

基于信誉管理模型的矿工类型鉴别机制设计

余佳仁^{1,2}, 田有亮^{1,2}, 林晖³

(1. 贵州大学计算机科学与技术学院, 贵州 贵阳 550025;

2. 贵州省公共大数据重点实验室, 贵州 贵阳 550025;

3. 福建师范大学数学与信息学院, 福建 福州 350117)

摘要: 在公开矿池中, 矿工可以随意进入矿池提交工作量证明从而获得奖励, 矿工的条件约束类型不同。因此, 会出现恶意矿工提交无效工作量和矿工在矿池中不提交工作量的情况, 占用矿池的验证计算资源, 降低矿池的验证效率, 导致矿池系统崩溃。针对矿池中难以分辨矿工类型而导致矿池系统崩溃的问题, 引入信誉管理机制对矿工的行为进行衡量, 部署合约防止矿工与矿池管理者合谋, 提出一种基于信誉管理模型的矿工类型鉴别机制设计。构造信誉机制对矿工的行为进行衡量, 当矿工进行恶意行为时, 会调低矿工的信誉值。当矿工的信誉值小于矿池的信誉阈值时, 系统会剔除该矿工, 从而该矿工不能再进入矿池提交工作量证明, 获得奖励。根据马尔可夫过程中的矿工行为状态转移, 对矿池中的矿工进行动态更新, 从而使得矿池中的矿工都在进行诚实的行为, 提交工作量证明。同时, 设计一种奖励制度对矿池中的矿工进行激励, 在矿池中部署智能合约, 防止矿工与矿池管理者进行共谋。从安全性和性能上对方案进行分析, 证明所提方案不仅在矿工提交工作量证明过程中是安全的, 并且解决了在公开矿池中矿工类型的鉴别问题, 从而解决恶意矿工提交无效工作量的问题, 剔除恶意矿工, 避免矿池验证无效工作量, 提高矿池的验证效率。

关键词: 区块链; 矿工; 矿池; 信誉管理; 马尔可夫过程

中图分类号: TP309

文献标志码: A

DOI: 10.11959/j.issn.2096-109x.2022002

Design of miner type identification mechanism based on reputation management model

YU Jiaren^{1,2}, TIAN Youliang^{1,2}, LIN Hui³

1. College of Computer Science and Technology, Guizhou University, Guiyang 550025, China

2. State Key Laboratory of Public Big Data, Guiyang 550025, China

3. College of Mathematics and Informatics, Fujian Normal University, Fuzhou 350117, China

收稿日期: 2021-06-01; **修回日期:** 2021-10-08

通信作者: 田有亮, youliangtian@163.com

基金项目: 国家自然科学基金 (61662009, 61772008); 贵州省科技重大专项计划 (20183001); 国家自然科学基金联合基金重点支持项目 (U1836205); 贵州省科技计划项目 ([2019]1098); 贵州省高层次创新型人才项目 ([2020]6008)

Foundation Items: The National Natural Science Foundation of China (61662009, 61772008), Science and Technology Major Support Program of Guizhou Province (20183001), The Key Program of the National Natural Science Union Foundation of China (U1836205), The Science and Technology Program of Guizhou Province ([2019]1098), The Project of High-level Innovative Talents of Guizhou Province ([2020]6008)

引用格式: 余佳仁, 田有亮, 林晖. 基于信誉管理模型的矿工类型鉴别机制设计[J]. 网络与信息安全学报, 2022, 8(1): 128-138.

Citation Format: YU J R, TIAN Y L, LIN H. Design of miner type identification mechanism based on reputation management model[J]. Chinese Journal of Network and Information Security, 2022, 8(1): 128-138.

Abstract: In the public mining pool, miners can freely enter the mining pool to submit proof of work to obtain rewards, and there are no conditions to restrict different types of miners. There will be malicious miners submitting invalid workloads and miners not submitting workloads in the mining pool, occupying the verification computing resources of the mining pool, reducing the verification efficiency of the mining pool, and causing the mining pool system to collapse. Aiming at the problem that it is difficult to distinguish the type of miners in the mining pool, which leads to the collapse of the mining pool system, a reputation management mechanism was introduced to measure the behavior of miners, and contracts were deployed to prevent miners from colluding with the pool manager. A design of miner type identification mechanism based on reputation management model was proposed. A reputation mechanism was constructed to measure the behavior of miners. When a miner conducts malicious behavior, the miner's reputation value would be lowered. When the miner's reputation value was less than the reputation threshold of the mining pool, the system would remove the miner, so that the miner can no longer enter the mining pool to submit proof of work and get rewards. The miners in the mining pool were dynamically updated by Markov process, so that the miners in the mining pool were conducting honest behaviors and submitting proof of work. At the same time, a reward system was designed to motivate the miners in the mining pool, and smart contracts were deployed in the mining pool to prevent miners from collusion with the mining pool manager. Finally, analyzing the scheme from the perspective of security and performance, the proposed scheme was not only safe in the process of miners submitting proof of workload, but also solved the problem of identifying miner types in public mining pools, thereby solving the problem of malicious miners submitting invalid workloads, eliminating malicious miners, and avoiding mining pools verifying invalid workloads, to improve the verification efficiency of the mining pool.

Keywords: blockchain, miner, mining pool, reputation management, Markov process

0 引言

2008年,中本聪发表一篇名为《比特币:一种点对点的数字货币》^[1]的白皮书中首次提出了区块链的概念。经过多年的研究发展,区块链技术在医疗、金融和物联网等^[2-6]各个领域被大力探索,最典型的是比特币的研究,运用区块链技术来实现比特币之间的正常交易^[7]。在区块链系统中,验证事务和参与生成新区块的节点称为矿工,区块链系统的比特币正常交易靠着矿工的维持^[8]。同时,在区块链系统中,矿工对交易进行打包挖掘,广播新的区块,连接到区块链上。

比特币是限量的,随着矿工的挖掘,币的数量逐渐减少。比特币的共识机制是随着比特币数量减少,挖矿难度增加^[9]。对于单个矿工而言,采矿事件之间的间隔显示出很大的差异,要想在后期挖出区块必须要提升自身的算力,来满足挖矿难度。并且,从单个矿工进行挖矿所获得收益对比所付出的成本来说,经济效益较低。所以,

矿工为了更好地获得收益,自然的形成一种组织,即:矿池。矿工集合算力进行挖矿,以使采矿收入更加客观、可预测。实际上在“数字货币”中,由于算力过于庞大,独立矿工想要发现新区块的概率几乎为零^[10]。

单个矿工倾向于加入矿池以确保稳定的收益,矿池对于攻击者来说是一个潜在有价值的攻击目标^[11]。以公开矿池为例,所有矿工只要支付一定费用就可以随意进出矿池,这样可能出现不诚实的矿工从而对矿池的安全性产生威胁。除了常见的针对区块链的攻击外,矿池可能出现如下的安全威胁:恶意的矿工节点进行分布式拒绝服务(DDoS, distributed denial of service)攻击,区块截留(BWH, block with holding)攻击和自私挖矿攻击。在BWH攻击中,恶意的矿工仅提交部分证据,并撤回表示工作的完整性证明。BWH攻击使用了这样一个事实:矿工会根据他们提交的股份获得奖励^[12],用另外部分的算力在矿池外进行诚实挖矿,这样就能获得更高的收益。在自私挖矿攻击中,强攻击者以牺牲其他节点^[13]

为代价来增加自己的收益。只有当公共分支的长度接近保持私有分支的长度时^[14], 自私矿工才会暴露私有链, 从而获得更大的收益, 使得之前的区块作废。在区块链矿池中, 矿工可以随意进入矿池提交工作量证明。矿池容易受到 DDoS、BWH 和自私挖矿等攻击, 要抵抗这些攻击有不同的办法。Jonhson 等^[15]研究针对比特币矿池的 DDoS 攻击背后的动机。研究表明, 攻击一个较大的矿池比攻击一个较小的矿池有更大的动机。并且, 矿池的收益大于阈值会受到经济动机的攻击, 而小于阈值的矿池则不会。Feng 等^[16]提出了一种在区块链网络中随机选择诚实矿工的协商共识机制。在协商共识机制下, 引入信任管理来评估矿工的可信度, 从而实现在区块创建过程中随机选择诚实的矿工。Lee 等^[17]为了解决自私挖矿故意制造区块链的区块分叉, 浪费诚实矿工计算能力的问题。分析了自私挖矿及针对其的对策, 提出了一种通过在事务数据结构中增加事务创建时间来防止自私挖矿。为了在公开矿池中避免受到区块截留攻击和分布式拒绝服务攻击等的威胁, 鉴别出矿工的类型, 选出诚实的矿工显得尤为重要。

基于信誉值鉴别出矿工类型, 选择诚实矿工是一种研究方向。Tang 等^[18]提出了一种机制, 每个矿工的声誉是由一个随机选择的矿工来评价的, 该矿工将扮演矿池管理者的角色。但是, 由于矿池管理者是随机选择的, 所以很容易受到攻击。如果选择了恶意的矿工作为矿池管理者, 将会对整个矿池造成严重的影响。因此, 基于博弈论, 文献[18]设计了一种基于声誉的算法来鼓励矿工诚实挖掘, 从而增加矿池的总收益。此外, 在文献[14]中, 矿池管理者能选择矿工, 但矿池管理者并不是由矿工选择的。Kaci 等^[19]提出了一种新的存储链, 对矿池中的管理者和矿工进行管理。其中, 存储链中存储着矿工对矿池管理者的满意度。但是, 矿工的信誉分数没有一个明确的标准。因此, 本文根据以上的问题, 设计了一种基于信誉管理模型的矿工类型鉴别机制, 对矿工的信誉分数进行标准化定义, 同时对矿池管理者的选择给出相应的准则。

在矿池中鉴别出诚实的矿工提交工作量证

明, 可以使矿池的收益更高。邸剑等^[20]提出了一个基于风险决策准则的矿池选择模型, 研究了矿池算力和奖励机制对矿工最优选择策略的影响; 计算了矿工在不同矿池中的收益, 给出收益矩阵。分别利用最大可能性准则和期望值准则得出最优选择策略。Xu 等^[21]为了谋得矿池的经济激励, 考虑了两种奖励共享策略: 每股平均付费 (PPS) 和最后一次平均每股付费 (PPLNS)。通过所需的哈希率、网络时延和奖励策略, 设计了一种演化平衡 (ESS) 方案, 提出了一种低复杂度分布式算法来提高矿池的收益, 同时对矿池进行经济激励。因此, 本文设计了一种信誉管理模型用于鉴别矿池中的矿工类型, 在矿池中选出诚实的矿工, 同时基于马尔可夫过程对矿池中的矿工进行动态更新, 最后对矿池中的矿工进行奖励。

矿池受到的这些攻击大部分是矿工的恶意行为所致, 恶意矿工不诚实提交完整的工作量证明, 自私挖矿损害矿池的利益, 致使矿池不能正常工作。因此, 鉴别出进入矿池中的矿工类型, 并排除恶意矿工, 成为维护矿池正常运转和提高矿池收益的一种有效方法。本文提出了一种信誉管理模型来对矿工的类别进行鉴别, 引入信誉阈值, 只有矿工的信誉值大于矿池的信誉阈值时, 矿工才能正常地在矿池中提交工作量证明。因此, 本文基于信誉管理模型鉴别矿池中的矿工类型, 选择出矿池中诚实的矿工, 对矿池中的矿工进行动态更新。本文的主要贡献如下。

1) 基于矿池中矿工与矿池管理者之间的相互监督对信誉函数进行改进, 构造一种信誉机制, 实现对矿池中的矿工类型鉴别。根据成员之间的相互监督更新矿池管理者, 解决矿池管理者权利过大而导致矿池奖励不均的问题。

2) 基于马尔可夫过程构造了一种矿工行为状态转移矩阵, 对矿池进行动态更新。设计一种在矿池中的奖励制度, 对在矿池中鉴别出的诚实矿工进行奖励。

3) 对所提方案进行安全性和性能分析, 证明所提方案不仅在矿工提交工作量证明过程中是安全的, 而且解决了在公开矿池中矿工类型的鉴别问题。

1 基础知识

1.1 工作量证明

工作量证明 (PoW, proof of work) 是求解一个特定的哈希原像问题的过程。由于在求解哈希原像问题中, 没有高效的算法, 只能通过暴力计算的方式求解, 从而使得计算资源多、计算能力强的矿工可以有更高的概率率先解出该问题^[22]。在密码“货币”中, 第一个解出该问题的矿工将获得一定数额的相应密码货币的奖励。例如, 在比特币系统中, 共识链中的区块创建者现阶段可以获得 12.5 比特币的奖励。于是在这种经济奖励的刺激下, 大量矿工参与到通过寻找哈希原像而创建区块的行动中, 这就是通常所说的挖矿, 挖矿的过程实现了分布式账本的维护。

1.2 矿池

矿池可分为公开矿池和封闭矿池。矿池里面分为矿池管理者和矿工。其中, 公开矿池允许矿工自由注册并参与该矿池的挖矿。当矿池挖出区块并获得相应的比特币奖励时, 矿池管理员将根据矿池成员的算力大小进行奖励分配。封闭矿池只允许特定的矿工加入^[23]。本文所说的矿池指的是公开矿池, 封闭矿池不在本文考虑范围内。

矿工选择加入矿池挖矿的主要原因在于减少不确定性的发生, 即矿工期望获得收益的方式更加稳妥 (即使该收益数量相对较少) 而非赌博式地获取大额收益^[24]。以典型的数字货币-比特币为例, 根据比特币的设计, 单个独立矿工或者矿池挖矿的目的是寻找当前系统工作量证明问题的解, 即寻找一个合法的区块 A , 使得 $\text{Hash}(A) < N$, 其中目标值 N 每隔一段时间由系统自动调整。在矿池内部, 矿池管理员在向矿池成员发布完整工作量证明 (FPoW, full proof of work) 任务的同时, 也向矿池成员发布部分工作量证明 (PPoW, partial proof of work) 任务。其中, 完整工作量证明任务要求矿工寻找使得 $\text{Hash}(A) < N$ 成立的区块 A , 而部分工作量证明任务是指寻找使得 $\text{Hash}(A_p) < N_p$ 成立的区块 A_p ^[25]。显然, 部分工作量证明任务包含完整工作量证明任务, 其难度

小于完整工作量证明任务的难度。矿池管理者将矿池内部矿工提交的部分工作量证明作为其分配奖励的依据。

矿池管理者检查提交的工作量, 以便在其中找到根据共识协议工作有效的充分证明。这个充分的证据将被用来要求获得采矿奖励。主流矿池里面有 4 种激励模式^[26]: pay per share (PPS)、pay per last N share (PPLNS)、full pay per shares (FPPS)、pay per shares plus (PPS+)。

1.3 马尔可夫过程

在一个时序过程中, 如果 $t+1$ 时刻的状态取决于 t 时刻的状态 s_t , 而与 t 时刻之前的任何状态都无关, 则认为 t 时刻的状态 s_t 具有马尔可夫性 (Markov property)^[27]。若过程中的每个状态都具有马尔可夫性, 则这个过程具备马尔可夫性, 具备了马尔可夫性的随机过程被称为马尔可夫过程 (Markov process), 马尔可夫过程的关键在于状态转移方程:

$$\rho_{ss'} = P[s_{t+1} = s' | s_t = s] \quad (1)$$

下一时刻的状态 s_{t+1} 仅与当前时刻的状态 s_t 有关, 而与 $s_1, \dots, s_{t-1}$ 无关。

2 方案构造

本文提出一种信誉管理模型, 用于管理矿池中矿工和矿池管理者的信誉。同时根据矿工的信誉值与矿池的信誉阈值比较来鉴别矿工的类型, 选出诚实的矿工。基于马尔可夫过程中的矿工状态转移对矿池中的矿工进行动态更新。设计一种奖励机制对矿工诚实提交工作量证明进行奖励。信誉管理模型如图 1 所示, 矿工通过提交工作量触发矿池管理者部署在矿池中的智能合约, 从而获得奖励和矿池标记。通过奖励来激励矿池中的矿工表现诚实, 使矿池保持正常运转而不受攻击。

2.1 矿工鉴别策略

为了鉴别矿工类型, 构造一种信誉管理机制来鉴别矿工, 鉴别出诚实矿工, 本文特规定两个条件。

条件 1: 矿工信誉值小于矿池信誉阈值 θ 时, 不能进入矿池。

条件 2: 矿池管理者必须从矿池中的矿工选择。

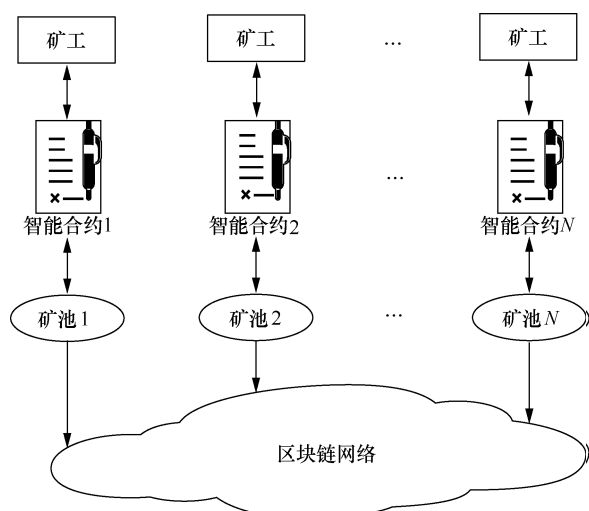


图 1 信誉管理模型
Figure 1 Reputation management model

在矿池的信誉机制设计中必须要考虑到矿工进入矿池之后,可能存在进行不诚实挖矿的情况。同时可能存在矿池管理者的权利过大,并且矿池管理者不诚实,影响整个矿池的情况。为避免以上这两种情况的发生,可以采用信誉值来评价矿池中的矿工和矿池管理者的信任度。在矿池中的矿工和矿池管理者之间进行着沟通和协作,这为矿工在矿池中所获得的经济收益和矿池管理者管理矿池提供了一种有效的方法。根据信誉机制条件,对通过触发智能合约进入矿池的矿工和矿池的管理者进行评价并且更新信誉值。然后,在该机制中根据矿工的信誉值鉴别出矿工的类型,在矿池中选择出诚实矿工。矿池管理者在矿池中会发布任务,矿工会根据任务和自己的算力情况,提交完整的工作量或者部分工作量。

在矿池引入信誉管理之后,如果恶意的矿工和恶意的矿池管理者进行不诚实行为,则相应的信誉值会低于诚实的矿工和诚实的管理者。在此情况下,设计出了在矿池中信誉评估的方案。

以第 i 个矿工,第 j 个矿池为例。参数 (r_i, f_i, c_i) 分别表示在矿池中矿工提交的有效工作量、无效工作量或者没有提交工作量、矿工对矿池管理者的监督值。在矿工达成共识过程中,矿工的信誉值分为验证者和提议者信誉值。如果提议者的提议被验证者验证成功,那么信誉值相应地加 1。同理,验证亦如此。但是,本文是考虑

在矿池情况中,并且引入矿池中的矿工对矿池管理者进行监督,监督值 c_i 为对矿池管理者进行约束。如果矿工提交的工作量是有效工作量, r_i 加 1; 反之, f_i 加 1。矿池管理者部署合约,写入奖励程序,矿池中的矿工在一轮工作中提交工作量,触发智能合约,根据合约程序给出相应的奖励。如果大多数矿工对于矿池管理者所分配的奖励有异议,那么会投诉矿池管理者, c_i 加 1。用 P_{M_i} 表示矿工 M_i 的信誉值。在矿工提交工作量时,触发智能合约,智能合约给出相应的信誉值。提交的工作量越多、越完整,得到的信誉值就越多。矿工 M_i 的信誉值函数表示为

$$P_{M_i} = \frac{P_{M_{i-1}} \cdot \eta + r_i - f_i - c_i}{r_i + f_i + c_i + 1} \quad (2)$$

其中,矿工首次进入矿池的信誉值 P_{M_i} 为矿池的信誉阈值 θ , 参数 η 表示矿工在一轮中提交的工作量。矿工进入矿池的初始信誉分数为 θ 。参数 η 可以表示为

$$\eta = \begin{cases} 1, & \text{完整的工作量} \\ \frac{n}{100}, & n\% \text{ 工作量} \\ 0, & \text{不提交工作量/无效工作量} \end{cases} \quad (3)$$

当区块链网络开始形成时,所有节点的行为都是未知的,节点都单独进行挖矿来获得奖励。在矿池开始形成时,矿池中的矿工鉴别类型机制不够完善。因此,根据构造的信誉管理机制,矿工开始可以随意进入矿池,矿工每进入一个矿池,都会带有矿池的标识参数。在矿池中,矿工每提交一轮工作量,矿池管理者根据事先写入的智能合约给出相应的奖励。在奖励分配时,可能存在矿工与矿池管理者进行合谋,从而使其他矿工的收入减少的情况。因此,当矿工提交工作量时,触发事先矿池管理者写入智能合约的程序,给出信誉值的同时也要给出相应的奖励。为了避免矿池中的恶意矿工再次进入矿池,矿工在收到奖励的同时,会内含一个矿池的标识参数 S 增加到矿工的公钥地址上。在矿池中,为了防止恶意矿工影响矿池的激励制度和矿池的安全,当矿工不诚实提交工作量时,会触发智能合约,降低矿工的信誉值。以矿池 j 为例,本文提出算法 1 鉴别矿

工类型，选择矿池中矿工。矿工在没有进入任何一个矿池时，没有矿池的标记。矿工首次进入一个矿池提交工作量后，就会被矿池标记。针对算法1中的矿工进入矿池提交一次工作量之后，根据式(2)得到相应的信誉值，通过信誉值来选择矿池中的矿工。

算法1 选择矿工

输入 矿工 M

输出 矿池中的矿工 I

- 1) 矿工 $M = \{M_1, M_2, \dots, M_n\}$ 进入矿池 j
- 2) for each $M_i \in M$ do
- 3) if $S(M_i) = S(j)$ then
- 4)
$$P_{M_i} = \frac{P_{M_{i-1}} \cdot \eta + r_i - f_i - c_i}{r_i + f_i + c_i + 1}$$
- 5) if $P_{M_i} \geq \theta$ then
- 6) $I = \{M_i\}$
- 7) end if
- 8) else
- 9) $I = \{M_i\}$
- 10) $P_{M_i} = \theta$
- 11) end if
- 12) $i = i + 1$
- 13) end for

根据算法1能鉴别矿池中矿工的类型，选择矿池中的矿工。选择了矿工后要选择矿池管理者。因此，本文提出算法2进行矿池管理者选择。矿池管理者由矿池中信誉值 P 最高和相互监督值 c 最小的矿工担任，但在第一轮矿池进行挖矿时，矿工的信誉值都是初始值 θ ，因此初始的矿池管理者是随机选择的。在后面的轮次中，根据矿工对矿池管理者的监督和矿池管理者的行为来选择矿池管理者。

矿工进入矿池之后，根据矿池所提供的数学问题，矿工提交解决该数学问题的工程量，触发智能合约，根据工程量给出相应的奖励。根据条件2，矿池管理者必须从已经进入矿池的矿工中选择。并且，选择信誉值最高的矿工和投诉最少的矿工作为矿池管理者。

算法2 选择矿池中的管理者

输入 矿池中的矿工 $I = \{M_i\}$

输出 矿池管理者 M_L

- 1) initial $M_L = \text{Rand}(I = \{M_i\})$
- 2) for each $M_i \in I$ do
- 3) if $((P_{M_i} \geq P_{M_{i+1}}) \cap (c_i \leq c_{i+1}))$ then
- 4) $\bar{M}_L = \{M_i\}$
- 5) end if
- 6) $i = i + 1$
- 7) end for
- 8) length = sizeof($\bar{M}_L$)
- 9) if length > 1 then
- 10) $M_L = \text{Rand}(\bar{M}_L)$
- 11) end if

在算法2中，根据信誉值和矿工对矿池管理者的监督值来选择矿池管理者。在被标记的矿工中选择信誉值最大和被投诉最少的矿工作为矿池管理者。如果出现多个矿工满足这两个条件，随机选择一个矿工作为矿池管理者。

2.2 矿池更新

矿池不是静态的，而是动态更新的。矿池中的矿工根据在第 k 轮次的状态是确定的，矿工在下一个轮次，即第 $k+1$ 次的状态是根据矿工在第 k 轮次矿工提交工程量证明来改变的，与之前轮次矿工的状态无关。因此，矿池中的矿工提交工程量证明的过程符合马尔可夫过程。根据马尔可夫过程，矿池中矿工的状态从提交有效工程量证明的状态转移到提交无效的工作量证明的状态。矿工提交有效工程量证明的状态表示为 H ，矿工提交无效工程量证明的状态表示为 D 。在本文方案中，矿池的总算力为1，诚实矿工的算力为 α ，则恶意矿工的算力为 $1-\alpha$ 。假设在矿池一轮提交工程量证明的过程中，可以挖掘出一整个区块，完整的工作量证明为1。矿池管理者 M_L 收到的有效工作量证明为 δ ，则无效工作量证明为 $1-\sigma$ 。假设诚实矿工提交的有效工作量的概率为 λ ，则诚实矿工提交无效工作量的概率为 $1-\lambda$ 。恶意矿工提交无效工作量的概率为 β ，则恶意矿工提交的有效工作量的概率为 $1-\beta$ 。矿池收到的有效工作量是由诚实矿工提交有效的工作量证明和恶意矿工提交的有效工作量证明组成。无效工作量由诚实矿工提交的无效工作量证明和恶意矿工提交的无效工作量证明组成。因此，可以得到如下等式：

$$\begin{cases} \alpha\lambda + (1-\alpha)(1-\beta) = \delta \\ \alpha(1-\lambda) + (1-\alpha)\beta = 1-\delta \end{cases} \quad (4)$$

由式(4)可以得出 $\beta = \frac{1+\alpha\lambda-\alpha-\delta}{1-\alpha}$ 。在马尔可夫过程中，矿工的状态转移矩阵 ρ 为：

$$\rho = \begin{bmatrix} \lambda & 1-\lambda \\ \frac{\delta-\alpha\lambda}{1-\alpha} & \frac{1+\alpha\lambda-\alpha-\delta}{1-\alpha} \end{bmatrix} \quad (5)$$

矿工在第 k 轮次中的信誉值为 P_k ，因此矿工在 k 轮次的状态为 $\rho_k = [P_k, 1-P_k]$ 。根据转移矩阵 ρ 可得矿工状态马尔可夫链，如图 2 所示。从图 2 可以得出矿工状态转移概率，并且可得下一个状态第 $k+1$ 轮次的状态 $\rho_{k+1} = \rho \cdot \rho_k$ 。第 $k+1$ 轮次的状态只与第 k 轮次的状态有关，与之前的矿工状态无关。通过状态转移来动态更新矿池，当矿池中的矿工一直处于提交无效工作量证明的状态时，会导致该矿工的信誉值减小，当矿工的信誉值小于 θ 时会被剔除出矿池。其中 λ 要尽可能大，但不能太大，因为在实际的情况中，诚实矿工可能在下一个状态进行恶意挖矿。

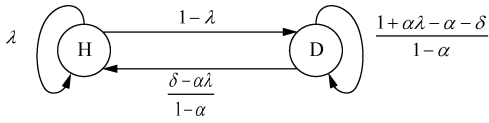


图 2 矿工状态马尔可夫链
Figure 2 Miner state Markov chain

2.3 奖励机制设计

矿池中的矿工根据算法 2 选出矿池管理者，矿池管理者在矿池中部署智能合约。矿工根据自身的算力提交工作量证明来触发合约，根据之前矿池管理者制定的规则，合约对矿工所提交的工作量证明进行验证审查，验证通过之后，合约给出相应的奖励和信誉值，并且在给出奖励时，给出矿池标识参数 S 。奖励机制设计如图 3 所示，矿池中的矿工选出矿池管理者，矿池管理者部署智能合约，矿工提交工作量，根据合约预先写好的程序得到奖励。要在矿池中的矿工提交工作量之前选择出矿池管理者，防止部分恶意矿工和矿池管理者进行合谋，导致矿池中奖励分配不均。

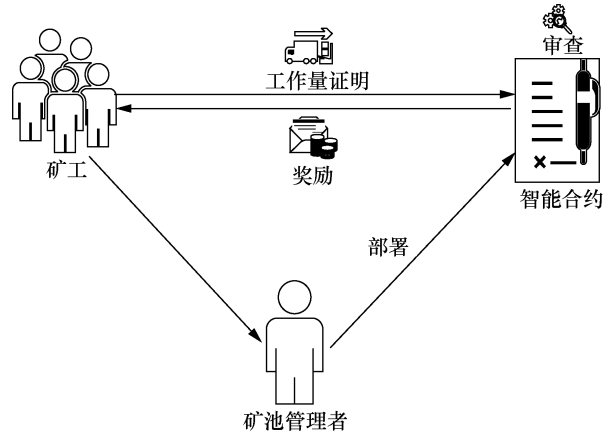


图 3 奖励机制设计
Figure 3 Design of reward mechanism

本文不考虑矿池的管理费用，即矿池所获得的全部收益区块奖励分配给矿工。在矿池系统中，每一轮创建区块的过程可以将完整性证明的工作量分为 N 个部分工作量证明。矿工提交的部分工作量证明 N 的位置是随机的，即矿池中的矿工发现工作量的概率为 $1/N$ 。同时在每轮挖矿过程中的挖矿难度 D 和一个区块的奖励 R 是固定不变的。挖掘区块的过程近似于泊松分布，在恒定算力下，区块以一定的概率被独立开采。由文献[28]可知，一个算力为 H 的节点在 t 时间段内，挖到的区块数量为 $Ht/2^{32}D$ ，获得的收益为 $HtR/2^{32}D$ 。由此可得，在 t 时间段内，矿工提交的工作量证明可以相当于矿工的算力，即 $\eta = H$ 。所以矿池中的矿工获得的收益如式(6)所示。

$$w = \frac{\eta R}{2^{32} D} \quad (6)$$

本文构造算法 3 设计信誉管理模型的奖励机制，矿工提交工作量证明，触发智能合约，智能合约检查正确性，然后自动执行程序，矿工得到相应的奖励 w_i 、信誉值 P_{M_i} 和矿池标识 S_j 。该奖励机制使得矿池中的诚实矿工能得到激励，维护矿池的正常运转。

算法 3 奖励机制设计

输入 $\eta(M_i)$

输出 w_i, S_j, P_{M_i}

- 1) for each $M_i \in I$
- 2) if $P_{M_i} \geq \theta$ then
- 3) 矿池管理者 M_L 部署合约

- 4) 矿工 M_i 提交工作量证明 η ，触发智能合约
- 5) 智能合约检查正确性给出相应的奖励
- 6)
$$P_{M_i} = \frac{P_{M_{i-1}} \cdot \eta + r_i - f_i - c_i}{r_i + f_i + c_i + 1}$$
- 7)
$$w_i = \frac{\eta t R}{2^{32} D}$$
- 8) $S = S_j$
- 9) end if
- 10) $i = i + 1$
- 11) end for

矿工不管提交的是有效的工作量还是无效的工作量，如果触发智能合约，矿工都会被该矿池所标记，并有相应的标记 S_j 。并且在提交工作量时，通过合约，矿工会收到相应的信誉值 P_{M_i} 和奖励 w_i 。

3 安全性和性能分析

3.1 安全性分析

本文围绕在矿池中如何鉴别矿工的类型，选出诚实的矿工。安全性分析主要从两个方面进行。安全地鉴别诚实矿工；在矿工提交工作量后，安全地收到奖励和信誉值。矿池中除了常见的区块链攻击，还包括分布式拒绝服务攻击、区块截留攻击，这些攻击主要是矿工的恶意行为导致的。

定理 1 如果基于椭圆曲线数字签名算法 (ECDSA, elliptic curve digital signature algorithm) 的签名是不可伪造的，则矿工和矿池管理者提交的工作量是安全的。

证明 矿工和矿池管理者在提交工作量证明时，需要验证各自签名是否正确。只有签名正确才能提交工作量证明来获取奖励。假设存在敌手在一轮提交工作量证明时，伪造矿工的签名 $\text{Sig}(M_i')$ 和矿池管理者的签名 $\text{Sig}(M_L')$ 。敌手为了获得矿工提交工作量证明之后的奖励，伪造签名提交工作量。敌手操作如下。

- 1) 获取要提交的工作量 η 。
- 2) 使用伪造的矿工的签名 $\text{Sig}(M_i')$ 和矿池管理者的签名 $\text{Sig}(M_L')$ 。
- 3) 验证签名是否正确。

$\text{Ver}[\eta, \text{Sig}(M_i')] = \text{true}$

$\text{Ver}[\eta, \text{Sig}(M_L')] = \text{true}$

- 4) 通过伪造的签名的工作量来获得奖励。

若敌手最终获得奖励，则说明敌手伪造的签名可以验证通过，这与假设相矛盾，故敌手不可能伪造签名来获取奖励。在矿池中只有验证签名通过，才能获得奖励。而基于 ECDSA 的签名是不可伪造的，所以矿工和矿池管理者提交工作量是安全的。

证毕。

定理 2 如果基于 ECDSA 的签名是不可伪造的，那么矿工信誉值不能被恶意篡改。

证明 由式(2)可得，矿工每提交一轮工作量，相应的信誉值发生变化。假设敌手伪造矿池管理者的签名 $\text{Sig}(M_L')$ ，敌手具体操作如下。

当矿工提交工作量证明给矿池管理者，矿池管理者再以工作量作为触发条件，触发智能合约。得到奖励 w 、信誉值 P 和矿池标识参数 S 。敌手通过伪造矿池管理者的签名对矿工信誉值进行签名，若矿工收到敌手伪造的信誉值，则说明敌手伪造的签名验证通过。这与假设相矛盾，故矿工收不到篡改的信誉值。因此基于 ECDSA 的签名是不可伪造的，矿工信誉值不能被恶意篡改。

证毕。

通过智能合约避免矿工和矿池管理者进行合谋，从而避免部分矿工和矿池管理者的收益更高，使矿池运行正常。同时，矿池管理者必须从矿池中选择，矿池管理者的信誉值应该最高。

3.2 性能分析

为了评估本文提出的信誉管理模型，对方案进行模拟实验，检测方案的正确性。考虑矿工的信誉值与所提交给矿池管理者工作量的关系，证明矿工的信誉值低于矿池的信誉阈值时，会被剔除出矿池外。同时根据全网的难度和单位时间内挖掘出一整个区块的奖励，可以得出奖励与部分工作量证明之间的关系。

矿池信誉阈值不能设置太高，这样会导致在矿池中工作的矿工比较少，矿池的收益比较少。同样矿池信誉值不能设置太低，这样会导致大量矿工进入矿池，其中会有大量的恶意矿工，导致矿池运转不正常。本文的信誉阈值引用文献[19]的信誉阈值，即 θ 为 0.5。

为了研究矿池中矿工的信誉值与矿工提交工作

量的关系。根据图 4 可得,通过改变矿工提交给矿池管理者所提交的工作量来观察矿池中矿工的信誉值。当矿工提交工作量触发智能合约,智能合约给出相应的信誉值。矿工在每一轮中提交的工作量越多,该矿工的信誉值越高。但是矿工进入矿池的信誉值最低不能低于信誉阈值 θ ,因此矿工的信誉值从信誉阈值 0.5 开始,随着提交工作量的提升而增加。

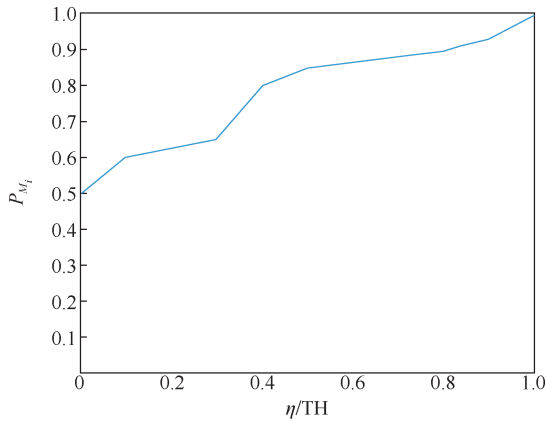


图 4 信誉值随工作量变化
Figure 4 Reputation value changes with workload

为了研究本文方案中模型的可靠性,研究矿工在矿池中的表现,模拟矿池运转多轮次工作。根据图 5 可得,本文的信誉管理模型可以鉴别出矿工的类型。在矿池中的矿工刚开始都在诚实地挖掘,诚实的矿工会一直诚实地挖掘,但恶意矿工后面会进行不诚实行为。根据本文提出的信誉管理模型,矿池管理者根据矿工的行为调整信誉值。当矿工的信誉值 $P_{M_i} < \theta = 0.5$ 时,矿工会被矿池管理者剔除矿池。并且,矿工会有矿池的标识,下次不能再进入矿池进行挖掘,提交工作量。

为了研究矿池的动态更新情况,根据图 2 中的马尔可夫链设置不同的 λ 值,在实际中矿池工作中,诚实矿工更倾向于继续进行诚实挖矿,但理论上存在诚实矿工进行不诚实挖矿的情况。因此, λ 的值设置为 0.6、0.7、0.8、0.9。图 6 和图 7 可以表明根据不同的 λ 值,诚实矿工和不诚实矿工在相同的轮次的信誉值不同,当 $\lambda = 0.9$ 时,矿池才能最快地识别不诚实的矿工。当不诚实矿工持续作恶,信誉值低于信誉阈值时,会被剔除出矿池,矿池进行动态更新。

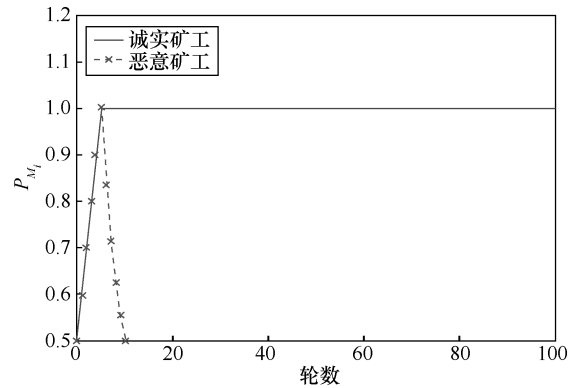


图 5 鉴别矿工类型
Figure 5 Identification of miner types

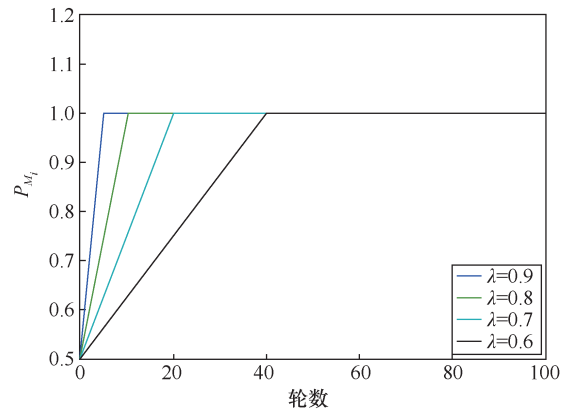


图 6 诚实矿工信誉值根据 λ 变化的情况
Figure 6 Honest miners reputation value changes according to λ

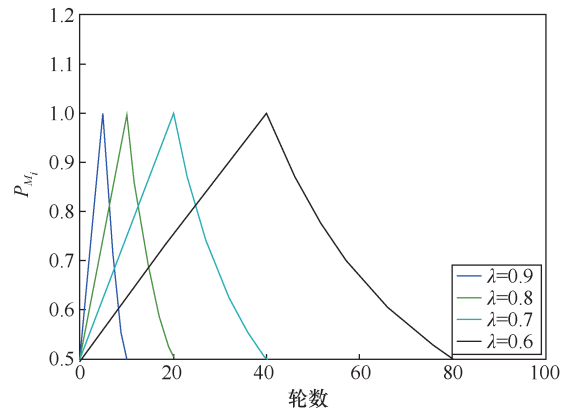


图 7 不诚实矿工信誉值根据 λ 的变化
Figure 7 Dishonest miners reputation value changes according to λ

矿工提交工作量证明触发智能合约,智能合约根据矿池管理者提前在智能合约设置的奖励程序和矿池中的信誉值程序,并且还设置了一个带有矿池标记的参数 S 。在单位时间内,全网挖矿的难度 D 和挖出整个区块的奖励 R 是不变的,不计算矿池所收的手续费。从图 8 可得出矿池中的矿工所获的奖励 w 和所提交的工作量 η 之间的关

系是成正比的。从获得奖励来看，单个矿工的算力要足够大，才能比较长的时间内，获得整个区块奖励。所以加入矿池获得奖励，才最具有经济效益。

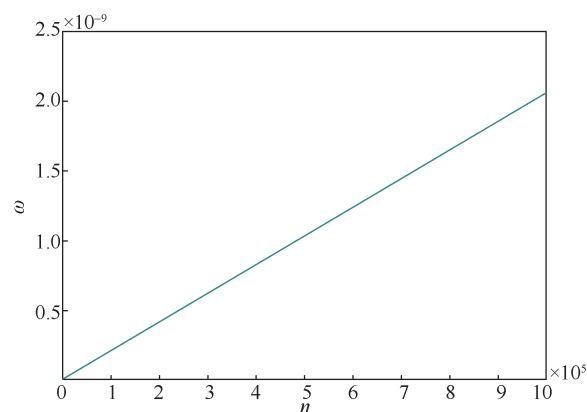


图8 矿工收益
Figure 8 Benefit of miners

本文方案与其他方案的对比如表1所示，引入智能合约部署在区块链网络中，设计了一种激励机制，并且在智能合约中设置矿池的标识参数 S 。实现了矿池中的矿工在提交工作量证明和收到相应的奖励时，自动分配，避免矿工和矿池管理者在此过程中进行合谋。

表1 本文方案与其他方案的对比
Table 1 Comparison of the scheme with other scheme

方案	公平性	奖励机制	动态更新
文献[18]	×	√	×
文献[19]	√	×	√
文献[29]	√	√	×
本文方案	√	√	√

文献[18]提出的机制中，每个矿工的声誉是由一个随机选择的矿工来评价的，这个矿工将扮演矿池的管理经理。但是，矿池管理者是随机选择的，所以很容易受到攻击，这样造成不公平。基于博弈论，文献[18]设计了一种激励算法来鼓励矿工诚实挖掘，从而增加矿池的总收益。

文献[19]提出了一种新的存储链，对矿池中的管理者和矿工进行管理，其中，存储链中存储着矿工对矿池管理者的满意度。对矿池管理者进行标准化的选取，但矿工的信誉分数没有一个明确的标准。同时没有一种激励方式来激励矿工诚实进行工作，但是在该方案中来用满意度对矿池

进行动态更新。

文献[29]提出了一种比特币矿池理性矿工的激励机制，通过设计一种激励机制，使得理性矿工进行诚实提交工作量。但是，在该工作中没有考虑到在公开矿池中对矿池进行动态更新。

本文提出了一种信誉管理模型对矿池中的矿工进行类型鉴别优化。有明确的选择矿池管理者和矿工的标准，并部署了智能合约，对矿工诚实挖矿进行激励。同时矿工的提交工作量证明的过程满足马尔可夫过程，因此，根据马尔可夫过程中的状态转移对矿池进行更新。

4 结束语

本文研究了区块链网络中矿池矿工类型鉴别问题。考虑了在区块链网络中矿池存在不诚实矿工，因此设计了一种信誉管理模型对矿工的类型进行鉴别，选出诚实的矿工。根据矿工的行为，得到相应的信誉值。同时对本文所提出的方案进行仿真，确保方案的可靠性和有效性。

本文的下一步研究：在区块链网络中，利用结构熵把区块链网络看成一个有权连通图，通过边上的权值来计算信誉阈值，并通过信誉阈值来预测下次矿工的行为，并进行相应的约束。

参考文献：

- [1] NAKAMOTO S. Bitcoin: peer-to-peer electronic cash system[R]. 2009.
- [2] 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.
SHAO Q F, JIN C Q, ZHANG Z, et al. Blockchain: architecture and research progress[J]. Chinese Journal of Computers, 2018, 41(5): 969-988.
- [3] DINH T T A, LIU R, ZHANG M H, et al. Untangling blockchain: a data processing view of blockchain systems[J]. IEEE Transactions on Knowledge and Data Engineering, 2018, 30(7): 1366-1385.
- [4] PETERS G, PANAYI E, CHAPPELLE A. Trends in cryptocurrencies and blockchain technologies: a monetary theory and regulation perspective[J]. Journal of Financial Perspectives, 2015, 3(3): 1-25.
- [5] REYNA A, MARTÍN C, CHEN J, et al. On blockchain and its integration with IoT. Challenges and opportunities[J]. Future Generation Computer Systems, 2018, 88: 173-190.
- [6] 蔡晓晴, 邓尧, 张亮, 等. 区块链原理及其核心技术[J]. 计算机学报, 2021, 44(1): 84-131.
CAI X Q, DENG Y, ZHANG L, et al. The principle and core technology of blockchain[J]. Chinese Journal of Computers, 2021, 44(1): 84-131.
- [7] 刘懿中, 刘建伟, 张宗洋, 等. 区块链共识机制研究综述[J]. 密

- 码学报, 2019, 6(4): 395-432.
- LIU Y Z, LIU J W, ZHANG Z Y, et al. Review of blockchain consensus mechanism [J]. Journal of Cryptography, 2019, 6(4): 395-432.
- [8] XIA J Z, ZHANG Y H, YE H, et al. A visual analysis system for mine pool supervision[J]. Frontiers of Information Technology & Electronic Engineering, 202, 21(4): 507-524.
- [9] LEWENBERG Y, BACHRACH Y, SOMPOLINSKY Y, et al. Bitcoin mining pools: a cooperative game theoretic analysis[C]//Proceedings of the 2015 International Conference on Autonomous Agents and Multiagent Systems. 2015: 919-927.
- [10] FISCH B, PASS R, SHELAT A. Socially optimal mining pools[C]//International Conference on Web and Internet Economics. 2017.
- [11] CHANG S Y, PARK Y, WUTHIER S, et al. Uncle-block attack: blockchain mining threat beyond block withholding for rational and uncooperative miners[C]//Proceedings of International Conference on Applied Cryptography and Network Security, 2019: 241-258.
- [12] LIU X J, WANG W B, NIYATO D, et al. Evolutionary game for mining pool selection in blockchain networks[J]. IEEE Wireless Communications Letters, 2018, 7(5): 760-763.
- [13] SAPIRSHTAIN A, SOMPOLINSKY Y, ZOHAR A. Optimal selfish mining strategies in bitcoin[C]//Proceedings of International Conference on Financial Cryptography and Data Security Financial Cryptography and Data Security. 2017: 515-532.
- [14] EYAL I, SIRER E G. Majority is not enough: bitcoin mining is vulnerable[M]//Financial Cryptography and Data Security. Berlin, Heidelberg: Springer Berlin Heidelberg, 2014: 436-454.
- [15] JOHNSON B, LASZKA A, GROSSKLAGS J, et al. Game-theoretic analysis of DDoS attacks against Bitcoin mining pools[C]//Proceedings of International Conference on Financial Cryptography and Data Security. 2014: 72-86.
- [16] FENG J Y, ZHAO X Y, CHEN K X, et al. Towards random-honest miners selection and multi-blocks creation: proof-of-negotiation consensus mechanism in blockchain networks[J]. Future Generation Computer Systems, 2020, 105: 248-258.
- [17] LEE J, KIM Y. Preventing bitcoin selfish mining using transaction creation time[C]//Proceedings of 2018 International Conference on Software Security and Assurance (ICSSA). 2018: 19-24.
- [18] TANG C B, WU L Y, WEN G H, et al. Incentivizing honest mining in blockchain networks: a reputation approach[J]. IEEE Transactions on Circuits and Systems II: Express Briefs, 2020, 67(1): 117-121.
- [19] KACI A, RACHEDI A. PoolCoin: Toward a distributed trust model for miners' reputation management in blockchain[C]//Proceedings of 2020 IEEE 17th Annual Consumer Communications & Networking Conference. Piscataway: IEEE Press, 2020: 1-6.
- [20] 邸剑, 吝伟华. 区块链中矿池选择策略的研究与分析[J]. 计算机应用研究, 2020, 37(6): 1804-1807.
- DI J, LIN W H. Research and analysis of mining pool selection strategy in blockchain[J]. Application Research of Computers, 2020, 37(6): 1804-1807.
- [21] XU C Z, ZHU K, WANG R, et al. Dynamic selection of mining pool with different reward sharing strategy in blockchain networks[C]//Proceedings of ICC 2020 - 2020 IEEE International Conference on Communications. Piscataway: IEEE Press, 2020: 1-6.
- [22] GERVAIS A, KARAME G O, WÜST K, et al. On the security and performance of proof of work blockchains[C]//Proceedings of CCS '16: Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security. 2016: 3-16.
- [23] YUAN G. The framework of consensus equilibria for mining-pool games in blockchain ecosystems[J]. arXiv preprint arXiv: 2003.05067, 2020.
- [24] FUJITA K, ZHANG Y Y, SASABE M, et al. Mining pool selection problem in the presence of block withholding attack[C]//Proceedings of 2020 IEEE International Conference on Blockchain (Blockchain). 2020: 321-326.
- [25] LI W B, CAO M W, WANG Y, et al. Mining pool game model and Nash equilibrium analysis for PoW-based blockchain networks[J]. IEEE Access, 2020, 8: 101049-101060.
- [26] QIN R, YUAN Y, WANG F Y. A novel hybrid share reporting strategy for blockchain miners in PPLNS pools[J]. Decision Support Systems, 2019, 118: 91-101.
- [27] LI Q L, MA J Y, CHANG Y X, et al. Markov processes in blockchain systems[J]. Computational Social Networks, 2019, 6: 5.
- [28] ROSENFELD M. Analysis of bitcoin pooled mining reward systems[J]. arXiv preprint arXiv:1112.4980, 2011.
- [29] XUE G, XU J, WU H W, et al. Incentive mechanism for rational miners in bitcoin mining pool[J]. Information Systems Frontiers, 2021, 23(2): 317-327.

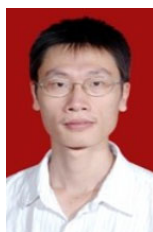
[作者简介]



余佳仁(1996-), 男, 湖北黄冈人, 贵州大学硕士生, 主要研究方向为区块链。



田有亮(1982-), 男, 贵州盘县人, 博士, 贵州大学教授、博士生导师, 主要研究方向为密码学与安全协议、大数据隐私保护与区块链技术等。



林晖(1977-), 男, 福建福州人, 博士, 福建师范大学教授, 主要研究方向为边缘计算、区块链、信任管理等。