Journal of Computer Applications
计算机应用,2020,40(8):2274 - 2278
ISSN 1001-9081
CODEN JYIIDU
2020-08-10
http://www.joca.cn

文章编号:1001-9081(2020)08-2274-05
DOI:10.11772/j.issn.1001-9081.2019122206

基于工作量证明和权益证明改进的区块链共识机制

吴梦宇,朱国胜*,吴善超
(湖北大学 计算机与信息工程学院,武汉 430062)
(*通信作者电子邮箱zhuguosheng@hubu.edu.cn)

摘　要:当前区块链工作量证明(PoW)机制浪费大量算力和电力的缺陷日益凸显,而权益证明(PoS)机制由于无成本权益以及权益无限增长容易产生分叉和富者愈富问题,不能保证区块链的稳定性。针对二者的缺陷,提出了一种基于PoW和PoS改进的区块链共识机制PoWaS。首先,降低哈希计算的难度并限制最大难度值,以减少寻找随机数所花费的算力和电力资源;其次,为有效持币时间和币龄设置上限,防止由于币龄无限增长而带来的富者无限富的问题;然后,引入信用值的概念,为每个节点赋予一个信用值,并根据节点行为升降信用值;最后,加入竞争等待时间,由寻找随机数所花费的时间、币龄和信用值计算得到一个值pStake,而pStake最大的节点获得打包记账权。实验搭建了一个拥有6个节点的PoWaS共识机制区块链,实验结果表明PoWaS可以减少算力浪费、加快出块速度和平衡记账权竞争。

关键词:区块链;共识机制;工作量证明;权益证明;信用值
中图分类号:TP301.6　　**文献标志码:**A

Improved consensus mechanism of blockchain based on proof-of-work and proof-of-stake

WU Mengyu, ZHU Guosheng*, WU Shanchao
(*School of Computer Science and Information Engineering*, *Hubei University*, *Wuhan Hubei* 430062, *China*)

Abstract: At present, the Proof-of-Work (PoW) mechanism of blockchain wastes a lot of computational power and electric power, and the Proof-of-Stake (PoS) mechanism is prone to bifurcation and makes the rich get richer due to the nothing-at-stake and unlimited growth of rights and interests, which cannot guarantee the stability of blockchain. In order to overcome the shortcomings of the two above mechanisms, an improved consensus mechanism of blockchain named Proof of Work and Stake (PoWaS) was proposed based on PoW and PoS. First, the difficulty of hashing calculation was reduced and the maximum value of difficulty was limited to reduce the computational power and electric power resources spent in searching for nonces. Second, the upper limits for the effective coin holding time and the coin age were set to prevent the problem of unlimited wealth of the rich caused by the infinite growth of the coin age. Third, with the concept of credit value adopted, the credit value was assigned to each node, and the credit value was increased or decreased based on node behaviors. Finally, the competition waiting time was added, and the time spent searching for nonces, coin age, and credit value were used to calculate a value named pStake. The node with the largest pStake gained the right to pack and account. A blockchain of PoWaS consensus mechanism with six nodes was built to carry out experiments. Experimental results show that the PoWaS can reduce the waste of computational power, speed up the block mining and balance the competition of accounting rights.

Key words: blockchain; consensus mechanism; Proof-of-Work (PoW); Proof-of-Stake (PoS); credit value

0　引言

2008年11月1日,一个化名为中本聪的人在网络上发表了一篇名为《比特币:一种点对点的电子现金系统》[1]的论文,首次提出了比特币的概念,并于2009年1月3日创建了第一个创世区块,获得了50枚比特币的挖矿奖励,比特币由此诞生。在比特币系统中,没有中心机构,完全开放自治,所有对等的节点组成一个去中心化的分布式账本,系统内的所有交易信息公开透明,每隔10 min创建一个区块,并将这10 min内全网的比特币交易记录打包并加密[2]存入该区块中,写入区块中的信息不能更改和撤销,参与竞争的矿工节点需要进行复杂的哈希计算来寻找一个随机数(Nonce),找到该随机数的节点获得打包记账权,并得到一定数量的比特币奖励。这种去中心化、公开透明、不可篡改的底层数据存储技术称为区块链[3]。

区块链的诞生引起了社会各界的极大兴趣[4],各大区块链平台应运而生,最为热门的有以太坊[5]、EOS(Enterprise Operation System)、波场等,不管是哪个区块链平台,都离不开共识机制,共识机制的作用就是使各节点在没有中心管理机

收稿日期:2020-01-02;**修回日期:**2020-03-04;**录用日期:**2020-03-18。
基金项目:赛尔网络下一代互联网技术创新项目(NGII20180803)。
作者简介:吴梦宇(1994—),男,安徽芜湖人,硕士研究生,主要研究方向:区块链、网络安全;　朱国胜(1972—),男,湖北大冶人,教授,博士,主要研究方向:下一代互联网、软件定义网络;　吴善超(1994—),男,安徽铜陵人,硕士研究生,主要研究方向:数据挖掘。

构的情况下,遵循一定的规则实现自治从而保证区块链的稳定运行。以太坊采用的是工作量证明(Proof of Work, PoW)机制,但由于PoW需要消耗巨大算力和电力并且效率不高,以太坊正在逐步迁移到其他区块链平台广泛采用的权益证明(Proof of Stake, PoS)机制[6],然而PoS机制由于其无成本权益(nothing-at-stake)的特性,很容易被分叉,并且可能存在富者愈富的问题。

针对PoW和PoS共识机制的缺陷,本文提出了一种基于PoW和PoS改进的区块链共识机制PoWaS(Proof of Work and Stake):首先降低哈希计算的难度,节点寻找随机数所花费的时间记为*fTime*;接着设置最大纳入币龄计算的持币时间,得到的币龄记为*coinAge*;然后引入信用值,节点的信用值记为*cPoint*;最后由*fTime*、*coinAge*和*cPoint*计算的到的值记为*pStake*,*pStake*最大的矿工节点获得打包记账权并得到相应的虚拟币和信用值奖励。

1　相关工作

作为区块链的核心组成部分,共识机制起着保证区块链系统稳定运行的作用,随着区块链技术的不断发展,共识机制也成为了当前国内外信息技术领域的一个研究热点,主流的区块链共识机制主要有PoW、PoS、委托权益证明(Delegated Proof of Stake, DPoS)[7]、实用拜占庭容错(Practical Byzantine Fault Tolerance, PBFT)[8]以及验证池(Pool)等。目前对共识机制的研究主要有四个方向:对PoW的改进、对PoS的改进、将PoW和PoS相结合以及对分布式一致性算法的改进。

2016年,英特尔为了改进PoW,提出了消逝时间证明(Proof of Elapsed Time, PoET)[9]机制,该机制下,各参与竞争的节点需要等待一个随机时间,第一个完成其等待时间的节点获得记账权,节点参与竞争的代价较低,拥有较为平等竞争的机会。为了解决PoW的资源浪费问题,空间证明(Proof of Space, PoSpace)[10]被提出,节点一次性提供一定的硬盘空间,后续的记账权竞争不需要花费算力,该共识机制目前已经在一些区块链项目中得到应用。2017年8月,基于PoS改进的Ouroboros共识机制被提出[11],它使用了新的激励机制,根据权益随机选出记账者。行动证明(Proof of Activity, PoA)[12]将PoW和PoS相结合,在该机制下矿工节点进行工作量证明后挖出的块并不包含交易数据,只是区块头部,需要将该头部发送给其他校验节点进行校验,校验者的选取与权益相关,最后一个校验者将交易数据加入该块中,完成一个区块的生成。小蚁共识(delegated BFT, dBFT)对拜占庭容错机制进行了改进,借鉴PoS的思想,利用基于权益的投票机制选取参与记账的节点,将拜占庭容错机制中的记账者由静态参与转变为动态调整。

1.1　PoW共识机制

PoW工作量证明机制是比特币所采用的共识机制[13],矿工节点通过不断的哈希(hash)计算寻找一个随机数(Nonce),使得Nonce拼接上前一个区块的哈希值再进行哈希计算所得到的哈希值前n位为零,n的大小对应计算难度的大小,在比特币中,难度值的计算公式为:

$$newDiff = oldDiff * (20\,160/totalTime) \tag{1}$$

其中:*newDiff*为新区块的难度值;*oldDiff*为前一个区块的难度值;*totalTime*为创建过去2 016个区块所花费的总时长,由于比特币将出块速度控制在10 min出一个块,从式(1)可以看出20 160/*totalTime*趋近于1,所以新区块的难度值与前一个区块的难度值近似相等。如果矿工的算力增强,可能出现不到10 min就出块的情况,这样20 160/*totalTime*就会大于1,根据式(1),*newsDiff*将大于*oldDiff*,难度值变高了,计算时长就会增加;反之,算力减小,难度值会降低,计算时长也会减少。这就是PoW的难度调整机制,比特币通过这种机制使得不管在什么算力情况下始终保持10 min左右的出块速度。

在PoW机制下,客户端之间发生交易后,会向全网节点广播,矿工节点收到交易信息后将其加入到自己创建的区块中,同时也在不断地进行哈希计算寻找Nonce,若某个矿工节点找到了Nonce,需要将自己打包的区块和Nonce信息向全网节点广播。其他节点收到消息后,立即验证Nonce是否正确以及区块中的所有交易是否有效,若验证通过,则认为该区块有效,然后停止当前的计算,将该区块作为区块链的最后一个区块进行新一轮的哈希计算,找到Nonce的矿工会获得一定数量的代币奖励。

从PoW的工作流程和其难度调节机制中可以看出,在创建新区块时,全网矿工节点都处于高负荷的计算中,算力再好的节点找到一个Nonce也需要10 min左右的时间,其他没有找到Nonce的节点花费了10 min的算力却得不到任何奖励。显然,产生巨大的算力和电力资源浪费是PoW机制的重大缺陷。

1.2　PoS共识机制

PoS权益证明机制在2012年由Sunny King在点点币(Peercoin)白皮书中提出,目的是为了解决比特币的PoW机制大量浪费算力、电力资源的问题。Sunny King希望通过一个可靠的机制来赋予每个节点参与系统中决策的权利,PoS机制中引入了币龄(*coinAge*)的概念,每个代币都有对应的价值来度量持币者参与决策的权重,叫作权益。币龄的计算公式为:

$$coinAge = coin * coinTime \tag{2}$$

其中:*coin*为代币数量;*coinTime*为持币时间,如果发生交易,这部分币龄将会被消耗。比如,Bob从Alice那里收到了10个币,并且持有90 d,那么Bob就收集到了900币天的币龄。如果Bob使用了从Alice收到的这10个币,那么Bob从这10个币上积累的币龄就被消耗了[14],每消耗一定的币龄都会产生一定的利息币。PoS中是通过权益来获得记账权的,权益大的节点获得记账权的概率较大。

PoS机制虽然解决了PoW大量浪费算力和电力资源的问题,但正因为不需要花费算力,记账权来源于权益,所以挖矿几乎是没有成本的(nothing-at-stake)[15]。一旦恶意节点制造分叉链,对于其他节点来说,不管在哪条链上挖矿都没有成本,他们可能会选择在每一条链上都进行挖矿,这样无论最终哪条链被选作主链,都会获得收益。如果大多数的矿工都选择在所有分叉上挖矿,那么区块链很可能被分叉,并且更容易遭到双花攻击,稳定性无法保证。通过币龄的计算方式可以看出,只要持币不交易,币龄是持续增长的,对应的权益也是持续增长的,那么持币较多的节点可能会选择大量囤积代币,一方面持币吃息,另一方面获取更大的权益,这样就会导致某些节点的权益越来越大,带来富者愈富的问题[16]。

2 PoWaS共识机制设计

2.1 优化PoW部分

针对PoW出块速度慢、交易等待时间长以及算力浪费大等问题，PoWaS作出优化方案：

1）降低哈希计算的难度，减少寻找随机数所花费的算力。将初始难度设为1，对应难度值为6，即找到的Nonce拼接前一个区块的hash值再进行哈希计算得到的hash值的前6位为0，这样矿工节点基本上只花数十秒就能找到Nonce，实验证明将在3.2节中详细阐述。工作量证明算法如算法1所示。

算法1 工作量证明算法。

输入 前一个区块hash值preHash，难度值n；

输出 随机数nonce。

```
def hash(preHash, nonce):
    str = f'{preHash}{nonce}'.encode()
    return hashlib.sha256(str).hexdigest()
def proof(preHash, n):
    nonce = 0
    while hash(preHash, nonce)[:n]!= str(0).zfill(n):
        nonce += 1
    return nonce
```

2）将出块速度保持在1 min左右，以获得更快的交易确认。设置一个竞争等待时间（*wTime*）为10 s，第一个找到Nonce的节点立即向全网广播，此时触发*wTime*，此后10 s内找到的节点都有机会获得记账权，10 s之后还没有找到的节点则失去获得本次记账权的机会，停止计算。找到Nonce所花费的时间记为*fTime*，作为确定打包记账权的一个因素。

3）将难度调整机制改为每创建720个区块调整一次，即每12 h左右调整一次难度。难度计算公式改为：

$$newDiff = oldDiff * (43\,200/totalTime) \tag{3}$$

其中：*newDiff*为新区块的难度；*oldDiff*为前一个区块的难度；*totalTime*为创建过去720个区块所花费的总时长，单位为s。由于出块速度在1 min左右，所以43 200/*totalTime*趋近于1，*newDiff*和*oldDiff*近似相等。如果算力增加，*totalTime*就会小于43 200 s，43 200/*totalTime*大于1，*newDiff*将大于*oldDiff*，难度增加；反之，算力减小，难度减小，以此来动态调整计算难度。

2.2 优化PoS部分

针对PoS可能会出现的节点权益无限增大的问题，PoWaS设置了一个有效持币时间（*valueTime*），并限制最大值为60 d，币龄的计算公式为：

$$coinAge = coin * valueTime \tag{4}$$

若持币时间超过有效持币时间最大值，则*valueTime*停止增长，由式（4）可以看出超出的时长不会纳入币龄的计算，以此来限制币龄的无限增长，并设置参与*pStake*计算的币龄最大值为2 000，防止由于币龄无限增长而带来权益无限增大问题。

2.3 引入信用值

引入信用值来反映节点的信用情况，为每个节点赋予一个信用值（*cPoint*），作为记账权的一个参考因素，根据节点的行为增加和扣除信用值：用信用值奖励来调动矿工节点的挖矿积极性，信用值扣除来减小节点作恶的几率。

信用值采用1 000分制，最高为1 000，每个节点的初始信用值为400，成功记账后会获得0.1信用值奖励，节点如果发生恶意行为，比如恶意分叉，将扣除20信用值。若信用值较低，则对节点竞争记账权进行限制，具体规则如下：

1）信用值低于400高于300时，限制120轮，即2 h左右无法参与记账权竞争；

2）信用值低于300高于200时，限制720轮，即12 h左右无法参与记账权竞争；

3）信用值低于200高于100时，限制4 320轮，即72 h左右无法参与记账权竞争；

4）信用值低于100时，剔除该节点，取消其矿工资格。

限制规则算法如算法2所示。

算法2 根据信用值限制记账权竞争

输入 信用值cPoint，当前区块号begIndex；

输出 限制状态limitStatus，解除限制区块号endIndex。

```
def limit_behavior(cPoint, begIndex):
    if cPoint >= 400:
        limitStatus = false
        endIndex = begIndex
    elif 400 > cPoint >= 300:
        limitStatus = true
        endIndex = begIndex + 120
    elif 300 > cPoint >= 200:
        limitStatus = true
        endIndex = begIndex + 720
    elif 200 > cPoint >= 100:
        limitStatus = true
        endIndex = begIndex + 4320
    else:
        limitStatus = true
        endIndex = -1
    return{'limitStatus':limitStatus,'endIndex':endIndex}
```

2.4 确定记账权

记账权竞争流程为：各矿工节点根据当前的难度值进行哈希计算寻找随机数Nonce，使得该Nonce拼接上前一个区块的hash值再进行哈希计算后得到的hash值的前*n*位为0，*n*等于难度值。当某矿工找到Nonce后，立即向全网广播，此时触发竞争等待时间*wTime*（为10 s），其他节点收到广播后还有10 s的计算时间，如果10 s内找到了Nonce，也立即向全网广播，10 s后仍然没有找到Nonce的节点失去本轮记账机会。找到Nonce的节点根据*fTime*、*coinAge*和*cPoint*这三个值计算出所有找到Nonce的节点的*pStake*值，*pStake*的计算公式为：

$$pStake = coinAge/1\,000 + (cPoint - fTime)/100 \tag{5}$$

由于这里的*coinAge*限制了最大值为2 000，*cPoint*为100至1 000，*fTime*为60左右，根据式（5）可知，*coinAge*/1 000为0至2，*cPoint*/100为1至10，*fTime*/100为0.6左右。这样就降低了权益和算力的比重，提高了信用值的比重，强化了信用值对记账权竞争的影响，有利于减少矿工节点作恶行为的发生。

若发现自己的*pStake*最大，则将所有的*pStake*信息以及自己打包好的区块广播至全网，宣布自己获得打包权，其他节点收到信息后进行验证，若验证通过，将收到信息中的区块作为区块链最后一个区块进行下一轮的挖矿计算；若发现自己的*pStake*不是最大的，则竞争失败，等待获得打包权节点的广播信息。没有找到Nonce的节点停止计算，收到获得记账权的节点的广播信息后，再进行下一轮的计算。完整的记账权竞争过程如图1所示。

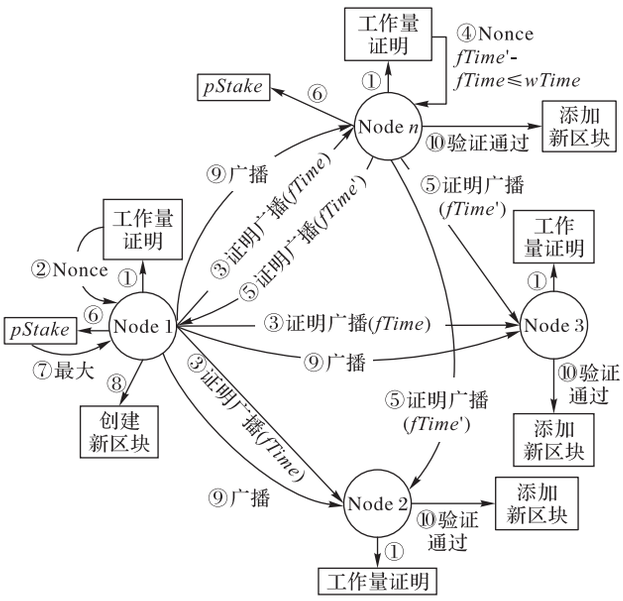

图1　记账权竞争过程示意图

Fig. 1　Schematic diagram of accounting right competition process

3　实验与结果分析

3.1　实验环境

使用Python3语言和Python Flask Web框架编写实现了一个区块链原型,并使用PoWaS共识机制搭建了一个测试区块链,实验室6台配置不同的计算机作为区块链节点,从寻找随机数所花时间、区块链出块时间以及记账权竞争等方面进行了实验。6个节点的配置信息如表1所示。

表1　节点配置信息

Tab. 1　Node configuration information

节点名	区块链地址	CPU	内存/GB	操作系统
Node1	02bf09204d6d4a7ca…	i5-8265U	8	Windows10
Node2	64288351138b4ae48…	i5-6500	8	Windows10
Node3	8a852a1c0d044f879…	i5-6500	8	CentOS 7
Node4	ddf6659cc8774dc3b…	i7-4700M	8	Windows10
Node5	620f94325331464d8…	i7-8700	8	Windows10
Node6	76aee9408b214dc99…	i7-8700	8	CentOS 7

3.2　优化后的PoW时间花销

PoWaS通过调低难度值来降低PoW部分寻找Nonce的时间花销,初始难度值设为6,即Nonce拼接前一个区块hash值再进行计算得出的hash值前6位为0,这样可以将平均计算时间控制在1 min以内。为了验证,将测试区块链的共识机制修改为只使用难度值为6的纯PoW机制,6个节点分别进行了50次的工作量证明计算,记录每次计算所花时间,统计后得到的结果如图2所示。

从实验结果可以看出,在配置不同的6个节点的50次计算时间里,虽然除节点6以外的5个节点均出现了计算时间超过60 s的情况,但绝大多数还是集中在小于40 s的区间内。由于哈希碰撞的不确定性,寻找随机数所花时间并不一致,配置较低节点存在少数的计算时间超过60 s的情况在所难免,但从全局来看影响并不大。该实验可以证明在难度值设为6的情况下,基本可以保证工作量证明的时间花销控制在1 min以内。

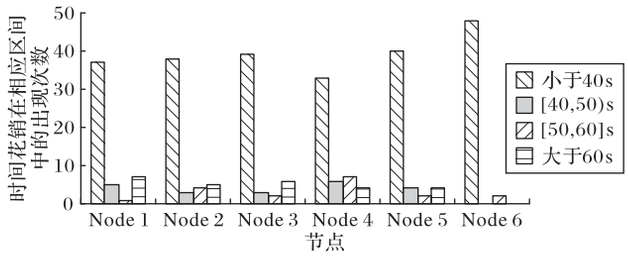

图2　PoW机制下50次工作量证明计算结果

Fig. 2　Work proof results of fifty times under PoW mechanism

3.3　区块链的出块时间

在实验所搭建的区块链运行一段时间后,在前50个区块中,以5个区块作为间隔,统计了10个区块的出块时间,结果如图3所示。从图3中可以看出,曲线有轻微波动,但波动幅度并不大,基本都在60上下,可以证明PoWaS共识机制下区块链的出块速度可以保持在1 min左右。

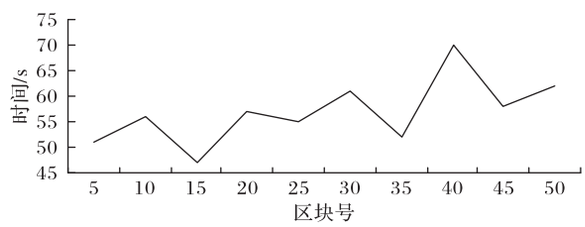

图3　前50个区块的出块时间统计

Fig. 3　Block mining time statistics of top fifty blocks

3.4　记账权竞争

节点的初始信用值为400,实验将节点中算力最好的节点6作为恶意节点,在产生第6个区块时,发生了恶意分叉行为,被扣除了20信用值。统计前120个区块中每个节点的记账次数,得到的结果如图4所示。从实验结果可以看出,虽然节点4的算力最弱,但依然获得了12次的记账权;算力最好的节点6由于恶意分叉行为被扣除20信用之后,信用值为380.4,低于400,被限制了120轮的记账权,所以它的记账次数仅为4。由此可以说明信用值和竞争等待时间的引入在一定程度上平衡了记账权的竞争。

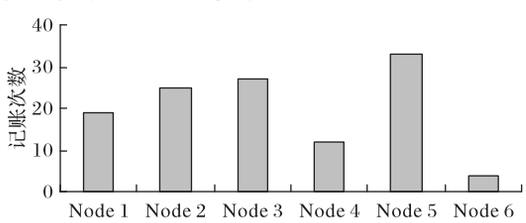

图4　发生恶意分叉行为时各节点记账次数统计

Fig. 4　Statistics of node accounting times of various nodes when malicious bifurcation occurs

3.5　安全性分析

PoWaS通过引入信用值来评估节点信用状况,节点的作恶行为会被扣除信用值,信用值较低时就会受到限制甚至被剔除。通过2.4节中对式(5)的分析可知,信用值在*pStake*值计算中的比重高于权益和算力的比重,这样就降低了恶意节点获得记账权的几率。通过3.4节的实验结果可知,算力最好的节点6因恶意行为被扣除信用值限制记账权竞争后,仅获得了4次记账权,远少于其他节点。

目前常见的对区块链的攻击方式有双花攻击、自私挖矿等。双花攻击就是同一笔资金多次交易，根据攻击手段的不同又有51%攻击、贿赂攻击和重放攻击等。

在PoW机制下，51%攻击的攻击者需要拥有全网51%的算力才能制造一个分叉并使之成为主链，使得自己支付给其他节点的那笔交易失效。而在PoWaS机制下，攻击者不仅需要拥有全网51%的算力，还需要自己的权益足够大、信用值足够高才能顺利地进行双花，否则不但会双花失败，而且还会受到扣除信用值的处罚，这是很难实现且得不偿失的。贿赂攻击的攻击者则通过贿赂其他矿工节点来制造分叉，在PoWaS机制下，由于矿工都有信用值，在分叉上挖矿的恶意行为会被扣除信用值影响后续记账权的竞争，矿工收受贿赂进行恶意挖矿的意愿会比较低，也就增大了攻击者的贿赂成本，很难实现成功贿赂全网超过51%的节点。当区块链有分叉链时，可能会遭受重放攻击，就是攻击者将在主链上的交易到分叉链上重新广播一次，实现双花，PoWaS机制对于重放攻击的防范，就是在分叉前尽可能多地改变分叉链的交易结构，使得主链和分叉链无法互通。

PoW机制下，自私挖矿的攻击者挖出区块后不公开，产生秘密分叉，然后在该分叉上挖矿，待到一定的时机再公开并使该秘密分叉成为主链，使得在原主链上挖矿的诚实矿工付出算力而得不到收益，自己获得更高算力比例的收益。在PoWaS机制下，由于记账权受信用值影响，如果矿工选择不公开新区块，并制造分叉，那么自己的信用值也不会增长，再次获得记账权的几率不断降低，很难攻击成功，反而还会因恶意分叉行为被扣除信用值。

4 结语

本文提出的PoWaS区块链共识机制，针对PoW和PoS的缺陷，通过降低哈希计算的难度、限制最大有效持币时间以及引入节点信用值的方式来作出改进。实验环境利用Python3语言和Flask Web框架搭建的测试区块链在拥有6个算力不同的节点的情况下，得出的实验结果在一定程度上证明了PoWaS在减少算力浪费、加快区块出块速度和平衡记账权竞争方面具有一定效果。但PoWaS仍然存在不足，下一步工作将会在出块速度稳定性和信用值调节方面加深研究，不断完善该共识机制，进一步提升其可用性。

参考文献（References）

[1] NAKAMOTO S. Bitcoin: a peer-to-peer electronic cash system[EB/OL]. [2019-08-16]. https://bitcoin.org/bitcoin.pdf.

[2] BONNEAU J, MILLER A, CLARK J, et al. SoK: research perspectives and challenges for bitcoin and cryptocurrencies[C]// Proceedings of the 2015 IEEE Symposium on Security and Privacy. Piscataway: IEEE, 2015: 104-121.

[3] UNDERWOOD S. Blockchain beyond bitcoin[J]. Communications of the ACM, 2016, 59(11): 15-17.

[4] 韩璇，刘亚敏. 区块链技术中的共识机制研究[J]. 信息网络安全，2017(9)：147-152.（HAN X, LIU Y M. Research on the consensus mechanisms of blockchain technology[J]. Netinfo Security, 2017(9): 147-152.）

[5] Ethereum. org. Ethereum Wiki White Paper[EB/OL]. [2019-08-16]. https://github.com/ethereum/wiki/wiki/White-Paper.

[6] WOOD G. Ethereum: a secure decentralised generalised transaction ledger[EB/OL]. [2019-08-16]. https://ethereum.github.io/yellowpaper/paper.pdf.

[7] LARIMER D. Delegated proof of stake consensus[EB/OL]. [2019-08-16]. https://bitshares.org/technology/delegated-proof-of-stake-consensus/.

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

[9] BUNTINX J P. What is proof of elapsed time? [EB/OL]. [2020-02-28]. https://themerkle.com/what-is-proof-of-elapsed-time.

[10] ATENIESE G, BONACINA I, FAONIO A, et al. Proofs of space: When space is of the essence[C]// Proceedings of the 9th International Conference on Security and Cryptography for Networks, LNCS 8642. Cham: Springer, 2014: 538-557.

[11] 袁勇，倪晓春，曾帅，等. 区块链共识算法的发展现状与展望[J]. 自动化学报，2018，44(11)：2011-2022.（YUAN Y, NI X C, ZENG S, et al. Blockchain consensus algorithms: the state of the art and future trends[J]. Acta Automatica Sinica, 2018, 44(11): 2011-2022.）

[12] BENTOV I, LEE C, MIZRAHI A, et al. Proof of activity: extending bitcoin's proof of work via proof of stake[J]. ACM SIGMETRICS Performance Evaluation Review, 2014, 42(3): 34-37.

[13] CONTI M, KUMAR E S, LAL C, et al. A survey on security and privacy issues of bitcoin[J]. IEEE Communications Surveys and Tutorials, 2018, 20(4): 3416-3452.

[14] KING S, NADAL S. PPCoin: peer-to-peer crypto-currency with proof-of-stake[EB/OL]. [2019-08-16]. https://www.peercoin.net/whitepapers/peercoin-paper.pdf.

[15] LI W, ANDREINA S, BOHLI J M, et al. Securing proof-of-stake blockchain protocols[C]// Proceedings of the 9th International Conference on Data Privacy Management, Cryptocurrencies and Blockchain Technology, LNCS 10436. Cham: Springer, 2017: 297-315.

[16] HOUY N. It will cost you nothing to "kill" a proof-of-stake crypto-currency[J]. Economics Bulletin, 2014, 34(2): 1038-1044.

This work is partially supported by the CERNET Innovation Project (NGII20180803).

WU Mengyu, born in 1994, M. S. candidate. His research interests include blockchain, network security.

ZHU Guosheng, born in 1972, Ph. D., professor. His research interests include next generation internet, software defined network.

WU Shanchao, born in 1994, M. S. candidate. His research interests include data mining.