

[电力用户]

对用电信息保护的拜占庭容错联盟链共识算法

文/国网新疆电力有限公司昌吉供电公司 张维忠 徐步尘
北京智芯微电子科技有限公司 高飞

针对用电信息保护的需要，利用区块链技术进行加密，本文基于信用模型的拜占庭容错联盟链共识算法和神经网络构建用电用户节点信用模型。在采用信用模型的基础上，对实用拜占庭容错算法进行了改进，提出了一种基于信用模型的拜占庭容错共识算法。

智能电网以自动化的方式来保证电网的高效性、可靠性和经济性，从而优化电网的管理和运营。随着智能测量技术的成熟和应用，更加准确、便捷及经济的电力抄表和实时监测抄表大大提高了抄表效率，使得电力公司能更加科学、快速地调整电力供应，解决了供电量与耗电量之间的供求均衡问题，在满足电力用户基本用电需求的同时，可有效地避免过量发电造成的浪费。

随着通信技术的发展，通信技术与智能电网的紧密结合，使得基于电网的双向通信成为可能。在用户和电网之间扮演重要角色的智能电表，就成了双向通信和给用户交互体验的直接终端。智能电表收集智能设备的用电信息，当用电量发生变化时，实时上传用电量、时间等信息到电力公司，电力公司进行用电量分配和预测。智能电表依赖于智能测量技术，随着智能测量技术的成熟应用，更加准确、便捷和经济的电力抄表和实时监测抄表大大提高了抄表效率，使得电力公司能更加科学、快速地调整电力供应，解决了供电量与耗电量之间的供求均衡问题，在满足电力用户基本用电的同时，可有效地避免多余发电。但是频繁的用电数据上传会给用户带来

个人隐私泄露的严重问题。在用电数据上传过程中，用电量和用电时间等数据可反映出用户的用电习惯等隐私信息。智能电表上传的数据也可能被不法者利用，可能导致用户用电信息、个人敏感信息及涉及商业机密信息被泄露以及被篡改，造成用户或电力公司的损失，从而给用户和电力公司带来威胁。

在智能电表环境中的三类主要隐私数据包括：用于对家庭或者用户进行唯一标识的智能电表的身份信息；用于实时向电力公司上传的用户用电量信息，即智能电表实时电量数据；还需要定期上传的用户总的用电量信息，即智能电表总电量数据。不法者获取了智能电表的唯一标识以及该智能电表实时上传的用户用电量数据后，就可以对用户进行攻击。对于智能电网中用户的用电信息保护的研究，还处在起步阶段。

区块链作为一项新兴技术，是由分布式系统、共识算法、密码学和点对点网络等多种技术深度融合实现的去中心化的分布式账本技术，提供了一个在去信任化的环境中进行信息价值传递的可信通道。联盟区块链简称联盟链，面向特定群体，只有经过授权的节点才可

以加入特定的区块链网络。联盟链中的节点需要事先认证注册，共识过程中通常不涉及加密，成员节点间有共同的目标，但在维护交易数据等方面并不完全信任彼此。相对于共有链，联盟链节点间通常有着良好的连接、较高的验证和确认速度、更快的出块时间及较低成本的系统维护费用。结合区块链的最新技术发展，联盟链可实现内部成员共同负责账本维护，同时注册机制可限制参与节点的行为，提供灵活的权限处理能力，在一定程度上构建出一个去中心、分布式的体系，摆脱了由唯一中心机构带来的单点故障等安全隐患，解决了节点之间的信任问题，可适用于当前金融、供应链和公益等应用场景，特别是在智能电网的用电信息隐私保护中具有非常重要的实践意义。而共识算法作为联盟链中的关键技术，直接影响着联盟链的交易处理能力、可扩展性和安全性，本文提出一种面向用电信息保护的基于信用模型的拜占庭容错联盟链共识算法。该算法基于BP（Back Propagation）神经网络构建节点信用模型，在采用信用模型的基础上，对PBFT（Practical Byzantine Fault Tolerance）进行了改进，提出了一种面向用电信息保护的联盟链CBFT（Credit-based Byzantine Fault Tolerance）算法。

联盟链共识算法

共识问题一直是分布式领域的重要研究课题，根据选取区块记账节点方式的不同，大致可以将共识算法分为以下四类。包括证明类共识算法：工作量证明（Proof of Work, PoW）和股权证明（Proof of Stake, PoS）；广播选举类共识算法：Raft算法；轮流类共识算法：PBFT；混合类共识算法：PoS + BFT。PoW等算法具有能源浪费严重、吞吐量低和交易时延长等问题，而PBFT算法作为拜占庭容错算法经典的实现，对联盟链具有重要意义，是联盟链共识算法的核心支撑，许多联盟链共识算法受其启发，针对特定场景进行了改进。

Miguel Castro和Barbara Liskov在1999年提出PBFT算法，可以在保证活性和安全性的前提下提供1/3的容错性，将BFT算法复杂度由指数级降低到多项式级，使得BFT算法在实际系统应用中变得可行。随后在此经典的PBFT算法基础上，研究者又做了大量的改进工作，主

要包括以Query/Update和Hybrid/Quorum为典型的基于Quorum的算法，以Zyzava为典型的基于Speculation方法的算法，以及以OBFT（Obfuscated BFT）为典型的基于客户端的算法等，以上算法都是在不同侧重点上针对没有错误的场景为简化PBFT算法而设计。因此，当遇到拜占庭错误时，这类算法的性能一般会有不同程度的下降，甚至很难保证系统的活性。

此外，PBFT算法基于状态机复制（State Machine Replication）原理，主要由一致性协议、视图切换协议和检查点协议组成，在正常情况下系统运行在一致性协议和检查点协议下，当主节点出错时，视图切换协议才会启动，以保证系统有序执行客户端请求。这是针对典型分布式数据库的场景，请求以很高频率输入系统，系统可能在1 s内进行上千次共识过程，一旦发生了超时，系统中的从节点会认为主节点是拜占庭节点。因此在该场景中，必须通过Commit阶段来提高共识效率。但是在联盟链系统中，通常是几分钟甚至更长时间共识一个区块，如果区块存在问题就直接共识一个区块体为空的默认区块，而不是回滚，所以并不需要Commit阶段。另外，在PBFT算法中，主节点的更换是轮流产生的，这样是有风险的，如果接连的几个当选为主节点的副本节点都是拜占庭的，那么就会大大降低系统的可用性。

技术方案

1. BP神经网络构建区块链节点信用模型

改变主节点选举方式，PBFT算法采用轮流当选主节点的方式，这种方式使得恶意主节点当选后引起视图更换，从而导致系统性能大大降低。因此，本文提出一种基于信用的主节点选举方法，基于BP神经网络构建区块链节点信用模型，选出最高信用的节点当选主节点，从而降低了拜占庭节点为主节点的概率，使得视图更换次数大大减少，系统性能得到提升。

BP神经网络是一类基于误差反向传播算法的多层神经网络，可以灵活地对样本数据建模并揭示其中隐含的非线性关系，适用于构建节点信用评估模型。本文采用的信用模型评估体系根据节点在共识过程中的诚信水平和性能表现，设计了8个评估指标，将其作为BP神经网络的输入，具体如下表所示。

表 节点评估指标

序号	指标	指标解释
1	网络延时时间	节点网络延时的时间
2	节点离线次数	区块链系统的节点的离线次数
3	节点离线时间	记录节点离线的次数
4	未参与上链次数	在线从节点因为拜占庭节点等原因未能参与新区块上链更新的次数
5	新区块上链时间	这一轮每次新区块验证、执行到上链时间的平均值
6	节点加入网络时间	节点参与系统的时间
7	是否提供无效区块	主节点是拜占庭节点可能提供无效区块
8	节点信用值	上一轮中节点的信用值

在节点信用评估要素中,包含了网络延时时间、节点离线时间、未参与上链次数、节点离线次数、新区块上链时间、节点加入网络时间、是否提供无效区块和节点信用值等离散数据,本算法所采用的数据均为非负数,但是因为各评估指标量纲差距大,需要对样本数据进行归一化处理,使其映射到[0, 1]区间,再作为BP神经网络模型的输入。

本算法设计的信用模型中输入层包括8个神经元,输入分别代表网络延时时间、节点离线次数、节点离线时间、未参与上链次数、新区块上链时间、节点加入网络时间、是否提供无效区块和节点信用值;输出层包含1个神经元;隐藏层设计为1层,隐藏层神经元个数一般靠经验法或试错法来选取。

2. CBFT算法流程

交易请求发送阶段:交易发起者C向全网广播交易,并附上发送者的签名,所有共识节点均独立监听全网的交易数据,验证交易的合法性,若合法则缓存起来;主节点收集到足够的交易请求或到一定的时间间隔以后,将这些请求打包成区块。

提案阶段:主节点将新生成的区块生成一个提案消息并签名,消息格式为<PROPOSE, v , n , p , $D(\text{block})$ > σ_p 。 v 为视图编号, n 为区块请求的编号, p 为主节点序号,需要共识的区块经过哈希变换后记为摘要 $D(\text{block})$ 。从节点在接收到新区块提案后,需要对提案合法性进行校验。当发现非法交易、无效区块时,将这种“不诚实行为”记录到节点状态记录表,放弃本次共识并发起视图更换协议;而当从节点经过验证并确认主节点发来的提案信息正确之后,则进入确认阶段。

确认阶段:从节点进入确认阶段之后,向其他从节点广播发送<CONFIRM, v , n , p , $D(\text{block})$ > σ_i 消息。 i 为节点自身序号,同时接收其他节点发来的确认消息。检查消息签名、摘要和视图编号是否正确等,如果都通过,就缓存下

来,当从节点接收到超过来自 $2f+1$ 不同节点的一致信息后,该节点进入确认阶段,执行此区块交易,并回复<REPLY, v , t , n , c , i , r > σ_i 消息给客户端。其中 t 是时间戳, n 是区块号, c 是客户端, i 是节点 i 的编号, r 是节点 i 的回复, σ_i 是节点 i 对消息的签名。

当客户端收到超过 $f+1$ 个节点的回复消息,并且他们的回复拥有相同的时间戳 t 和回复 r 后,共识即达成,各节点执行区块上链。

3. 改进视图更换协议

当从节点发现检测到超时或者主节点有错误时,向区块链系统网络内所有节点广播视图变更消息,视图更换消息格式为(VIEW-CHANGE, $v+1$, L , Q , i) σ_i 。 L 为按照节点信用排名表选出的下一个信用值最高的节点的序号, Q 存储了节点 i 在之前视图中所有已完成PROPOSE的请求集合信息。

节点收到VIEW-CHANGE消息后,校验消息的签名、视图、新的主节点序号 L 、 Q 集合信息等是否合法,都合法时则向新的主节点发送(VIEW-CHANGE-ACK, $v+1$, i , j , d) σ_i ,如果新的主节点收到了 $2f+1$ 个VIEW-CHANGE报文,则会由其选出最近的checkpoint,根据 Q 集合计算区块请求对应的序号 n ,最后封装到(VIEW-CHANGE-ACK, $v+1$, V , X) σ_p 消息中去并广播。其中 V 包含了其他从节点发来的VIEW-CHANGE消息和相对应的VIEW-CHANGE-ACK的消息集合, X 标识了所选的检查点和请求值。

从节点收到视图 $v+1$ 新主节点发来的new-view消息后,校验消息签名以及是否重复处理过该报文,重新根据 V 集合和 X 集合,为每个序号 n 赋值区块摘要,同时验证自己分配的结果跟主节点发送的NEWVIEW报文中的分配结果是否一致(验证消息摘要),一致时则同步当前节点的数据状态到checkpoint的时间点位置,然后遍历 X 集

合生成报文信息。

后续共识就是经典PBFT算法的共识处理流程。

仿真验证

1. 吞吐量测试

此共识算法主要针对联盟链，因此采用Hyperledger Fabric作为区块链框架，采用CBFT算法作为其共识算法，并将该系统与采用PBFT共识算法的Hyperledger Fabric v0.6开源框架进行比较。

交易吞吐量是指区块链网络在定义的时间内提交有效交易的速率。它以每秒交易数

$$TPS = \frac{T_{\Delta t}}{\Delta t} \quad (1)$$

式中， $T_{\Delta t}$ 为出块时间内的交易总量； Δt 为出块时间。

对在模型的仿真实验分析中，考虑单点的测量数据。区块容量大小会影响吞吐量，区块越大需要的网络带宽越大，时延相应也会增加，因此为了控制变量便于对照，将一个区块中MaxMessages项设置为20。分别测试了在4、5和6个共识节点下，CBFT共识算法与PBFT共识算法的三组对照实验。多次测试取平均值，得出统计结果，如图1所示。

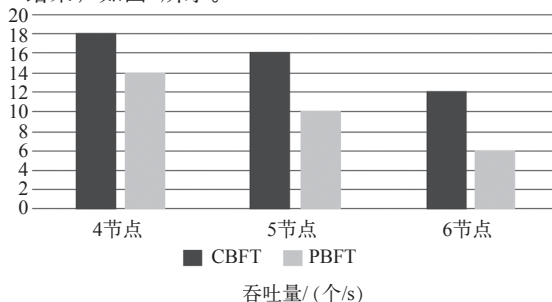


图1 CBFT算法与PBFT算法吞吐量测试

由图1可以看出，随着节点数增加，CBFT和PBFT这两种算法的吞吐量都随之减少，但是CBFT的吞吐量更高，而且随节点数增加吞吐量减少速度比PBFT小。这是因为信用模型的采用减少了视图更换的次数，因此操作回滚等引起的带宽消耗和时延减少，区块链系统的吞吐量增加。

2. 时延测试

区块链系统中的时延测试通常指的是一笔交易从提出到确认提交的时间间隔，在本文的性能测试中，为了与PBFT的性能作比较，将其简化为共识时延测试，即区块提案广播到区块共识完成

的时间，共识时延是测量共识算法运行速度的重要指标，时延越小，交易越快得到确认。

$$T_{\text{delay}} = T_{\text{conform}} - T_{\text{propose}} \quad (2)$$

式中， T_{conform} 为区块共识完成时间； T_{propose} 为主节点开始广播提案时间。

多次测试取平均值，得到CBFT共识算法与PBFT共识算法的共识时延对比统计结果，如图2所示。

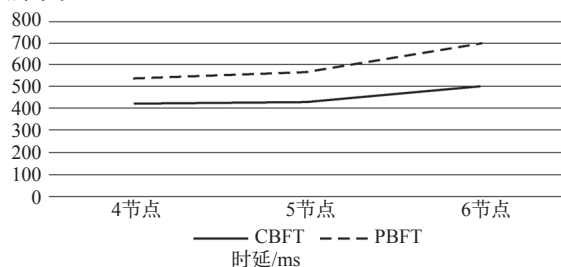


图2 CBFT算法和PBFT算法共识时延对比

由图2可以得出，因为信用模型的采用，视图更换的次数减少，因此其引起的操作回滚等操作减少，从而减少区块链系统的带宽消耗并降低系统时延。

3. 安全性分析

实验表明，CBFT共识算法在经典PBFT算法基础上减少了通信开销，增加了吞吐量，在减少了区块共识时延的基础上，保证了区块链这一分布式系统的一致性和安全性，并且与PBFT算法一样提供 $f = \frac{n-1}{3}$ 的容错性。

测试结果表明，在CBFT算法共识过程中，若系统中拜占庭节点个数少于1/3，主节点传播恶意请求或者主节点宕机的情况下，系统发生视图变更重新选择下一个信用值最大的节点，仍可以保证系统安全性和活性的前提下完成共识；而当超过1/3的情况时，则超出了系统所能承受的最大拜占庭节点数量，无法完成共识。

结束语

在PBFT算法的一致性协议和视图更换协议的基础上改进共识算法，本文提出了一种基于模型的拜占庭容错CBFT共识算法。由于采用基于节点信用模型，可以大大减少视图更换次数，因此一致性协议省略PBFT的commit阶段，大大减少了节点通信量，减少了区块确认时间，加快了交易确认速度。EA

(收稿日期：2019.11.19)

(编辑：朱金凤)