

## 基于区块链的高效能源交易共识与存储优化方法研究<sup>①</sup>

崔蔚<sup>②\*</sup> 于卓<sup>\*\*</sup> 王璇<sup>\*</sup> 吴晓亭<sup>\*\*</sup> 文治<sup>\*\*</sup> 张巧莲<sup>\*\*\*</sup> 沈韬<sup>③\*\*\*</sup>

(\* 国网信息通信产业集团有限公司 北京 100031)

(\*\* 北京中电普华信息技术有限公司 北京 100192)

(\*\*\* 昆明理工大学信息工程与自动化学院 昆明 650000)

**摘要** 随着能源互联网不断渗透,能源数据量与交易量呈指数型增长。为了进一步提升能源交易效率、降低能源数据存储压力、实现能源互联网跨企业之间的数据共享,本文利用区块链共识算法保证数据强一致性、存储安全等特点,提出一种改进的基于节点贡献度的实用拜占庭容错共识机制(NCPBFT),在保证节点可靠性、能源数据不可篡改的同时可降低通信复杂度,提升能源交易效率。其次,提出适用于能源互联网领域的联盟链数据分区存储优化策略,该策略基于节点的地理位置划分出的不同域组,每个域只有两种类型的节点:一个存储节点和若干个普通节点,只有存储节点保存区块链中全部数据,其余节点只需要保存区块头,进一步减轻区块链存储压力。通过实验验证了本文所提方案与现有方案相比能够有效提升能源交易效率,降低区块链存储压力。

**关键词** 能源互联网; 区块链; 数据共享; 区块链共识; 数据存储

### 0 引言

在能源转型和电力体制改革的新形势下,我国能源互联网体系呈现出新的发展态势。以绿色新能源为主体的分布式能源已然成为能源交易市场中的重要组成部分,为降低通信复杂度、提高能源利用率、多渠道扩展分布式能源就地消纳,分布式能源获得合法就近售电资质,其能源生产和消费结构呈无中心、多节点状特点。

现有能源运营模式由于具有集中式管理的特点且依赖于第三方机构,其交易流程多、电力损耗大、效率低、时间长、交易成本高。由于区块链技术和分布式能源交易在理念上的相似性,基于区块链的能源交易已成为众多专家学者的研究热点。

### 1 相关研究

文献[1]重点研究了基于拜占庭式区块链共识框架下电动汽车与配电网分布式网络(distribution network, DN)之间的能源交易过程。文献[2]使用区块链技术来管理分布式能源交易的系统运行。文献[3]提出了一种基于软件定义网络(software defined networking, SDN)的区块链能源互联网分布式能源交易方案。该方案在保护隐私的前提下实现了交易对象的合理匹配。为了应对当前电动汽车集成量大的现状,文献[4]提出了点对点电力区块链交易(peer-to-peer electricity blockchain trading, P2PEBT)的效益证明(proof of benefit, PoB)共识机制,通过在新型区块链系统中提供平衡本地电力需求的激励机制来实现需求响应。文献[5]提出了一

① 国网信通产业集团两级协同研发项目(SGIT0000XMJS2000538)资助。

② 男,1987年生,硕士,高级工程师;研究方向:区块链,人工智能;E-mail: abcui@qq.com。

③ 通信作者,E-mail: shentao@kmust.edu.cn。

(收稿日期:2021-07-16)

个区块链平台的通用框架,该平台支持零售电力市场的点对点(peer-to-peer, P2P)能源交易,从供需双方寻找能源匹配对,鼓励生产者和消费者直接进行能源交易,实现了一个完整的能源交易流程。针对联盟区块链不能智能地选举实时交易的领导者、不能满足数据交易平台稳定性要求的问题,文献[6]提出了一种联盟区块链动态领导者的选择方法。基于Hyperledger Fabric的共识协议,将计算每个对方用户得分的交易评估模块引入联盟区块链。文献[7]提出了一种基于分层模型的多中心的共识机制,与其他共识机制不同的是,该文设计了主从链,用以提高区块链系统的吞吐量。文献[8]提出了一种新的协商一致协议——委托式拜占庭容错协议(credit-delegated Byzantine fault tolerance, CDBFT),并提出了一种投票奖惩方案及其相应的信用评估方

案和基于实用拜占庭容错(practical Byzantine fault tolerance, PBFT)的一致性和检查点协议。文献[9]提出一种基于动态信誉值的实用拜占庭容错(dynamic-reputation practical Byzantine fault tolerance, DPBFT)共识算法。文献[10]提出一种基于分片的共识算法。文献[11]提出了基于跳跃 Hash 和动态权重分片构建算法,同时引入异步共识组机制,提升分片的交易安全性,有效处理跨分片交易。文献[12]针对区块链系统中节点诚信问题,对于 PBFT 的节点划分阶段进行优化,利用聚类算法根据节点类型进行划分,提高了区块链系统中的节点质量,进而降低了故障概率。文献[13]针对能源领域提出一种基于区块链技术的分布式能源信息互通互联模式,优化了 RAFT 算法来满足电力数据上链实时性的要求。表 1 为主流共识算法的对比分析。

表 1 主流共识机制对比

	优势	劣势	目的
工作量证明 (proof of work, POW)	容忍 51% 以下的攻击、完全去中心化	算力浪费、依赖代币、吞吐量低	第一代区块链共识算法
股权证明 (proof of stake, PoS)	算力资源消耗略少、区块生成速度稍快	依赖代币、易于拆分、吞吐量低	降低资源消耗,提高效率
委托股权证明 (delegated proof of stake, DPoS)	不完全去中心化、算力资源消耗略少	依赖代币、吞吐量低	解决 PoW 和 PoS 资源消耗和效率问题
实用拜占庭容错 (practical Byzantine fault tolerance, PBFT)	不依赖代币、算力资源消耗略少	仅容忍 1/3 的恶意节点、吞吐量不高	解决拜占庭问题
Raft	不依赖代币、算力资源消耗略少	不能容忍恶意节点、吞吐量不高	解决节点保持一致性问题

随着能源工业互联网发展的不断渗透,能源数据量与交易量呈指数型增长。为了缓解区块链系统带来的存储压力,众多学者专家对区块链中的区块存储方案进行优化。区块存储优化方案主要是在不影响交易吞吐量的情况下改变区块的存储方式。链下存储优化方案是一种将区块体中数据内容从原区块体转移到链下存储系统,区块体中仅存储指向这些数据的“指针”和其他非数据信息,以解决区块链存储可扩展性问题的方法。星际文件系统(interplanetary file system, IPFS)是一种旨在将所有计算设备与相同文件系统连接起来的点对点分布式文件系统<sup>[14]</sup>,IPFS 是内容寻址的,即内容本身决定了内

容的位置<sup>[15]</sup>,是目前作为区块链链下存储中使用较多的一种方案。文献[16]针对物联网数据隐私问题提出了一种基于区块链和 IPFS 的“模块化联盟架构”,既克服了传统区块链网络无法存储海量数据的缺点,又消除了物联网(Internet of Thing, IoT)数据的中心化管理模式。Desema<sup>[17]</sup>是一个基于 Ethereum 和 IPFS 的分布式服务市场系统。在 Desema 中,服务的元数据和大型数据都存储在 IPFS 中,而区块链中仅存储这些数据的散列值。Chameleon<sup>[18]</sup>是一个动态适应、可扩展的私有链架构。它将最近一段时期(一天或者一周)的数据存储在区块链中,以前的数据存储到云上。分布式哈希表

(distributed hash table, DHT)<sup>[19]</sup>是一种分布式存储方法。DHT 在不需要中心服务器的情况下,每个节点负责一个小范围内的路由,同时存储一小部分数据,从而实现 DHT 网络的寻址和存储。文献[20]改变了传统区块链网络(例如比特币)存储所有交易的存储模式,将数据与数据引用进行分离式存储,设计了一种使用 DHT 的链下存储模式,其中,DHT 由 Kademlia<sup>[21]</sup>实现。原始数据的引用(即原始数据 SHA-256 计算后的散列值)保存在区块链中,而原始数据则保存在链下的 DHT 中。

以上述可知,现存的共识机制如 POW、POS 共识机制均存在参与的节点数目较多、共识时间较长以及效率低的问题,且大多用于公有链中。同样现有大多数区块链链下存储优化方案均是基于公有链或私有链,在联盟链中的存储优化方案较少。因此,本文针对区块链在能源交易过程中存在的交易效率与存储容量问题,提出基于节点贡献度的实用拜占庭容错共识算法和位置分区的联盟链存储优化策略。共识算法保证加入联盟链中节点的可靠性与能源交易数据的不可篡改。存储策略基于节点的地理位置划分出的不同域组,每个域之间功能与地位都相同。功能上,每个域只有两种类型的节点:一个存储节点和若干个普通节点,只有存储节点保存区块链中全部数据,其余节点只需要保存区块头,以此减轻区块链的存储压力。

## 2 基于节点贡献度的实用拜占庭容错共识机制(NCPBFT)

区块链本质上是一个全网节点共同参与记账的分布式数据库,而共识机制是其中的核心要素,能够确保全网节点保存在区块链上的数据是一致的。现存的共识机制如 POW、POS 共识机制基本用于公有链中,参与的节点数目较多,共识时间较长、效率低。而在能源互联网场景中,为了满足能源快速交易的需求,本文基于联盟链节点准入准出机制,提出了一种基于节点贡献度的实用拜占庭容错(node-based contribution practical Byzantine fault tolerance, NCPBFT)共识算法。该算法将网络中的参与节点分为具有不

同职责的4种类型,分别为主节点、监控节点、共识节点和存储节点。共识节点以及存储节点是由监控节点根据其自身的贡献度进行动态更新,然后主节点从贡献度较高的那一半共识节点中随机选出,并根据节点贡献度对节点进行降序排序及动态变更。在 PBFT 共识机制中,共识的通信复杂度为  $O(n^2)$  级别。若系统中的节点数较多,则通信压力会较大,为了缓解通信压力,本文使用简化的共识过程,将共识的通信复杂度减少为  $O(n)$ 。

### 2.1 网络结构

在 NCPBFT 中,节点主要分为监控节点、主节点、共识节点和存储节点几种类型。

监控节点:(1)监控全网中节点的共识行为及该节点接入网络的具体时间;(2)根据节点贡献度对共识节点和存储节点进行动态变更;(3)选取主节点;(4)验证节点同步性。

主节点:(1)接收客户端发送的交易,对交易进行排序;(2)打包交易生成预备消息,并向其他共识节点广播;(3)统计共识节点发送的反馈消息,生成准备消息并广播给其他共识节点以及存储节点;(4)维护区块链账本。

共识节点(consensus node, CN):(1)对主节点发送的预准备消息进行验证,然后生成反馈消息返回给主节点;(2)接收准备消息并将其写入到区块链账本,然后返回确认消息给主节点。

存储节点(storage node, SN):不参与共识过程,只将正式区块存储到区块链账本。

在该算法中共识节点的数量为  $n$ ,其中主节点是在贡献度较高的共识节点中随机选择,存储节点的数量为  $k$ ,监控节点的数量为 1。假设网络中的恶意节点数量为  $f$ ,则恶意节点和共识节点仍满足  $f \leq (n-1)/3$ 。

由图 1 所示,在 NCPBFT 中,只有共识节点才能参与共识过程进行投票和验证等过程,将高耗性能操作与共识操作分开执行能在一定程度上加快共识过程,提升业务操作区块的生成速度,进而达到用户与应用交互的需求。同时,共识过程通过主节点确认区块合法性,降低原始 PBFT 的通信复杂度,也缩短了共识周期所需的时间,进而提高共识效率。

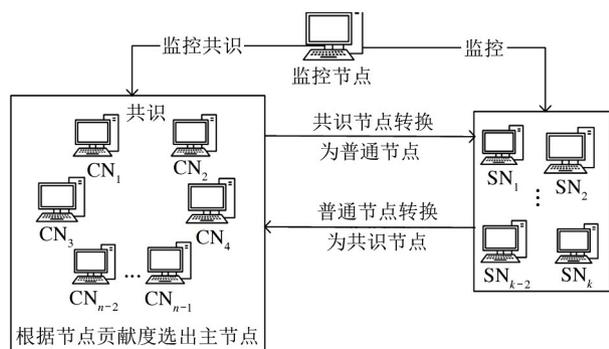


图1 NCPBFT 共识网络结构图

### 2.2 NCPBFT 共识协议

PBFT 算法中共识过程主要分为预准备、准备、确认以及回复这几个阶段。其中在准备阶段和确认阶段的通信量较多。在准备阶段,除主节点外的各共识节点会将准备消息向其他共识节点进行广播,在确认阶段各共识节点会将确认消息向其他的共识节点进行广播,PBFT 算法的通信复杂度为  $O(n^2)$  级别。参与共识的节点数量越多,则共识的效率将越低,针对该问题本文提出简化的一致性协议,由主节点对交易进行排序打包生成预准备消息广播给各共识节点,共识节点对其进行验证然后将结果返回给主节点,然后由主节点生成准备消息广播给共识节点以及存储节点进行验证保存,共识节点以及存储节点返回确认消息给主节点,NCPBFT 通信复杂度将降为  $O(n)$ 。

图2中PBFT算法在预准备阶段、准备阶段、接受阶段的通信消耗量比较多。假设共识节点数量为  $n$ , 预准备阶段的通信消耗量为  $n - 1$ , 准备阶段的通信消耗量为  $(n - 1)^2$ , 接受阶段的通信消耗量为  $n(n - 1)$ , 所以这几个阶段的总消耗量为  $T = 2n(n - 1)$ 。

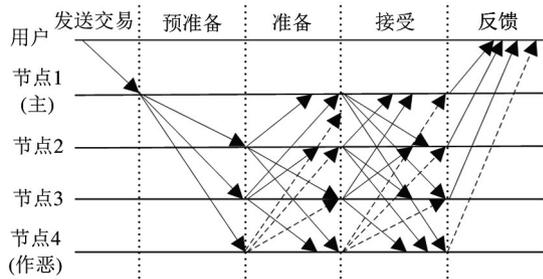


图2 PBFT 协议过程图

图3所示NCPBFT中,假设共识节点数量为  $n$ , 存储节点数量为  $k$ , 预准备阶段的通信消耗量为  $n - 1$ , 反馈阶段的通信消耗量为  $n - 1$ , 准备阶段的通信消耗量为  $n + k - 1$ , 接受阶段的通信消耗量为  $n + k - 1$ , 所以这几个阶段的总消耗量为  $T = 4n + 2k - 4$ 。

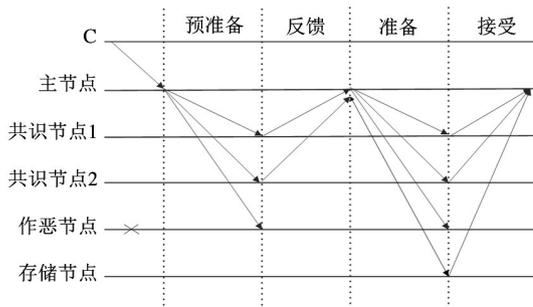


图3 NCPBFT 协议过程图

所以相较于PBFT算法,NCPBFT的通信复杂度降为  $O(n)$ , 基于节点贡献度机制的拜占庭容错共识算法在参与节点较多并处理能源互联网中大量能源交易时有更高的效率。

### 2.3 共识过程

节点共识过程如图4所示。

如图4所示,在预准备阶段,主节点对交易进行打包生成预准备消息的条件有:设置预准备消息包含的交易最大数量  $Th_{tx}$ , 当交易池里的交易量  $\sum TX$  超过所设置的预准备消息包含的交易最大数量阈值时,主节点会对最早的一批交易进行打包;设置两个区块生成的最大时间间隔为  $Th_{btime}$ , 当前区块时间戳  $T_k$  减去前一区块时间戳  $T_{k-1}$  所获得值大于等于所设置的  $Th_{btime}$  时,即使交易池里的交易数量低于预准备消息包含的交易最大数量,主节点也会对交易进行打包,生成预备区块。公式表示如下:

$$\begin{cases} Th_{btime} \geq T_k - T_{k-1} \\ \sum TX \geq Th_{tx} \end{cases} \quad (1)$$

在反馈阶段,会设置主节点接收各共识节点返回消息的定时器,当主节点接收到所有共识节点返回的反馈消息时,会生成正式区块;当定时结束,主节点统计返回的反馈消息数量,当数量大于等于  $2\lfloor \frac{n-1}{3} + 1 \rfloor$  ( $n$  为共识节点数),则会生成准备消息。公式表示为

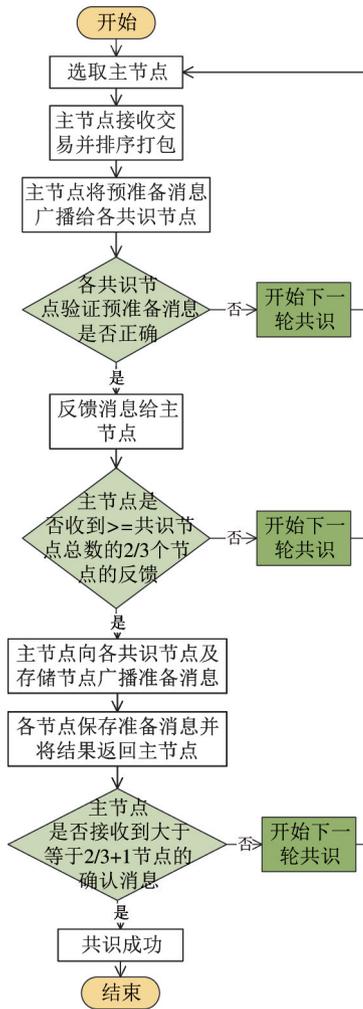


图4 共识流程图

$$\begin{cases} V_{\text{Total}} = n & \text{定时未结束} \\ V_{\text{Total}} \geq 2 \lfloor \frac{n-1}{3} + 1 \rfloor & \text{定时结束} \end{cases} \quad (2)$$

### 2.4 节点贡献度的计算

如图5所示,监控节点根据各节点在共识过程中的表现,对各节点的贡献度进行相应的更新,然后根据贡献度对节点进行类别更新。计算节点的贡献度以及更新节点类型方法如下所述。

对于新加入系统的节点给予其初始值:  $C_{\text{init}} = 0.5$ 。节点贡献值,即根据各节点共识行为来进行计算:

$$T_n = \exp\{[(\sum_{x=1}^n s(x) - \vartheta \times \sum_{x=1}^n f(x)) - (\alpha \times \sum_{x=1}^n z(x) + \beta \times \sum_{x=1}^n d(x))] / (n-1)\} \quad (3)$$

其中  $\sum_{x=1}^n s(x)$  代表在以往的共识过程中节点成

功共识的次数;  $\sum_{x=1}^n f(x)$  表示在以往的共识过程中节点共识失败的次数;  $\vartheta$  代表共识节点共识失败的惩罚因子;  $\sum_{x=1}^n z(x)$  表示在以往的共识过程中节点作为主节点成功的次数;  $\alpha$  表示主节点共识成功的消耗因子,降低主节点一直为一个节点的可能性;  $\sum_{x=1}^n d(x)$  表示在以往的共识过程中节点作为主节点失败的次数;  $\beta$  表示主节点共识失败的惩罚因子。其中,  $\vartheta$ 、 $\alpha$ 、 $\beta$  的值可根据实际情况进行调整。

根据各节点连续参与网络的时间计算网络稳定值为

$$P_n = \frac{2}{1 + \exp(- (t_{\text{now}} - t_{\text{start}}))} \quad (4)$$

其中  $t_{\text{now}}$  表示现在的时间值,  $t_{\text{start}}$  表示节点接入网络的时间。

最终节点的贡献度为

$$C_{\text{final}} = C_{\text{init}} + \lambda T_n + (1 - \lambda) P_n \quad (5)$$

其中  $\lambda$  为调节参数,可调整节点贡献值和网络稳定值所占的比重。而当节点为恶意节点则将节点贡献度设为0,并将其剔除系统。

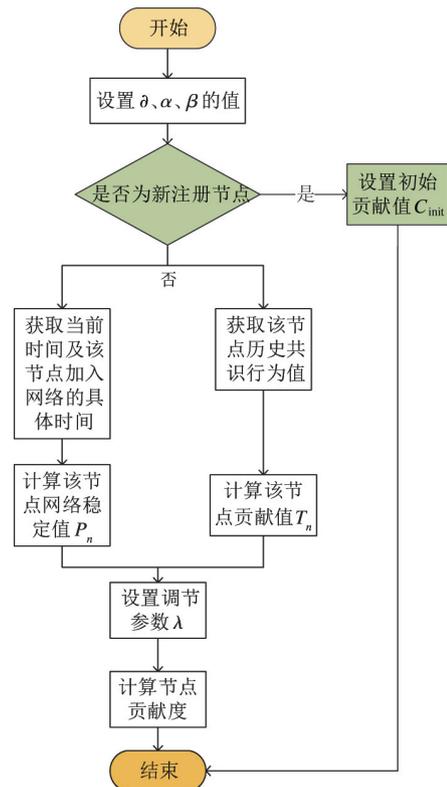


图5 节点贡献度计算流程图

则各节点的贡献度为

$$C = \begin{cases} C_{init} & \text{节点为新注册节点} \\ C_{final} & \text{节点为非作恶节点} \\ 0 & \text{节点为作恶节点} \end{cases} \quad (6)$$

### 3 基于位置分区的联盟链存储优化原理

#### 3.1 存储优化模型

在该模型中,节点分为监控节点、存储节点两类。其中存储节点根据性能评价指标分为存储节点和普通存储节点。该优化模型根据不同的位置划分节点域,不同域间通过存储节点进行关联。存储优化模型如图6所示。每个域内都会有一个存储节点和若干普通存储节点,正常情况下每隔时间  $t$  监控节点会根据性能评价指标选择出性能最好的节点作为存储节点,其余节点均作为普通存储节点;同时为确保系统正常运行,所有的存储节点要求定时发送心跳到监控节点并由监控节点进行监督,一旦发现存在状态异常的节点,由监控节点负责计算各节点的性能评价指标值并选出状态良好的节点作为该异常节点的替代。在存储数据的过程中存储节点会分别负责不同的模块,普通存储节点只负责存储区块链数据较少的区块头,并形成区块头链;而存储节点负责存储整条区块链生成的区块数据。为降低域与域间由于距离引起的通信时延,当有新的节点想要加入到该区块链系统时,通过该节点给出的位置信息将其分配到离它最近的节点域。

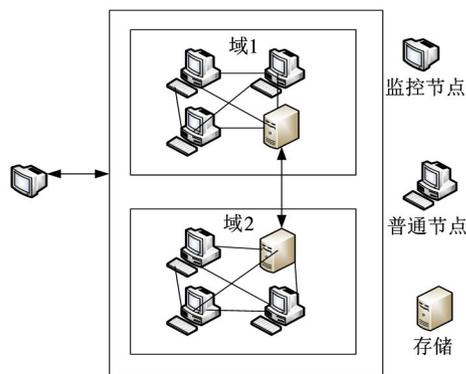


图6 存储优化模型示意图

#### 3.2 数据存储过程

本文提出的联盟链存储优化策略的数据存储过

程如图7所示。在一个域内,正常情况下的具体流程如下。

**步骤1** 某个节点接收到能源交易的数据时,首先对自身身份作出判断,即是否为普通存储节点。若该节点为存储节点而非普通存储节点,可以直接对交易数据进行投票验证其合法性;反之,则需要将该交易数据广播到全网直至有存储节点接收到转发的信息。

**步骤2** 存储节点接收到该交易数据后,首先通过投票验证该交易数据的合法性。同时为了避免不必要的带宽开销,该存储节点只将验证合格的交易广播到其他存储节点。

**步骤3** 存储节点打包验证合格的交易形成区块,并开始参与共识。

**步骤4** 存储节点向系统模型发送存储数据的请求,存储共识生成的区块,并向全网广播区块头的信息。

**步骤5** 普通节点接收区块头数据并存储。

**步骤6** 结束。

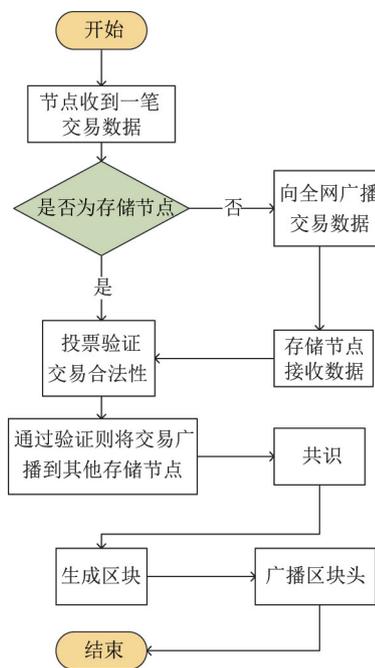


图7 存储过程

#### 3.3 交易验证

只有在保存完整交易数据的节点上才能进行相应的交易验证。该模型中,每个节点域都存在一个保存完整区块数据的存储节点,普通存储节点若想

进行交易验证,则需要和存储节点合作才能获取相应的验证结果。验证过程中,一旦存储节点表现异常,无法与普通存储节点合作验证,则需要请求监控节点获取到网络中其他存储节点的节点列表并选出若干个存储节点完成该交易的验证。交易验证的步骤如图 8 所示。

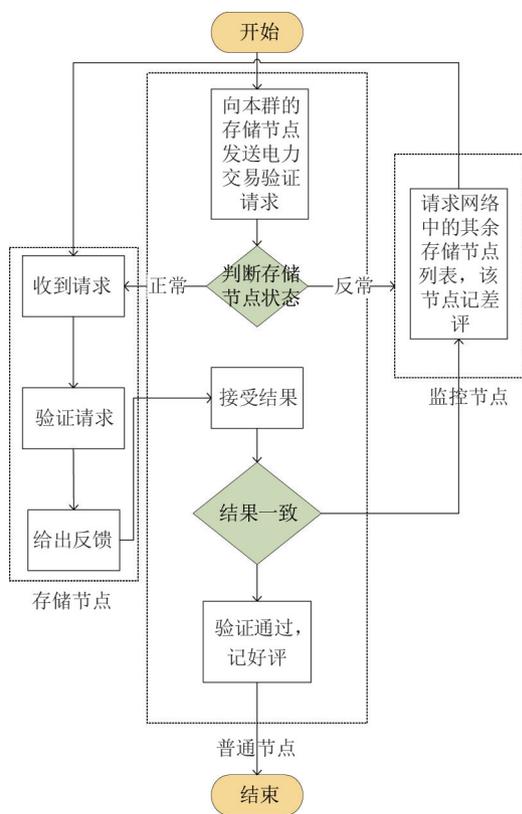


图 8 验证过程

具体的交易验证过程如下。

**步骤 1** 普通存储节点想要验证某条交易信息,首先需要向该节点所在节点域中的存储节点发送验证请求,并对该节点状态进行判断。若节点状态正常,存储节点会对收到的验证请求进行验证处理并将带有数字签名的处理结果反馈给普通存储节点;反之,普通存储节点要继续请求网络中的其他类似的存储节点进行验证,并对当前存储节点作差评处理并记录。

**步骤 2** 普通存储节点接收验证结果。

**步骤 3** 普通存储节点对验证结果进行一致性判断,若结果一致则通过验证并对该存储节点作良好评价,最后将评价结果回馈给监控节点;反之,认

为返回验证结果的存储节点状态异常,需给予该节点差评处理并将评价结果回馈到监控节点并请求选择新的存储节点进行验证操作。

**步骤 4** 结束。

## 4 实验部分

### 4.1 实验环境设置

该存储优化方法的共识模块选择采用第 2 节提到的 NCPBFT 算法,存储模块应用本文第 3 节所提出的优化方案。使用本地数据库提供外部服务,如交易数据和块查询。系统底层仍采用区块链技术架构体系、椭圆曲线密码(ECC)非对称加密算法等以保证系统安全性。模拟实验在 CPU 为 Intel Xeon Processor 的服务器上进行,运用 Openstack 虚拟出 17 个节点的 ubuntu18.04 系统,每个节点的硬件配置为 CPU 频率为 2.4 GHz,内存大小为 2 GB,存储容量为 20 GB。划分一个监控节点和 4 个域,每个域 4 个节点。选用 Hyperledge Fabric 0.6 在相同的环境下做对比实验。

### 4.2 安全性分析

本次实验共识模块采用 NCPBFT 算法,一种改进的 PBFT 算法,虽然只有部分节点参与共识过程,但同样满足恶意节点数量不超过总共识节点数量的 1/3 时整个共识过程将顺利进行,进而能够有效降低通信复杂度、提高共识效率;同时采用基于位置分区的联盟链存储优化策略,保证只有性能评价好的节点即存储节点存储整个区块信息,其余普通存储节点只负责存储区块链头信息。在降低存储压力的同时,进一步降低了恶意节点入侵造成重大损失的几率。

### 4.3 结果及分析

#### 4.3.1 节点共识性能测试

由于共识算法性能差异,为验证 NCPBFT 的有效性,通过发送 1000 条能源交易数据,4 个节点对生成连续 20 个区块进行测试。从图 9 可以看出,与其他几种经典共识算法如 PBFT、PoS-PBFT、RAFT 等相比,本文所提 NCPBFT 吞吐量的平均值有了明显提升,整个交易处理过程花费时间较少。这主要

是由于 NCPBFT 优化了主节点选取过程,降低了共识算法通信复杂度。

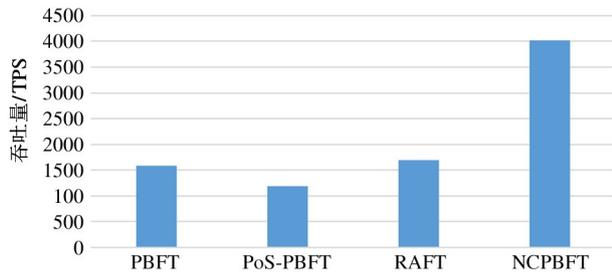


图 9 经典共识算法吞吐量比较

当参与共识的节点数为 4 的时候,分别选择包含 50、100、200、300、500、700、1000、1500、2000、2500、3000 等交易量的区块大小,针对本文所提出的算法 NCPBFT 及传统 PBFT 算法的时延、吞吐量进行相应的实验分析。具体实验结果如图 10 和图 11 所示。

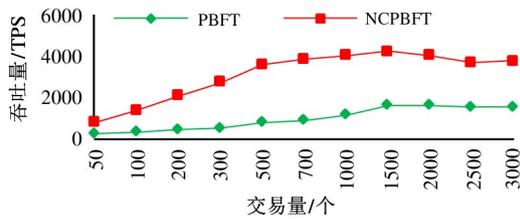


图 10 区块大小不同时传统 PBFT 及 NCPBFT 中吞吐量对比图

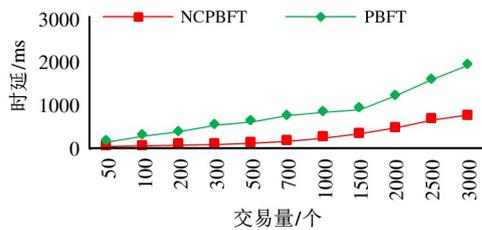
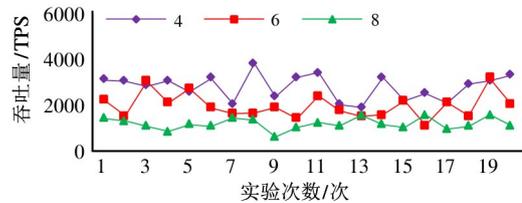


图 11 区块大小变化时传统 PBFT 及 NCPBFT 算法时延对比图

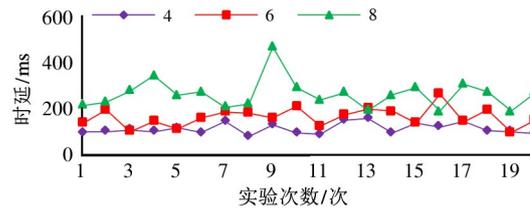
由图 10、11 可以看出,本文方案相较于 PBFT 算法有着较高的吞吐量和较低的时延,两个方案中吞吐量在开始时会随着区块内交易数量的增多而升高,但在区块的大小到达某一值之后其吞吐量则增长缓慢甚至会降低。而时延是随着区块的增大而不断在增大的。所以区块的大小要选择一个最适值来

获得最佳的性能。总体来说,本文方案较 PBFT 算法的性能更优。

接下来在区块大小为 300,共识节点数为 4 个、6 个、8 个时,分别给出了 NCPBFT 共识算法在 20 次实验中吞吐量和时延的变化值,结果如图 12 所示。



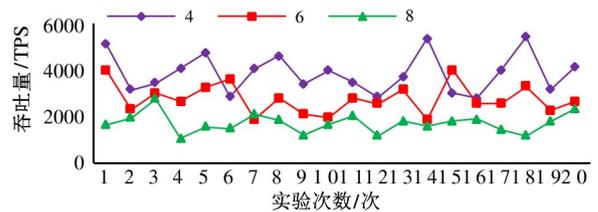
(a) NCPBFT 吞吐量



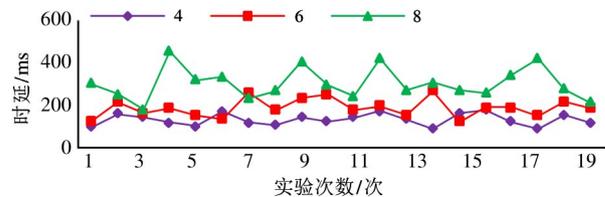
(b) NCPBFT 时延

图 12 NCPBFT 算法区块大小为 300 时不同共识节点数下的性能

在区块大小为 500,共识节点数分别为 4 个、6 个、8 个时,NCPBFT 算法在 20 次实验中的吞吐量和时延的变化值如图 13 所示。



(a) NCPBFT 吞吐量



(b) NCPBFT 时延

图 13 NCPBFT 算法区块大小为 500 时不同共识节点数下的性能

图12和图13是基于NCPBFT共识算法,在不同的共识节点情况下,在多次实验中吞吐量和时延的变化,由图可以看出在区块大小固定不变时,共识节点数越多,其吞吐量会降低,而时延会增高。这是因为节点数增加了,各节点的通信次数就会增加,所以时延会增大,吞吐量则会减小。

#### 4.3.2 存储开销测试

网络中全部节点正常工作且不受攻击时,比较在本文及Fabric存储策略下每个区块存储500、1000、2000、3000个区块数据的存储开销,其结果如图14所示。

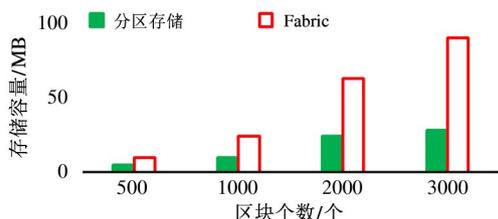


图14 文中策略与Fabric存储占比对比图

通过分析图14的实验结果,可以得出如下结论。

(1) 当整个区块链中只生成少量区块时,本文所提出的存储优化策略较Fabric存储而言其优势不是很明显,但当交易量的增多导致区块链中区块逐渐增多时,本文提出的存储策略所要占用的存储空间比Fabric的要小很多。

(2) 交易量增多导致区块链中区块逐渐增多的情况下,本文所提存储方案的存储占用增长速率要远远低于Fabric存储。

Fabric内的每个节点都存储完整的区块数据,而本文所提存储方案中每个节点域只有存储节点才会存储完整的区块数据,在普通存储节点内部只对区块链中的每个区块的区块头进行相应的存储;当区块数逐渐增大时,本文方案的优势更加明显,与Fabric相比存储占用虽然也在逐渐增加,但其增长速度明显变缓。此次实验结果证明了本文所提策略的有效性。

#### 4.3.3 交易验证测试

交易验证过程中,区块链系统对验证请求的响应时间对当次交易验证能否有合理的反馈结果起着

至关重要的作用,此次验证主要以不同节点对相同交易验证请求进行处理的时间为基准进行验证测试。假设区块链系统中节点运行状态正常,选择存储节点、普通存储节点、Fabric中的节点,比较同一节点在查询验证500、1000、2000、3000条交易所需的验证时间。具体结果如图15所示。

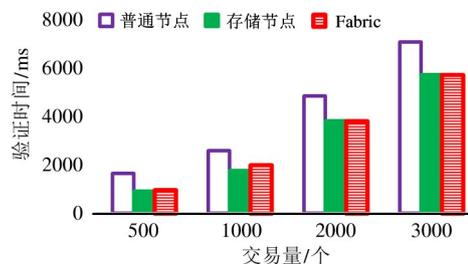


图15 交易验证对比图

根据图15结果,可得出以下结论。

(1) 查询的交易数量相同的情况下,普通存储节点、存储节点和Fabric节点的查询验证时间均会随着数据量的增大而变长。

(2) 查询的交易数量相同的情况下,在存储节点上和Fabric节点上查询验证的时间几乎一致。

(3) 查询的交易数量相同的情况下,在普通存储节点上进行查询验证的时间要远远高于在存储节点和在Fabric节点上的时间。

基于分区的存储优化策略下,区块数据分别由存储节点和普通存储节点进行存储,其中只有存储节点才有权存储完整的区块信息,普通存储节点只负责区块头信息的存储。由普通节点发起的验证请求要通过进一步转发给存储节点才能进行交易的验证,故而查询会稍慢一些。Fabric的所有节点均存有区块的完整数据,故而查询验证Fabric节点的时间与查询验证存储节点的时间相差无几。综上所述,尽管普通存储节点查询验证时间的会稍长,但并不影响整个区块链能源交易系统的正常运行。

## 5 结论

为了提升能源互联网中能源交易效率、降低通信复杂度及能源数据的存储压力、实现能源互联网跨企业之间的数据共享,本文基于区块链共识算法、

存储策略等技术,提出了一种改进的基于节点贡献度的实用拜占庭容错共识机制。根据节点贡献值计算并进行共识节点的选取,保证节点进入区块链网络的可靠性、能源数据的不可篡改性的同时降低通信复杂度、提升能源交易效率;在联盟链数据分区存储节点存储优化策略中,基于存储节点的地理位置划分出的不同域组,每个域只有一个存储节点和若干个普通存储节点,只有存储节点保存区块链中全部数据,其余节点只需要保存区块头,进一步减轻区块链存储压力。通过实验验证了本文所提方案能够有效提升能源交易效率、降低通信复杂度及区块链存储压力。

#### 参考文献

- [ 1 ] SHEIKH A, KAMUNI V, UROOJ A, et al. Secured energy trading using byzantine-based blockchain consensus [J]. *IEEE Access*, 2019(8): 8554-8571
- [ 2 ] WANG S, TAHA A F, WANG J, et al. Energy crowdsourcing and peer-to-peer energy trading in blockchain-enabled smart grids [J]. *IEEE Transactions on Systems, Man, and Cybernetics: Systems*, 2019, 49(8): 1612-1623
- [ 3 ] LU X, SHI L, CHEN Z, et al. Blockchain-based distributed energy trading in energy Internet: an SDN approach [J]. *IEEE Access*, 2019, 7: 173817-173826
- [ 4 ] LIU C, CHAI K K, ZHANG X, et al. Peer-to-peer electricity trading system: smart contracts based proof-of-benefit consensus protocol [J]. *Wireless Networks*, 2021, 27(6): 4217-4228
- [ 5 ] HAN D, ZHANG C, PINGJ, et al. Smart contract architecture for decentralized energy trading and management based on blockchains [J]. *Energy*, 2020, 199: 117417
- [ 6 ] WANG X, FENG Q, CHAI J. The research of consortium blockchain dynamic consensus based on data transaction evaluation [C] // 2018 11th IEEE International Symposium on Computational Intelligence and Design (ISCID), Hangzhou, China, 2018, 2: 214-217
- [ 7 ] 闵新平, 李庆忠, 孔兰菊, 等. 许可链多中心动态共识机制 [J]. *计算机学报*, 2018, 41(5): 1005-1020
- [ 8 ] WANG Y, CAI S, LIN C, et al. Study of blockchains' s consensus mechanism based on credit [J]. *IEEE Access*, 2019(7): 10224-10231
- [ 9 ] CAI W J, JIANG W, XIE K, et al. Dynamic reputation-based consensus mechanism: real-time transactions for energy blockchain [J]. *International Journal of Distributed Sensor Networks*, 2020, 16(3): 1-13
- [ 10 ] HU M, SHEN T, MEN J, et al. CRSM: an effective blockchain consensus resource slicing model for real-time distributed energy trading [J]. *IEEE Access*, 2020(8): 206876-206887
- [ 11 ] 潘吉飞, 黄德才. 基于跳跃 Hash 和异步共识组的区块链动态分片模型 [J]. *计算机科学*, 2020, 47(3): 273-280
- [ 12 ] 陈子豪, 李强. 基于 K-medoids 的改进 PBFT 共识机制 [J]. *计算机科学*, 2019, 46(12): 101-107
- [ 13 ] 方响, 马笛, 侯伟宏, 等. 分布式新能源接入下的区块链共识机制研究 [J]. *浙江电力*, 2019, 38(7): 1-6
- [ 14 ] BENET J. IPFS-content addressed, versioned, P2P file system (DRAFT 3) [EB/OL]. <https://arxiv.org/pdf/1407.3561.pdf>; arXiv, [2014-07-14], (2021-07-16)
- [ 15 ] HASAN S S, SULTAN N H, BARBHUIYA F A. Cloud data provenance using IPFS and blockchain technology [C] // Proceedings of the 7th International Workshop on Security in Cloud Computing, Auckland, New Zealand, 2019: 5-12
- [ 16 ] ALI M S, DOLUI K, ANTONELLI F. IoT data privacy via blockchains and IPFS [C] // Proceedings of the 7th International Conference on the Internet of Things, Linz, Austria, 2017: 1-7
- [ 17 ] KLEMS M, EBERHARDT J, TAI S, et al. Trustless intermediation in blockchain-based decentralized service marketplaces [C] // International Conference on Service-Oriented Computing, Malaga, Spain, 2017: 731-739
- [ 18 ] HE G, SU W, GAO S. Chameleon: a scalable and adaptive permissioned blockchain architecture [C] // 2018 1st IEEE International Conference on Hot Information-Centric Networking (HotICN), Shenzhen, China, 2018: 87-93
- [ 19 ] ANDROUTSELLIS-THEOTOKIS S, SPINELLIS D. A survey of peer-to-peer content distribution technologies [J]. *ACM Computing Surveys*, 2004, 36(4): 335-371
- [ 20 ] ZYSKIND G, NATHAN O. Decentralizing privacy: using blockchain to protect personal data [C] // 2015 IEEE Security and Privacy Workshops, San Jose, USA, 2015: 180-184
- [ 21 ] MAYMOUNKOV P, MAZIERES D. Kademlia: a peer-to-peer information system based on the xor metric [C] // In-

ternational Workshop on Peer-to-Peer Systems, Cambridge, USA, 2002: 53-65

## Research on efficient energy transaction consensus and storage optimization method based on blockchain

CUI Wei<sup>\*</sup>, YU Zhuo<sup>\*\*</sup>, WANG Xuan<sup>\*</sup>, WU Xiaoting<sup>\*\*</sup>, WEN Zhi<sup>\*\*</sup>, ZHANG Qiaolian<sup>\*\*\*</sup>, SHEN Tao<sup>\*\*\*</sup>

(<sup>\*</sup> State Grid Information & Telecommunication Group Co., Ltd., Beijing 100031)

(<sup>\*\*</sup> Beijing Zhongdian Puhua Information Technology Company, Beijing 100192)

(<sup>\*\*\*</sup> Faculty of Information Engineering and Automation, Kunming University of Science and Technology, Kunming 650000)

### Abstract

With an improved practical byzantine fault tolerant consensus mechanism based on nodes' contribution of the energy Internet, the amount of energy data and transaction volume has increased exponentially. In order to further improve the efficiency of energy transactions, reduce the pressure of energy data storage, and realize data sharing between the energy Internet across enterprises, this paper uses the blockchain consensus algorithm to ensure strong data consistency and storage security, and proposes an improved node-based contribution practical Byzantine fault-tolerant (NCPBFT) consensus mechanism, which reduces communication complexity and improves energy transaction efficiency while ensuring node reliability and energy data cannot be tampered with. Then the data partition based storage optimization strategy for the alliance chain is proposed for the energy Internet field. This strategy is based on different domain groups divided by the geographical location of the nodes. Each domain has only two types of nodes: a storage node and several ordinary nodes. Only the storage node saves all the data in the blockchain, and the remaining nodes only need to save the block header, further reducing the storage pressure of the blockchain. It is verified through experiments that the scheme proposed in this article can effectively improve the efficiency of energy transactions and reduce the pressure of blockchain storage compared with the existing schemes.

**Key words:** energy Internet, blockchain, data sharing, blockchain consensus, data storage