(19)国家知识产权局

(12)发明专利

(10)授权公告号 CN 113452747 B
(45)授权公告日 2022.12.16

(21)申请号 202110523673.5

(22)申请日 2021.05.13

(65)同一申请的已公布的文献号
申请公布号 CN 113452747 A

(43)申请公布日 2021.09.28

(73)专利权人 西安电子科技大学
地址 710071 陕西省西安市太白南路2号西安电子科技大学
专利权人 西安链融科技有限公司

(72)发明人 裴庆祺 朱发远 肖阳

(74)专利代理机构 西安长和专利代理有限公司 61227
专利代理师 黄伟洪

(51)Int.Cl.
H04L 67/10(2022.01)
H04L 67/1095(2022.01)
H04L 9/40(2022.01)
H04L 65/1073(2022.01)

(56)对比文件
CN 112511312 A,2021.03.16
US 2020106623 A1,2020.04.02
CN 106878071 A,2017.06.20
US 9875510 B1,2018.01.23

审查员 赵冰

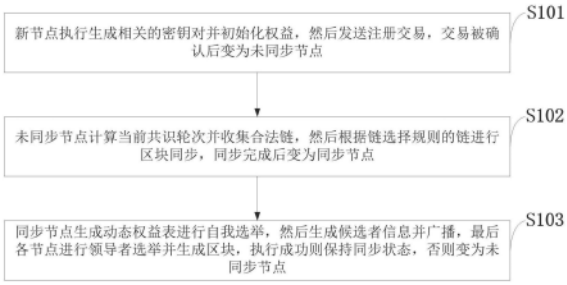
权利要求书3页 说明书9页 附图4页

(54)发明名称

可扩展和安全的共识方法、系统、存储介质、智能终端

(57)摘要

本发明属于分布式系统共识机制和区块链公链技术领域，公开了一种可扩展和安全的共识方法、系统、存储介质、智能终端，包括节点注册、区块生成和区块同步三个协议；节点注册协议，新节点生成初始信息和初始化权益信息，使用公共信息和权益信息生成节点注册交易，再发送到共识网络进行节点注册成为网络节点；区块生成协议，共识节点生成节点权益份额表和随机数进行候选者选举，然后由候选者生成压缩候选区块并广播，其他节点验证候选区块信息后选择符合条件的作为领导者生成区块；区块同步协议，未同步节点计算当前共识轮次并对收到的链的合法性验证，使用链选择规则选择一条链进行同步。本发明提高方案的安全属性，有效提升了方案的可扩展性。



CN 113452747 B

1.一种可扩展和安全的共识方法,其特征在于,所述可扩展和安全的共识方法包括节点注册、区块生成和区块同步三个协议;

节点注册协议,新节点生成初始信息和初始化权益信息,使用公共信息和权益信息生成节点注册交易,再发送到共识网络进行节点注册成为网络节点;

区块生成协议,共识节点生成节点权益份额表和随机数进行候选者选举,然后由候选者生成压缩候选区块并广播,其他节点验证候选区块信息后选择符合条件的作为领导者生成区块;

区块同步协议,未同步节点计算当前共识轮次并对收到的链的合法性进行验证,然后使用链选择规则选择一条链进行同步;

所述可扩展和安全的共识方法具体包括:

第一步,新节点执行节点注册协议进行注册,新节点生成相关的密钥对并初始化权益,然后将注册交易发送到共识网络中,交易被确认后节点注册成功,新节点变成未同步节点;

第二步,同步节点执行区块生成协议保持同步状态,同步节点生成动态权益表后进行自我选举,然后候选者生成压缩的区块并广播区块和VRF证明,最后各节点验证候选区块并生成区块,执行成功则保持同步状态,否则变为未同步节点;

第三步,未同步节点执行区块同步协议变成同步节点,未同步节点先计算当前共识轮次,然后收集网络中合法的链,最后选择一条合适的链进行区块同步,同步完成后未同步节点变成同步节点。

2.如权利要求1所述的可扩展和安全的共识方法,其特征在于,所述可扩展和安全的共识方法的分布式网络系统中的参与方有3个,分别是未注册的新节点、已同步的网络节点和未同步的网络节点;分别执行3个协议,分别为基于权益机制的节点注册协议、基于随机可验证函数的区块生成协议和基于最长链规则的区块同步协议。

3.如权利要求1所述的可扩展和安全的共识方法,其特征在于,所述可扩展和安全的共识方法的基于权益机制的节点注册协议包括节点信息初始化和注册交易发送两个阶段:

节点信息初始化的步骤为:

1)新节点使用签名密钥生成算法和随机生成的安全参数生成密钥对,包括签名私钥和验签公钥;

2)新节点使用随机可验证函数密钥生成算法和随机生成的安全参数生成密钥对,包括随机数生成私钥和随机数验证公钥;

3)新节点生成初始权益值;

注册交易发送的步骤为:

1)新节点将签名公钥、随机数验证公钥和初始权益值公共信息附加到交易中生成注册交易;

2)新节点将生成的注册交易发送到共识网络节点,等待打包该交易的区块生成并被确认后节点注册成功。

4.如权利要求1所述的可扩展和安全的共识方法,其特征在于,所述可扩展和安全的共识方法的基于随机可验证函数的区块生成协议包括候选者选举、候选区块生成与广播和领导者选举3个阶段:

候选者选举的步骤为:

1)共识节点读取链中的区块数据,根据区块中的交易数据信息计算所有节点的权益值,然后生成所有节点的权益份额表;

2)共识节点使用当前区块的随机数和共识轮次作为随机种子计算可验证随机数;

3)共识节点根据生成的随机数和现在的自身权益份额进行自我选举,即判断自身是否满足候选者条件,满足则成为候选者执行后续的候选区块生成流程,否则执行新区块生成流程;

候选区块生成步骤为:

1)候选者节点根据候选区块的所有交易生成区块头,生成区块主体时,对于已经广播的交易,只放入其唯一标识,未广播的交易则放入完整数据;

2)候选者将生成的候选区块、可验证随机数、随机数证明和验证公钥打包为候选者信息广播到网络中的其他节点;

领导者选举步骤为:

1)共识节点对收到的候选者信息进行验证,先验证共识轮次公共信息是否一致,然后验证随机数合法性,再验证候选者身份的合法性,若都满足则加入候选池中,否则丢弃候选信息;

2)对于候选池中的候选信息,共识节点选择可验证随机数最小的那个候选者作为领导者,并使用其候选区块信息生成新区块,若候选池中没有候选信息,则此轮不生成新区块,然后开始下一轮共识。

5.如权利要求1所述的可扩展和安全的共识方法,其特征在于,所述可扩展和安全的共识方法的基于最长链规则的区块链同步协议包括链选择规则与区块同步两个部分:

链选择规则是结合最长链规则和可验证随机数的新规则,描述如下:

1)如果有两条链长度不同,选择长度更长的链;

2)如果两条链长度相同,先选择它们的分叉点后区块的共识轮次更早的那条;

3)若轮次相同,则选择分叉点后区块的可验证随机数更小的那条链;

区块同步步骤如下:

1)节点从创世区块中获得创世时间戳,然后使用当前时间戳计算出当前共识轮次;

2)节点向网络中其他节点请求链数据,并对收到的链数据合法性进行验证,先验证最新区块的共识轮次,然后验证创世区块的合法性,再验证链的合法性,若都满足则将链加入链候选池中,否则丢弃该链及其数据;

3)节点使用上面介绍的链选择规则选择唯一一条链,并同步其区块数据,同步完成后成为同步节点。

6.一种计算机可读存储介质,存储有计算机程序,所述计算机程序被处理器执行时,使得所述处理器执行如下步骤:

第一步,新节点执行节点注册协议进行注册,新节点生成相关的密钥对并初始化权益,然后将注册交易发送到共识网络中,交易被确认后节点注册成功,新节点变成未同步节点;

第二步,同步节点执行区块生成协议保持同步状态,同步节点生成动态权益表后进行自我选举,然后候选者生成压缩的区块并广播区块和VRF证明,最后各节点验证候选区块并生成区块,执行成功则保持同步状态,否则变为未同步节点;

第三步,未同步节点执行区块同步协议变成同步节点,未同步节点先计算当前共识轮

次，然后收集网络中合法的链，最后选择一条合适的链进行区块同步，同步完成后未同步节点变成同步节点。

7.一种信息数据处理终端，其特征在于，所述信息数据处理终端用于实现权利要求1～6任意一项所述的可扩展和安全的共识方法。

8.一种执行权利要求1～6任意一项所述可扩展和安全的共识方法的可扩展和安全的共识系统，其特征在于，所述可扩展和安全的共识系统包括：

交易信息处理模块，用于实现新节点执行生成相关的密钥对并初始化权益，然后发送注册交易，交易被确认后变为未同步节点；

同步节点处理模块，用于未同步节点计算当前共识轮次并收集合法链，然后根据链选择规则的链进行区块同步，同步完成后变为同步节点；

区块生成模块，用于同步节点生成动态权益表进行自我选举，然后生成候选者信息并广播，最后各节点进行领导者选举并生成区块，执行成功则保持同步状态，否则变为未同步节点。

9.一种区块链终端，其特征在于，所述区块链终端用于实现权利要求1～6任意一项所述的可扩展和安全的共识方法。

可扩展和安全的共识方法、系统、存储介质、智能终端

技术领域

[0001] 本发明属于分布式系统共识机制和区块链公链技术领域，尤其涉及一种可扩展和安全的共识方法、系统、存储介质、智能终端。

背景技术

[0002] 目前：区块链技术是构建在分布式点对点网络上的一种全新的分布式基础架构与计算范式，使用链式数据结构、共识算法、密码学技术和自动化智能合约等技术来存储和管理数据，并保证数据安全性。公有链是无需许可、节点规模大的区块链网络，具有去中心化和去信任等优秀特性，在多方参与的分布式身份、数据防篡改、数据溯源、社会治理和去中心化应用领域具有技术优势。

[0003] 分布式系统共识机制是多个对等节点之间对某个问题达成一致的协议和方案。传统的分布式系统共识机制针对的是失效节点的一致性协议，即系统运行时节点因网络或自身因素导致失效的情况下如何保证系统正常对外提供服务，节点之间默认是互相信任且不会作恶的。区块链的共识机制还包括互不信任且存在恶意节点的网络，能够适用于更加灵活的应用场景。

[0004] 目前最接近的现有技术是基于Ouroboros的Cardano。Ouroboros是一个基于权益证明机制的公链共识机制，旨在解决工作量证明的资源消耗问题并保证数据安全性。Cardano项目由Charles Hoskinson在2017年发布，致力于创建一个完善的区块链智能合约平台，使得用户在点对点支付网络中快速并且低费用的交易，同时保证交易安全性。该项目的底层区块链网络共识协议的原型就是Ouroboros，通过这个协议来保证网络节点数据的一致性和安全性。

[0005] 然而Ouroboros共识方案主要关注的是公链共识方案的安全性，协议中还引入了精确时钟来进行区块生成，实现代价较高。另外Ouroboros没有考虑方案的可扩展性问题，以及权益机制对共识方案的影响，使得方案不适用于性能要求不断增加的实际应用场景。Cardano的具体实现中要求具有一定比例以上的节点才能参与共识，实际上违背了区块链的去中心化属性，使得Cardano并不能完全成为一个去中心化公链系统。

[0006] 通过上述分析，现有技术存在的问题及缺陷为：

[0007] (1)现有Ouroboros共识方案主要关注的是公链共识方案的安全性，协议中还引入了精确时钟来进行区块生成，实现代价较高。

[0008] (2)现有Ouroboros没有考虑方案的可扩展性问题，以及权益机制对共识方案的影响，使得方案不适用于性能要求不断增加的实际应用场景。

[0009] (3)现有Cardano的具体实现中要求具有一定比例以上的节点才能参与共识，实际上违背了区块链的去中心化属性，使得Cardano并不能完全成为一个去中心化公链系统。

[0010] 解决以上问题及缺陷的难度为：减少方案对第三方如全局时钟的依赖同时保证方案安全性较难；设计完整可行且可扩展性高的新共识方案需要考虑多个方面的因素；去中心化公链系统需要平衡每个节点的功能与作用，系统设计存在困难。

[0011] 解决以上问题及缺陷的意义为:能够使得公链共识方案减少对第三方的依赖,更加去中心化,保证公链安全性;能够提高使用该可扩展性高的共识方案的公链的性能,使得公链能够适用于更多领域,推动公链技术的应用和发展。

发明内容

[0012] 针对现有技术存在的问题,本发明提供了一种可扩展和安全的共识方法、系统、存储介质、智能终端。

[0013] 本发明是这样实现的,一种可扩展和安全的共识方法,所述可扩展和安全的共识方法包括节点注册、区块生成和区块同步三个协议;

[0014] 节点注册协议,新节点生成初始信息和初始化权益信息,使用公共信息和权益信息生成节点注册交易,再发送到共识网络进行节点注册成为网络节点;

[0015] 区块生成协议,共识节点生成节点权益份额表和随机数进行候选者选举,然后由候选者生成压缩候选区块并广播,其他节点验证候选区块信息后选择符合条件的作为领导者生成区块;

[0016] 区块同步协议,未同步节点计算当前共识轮次并对收到的链的合法性进行验证,然后使用链选择规则选择一条链进行同步。

[0017] 进一步,所述可扩展和安全的共识方法具体包括:

[0018] 第一步,新节点执行节点注册协议进行注册,新节点生成相关的密钥对并初始化权益,然后将注册交易发送到共识网络中,交易被确认后节点注册成功,新节点变成未同步节点。在新节点初始化时同时初始化权益,通过将节点权益值写入注册交易中来把权益机制与共识方案结合。

[0019] 第二步,同步节点执行区块生成协议保持同步状态,同步节点生成动态权益表后进行自我选举,然后候选者生成压缩的区块并广播区块和VRF证明,最后各节点验证候选区块并生成区块,执行成功则保持同步状态,否则变为未同步节点。该步骤保证共识的可靠性与公平性,并通过候选区块压缩方法来减小广播区块的尺寸,从而降低共识的通信消耗来提高共识效率。

[0020] 第三步,未同步节点执行区块同步协议变成同步节点,未同步节点先计算当前共识轮次,然后收集网络中合法的链,最后选择一条合适的链进行区块同步,同步完成后未同步节点变成同步节点。诚实节点能够根据链选择规则选择同一条主链进行同步,使得方案不依赖第三方就能支持动态可用性。

[0021] 进一步,所述可扩展和安全的共识方法的分布式网络系统中的参与方有3个,分别是未注册的新节点、已同步的网络节点和未同步的网络节点;分别执行3个协议,分别为基于权益机制的节点注册协议、基于随机可验证函数的区块生成协议和基于最长链规则的区块同步协议。

[0022] 进一步,所述可扩展和安全的共识方法的基于权益机制的节点注册协议包括节点信息初始化和注册交易发送两个阶段:

[0023] 节点信息初始化的步骤为:

[0024] 1)新节点使用签名密钥生成算法和随机生成的安全参数生成密钥对,包括签名私钥和验签公钥;

[0025] 2)新节点使用随机可验证函数密钥生成算法和随机生成的安全参数生成密钥对，包括随机数生成私钥和随机数验证公钥；

[0026] 3)新节点生成初始权益值；

[0027] 注册交易发送的步骤为：

[0028] 1)新节点将签名公钥、随机数验证公钥和初始权益值等公共信息附加到交易中生成注册交易；

[0029] 2)新节点将生成的注册交易发送到共识网络节点，等待打包该交易的区块生成并被确认后节点注册成功。

[0030] 进一步，所述可扩展和安全的共识方法的基于随机可验证函数的区块生成协议包括候选者选举、候选区块生成与广播和领导者选举3个阶段：

[0031] 候选者选举的步骤为：

[0032] 1)共识节点读取链中的区块数据，根据区块中的交易数据信息计算所有节点的权益值，然后生成所有节点的权益份额表；

[0033] 2)共识节点使用当前区块的随机数和共识轮次作为随机种子计算可验证随机数；

[0034] 3)共识节点根据生成的随机数和现在的自身权益份额进行自我选举，即判断自身是否满足候选者条件，满足则成为候选者执行后续的候选区块生成流程，否则执行新区块生成流程；

[0035] 候选区块生成步骤为：

[0036] 1)候选者节点根据候选区块的所有交易生成区块头，生成区块主体时，对于已经广播的交易，只放入其唯一标识，未广播的交易则放入完整数据；

[0037] 2)候选者将生成的候选区块、可验证随机数、随机数证明和验证公钥打包为候选者信息广播到网络中的其他节点；

[0038] 领导者选举步骤为：

[0039] 1)共识节点对收到的候选者信息进行验证，先验证共识轮次等公共信息是否一致，然后验证随机数合法性，再验证候选者身份的合法性，若都满足则加入候选池中，否则丢弃该候选信息；

[0040] 2)对于候选池中的候选信息，共识节点选择可验证随机数最小的那个候选者作为领导者，并使用其候选区块信息生成新区块，若候选池中没有候选信息，则此轮不生成新区块，然后开始下一轮共识。

[0041] 进一步，所述可扩展和安全的共识方法的基于最长链规则的区块链同步协议包括链选择规则与区块同步两个部分：

[0042] 链选择规则是结合最长链规则和可验证随机数的新规则，描述如下：

[0043] 1)如果有两条链长度不同，选择长度更长的链；

[0044] 2)如果两条链长度相同，先选择它们的分叉点后区块的共识轮次更早的那条；

[0045] 3)若轮次相同，则选择分叉点后区块的可验证随机数更小的那条链；

[0046] 区块同步步骤如下：

[0047] 1)节点从创世区块中获得创世时间戳，然后使用当前时间戳计算出当前共识轮次；

[0048] 2)节点向网络中其他节点请求链数据，并对收到的链数据合法性进行验证，先验

证最新区块的共识轮次，然后验证创世区块的合法性，再验证链的合法性，若都满足则将链加入链候选池中，否则丢弃该链及其数据；

[0049] 3)节点使用上面介绍的链选择规则选择唯一一条链，并同步其区块数据，同步完成后成为同步节点。

[0050] 本发明的另一目的在于提供一种计算机可读存储介质，存储有计算机程序，所述计算机程序被处理器执行时，使得所述处理器执行如下步骤：

[0051] 第一步，新节点执行节点注册协议进行注册，新节点生成相关的密钥对并初始化权益，然后将注册交易发送到共识网络中，交易被确认后节点注册成功，新节点变成未同步节点；

[0052] 第二步，同步节点执行区块生成协议保持同步状态，同步节点生成动态权益表后进行自我选举，然后候选者生成压缩的区块并广播区块和VRF证明，最后各节点验证候选区块并生成区块，执行成功则保持同步状态，否则变为未同步节点；

[0053] 第三步，未同步节点执行区块同步协议变成同步节点，未同步节点先计算当前共识轮次，然后收集网络中合法的链，最后选择一条合适的链进行区块同步，同步完成后未同步节点变成同步节点。

[0054] 本发明的另一目的在于提供一种信息数据处理终端，所述信息数据处理终端用于实现所述的可扩展和安全的共识方法。

[0055] 本发明的另一目的在于提供一种执行所述可扩展和安全的共识方法的可扩展和安全的共识系统，所述可扩展和安全的共识系统包括：

[0056] 交易信息处理模块，用于实现新节点执行生成相关的密钥对并初始化权益，然后发送注册交易，交易被确认后变为未同步节点；

[0057] 同步节点处理模块，用于未同步节点计算当前共识轮次并收集合法链，然后根据链选择规则的链进行区块同步，同步完成后变为同步节点；

[0058] 区块生成模块，用于同步节点生成动态权益表进行自我选举，然后生成候选者信息并广播，最后各节点进行领导者选举并生成区块，执行成功则保持同步状态，否则变为未同步节点。

[0059] 本发明的另一目的在于提供一种区块链终端，所述区块链终端用于实现所述的可扩展和安全的共识方法。

[0060] 结合上述的所有技术方案，本发明所具备的优点及积极效果为：本发明在权益证明机制的基础上提出一种可扩展且安全的共识方案，通过结合随机可验证函数设计区块生成协议和结合新的最长链规则设计区块同步协议来保证安全性；通过结合独立的权益机制设计节点注册协议和权益交易记录支持动态权益场景提高可扩展性，在保证方案安全性的前提下提高公链的可扩展性，使得基于该方案的公链能够适用于更多实际的应用场景。本发明克服了传统权益证明机制的效率低和安全性不足等问题，使得权益证明机制能够更加适用于公链共识机制，对于公链技术发展意义重大。

[0061] 本发明通过将权益证明机制和公链共识机制相结合，设计了一个安全且可扩展性高的共识方案。基于独立的权益机制设计节点注册协议，在新节点初始化时同时初始化权益，通过将节点权益值写入注册交易中来把权益机制与共识方案结合。基于随机可验证函数设计区块生成协议，通过可验证保证共识的可靠性与公平性，并提出了一种候选区块压

缩的方法来减小广播区块的尺寸，降低共识的通信消耗来提高共识效率。结合最长链规则设计区块同步协议，结合共识轮次和可验证随机数提出新的最长链规则，使得诚实节点能够根据其选择同一条主链进行同步，使得方案不依赖第三方就能支持动态可用性。

[0062] 本发明提供了一种基于权益机制的节点注册协议。该协议通过节点注册时单独初始化权益来将权益机制与激励机制独立开。提出独立于激励机制的权益机制，在节点初始化注册信息时就将节点权益值初始化。然后与节点的公开信息一起生成注册交易，在将交易发送到共识网络中进行节点注册。当包含该注册交易的区块被确认时，节点注册信息就被记录在区块链上，以此将节点与权益机制绑定起来。

[0063] 本发明提供了一种基于随机可验证函数的区块生成协议。该协议通过结合权益机制和随机可验证函数来进行区块生成共识，节点的权益份额就是共识时节点生成符合条件的可验证随机数的概率。节点先生成节点权益份额表，即根据区块链中的权益交易生成所有节点的权益份额表；然后进行候选者选举，即生成可验证随机数并根据自己的权益份额判断是否成为候选者，满足条件则广播候选区块和可验证证明；最后进行领导者选举，节点根据权益份额表对候选信息进行验证，然后选出最符合条件的候选者作为此次共识领导者并按照其区块信息生成新区块。另外对于提出一种候选区块压缩的方法，能够有效减少共识的通信消耗，提高共识效率。

[0064] 本发明提供了一种基于最长链规则的区块同步协议。该协议通过VRF随机数和新的最长链规则来进行节点区块同步。由于方案的区块生成协议将权益机制转换成工作量机制的方式，最长链规则能够保证链数据的安全性和不可篡改性。结合领导者选举规则和最长链规则设计新的链选择规则，使得诚实节点能选择最符合条件主链进行同步，在不依赖第三方的情况下支持节点动态可用性。

附图说明

[0065] 图1是本发明实施例提供的可扩展和安全的共识方法流程图。

[0066] 图2是本发明实施例提供的可扩展和安全的共识系统的结构示意图；

[0067] 图2中：1、交易信息处理模块；2、同步节点处理模块；3、区块生成模块。

[0068] 图3是本发明实施例提供的共识节点架构图。

[0069] 图4是本发明实施例提供的系统网络模型。

[0070] 图5是本发明实施例提供的方案详细流程图。

[0071] 图6是本发明实施例提供的系统性能仿真图。

具体实施方式

[0072] 为了使本发明的目的、技术方案及优点更加清楚明白，以下结合实施例，对本发明进行进一步详细说明。应当理解，此处所描述的具体实施例仅仅用以解释本发明，并不用于限定本发明。

[0073] 针对现有技术存在的问题，本发明提供了一种可扩展和安全的共识方法、系统、存储介质、智能终端，下面结合附图对本发明作详细的描述。

[0074] 如图1所示，本发明提供的可扩展和安全的共识方法包括以下步骤：

[0075] S101：新节点执行生成相关的密钥对并初始化权益，然后发送注册交易，交易被确

认后变为未同步节点。

[0076] S102:未同步节点计算当前共识轮次并收集合法链,然后根据链选择规则的链进行区块同步,同步完成后变为同步节点。

[0077] S103:同步节点生成动态权益表进行自我选举,然后生成候选者信息并广播,最后各节点进行领导者选举并生成区块,执行成功则保持同步状态,否则变为未同步节点。

[0078] 本发明提供的可扩展和安全的共识方法业内的普通技术人员还可以采用其他的步骤实施,图1的本发明提供的可扩展和安全的共识方法仅仅是一个具体实施例而已。

[0079] 如图2所示,本发明提供的可扩展和安全的共识系统包括:

[0080] 交易信息处理模块1,用于实现新节点执行生成相关的密钥对并初始化权益,然后发送注册交易,交易被确认后变为未同步节点。

[0081] 同步节点处理模块2,用于未同步节点计算当前共识轮次并收集合法链,然后根据链选择规则的链进行区块同步,同步完成后变为同步节点。

[0082] 区块生成模块3,用于同步节点生成动态权益表进行自我选举,然后生成候选者信息并广播,最后各节点进行领导者选举并生成区块,执行成功则保持同步状态,否则变为未同步节点。

[0083] 下面结合附图对本发明的技术方案作进一步的描述。

[0084] 本发明的区块链公链节点系统包括存储层、接口层和共识层3层,为上层应用提供节点共识服务。该方案包括初始化节点信息和独立的权益信息并进行节点注册的节点注册协议。该方案包括读取区块数据生成节点权益份额表并根据公共的随机种子生成可验证随机数进行自我选举的候选者选举。该方案包括打包广播交易和未广播交易生成压缩候选区块的候选区块生成。该方案包括收集合法候选者信息并从多个候选者中选择一个的领导者选举。该方案包括结合最长链规则和可验证随机数的链选择规则。该方案包括收集合法链并从中选择唯一一条的区块同步协议。因此,本公开的实例基于权益证明机制和公有链提出了一个可扩展的和安全的公链共识方案,通过将节权益机制与共识方案结合提高方案的灵活性,通过随机可验证函数的保证共识的可靠性与公平性,并提出了一种候选区块压缩的方法来减小广播区块的尺寸并提高共识效率,通过链选择规则使得方案不依赖第三方就能支持动态可用性,方案避免了工作量证明机制的能耗问题并拥有安全性和可扩展性,能够支持公链在各种延伸场景下的应用。

[0085] 图3为本发明方案的节点架构图,其中区块链数据库和交易缓存池为存储层,接口层包括密钥演进签名方案、权益机制、随机可验证函数和最长链规则四个模块,为共识层的节点注册协议、区块生成协议和区块同步协议提供支撑服务。

[0086] 图4为本发明方案的网络模型图,区块链公链网络是动态的,节点可以随时加入或退出网络,主要包括新节点、未同步节点与同步节点3种节点,分别执行节点注册、区块生成和区块同步三个协议。节点注册协议主要包括密钥对生成和权益初始化2个阶段,新节点执行节点注册协议后发送注册交易进行节点注册,交易被确认后注册成功并成为未同步节点。区块生成协议包括候选者选举,压缩区块广播和领导者选举3个阶段,所有同步节点通过执行该协议生成新区块并保持同步状态。区块同步协议包括合法链收集和链选择2个阶段,未同步节点或者新节点通过执行该协议同步到主链并成为同步节点。

[0087] 图5为本发明方案的总体流程图。方案参与方有3个,分别是新节点、未同步节点和

同步节点。方案分为3个协议，分别为节点注册协议、区块生成协议和区块同步协议。

[0088] 新节点是还未加入共识网络的节点，需要执行节点注册协议来加入网络。基于权益机制的节点注册协议包括节点信息初始化和注册交易发送两个阶段。

[0089] 节点信息初始化的步骤为：

[0090] 1)新节点n使用签名密钥生成算法和随机生成的安全参数生成签名私钥sigSK和验签公钥sigVK。

[0091] 2)新节点n使用随机可验证函数密钥生成算法和随机生成的安全参数生成随机数生成私钥vrfSK和随机数验证公钥vrfVK。

[0092] 3)新节点n生成初始权益值s。

[0093] 注册交易发送的步骤为：

[0094] 1)新节点n将签名公钥sigVK、随机数验证公钥vrfVK和初始权益值s等公共信息附加到交易信息中生成注册交易regTx。

[0095] 2)新节点将生成的注册交易regTx发送到共识网络节点m，等待打包该交易的区块b生成并被确认后节点n注册成功，变成未同步节点nAsyn。

[0096] 节点注册成功后变成未同步节点，需要执行区块同步协议才能变成同步节点，基于最长链规则的区块链同步协议包括链选择规则与区块同步两个部分。

[0097] 本发明的链选择规则是结合最长链规则和可验证随机数设计的，主要描述如下：1)如果有两条链长度不同，选择长度更长的链;2)如果两条链长度相同，先选择它们的分叉点后区块的共识轮次更早的那条;3)若轮次相同，则选择分叉点后区块的VRF随机数更小的那条链。举例来说，假如未同步节点进行区块同步时收到4条合法链，长度分别为99，100，100，100，那么长度为99的链会首先被排除，然后对比此时剩下3条链的编号为100的区块，假设其前99个区块都一样，若其共识轮次分别为122，121，121，那么共识轮次为122的链会被排除，最后比较剩下两条链最新区块的可验证随机数，若其分别为1023和865，那么未同步节点最终会选择最新区块的随机数为865的那条链的数据进行同步。

[0098] 区块同步协议步骤如下：

[0099] 1)未同步节点nAsyn从创世区块BlockGenesis中获得创世时间戳T，然后使用当前时间戳t计算出当前共识轮次r。

[0100] 2)未同步节点nAsyn向共识网络中其他同步节点请求链数据，并对收到的链数据合法性进行验证，先验证最新区块的共识轮次是否大于等于r，然后验证链创世区块的合法性，再验证链的合法性，即各区块的合法性，若都满足则将链加入此次区块同步的链候选池中，否则丢弃该链及其数据。

[0101] 3)未同步节点nAsyn使用上面介绍的链选择规则从链候选池中选择唯一一条链chain，并同步其区块数据，同步完成后成为同步节点nSyn。

[0102] 本发明的共识方案提出了一种独立的权益机制，使得权益机制与激励机制区分开，使得两个机制各自负责对应的职能，防止了二者互相干扰对公链系统的运行造成影响。本发明将权益机制与激励机制分开，单独作为PoS共识方案的一个部分，并在节点注册时就与其绑定，能够很好的支持权益机制的灵活性。另外，本发明不讨论共识的激励机制，节点权益不再与激励机制绑定，而是在新节点注册时将权益与注册交易绑定，节点权益值的变化都需要通过交易记录到链上在现实的网络中，每一次共识后节点权益都会发生变化，相

关工作很难支持动态权益场景。在拥有了独立的权益机制后，可以使用权益份额表支持动态权益场景。

[0103] 同步节点通过执行区块生成协议保持同步状态，基于随机可验证函数的区块生成协议包括候选者选举、候选区块生成与广播和领导者选举3个阶段。

[0104] 候选者选举的步骤为：

[0105] 1)共识节点nSyn读取链中的区块数据，根据区块中的交易数据信息计算所有节点的权益值S，然后生成包含所有节点权益份额W的权益份额表StakeTable。

[0106] 2)共识节点nSyn使用当前最新区块的随机数nonce和共识轮次r作为随机种子计算可验证随机数vrfNonce。

[0107] 3)共识节点根据生成的可验证随机数vrfNonce和自身权益份额W进行自我选举，即判断自身是否满足候选者条件，满足则成为候选者执行后续的候选区块生成流程，否则执行新区块生成流程。

[0108] 节点权益份额表生成流程为共识节点读取区块中所有有关节点权益信息的交易，计算出网络中每个节点的权益值和权益值总和，假设此次共识节点权益值总和为1000，其中一个共识节点权益值为100，那么该共识节点的权益份额为10％。自我选举条件为生成的可验证随机数是否处于随机数空间的某个区间，该区间取决于节点的权益份额，假设随机数空间为0到1000，那么节点生成的随机数只有小于等于100才能满足候选者条件。本发明方案通过将节点权益份额模拟成节点算力的方法，避免了算力消耗问题，而且通过可验证随机数保证共识的公平性与安全性。

[0109] 候选区块生成步骤为：

[0110] 1)候选者节点nCandi根据候选区块的所有交易生成区块头，生成区块主体时，对于已经广播的交易txBroaded，只放入其唯一标识ID，未广播的交易tx则放入完整数据。

[0111] 2)候选者将生成的候选区块bCandi、可验证随机数vrfNonce、随机数证明proof和验证公钥vrfVK打包为候选者信息广播到网络中的其他节点。

[0112] 领导者选举步骤为：

[0113] 1)共识节点nSyn对收到的候选者信息进行验证，先验证共识轮次、创世区块、随机种子等公共信息是否一致，然后使用验证公钥vrfVK验证随机数合法性，再验证候选者身份的合法性，即该候选者的随机数是否在随机数空间中的权益份额区间内，若都满足则加入候选池中，否则丢弃该候选信息。

[0114] 2)对于候选池中的候选信息，共识节点选择可验证随机数vrfNonce最小的那个候选者作为领导者，并使用其候选区块信息生成新区块，若候选池中没有候选信息，则此轮不生成新区块，然后开始下一轮共识。

[0115] 本发明的实施例提出了候选区块压缩方法，在区块生成时减小候选区块的尺寸，降低在分布式网络广播的通信消耗，能够通过降低共识时间来提高共识效率，从而提高协议系统性能的可扩展性。在区块链系统中，交易数据实际上被广播了2次，第一次是在交易广播阶段，交易被节点验证之后会被广播到网络中所有节点，第二次在区块广播阶段，领导者会将交易信息打包到区块主体，然后将区块广播到全网所有节点。在本实施例中，网络节点先验证收到交易的签名和合法性，通过后保存在交易缓存池中，通过广播接口转发的交易则标记为已广播交易，并保存在已广播交易缓存池中。打包区块时使用交易哈希替代候

选区块中已经广播的交易，交易的尺寸远小于区块，一般来说能比区块更快达到网络中其他节点。

[0116] 本发明的实施例描述了节点在共识网络注册时绑定的初始化权益值，到记录节点权益变化的交易都记录到区块中，再到权益成为区块进行候选者选举的评判标准，层层递进，权益成为整个共识系统的基础，也是整个共识系统的核心。而本发明的权益证明机制从以往激励机制的桎梏中脱离出来，实现了真正独立的权益证明机制，网络的扩展性和灵活性得到了很大的提高。

[0117] 使用权益份额和可验证随机数作为候选者的选举条件。利用区块记录节点权益变化使得其可靠性得到保障，可验证随机数计算非常简单，节点间验证也是简洁可靠高效的。该共识算法摒弃了现在主流的工作量证明机制过量的算力竞争，将达成共识的时间降低为通信网络的时延，节约了计算资源，还保留了验证快速高效、计算简单和通信量少的优点。

[0118] 本发明的实施例通过将权益证明机制和公有链系统相结合，通过权益机制、可验证随机数和链选择规则设计了一个共识方案，将权益证明机制的特点与公链共识结合起来，从而解决了现在公链共识存在的可扩展性和安全性等问题，将达成共识的竞争条件由工作量证明单纯的算力大小转换成节点权益值大小，不仅节约了算力资源，而且提供灵活的权益机制，能够支持更多应用场景另外保留了工作量证明的大部分优点。

[0119] 下面结合实验对本发明的技术效果作详细的描述。

[0120] 图6是系统性能仿真图，两种情况仿真结果汇总对比图，当区块尺寸一样，交易压缩比例为100％，75％，50％，区块广播到网络75％节点的系统TPS是普通PoS系统的8倍，2.9倍，1.8倍；广播到网络90％节点时也是一样的。另外，其他条件一样时，区块广播到网络90％节点比75％节点的系统TPS要低约24％。这只是存储普通交易的PoS系统的TPS表现，当交易尺寸远远大于交易标识时，系统的TPS提升会更加明显。

[0121] 应当注意，本发明的实施方式可以通过硬件、软件或者软件和硬件的结合来实现。硬件部分可以利用专用逻辑来实现；软件部分可以存储在存储器中，由适当的指令执行系统，例如微处理器或者专用设计硬件来执行。本领域的普通技术人员可以理解上述的设备和方法可以使用计算机可执行指令和/或包含在处理器控制代码中来实现，例如在诸如磁盘、CD或DVD-ROM的载体介质、诸如只读存储器(固件)的可编程的存储器或者诸如光学或电子信号载体的数据载体上提供了这样的代码。本发明的设备及其模块可以由诸如超大规模集成电路或门阵列、诸如逻辑芯片、晶体管等的半导体、或者诸如现场可编程门阵列、可编程逻辑设备等的可编程硬件设备的硬件电路实现，也可以用由各种类型的处理器执行的软件实现，也可以由上述硬件电路和软件的结合例如固件来实现。

[0122] 以上所述，仅为本发明的具体实施方式，但本发明的保护范围并不局限于此，任何熟悉本技术领域的技术人员在本发明揭露的技术范围内，凡在本发明的精神和原则之内所作的任何修改、等同替换和改进等，都应涵盖在本发明的保护范围之内。

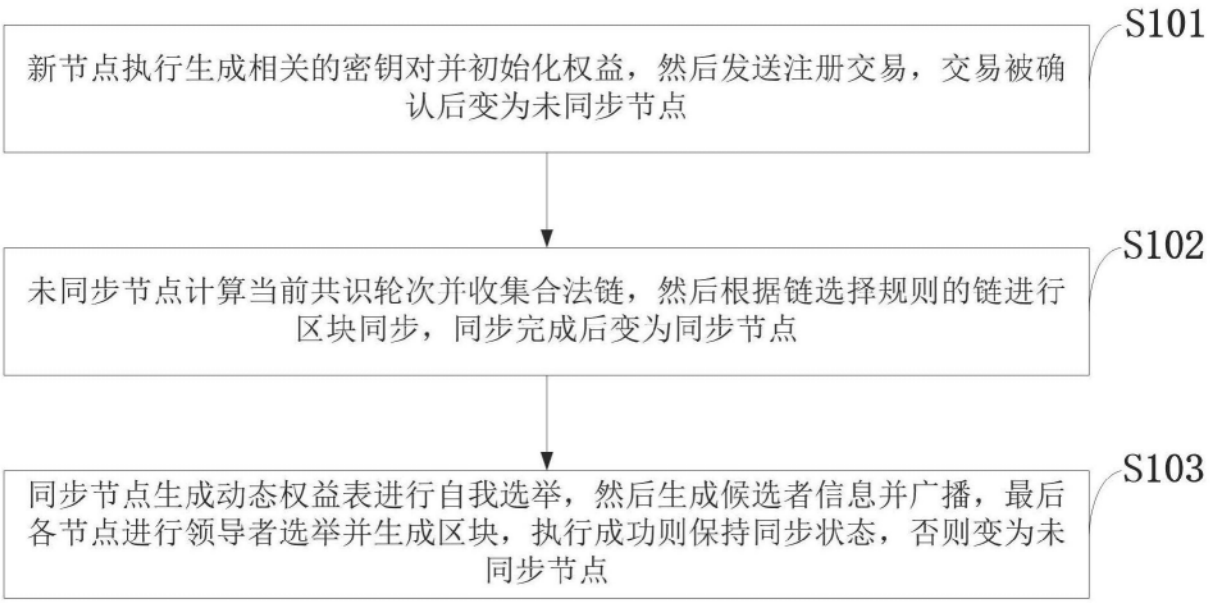

新节点执行生成相关的密钥对并初始化权益，然后发送注册交易，交易被确认后变为未同步节点
S101
未同步节点计算当前共识轮次并收集合法链，然后根据链选择规则的链进行区块同步，同步完成后变为同步节点
S102
同步节点生成动态权益表进行自我选举，然后生成候选者信息并广播，最后各节点进行领导者选举并生成区块，执行成功则保持同步状态，否则变为未同步节点
S103

图1

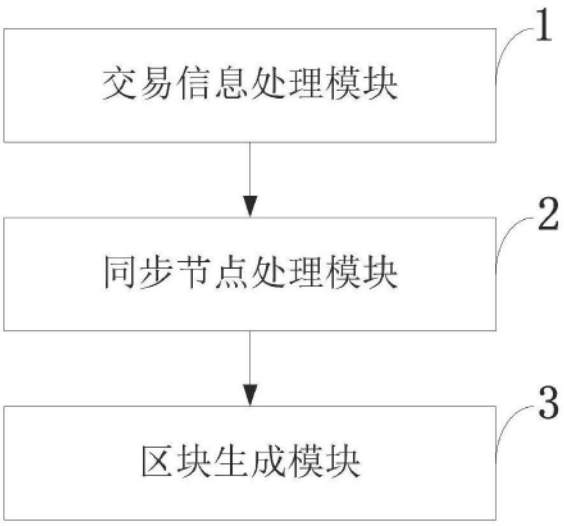

交易信息处理模块
1
同步节点处理模块
2
区块生成模块
3

图2

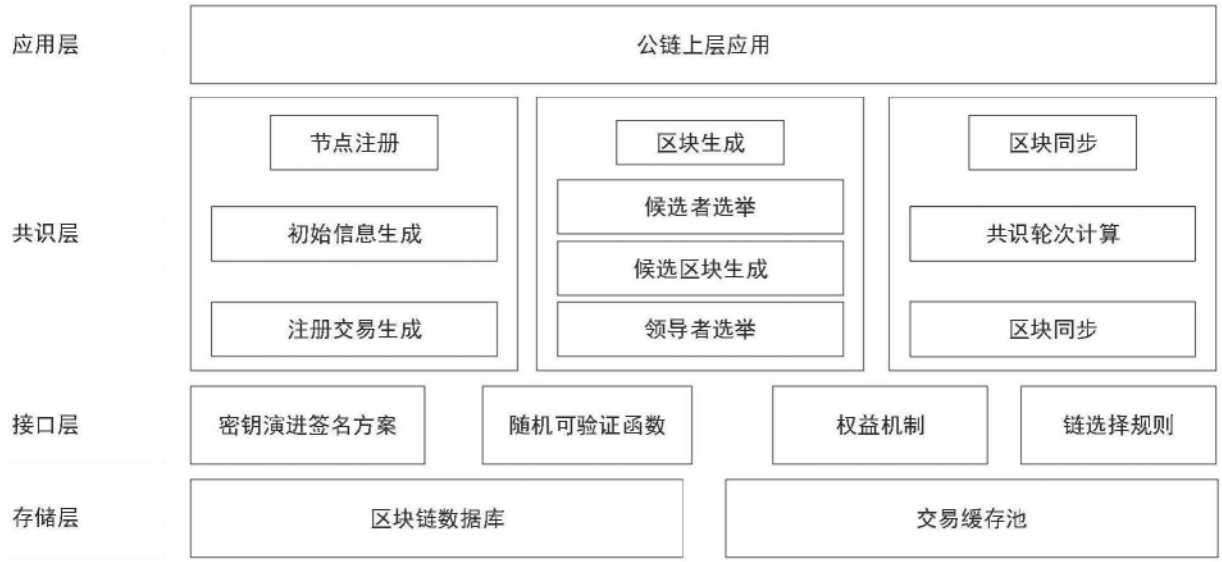

应用层
公链上层应用
共识层
节点注册
初始信息生成
注册交易生成
区块生成
候选者选举
候选区块生成
领导者选举
区块同步
共识轮次计算
区块同步
接口层
密钥演进签名方案
随机可验证函数
权益机制
链选择规则
存储层
区块链数据库
交易缓存池

图3

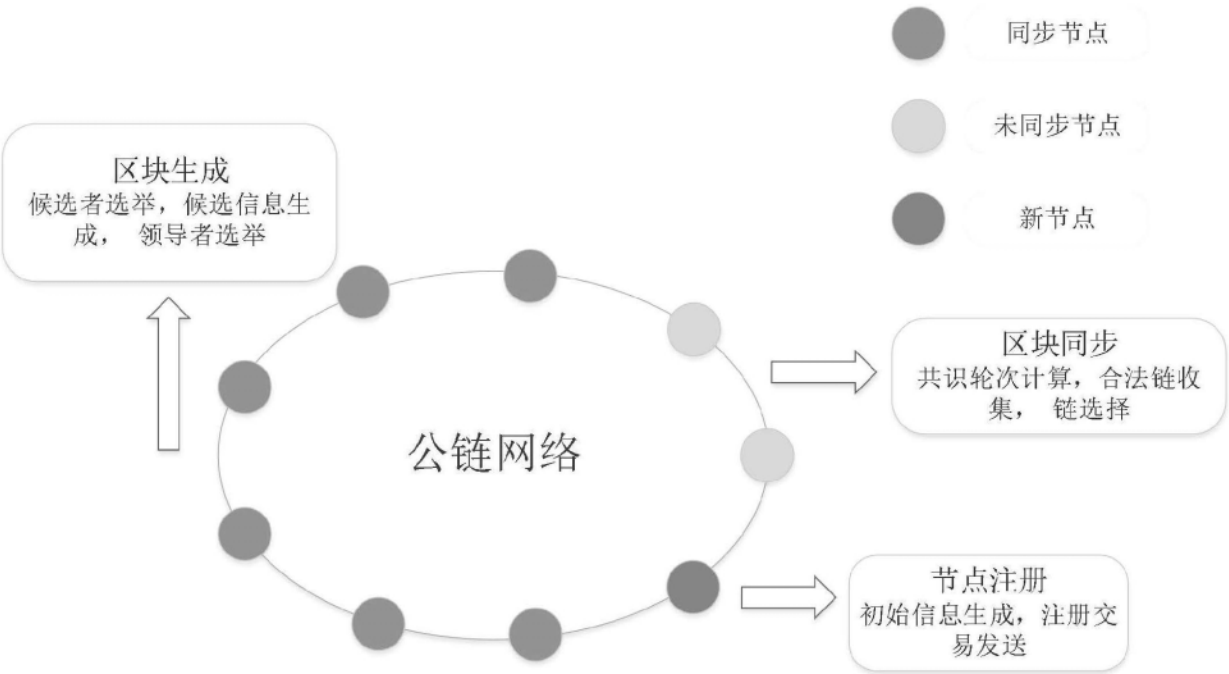

同步节点
未同步节点
新节点
区块生成
候选者选举，候选信息生成， 领导者选举
公链网络
区块同步
共识轮次计算，合法链收集， 链选择
节点注册
初始信息生成，注册交易发送

图4

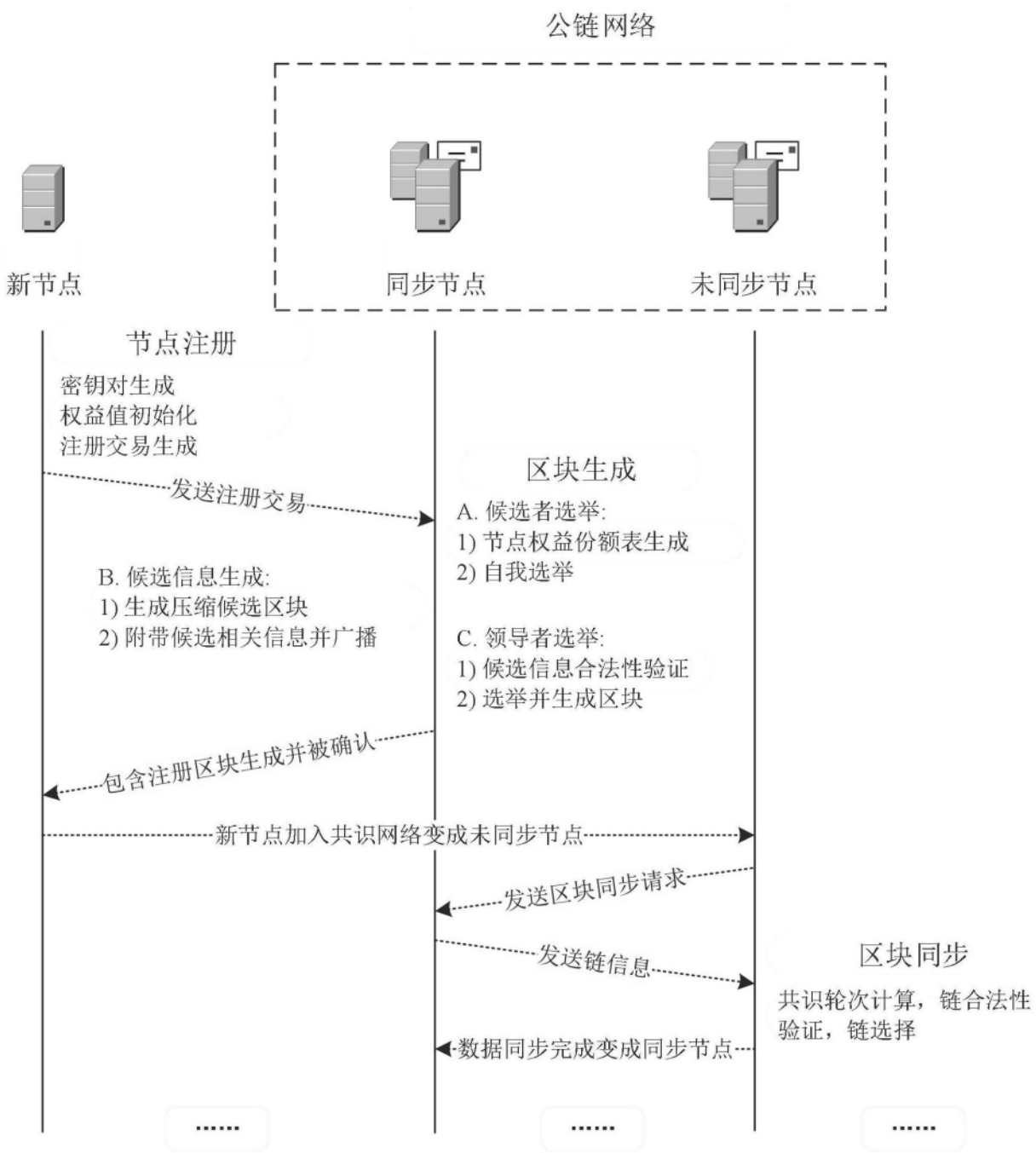

公链网络
新节点
同步节点
未同步节点
节点注册
密钥对生成
权益值初始化
注册交易生成
发送注册交易
区块生成
A. 候选者选举:
1) 节点权益份额表生成
2) 自我选举
B. 候选信息生成:
1) 生成压缩候选区块
2) 附带候选相关信息并广播
C. 领导者选举:
1) 候选信息合法性验证
2) 选举并生成区块
包含注册区块生成并被确认
新节点加入共识网络变成未同步节点
发送区块同步请求
发送链信息
区块同步
共识轮次计算，链合法性验证，链选择
数据同步完成变成同步节点
.....
.....
.....

图5

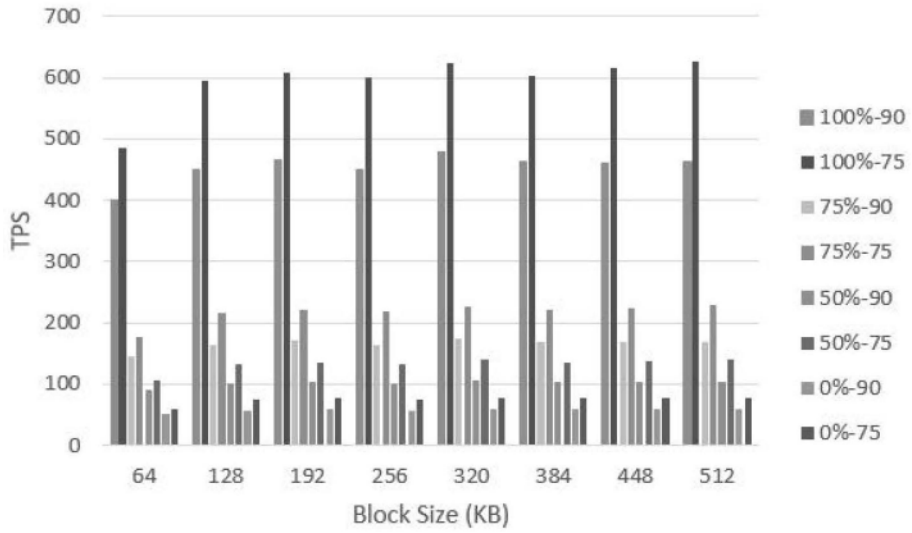

700
600
500
400
300
200
100
0
TPS
64
128
192
256
320
384
448
512
Block Size (KB)
100%-90
100%-75
75%-90
75%-75
50%-90
50%-75
0%-90
0%-75

图6