(19)国家知识产权局

(12)发明专利

(10)授权公告号 CN 110555682 B
(45)授权公告日 2023.04.07

(21)申请号 201910854426.6

(22)申请日 2019.09.10

(65)同一申请的已公布的文献号
申请公布号 CN 110555682 A

(43)申请公布日 2019.12.10

(73)专利权人 苏州阿尔山数字科技有限公司
地址 215000 江苏省苏州市高铁新城南天成路55号相融大厦20层

(72)发明人 袁力

(74)专利代理机构 苏州拓源科佳知识产权代理事务所(普通合伙) 32533
专利代理师 赵艾亮

(51)Int.Cl.
G06Q 20/02(2012.01)
G06F 16/27(2019.01)
G06F 16/22(2019.01)

(56)对比文件
CN 109858908 A,2019.06.07
CN 108881187 A,2018.11.23
CN 109242456 A,2019.01.18
CN 109246179 A,2019.01.18
CN 109255610 A,2019.01.22
自游.一文理解超级账本 Hyperledger Fabric 的架构与坑.《百度》.2018,

审查员 鹿凤

权利要求书1页 说明书4页 附图2页

(54)发明名称

基于联盟链的多通道实现方法

(57)摘要

发明涉及区块链技术领域,尤其是基于联盟链的多通道实现方法。该多通道实现方法的步骤为:a)联盟链创建有代币的通道或无代币的通道;b)在联盟链创建的有代币的通道或无代币的通道内发生交易;或在联盟链创建的有代币的通道或无代币的通道内关闭通道;或跨链交易。本发明当需要跨链操作时,通过发送信息给背书节点,背书节点返回相应的结果集操作。针对多通道的联盟链,通过建立排序链记录所有区块的唯一hash值,当通道中的链上有新的区块生成时,向排序链中增加区块信息,通过区块信息去获取对应链上的区块内容。通过引入排序链可以确定不同通道的区块顺序,当多个交易对同一个区块操作时,不会导致其他交易失败。

CN 110555682 B

1.一种基于联盟链的多通道实现方法,其特征在于:该多通道实现方法的步骤为:

a)联盟链创建有代币的通道或无代币的通道;

b)在联盟链创建的有代币的通道或无代币的通道内发生交易;或在联盟链创建的有代币的通道或无代币的通道内关闭通道;或跨链交易;

步骤a)中,所述联盟链创建有代币的通道的具体步骤为:创建新通道时,通过数字证书进行权限控制,当身份验证通过时,开始创建通道,否则创建通道失败并退出,然后写入初始token值,以便后续进行账户交易,接着配置信息,并生成配置信息块写入系统通道链中,最后信息在新的通道中生成块信息并打包hash写入链中,通道创建成功;

步骤a)中,所述联盟链创建无代币的通道的具体步骤为:客户端开始创建新通道时,通过数字证书进行权限控制,当身份验证通过时,开始创建通道,否则创建通道失败并退出,然后写入通道的配置信息,并生成配置信息块写入系统通道链中,最后根据配置信息在新的通道中生成块信息并打包hash写入链中,通道创建成功;

步骤b)中,所述在联盟链创建的有代币的通道或无代币的通道内发生交易的具体步骤为:客户端发生交易时,通过数字证书进行权限控制,当身份验证通过时,开始发生交易,否则交易失败并退出,然后检测该交易是否带token信息,如果存在,系统将根据交易区块信息对账户token进行处理去,如果不存在,则不处理,接着根据order节点的排序结果打包生成区块信息,将区块信息广播给组织的其他节点并执行交易,最后把交易结果返回给客户端,交易完成;

步骤b)中,所述在联盟链创建的有代币的通道或无代币的通道内关闭通道的具体步骤为:当客户端需要关闭通道时,系统首先会通过数字证书对身份认证,如果认证成功,开始执行关闭通道行为,否则通道关闭失败并退出;如果该通道有token,最终将客户端的token值写入账户链中,并将结果返回给客户端;果没有涉及token,则直接关闭通道,停止交易;

步骤b)中,所述跨链交易的具体步骤为:当通道中有新的区块产生时,将区块的哈希值写入到全局排序链中,当某一时刻需要跨链操作时,直接访问全局排序链,获取这个时间节点的区块信息。

基于联盟链的多通道实现方法

技术领域

[0001] 发明涉及区块链技术领域,尤其是基于联盟链的多通道实现方法。

背景技术

[0002] 在公有链中,所有的节点都属于同一个链,所有的节点都会同步相同的数据,随着数据量的增大,每个节点都会同步和存储一些不必要的数据,增加了每个节点的压力,同时网络中的节点都能读取到所有的数据,一些敏感数据可能分发给不应该访问这些数据的节点,这会带来安全隐患。

[0003] 而且所有公链都有一个致命弱点,每一个节点都必须参与每一笔交易,并通过保存交易的副本来保护系统,这限制了区块链可以处理的交易数量,导致吞吐量低,随着区块链中交易量的增加,也增加了对节点存储、带宽和算力的需求。

[0004] 公有链解决方式其实有很多如分片、链下计算、DAG等,分片技术通过将区块链的所有内容分成不同的碎片,每个碎片都由网络中不同节点存储和处理,通过分布式存储和计算来降低每个节点的压力。或者以一种安全和可验证的方式链下计算,提升吞吐量,基于以太坊的TrueBit就是一个好的例子。基于DAG的数据结构来维护系统还处于起步阶段,没有得到大规模的推广,在最终理论完善之前其应用场景应慎重选择。

[0005] Hyperledger Fabric是区块链的基础核心平台,目标是成为面向企业的开发应用和解决方案的分布式账本平台,创新的引入权限管理支持,设计上支持可插拔、可扩展,是首个面向联盟链场景的开源项目,也是最早加入到Hyperledger项目中的顶级项目,由IBM、DAH等企业于2015年底提交到社区,它提出了联盟链的多通道技术,指的是部分网络成员之间拥有独立的通信渠道,在通道中发送的交易只有属于通道的成员才可见,因此通道可以看做网络中部分成员的私有通信子网。在联盟之下若干不同的组织建立了一个一个的通道,每个通道都有一个独立的账本,只有通道成员组织之间才能共享账本。在实际应用中,它通常承载着诸如资产和交易之类的敏感数据,因此安全和隐私保护是两个非常重要的问题。

[0006] 但是现有的公有链虽然可以解决节点的可扩展性问题,但是隐私权受限,将关键业务数据上传到区块链后,黑客,竞争对手或其他未授权方就可以查看区块链上的信息,这对大部分公司都不愿意这样做的。对于关心隐私和个人权益的个人、组织和行业来说,隐私权是底线。许多区块链和加密货币的拥护者都有共同的期许,希望能够建立一个无需信任的、不受审查的系统,让每个人都可以参与记账。矛盾的是,我们使用的是一个公共的、易于追踪的分类帐。公链缺乏正式的合同验证,对智能合约的核查仍然是一个尚未解决的问题,首先,智能合约是不可变的,这意味着一旦他们被放到以太坊主网,就不能再进行更新和修复。此外,智能合约里面的内容都是公开的,任何人都可以查看,任何人也可以调用智能合约的公共算法,虽然这提供了公开性和透明度,但他也使智能合同成为黑客的目标,事实上,无论您采取了多少预防措施,都很难使智能合约完美无缺,无论如何,正式验证是减少错误和攻击的有力方法。它确保了比传统方法(如测试、同行评审等)更高的更高的安全性。

目前迫切需要更好的解决方案。Hyperlenger Fabric是目前联盟链中的代表，采用读写集进行进行链上交易操作，虽然安全性很好，但是并发性很差，如果多次更新同一个区块只有一个成功，后续交易失败，只能重新提交交易等待执行，体验性差，只保证了一致性，但是不满足可用性，不符合实际的应用场景。Hyperledger Fabric多通道技术缺乏全局序，所以导致其不能很好的支持经济模型、跨链调用等。

发明内容

[0007] 为了解决背景技术中描述的技术问题，本发明提供了一种基于联盟链的多通道实现方法，Hyperlenger Fabric在交易发生时需要通过背书节点模拟交易生成读写集，然后将结果返回给客户端，当需要跨链操作时，通过发送信息给背书节点，背书节点返回相应的结果集操作。针对多通道的联盟链，通过建立排序链记录所有区块的唯一hash值，相当于记录当前时刻每个区块的索引值，当通道中的链上有新的区块生成时，向排序链中增加区块信息，如果对于跨链操作不是特别频繁，可以每隔一段时间对区块进行批量操作记录，当进行跨链操作时，主链通过访问排序链，获取当前操作涉及的相关区块，然后通过区块信息去获取对应链上的区块内容。通过引入排序链可以确定不同通道的区块顺序，不需要与背书节点连接，当多个交易对同一个区块操作时，可以排队执行，不会导致其他交易失败。

[0008] 本发明解决其技术问题所采用的技术方案是：

[0009] 一种基于联盟链的多通道实现方法，该多通道实现方法的步骤为：

[0010] a)联盟链创建有代币的通道或无代币的通道；

[0011] b)在联盟链创建的有代币的通道或无代币的通道内发生交易；或在联盟链创建的有代币的通道或无代币的通道内关闭通道；或跨链交易。

[0012] 具体地，步骤a)中，所述联盟链创建有代币的通道的具体步骤为：创建新通道时，通过数字证书进行权限控制，当身份验证通过时，开始创建通道，否则创建通道失败并退出，然后写入初始token值，以便后续进行账户交易，接着配置信息，并生成配置信息块写入系统通道链中，最后信息在新的通道中生成块信息并打包hash写入链中，通道创建成功。

[0013] 具体地，步骤a)中，所述联盟链创建无代币的通道的具体步骤为：客户端开始创建新通道时，通过数字证书进行权限控制，当身份验证通过时，开始创建通道，否则创建通道失败并退出，然后写入通道的配置信息，并生成配置信息块写入系统通道链中，最后根据配置信息在新的通道中生成块信息并打包hash写入链中，通道创建成功。

[0014] 具体地，步骤b)中，所述在联盟链创建的有代币的通道或无代币的通道内发生交易的具体步骤为：客户端发生交易时，通过数字证书进行权限控制，当身份验证通过时，开始发生交易，否则交易失败并退出，然后检测该交易是否带token信息，如果存在，系统将根据交易区块信息对账户token进行处理去，如果不存在，则不处理，接着根据order节点的排序结果打包生成区块信息，将区块信息广播给组织的其他节点并执行交易，最后把交易结果返回给客户端，交易完成。

[0015] 具体地，步骤b)中，所述在联盟链创建的有代币的通道或无代币的通道内关闭通道的具体步骤为：当客户端需要关闭通道时，系统首先会通过数字证书对身份认证，如果认证成功，开始执行关闭通道行为，否则通道关闭失败并退出；如果该通道有token，最终将客户端的token值写入账户链中，并将结果返回给客户端；果没有涉及token，则直接关闭通

道,停止交易。

[0016] 具体地,步骤b)中,所述跨链交易的具体步骤为:当通道中有新的区块产生时,将区块的哈希值写入到全局排序链中。当某一时刻需要跨链操作时,直接访问全局排序链,获取这个时间节点的区块信息。

[0017] 本发明的有益效果是:本发明提供了一种基于联盟链的多通道实现方法,Hyperlenger Fabric在交易发生时需要通过背书节点模拟交易生成读写集,然后将结果返回给客户端,当需要跨链操作时,通过发送信息给背书节点,背书节点返回相应的结果集操作。针对多通道的联盟链,通过建立排序链记录所有区块的唯一hash值,相当于记录当前时刻每个区块的索引值,当通道中的链上有新的区块生成时,向排序链中增加区块信息,如果对于跨链操作不是特别频繁,可以每隔一段时间对区块进行批量操作记录,当进行跨链操作时,主链通过访问排序链,获取当前操作涉及的相关区块,然后通过区块信息去获取对应链上的区块内容。通过引入排序链可以确定不同通道的区块顺序,不需要与背书节点连接,当多个交易对同一个区块操作时,可以排队执行,不会导致其他交易失败。

附图说明

[0018] 下面结合附图和实施例对发明进一步说明。

[0019] 图1是本发明的联盟链创建有代币的通道的流程图;

[0020] 图2是本发明的联盟链创建无代币的通道的流程图;

[0021] 图3是本发明的在联盟链创建的有代币的通道或无代币的通道内发生交易的流程图;

[0022] 图4是本发明的在联盟链创建的有代币的通道或无代币的通道内关闭通道的流程图;

[0023] 图5是本发明的跨链交易的流程图;

具体实施方式

[0024] 现在结合附图对发明作进一步详细的说明。这些附图均为简化的示意图,仅以示意方式说明发明的基本结构,因此其仅显示与发明有关的构成。

[0025] 图1是本发明的联盟链创建有代币的通道的流程图,图2是本发明的联盟链创建无代币的通道的流程图,图3是本发明的在联盟链创建的有代币的通道或无代币的通道内发生交易的流程图,图4是本发明的在联盟链创建的有代币的通道或无代币的通道内关闭通道的流程图,图5是本发明的跨链交易的流程图。

[0026] 联盟链的通道创建分为代币与非代币,当涉及到账户交易时,需要创建代币。

[0027] 如附图1所示,联盟链创建有代币的通道时:

[0028] 1)创建新通道时,通过数字证书进行权限控制,当身份验证通过时,开始创建通道,否则创建通道失败并退出。

[0029] 2)写入初始token值,以便后续进行账户交易。

[0030] 3)的配置信息,并生成配置信息快写入系统通道链中。

[0031] 4)信息在新的通道中生成块信息并打包hash写入链中,通道创建成功。

[0032] 如附图2所示,联盟链创建无代币的通道时:

[0033] 1)客户端开始创建新通道时,通过数字证书进行权限控制,当身份验证通过时,开始创建通道,否则创建通道失败并退出。

[0034] 2)写入通道的配置信息,并生成配置信息块写入系统通道链中。

[0035] 3)根据配置信息在新的通道中生成块信息并打包hash写入链中,通道创建成功。

[0036] 如附图3所示,在联盟链创建的有代币的通道或无代币的通道内发生交易:

[0037] 1)客户端发生交易时,通过数字证书进行权限控制,当身份验证通过时,开始发生交易,否则交易失败并退出。

[0038] 2)检测该交易是否带token信息,如果存在,系统将根据交易区块信息对账户token进行处理去,如果不存在,则不处理。

[0039] 3)根据order节点的排序结果打包生成区块信息,将区块信息广播给组织的其他节点并执行交易。

[0040] 4)最终把交易结果返回给客户端,交易完成。

[0041] 如附图4所示,在联盟链创建的有代币的通道或无代币的通道内关闭通道:

[0042] 1)当客户端需要关闭通道时,系统首先会通过数字证书对身份认证,如果认证成功,开始执行关闭通道行为,否则通道关闭失败并退出。

[0043] 2)如果该通道有token,最终将客户端的token值写入账户链中,并将结果返回给客户端;果没有涉及token,则直接关闭通道,停止交易。

[0044] 如附图5所示,跨链交易:

[0045] 当通道中有新的区块产生时,将区块的哈希值写入到全局排序链中。当某一时刻需要跨链操作时,直接访问全局排序链,获取这个时间节点的区块信息,即使后续有区块增加,也不会影响当前时刻区块操作的一致性。

[0046] 全局排序链:当通道中有新的区块产生时,顺序记录所有区块的hash值。

[0047] 以上述依据发明的理想实施例为启示,通过上述的说明内容,相关工作人员完全可以在不偏离本项发明技术思想的范围内,进行多样的变更以及修改。本项发明的技术性范围并不局限于说明书上的内容,必须要根据权利要求范围来确定其技术性范围。

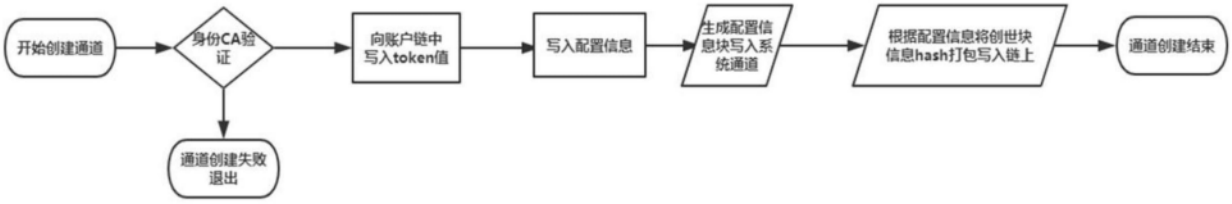
开始创建通道
身份CA验证
通道创建失败退出
向账户链中写入token值
写入配置信息
生成配置信息块写入系统通道
根据配置信息将创世块信息hash打包写入链上
通道创建结束

图1

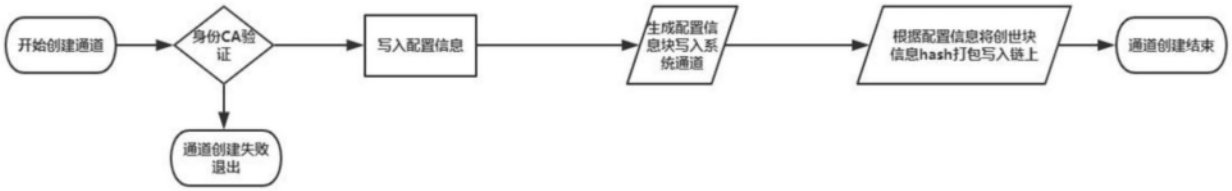
开始创建通道
身份CA验证
通道创建失败退出
写入配置信息
生成配置信息块写入系统通道
根据配置信息将创世块信息hash打包写入链上
通道创建结束

图2

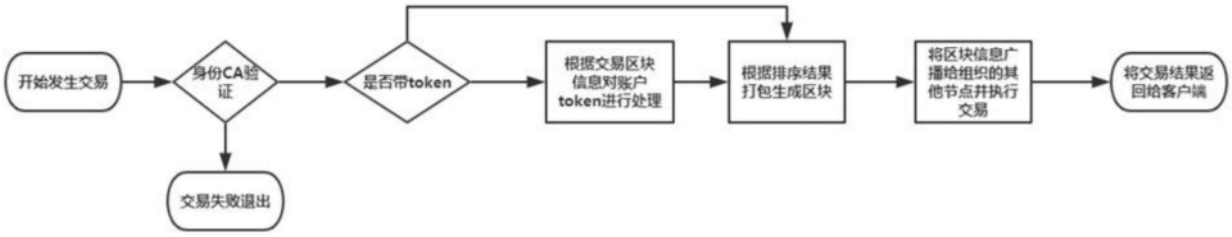
开始发生交易
身份CA验证
交易失败退出
是否带token
根据交易区块信息对账户token进行处理
根据排序结果打包生成区块
将区块信息广播给组织的其他节点并执行交易
将交易结果返回给客户端

图3

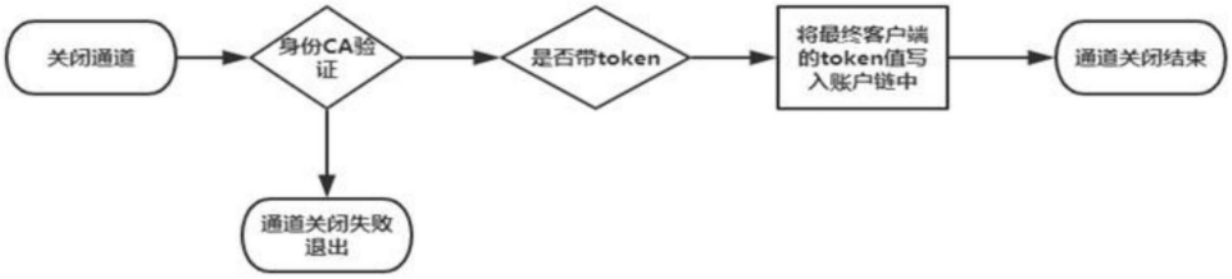
关闭通道
身份CA验证
通道关闭失败退出
是否带token
将最终客户端的token值写入账户链中
通道关闭结束

图4

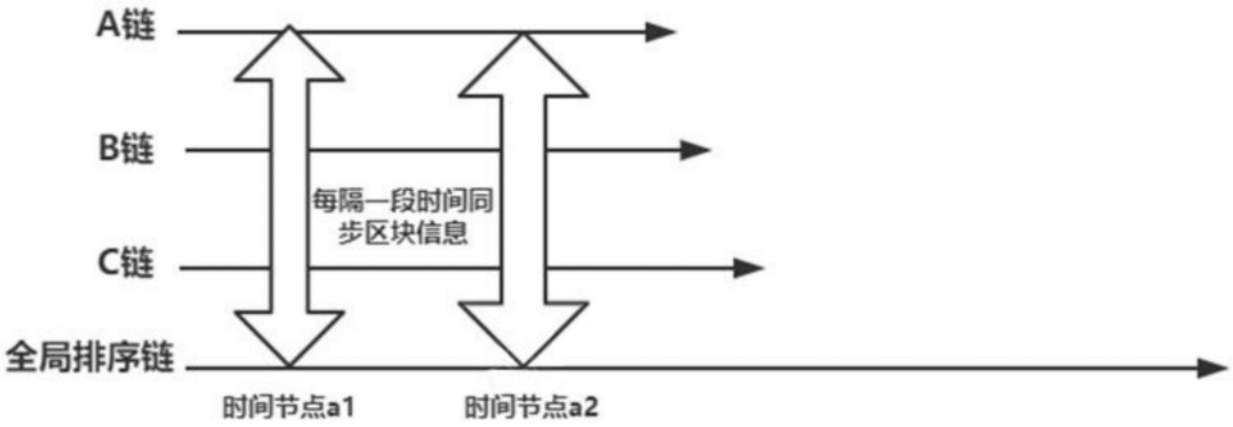

图5