DOI:10.7544/issn1000-1239.2019.20190053
56(12):2671-2683,2019

基于门限密码方案的共识机制

王 缵[1,2,4] 田有亮[1,2,4] 岳朝跃[1,3,4] 张 铎[1,2,3,4]
[1](贵州省公共大数据重点实验室(贵州大学) 贵阳 550025)
[2](贵州大学计算机科学与技术学院 贵阳 550025)
[3](贵州大学数学与统计学院 贵阳 550025)
[4](贵州大学密码学与数据安全研究所 贵阳 550025)
(vinheres@163.com)

Consensus Mechanism Based on Threshold Cryptography Scheme

Wang Zuan[1,2,4], Tian Youliang[1,2,4], Yue Chaoyue[1,3,4], and Zhang Duo[1,2,3,4]
[1](*Guizhou Provincial Key Laboratory of Public Big Data* (*Guizhou University*), *Guiyang* 550025)
[2](*College of Computer Science & Technology*, *Guizhou University*, *Guiyang* 550025)
[3](*College of Mathematics and Statistics*, *Guizhou University*, *Guiyang* 550025)
[4](*Institute of Cryptography & Data Security*, *Guizhou University*, *Guiyang* 550025)

Abstract Aiming at the huge resource consumption, the bottleneck of the system performance and "tragedy of the commons" in the PoW(proof of work) consensus mechanism of bitcoin, we analyze the "tragedy of the commons" caused by only transaction fees rewarding in the later stage of the bitcoin system from the perspective of game theory and propose a consensus mechanism based on threshold cryptography (TCCM) in this paper. Firstly, the new consensus protocol introduces the idea of margin, and proposes a margin model based on threshold group signature theory. The model not only ensures the security of the margin, but also provides a guarantee for the node to honestly produce the block. Secondly, a bidding model of the right of accounting is also constructed using the idea of threshold encryption to generate a node that can produce the block. This model can guarantee the fairness of the bidding model environment and select the accounting node randomly. Then, a new incentive mechanism is redesigned based on the original block rewards so that more nodes can participate in the consensus process. Finally, the results of security and performance analysis show that TCCM not only effectively reduces the huge resource consumption, but also improves the transaction processing efficiency and makes the whole blockchain system more secure.

Key words blockchain; PoW consensus mechanism; tragedy of the commons; threshold cryptography; margin model

收稿日期:2019-01-23;**修回日期**:2019-08-12

基金项目:国家自然科学基金项目(U1836205, 61662009, 61772008);贵州省教育厅科技拔尖人才基金项目(黔教合 KY 字[2016]060);贵州省科技重大专项计划项目(20183001);贵州省科技计划项目(黔科合平台人才[2017]5788);教育部-中国移动科研基金项目(MCM20170401);贵州大学培育项目(黔科合平台人才[2017]5788);贵州省科技计划项目(黔科合基础[2019]1098);贵州省科学技术基金项目(黔科合 J 字[2008]2121)

This work was supported by the National Natural Science Foundation of China (U1836205, 61662009, 61772008), the Topnotch Talent in Science and Technology Support Program of Guizhou Province Education Department ([2016] 060), the Science and Technology Major Support Program of Guizhou Province (20183001), the Guizhou Provincial Science and Technology Plan Project ([2017]5788), the Ministry of Education-China Mobile Research Fund Project (MCM20170401), the Guizhou University Cultivation Project ([2017]5788), the Science and the Technology Program of Guizhou Province ([2019]1098), and the Science and Technology Foundation of Guizhou Province ([2008]2121).

通信作者:田有亮(youliangtian@163.com)

摘 要 针对比特币的PoW(proof of work)共识机制中资源消耗巨大、系统性能存在瓶颈和“公地悲剧”问题,从博弈论的角度分析了比特币系统后期只有交易费奖励所带来的“公地悲剧”现象,提出了基于门限密码方案的共识机制(a consensus mechanism based on threshold cryptography, TCCM).首先,新共识协议引入了节点保证金的思想,提出了一种基于门限群签名理论的保证金模型.该模型既能够确保保证金的安全,又为节点诚实地记账提供保障.其次,利用门限加密的思想构造了记账权竞价模型来产生区块链记账节点,这能够保证记账权竞价环境的公平性和记账节点产生的随机性.同时,在原有的区块奖励基础上,设计了新的激励机制,使得更多的节点能够参与共识的全过程.最后,安全性和性能分析结果表明,该共识机制既有效地降低了资源消耗,又提高了交易处理效率,使得整个区块链系统变得更加安全可靠.

关键词 区块链;PoW 共识机制;公地悲剧;门限密码;保证金模型

中图法分类号 TP309

近年来,随着比特币等虚拟货币持续火爆,区块链技术的研究呈现出井喷式增长态势,被誉为未来10年内最有可能提高人类社会生成力的新科技之一.2008年比特币电子现金系统被提出[1],实现了真正意义上的去中心化可信任的P2P自组织网络[2]交易平台.在该文献中,区块链被描述为用于记录比特币交易的一种分布式账本技术[3].该技术利用数字签名技术实现点对点的交易,通过对交易和时间戳等信息进行随机Hash,并将Hash结果利用工作量证明机制(proof of work, PoW)写入一个可以无限延伸的链式数据结构中,并通过发放代币(比特币)来激励全网节点共同维护区块链系统.但是区块链的应用不仅仅局限于比特币等电子货币系统[4],现在人们在隐私保护[5]、物联网[6]、供应链[7]、医疗健康[8]等众多领域不断进行区块链应用场景的研究与应用开发.

区块链是一种分布式的系统,系统中的所有节点共同保障该系统的正常运行.在这种分布式系统中,区块链为解决网络延时、传输错误、去中心化导致的数据分歧(拜占庭节点)等问题,需要一种共识机制来使各个节点达成共识,保证数据的最终一致性,其主要思想是解决区块链分布式账本的一致性和记账权问题,其目标是使所有的诚实节点保存一致的区块链账本.由此可见,共识机制是区块链技术的核心所在.

“共识机制”一词近几年被频繁使用,其名主要由工作量证明机制而得来.随着对分布式账本一致性问题的不断探索,很多算法被提出来,其中有很多算法回归了对传统分布式一致性算法的改进,其在算法思路上已经跳出了“证明”的语义,故可以进一步概括为共识机制.因此,可以将共识机制研究热点概括为2个方向:传统分布式一致性算法的改进算法和证明机制算法.如Paxos和Raft算法就是传统分布式一致性算法的代表,它们一般不能直接作为区块链的共识机制使用[9],这是由于其假设系统中每个节点都是诚实的、不作恶的,而实际的去中心化的区块链网络中,节点之间互不了解、互不信任,存在欺骗和作恶的可能.而在这种情况下,不得不提到适用于联盟链的BPFT(practical Byzantine fault tolerance)算法[10],它可以在拜占庭节点数不超过全网节点数量1/3的情况下保障数据的一致性,但是其效率与参与共识的节点数量相关,并不适用于节点数量过多的公有区块链系统,并不具备良好的扩展性;另一类是证明机制算法,如基于工作量证明的PoW共识算法[11-12],严重浪费资源(电力消耗),且长达10 min的交易确认时间使其不适用于中小额交易的场景;基于权益证明的PoS(proof of stake)共识算法,在2012年8月应用于电子货币系统点点币(peercoin)[13],在其共识机制中,节点消耗的币龄(代币数量乘以拥有代币时长)越多,其产生区块的难度就越低。这也导致某些节点积累币龄,长时间不参加记账,同时较PoW算法也更容易引起区块链分叉,而且其本质仍采用“挖矿”机制来产生区块,同样还面临性能瓶颈;基于PoW和PoS算法的有机结合算法,如权益速度证明(proof of stake velocity, PoSV)[14]、燃烧证明(proof of burn, PoB)[15]、行动证明(proof of activity, PoA)[16]和2跳共识算法[17]等.为解决PoS中“屯币”现象,2014年4月Ren提出了PoSV共识算法,在这份蜗牛币(reddcoin, RDD)白皮书中,其改进了PoS中币龄是时间的线性函数的问题,在PoSV算法前期使用PoW实现代币分配,在后期则使用PoSV维护网络长期安全;2014年5月基于PoW和PoS提出了PoB共识算法,并发行了Slimcoin.PoB共识算法通过“燃烧”矿

工持有的 Slimcoin(把 Slimcoin 发送至特定的无法找回的地址)来竞争新区块的记账权,燃烧的 Slimcoin 越多则挖到新区块的可能性就越大;2014 年 12 月提出的 PoA 共识机制,采用 PoW 挖出的部分代币以抽奖的方式分发给所有活跃节点,而节点拥有的权益越高,其被抽中的概率也就越大,Bentov 等人[16]不仅提出了 PoA 共识机制,还指出了 PoW 共识机制在比特币系统后期带来的"公地悲剧"问题,但并没有结合博弈论给出分析与证明;2017 年 4 月 2 跳共识被提出,其解决思路是在 PoW 算力的基础上引入 PoS 权益,使得新区块的产生依赖于诚实节点占有大多数的联合资源(算力+权益).综上而言,这些共识算法都致力于取长补短、解决 PoW 与 PoS 存在的能源消耗与安全风险问题,在能源消耗、安全风险、吞吐量与性能等方面都有所突破,但都没有跳出"挖矿"式共识模式.

因此,本文针对比特币系统后期可能出现的"公地悲剧"问题、系统的性能瓶颈及"挖矿"的资源消耗等问题,首先利用博弈论分析比特币系统后期"公地悲剧"现象,在此基础上提出了一种基于门限密码方案[18]的共识机制(a consensus mechanism based on threshold cryptography, TCCM).在 TCCM 共识机制中,本文利用门限群签名理论[19-21]构建了记账节点保证金模型,获得区块链记账权的节点可以通过该模型提交保证金,同时该模型也保证了保证金的安全.其次,本文还利用门限加解密理论[22-23]构造了区块链记账权竞价模型,该模型通过节点竞价的方式产生记账节点,获得记账权的节点提交保证金来实现节点信用背书.最后,重构奖励机制,让收益能够奖励给存储、验证、传播区块的节点,使得更多的节点参与到共识的全过程中.

本文的主要贡献有 4 个方面:

1) 结合博弈论分析并证明了比特币系统后期"公地悲剧"的存在性,解释了"公地悲剧"所引发的比特币系统后期的安全问题;

2) 设计了基于门限群签名方案的保证金模型,该模型不仅为节点能够诚实地产生新区块提供背书,也设计了一种特殊的交易形式以确保保证金的安全;

3) 设计了基于门限加解密理论的区块链记账权竞价模型,该模型使得节点通过竞价拍卖的方式获得记账权,并能够保证记账节点产生的随机性,有效地防止记账权垄断现象;

4) 重构了区块链的奖励规则,使得越来越多的节点参与到共识的各个环节,能让更多的非记账节点通过系统获利,解决了"公地悲剧"问题,新共识机制打破了原有的"挖矿"式共识模式,有效地降低了资源消耗.

1　比特币系统的"公地悲剧"问题分析

在文献[16]中,Bentov 等人指出 PoW 共识机制在比特币系统后期会导致"公地悲剧"问题,主要指:当区块奖励可以忽略不计时,即奖励(几乎)完全是交易费用组成,比特币系统会出现显著的利润减少.由于节点存在自私的心理,都想尽可能不花费更多费用去使用系统的公共资源(矿工算力),比如转账、支付等.于是,使用者都不愿意把费用支付给"矿工"用于系统维护,大量低价值交易就不断出现.这必然导致"矿工"挖出来的交易费越来越少,于是造成网络算力下降,敌手攻击成本降低,系统越来越不安全,越来越多的使用者(节点)离开,网络节点数下降,直至整个比特币网络系统崩溃,这就是"公地悲剧"问题.为解决该问题,Bentov 等人[16]认为矿工可以尝试形成只接受高额交易的协议,设置每个块中的交易传递的总价值上限、限制块的大小等,但没有从博弈论的角度给出分析.本文在此基础上,结合博弈论具体分析并证明了比特币系统的"公地悲剧"的存在性.

在区块链系统中,假设有 m 个节点维护系统,且每个节点都是理性的参与者.$g_i \in [0,+\infty)$表示节点 i 产生的交易数量,$i=1,2,\cdots,m$;$G=\sum_{i=1}^{m} g_i$ 代表 m 个节点每轮(1 次共识过程)产生交易的总数;v 表示每笔交易的交易费用.假设是 v 是 G 的函数,$v=v(G)$.因为每笔交易至少有一定比特币的交易费用才会吸引节点由于利益的驱使去进行"挖矿",如若不然,整个比特币系统的安全性就会受到挑战.假设每轮系统存在最大的交易总数 $G_{\max}$,当 $G<G_{\max}$ 时,$v(G)>0$;当 $G\geqslant G_{\max}$,$v(G)=0$.随着交易总数的增加,每笔交易的费用就会降低.从另一方面说,当记账节点尽可能包含更多的交易时,会使得单笔交易的交易费降低,导致更多地交易总量.因此,本文假设:

$$\frac{\partial v}{\partial G}<0,\ \frac{\partial^2 v}{\partial G^2}<0. \tag{1}$$

如图 1 所示:

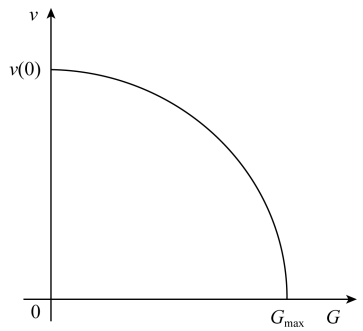

Fig. 1 The fee for each transaction decreases as the total number of transactions increases

图 1 每笔交易的交易费随着交易总数增加而下降

在系统中,节点会根据收集的交易费总价值来确定是否竞争“挖矿”.假设进行 Hash 计算时,每笔交易的平均资源消耗为 c,对于“挖矿”成功的节点 s,其利润函数为

$$S(g_s)=\sum_{i=1}^{m}g_i v\Big(\sum_{i=1}^{m}g_i\Big)-\sum_{i=1}^{m}g_i c, \tag{2}$$

其中,$\sum_{i=1}^{m}g_i$ 表示节点 s 收集的交易总数.而对于“挖矿”失败的节点,其利润函数(挖矿成功的节点 s 除外)为

$$Q_{fail}(g_1,g_2,\cdots,g_m)=-\sum_{i=1}^{m}g_i c, \tag{3}$$

其中,$fail\neq s$.式(2)(3)的一阶导数分别为

$$\frac{\partial S}{\partial g_s}=v(G)+Gv'(G)-c, \tag{4}$$

$$\frac{\partial Q}{\partial g_i}=-c,i=1,2,\cdots,m. \tag{5}$$

设节点成功“挖矿”跟节点算力有关,算力越大,“挖矿”成功的概率越大.节点参与“挖矿”的概率为 ξ,总算力为 1,p_i 代表节点 i 的算力(其中 $\sum_{i=1}^{m}p_i=1$),即挖矿“成功”的概率为 p_i,“失败”的概率为 $1-p_i$,则节点 i 的期望利润函数为

$$S'(g_1,g_2,\cdots,g_m)=\xi(p_i\times S(g_1,g_2,\cdots,g_m)+(1-p_i)\times Q(g_1,g_2,\cdots,g_m)),i=1,2,\cdots,m, \tag{6}$$

式(6)的最优化的一阶条件是

$$\frac{\partial S'}{\partial g_i}=p_i\times(v(G)+Gv'(G)-c)-(1-p_i)\times c=0,i=1,2,\cdots,m, \tag{7}$$

式(7)可以解释为增加一笔交易有正负 2 方面的效应,正的效应是这笔交易产生交易费 $v(G)$,负的效应是这笔交易会导致该轮每笔交易的交易费都降低.

m 个节点一阶条件定义了 m 个反应函数:

$$g^*=g_i(g_1,\cdots,g_{i-1},g_{i+1},\cdots,g_m),\quad i=1,2,\cdots,m, \tag{8}$$

因为:

$$\frac{\partial^2 s'}{\partial g_i^2}=p_i\times(v'(G)+v'(G)+Gv''(G))<0, \tag{9}$$

$$\frac{\partial^2 s'}{\partial g_i\partial g_j}=p_i(v'(G)+v'(G)+Gv''(G))<0, \tag{10}$$

所以根据隐函数存在定理可得:

$$\frac{\partial g_i}{\partial g_j}=-\frac{\dfrac{\partial^2 s}{\partial g_i\partial g_j}}{\dfrac{\partial^2 s}{\partial g_i^2}}<0, \tag{11}$$

即第 i 个节点的最优交易量随着其他节点的交易量的增加而递减.m 个反应函数的交叉点就是纳什平衡:$g^*=(g_1^*,\cdots,g_{i-1}^*,g_i^*,\cdots,g_m^*)$,纳什平衡的总交易数为 $G^*=\sum_{i=1}^{n}g_i^*$.

将 m 个节点的一阶条件(即式(7))相加,可得:

$$\frac{v(G^*)}{m}+\frac{G^*}{m}v'(G^*)=c, \tag{12}$$

系统最优的目标是最大化:

$$\max_G Gv(G)-\bar{\omega}Gc, \tag{13}$$

其中,$\bar{\omega}$ 表示系统实际情况下参与“挖矿”的节点数量且满足 $\bar{\omega}<m$.因为系统运行的现实中,总有节点不“挖矿”.换而言之,如果所有节点都“挖矿”,那么节点就不是理性参与者(与假设矛盾).

式(13)的最优化的一阶条件为

$$v(G^{**})+G^{**}v'(G^{**})=\bar{\omega}c, \tag{14}$$

这里,G^{**} 是比特币系统最优的交易数量,比较整个系统最优(见式(14))与单个节点最优的一阶条件(见式(12))可以看出,$G^*>G^{**}$,即系统实际运行时产生的交易数量过多,系统负荷过大,系统的矿工数量不足以满足交易数量,公共资源(矿工算力)被过度使用,从而引起比特币系统安全性的担忧.

2 系统模型

本节主要提出了节点保证金模型和区块链记账权竞价模型.

2.1 保证金模型

为了防止参与共识节点的作弊、无故离线、频繁分叉等拜占庭行为,本文提出了一种基于门限群签名理论的保证金模型,旨在通过抵押保证金抑制节点的拜占庭行为,利用门限群签名技术提高保证金的安全.

如图 2 所示,该保证金系统模型的参与方包括:可信中心(trust center, TC)(这一般由区块链系统监管机构负责);缴纳保证金的节点 ID_0;签名合成者(signature combiner, SC);保证金管理节点集合 $T=\{T_1,T_2,\cdots,T_n\}$,其身份信息分别为 ID_1,ID_2,…,ID_n.本文将缴纳和退还保证金的行为看成是一种特殊的交易,在该交易中,由缴纳保证金的节点 ID_0 向 T(由区块链系统中多个节点构成)缴纳保证金.每一位缴纳保证金的节点需要通过对前一次交易(一般交易)和下一位拥有者(保证金管理者集合)的公钥签署一份随机散列的数字签名,并将这个签名附加在保证金的末尾,那么保证金就提交给了 T.当缴纳保证金的节点诚实地完成了 1 轮或者多轮区块链共识,由保证金管理者集合 T 对前一次交易(特殊的交易)和下一位拥有者(需返还保证金的节点 ID_0)利用门限群签名技术签署一份随机散列的数字签名,并将这个签名附加在返回的保证金的末尾,保证金就返还给了之前缴纳保证金的节点 ID_0.

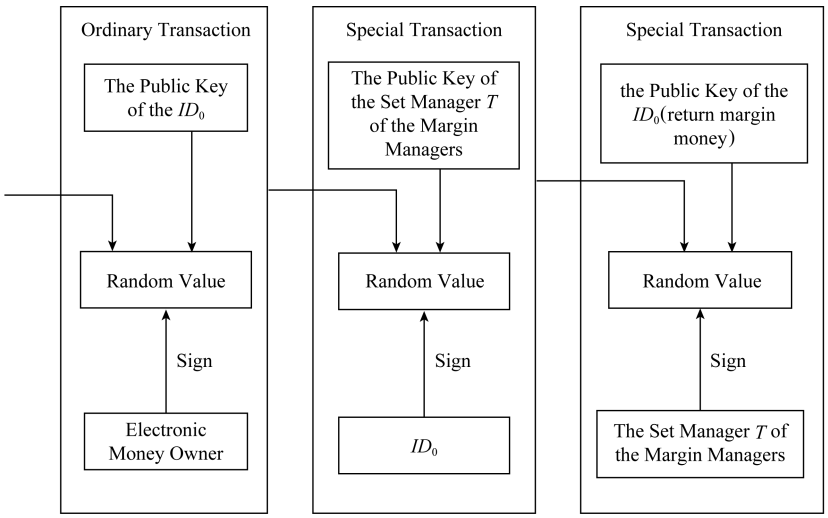

Fig. 2　The schematic diagram of margin model

图 2　保证金模型示意图

该保证金模型包含保证金缴纳和保证金退,对于缴纳保证金部分与比特币系统类似,只是将下一位拥有者的公钥替换成金管理节点集合 T 的群公钥 g_p,故不作详细阐述;保证金退还部分利用了门限群签名技术,在文献[24]的方案基础上做出了调整与修改,具体包含系统初始化、签名、签名验证 3 个部分.每个部分具体为:

1) 初始化 $setup(t,n)$

① 设置系统参数

首先设定保证金管理节点集合(群)的大小为 n,门限值为 t,其中 $t<n$.然后随机选定一个大素数 p,F_p 表示有限域.随机选择 $a,b\in F_p$,构造该有限域 F_p 上的椭圆曲线 E.最后选择椭圆曲线 E 上的一个生成元 G,它的阶 q 为一个大素数.同时,设椭圆曲线上的 2 个点 P_1,P_2,存在 $k\in\mathbb{Z}_p^*$,使得 $P_1=kP_2$,由 k 和 P_2 计算 P_1 是可行的,但是通过 P_1 和 P_2 计算 k 是不可行的.

② 设定相关密钥及参数

首先设定可信中心 TC 私钥为 $T_s=s$,TC 公钥为 $T_p=sG$,其中 $s\in_R\mathbb{Z}_p^*$.然后秘密选定一个 $t-1$ 次多项式:$f(x)=a_{t-1}x^{t-1}+a_{t-2}x^{t-2}+\cdots+a_1x+a_0$,其中 $a_i\in[1,p-1](i=0,1,\cdots t-1)$ 的整数.那么群私钥为 $g_s=f(0)=a_0$,群公钥为 $g_p=f(0)G=a_0G$;接着选择一个单向的 Hash 函数 $h(\cdot)$;最后公开参数 a,b,G,g_p,p 和 $h(\cdot)$,g_s 和 $f(x)$ 被 TC 秘密保存.

③ 密钥分发

TC 为保证金管理节点集合颁发另一部分私钥,这一过程需要节点和 TC 交互执行:

首先,TC 计算节点的另一部分私钥:

$$y_i=f(ID_i),\tag{15}$$

将 y_i 通过秘密通道发送给相应的节点,并广播 α_iG 的值.

节点接收到私钥 y_i 后,验证:

$$y_iG=\sum_{i=0}^{t-1}a_iGID_i.\tag{16}$$

如果式(16)成立,节点则接收 y_i 为其另一部分

私钥;反之,拒绝接收并要求 TC 重新生成另一部分私钥.

至此,节点生成了私钥 $d_i = x_i + y_i = x_i + f(ID_i)$,公钥 $D_i = d_iG$,并公开节点公钥 D_i 和用户身份信息 ID_i.

2) 签名

① 节点生成份额签名 $Sign(T_i, ID_i, d_i, preTr, D_f)$

设门限群签名的参与成员为部分保证金管理节点集合 $T = \{T_1, T_2, \cdots, T_t\}(t<n)$,对应的公开身份信息集合为 $ID = \{ID_1, ID_2, \cdots, ID_t\}$.每个节点 $T_i(i \in [1,t])$ 利用私钥 d_i,对前一次交易 $preTr$ (previous transaction)和被返还保证金的节点 T_f 的公钥 D_f 进行签名,生成份额签名.具体步骤包括:随机选择 $k_i \in_R \mathbb{Z}_p^*$,计算 $r_i = k_iG = (x_{r_i}, y_{r_i})$;计算需要签名的消息的随机 Hash 值 $z = h(preTr + D_f)$;计算份额签名 $s_i = k_i x_{r_i} - zd_i I_i \bmod p$,其中满足 $I_i = \prod_{i \neq j} \frac{ID_i}{ID_i - ID_j}, (i, j \in [1,t])$.

为了防止签名被敌手追踪,本文使用 SC 的公钥 PK_{SC} 加密自身的身份,同时选取一个随机值 $Random$ 使每次加密后的密文均不相同:

$$ID_i' = E_{PK_{SC}}(Random \parallel ID_i), \quad (17)$$

至此,节点 T_i 生成了份额签名 (r_i, s_i),并将 (r_i, s_i) 和 ID_i' 发送给签名合成者 SC,SC 由公式 $Num_{SC} = L \bmod n$,其中 Num_{SC} 表示 SC 的编号,L 为区块链长度,n 为保证金管理节点个数.

② 合成门限群签名 $Combine(r_i, s_i, D_i, preTr, D_f)$

本过程由签名合成者 SC 完成,包括份额签名验证和签名合成 2 个方面.

份额签名的验证:SC 收到成员 T_i 的份额签名 (r_i, s_i) 后,分别验证其正确性.首先使用自身私钥 SK_{SC} 解密 ID_i' 得到签名者的身份 ID_i;然后通过集合 ID 计算 I_i,$I_i = \prod_{i \neq j} \frac{ID_i}{ID_i - ID_j}$;接着计算 $z = h(preTr + D_f)$,再验证等式 $s_iG + zD_iI_i = r_i x_{r_i}$ 是否成立.如果成立,那么份额签名 (r_i, s_i) 合法,否则拒绝该份额签名.

签名的合成:首先以 SC 验证的 t 个份额签名合法为前提,再计算 $R = \sum_{i=1}^{t} r_i x_{r_i} \bmod p$,将所有份额签名合并,计算 $S = \sum_{i=1}^{t} s_i$,公开 $W = \sum_{i=1}^{t} I_i X_i$,其中 $X_i = x_iG$.SC 生成门限群签名 (R, S),即该笔返还的保证金交易的签名,并将其广播至全网.

3) 签名验证

其他节点接收到门限群签名 (R, S) 后,根据 $z = h(preTr + D_f)$ 计算 z,并验证 $SG + z(g_p + W) = R$ 是否成立.如果成立则接收签名,即将其放入交易池中;否则拒绝该门限群签名,即抛弃该笔交易,意味着保证金返还失败.

2.2 记账权竞价模型

关于区块链记账权问题,本文考虑到区块链网络中可能存在拜占庭节点,提出了一种基于门限加密方案的记账权竞价模型,旨在通过参与共识的节点之间相互竞价来产生区块链的记账节点,同时利用多方参与决策来抑制拜占庭节点的恶意行为.

记账权竞价模型如图 3 所示,设参与共识节点集合 $U = \{U_1, U_2, \cdots, U_m\}$,其身份信息分别为 ID_1, $ID_2, ID_3, \cdots, ID_m$,解密服务器节点集合 $T = \{T_1, T_2, T_3, \cdots, T_n\}$,其中,$T \subseteq U$,且解密服务器集合即保证金节点集合,由 n 个解密服务器利用自己的私钥联合产生秘密份额和系统公钥,参与共识的节点利用产生的系统公钥加密竞价金额得到密文,同时利用自己私钥对密文和上一轮记账节点编号的 Hash 值进行签名,并在区块链系统中广播签名和密文.当解密服务器节点收到密文和签名,先根据密文验证签名的正确性,如果不正确,则丢弃签名;如果正确,利用自己的秘密份额解密出解密因子,并在全网广播解密因子,任何收到 t 个解密因子的解密服务器节点验证解密因子的正确性后,就可以通过

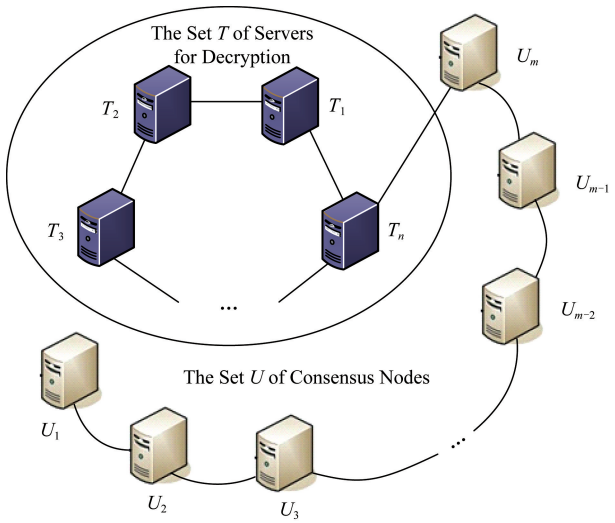

Fig. 3 The bidding model of the right of accounting

图 3 记账权竞价模型

组合解密出竞价金额.值得注意的是 $t>f$,f 为解密服务器节点集合中拜占庭节点个数,且假设:

$$f<\lfloor(n-1)/3\rfloor.$$

与(k,n)门限加密方案类似,该记账权竞价模型由 5 个步骤组成:

1) 系统初始化

设秘密选定一个大素数 p,F_p 表示有限域,$E(a,b)$为 F_p 上的椭圆曲线,G 为椭圆曲线的基点,q 为G 的阶(p,q 为奇素数).公开 $E(a,b)$和 G.这与保证金模型初始化系统参数类似,椭圆曲线采用 E.

2) 设置秘密份额及公钥

由 T_i 运行,每个解密服务节点执行步骤:

① T_i 随机选择一个整数 $d_i\notin[1,q-1]$作为私钥,并计算公钥 $Q_i=d_iG$.

② T_i 产生随机整数集$\{a_{i,k}\mid k=1,2,\cdots,t-1\}\subseteq F_p$ 且 $a_{i,t-1}\neq0$,构造 $t-1$ 次多项式:

$$f_i(x)=d_i+a_{i,1}x+\cdots+a_{i,1}x^{t-1}\bmod q,\tag{18}$$

其中,$f_i(0)=d_i$.

③ T_i 计算 $f_i(ID_j)$并发送给 $T_j(j\neq i)$,$f_i(ID_j)$保留.同时计算并广播验证参数:

$$a_{ik}=a_{ik}G,k\in\{1,2,\cdots,t-1\},\tag{19}$$

当 $T_j(j\neq i)$接到其他 $n-1$ 个解密服务器节点的广播信息后,验证 $f_i(ID_j)$的有效性为

$$f_i(ID_j)G=d_iG+\sum_{k=1}^{t-1}a_{ik}\ (ID_j)^k,\tag{20}$$

若式(20)成立,则 $f_i(ID_j)$有效;否则 T_j 拒绝接收 $f_i(ID_j)$并要求 P_i 重新发送.

④ T_i 收到其他 $n-1$ 个解密服务器节点 T_j 发送的 $f_i(ID_j)$之后,自己的秘密份额 $F(ID_i)$可计算为

$$F(ID_i)=\sum_{j=1}^{n}f_i(ID_i)\bmod q,\tag{21}$$

T_i 计算 $Y_i=F(ID_i)G\bmod q$,并广播 Y_i.

⑤ 由 Lagrange 插值法,利用公开信息 Y_i 计算解密服务器节点组公钥:

$$y=F(0)G\bmod q=\sum_{i=1}^{t}\left(\prod_{j=1,j\neq i}^{t}\frac{-ID_j}{ID_i-ID_j}Y_i\right)\bmod q,\tag{22}$$

公开解密服务器节点组公钥 y.

3) 加密

将竞价金额 Mo(明文)映射为有限域 F_P 上的一个元素 M,并分割成 2 个部分 $M=m_1+m_2$.设竞价区块链记账权节点 U_i.

① U_i 选取一个随机数 k,$1\leqslant k\leqslant q-1$.

② U_i 进行计算:

$$\begin{aligned}&c_0=kG,\\&(x_1,y_1)=k\times y,\\&c_1=(x_1,m_1)\bmod p,\\&c_2=(y_1,m_2)\bmod p.\end{aligned}\tag{23}$$

③ 利用 ECC 进行签名:

$$\sigma=Sign(h((c_0,(c_1,c_2)),ID_{\mathrm{pr}}),SK_{u_i}),\tag{24}$$

其中,SK_{u_i} 为竞价节点的私钥,$h(\cdot)$为单向函数,ID_{pr}为上一次记账节点的编号.

④ 将密文 $C_M=(c_0,(c_1,c_2))$和 σ 发送给 T.

4) 部分解密

由 T_i 运行,设 T 中 t 个解密服务器节点集合为 $W=\{T_1,T_2,\cdots,T_t\}$,W 中的成员 T_i 收到密文 C_M 后,计算:

$$hashValue=h(C_M,ID_{\mathrm{pr}}),\tag{25}$$

通过解密签名,得到:

$$\tau=Unsign(\sigma,P_u).\tag{26}$$

比较 $hashValue$ 和 τ,如果不相等,则选择丢弃密文 C_M 与签名 σ;反之,T_i 使用自己的秘密份额 $F(ID_i)$,计算各自的解密因子 S_i:

$$S_i=c_0F(ID_i)\prod_{j=1,j\neq i}^{t}\frac{-ID_j}{ID_i-ID_j}.\tag{27}$$

5) 组合与比较

由 W 中的解密服务器节点运行.该步骤包括 2 个部分,验证解密因子 S_i 的真实性和组合 S_i 恢复明文 M.

① W 中的节点彼此交换 S_i,并验证解密因子 S_i 的真实性:

$$S_iG=c_0Y_i\prod_{j=1,j\neq i}^{t}\frac{-ID_j}{ID_i-ID_j},\tag{28}$$

若式(28)成立,则 T_i 提交的 S_i 是正确的,否则要求重新 T_i 重新发送解密因子.

② 当 W 中解密服务器收到 t 份正确的 S_i 后,就按步骤计算 m_1 和 m_2 以此来解密明文 M:

$$\begin{aligned}&(x_1,y_1)=\sum_{i=1}^{t}S_i,\\&m_1=(c_1-x_1)\bmod p,\\&m_2=(c_2-y_1)\bmod p,\\&M=m_1+m_2.\end{aligned}\tag{29}$$

③ 通过映射关系,根据 M 求得竞价金额 Mo.

3　共识机制设计

本节主要从初始化、区块构建、区块验证和区块链组装 4 个部分阐述共识机制(TCCM).

3.1 初始化阶段

当节点收到新区块并通过验证(*round* 轮共识结束),节点中的伪随机数生成程序就会自动运行,并以 *round* 轮记账节点的身份编号作为随机种子从参与共识的节点中选出 n 个解密服务器节点,需要注意的是该程序产生的 n 个伪随机值是在 1～ m (m 为参与共识节点的个数)之间,具有良好的随机性.因为随机种子为 *round* 轮记账节点的 ID,所以产生的 n 个解密服务器节点具有一致性.

当 *round*+1 轮的记账权竞价正式开始后,决定竞争记账权的节点们,通过区块链记账权竞价模型提交报价金额.如算法 1 所示,当报价阶段结束后,所有解密服务器节点 i 会广播自己保存的最大的竞价金额 Mo_i(理论上可以是 ε 位小数,$0<\varepsilon<+\infty$)和竞价节点编号 N,*round* 轮记账节点通过广播收到这些竞价金额和竞价节点编号,选取最大的竞价金额的节点,并通过签名的形式提议获得此次记账权的节点.当解密服务器节点收到 *round* 轮记账节点的提议后,如果发现它该报价金额的确是最大的(即该记账金额大于等于它保存的竞价金额),它也会继续提议由自己重新签名的信息.当 *round*+1 轮记账节点接收到至少 t 条这样的提议信息后,并验证签名的正确性后,就通过保证金模型提交保证金.需要注意的是,保证金金额一般要大于单个区块交易总价值上限 1/2,这也是为了保证交易的安全性并提高获取记账权的门槛.同时,当记账节点没有在规定的时间产生新区块,*round* 轮的记账节点再次广播竞价金额次之的节点编号,以此类推,直至在提交保证金的情况下产生新区块.

算法 1. 记账权竞价算法.

/ * 广播阶段 * /

① Mo_i = 节点 i 的报价金额;

② if Mo_i 为解密服务器节点 T_x 解密的最大金额 then

③ 广播 "Mo_i + 竞价节点编号 N" + 其签名;

④ end if

/ * 提议阶段 * /

⑤ if Mo_j 为 *round* 轮记账节点接收到最大金额 then

⑥ 提议"Mo_j + 竞价节点编号 N" + 其签名;

⑦ end if

⑧ if 解密服务器节点 T_y 解密金额不大于 Mo_j then

⑨ 提议"Mo_j + 竞价节点编号 N" + 其签名;

⑩ else

⑪ 丢弃;

⑫ end if

⑬ if 记账节点接收提议次数不少于 t 且签名正确 then

⑭ 通过保证金模型提交保证金 Mo_j;

⑮ end if

3.2 区块构建

构建区块是区块数据的填充过程.本文将由节点产生的含有代币的数据称为"交易".所有的节点都需要检查交易的合法性,再将交易保存在交易池.本节首先定义了区块头的数据结构:

nVersion,区块版本号,4 B;

hashPrevBlock,上一个区块的区块头的 Hash 值,32 B;

hashMerkleRoot,由区块中所有交易构造的 Merkle 根,32 B;

nTime,Unix 时间戳,4 B.

为了避免比特币后期会导致的"公地悲剧"问题,本文对区块的交易填充做了详细规定:1)设置每个区块中交易传递的总价值上限;2)在满足条件规定 1 的前提下,规定每个区块中的交易总量不得超过 G^{**}.G^{**} 代表了系统最优情况下的交易量,即保证区块链网络安全的交易量.

由于区块收入是整体网络安全的基础,在"公地悲剧"的情况下,系统安全性将会很弱.因此,维护健康的网络需要一些协议执行的规则来保护参与共识的节点作为一个群体,例如设置每个块中的交易量上限.如果适当选择上限,矿工实际上可以通过这种上限获得更多的收益,从而保证了区块链系统的安全.通过这种方式使得块空间成为稀少资源,交易费就会上涨;为了将交易填充到区块中必须与其他节点竞争,并支付更高的交易费用.设置每个块中的交易总量,使得记账节点不能通过接受低收费交易来打破市场,因为记账节点只能把这么多的交易放到块中.同时,单笔交易的交易费具有波动性会导致交易的总费用是一个不确定的,即区块收入不确定,节点无法准确估计竞价金额 Mo,这也给节点竞争区块链记账权带来了挑战.

当记账节点完成了区块数据的正确填充,就会立刻将新区块发送给其所有相邻节点.这些相邻节点成功验证并接受这个新区块后,也会继续以类似的方式传播该区块.

3.3　区块校验

新区块在网络中以广播的方式进行扩散,其验证由节点独立进行,确保只有有效的区块才会在网络中传播,从而获得奖励.反之,由于区块的无效性会导致节点失去奖励,并扣押保证金.记账节点的奖励 R:

$$R=AllTrExp-Mo, \tag{30}$$

其中,$AllTrExp$ 表示该区块的交易费总价值,Mo 表示竞价金额,且新区块的交易费总价值是由记账节点自己独立收集,由于网络原因存在差异.

当节点收到新区块时,它会按照标准验证清单对该区块进行一一核查,其标准一般包括:

1) 验证记账节点的合法性.在提交保证金的前提下,通过执行区块链记账权竞价模型中最后一步,利用收集到的广播的解密因 S_i 合成竞价金额,核实竞价金额的节点身份信息.

2) 验证区块数据填充的有效性.

3) 区块大小在长度限制之内.

若没有通过验证,这个区块将被拒绝,同时广播所有验证数据.当 n 个解密服务器节点中,有 t 个解密服务器节点通过对验证数据的计算,发现该区块是不合法的,这 t 个解密服务器节点就可以通过保证金模型,与参与共识的节点瓜分保证金.同时,重新产生记账节点.反之,如果验证通过了,本轮将通过保证金模型返还上一轮记账节点的保证金,同时由参与共识的节点通过保证金模型分享竞价金额.

需要注意的是,返回保证金的交易并没有打包到当前区块中,而是区块链系统会在产生足够多区块后,才会触发保证金模型返回保证金,这是为了保证记账节点的诚实性,不会发起区块链"分叉"攻击而导致"双花"问题.

同时,本文借鉴了"闪电网络"的思想[25],只有参与共识的节点积累了足够的奖励,才会启动保证金模型进行奖励分发,这是为了减少区块链网络中小额交易数量,缓解节点的通信与计算压力.

3.4　区块装配

在区块的装配阶段,主要是将新区块装配至区块链主链中.当某个节点接收并验证通过了新区块,它会将新区块连接到现有的区块链上,将它们组装起来.由于新共识机制明确规定了记账节点,故不存区块链的分叉问题,也就不存在由于分叉而导致的区块链系统资源的浪费.

随着越来越多的节点加入区块链系统,单位时间的交易量也会持续增加,节点为了竞争区块空间,势必会提高交易费,区块收入也会相应增加.由于区块收入是整体网络安全的基础,区块收入的增加必将带来区块链系统安全性的提高.

4　安全性分析与讨论

本节我们主要对 TCCM 共识机制的安全性进行分析,并从中小额交易、激励机制等方面进行讨论.

4.1　抗"公地悲剧"攻击

首先考虑 2 个节点竞争区块链记账权,$i=1,2$.令 $b_i\geqslant 0$ 是竞价节点的竞价金额,v_i 为该轮区块的交易费总价值.由于各个节点收集的交易并不相同且不确定,所以对于不同竞价节点 v_i 是一个不确定的值,且任意俩竞价节点都不知道对方的竞价金额 b_i.但可以确定的是,v_i(被标准化)在[0,1]区间均匀独立分布,竞价节点 i 的效用函数如下(如果 2 节点的竞价金额相同,节点以等概率获得记账权):

$$u_i(b_i,b_j;v_i)=\begin{cases}v_i-b_i, & b_i>b_j;\\ \dfrac{1}{2}(v_i-b_i), & b_i=b_j;\\ 0, & b_i<b_j.\end{cases} \tag{31}$$

设节点 i 的出价 $b_i(v_i)$ 是关于其价值 v_i 的严格递增可微函数.从理性前提出发,没有节点愿意支付高于交易费总价值的竞价金额,即 $b_i>1\geqslant v_i$ 不可能是最优的情况.由于该博弈是对称的,故只需要考虑对称出价战略:$b=b^*(v)$.给定 v 和 b,节点 i 的期望效用为

$$u_i=(v-b)\ Prob\ (b_j<b), \tag{32}$$

其中,b_j 是节点 j 的出价策略,$Prob(\cdot)$代表 $b_j<b$ 的概率.在式(32)中,$(v-b)$是成功获得记账权的情况下节点 i 的净收益,$Prob(\cdot)$表示获得记账权的概率.

根据对称性,$b_j=b^*(v_j)$,有:

$$Prob\{b_j<b\}=Prob\{b^*(v_j)<b\}=$$
$$Prob\{v_j<b^{*-1}(b)\equiv\Phi(b)\}=\Phi(b), \tag{33}$$

这里 $\Phi(b)=b^{*-1}(b)$是 b^*的逆函数(节点选择 b 时他的价值是 $\Phi(b)$).在式(33)中,由于 v 在区间[0,1]均匀分布,$\Phi(b)\in[0,1]$,则 $Prob(v_j<\Phi(b))=\Phi(b)$.因此,节点 i 面临的问题是:

$$\max_b u_i=(v-b)\ Prob\ (b_j-b)=(v-b)\Phi(b), \tag{34}$$

最优化的一阶条件是:

$$-\Phi(b)+(v-b)\Phi'(b)=0. \tag{35}$$

如果 $b^*(\cdot)$是节点 i 的最优战略,$\Phi(b)=v$.因此:

$$(\Phi(b)-b)\Phi'(b)=\Phi(b), \tag{36}$$

式(36)微分方程可以写成:

$$\frac{\partial(vb)}{\partial v}=v, \tag{37}$$

解式(37)偏微分方程可得:

$$b^*=v/2, \tag{38}$$

如式(38)所示,这里的贝叶斯均衡为,每个节点的出价是它在该轮收集到的交易费总价值的一半.根据出价最高的节点获得区块链记账权,去除竞价金额,记账节点还是获得一半的交易费,这对于众多验证、存储、传播的节点来说是不公平的.

但是,节点出价与实际单个区块的总交易费之间的差距随着竞价节点个数的增加而递减.设有 m 个节点,每个节点开始对于 v_i 是不确定的,但都在[0,1]区间上的均匀分布,如果最终收集到的交易费总价值 v_i 的节点 i 出价为 b,则期望效用函数为

$$u_i=(v-b)\prod_{j\neq i}Pro\,b(b_j<b)=(v-b)\Phi^{m-1}(b), \tag{39}$$

最优化的一阶条件为

$$-\Phi^{m-1}(b)+(v-b)(m-1)\Phi^{m-2}\Phi'(b)=0, \tag{40}$$

解式(40)微分得:

$$b^*(v)=\frac{m-1}{m}v. \tag{41}$$

如图4所示($v=1$),$b^*(v)$随着 m 的增加而增加.当 $m\to\infty$时,$b^*\to v$.即参与共识的竞价节点越多,记账所花费的竞价金额就越高.可见,当 m 趋于无穷时,记账节点由于高昂的竞价金额而几乎分不到交易费.

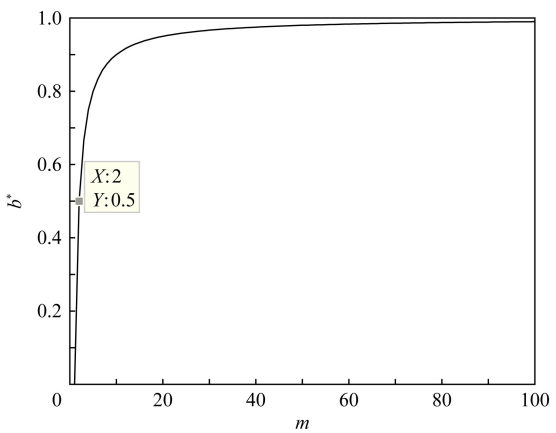

Fig. 4 The trend of the bidding amount with the number of bidding nodes

图4 竞价节点数量与竞价金额变化趋势

综上,一方面,m 趋于无穷这种情况也是不可能存在的,由于节点提交的保证金对于大多数节点来说是个门槛,很多节点没有那么多保证金,所以会选择参与验证、存储等非记账过程.另一方面,更多节点参与竞争记账权,竞价金额就会越高,用于非记账行为的奖励就会越高,就会吸引更多的节点参与区块的验证、存储等非记账过程,有利于区块链系统的利益分配.新的激励机制会导致越来越多的节点参与共识过程,不会出现"节点少交易多"的情况,能达到抑制"公地悲剧"的目的,区块链系统也会变得更加安全可靠.

4.2 抗"垄断"性

抗"垄断"性质主要是指竞争区块链记账权具有随机性.以 PoW 算法为例,它并不具有良好的随机性,主要是其记账权依赖算力竞争,算力越来,获得记账权的概率就越大.至目前为止,全球大部分算力被矿池垄断,全球前5的大矿池共计拥有超50%的算力.共识机制安全的一个关键因素就是记账节点的随机性(抗"垄断").

在 TCCM 共识机制中,由于每个节点都是自私且理性的,都希望用最小的代价获得记账权来使得自己利益最大化.在拍卖记账权的过程中,竞争区块记账权的节点无法提前预知本轮共识的交易费总量且各个节点收集的交易费具有不确定性(见3.2节),所以节点无法准确给出竞价金额 Mo;其次 Mo 表示一个理论值是 $\varepsilon(0<\varepsilon<+\infty)$ 位小数,在一个合理区间有无数种可能.在这种理性前提下,这些都导致没有节点可以垄断记账权.

4.3 讨 论

在中小额交易方面,TCCM 共识机制是 PoW 共识机制的良好扩展;对于大额交易,TCCM 共识机制有所欠缺,这是由于保证金的金额只大于单个区块交易总价值上限1/2,当单笔金额或者新区块中某账户累计金额超过单个区块交易总价值上限1/2时,出于安全考虑,仍采用 PoW 共识机制.幸运的是,在区块链系统中大额交易很少,中小额交易占大多数,显然依赖大量计算资源消耗的 PoW 共识机制并不适用,而 TCCM 共识机制在资源消耗方面更有优势,且更适用于中小额交易的处理,有利于提高交易处理效率.

TCCM 共识机制改进了区块链系统的激励机制.在 PoW 共识机制中,交易费只支付给创建区块的矿工,而传播、验证和存储交易的成本是由网络中的所有节点分担,并没有给予奖励,这就导致矿工(矿池)尽可能自己保持每笔交易来收取费用,尽可

能地避免传播自己产生的交易.在 TCCM 共识机制中,虽然每个区块都设置价值上限,但是对于解决"公地悲剧"问题帮助不大,因为整个用户仍然希望发送大量的低价值交易.因此,3.3 节考虑给予奖励给每个参与共识验证的节点,这使得节点更愿意参与节点验证工作,进一步提高系统安全.

5　性能分析

本文将从时间开销、吞吐量等指标分析该共识机制的性能.

假设 T_{MUL} 表示模乘法运算的时间开销,T_{EC_MUL} 表示椭圆曲线上乘法运算的时间开销,T_{EC_ADD} 表示椭圆曲线上加法运算的时间开销,T_H 表示 Hash 运算的时间开销,T_{block} 表示区块产生时间.根据文献[20],有 $T_{EC\_MUL}\approx 29T_{MUL}$,$T_{EC\_ADD}\approx 0.12T_{MUL}$.由于模加法和模减法的计算开销很低,可忽略不计.本文所提出的共识机制时间开销为:归还保证金 T_{mon}、产生记账节点 T_{acc}、产生区块 T_{block}.假设参与记账权竞争的节点个数为 J.

归还保证金的开销为

$$T_{mon}=(4t+2)T_{EC\_MUL}+2(t-1+2)T_{EC\_ADD}+3tT_{MUL}+(t+1+1)T_H=(119.24t+58)T_{MUL}+(t+2)\ T_H,$$

产生记账节点的时间开销为

$$T_{acc}=(2+2t)JT_{EC\_MUL}+T_H+(2t+1)JT_{EC\_ADD}=(58.12+58.24t)JT_{MUL}+T_H,$$

则总的时间开销为

$$T_{sum}=T_{mon}+T_{acc}+T_{block}=(119.24t+58+58.12J+58.24tJ)\ T_{MUL}+(t+3)\ T_H+T_{block}.$$

根据官方文档和已有的测试,本文对比了 PoW 和 PoS 公有链共识算法与 TCCM 共识机制,如表 1 所示,发现 TCCM 共识机制在 TPS、时延、交易确认时间、交易不可更改时间、资源消耗、时间复杂度等方面都具有优势.

Table 1　Performance Indicators of PoW, PoS, TCCM

表 1　PoW, PoS, TCCM 性能指标

Indicators	PoW	PoS	TCCM
TPS	<7	5−10	10 000
Delay Time	minute level	minute level	second level
Confirmation Time/min	10	10	<1
Time of Altering the Transaction/h	1	1	do not alter the transaction
Resource Consumption	high	a little high	low
Time Complexity	$O(n)$	$O(n)$	$O(1)$

针对区块链共识机制比较了 PBFT 算法和 TCCM 共识机制(解密服务器节点集合 T 在安全范围内尽量小)的吞吐量.吞吐量是衡量系统单位时间内处理交易的能力.本文适用每秒交易数 (transaction per second, TPS)来表示.区块链应用中交易吞吐量指单位时间内交易从产生到被确认并写入区块链中的交易总数:

$$TPS_{\Delta t}=SumTransactions_{\Delta t}/\Delta t,\qquad (42)$$

其中,Δt 为交易产生到区块被确认的时间间隔,即出块时间;$SumTransactions_{\Delta t}$ 为该时间间隔内被确认区块中包含的交易总数.

本文取 Δ 时间间隔分别为 50 s, 60 s,100 s,300 s 等不同时间间隔,每个时间间隔测试 20～30 次,取其均值作为共识机制的 TPS 值.如图 5 所示,本文通过 Matlab 绘制了 TPS 随着间隔变化的趋势图.

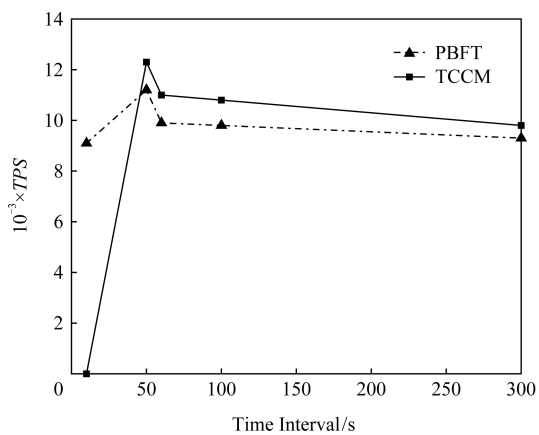

Fig. 5　Comparison of throughput between PBFT algorithm and TCCM consensus mechanism

图 5　PBFT 算法和 TCCM 共识机制的吞吐量比较

6 总 结

本文提出了一种基于门限密码方案的共识机制,它是 PoW 共识机制一种良好的扩展.在新的共识机制中,设计的保证金模型既能够保证记账节点能诚实地产生区块,也确保了保证金的安全转移;设计的记账权竞价模型不但为竞价拍卖提供了安全的环境,而且记账节点的产生具良好的随机性,有效地防止了记账权垄断.在此基础上,本文重新设计了节点的激励机制,利用记账节点的竞价金额对区块验证、传播和存储等活动进行奖励,极大地维护了区块链系统的安全,避免了"公地悲剧"问题.同时,TCCM 共识机制能更好地处理中小额交易,极大地提高了区块链系统的吞吐量,但 TCCM 在大额交易方面需要 PoW 协议的介入以保证交易安全,后续工作将对其改进与完善.

参 考 文 献

[1] Nakamoto S. Bitcoin: A peer-to-peer electronic cash system [OL]. [2016-11-26]. http://www.academia.edu/download/54517945/Bitcoin_paper_Original_2.pdf

[2] Drescher D. Blockchain Basics [M]. Berkeley, CA: Apress, 2017

[3] McConaghy T, Marques R, Müller A, et al. BigchainDB: A scalable blockchain database [OL]. 2016 [2017-07-10]. https://www.bigchaindb.com /whitepaper/bigchaindb-whitepaper.pdf

[4] Martin W. Cryptocurrencies and the blockchain [OL]. 2015 [2017-06-22]. https://martinw.eu/documents/Cryptocurrencies%20and%20the%20Blockchain.pdf

[5] Zyskind G, Nathan O. Decentralizing privacy: Using blockchain to protect personal data [C] //Proc of 2015 IEEE Security and Privacy Workshops. Piscataway, NJ: IEEE, 2015: 180-184

[6] Christidis K, Devetsikiotis M. Blockchains and smart contracts for the Internet of things [J]. IEEE Access, 2016, 4: 2292-2303

[7] Tian Feng. An agri-food supply chain traceability system for China based on RFID & blockchain technology [C] //Proc of the 13th Int Conf on Service Systems and Service Management. Piscataway, NJ: IEEE, 2016: 33-38

[8] Linn L A, Koo M B. Blockchain for health data and its potential use in health IT and health care related research [OL]. [2017-05-11]. https://www.healthit.gov/sites/default/files/11-74-ablockchainforhealthcare.pdf

[9] Shao Qifeng, Jin Cheqing, Zhang Zhao, et al. Blockchain: Architecture and research progress [J]. Chinese Journal of Computers, 2018, 41(5): 969-988 (in Chinese)
(邵奇峰, 金澈清, 张召, 等. 区块链技术: 架构及进展[J]. 计算机学报, 2018, 41(5): 969-988)

[10] Castro M, Liskov B. Practical Byzantine fault tolerance and proactive recovery [J]. ACM Transactions on Computer Systems, 2002, 20(4): 398-461

[11] Dwork C, Naor M. Pricing via processing or combatting junk mail [C] //Proc of Annual Int Cryptology Conf. Berlin: Springer, 1992: 139-147

[12] Back A. Hashcash—A denial of service counter-measure [C] //Proc of USENIX Technical Conf. Berkeley, CA: USENIX Association, 2002

[13] King S, Nadal S. PPcoin: Peer-to-peer crypto-currency with proof-of-stake [OL]. [2016-11-26]. https://bitcoin.peryaudo.org/vendor/peercoin-paper.pdf

[14] Ren L. Proof of stake velocity: Building the social currency of the digital age [OL]. [2016-11-26]. https://assets.coss.io/documents/white-papers/reddcoin.pdf

[15] P4Titan. Slimcoin: A peer-to-peer crypto-currency with proof-of-burn [OL]. [2017-12-11]. https://www.chainwhy.com/upload/default/20180703/4ae7cee40462e7951f508b28dd1d9936.pdf

[16] Bentov I, Lee C, Mizrahi A, et al. Proof of activity: Extending bitcoin0s proof of work via proof of stake [J]. ACM SIGMETRICS Performance Evaluation Review, 2014, 42(3): 34-37

[17] Duong T, Fan Lei, Zhou Hongsheng. 2-hop blockchain: Combining proof-of-work and proof-of-stake securely [OL]. [2018-10-17]. https://eprint.iacr.org/2016/716

[18] Shamir A. How to share a secret [J]. Communications of ACM, 1979, 22(11): 612-613

[19] Hwang J Y, Kim H J, Lee D H, et al. An enhanced (t, n) threshold directed signature scheme [J]. Information Sciences, 2014, 275: 284-292

[20] Chen T S, Hsiao T C, Chen T L. An efficient threshold group signature scheme [C] //Proc of 2004 IEEE Region 10 Conf. Piscataway, NJ: IEEE, 2004: 13-16

[21] Chung Y F, Chen T L, Chen T S, et al. A study on efficient group-oriented signature schemes for realistic application environment [J]. International Journal of Innovative Computing, Information and Control, 2012, 8(4): 2713-2727

[22] Oh J H, Lee K K, Moon S J. How to solve key escrow and identity revocation in identity-based encryption schemes [C] //Proc of the 1st Int Conf on Information Systems Security. Berlin: Springer, 2005: 290-303

[23] Ertaul L, Lu Weimin. ECC based threshold cryptography for secure data forwarding and secure key exchange in MANET (I)[C] //Proc of the 4th Int Conf on Research in Networking. Berlin: Springer, 2005: 102-113

[24] Chen Liquan, Zhu Zhen, Wang Muyang, et al. A threshold group signature scheme for mobile Internet application [J]. Chinese Journal of Computers, 2018, 41(5): 1052-1067 (in Chinese)
(陈立全, 朱政, 王慕阳, 等. 适用于移动互联网的门限群签名方案[J]. 计算机学报, 2018, 41(5): 1052-1067)

[25] Poon J, Dryja T. The bitcoin lightning network: Scalable off-chain instant payments [OL]. [2017-11-12]. http://the-blockchain.com

Wang Zuan, born in 1992. PhD candidate in the School of Computer Science & Technology, Huazhong University of Science and Technology, Wuhan, China. Received his MS degree in computer science and technology from Guizhou University in 2019. Student member of CCF. His main research interests include information security, blockchain, query processing and privacy.

Tian Youliang, born in 1982. PhD, professor, PhD supervisor in the College of Computer Science & Technology, Guizhou University, Guiyang, China. His main research interests include algorithmic game theory, cryptography and security protocols, big data security and privacy protection, blockchain and electronic currency etc.

Yue Chaoyue, born in 1992. Received his MS degree in computational mathematics from Guizhou University in 2019. His main research interests include rational outsourcing computing and cryptography theory, etc.

Zhang Duo, born in 1987. PhD candidate, lecturer in the College of Mathematics and Statistics. His main reaserch interests include the cryptography, information security.