现无阻塞的运行。

[0048] (3)参与链2(PPC2)向中间链1(ICC1)发送该交易请求是否成功被参与链2(PPC2)接受的消息，如果是，向中间链1(ICC1)发送该参与链2(PPC2)能够接受该交易的证明；

[0049] 若该请求被成功接受，将该交易状态标记为待定(tentative)；

[0050] 下面过程(4a)与过程(4b)同时执行；

[0051] (4a)中间链1(ICC1)向参与链1(PPC1)告知该交易满足执行条件，可以执行；

[0052] (4b)中间链1(ICC1)向参与链2(PPC2)告知该交易满足执行条件，可以执行；

[0053] 该交易等待该结算周期结束时，执行过程(5)；

[0054] (5)此时该结算周期结束，停止所有的即将开始或正在初始化的交易及待定交易，完成正在执行的交易，并由中间链1(ICC1)对所有该结算周期之内的被标记为待定(tentative)的交易进行多边净额结算，进入完成交易(commit)阶段。

[0055] 优选的，一条中间链由ABC与TBC与两条参与链进行交易的示意图见图2。对于过程(1)至(4)，对其交易过程及过程中ABC及TBC的作用的描述如下：当一条中间链在与一条参与链进行交易时，可以利用TBC与参与链的一个或者多个节点相连，由TBC负责处理该参与链与中间链的交易，在每条中间链中，有一个ABC，负责储存与维护账户信息，ABC与各个TBC相连，每个TBC与一个与该中间链相连的参与链相连，负责进行交易；每当一个TBC向ABC发送信息前，或当ABC向TBC发送信息前，该TBC或ABC都将首先自己进行共识；当该ABC或TBC收到信息(如请求等)后，都将首先由各个节点进行共识；当一个TBC向参与链发送信息前，也需首先进行共识；当一个TBC收到来自参与链的信息时，也需先进行共识。只有当每次的共识通过后，才能运行。

[0056] 优选的，当一条链向另一条链传递信息时，其传递模式为散装传递，一条链的每一个节点分别向另一条链的每一个节点传递信息，以防止某个或某几个节点作弊而影响整个传输过程的正确性。例如，当参与链1(PPC1)向TBC1发送请求时，若参与链1(PPC1)共有m个节点，分别为P1，P2，…，Pm，TBC1共有n个节点，分别为T1，T2，…，Tn，则由Pi(i＝1，2，…，n)分别向T1，T2，…，Tn发送请求，所有节点总共发送m＊n次请求。

[0057] 优选的，以下为对两条参与链，参与链1(PPC1)与参与链2(PPC2)通过中间链进行交易，对于过程(1)至(4)的每一个步骤的简要描述，详细描述见《说明书》中《具体实施方式》中的算法描述与伪代码。在交易过程中，每当一条链要向另一条链发送信息(如交易请求、交易成功信息等)前，都需要自己首先进行共识，决定是否执行该信息的指令；每当一条链收到了另一条链的信息时，都需要首先进行验证与共识，以决定是否接受或执行该信息，在算法描述与伪代码中省略了部分共识过程(省略部分可根据以前发布的专利技术解决：一种基于区块链技术的DVP结算方法(CN 106504085 A)、一种将交易信息和账户信息分别存储的区块链(CN 106503992 A)，本专利不再重复讨论)，保留了重要的共识过程。

[0058] (1)参与链1(PPC1)向中间链1(ICC1)发起交易：

[0059] (1.1)参与链1(PPC1)(金融机构)发起交易：参与链经过内部的投票(CBFT或PBFT等拜占庭容错共识协议或数据库事物协议)决定是否发起交易，若是，参与链1(PPC1)对该交易信息进行加密认证(使用数字签名等)，选定本次交易中在即将使用的TBC1(该TBC1在中间链内并与参与链1(PPC1)相连)，并将进行了加密认证的交易信息发送给该TBC1；若否，向参与链1(PPC1)返回错误信息，并将该过程标记为失败(failure)；

[0060] (1.2)中间机构验证信息：TBC1收到交易信息，并向ABC发送请求，ABC收到请求后，对交易信息进行验证(使用数字签名等)，若验证成功，则将该参与链的账户信息传给ABC；若验证失败，则返回错误信息，并将前面步骤均标记为失败(failure)；

[0061] (1.3)TBC1待定交易:TBC1中的各个节点对该交易进行投票与建块,并将该交易为待定(pending)状态。

[0062] 下面的过程(2)分为两种模式:

[0063] 模式(I):

[0064] (2)中间链1(ICC1)向参与链2(PPC2)发送交易请求:

[0065] (2.1)中间链(ICC1)传递交易:中间链(ICC1)经过内部的投票(CBFT或PBFT等拜占庭容错共识协议或数据库事物协议)决定是否向参与链2(PPC2)传递交易,若是,则中间链(ICC1)对该交易进行加密认证(使用数字签名等),并选定本次交易中将要使用的TBC2(该TBC2在中间链内并与参与链2(PPC2)相连),并将进行了加密认证的交易信息发送给该TBC2;若否,则返回错误信息,并将前面步骤均标记为失败(failure);

[0066] (2.2)参与链2(PPC2)验证信息:TBC2向参与链2(PPC2)发送对已经过加密认证的交易的验证请求,参与链2(PPC2)对该请求的交易进行验证(使用数字签名等),若验证通过,则参与链2(PPC2)则进行内部投票决定是否接受该交易;若验证失败,则返回失败信息,并将前面步骤均标记为失败(failure)。

[0067] 模式(II):

[0068] (2a)中间链1(ICC1)向参与链1(PPC1)返回待定交易成功与否的信息:

[0069] 若待定交易状态(pending)设定成功,则向参与链1(PPC1)返回待定交易成功的信息,TBC1则等待执行(pending);若交易失败,则向参与链1(PPC1)返回交易失败的信息,并将前面步骤均标记为失败(failure)。

[0070] (2b)与(2a)同时进行,同模式(I)中的过程(2)。

[0071] (3)参与链2(PPC2)向中间链1(ICC1)发送该交易请求是否成功被参与链2(PPC2)接受的消息,如果是,向中间链1(ICC1)发送该参与链2(PPC2)能够接受该交易的证明:

[0072] (3.1)若参与链2(PPC2)投票成功,同意接受该交易,则向中间链1(ICC1)返回成功信息,并进行(3.2);否则,则向中间链1(ICC1)返回失败信息,并将前面步骤均标记为失败(failure);

[0073] (3.2)参与链2(PPC2)向中间链1(ICC1)发送该参与链2(PPC2)能够接受该交易的证明,如参与链2(PPC2)有足量相关资源以完成此交易,并将TBC2待定执行与参与链2(PPC2)的交易设为待定(pending)状态。

[0074] (4)中间链验证参与链2(PPC2)返回的信息,并决定该交易是否满足执行条件,若是,则进行(4a)与(4b);若否,则进行投票决定是否取消待定交易,并将前面步骤均标记为失败(failure)。

[0075] (4a)中间链1(ICC1)向参与链1(PPC1)告知该交易满足执行条件,可以执行;

[0076] (4b)中间链1(ICC1)向参与链2(PPC2)告知该交易满足执行条件,可以执行。

[0077] 为了改进现有的针对金融系统设计的链网结果无法并行操作、效率慢的问题,目前设计的分布式的新型链网结构模型,具有如下优点:

[0078] (1)支持并行操作:该模型由于是一个完全分布式的架构,所有的链在这个模型上都可以并行运行,提高整个金融系统的运行速度:由于不同的参与链可以与不同的中间链进行交易,而由不同的参与链处理的交易可以同时进行,无需每笔交易都通过一个总的中央机构,各个中间机构的交易量和负载量都大大减轻,并可以进行并行操作,进而提高了交

易的效率，增快了交易的速度。

[0079] (2)多边净额结算：两个或多条参与链通过一条中间链进行交易时，中间链对多个交易进行相互冲抵轧差，减少了结算的处理量，也减轻了大型交易的难度，提高了交易的速度，提升了市场效率。

[0080] (3)可扩展性：任意数量的金融机构与中间机构可以随时容易的加入该链网结构，并通过TBC将即将加入的新的金融单位与已有的中间机构连接起来，这使得该链网可以扩张并适应大型网络及高交易量。

[0081] (4)支持监管：难以篡改的账本记录，记录了真实的交易过程，方便政府部门监管查账。

[0082] (5)交易记录与余额账户分离：该模型的中间链结构中账户区块链(ABC)与交易区块链(TBC)的分开设计以及分别进行共识的机制适用于金融系统，提高了隐私保护性及交易效率。

[0083] (6)不同存储模式：该模型的中间链中账户区块链(ABC)与交易区块链(TBC)的不同存储模式可以适用于不同的应用情形。

[0084] (7)保证了链网的基本原则，包括：(a)高性能，完全分布式结构支持每个中间机构并行运行，提高网络的交易效率；(b)数据可靠性(难以篡改性、安全性)，各个节点采用拜占庭容错协议来保证各个节点的一致性和难以篡改性；(c)保护隐私，各个链内部的信息无法被外部获取；(f)可扩展性，任何金融机构可以随时容易的加入该链网，并由于并行运算，增加新的金融机构不会造成通讯阻塞；(e)完备性，每条链都可以追踪其完备性，一旦一个节点作弊，其完备性将降低，并可以被追踪和查看。

[0085] 根据下文结合附图对本发明的具体实施方案的详细描述，本领域技术人员将会更加明了本发明的上述以及其它目的、优化和特征。

附图说明

[0086] 后文将参照附图以示例性而非限制性的方式详细描述本发明的一些具体实施例。附图中相同的附图标记标示了相同或类似的部件或部分。本领域技术人员应该理解，这些附图未必是按比例绘制的。本发明的目标及特征考虑到如下结合附图的描述将更加明显。附图中：

[0087] 图1是根据本发明优先实施例的一种双链式跨链交易的区块链互联网模型(金丝猴模型)的整体示意图；

[0088] 图2是根据本发明优先实施例的两条参与链(PPC)之间由TBC与ABC进行交易的示意图(ICC为中间链)；

[0089] 图3是根据本发明优先实施例的参与链1(PPC1)与参与链2(PPC2)通过中间链1(ICC1)进行交易的过程示意图；

[0090] 图4是根据本发明优先实施例的中间链(ICC)可能有两个TBC的示意图；

[0091] 图5是根据本发明优先实施例的中间链(ICC)可能有三个TBC的示意图；

[0092] 图6是根据本发明优先实施例的中间链(ICC)可能有四个TBC的示意图；

[0093] 图7是根据本发明优先实施例的模式(I)的实时交易过程的示意图(PPC为参与链，ICC为中间链)；

[0094] 图8是根据本发明优先实施例的模式(I)实时交易各个过程的流程图；

[0095] 图9是根据本发明优先实施例的模式(I)的采用多方净额结算的交易过程的示意图(PPC为参与链，ICC为中间链)；

[0096] 图10是根据本发明优先实施例的模式(I)的采用多方净额结算的交易过程的流程图；

[0097] 图11是根据本发明优先实施例的模式(II)的实时交易过程的示意图(PPC为参与链，ICC为中间链)；

[0098] 图12是根据本发明优先实施例的模式(II)实时交易各个过程的流程图；

[0099] 图13是根据本发明优先实施例的模式(II)的采用多方净额结算的交易过程的示意图(PPC为参与链，ICC为中间链)；

[0100] 图14是根据本发明优先实施例的模式(II)的采用多方净额结算的交易过程的流程图。

[0101] 图15是根据本发明优先实施例的中间链物理及逻辑隔离的存储模式示意图。

[0102] 图16是根据本发明优先实施例的中间链逻辑隔离的存储模式示意图。

具体实施方式

[0103] 为了更好的理解本发明实施例提供的技术方案，也更好的与本发明实施例的技术方案进行对比，下面首先通过算法和伪代码结合附图对本发明进一步说明。

[0104] 该种双链式跨链交易的区块链互联网模型(金丝猴模型)的具体实施方式主要包括以下三部分：

[0105] (1)整个网络从零开始搭建；

[0106] (2)交易：一条参与链通过一条中间链与另一条参与链进行交易；

[0107] (3)新链加入网络。

[0108] 对于(1)整个网络从零开始搭建，其输入包括若干多条中间链(Inter-chain Blockchain，伪代码中由ICC表示)，若干多条参与链(Participant Blockchain，伪代码中由PPC表示)，以及各条参与链与中间链之间是否应相连的关系，具体过程如下。

[0109] (1)对于所以将要加入该网络的链，将所有的参与链放入一条参与链集合，将所有的中间链放入一条中间链集合；

[0110] (2)对于中间链集合中的每一条中间链，以及参与链集合中的每两条参与链，利用已知的该网络的即将达成的链与链间的关系，判断：如果该中间链将要与此两条参与链连接，则该中间链与此两条参与链分别建立连接；否则，继续考虑其它链。

[0111] 该过程的主要算法以伪代码的形式展示如下，记为算法0，建立网络。

[0112]
```
Algorithm 0: build_the_network
Input: ICCs（中间链）, PPCs（参与链）, connection_information
1 put all the ICCs in a set ICCSet, put all the PPCs in a set PPCSet
2 for (each ICC in ICCSet), and (each two different PPCs in PPCSet), denote as PPC1 and PPC2, do:
3 if (ICC, PPC1 and PPC2) should be connected, then: // Two or more PPCs connect with each ICC
4 add connection (ICC, PPC1) into the network by calling Algorithm 7 (link_an_ICC_with_a_PPC)
5 add connection (ICC, PPC2) into the network by calling Algorithm 7 (link_an_ICC_with_a_PPC)
6 end if
7 end for
8 // Assuming if PPC1 and PPC2 are already connected to ICC1,
9 // adding PPC3 into ICC1 will result in PPC1, PPC2, PPC3 connected with each other via ICC1
10 // similarly, if PPCi already connected to ICC1, adding PPCj with ICC1
11 // will result all PPCi and PPCj connected to each other via ICC1
```

以下伪代码中的“consensus protocol”（共识协议）表示“CBFT or PBFT or other Byzantine consensus protocol or database consistency”。

[0113] 对于(2)交易:一条参与链通过一条中间链与另一条参与链进行交易,示意图可见图2。其输入包括中间链1(ICC1)、参与链1(PPC1)与参与链2(PPC2)。参与链1(PPC1)负责发起交易,并由中间链1进行交易,由参与链2(PPC2)负责接收该交易。例如,参与链1(PPC1)向参与链2(PPC2)进行美元兑换黄金的交易,参与链1(PPC1)发起提供美元并换取黄金的交易,提供特定数目的金额,由中间链1执行交易过程,由参与链2(PPC2)负责接收这笔美元并提供黄金。

[0114] 对于每一次交易,包含了实时交易与多边净额结算两种情况,其具体交易过程如下。

[0115] (1)参与链1(PPC1)通过对其内部的各个节点进行投票(使用CBFT、或PBFT、或其它的拜占庭共识协议、或数据库事物协议)来决定是否发起此交易,如果投票成功,则进入第(2)步;如果投票失败,则返回错误信息;

[0116] (2)选定一个用于参与链1(PPC1)与中间链1执行交易的TBC1,该TBC1为中间链1的一部分;

[0117] (3)参与链1(PPC1)随后向TBC1发送交易请求,即为过程(1);

[0118] (4)调用算法2,由中间链1对该交易请求进行验证(利用电子签名等),如果验证成

功，则进入第(5)部；如果验证失败，则向参与链1(PPC1)返回错误信息；

[0119] (5)中间链1对其内部各个节点进行投票(使用CBFT、或PBFT、或其它的拜占庭共识协议、或数据库事物协议)来决定是否可以执行该交易，如果投票成功，则进入第(6)步；如果投票失败，则向参与链1(PPC1)返回投票失败的信息，并将之前所有的步骤标记为“失败”；

[0120] (6)将参与链1(PPC1)与中间链1(ICC1)之间的交易状态设为“待定”(pending)；

[0121] (7)如果需要实时交易，则将该交易状态标记为“待定”(tentative)；如果需要多边净额结算，则将该交易状态标记为“预待定”(pre-tentative)；

[0122] (8)若为模式(I)，则调用算法3，中心链1(ICC1)开始准备发起向参与链2(PPC2)的交易请求，即为过程(2)；如果过程(2)返回中心链1(ICC1)对参与链2(PPC2)的交易请求成功，则进入第(9)步，否则，将之前所有的步骤标记为“失败”，并调用算法12，由中间链1(ICC1)与参与链1(PPC1)及参与链2(PPC2)进行共识，决定是否取消中间链1(ICC1)与参与链1(PPC1)的待定交易，并返回错误信息；若为算法(b)，则中间链1(ICC1)告知参与链1(PPC1)目前的交易状态，即为过程(2a)，同时进行模式(I)中的过程(2)；

[0123] (9)参与链2(PPC2)向中间链1(ICC1)告知当前参与链2(PPC2)是否同意该交易，如果同意则向中间链1(ICC1)发送参与链2(PPC2)证明能够进行该交易的信息，以供中间链1(ICC1)验证，即为过程(3)；

[0124] (10)中间链1(ICC1)对该信息进行验证，如果验证通过，则进入第(12)步，否则将之前所有步骤标记为“失败”，并调用算法12，由中间链1(ICC1)与参与链1(PPC1)及参与链2(PPC2)进行共识，决定是否取消中间链1(ICC1)与参与链1(PPC1)的待定交易，并返回错误信息；

[0125] (11)中间链1(ICC1)向参与链1(PPC1)即参与链2(PPC2)告知该交易是否满足交易条件，是否可以执行，即为过程(4a)和过程(4b)；

[0126] (12)若在一定时间(Time1)内，参与链1(PPC1)未能收到交易可以执行的通知，则中间链(ICC1)与参与链1(PPC1)及参与链2(PPC2)进行共识，决定是否取消该交易，如果是，则进入第(13)步，否则进入第(14)步；

[0127] (13)将之前所有的步骤标记为“失败”，并取消中间链(ICC1)与参与链1(PPC1)的待定交易，及取消中间链(ICC1)与参与链2(PPC2)的待定交易，随后中间链1(ICC1)再次与参与链1(PPC1)及参与链2(PPC2)进行共识，并返回失败信息；

[0128] (14)如果需要实时交易，则调用下面的算法10来执行实时交易；如果需要多边净额结算，则将该交易状态标记为“待定”(tentative)，并调用算法11来进行多边净额结算(在算法11中，需首先等待至该结算周期结束)。

Algorithm 1: a_transaction_between_an_ICC_and_two_PPCs.
Input: ICC1, PPC1, PPC2
1 PPC1 votes using consensus protocol within itself to determine whether conduct the transaction
2 if (yes), then:
3 determine the TBC1 to be used for this transaction between PPC1 and ICC1 // the TBC1 is a part of ICC1
4 PPC1 sends transaction request to the TBC1 and the ABC // Process 1, the ABC is a part of ICC1
5 if (mode (a)), then:
6 PPC1 waits until receives the transaction confirmation from ICC1
7 end if
8 ICC1 verifies the requested transaction using digital signature by calling Algorithm 2 (ICC_verifies_requested_transaction)
9 if (yes), then:
10 ICC1 votes using consensus protocol within itself to determine whether to conduct the transaction

[0129]

11 if (yes), then:
12 set the transaction between PPC1 and ICC1 as “pending”
13 if (real-time transaction processing), then:
14 mark this transaction condition as “tentative”
15 else if (multilateral netting processing), then:
16 mark this transaction condition as “pre-tentative”
17 end if
18 if (mode (b)), then:
19 ICC1 informs PPC1 the pending transaction // Process 2a
20 end if
21 initiate the transaction between ICC1 and PPC2 by calling Algorithm 3 (initiate_the_transaction_between_ICC1_and_PPC2) // Process 2 for mode (a); Process 2b for mode (b)

```
22          if (success), then:
23             PPC2 informs ICC1 the transaction
approval between ICC1 and PPC2, and send transaction
information for verification to ICC1   // Process 3
24             ICC1 verifies the transaction using
digital signature by calling Algorithm 2
(ICC_verifies_requested_transaction)
25             if (yes), then:
26                set the transaction between ICC1 and
PPC2 as “pending”
27                ICC1 informs PPC1 and PPC2 the
transaction confirmation      // Process 4a and 4b, the
transaction satisfy the requirement and can be conducted
28                if (PPC1 does not receive the
transaction confirmation in Time1), then: // Time1 is the
maximum amount of time PPC1 can wait
29                   ICC1 conducts consensus with PPC1
and PPC2 to decide whether the transaction between PPC1 and
PPC2 failed
30                   if (yes), then:
31                      mark all previous steps as
[0130]  “failure”
32                      cancel the pending transactions
33                      ICC1 conducts consensus with
PPC1 and PPC2
34                      return (time out error)
35                   end if
36                end if
37                if (real-time transaction processing),
then:
38                   conduct a real-time transaction by
calling Algorithm 10 (ICC_conducts_real_time_transaction)
39                else if (multilateral netting
processing), then:
40                   mark this transaction condition as
“tentative”
41                   conduct multilateral netting by
calling Algorithm 11 (ICC_conducts_multilateral_netting)
42                end if
43             else:
44                mark all previous steps as “failure”
   45             cancel the pending transaction
between ICC1 and PPC1 by calling Algorithm 12
```

```
(cancel_pending_transaction_between_ICC_and_PPC1)
   46                return (transaction with PPC2 failure)
to PPC1
   47             end if
   48          else:
   49             mark all previous steps as “failure”
      50             cancel the pending transaction between
ICC1 and PPC1 by calling Algorithm 12
(cancel_pending_transaction_between_ICC_and_PPC1)
   51             return (transaction with PPC2 failure) to
PPC1
   52          end if
   53       else:
   54          return (Byzantine failure) to PPC1
   55          mark all previous steps as “failure”
   56       end if
   57    else:
   58       return (verification failure) to PPC1
   59       mark all previous steps as “failure”
   60    end if
   61 else:
   62    return (failure)
   63 end if
```

[0131]

[0132] 对于算法1中所调用的算法2，中间链验证请求的交易，其输入包括中间链及其TBC，以及请求的交易信息。其具体过程如下。

[0133] (1)TBC将对其收到的交易信息进行验证的请求发送给ABC，其中ABC是中间链的一部分；

[0134] (2)通过调用算法4，ABC对该请求的交易进行验证，如果验证成功，则向TBC返回验证成功的信息；否则，返回失败信息。

[0135] 该过程的主要算法以伪代码的形式展示如下，记为算法2，中间链验证请求的交易。

[0136]

```
Algorithm 2: ICC_verifies_requested_transaction
Input: TBC, ICC, requested transaction
1 the TBC sends verification request of the received
requested transaction to the ABC // the ABC is a part of
the ICC
2 the ABC verifies the requested transaction by calling
Algorithm 4
(verify_requested_transaction_by_using_digital_signature)
3 if (yes), then:
4    return (verification success) to TBC
5 else:
6    return (verification failure) to TBC
7 end if
```

[0137]

[0138] 对于算法1中所调用的算法3，中心链1(ICC1)开始准备向参与链2(PPC2)发起交易请求，其输入包括中间链1(ICC1)和参与链2(PPC2)。其具体过程如下。

[0139] (1)中间链1对其各个节点进行投票(使用CBFT、或PBFT、或其它的拜占庭共识协议、或数据库事物协议)，来决定是否执行其与参与链2(PPC2)的交易，如果投票成功，则进入第(2)步；如果投票失败，则返回失败信息；

[0140] (2)选定一个用于中间链1与参与链2(PPC2)执行交易的TBC2，该TBC2为中间链1的一部分；

[0141] (3)TBC2随后向参与链2(PPC2)发送交易请求，即为过程(2b)；

[0142] (4)调用算法4，由参与链2(PPC2)对该交易请求进行验证(利用电子签名等)，如果验证成功，则进入第(5)步；如果验证失败，则返回错误信息，并将之前所有的步骤标记为“失败”；

[0143] (5)参与链2(PPC2)对其内部各个节点进行投票(使用CBFT、或PBFT、或其它的拜占庭共识协议、或数据库事物协议)来决定是否接受该交易，如果投票成功，则返回成功信息；如果投票失败，则返回投票失败的信息，并将之前所有的步骤标记为“失败”。

[0144] 该过程的主要算法以伪代码的形式展示如下，记为算法3，中心链1开始向参与链2发起的交易请求。

[0145]

```
Algorithm 3: initiate_the_transaction_between_ICC1_and_PPC2
input: ICC1, PPC2
1 ICC1 votes using CBFT or PBFT or other Byzantine consensus protocol within itself to determine whether to conduct the transaction with PPC2
2 if (yes), then:
3 determine the TBC2 to be used for this transaction between PPC2 and ICC1 // the TBC2 is a part of ICC1
4 the TBC2 sends transaction request to PPC2 // Process 2 for mode (a); Process 2b for mode (b)
5 PPC2 verifies the transaction request using digital signature, be calling Algorithm 4 (verify_requested_transaction_by_using_digital_signature)
6 if (yes), then:
7 PPC2 votes using CBFT or PBFT or other Byzantine consensus protocol within itself to determine whether to receive this transaction
8 if (yes), then:
9 return (success)
10 else:
11 return (failure)
12 mark all previous steps as “failure”
13 end if
14 else:
15 return (failure) to ICC1
16 mark all previous steps as “failure”
17 end if
18 else:
19 return (failure)
20 end if
```

[0147] 对于算法1中所调用的算法4,用数字签名验证交易信息,其输入包括请求者、验证者与请求的交易。其具体过程如下。

[0148] (1)验证者使用数字签名对请求者进行验证,如果验证成功,则进入第(2)步;如果验证失败,则返回向请求者返回验证失败的信息;

[0149] (2)验证者检查请求者是否具有相关的资源以进行其请求的交易,如果有,则进入第(3)步;否则,向请求者返回没有相关资源的失败信息;

[0150] (3)验证者检查请求者是否有足够量的资源或余额已完成该请求的交易,如果有,则返回验证成功的信息;否则,向请求者返回资源不足的失败信息。

[0151] 该过程的主要算法以伪代码的形式展示如下,记为算法4,用数字签名验证交易信息。

[0152]

```
Algorithm 4: verify_requested_transaction_by_using_digital_signature
Input: requester, verifier, requested transaction
1 the verifier verifies the requester using digital signature
2 if (yes), then:
3    the verifier checks if the requester has the assets associated with the requested transaction
4    if (yes), then:
5       the verifier checks if the assets are sufficient for the requested transaction
6       if (yes), then:
7          return (verification success)
8       else:
9          return ("insufficient assets") to the requester
10      end if
11   else:
12      return ("no associated asset") to the requester
13   end if
14 else:
15   return (failure) to the requester
16 end if
```

[0153]

[0154] 对于(3)新链加入网络，分为两种情况：(A)新的参与链加入网络；(B)新的中间链加入网络。下面对两种情况分别进行讨论。

[0155] 对于情况(A)，新的参与链加入网络，其输入为将要加入该网络的新的参与链，以及该网络(包括该网络中的其它参与链与中间链)。当一个新的参与链将要加入网络，该参与链自己可能产生一个或多条中间链，并且这些新产生的中间链与在该网络中已经存在的其它参与链项链，同时，该参与链也可能与其它在该网络中已经存在的中间链相连；该参与链也可能并不自己产生中间链，那么该参与链必须链接一个或多个已经存在的中间链。其具体的过程如下。

[0156] (1)在该参与链需要自己产生新的中间链的情况下，执行以下过程，直到该参与链不再需要自己产生新的中间链为止：

[0157] (a)该参与链产生一个新的中间链；

[0158] (b)通过调用算法7，此中间链与该参与链相连；

[0159] (c)找出所有其他的需要与此中间链相连的已经存在的参加链(每一条中间链需要连接两个及以上参与链)，并放入一个其它参与链集合中；

[0160] (d)对于所得的其它参与链集合中的每一条参与链，通过调用算法7，将这条参与链与此中间链相连；

[0161] 随后，执行：

[0162] (2)判断该参与链是否需要与该网络中已经存在的中间链相连，如果是，则进入第(3)步；

[0163] (3)找出所有需要该参与链需要与之进行交易的其他参与链，并找出所有与这些参与链相连的中间链；

[0164] (4)在保证所有在上一步中被找出的参与链都被包括的情况下，从上一部找出的所有中间链中找出一条中间链子集，这是由于每一条参与链可以与多条中间链相连，所以可以找出一条中间链自己来保证所有的需要的参与链都与这些中间链相连；

[0165] (5)对于中间链子集中的每一条中间链，通过调用算法7来将该参与链与这条中间链相连。

[0166] 该过程的主要算法以伪代码的形式展示如下，记为算法5，新的参与链加入网络。

[0167]
```
Algorithm 5: add_a_new_PPC_into_the_network
Input: PPC, network
1  while (this PPC needs to generate new ICCs), do:
2      this PPC generates a new ICC
3      link the ICC with this PPC by calling Algorithm 7
(link_an_ICC_with_a_PPC)
4      identify other existing PPCs need to link to the
```

```
ICC   // because one ICC needs to link to two or more PPCs
   5      put those PPCs into a set OtherPPCSet
   6      for (each PPC in OtherPPCSet), do:
   7         link the ICC with the PPC by calling Algorithm
7 (link_an_ICC_with_a_PPC)
   8      end for
   9  end while
   10 determine whether this PPC needs to link to existing
ICCs  // the PPC may need to link to other existing ICCs
   11 if (yes), then:
   12    identify all the PPCs that this PPC needs to make
transaction with
```

[0168]

```
   13    identify all the ICCs connect to those PPCs
   14    select a subset of all those ICCs identified in
the previous step, under the constraint that all the PPCs
identified in the first step are included //  because  each
PPC can connect with multiple ICCs, so can select a subset
of the ICCs to be included in the ICCSet, but all the
needed PPCs are included
   15    put the subset of ICCs into a set ICCSet
   16    for (each ICC in ICCSet), do:
   17       link this PPC with the ICC by calling Algorithm
7 (link_an_ICC_with_a_PPC)
   18    end for
   19 end if
```

[0169] 对于情况(B),新的中间链加入网络,其输入为将要加入该网络的新的中间链,以及该网络(包括该网络中的其它参与链与中间链)。其具体的过程如下。

[0170] (1)找到需要与该即将加入的新中间链相连的所有的网络中已经存在的参与链;

[0171] (2)如果没有或只有一条参与链将要与该中间链相连,则向该中间链返回错误信息,这是因为每条中间链需要与两条及以上条参与链相连;如果有两条或以上条参与链将要与该中间链相连,则进入第(3)步;

[0172] (3)将这些将要与该中间链相连的参与链放入一个集合中,通过调用算法7,将该集合中的每一条参与链与该中间链相连。

[0173] 该过程的主要算法以伪代码的形式展示如下,记为算法6,新的中间链加入网络。

```
Algorithm 6: add_a_new_ICC_into_the_network
Input: ICC, network
```

[0174]

```
1  identify all the PPCs need to be linked to this ICC
2  if (0 or 1 PPC need to be linked to this ICC), then:
// each ICC should be linked to two or more PPCs
```

```
    3     return (failure to this ICC)
    4  else:
    5     put all the PPCs need to be linked to this ICC
into a set PPCSet
[0175]  6     for (all PPC in PPCSet), do:
    7        link the PPC with this ICC by calling Algorithm
7: (link_an_ICC_with_a_PPC)
    8     end for
    9  end if
```

[0176] 对于算法5与算法6中所调用的算法7:一条参与链与一条中间链相连接,其输入包括一条参与链和一条中间链。其具体过程如下。

[0177] (1)如果该中间链中没有TBC可以被使用,则产生一个新的属于该中间链的TBC;

[0178] (2)通过调用算法8,连接该参与链与该TBC。

[0179] 该过程的主要算法以伪代码的形式展示如下,记为算法7,一条参与链与一条中间链相连接。

```
    Algorithm 7: link_an_ICC_with_a_PPC
    Input: ICC, PPC
    1  if (no TBC associated with the ICC can be used), then:

[0180]  2     create a new TBC associated with the ICC
    3  end if
    4  link the PPC with the TBC associated with the ICC,
using Algorithm 8
(link_a_PPC_with_the_TBC_associated_with_an_ICC)
```

[0181] 对于算法7中所调用的算法8:一条参与链与一个TBC相连接,其输入包括一条参与链,一个TBC,与该TBC所在的中间链。其具体过程如下。

[0182] (1)该参与链对其各个节点进行投票(使用CBFT、或PBFT、或其它的拜占庭共识协议、或数据库事物协议),来决定是否与该TBC相连,如果投票成功,则进入第(2)步;否则,返回错误信息;

[0183] (2)该参与链向该TBC发送验证信息(如数字签名等);

[0184] (3)通过调用算法9,该TBC所在的中间链验证所收到的信息(利用数字签名等),如果验证通过,则进行第(4)步;否则,返回失败信息;

[0185] (4)该中间链对其各个节点进行投票(使用CBFT、或PBFT、或其它的拜占庭共识协议、或数据库事物协议),来决定是否与该参与链相连,如果投票成功,则将该TBC与该参与链相连;否则,返回错误信息。

[0186] 该过程的主要算法以伪代码的形式展示如下,记为算法8,一条参与链与一个TBC相连接。

[0187] Algorithm 8: link_a_PPC_with_the_TBC_associated_with_an_ICC

```
Input: PPC, TBC, ICC
1 the PPC vote using consensus protocol within itself
to determine whether link to the TBC
2 if (yes), do:
3    the PPC sends verification information (such as
digital signature) to the TBC
4    the ICC verifies the received information (using
such as digital signature) by calling Algorithm 9
(ICC_verifies_the_received_information)
5    if (verified), do:
6       the ICC votes using consensus protocol within
itself to determine whether to link the PPC
7       if (yes), do:
8          connect the TBC with the PPC
9       else:
10         return (failure to the PPC)
11      end if
12   else:
13      return (failure to the PPC)
14   end if
15 else:
16   return (false)
17 end if
```

[0189] 对于算法8中所调用的算法9:中间链验证收到的信息,其输入包括一条中间链,包括其中的TBC与ABC,以及该中间链所收到的信息。其具体过程如下。

[0190] (1)该TBC向ABC发送验证请求,验证该TBC收到的信息;

[0191] (2)此ABC使用数字签名等方法验证该收到的信息,如果验证成功,则向TBC返回验证成功的信息;否则,则向TBC返回验证失败的信息。

[0192] 该过程的主要算法以伪代码的形式展示如下,记为算法9,中间链验证收到的信息。

```
Algorithm 9: ICC_verifies_the_received_information
Input: ICC, received information
1 the TBC sends verification request of the received
information to the ABC  // the ABC is a part of the ICC
2 the ABC verifies the requested information using
digital signature
3 if (yes), then:
4    return (verification success) to TBC
5 else:
6    return (verification failure) to TBC
7 end if
```

[0194] 对于算法1中所调用的中间链执行实时交易,当参与链1(PPC1)与参与链2(PPC2)

收到中间链发送的确认该交易可以发生的信息后，即完成过程(4a)与(4b)后，中间链与参与链1(PPC1)以及中间链与参与链2(PPC2)的被标记为待定(pending)的交易在该过程中立即执行，达到完成交易(commit)。其具体过程如下。

[0195] (1)执行中间链与参与链1(PPC1)以及中间链与参与链2(PPC2)的被标记为待定(pending)的交易，直到该参与链1(PPC1)对参与链2(PPC2)的交易成功完成。

[0196] (2)中间链告知参与链1(PPC1)与参与链2(PPC2)交易完成。

[0197] (3)TBC1与TBC2纪录该交易信息。

[0198] 该过程的主要算法以伪代码的形式展示如下，记为算法10，中间链执行实时交易。

[0199]
```
Algorithm 10: ICC_conducts_real_time_transaction
Input: ICC, PPC1, PPC2
1  while (transaction not completed), do:
2     conduct all the “pending” transactions  // commit
3  end while
4  ICC informs PPC1 and PPC2 the transaction completion
5  record the transaction information in TBC1 and TBC2
```

[0200] 对于算法1中所调用的中间链进行多边净额结算，当中间链完成一定时间量(一个结算周期：一小时、一天、或一周等)的交易记账(各条参与链在该时间量内的的交易记于该中间链中)，中间链进行多边净额结算。其具体过程如下。

[0201] 当一个结算周期结束，则中间链进行下面的操作；

[0202] (1)停止初始化或开始任何新的交易，并完成所有正在进行的交易或待定(tentative)交易；

[0203] (2)中间链找出所有在前一个结算周期中与该中间链进行试图交易的参与链，并将这些参与链放入一个集合中；

[0204] (3)中间链找出所有在前一个结算周期中的交易记录；

[0205] (4)对于每一条参与链，中间链对其在上一个结算周期中的所有交易的应付与应收资金或资源进行冲抵轧差，并根据轧差所得的净值向该参与链进行交收。

[0206] (5)核实该多方净值结算结果是否正确：判断在进行冲抵轧差之后，该结算周期内通过该中间链进行交易的所有的参与链的交易进出的总和是否为0，如为0，则认为正确，如果不为0，则错误；

[0207] (6)如果正确，则中间链根据结算结果向各条参与链执行最终交易；若不正确，则重新进行多方净值结算或进行人工核查。

[0208] 该过程的主要算法以伪代码的形式展示如下，记为算法11，中间链进行多边净额结算。

[0209]
```
Algorithm 11: ICC_conducts_multilateral_netting
Input: ICC, PPCs
```

[0210]
```
1 if (time period for conducting multilateral netting is due), then:
2     stop initiating any new transactions
3     complete all transactions or tentative transactions already in process
4     ICC identifies all the PPCs that made tentative transactions with ICCs during the last time period
5     put those PPCs into a set PPCSet
6     ICC identifies all the recorded tentative transactions of the last time period
7     for (each PPC in PPCSet), do:
8         ICC nets all the tentative transactions of the PPC on a multilateral basis // this is done by adding or subtraction for each transactions depending on the direction of payment, the result is the net payment from one PPC to another PPC
9     end for
10    verify if the multilateral netting is success by checking if the sum of all transactions of the participating PPCs in the last time period is 0
11    if (yes), then:
12        ICC commits the results of the netting to each participating PPC
13    else:
14        conduct multilateral netting again or conduct manual verification
15    end if
16 end if
```

[0211] 对于算法1中所调用的取消中间链(ICC)与参与链1(PPC1)之间的待定交易,每次进行取消操作之前都需要由中间链与所有参与到本次交易的参与链进行共识,来决定是否取消该待定交易。如果取消了该待定交易,中间链需要再一次进行共识来告知所有参与到本次交易的参与链。其具体过程如下。

[0212] (1)中间链(ICC)与参与链1(PPC1)及参与链2(PPC2)进行共识,以决定是否取消参与链1(PPC1)与中间链(ICC)之间的待定(pending)交易;

[0213] (2)如果是,则将该待定交易取消,并且中间链(ICC)与参与链1(PPC1)及参与链2(PPC2)进行共识,以告知该待定交易已被取消。

[0214] 该过程的主要算法以伪代码的形式展示如下,记为算法12,取消中间链与参与链1(PPC1)之间的待定交易。

[0215] Algorithm 12: cancel_pending_transaction_between_ICC_and_PPC1

```
Input: ICC, PPC1, PPC2
1 the ICC conducts consensus with PPC1 and PPC2 to
decide whether to cancel the pending transaction between
PCC1 and the ICC
2 if (yes), then:
3     cancel the pending transaction between PCC1 and ICC

4     the ICC conducts consensus with PPC1 and PPC2
5 end if
```

[0216]

[0217] 虽然本发明已经参考特定的说明性实施例进行了描述，但是不会受到这些实施例的限定而仅仅受到附加权利要求的限定。本领域技术人员应当理解可以在不偏离本发明的保护范围和精神的情况下对本发明的实施例能够进行改动和修改。

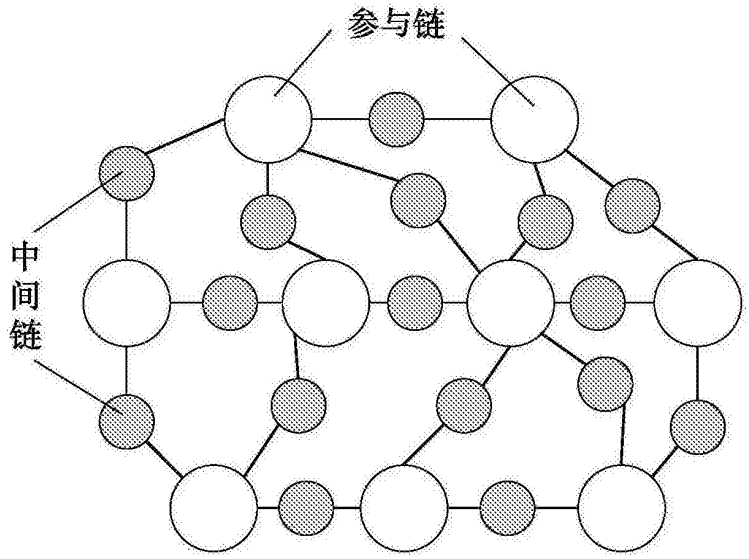


图1

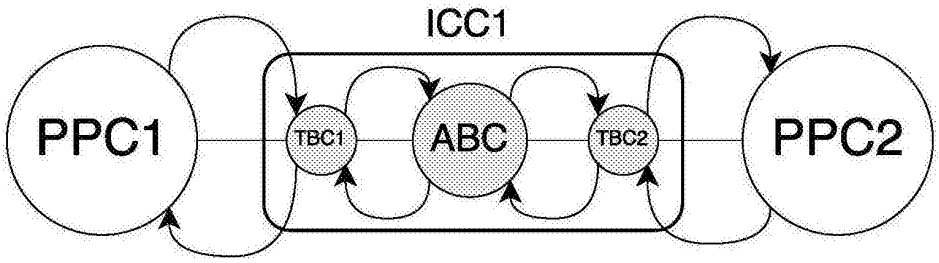


图2

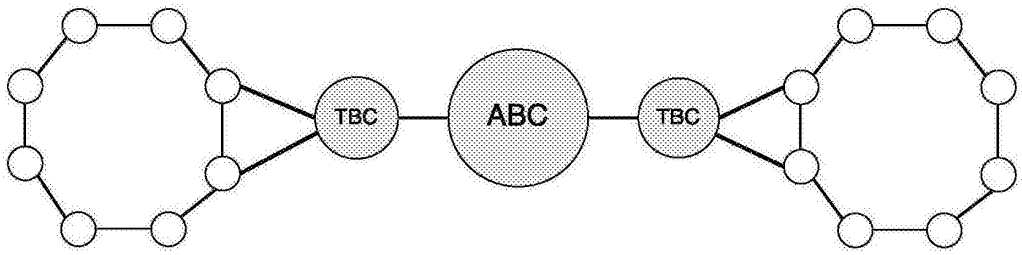


图3

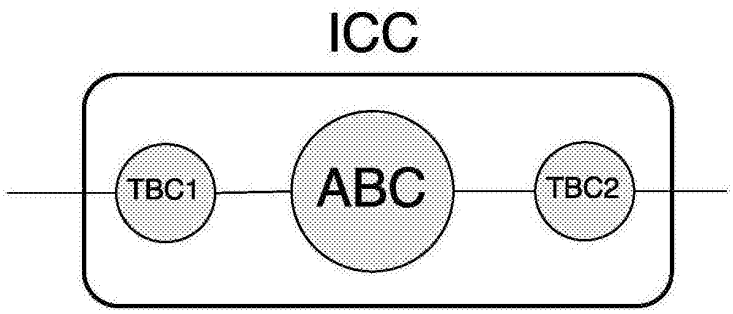

ICC
TBC1
ABC
TBC2

图4

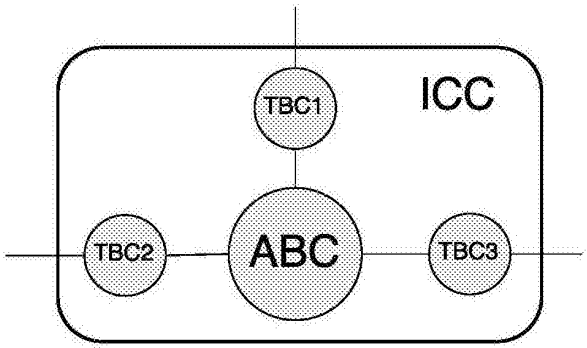

ICC
TBC1
TBC2
ABC
TBC3

图5

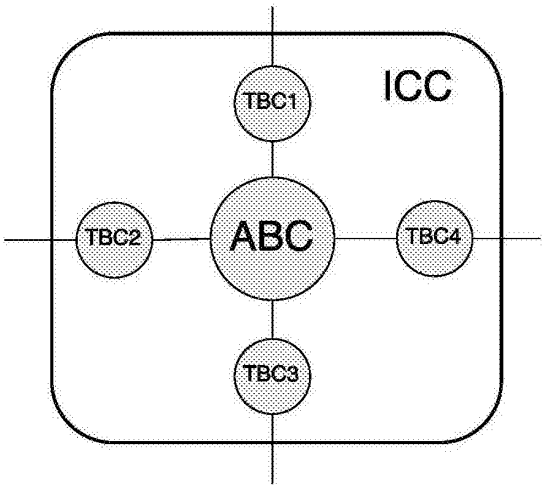

ICC
TBC1
TBC2
ABC
TBC4
TBC3

图6

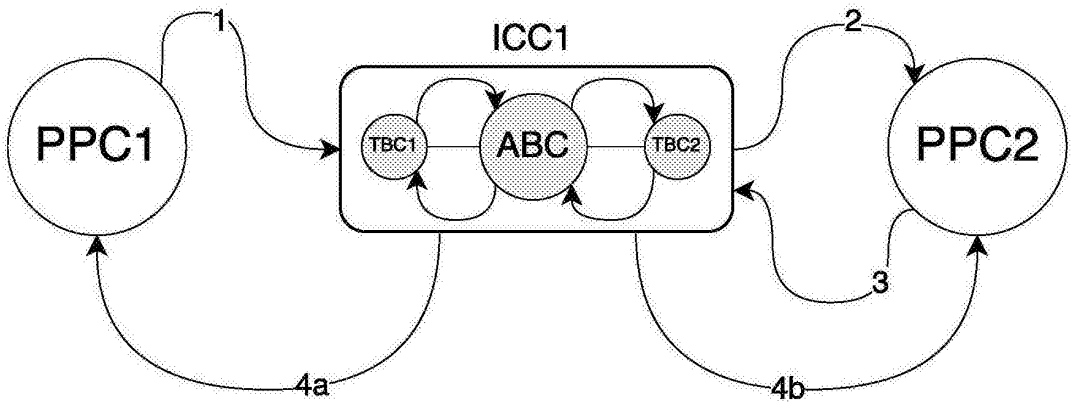

ICC1
PPC1
PPC2
TBC1
ABC
TBC2
1
2
3
4a
4b

图7

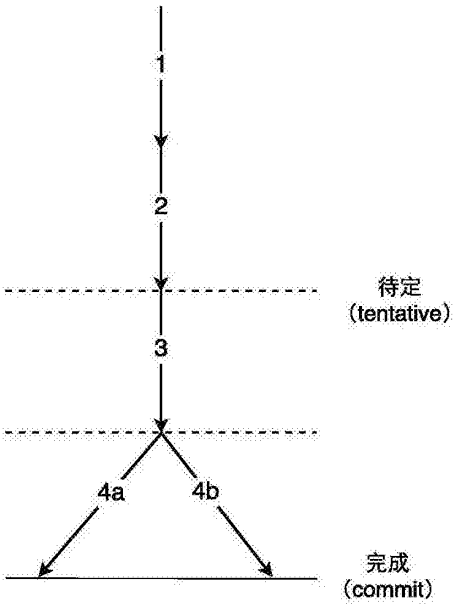

1
2
待定
(tentative)
3
4a
4b
完成
(commit)

图8

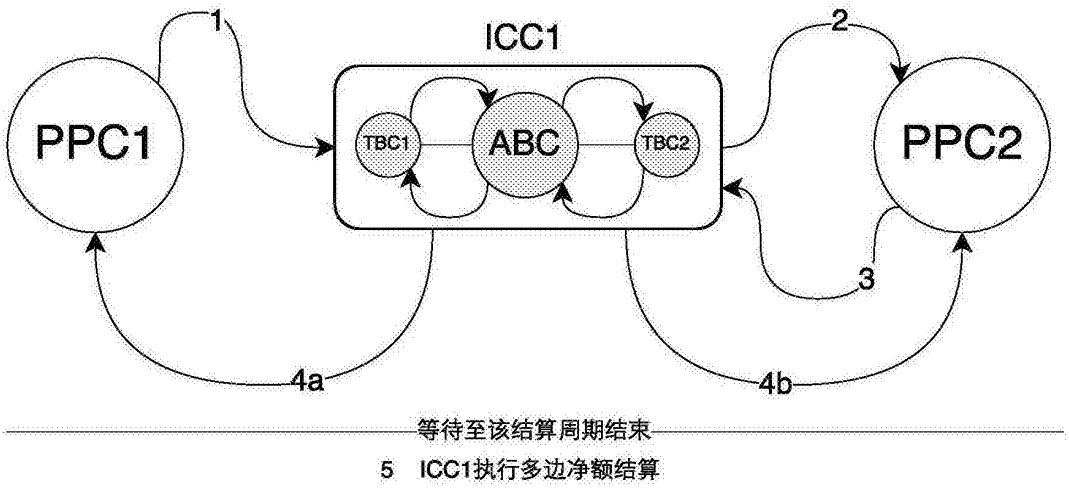

ICC1
PPC1
PPC2
TBC1
ABC
TBC2
1
2
3
4a
4b
等待至该结算周期结束
5 ICC1执行多边净额结算

图9

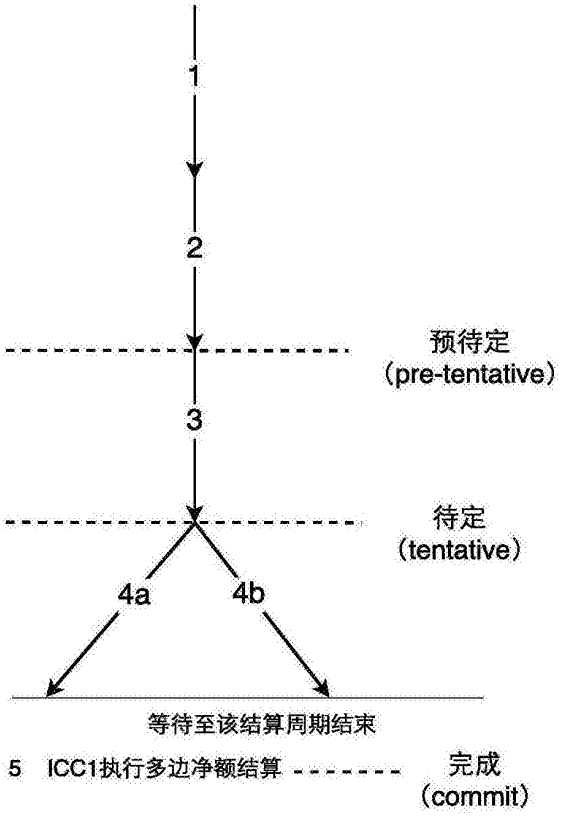

1
2
预待定
(pre-tentative)
3
待定
(tentative)
4a
4b
等待至该结算周期结束
5 ICC1执行多边净额结算
完成
(commit)

图10

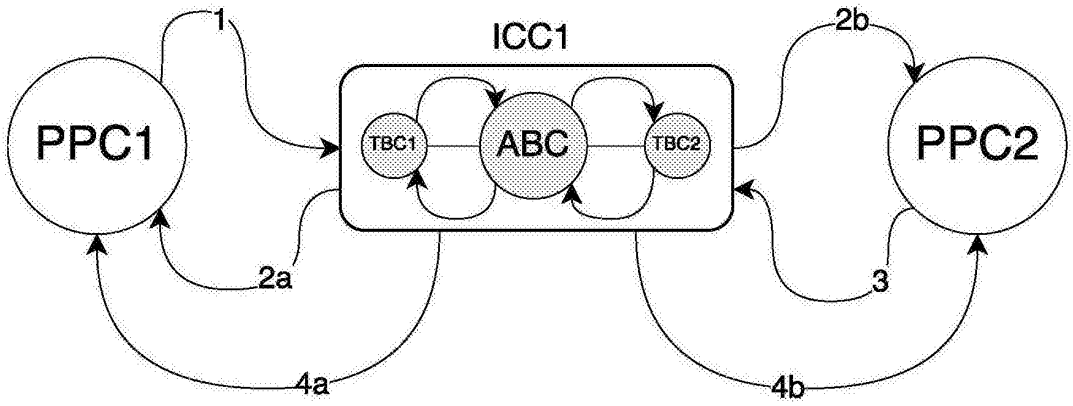

1
ICC1
2b
PPC1
TBC1
ABC
TBC2
PPC2
2a
3
4a
4b

图11

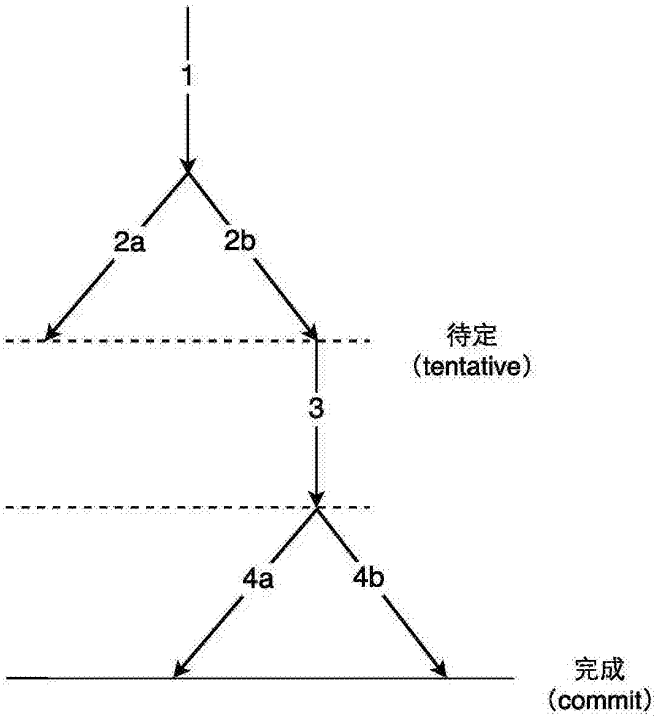

1
2a
2b
待定
(tentative)
3
4a
4b
完成
(commit)

图12

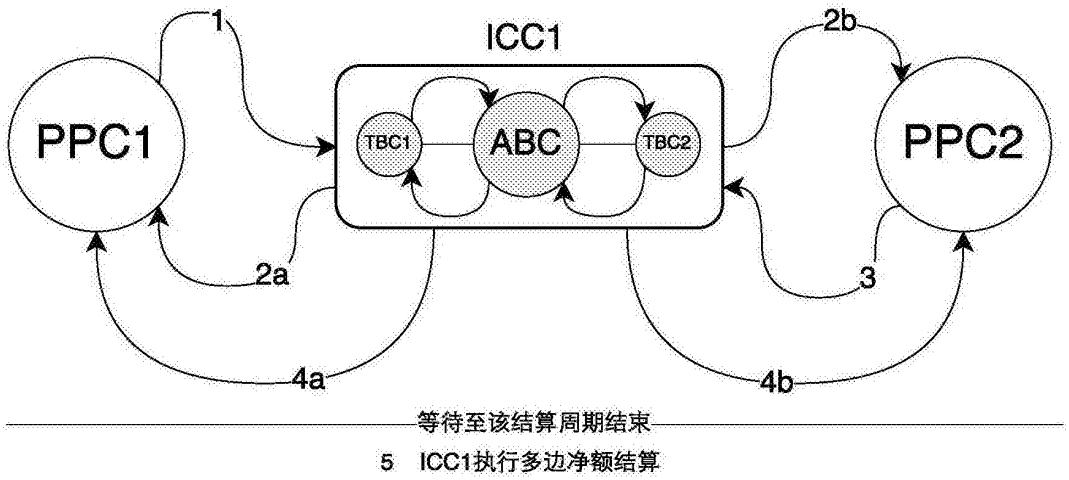

1
ICC1
2b
PPC1
TBC1
ABC
TBC2
PPC2
2a
3
4a
4b
等待至该结算周期结束
5 ICC1执行多边净额结算

图13

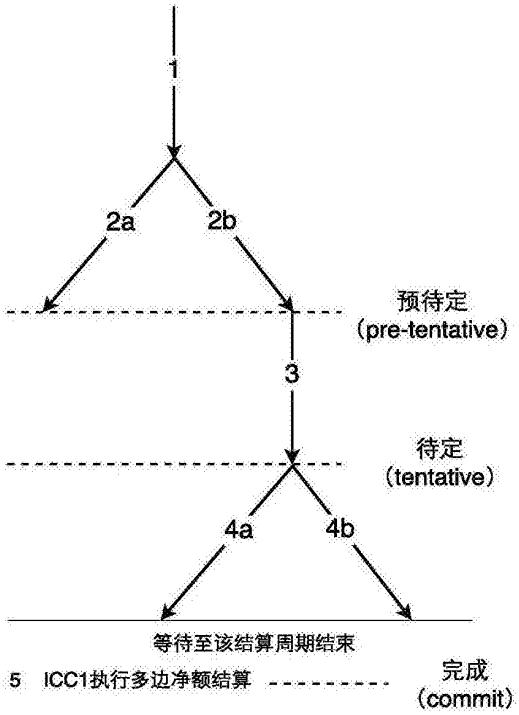

1
2a
2b
预待定
(pre-tentative)
3
待定
(tentative)
4a
4b
等待至该结算周期结束
5 ICC1执行多边净额结算
完成
(commit)

图14

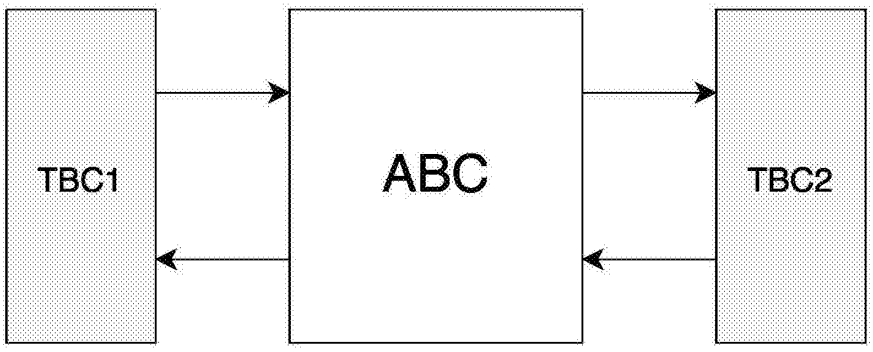


图15

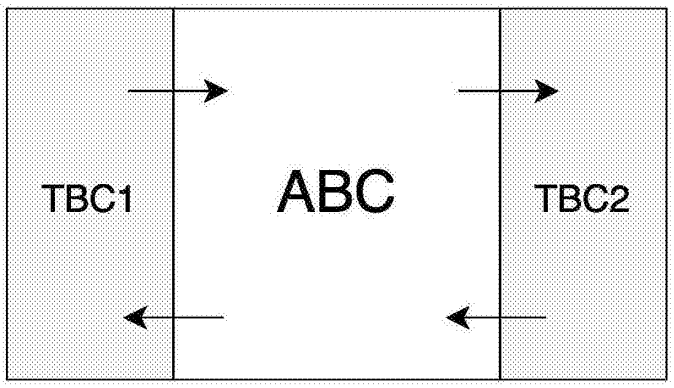


图16