软件学报 ISSN 1000-9825, CODEN RUXUEW
Journal of Software,2019,30(9):2593−2607 [doi: 10.13328/j.cnki.jos.005772]

E-mail: jos@iscas.ac.cn
http://www.jos.org.cn
Tel: +86-10-62562563

基于动态授权的信任度证明机制*

黄建华, 夏 旭, 李忠诚, 李建华, 郑 红

(华东理工大学 信息科学与工程学院,上海 200237)

通讯作者: 黄建华, E-mail: jhhuang@ecust.edu.cn

摘 要: 提出一种基于动态授权的信任证明机制(proof of trust,简称 PoT),并在该机制的基础上修正了现有区块生成策略中存在的诸如权益粉碎攻击和贿赂攻击等问题.PoT 将网络中的节点分为矿工节点和基本权益代表(stakeholder)节点,根据节点参与创建区块的行为赋予其相应的信任度,stakeholder 节点对区块进行签名操作并赋予区块信任度,最终根据区块所获得信任度权重竞争上链.同时,还针对贿赂攻击和常见的权益累积攻击的攻击成本以及系统对于攻击的反应进行了分析.仿真实验的结果表明,PoT 机制在应对权益粉碎攻击、贿赂攻击以及权益累积攻击方面相比于传统权益证明机制有着显著优势.

关键词: 区块链;比特币;共识机制;信任证明;信任度

中图法分类号: TP309

中文引用格式: 黄建华,夏旭,李忠诚,李建华,郑红.基于动态授权的信任度证明机制.软件学报,2019,30(9):2593−2607. http://www.jos.org.cn/1000-9825/5772.htm

英文引用格式: Huang JH, Xia X, Li ZC, Li JH, Zheng H. Proof of trust: Mechanism of trust degree based on dynamic authorization. Ruan Jian Xue Bao/Journal of Software, 2019,30(9):2593−2607 (in Chinese). http://www.jos.org.cn/1000-9825/5772.htm

Proof of Trust: Mechanism of Trust Degree Based on Dynamic Authorization

HUANG Jian-Hua, XIA Xu, LI Zhong-Cheng, LI Jian-Hua, ZHENG Hong

(School of Information Science and Engineering, East China University of Science and Technology, Shanghai 200237, China)

Abstract: A trust degree mechanism based on dynamic authorization, proof of trust (PoT), is proposed in this study. Based on the mechanism, problems such as nothing-at-the-stake and bribe attack in the existing block generation strategies are fixed. There are two types of nodes in the network: miners and stakeholders. The trust degree is given according to the behavior of the node participating in the creation of a block. Once a node becomes a stakeholder of the network, it entrusts the block by signing its private key to the block. Finally, the blocks with trust degree compete with each other to be accepted as a legal extension of the blockchain. The cost of attacks against bribe attacks and common stake accumulation attacks, and the system's response to attacks is also analyzed. Simulation results show that the PoT mechanism can defend more efficiently against nothing-at-the-stake attack, bribe attack, and stake accumulation attack compared to proof of stake.

Key words: blockchain; bitcoin; consensus mechanism; proof of trust; trust degree

自 2008 年比特币[1]诞生伊始,比特币的底层技术——区块链技术开始进入人们视野.这种加密公共账本技术具有去中心化、防篡改和可追溯等特性,激发了业界对于区块链技术的研究热情,由此也产生了众多的数字

* 基金项目: 国家自然科学基金(61472139); 国家重点研发计划(2016YFA0502300)

Foundation item: National Natural Science Foundation of China (61472139); National Key Research and Development Plan Task of China (2016YFA0502300)

本文由"区块链数据管理"专题特约编辑于戈教授、牛保宁教授、金澈清教授推荐.

收稿时间: 2018-06-09; 修改时间: 2018-08-28; 采用时间: 2018-12-14; jos 在线出版时间: 2019-04-10

CNKI 网络优先出版: 2019-04-09 17:32:17, http://kns.cnki.net/kcms/detail/11.2560.TP.20190409.1732.002.html

货币加密技术,如以太币(Ether)[2]、点点币(PPCoin)[3]等,以及衍生出来的用于区块扩容的闪电网络(lightning network)[4].2015 年,Linux 基金会发起 HyperLedger 项目,其中最著名的是 Fabric 项目,Fabric 中没有挖矿机制,也没有使用代币作为激励机制,它是有准入资格授权的私有区块链网络,Fabric 的成员要在会员服务提供商进行注册[5].文献[6]详细介绍了基于区块链的平行社会发展趋势,讨论了智能合约的理念、应用和意义.针对第三方机构利用大量用户隐私数据来提供个性化定制服务导致用户个人隐私泄露的问题,文献[7]提出了基于区块链的个人数据保护系统,使用户能够在享受个性化定制服务的同时保护个人信息.但是,在点对点网络中面临着广播带来的网络开销较大问题,各个节点所观察到的交易事务先后顺序不可能完全一致.因此,区块链系统需要设计一种机制,对在一定时间内发生事务的先后顺序进行共识,这种对事务的先后顺序达成共识的算法就是共识机制.区块链分为公有链、联盟链和私有链:公有链主流的共识机制是工作量证明(proof of work,简称 PoW)和权益证明(proof of stake,简称 PoS),私有链或者联盟链的共识机制以实用型拜占庭容错协议(practical Byzantine fault tolerance,简称 PBFT)为主.以 PoW 为基础的加密货币可能会遭受双重支付攻击,为了降低风险,交易通常需要等待一定数量的确认区块(6 个).但是,这使得拒绝服务攻击(DoS)有了实现的可能,例如,攻击者可以发起很多低价值的交易来冲击网络.2015 年 7 月,就有一次针对比特币网络的洪泛攻击[8].比特币系统的另一问题就是能耗巨大,2017 年,整个比特币系统至少消耗 2.55GW 电力,并且未来可能达到 7.67GW,与奥地利全年耗电量相当[9,10].PoW 机制高昂的计算代价使其难以满足一些每秒高达数万笔交易的系统需求.目前,比特币社区正在尝试使用闪电网络等解决方案,以改善网络的吞吐量并降低耗电量.为了提高区块链网络交易吞吐量,King 于 2012 年创立了点点币,这是第 1 种基于 PoS 的加密货币.PoS 的提出虽然提高了网络吞吐量,但是带来了诸如短程攻击(贿赂攻击)、币龄累积攻击等新问题.PBFT 虽然可以每秒支持数千笔交易,但较低的节点可扩展性和较高的网络开销也使得 PBFT 在公有链领域应用范围有限.但是 PBFT 在联盟区块链方面应用广泛,典型的应用有腾讯公司发布的可信区块链平台 TrustSQL 以及 Linux 基金会发起的 Hyperledger Fabric 项目.

本文分析了 PoW 机制和 POS 机制的优点和不足,提出基于信任度证明的共识机制(proof of trust,简称 PoT),旨在解决权益证明机制中存在的易受贿赂攻击、币龄累积攻击以及工作量证明机制中存在的自私挖矿问题,并对 PoT 性能以及安全性进行了测试和分析.结果表明,PoT 的效率较 PoW 有较大提高.同时,对于贿赂攻击、权益粉碎攻击以及权益累积攻击,比 PoS 有更高的防范能力.

1 共识机制

共识机制的目标是使所有的诚实节点保存一致的区块链视图,在尽可能短的时间内建立安全和不可篡改的去中心化系统.目前存在的共识机制主要分为 PoW 和 PoS,其中,PoW 是区块链最早使用的共识机制,PoS 的概念则是由 2012 年出现的点点币引出的.

1.1 工作量证明机制(PoW)

比特币系统是区块链技术的首个应用,其采用的 PoW 机制使得区块的产生具有计算方面的难度.比特币系统平均每 10 分钟产生一个区块,每个节点都收集新的交易数据,并试图根据这些交易生成新的区块.PoW 解决共识问题的基本思路是寻找随机数(nonce),该随机数要使得给定区块的哈希值前部分出现所需的足够数量的 0,而找到这个 nonce 所需要的工作量与 0 的数目呈指数增长.矿工节点进行循环的 SHA-256 计算,最先找到这个 nonce 的节点向全网广播其工作量证明和新产生的区块,其他节点验证成功后就接受该区块,然后跟随在该区块的末尾制造新的区块,计算出结果的节点获取比特币作为奖励.虽然这种机制截至目前为止被证明是安全的,但是任何拥有巨大算力(超过 51%算力)的组织或者国家都有可能制造一个更长的区块链.尤其是在攻击者购买算力更强的矿机(ASIC)[11]之后,他将获取比一般矿工更强的算力.

针对比特币系统的一个可能的攻击就是自私挖矿(selfish mining)[12],目的是获得更大利润.自私挖矿的攻击者挖到新区块后不在第一时间公布,其他诚实矿工因为不知道新区块的存在,会继续在旧区块基础上挖矿.等到攻击者挖到第 2 个区块后,便会同时公布手中藏着的两个区块,这时,区块链就出现了分叉.只要攻击者比诚实矿工多挖一枚区块,攻击者所在的分叉就是最长链.自私挖矿的攻击者只需要拥有全网 1/3 的算力,就可以保证

自己获得更多的收益,相比51%攻击,自私挖矿显得更容易.作为矿工,在比特币规则中一般都会采用有利于自己的自私挖矿策略.事实上,当有节点拥有超过25%算力的时候,比特币的安全性就不能简单地以51%为阈值来考虑[13],因为不能保证此时所有的矿工都遵守规则.但是在本文提出的PoT机制中,产生区块不需要投入过多的算力资源,这种攻击反而变得没有效率.

1.2 权益证明机制

权益证明的核心思想是产生区块的难度与节点在网络中所占权益成反比,即:所持权益越多,越容易产生区块.这是一种效率更高的共识算法,使区块链无需高昂的硬件和电力挖矿成本就能正常运行.

权益证明主要有两大类:一种是基于链的权益证明,其模仿工作量证明机制,随机地为权益人(stakeholder)分配创建区块的权力,典型的有PPCoin、黑币(blackcoin)[14]、活动链(CoA)[15]、DPoS[16]和PoA[17];另一种是基于拜占庭容错的权益证明,在该机制中,只要有超过2/3的节点遵循协议,无论网络延时如何,协议都可以正常运行,典型的有Tendermint[18]和Casper[19].

在基于链的权益证明机制的虚拟币PPCoin,Clockcoin[20]和Novacoin[21]中,区块的创建是通过消耗币龄(coin age)来完成的.该协议被诟病的地方就在于:即使节点没有连接到网络,币龄也会增加.当前的系统事实上鼓励节点滥用这一机制,它们平时保持离线,只在累积了可观的币龄以后才连线以获得利息,然后再关闭连接.攻击者可以利用这一点,当其所持权益足够大时,对区块链进行分叉并达成双花.区块生成后,币龄就会归零,攻击者必须再次累积币龄才能继续攻击.VeriCoin[22]使用基于币龄的权益时间(stake time)来对节点所持权益进行度量,并且当节点不再参与共识时,其权益时间就开始衰减.Ouroboros[23]使用了一种新的奖励机制来增加对节点诚实行为的奖励,同时还使用了安全多方计算来保持节点中领导者的不可预测性,但是这种方法需要网络中验证节点之间的协调.

1.3 其他共识机制

文献[24]基于可信执行环境(trust execution environments)提出了共识机制proof of luck,该机制运行在支持SGX的CPU上,用来抵御挖矿对于能源的消耗,但是算法的执行依赖于Intel的特制CPU,违背了区块链的去中心化思想.文献[25]尝试用一种空间证明(proof of space)的概念来取代PoW,并且已经在区块链的框架背景下进行了专门研究.在空间证明中,证明者希望运用计算机存储资源代替PoW中的算力资源进行证明.空间证明虽然利用了一定的硬件资源,但是随着时间的推移,对硬件资源的消耗量会减少.类似地,文献[26]也提出了时空证明(proof of space-time)算法,但无论是空间证明还是时空证明都需要昂贵的硬件资源,到最后都会出现硬件资源集中化的现象.文献[27]提出了一种有趣的燃烧货币机制PoB(proof of burn),该算法通过将代币转移到不可逆转的地址上以销毁代币,节点燃烧的代币量与被选中挖到下一个块的概率成正比.在PoB中,随着时间的推移,节点在系统中所持的份额可能会减少,这会驱动节点燃烧货币来获取更多的挖矿机会.这种机制虽然是一个不错的尝试,但是造成了代币资源的浪费,并且挖矿的能力会逐渐被那些掌握更多资源并且愿意燃烧代币的人所掌控.文献[28]提出了一个重要性证明(proof of importance)算法,该算法运行时,节点需要提供自己的重要性才能获取出块权.在重要性证明下,节点所持权益不再是重要性的主要因素,取而代之的是节点的交易量以及交易双方的关系.在重要性证明中,根据钱包的交易次数和货币资产来评估节点的重要性.但是该协议可能会鼓励节点之间相互串通互刷交易量,同时,大资产节点的频繁交易也会造成重要性中心化的问题.

2 基于信任度的共识机制

公有链假定所有节点都是不可信的,产生区块的策略主要有两种:基于算力的PoW机制和基于权益的PoS机制.在PoS中,每个节点的可信度与它本身所持的资源(比如加密货币数量)呈正相关,这就决定了该节点在网络中所占的权重(以票数计).这种机制会带来许多严重后果,最直接的就是权益粉碎攻击[29,30].PoS的一大优势就是所持权益越多者越愿意维护系统,反之,所持权益越少责任也就越少.假设矿工只有1%的权益,其成功的概率只有1%,那么该节点可以尽可能尝试分叉,因为在PoS中分叉并不消耗任何资源.在比特币系统采用的PoW

机制中,创建分叉得不偿失,因为必须为此付出大量算力资源.目前,比特币网络每 10 分钟产生一个区块并奖励 12.5 个比特币,即使耗费大量电力,挖矿仍然是一件有利可图的事情,但是每产生 21 万个区块后,收益会减半.当收益不足以维持挖矿所耗费的电力成本时,矿工们就不再有足够的动机去维持区块链的一致性.这就是经济学领域所说的公地悲剧[31].中本聪预见到这个事情的发生,提出了交易费率的解决办法[1].但是在公地悲剧中,参与者有机会自行其是,以牺牲他人的代价来实现自己的利益最大化,所以希望其他节点支付相应费用.每一个理性的矿工总是会采取这样的行动,因为它只寻求自身最优解.如果网络中每一个个体都表现得很自私,那么整个网络环境安全性的下降就在所难免.

迄今为止,权益证明仍然是对区块链公地悲剧的唯一解决方案.为了避免公地悲剧以及权益粉碎攻击带来的网络安全问题,本文提出了基于信任度证明的 PoT 共识机制.由于采用 PoW 共识的区块链网络因其计算上的难度而不易受到攻击,因此,PoT 中引入了少部分的工作量证明以避免权益粉碎攻击.有别于工作量证明机制中的低吞吐量和巨大的资源耗费,以及纯权益证明机制中币龄累积所造成的权益中心化和易受权益粉碎攻击,PoT 旨在建立一个高吞吐量、安全和低资源消耗的去中心化区块链网络.

PoT 的运行从时间上被划分为一系列周期(epoch),每一个 epoch 又被划分为多个时隙(slot),一个 slot 内产生一个区块,权益的计算以每个 epoch 开始前的历史计算.在每个 epoch 开始时,矿工节点都会计算生成一个满足当前难度的空区块,通过这个空区块衍生出一组参与者(participants)集合$\{P_1,P_2,P_3,\ldots,P_T\}$,然后,每个 slot 均从这些 Participants 集合中随机选取 N 个节点作为基本权益代表(stakeholder),这些代表用集合$\{S_1,S_2,S_3,S_4,\ldots,S_N\}$表示,这里 $N<T$.通过节点在每个 slot 中的诚实签名与恶意签名行为的判别,进行动态的信任度授信.本文基于 logistic 回归模型提出了节点信任度的动态度量方法,见公式(1).

$$trust_{cur}^{(i)}=\frac{1}{1+e^{-\alpha\left(\sum\limits_{x=0}^{n-1}\vartheta_x-\gamma\times\sum\limits_{x=0}^{n-1}\tau_x\right)}} \tag{1}$$

其中,$trust_{cur}^{(i)}$ 是在投票前,系统根据节点 i 之前的行为给予节点的当前信任度;n 表示当前第 n 个 slot;α是步长,即该节点累计参与的 slot 数量;ϑ_x 表示节点 i 在第 x 个 slot 中是否正常参与投票,正常为 1,反之为 0;τ_x 表示节点 i 在第 x 个 slot 中是否恶意投票,恶意为 1,反之为 0;γ表示对于恶意投票的惩罚权重,由用户设置,γ值越大,对节点恶意投票的惩罚就越大.

logistic 回归模型在对数增长期节点的信任度的增长是相当快的,不利于合理地判断节点信任的增长.为了避免出现这种情况,本文提出了对 logistic 回归模型产生的信任度进行修正的算法,根据节点当前信任度和上一轮投票时的信任度,对在投票时的信任度进行权重均衡.最终进行投票时的信任度度量公式如下:

$$trust(i)_h^t=\beta\times trust_{cur}^{(i)}+(1-\beta)\times trust(i)_{h-1}^t \tag{2}$$

其中,h 表示当前 epoch 内第 h 个 slot.节点在第 t 个 epoch 中的第 1 个 slot 开始时的信任度与第 t–1 个 epoch 的最后一个 slot 结束时的信任度相等,即 $trust_0^t=trust_{last}^{t-1}$,并且 $trust_0^0=\frac{1}{1+e^{-\alpha(0-0)}}=0.5$.通过$\beta$可以对信任度的增加速率进行修正,使其增长不会太快,避免在网络初期阶段的信任度中心化.初始时,β值为 1,因为刚开始并不知道节点是否会有作恶倾向.

β的变化基于累计偏差 $\xi_h^t trust$,具体变化算法由公式(3)确定:

$$\beta=threshold+c\times\frac{\delta_h^t trust^{(i)}}{1+\xi_h^t trust} \tag{3}$$

同样地,在第 t 个 epoch 开始时的信任度累积偏差与第 t–1 个 epoch 的最后一次参与共识时的信任累积偏差相等,即 $\xi_0^t trust=\xi_{last}^{t-1}trust$,并且 $\xi_0^0 trust=0$.参数 c 是用户定义的参数,用于控制对节点的最近行为的反应权重.$threshold$ 是为了防止β过于饱和趋近于 1 而设置的阈值,其初始值为 0.25(在社会学范畴中,对于人的历史信任度比当前信任度能更好地分析人的信誉.$threshold$ 初始值设为 0.25 可以在防止β过于饱和趋近于 1 的同时,也能让 $trust(i)_h^t$ 不会过分倚重当前信度函数直接评价所得的信任度).$\delta_h^t trust$ 表示信任度的偏差,其计算方法见公式(4).

$$\delta_h^t trust = | trust_{h-1}^t - trust_{cur}^{(i)} | \tag{4}$$

在第 t 个 epoch,节点对第 h 个 slot 进行共识时的信任度偏差等于当前信任度与对第 h–1 个 slot 进行投票时的投票信任度的绝对值之差.最终的累积偏差见公式(5).

$$\xi_h^t trust = c \times \delta_h^t trust + (1-c) \times \xi_{h-1}^t trust \tag{5}$$

从公式(5)可以看出:c 值越大,说明用户给予的最近的信任度偏差的权重比之前累积信任度偏差要高.

2.1 节点行为判别策略

传统的共识机制单纯依靠提高准入门槛,比如算力或者权益来维护区块链网络的稳定与安全,但是算力和基于币龄的权益都会使区块链网络倾向于中心化.本文提出了一套完整的对于节点行为的判别策略,通过对节点运行机制的检测与判别,以识别恶意的节点,并进行信任度惩罚.

本文将节点行为定义为#good 和#bad 两种.

- #good:每一个 stakeholder 对于区块的签名被认为是对该区块的投票,投票时使用自己的私钥进行签名,可以用公钥去验证.只要节点参与生成的区块的签名合法,满足当前难度,具备竞争上链资格,则将其行为定义为#good;
- #bad:如果前 N–1 个 stakeholder 发现它要签名的区块存在问题,那么根据协议就不予签名.如果仍要签名,那么具有区块打包权的第 N 个 stakeholder 在将区块打包之前完全可以决定是否打包区块.如果不打包,则认为该区块无效,所有对该区块进行的签名操作都被视为无效,这将消耗这些 stakeholder 的信任度.如果打包成功并且与其他区块一起进行信任度竞争,网络中的其他节点会对区块的签名进行验证.如果区块中有的签名是非法的或者区块头哈希不正确,则认为该区块非法.对该区块进行签名操作的所有 stakeholder 均被认为是恶意的,使用相应的惩罚机制进行信任度惩罚.

基于经典的 PBFT 的 2/3 原则,可以设定一个投票上链的阈值.只有在区块中拥有超过 2/3 的 stakeholder 投票的情况下才具有上链资格.节点成为 stakeholder 的概率由公式(6)计算:

$$Prob(S_{(i)}^{\exp}) = \frac{\sum_{t=1}^{n} \vartheta_t^{(i)} \cdot \mu_t}{\sum_{t=1}^{n} \sigma_t} \tag{6}$$

其中,$\vartheta_t^{(i)}$ 表示第 t 个 epoch 内节点 i 成功参与共识的次数,μ_t 表示第 t 个 epoch 内成功参与共识可获得的代币奖励,σ_t 表示第 t 个 epoch 内所发放的所有代币奖励.

2.2 区块生成

在 PoT 中,区块的产生过程被一分为二:首先,通过简单难度的工作量证明产生一个空区块;然后,通过 stakeholder 的投票来确定该区块是否有上链资格.在区块产生过程中引入计算以求规避权益粉碎攻击,在将交易放入区块打包广播到网络的过程中,引入基于链的权益证明机制,所持信任度高的区块相比于其他区块上链机会更大.相比于单纯基于算力的竞争,这种方法可以大幅度提高网络的吞吐量,减少网络的资源消耗.其具体架构如图 1 所示.

其中,stakeholder 由 PoT 的跟随币机制衍生出来.在其产生后对其认可的空区块进行私钥签名,最后一个 stakeholder 即 $stakeholder_N$ 将其认可的交易进行打包,满足要求的区块被打包之后上就可以上链.

PoT 共识机制产生区块的过程如下.

(1) 首先,每个矿工都尝试去产生一个区块头,这个区块头中包含了先前区块的哈希(B_{prev})、矿工地址($Adress_{miner}$)、该区块在区块链中的索引(height)以及一个随机值(nonce).同时,区块头中不能包含任何交易.进行工作量证明计算.当矿工生成区块头之后,如果符合当前网络难度目标,就向全网广播该区块头;

(2) 所有节点将这个区块头的散列值作为确定 T 个 participants 的数据.具体算法是:通过将 T 个固定的值

与区块头的散列值进行哈希运算,得到的第 i 个结果 x 将被用来确定第 i 个 participant.这个过程就是在 PoT 中引入一个跟随币机制,有意向成为 participant 的节点将所有未花费的输出(UTXO)按照字典的方式进行排序,这里假设 UTXO 不为空,具体格式为{*NodeID*,*Coin*},其中,*NodeID* 为节点的公钥地址,*Coin* 表示节点所持币的数量.同时,*CurrentID* 表示当前 participant 的序号,并且 $CurrentID \leqslant T$.具体过程如下:节点选取一个其值介于 1 和系统中 UTXO 总数量之间的随机数 x,为了找到第 x 个币的持有者,节点找到一个最小的 i,使得列表从最开始到 i 的节点所持 UTXO 代币数量不小于 x.这样,第 i 个地址就是第 x 个币的拥有者;

(3) 在确定了 T 个 participants(参与者)之后.在每一个 slot 中,都会从中随机选取 N 个节点作为 stakeholder 参与共识,这里 $N<T$.每个在线的权益代表检查这个矿工广播的区块头是否有效,一旦认为有效,则该权益代表就检查它自己是否是 N 个权益代表之一,如果是前 N–1 个权益代表,那么它就在区块头上用自己的私钥进行签名.该过程是对区块进行 stakeholder 信任度(*trust*)的权重,并将其签名进行广播.当节点确认自己是第 N 个权益代表,它就将尽可能多地交易打包进区块,再加上前 N–1 个签名以及自己的签名来扩展区块头,并最终生成该区块的哈希值;

(4) 第 N 个 stakeholder 向网络广播打包后的区块,当其他节点收到这个区块并验证是有效时,这些节点将该区块认为是区块链的合法扩展.考虑到以后的网络会拓展得很大,所以如果有两个区块同时在全网传播,那么两个区块就进行基于链的权益证明竞争上链.当区块被扩展到了链上,则给该区块签名的所有 stakeholder 的行为均被定义为#good;

(5) 区块产生之后的奖励由第 N 个 stakeholder 收集,并且将之分享给矿工和前 N–1 个 stakeholder.

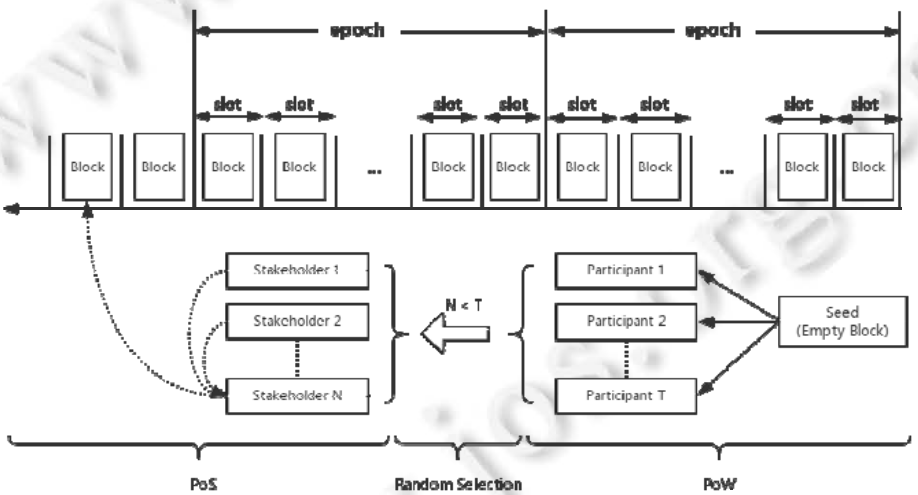


Fig.1 Proof of trust framework basedon dynamic authorization

图 1 基于动态授权的信任证明机制

共识生成区块的伪代码算法见算法 1.

算法 1. Proof of Trust Consensus.

Input: B_{prev} previous block; $Adress_{miner}$: The miner's public address; *Height*: Height relative to the genesis block; Nonce; *CurrentID*: The index of the stakeholder; *M*: User-defined parameters; *D*: The degree of difficulty that the network needs to satisfy; *UTXO_List*: The dictionary which is defined with {*NodeID*:*Coin*};

Output: A block with transactions.

1: **procedure** *CreateBlockHeader*

2: **while** $hash(hash(B_{prev}),Adress_{miner},Height,Nonce)>M/D$ **do**

```
        Nonce←Nonce+1
    end while
    Address←Adress_miner
    PreviousHash←B_prev
    Height←Height+1
    CurrentNonce←Nonce
    BlockHeader←(PreviousHash,Address,Height,CurrentNonce)
    return BlockHeader
end procedure
procedure SelectParticipants
    //Select Tparticipants
    CurrentID←1
    while CurrentID≤T do
        x←hash(hash(BlockHeader),CurrentID)
        choose x as x^th minted coin
        Coins←0
        for i in UTXO_List
            Coins+=i.Coin
            if Coins≥x
                participants.append(i.NodeID)
                break
            end if
        end for
        CurrentID←CurrentID+1
    end while
    return participants
end procedure
procedure WrapBlock
  //Wrap the block
  if hash(hash(B_prev),Adress_miner,Nonce)<M/D
    stakeholder←random.sample(participants,N)
    if node in stakeholder
        Signature(BlockHeader)
        if node.index==N
            Block.wrap(transaction)
            //The N^th stakeholder creates a warpped block that includes as many transcations as it wishes to
            include
        end if
    end if
  end if
  return Block
end procedure
```

2.3 信用消耗

信任度是节点诚实参与区块生成而获取的奖励,同时也是节点信誉的表现形式.为了保持网络中在线节点的数量,PoT 中引入了信用消耗机制.同时,因为 logistic 回归模型的特性,节点的信任度是有信用上限的.

(1) 信用消耗

信用消耗是为了保证节点的参与度而设置,而不是为了让节点以消耗信用度的方式参与区块的生成.因为当网络中的 stakeholder 过少时,网络的安全与稳定就得不到保证.在本机制中,节点的信用度会随着时间的推移而降低.即使节点不是 stakeholder,为了保证网络安全,它也要参与区块的验证.只要参与区块的验证,就不会产生信用消耗.节点 i 的信任度具体消耗算法如公式(7)所示:

$$trust_{cur}^{(i)}=\begin{cases}\dfrac{1}{1+\mathrm{e}^{-\alpha\left(\sum_{x=0}^{n-1}\vartheta_x-\gamma\times\sum_{x=0}^{n-1}\tau_x\right)}}, & \text{if } \Delta B=0\\ trust_{last}^{(i)}\times\mathrm{e}^{-D\cdot\Delta B}, & \text{otherwise}\end{cases} \tag{7}$$

其中,ΔB 表示区块间隔,即上次参与生成的区块与当前区块之间的间隔(从 0 开始),算法如下:

$$\Delta B=B_{current}-B_{previous} \tag{8}$$

如果刚好两个区块是连续的,则ΔB=0.此时,节点以当前信任度继续参与区块生成,信任消耗函数就不会执行,这就最大程度地保证了网络中节点积极在线参与区块的验证.D 值表示当前一段时间内网络的难度值,D 的值越大,就表示越需要多次地反复尝试才能找到有效的区块.D 的值根据网络中的出块速率进行动态调节,最终将网络的出块速率维持在一个稳定的水平.难度的提升,意味着区块上链需要更多的信任度加权,上链成本就会增加,理性节点可能会选择暂时不参与区块生成,以寻求网络难度更低、机会更大的时候参与区块生成.当节点参与度过低时,恶意节点成功的概率也就越大.因此,在网络难度提高的同时,也增大对于不参与区块生成的节点的信任消耗,将有助于提高节点的参与度,维护区块链网络的运行安全.

(2) 信用上限

PoT 中的节点可以不通过自身所持资源来确定其拥有的投票权重,并且其所持信任度上限最高为 1,一定程度上解决了原始 PoS 协议中的币龄累积导致的中心化问题.传统的 PoS 机制中,投票权重的增长是线性的,PoT 中信任度增长呈非线型的,信任度的提升速率随着时间的推移会下降,最后趋近于 0,因此不会造成单一节点信任度过高导致的网络中心化问题.

2.4 投票机制

在 PoT 中,原先的基于币龄或者加密货币所有权的权益被修改为基于节点自身的信任度的权益,不再依赖于节点自身所持资源.stakeholder 通过对于区块的签名来赋予区块信任度,信任度越高,则得到哈希结果的速度就越快,计算公式见公式(9).

$$hash(hash(B_{prev}),Block_{cur},A,t)\leqslant\delta_t\cdot trust(A)\cdot M/D \tag{9}$$

这里,B_{prev} 是节点投票区块的前置区块;投票节点的地址是 A,它的信任度为 $trust(A)$;$Block_{cur}$ 是 $stakeholder_N$ 打包后的区块;t 是世界标准时间(UTC)的时间戳;$M\in[1,D]$是一个常数,可以根据网络实时状况动态变化;D 值代表难度;δ_t 则是从 B_{prev} 创建以后所经过的时间.当一个区块被上传到整个网络之后,最初区块满足公式(9)的可能性是很低的;但是随着时间的推移,成功概率将逐渐增加,首先计算出来的区块才能成为区块链的合法扩展.

对于地址为 A 的 stakeholder 节点,其信任度是被锁定的,即该节点一次只允许投票一次.基于所提供的地址 A 和上述公式的时间戳 t,stakeholder 就能保证其签名的有效性.

3 攻击成本分析

3.1 贿赂攻击

传统双花攻击场景如下.

(1) 攻击者发起一个之后会被他自己撤销的一个交易;

(2) 在该交易之后,攻击者在该交易所在区块之前的那个区块上开始建立侧链;

(3) 当新交易进入区块并且获得了足够的确认数目(6 个区块)且攻击者的侧链长度超过主链时,攻击者的侧链就成为了主链,攻击者发起的第 1 笔交易被判定为无效,双花攻击成功.

要想成功地进行双花攻击,攻击者必须在整个攻击过程中控制超过 50%的网络资源(PoW 算力、PoS 权益).相对于控制 51%的算力,控制 51%的流通代币是非常困难的[3].但是这并不意味着在权益证明中就无法展开攻击,攻击者可以提供报酬给那些愿意在他指定的区块上铸造新区块的节点.如果攻击失败,参加攻击的用户并不会遭受太多损失.对于攻击者而言,只要贿赂的金额小于商品交易价格,那么总是有利可图的.

在 PoT 中,如果要进行贿赂攻击是不可行的,因为每次生成区块的 stakeholder 都不相同,并且在区块产生之前 stakeholder 是不确定的.一旦被发现参与恶意投票,对于信任度的惩罚是极高的,而且只有第 N 个 stakeholder 具有对交易进行打包的权力.除非攻击者提前找到第 N 个 stakeholder,一旦 $stakeholder_N$ 对无效交易进行打包操作,就将受到信任度惩罚.因惩罚系数 γ 的存在,高昂的信任度惩罚对其来说是不可承受的.证明过程见公式(10)~公式(12).

$$trust_{\vartheta_x}^{(i)}=\frac{1}{1+\mathrm{e}^{-\alpha\left(\sum_{x=0}^{n-1}\vartheta_x\right)}} \tag{10}$$

$$trust_{\tau_x}^{(i)}=\frac{1}{1+\mathrm{e}^{-\alpha\left(\sum_{x=0}^{n-1}\vartheta_x-\gamma\times\sum_{x=0}^{n-1}\tau_x\right)}} \tag{11}$$

$$\lim_{n\to\infty}Rat_{\tau_x,\vartheta_x}^{(i)}=\lim_{n\to\infty}\frac{1+\mathrm{e}^{-\alpha\left(\sum_{x=0}^{n-1}\vartheta_x\right)}}{1+\mathrm{e}^{-\alpha\left(\sum_{x=0}^{n-1}\vartheta_x-\gamma\times\sum_{x=0}^{n-1}\tau_x\right)}}=0 \tag{12}$$

公式(10)是节点 i 诚实参与共识所获取的信任度,公式(11)是节点 i 在诚实投票之后进行恶意投票被系统识别后更新的信任度,公式(12)是节点 i 诚实投票后进行恶意投票的信任度与之前诚实投票的信任度所占比例.

假设 t=2,γ=2,ϑ_x=τ_x=α=1 时,$Rat_{\tau_x,\vartheta_x}^{(i)}=\frac{1+\mathrm{e}^{-\alpha\cdot\vartheta_x}}{1+\mathrm{e}^{-\alpha(\vartheta_x-\gamma\cdot\tau_x)}}=\frac{1+\mathrm{e}^{-\alpha}}{1+\mathrm{e}^{\alpha\gamma-\alpha}}=0.36$.在 epoch 的第 2 个 slot 中,在诚实参与共识一次之后,恶意攻击者进行恶意投票被系统识别后的信任度只有之前的 36%.并且这种信任度惩罚会随着轮数以及时间的递增而快速上升,α越大,惩罚越重.这种惩罚力度的存在,对任何理性节点都是难以接受的.

3.2 累积攻击

累积攻击最原始的版本是币龄累积攻击,是针对 PPCoin 和其他使用币龄作为用户权益的系统而发起的攻击.在后来的 PPCoin 版本中,UTXOs 的币龄都以 90 天为限制.在 Novacoin 和 BlackCoin 中,对于币龄同样也有限制.然而,通过限制币龄来大幅降低攻击的可能的同时,也减弱了以币龄作为权益的好处.

在 PoT 中,信任度的累积不是线性的,而是基于非线性的 logistic 回归模型.在 PoT 中,如果想要进行累积攻击,就需要对信任度进行累积.本文提出的修正 logistic 算法使得信任度的累积变得十分漫长,并且节点恶意行为一旦被发现,对节点的信任度惩罚力度将是任何理性节点都不可承受的,因此在 PoT 中,想要通过积累信任度发起攻击的收益不足以抵消其遭受的信任度惩罚损失.如果攻击者要绕过信任度,仅通过自身所持权益生成区块与其他区块进行上链竞争,其成功的概率也是相当低的.

证明:首先,攻击者想要控制 stakeholder 进行 2/3 投票.在拥有 n 个 stakeholder 节点的网络中,攻击者必须要控制至少 2/3 的 stakeholder 节点;同时,攻击者还需要最后一个 stakeholder 将自己捏造的虚假交易打包进区块中,即攻击者控制的 stakeholder 中必须有一个是交易打包者.因此,攻击者成功的总概率为

$$Suc_n^{(i)} = p\sum_{k=\left\lceil\frac{2n}{3}\right\rceil-1}^{n-1} C_{n-1}^{k} p^k (1-p)^{n-1-k} \tag{13}$$

p 表示成为 stakeholder 的概率.假设一个拥有 6 个 stakeholder 的网络,攻击者持有 20%的总权益,那么攻击者绕过信任度,成功上链竞争.那么他成功的概率为

$$Suc_n^{(i)} = 0.2\times(C_5^3\times 0.2^3\times 0.8^2 + C_5^4\times 0.2^4\times 0.8^1 + C_5^5\times 0.2^5) = 0.011 \tag{14}$$

相比其拥有的 20%的权益,区区 1%的成功率实在是微不足道的.

3.3 权益粉碎攻击

权益粉碎攻击是针对 PoS 特有的攻击方式,其具体场景如下:在运行 PoS 协议的网络中,如果某个节点所持权益很低(比如 1%),那么它成功生成区块的概率也就是 1%.任何一个理性的节点都愿意去尝试分叉,因为在纯 PoS 协议中,分叉不需要消耗任何资源,唯一消耗的就是币龄.如果该区块没有被接受,则币龄也不会消耗.尽管这样会造成整个网络的加密货币价值降低,但是因为该节点所占权益很少,所以它们并不在乎.

在 PoT 中,只有随机生成的 N 个 stakeholder 有权利扩展区块链,矿工只负责生成区块供 stakeholder 进行签名,并没有决定权.在制定决策时就很清楚,不会有二义性,具有很强的治理能力.正常情况下是不会经历任何分叉,因为 N 个 stakeholder 是合作生产区块而不是竞争.

4 实验分析

基于提出的 PoT 机制,在 Docker version 18.03.0-ce,build 0520e24 中实现了原型系统,实验环境为 Intel I7-4702MQ CPU 2.20GHz 和 16G 内存,操作系统为 64 位 Win10.通过搭建原型验证模型,验证 PoT 协议的共识时延能否随着时间的增长而降低以及对恶意节点的惩罚,并对节点信任度增长与消耗进行实验.

4.1 信任度增长

原型系统信任度增长采用改进后的 logistic 线性回归模型.网络中一共有 10 个矿工节点,其中 4 个作为 stakeholder.因为 stakeholder 节点每次的选取都是随机的,所以在每一个 slot 中,参与共识的 stakeholder 不尽相同,网络中节点信任度增长过程如图 2 所示.投票结果统计公式中常量 *threshold*=0.25,用户自定义常量 c 值分别为 0.1,0.5,0.9.

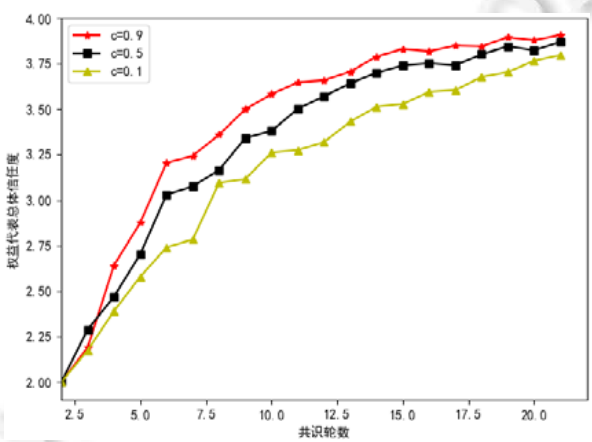


Fig.2 Trust increase in network nodes

图 2 网络节点信任度增长

图 2 表明:不同 c 值的信任度增长速率是不同的,但是最后都趋近于上限.c 值越大,即说明用户给予的最近的信任度偏差的权重比累积信任度偏差要高,从而最近时间片内的信任度增长率在总体信任度增长率中占比升高.经过多轮共识,网络中节点的信任度均会维持在一个恒定的水平,因此不会产生单个节点权益过大而导致

的权益中心化问题.

4.2 信任度惩罚

假设原型系统中所有 stakeholder 在其信任度到达高峰时保持离线状态,不再参与共识,整个网络将会变得不再安全,其总体信任度下降过程如图 3 所示.

可以看出:如果网络中被选出的 stakeholder 都不参与区块的生成过程,开始几轮其总体信任度还能保持基本稳定,但从第 5 轮开始,信任度明显下降,并呈现非线性的下降过程,在 17 轮后逐渐趋于 0.

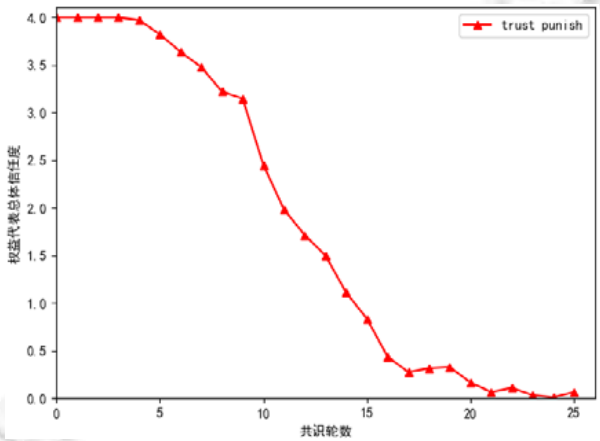


Fig.3 Trust consumption in network nodes

图 3 信任度消耗

4.3 共识时延

原型系统搭建了拥有 10 个节点的分布式网络,stakeholder 节点有 4 个.投票结果统计公式中常量的取值为:难度 D=4,5,M=2,一共进行 25 轮共识,并且对最终的时延结果进行了最小二乘曲线拟合,结果如图 4 所示.

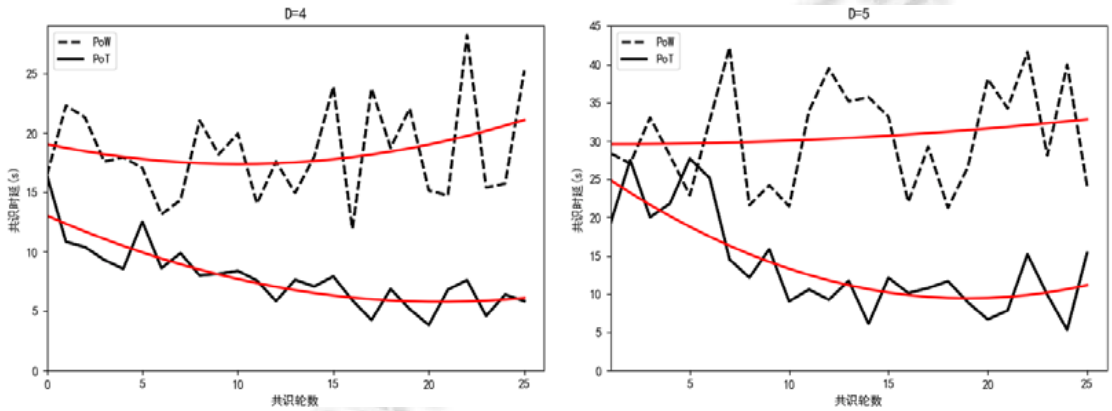


Fig.4 Time delay in consensus

图 4 共识时延对比图

图 4 表示在难度值 D 分别为 4 和 5 时,经过 25 轮之后,PoT 协议与的 PoW 协议的共识时延变化情况.共识时延表示区块链网络中的出块时间,即区块上链所经过的时间,时延单位为秒(s).虚线部分是 PoW 的共识时延变化过程,实线是 PoT 的共识时延变化过程.在此基础上分别进行了拟合,因为哈希计算的随机性,PoW 时延波动性很大,但是拟合的结果趋于稳定.这说明实验平台的算力是稳定的.相反,PoT 协议的共识时延随着共识轮数的增加而降低,最终会维持在稳定的水平.

图 5 表示在 D=4 时,网络中 stakeholder 节点数量的不同对于共识时延的影响.参与共识的 stakeholder 节点数量分别取 N=5,N=6,N=8.

由图 5 可知:随着网络中 stakeholder 节点数量的增加,网络共识时延会有所下降,最终会维持稳定的水平.但是 stakeholder 数量的增加不能是无限制的,当网络中 stakeholder 节点数量过多时,节点被攻击者贿赂的概率也将上升.同时,如果网络中 stakeholder 节点过少,网络共识时延将增大,导致 stakeholder 暴露时间过长,增大了 stakeholder 节点被攻击者贿赂的概率.图中曲线的波动是因为网络中每次参与共识的 stakeholder 的不确定造成了区块信任度的波动,从而最终导致共识时延的波动,但是共识时延都是呈下降趋势.

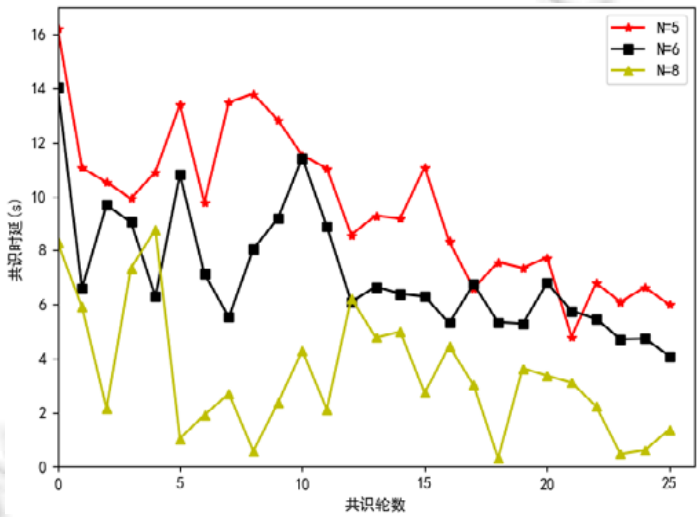


Fig.5 Effect of the number of stakeholder on time delay in consensus

图 5 stakeholder 数量对时延影响

4.4 节点数量对共识时延的影响

图 6 表示在 D=4,stakeholder 数量增长到 7 时,网络中节点数量的变化对于共识时延的影响.一共进行了 30 轮共识,普通节点数量分别为 20,50 和 100.

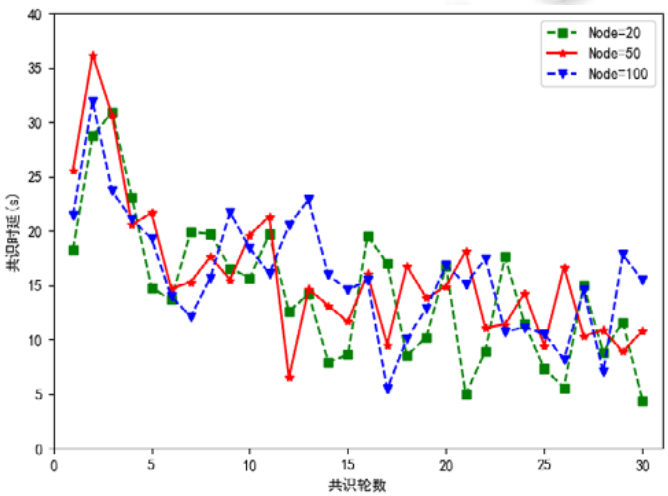


Fig.6 Effect of the number of nodes on time delay in consensus

图 6 节点数量对时延影响

由图 6 可知:随着网络中节点数量的增加,共识时延并没有发生特别大的改变.这是因为在 PoT 中,只有 stakeholder 才能决定区块是否上链,区块产生的难易程度与普通节点的数量没有直接关系.这也说明 PoT 具有一定的节点可扩展性,出块效率并不因普通节点数量的变化而变化.

4.5 惩罚系数

惩罚系数测试分别对节点行为所占不同比重以及不同惩罚系数下,节点在经过恶意投票之后信任度的下降比例进行实验验证,结果如图 7(a)~图 7(d)所示.在一个 epoch 中,当节点诚实行为占比较大时,比如图 7(a)中诚实行为占 70%,恶意行为占 30%,惩罚系数对于信任度下降比的影响很大:当惩罚系数较低时,如γ=1,节点仍然可以通过进行诚实投票来努力恢复自己的信任度;但是随着惩罚系数的增大,如γ=3 时,节点越来越难以恢复到作恶前的信任度.并且随着诚实行为所占比越来越少,例如当诚实行为仅占 50%时,信任度最高也只能维持在恶意投票之前的 50%.随着恶意投票行为占比的扩大,节点信任度下降速度也会随之增大.

由图 7(c)和图 7(d)可知:当恶意行为所占比重很大时,惩罚系数对于节点信任度的惩罚使得节点信任度下降极快,经过两至三个 epoch 信任度就下降为 0.因此,无论诚实行为所占比重如何,一旦被检测有恶意行为发生,其信任度的下降速率将是极快的,对于任何理性节点而言这都是难以承受的下降速率.

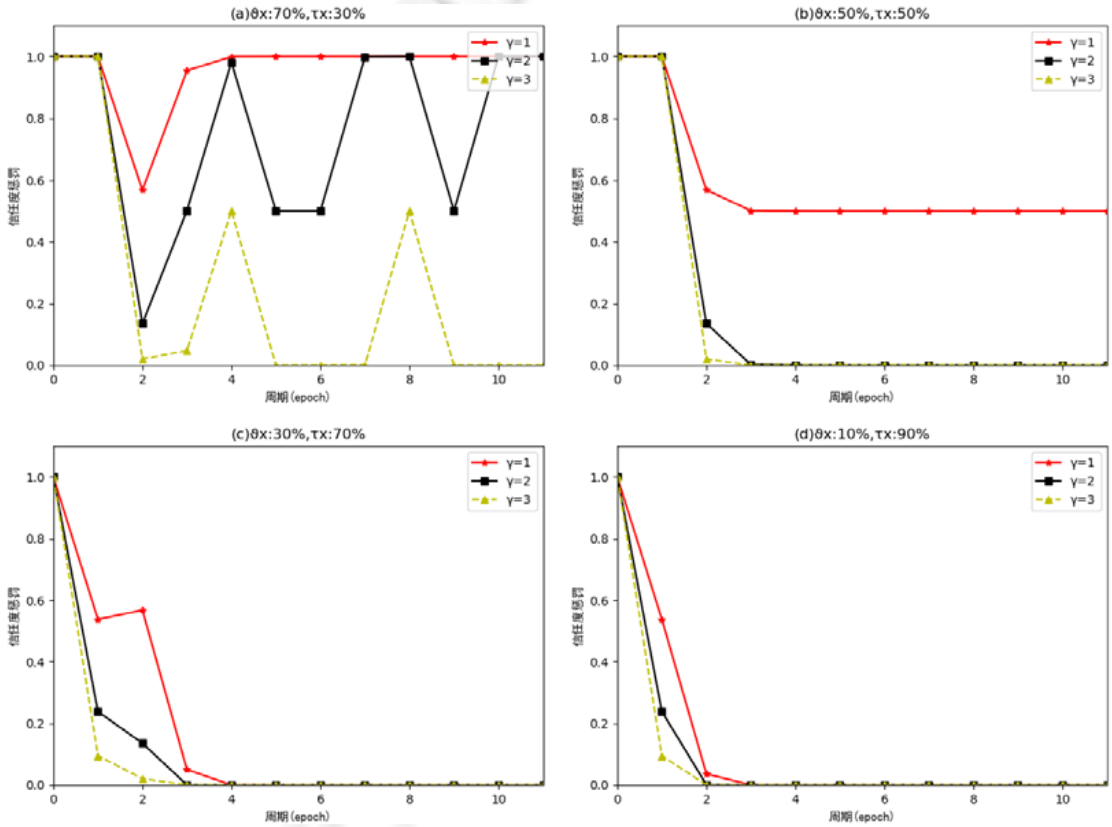


Fig.7 Trust penalty in network nodes

图 7 信任度惩罚

5 结束语

区块链是近年来研究的热点,许多行业在使用区块链技术进行行业内的技术革新.然而针对不同的应用场景,单一的共识机制是不足以满足所有业务需求的,不同业务场景采用的共识机制也不尽相同.本文针对现有共

识机制中存在的问题进行了研究与改进,解决了权益证明机制中存在的易受贿赂攻击、币龄累积攻击以及工作量证明机制中存在的自私挖矿等问题.与 PoW 相比,在保证网络安全的前提下,PoT 降低了共识时延.本文提供了一种共识机制的改进思路,并且通过实验对改进的共识机制的可行性和性能进行了分析和验证.结果表明:在共识时延方面,PoT 相比 PoW 有较大优势;在预防贿赂攻击、累积攻击以及权益粉碎攻击方面,相较于 PoS 也有着显著优势.此外,PoT 还可以实现维护网络拓扑结构、保持在线节点数量以及更高效的资源利用.

References:

[1] Nakamoto S. Bitcoin: A peer-to-peer electronic cash system. 2008.

[2] Buterin V. A next-generation smart contract and decentralized application platform. White Paper, 2014.

[3] King S, Nadal S. Ppcoin: Peer-to-peer crypto-currency with proof-of-stake. Self-Published Paper, 2012.

[4] Poon J, Dryja T. The bitcoin lightning network: Scalable off-chain instant payments. 2016. URL:https://lightning.network/lightning-network-paper.pdf

[5] Cachin C. Architecture of the hyperledgerblockchain fabric. In: Proc. of the Workshop on Distributed Cryptocurrencies and Consensus Ledgers. 2016.

[6] Yuan Y, Wang FY. Blockchain: The state of the art and future trends. Acta Automatica Sinica, 2016,42(4):481−494 (in Chinese with English abstract). [doi: 10.16383/j.aas.2016.c160158]

[7] Zyskind G, Nathan O. Decentralizing privacy: Using blockchain to protect personal data. In: Proc. of the 2015 IEEE Security and Privacy Workshops (SPW). IEEE, 2015. 180−184.

[8] July 2015 flood attack In: Bitcoin Wiki. 2015. https://en.bitcoin.it/wiki/July_2015_flood_attack

[9] Int'l Energy Agency. World energy statistics 2017. 2017. https://www.iea.org/publications/freepublications/publication/KeyWorld2017.pdf

[10] de Vries A. Bitcoin's growing energy problem. Joule, 2018,2(5):801−805.

[11] Hanke T. AsicBoost—A speedup for bitcoin mining. 2016.

[12] Eyal I. The miner's dilemma. Computer Science, 2014. 89−103.

[13] Sapirshtein A, Sompolinsky Y, Zohar A. Optimal selfish mining strategies in bitcoin. In: Proc. of the Financial Crypto 2016. 2016.

[14] Vasin P. Blackcoin's proof-of-stake protocol v2. 2014. https://blackcoin.org/blackcoin-pos-protocol-v2-whitepaper.pdf

[15] Bentov I, Gabizon A, Mizrahi A. Cryptocurrencies without proof of work. In: Proc. of the Int'l Conf. on Financial Cryptography and Data Security. Berlin, Heidelberg: Springer-Verlag, 2016. 142−157.

[16] Larimer D. Delegated proof-of-stake consensus. 2018.

[17] Bentov I, Lee C, Mizrahi A, *et al*. Proof of activity: Extending bitcoin's proof of work via proof of stake [extended abstract]. Performance Evaluation Review, 2014,42(3):34−37.

[18] Buchman E. Tendermint: Byzantine fault tolerance in the age of blockchains [Ph.D. Thesis]. 2016.

[19] Buterin V, Griffith V. Casper the friendly finality gadget. arXiv preprint arXiv:1710.09437, 2017.

[20] ENIGMA. A private, secure and untraceable transaction system for cloakcoin. 2018. URL:https://www.cloakcoin.com/user/themes/g5_cloak/resources/CloakCoin_Whitepaper_v2.1.pdf

[21] Novacoin—Proof of stake [EB/OL]. 2014. URL: https://github.com/novacoin-project/novacoin/wiki/Proof-of-stake

[22] Pike D, Nosker P, Boehm D, Grisham D, Woods S, Marston J. Proof-of-Stake-Time whitepaper. 2017. URL:https://www.vericoin.info/downloads/VeriCoinPoSTWhitePaper10May2015.pdf

[23] Kiayias A, Russell A, David B, *et al*. Ouroboros: A provably secure proof-of-stake blockchain protocol. In: Proc. of the Int'l Cryptology Conf. Cham: Springer-Verlag, 2017. 357−388.

[24] Kanwal M, Kanwal M, Kanwal M, *et al*. Proof of luck: An efficient blockchain consensus protocol. In: Proc. of the Workshop on System Software for Trusted Execution. ACM Press, 2016.

[25] Dziembowski S, Faust S, Kolmogorov V, Pietrzak K. Proofs of space. In: Gennaro R, Robshaw M, eds. Proc. of the CRYPTO 2015. LNCS 9216, Heidelberg: Springer-Verlag, 2015. 585−605. [doi: 10.1007/978-3-662-48000-729]

[26] Moran T, Orlov I. Proofs of space-time and rational proofs of storage. IACR Cryptology ePrint Archive, 2016.

[27] P4Titan. Slimcoin: A peer-to-peer crypto-currencywith proof-of-burn. 2014. https://www.chainwhy.com/upload/default/20180703/4ae7cee40462e7951f508b28dd1d9936.pdf

[28] Beikverdi A. NEM technical reference. 2018. https://nem.io/wp-content/themes/nem/files/NEM_techRef.pdf

[29] Poelstra A. Distributed consensus from proof of stake is impossible. 2015. https://download.wpsoftware.net/bitcoin/pos.pdf

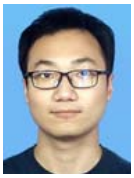
[30] Buterin V. On stake. 2014. https://blog.ethereum.org/2014/07/05/stake/

[31] Hardin G. The tragedy of the commons. Science, 1968,162(3859):1243−1248. [doi: 10.1126/science.162.3859.1243]

附中文参考文献:

[6] 袁勇,王飞跃.区块链技术发展现状与展望.自动化学报,2016,42(4):481−494. [doi: 10.16383/j.aas.2016.c160158]

黄建华(1963－),男,湖南怀化人,博士,副教授,CCF 专业会员,主要研究领域为信息安全,分布式计算.



夏旭(1994－),男,硕士生,CCF 学生会员,主要研究领域为分布式系统,区块链.

李忠诚(1994－),男,硕士生,主要研究领域为区块链性能与安全.

李建华(1977－),男,博士,副教授,CCF 专业会员,主要研究领域为生物信息学,计算机辅助技术,计算机新技术研究.

郑红(1973－),女,博士,副教授,CCF 专业会员,主要研究领域为形式化建模,服务计算.