基于博弈论抗共谋攻击的全局随机化共识算法

张宝[1,2]，田有亮[1,2]，高胜[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. 中央财经大学信息学院，北京 100081）

摘 要：随着区块链技术的不断发展，作为区块链技术基石的共识技术受到更多关注，共识技术的发展越发迅速，但依旧存在相关难题。容错类共识算法作为区块链共识技术的代表性之一，依然存在诸多难题待研究，针对容错类共识算法中节点随机性和节点共谋攻击问题进行了研究，提出基于博弈论抗共谋攻击的全局随机化共识算法，通过实现节点的随机化和解决相关安全问题提高区块链网络的安全性和吞吐量。在选择参与容错类共识算法的节点过程中，利用映射函数和加权随机函数实现发起者和验证者节点的全局随机化，从而保证发起者和验证者节点的身份匿名，提高区块链网络的安全性。利用信誉更新模型实现信誉动态更新的同时利用博弈论分析容错类共识算法的安全问题，构造更加正确和高效的算法模型以提高算法的吞吐量并分析发现这类算法中存在超过 1/3 节点的共谋攻击问题，利用精炼贝叶斯博弈构造共谋合约，分析求得共谋者之间的纳什均衡点，从而解决超过 1/3 节点的共谋攻击问题。通过安全性分析和实验表明，基于博弈论抗共谋攻击的全局随机化共识算法相对工作量证明（PoW，proof of work）、权益证明（PoS，proof of stake）和实用拜占庭容错（PBFT，practical Byzantine fault tolerance）共识算法不仅提高吞吐量、降低计算资源消耗，而且该算法抵抗分布式拒绝服务（DDoS，distributed denial of service）、Eclipse attacks 和超过 1/3 节点共谋攻击。

关键词：共识算法；全局随机化；博弈论；共谋攻击
中图分类号：TP393
文献标志码：A
DOI: 10.11959/j.issn.2096−109x.2022048

Global randomized consensus algorithm resist collusion attack based on game theory

ZHANG Bao[1,2], TIAN Youliang[1,2], GAO Sheng[3]

收稿日期：2021−11−22；**修回日期**：2022−03−01
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）；贵阳市科技计划项目（[2021]1-5）
Foundation Items: The National Natural Science Foundation of China (61662009, 61772008), Science and Technology Major Support Program of Guizhou Province (20183001), Key Program of the National Natural Science Union Foundation of China (U1836205), Science and Technology Program of Guizhou Province ([2019]1098), Project of High-level Innovative Talents of Guizhou Province ([2020]6008), Science and Technology Program of Guiyang ([2021]1-5)

引用格式：张宝, 田有亮, 高胜. 基于博弈论抗共谋攻击的全局随机化共识算法[J]. 网络与信息安全学报, 2022, 8(4): 98-109.
Citation Format: ZHANG B, TIAN Y L, GAO S. Global randomized consensus algorithm resist collusion attack based on game theory[J]. Chinese Journal of Network and Information Security, 2022, 8(4): 98-109.

1. Computer Science and Technology Institute, Guizhou University, Guiyang 550025, China
2. Guizhou Provincial Key Laboratory of Public Big Data, Guiyang 550025, China
3. Information Institute Central University of Finance and Economics, Beijing 100081, China

Abstract: As the cornerstone of blockchain technology, consensus technology has received more attention with the continuous development of blockchain technology. The development of consensus technology has become more and more rapid, but there are still related problems. Nowadays, fault-tolerant consensus algorithms, as one of the representative blockchain consensus technologies, still have many problems to be studied. The problem of node randomness and node collusion attacks in fault-tolerant consensus algorithms had been studied, and a game-theoretic-based anti-corruption algorithm was proposed. The global randomization consensus algorithm of collusion attack improved the security and throughput of the blockchain network by realizing the randomization of nodes and solving related security problems. In the process of selecting nodes participating in the fault-tolerant consensus algorithm, the global randomization of the initiator and verifier nodes was realized by using the mapping function and the weighted random function, thereby ensuring the identity anonymity of the initiator and verifier nodes and improving the blockchain network security accordingly. The reputation update model was used to realize the dynamic update of the reputation, and the game theory was used to analyze the security problems of the fault-tolerant consensus algorithm. A more correct and efficient algorithm model was constructed to improve the throughput of the algorithm and analyze the problem of collusion attack of more than one third of the nodes in this kind of algorithm, the refined Bayesian game was used to construct a collusion contract and analyze the collusion The Nash equilibrium point between the two nodes was adopted to solve the collusion attack problem of more than one third of the nodes. The security analysis and experiments show that the global randomization consensus algorithm based on the game theory anti-collusion attack is better than PoW、PoS and PBFT. The consensus algorithm is not only effective to improve throughput and reduce computing resource consumption, but also resistant to DDoS, Eclipse attacks and collusion attacks by more than one third of nodes.

Keywords: consensus algorithm, global randomization, game theory, conspiracy attack

0　引言

随着区块链技术的发展，对数据上链速度的要求越来越高，用高效且安全的共识协议来保证数据上链成为区块链系统的关键问题。在该背景下，如何解决基于工作量证明（PoW，proof of work）[1]和基于权益证明（PoS，proof of stake）的共识协议[2]中高资源浪费、低效率上链[3]、权益过大、富者越富、易分叉、易双花[4]等问题是重点。近年来，代理权益证明（DPoS，delegated proof of stake）[5]被认为是解决资源浪费、权益过大和低效率等问题的有效技术。该技术是一种基于投票选举的共识算法，只需要少部分的节点就能达成共识实现交易数据快速上链。基于拜占庭容错协议的 Tendermint[6]和 True Decentralization[7]协议的出现不仅保证了 1/3 节点的容错，而且只需要少部分节点对交易进行验证就可以达成最后的共识。

文献[8]提出了一种将 PoW 和 PoS 相结合的共识协议，该协议提供了更高的安全性和效率。文献[9]研究了交互式的 PoS 共识算法，将通信引入块，减少交互，提高效率和安全性，但该协议依然没有解决 PoS 存在的权益过大、易分叉和易双花问题。文献[10]利用 Kgmedoids 聚类算法根据参与区块链共识的大规模网络节点的特征进行聚类与层次划分，再将改进的多中心化实用拜占庭容错算法应用于这种聚类后的分层模型。文献[11]研究了新的共识算法固定验证器，但它依赖于极端信任的假设。文献[12]提出了一个无发起者、完全异步的拜占庭容错共识协议。文献[13]提出了一个委托随机拜占庭容错共识协议。文献[14]利用博弈论和智能合约解决了委托计算中不诚实双方的共谋问题。文献[15]提出了休眠共识（SC，sleepy consensus）机制，该机制只要在线诚实节

点超过故障节点就可以保证安全性。文献[16]基于发起者的拜占庭容错复制协议提出了 HB-BFT（honey badger of BFT）。文献[17]基于拜占庭提出了一种新的共识机制 Proteus，无论网络中出现多少次故障，Proteus 都能保证稳定的性能。

基于拜占庭容错的这类共识算法中，当提议者提出新块后，发起者接收到提议者指令后开始选择验证者，当验证者确定后由验证者投票达成最终的共识。共识的过程中实现参与节点的随机化是保证共识算法安全性的关键难题。而本文提出的基于博弈论抗共谋攻击的全局随机化共识算法（GRCACAGT，global randomized consensus algorithm resist collusion attack based on game theory）可以解决节点的全局随机化问题以及这类算法中存在的共谋攻击，主要贡献如下。

1) 提出 GRCACAGT，利用映射函数和加权随机函数实现共识算法中发起者节点的随机化。

2) 分析容错类共识算法发现 1/3 节点共谋攻击问题，并利用智能合约和贝叶斯博弈构造共谋合约解决了该问题。

3) 安全性分析和实验表明，GRCACAGT 不仅抗分布式拒绝服务（DDoS，distributed denial of service）、1/3 节点共谋等攻击，而且相比其他的共识算法，吞吐量和效率方面都有优势。

1 本文算法

本文基于 True Decentralization[7] 提出 GRCACAGT，GRCACAGT 与 True Decentralization 逻辑很像但构造不同。第一，确定所需要的验证者人数方法不同。GRCACAGT 是根据提议者的动态信誉值确定验证者人数，而 True Decentralization 是根据提议者的不诚实概率来确定验证者人数。第二，确定发起者的方法不同。True Decentralization 在起始块创建时就确定了发起者。而 GRCACAGT 每轮共识都需要选择新的发起者，因为 True Decentralization 中选择发起者的方法存在发起者节点身份暴露的安全问题。分析发现，当所有验证节点身份全部暴露时，节点池中剩下的节点就是发起者节点，此时发起者的身份也会暴露。第三，发起者选择验证者的方法不同。True Decentralization 是将节点池平均分为 4 个小的节点池，每个发起者对应一个小节点池，从对应的节点池中选择验证者。这样风险较大，因为在 True Decentralization 中虽然每次参与验证节点的身份在节点完成验证之后才会暴露，但经过多轮验证后，每个节点池中节点的身份都会暴露，此时通过节点出现的次数能确定哪些节点被选择的概率最大，所以少数的节点就能实现攻击。而 GRCACAGT 利用抽样不放回和加权随机的方法，相对 True Decentralization 不仅能增加 4 倍的安全性而且节点不会被重复选择。

在 GRCACAGT 中，每轮共识开始后首先随机选出发起者，并根据提议者的信誉大小确定验证者人数；然后根据更新后的信誉值加权随机选择验证者，该过程是利用抽样不放回的方法实现的，这样能够保证节点不被重复选择；最后利用博弈论分析 GRCACAGT 发现在验证上链阶段存在节点之间的共谋安全问题。本文将这种共谋定义为 1/3 节点共谋攻击，并提出共谋合约解决了该安全问题。图 1 为 GRCACAGT 模型。

区块链中每一个节点都有唯一的密钥（公钥 pk，私钥 sk），公钥作为每个节点的身份识别。每个节点都有自己的一个信誉值，这个信誉值是每个节点被选为发起者和验证者的权重，在该协议中存在 4 种类型的节点。

1) 提议者：创建新区块并向全网广播这个块。

2) 发起者：新区块广播后确定所需要的验证者。

3) 验证者：对新提出的区块进行投票达成共识。

4) 其余节点：矿池中没有参与共识的节点。

1.1 发起者的选择

该阶段博弈在提议者（Alice）和发起者（Bob）间进行，通过博弈结果确定发起者人数。发起者有两个策略，即最小验证者（MV）和更多的验证者（AMV），AMV 的大小是根据博弈结果确定的。Alice 和 Bob 存在两种状况（诚实或不诚实），Alice 不同的状况下有两种类型（作弊或不作弊）。

把 4 个发起者之间博弈看作一对一的独立博弈。由于 Bob 不知道 Alice 的类型，且提议者行动在先，发起者行动在后，两者的行动具有非同时性，所以该博弈是精炼贝叶斯纳什均衡（PBNE），发起者和提议者的博弈树如图 2 所示。

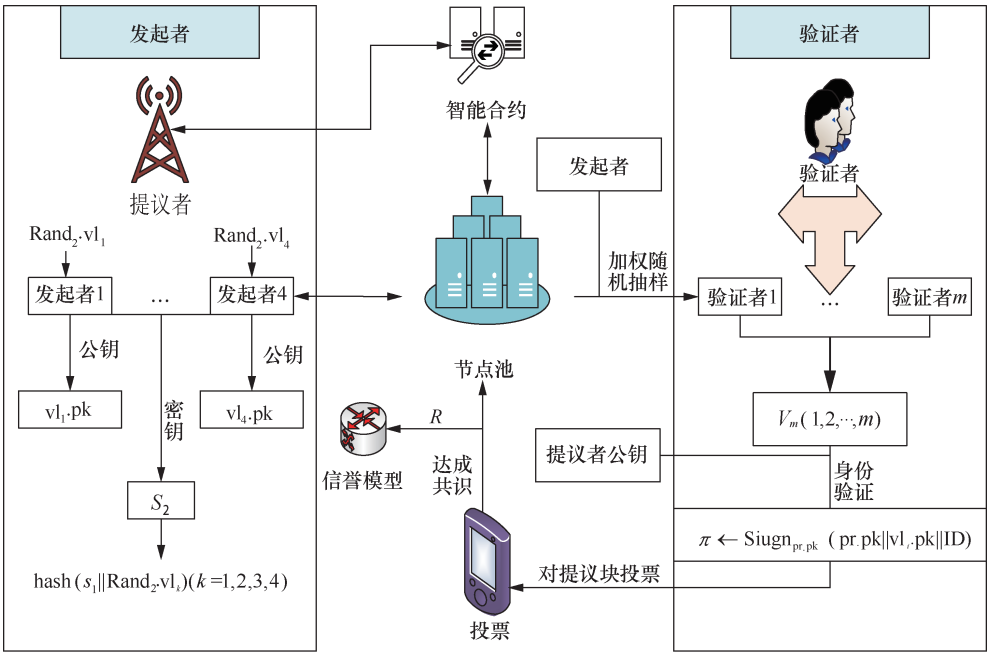

图 1　GRCACAGT 模型
Figure 1　GRCACAGT model

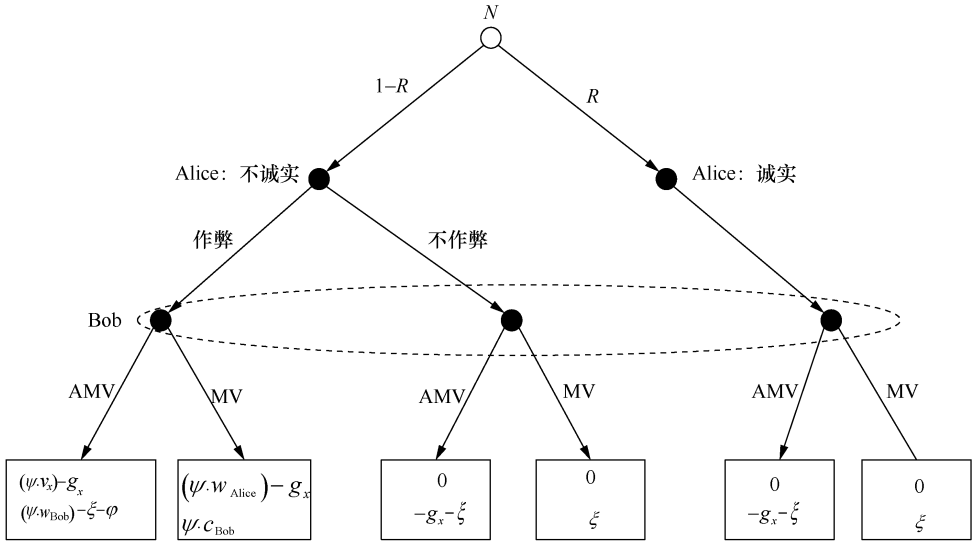

图 2　发起者和提议者的博弈树
Figure 2　Game tree of initiators and proposers

表 1 为系统中提议者和发起者间博弈的参数说明。图 3 表示提议者（Alice）为不诚实节点的收益矩阵，第一个收益是 Alice，第二个是 Bob。图 4 表示提议者（Alice）为诚实节点的收益矩阵。

纯策略：假设玩家 Alice 知道玩家 Bob 的信誉值为 R，那么 Alice 确定他的策略之后，对于玩家 Bob 选择 AMV 的预期收益为

$$E_{R-\mathrm{Bob}}(\mathrm{AMV})=\left\{(1-R)\cdot\left[\left(\psi w_{\mathrm{Bob}}\right)-\xi-\varphi\right]\right\}+\left\{R\cdot\left(-g_x-\xi\right)\right\} \tag{1}$$

同理，玩家 Bob 选择 MV 的预期收益为

$$E_{R-\mathrm{Bob}}(\mathrm{MV})=\left[\psi\cdot c_{\mathrm{Bob}}(1-R)\right]+R\cdot\xi \tag{2}$$

当 $E_{R-\mathrm{Bob}}(\mathrm{AMV})\succ E_{R-\mathrm{Bob}}(\mathrm{MV})$ 时，即

$$\left\{(1-R)\cdot\left[(\psi w_{\text{Bob}})-\xi-\varphi\right]\right\}+\left\{R\cdot(-g_x-\xi)\right\}\succ \left[\psi\cdot c_{\text{Bob}}(1-R)\right]+R\cdot\xi \tag{3}$$

表 1　参数说明

Table 1　Parameter description

参数	含义
ψ	提议者节点的比重
λ	最小发起者相对更多发起者的收益
ξ	最小验证者相对更多验证者的收益
g_x	节点作弊的影响
v_x	节点作弊被发现的损失
w_{Alice}	提议者作弊没被抓的利益
w_{Bob}	发起者作弊被抓的损失
c_{Bob}	发起者不能抓住作弊提议者的损失
φ	AMV 大于 MV 部分节点作弊的损失

博弈矩阵		发起者（Bob）	
		AMV	MV
提议者（Alice）	作弊	$(\psi\cdot v_x)-g_x$ $\left[(\psi\cdot w_{\text{Bob}})-\xi\right]-\varphi$	$(\psi\cdot w_{\text{Alice}})-g_x$ $\psi\cdot c_{\text{Bob}}$
	不作弊	$0,-g_x-\xi$	$0,\xi$

图 3　提议者（Alice）为不诚实节点的收益矩阵

Figure 3　The utility matrix when the proposer (Alice) is the dishonest nodes

博弈矩阵		发起者(Bob)	
		AMV	MV
提议者（Alice）	不作弊	$0,-g_x-\xi$	$0,\xi$

图 4　提议者(Alice)为诚实节点的收益矩阵

Figure 4　The utility matrix when the proposer (Alice) is the honesty nodes

通过化简之后得到

$$R\prec 1-\frac{2\xi+g_x}{\psi\left(w_{\text{Bob}}-c_{\text{Bob}}\right)+\xi-\varphi-g_x} \tag{4}$$

这时对于玩家 Bob 来说，最好的选择是 AMV。如果玩家 Bob 选择了 AMV，那么作弊对于玩家 x 为不诚实节点就不再是最好的决策，这时他会选择不作弊，所以((不诚实节点且作弊, 诚实节点不作弊)，选择 AMV, R)不是一个贝叶斯纳什均衡点。

当 $E_{R-\text{Bob}}(\text{AMV})\prec E_{R-\text{Bob}}(\text{MV})$ 时，即

$$R\succ 1-\frac{2\xi+g_x}{\psi\left(w_{\text{Bob}}-c_{\text{Bob}}\right)+\xi-\varphi-g_x} \tag{5}$$

这时玩家 Bob 最好的选择是 MV，((不诚实节点且作弊, 诚实节点不作弊)，选择 MV, R)是一个纯策略的精炼贝叶斯纳什均衡。

混合策略：在式(4)成立时，不存在纳什均衡，所以存在 PBNE 的混合策略，假设玩家(Alice)作弊的概率为 p，玩家 Bob 选择 AMV 的概率为 q，则玩家 Bob 选择 AMV 的预期收益为

$$E_{R-\text{Bob}}(\text{AMV})=\left\{p(1-R)\left[\left((\psi\cdot w_{\text{Bob}})-\xi-\varphi\right)\right]\right\}+\left\{(1-p)(1-R)(-g_x-\xi)\right\}\left[R\cdot(-g_x-\xi)\right] \tag{6}$$

玩家 Bob 选择 MV 的预期收益为

$$E_{R-\text{Bob}}(\text{MV})=\left[p(1-R)(\psi\cdot w_{\text{Alice}}-g_x)\right]+(1-p)\left[(1-R)\cdot\xi+R\cdot\xi\right] \tag{7}$$

当 $E_{R-\text{Bob}}(\text{AMV})\succ E_{R-\text{Bob}}(\text{MV})$ 时，即

$$p\succ\frac{\varphi+2\xi}{(1-R)\left[\left(w_{\text{Bob}}-w_{\text{Alice}}\right)+\xi\right]} \tag{8}$$

同理，当 Alice 不诚实时，可预期收益函数为

$$E_{R-\text{Alice}}(\text{不诚实})=\left\{q(1-R)(\psi\cdot w_{\text{Bob}}-g_x)\right\}+\left\{(1-q)(1-R)(\psi\cdot w_{\text{Alice}}-g_x)\right\} \tag{9}$$

玩家 x 不作弊的收益为

$$E_{R-\text{Alice}}(\text{诚实})=0 \tag{10}$$

当 $E_{R-\text{Alice}}(\text{不诚实})\succ E_{R-\text{Alice}}(\text{诚实})$ 时，即

$$q\succ\frac{g_x-\psi w_{\text{Bob}}}{(1-R)\left(w_{\text{Bob}}-c_{\text{Bob}}\right)} \tag{11}$$

PBNE 的混合策略为

$$\left((\text{不诚实}q,\text{诚实不作弊}),p,(1-p)\right) \tag{12}$$

然而，这个策略是在一对一的博弈下得到的，事实上，每个 Alice 节点都对应 4 个发起者节点，所以 $((\text{不诚实}q,\text{诚实不作弊}),p,(1-p))$ 并不是 PBNE 混合战略下的最优策略。根据之前的假设，每个发起者之间都是独立存在的，4 个发起者中只要有一个选择 AMV，就满足 4 个发起者选择的验证者数量之和大于 16，所以 4 个发起者选择 AMV 的概率 p^* 定义为

$$p^*=1-(1-p)^4 \tag{13}$$

这里，p^*是一个发起者选择 AMV 的概率。

当确定了 4 个发起者选择 AMV 的概率 p^* 后，只要 4 个发起者有 3 个发起者是诚实的，玩家 Alice 就不会选择作弊，此时玩家 Alice 的概率等于之前的概率减去 3 个发起者选择 AMV 的概率，则玩家 Alice 作弊的概率 q^* 为

$$q^* = q - \left(p^* - p\right) \tag{14}$$

PBNE 混合战略的策略为

$$\left(\text{不诚实}q^*, \text{诚实不作弊}，\ p, (1-R)\right) \tag{15}$$

1.2　验证者的选择

发起者确认后，利用加权随机抽样（WRS）算法和抽样不放回的方法确定验证者节点。先通过提议节点的信誉值 R 确定所需要验证者的数量，每个发起者都需要在剩余节点集 U_K 中随机选择验证者，这就存在两种可能情况：同一个发起者会选择同一个节点作为验证者；不同的发起者选择同一个节点作为验证者。设 $m(m=0,1,2,\cdots,n)$ 个验证者对应的序列集合 $V_m(j_1,j_2,\cdots,j_m)$，V_j 的元素个数等于 m 的大小，随着验证者个数的增加，V_j 的元素个数也增加，确定 m 个验证者时剩余节点的集合 U_t 为

$$U_t \leftarrow \left(U_K - V_m\right) \tag{16}$$

这一部分存在 3 个表：第一个是集合 A，表示节点池中所有节点并且包含每个节点的信誉值 R；第二个是集合 B，它包含提议者选定的发起者的公钥，这个表在一个节点确定了发起者并且通过验证之后进行更新；第三个是集合 C，C 存储 4 个元组，每个元组对应一个发起者，每个元组包括秘密 $s2$ 、随机数 Rand2、证明 π 和剩余节点 U_t，当节点成为提议节点时将确切地使用一个提议者的秘密 $s1$ 。

1.3　节点的信誉更新

利用层次自组网中基于节点角色的新信誉模型实现 R 动态更新[18]，可以通过将节点自身的经验与其行为和其在路由过程中的合作有效性相结合来评估信誉，通过信誉值确定节点的安全情况来选择具有较高价值的节点，以确保通信可靠。因为不同节点之间可能存在一定的关系，可以根据节点的作用将信誉分为提议者发起者之间的信誉（PLR）、发起者验证者之间的信誉（LVR）、提议者验证者之间的信誉（PVR），根据各个信誉之间的关系制定的信誉更新模型如图 5 所示。

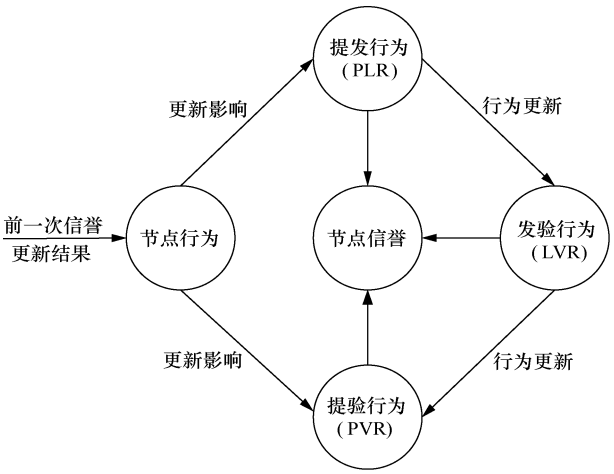

图 5　信誉更新模型

Figure 5　Credibility updating model

在一轮的验证过程中，节点池中节点分为提议者、发起者、验证者和其他，每一个节点都有自己的任务，任务结束后每个节点的信誉会有所变动，通过影响信誉值元素的大小变化而更新对应节点的信誉值。随着 PLR、LVR 和 PVR 大小的变化实现节点信誉的更新。提议者提出假的交易块信誉就会被降低，区块通过验证则信誉增大。对于发起者，只有在积极参与验证的情况下信誉才会有所增加。对于验证者也是如此。

2　GRCACAGT 共谋攻击

2.1　1/3 节点共谋攻击

GRCACAGT 在达成共识部分分为身份验证和投票达成两个阶段。首先将验证者人数平均分为两部分，一部分作为发起者身份验证阶段的验证，身份验证成功后另一部分验证者再进行投票达成共识。所以，只有身份验证和投票达成阶段结果正确共识结果才可信。通过博弈论分析发现这个过程中存在严重的安全问题。分析发现通过多次共识后，节点被选择的概率就会被暴露，概率大的节点会选择共谋，当共谋节点数量大于整体的 1/3，整个区块链系统就会面临严重的安全问题。本文将这种共谋攻击称为 1/3 节点共谋攻击，并构建共谋合约解决了该安全问题。

对于该共谋攻击问题，本文首先分析了实现攻击的共谋节点数量及对应的概率，主要分为两个部

分（最大数量的共谋节点，最小数量的共谋节点），然后利用智能合约设立共谋合约，再通过博弈论分析不同选择的效用函数证明该共谋合约的正确性。

假设所有节点被选择的概率都一样，节点池中节点个数为 n，通过博弈确定 m 个验证者参与验证，把 m 个验证者分为（$m1, m2$）两个部分，分别进行发起者身份验证和投票共识阶段。假如在 n 中存在 1/3 以上的人共谋，那么 m 中存在 1/3 以上节点共谋的概率 p_a 为

$$p_a \geqslant 1-\frac{A_{\left\lceil\frac{n}{3}\right\rceil}^{\left\lceil\frac{m}{3}\right\rceil}}{A_n^m} \tag{17}$$

其中，$\lceil x\rceil$ 表示向上取整函数。

在发起者身份验证阶段中，参与的验证者为 $m1$，验证结果不可信的概率 p_{one} 为

$$p_{\text{one}} \geqslant p_a\left(1-\frac{A_{\left\lceil\frac{m}{3}\right\rceil}^{\left\lceil\frac{m1}{3}\right\rceil}}{A_m^{m1}}\right) \tag{18}$$

第二阶段共识结果不可信的概率 p_{two} 为

$$p_{\text{two}} \geqslant p_{\text{one}}+p_a\left(1-\frac{A_{\left\lceil\frac{m}{3}\right\rceil}^{\left\lceil\frac{m2}{3}\right\rceil}}{A_m^{m2}}\right) \tag{19}$$

攻击者人数越多，攻击成功的概率越大，攻击者的期望值越高，因此共谋人数通常远高于节点池中的 1/3 节点。

对于这种情况，本文假设存在 $\lfloor kN\rfloor$ $(\frac{1}{3}\prec k\prec 1)$ 个节点形成共谋，那么共识结果不可信的概率为

$$P\geqslant\left(1-\frac{A_{kn}^{\left\lceil\frac{m}{3}\right\rceil}}{A_N^m}\right)\left(1-\frac{A_{\left\lceil\frac{m}{3}\right\rceil}^{\left\lceil\frac{m1}{3}\right\rceil}}{A_m^{m1}}\right)+\left(1-\frac{A_{kn}^{\left\lceil\frac{m}{3}\right\rceil}}{A_n^m}\right)\left(1-\frac{A_{\left\lceil\frac{m}{3}\right\rceil}^{\left\lceil\frac{m2}{3}\right\rceil}}{A_m^{m2}}\right) \tag{20}$$

其中，k 的大小可以通过 P 的大小和各自的效用函数确定，则最大的共谋节点数量为 $\lfloor kN\rfloor$。

而最小的共谋节点数量为发起者身份验证节点成功实现 1/3 节点共谋攻击时的共谋节点个数，设为 m_a。

$$m_a=\frac{m1}{3} \tag{21}$$

若共谋者要实现发起者身份验证结果不可信，则所有共谋节点都要在该阶段选择验证者时被选中，该概率为

$$p_a'\geqslant 1-\frac{A_{N-m}^{m-m_a}+A_{m_a}^{m_a}}{A_n^m} \tag{22}$$

则发起者身份验证结果不可信的概率 p' 为

$$\begin{aligned}p'\geqslant p_a'\left(\frac{A_{m-m1}^{m1-m_a}+A_{m_a}^{m_a}}{A_m^{m1}}\right)=\\ \left(\frac{A_n^m-A_{N-m}^{m-m_a}+A_{m_a}^{m_a}}{A_n^m}\right)\left(\frac{A_{m-m1}^{m1-m_a}+A_{m_a}^{m_a}}{A_m^{m1}}\right)\end{aligned} \tag{23}$$

通过以上分析可知在 1/3 节点共谋攻击中，当一些节点之间达成共谋之后，该协议被攻击的概率是一个不能忽视的大小，因此解决 1/3 节点共谋攻击问题对该类算法的安全性具有重要意义。

2.2 共谋合约

2.2.1 建立合约

当矿池中的节点被选为发起者或验证者节点后，每个节点都上传一笔保证金，保证节点的诚实行为。若节点行为诚实，完成共识后将会退回，但发现节点行为不诚实时将会被扣除，在共识阶段，理性的矿工为了使自己的利益最大化会寻求共谋，对于这个共谋问题，本文利用构建共谋合约来解决。合约规定，当节点发起共谋后，接收到共谋消息的节点可以选择同意或举报，当节点选择举报策略后，发起共谋节点保证金将被扣除，而举报者获得共谋节点的保证金作为举报奖金，并且两者信誉值将会更新，合约如下。

实现共谋攻击需要矿池中多个节点共谋，矿池中每个节点之间的共谋相互独立，假设每次的共谋节点为 c1 和 c2，节点 c1 和 c2 之间共谋，共谋合约参数如表 2 所示。

1) c1, c2 输入 x 时，系统自动执行 $f(x)$函数。

2) 节点加入区块链时支付保证金 w 到系统，执行 $f(x)$函数确定 w 是否要被扣除。

3) 举报共谋，假设 c1 给 c2 发起共谋，然后其中一方举报另一方。分为两种情况：c1 给 c2 发起共谋，c2 同意之后，c1 反过来举报 c2 获得 c2 的保证金；c1 给 c2 发起共谋，c2 假装答应，等 c1 签字确认共谋后，c2 举报 c1 获得 c1 保证金。

4) 将共谋者信誉值 R 归零，举报者信誉增加。

表 2　合约参数
Table 2　The contract parameters

参数	含义
φ	确定节点性质的方法数
R	节点的信誉值
col	节点发起共谋的成本
caf	节点提价的保险金
ei	节点共谋攻击成功的收益
vc	系统验证举报信息的费用
ni	节点之间不存在共谋时的收益

2.2.2　合约分析

通过合约的建立可以得到节点 c1 和 c2 共谋双方的博弈树，如图 6 所示。假设 c1 发起共谋，c2 同意的概率为 $p1$，c1 举报 c2 的概率为 $p2$，因为在该共谋合约中作为 c1 不知道当它发起共谋时 c2 是否会同意共谋，但是可以根据共谋攻击获得的利润、获得的举报奖金以及它的信誉值等这些信息判断 c2 同意共谋的概率 $p1$。同样的 c2 会根据举报奖金、攻击成功获得的利益以及 c1 的一个信誉值确定被 c1 举报的概率 $p2$。利用不完全信息动态博弈分析该博弈，确定最后的精炼贝叶斯纳什均衡解。

本文利用精炼贝叶斯纳什均衡的方法求均衡解，要达到最优必须每步最优。如图 6 所示。先分析 c2 同意共谋是否最优，对于 c2 来说，当它选择了同意，那么希望 c1 不举报它，最终达成共谋成功获得额外收益。如果 $p2$ 较大，那 c2 相对于同意的策略不是最优，即相对于 c1 来说选择不举报是 c2 选择同意的目的，即

$$p_2\left(-\text{col}+\text{caf}+\text{ni}-\text{vc}\right)>\left(1-p_2\right)\left(-\text{col}+\text{ei}+\text{ni}\right) \tag{24}$$

化简之后为

$$p_2>\frac{-\text{col}+\text{ei}+\text{ni}}{-2\text{col}+\text{caf}+2\text{ni}-\text{vc}+\text{ei}} \tag{25}$$

由

$$\begin{aligned}&\left(-2\text{col}+\text{caf}+2\text{ni}-\text{vc}+\text{ei}\right)-\\&2\left(-\text{col}+\text{ei}+\text{ni}\right)=\text{caf}-\left(\text{ei}+\text{vc}\right)\end{aligned} \tag{26}$$

其中，ei 为共谋攻击的收益，在 c2 同意共谋的情况下肯定有 $\text{caf}<\text{ei}$，则

$$\left(-2\text{col}+\text{caf}+2\text{ni}-\text{vc}+\text{ei}\right)-2\left(-\text{col}+\text{ei}+\text{ni}\right)<0 \tag{27}$$

则有

$$p_2>\frac{1}{2} \tag{28}$$

因此，c1 会大概率举报 c2，而对于 c2 来说，同意共谋就不再是当前最优策略，因此 c2 会举报 c1，而这时对于 c1 来说，发起共谋也不是最

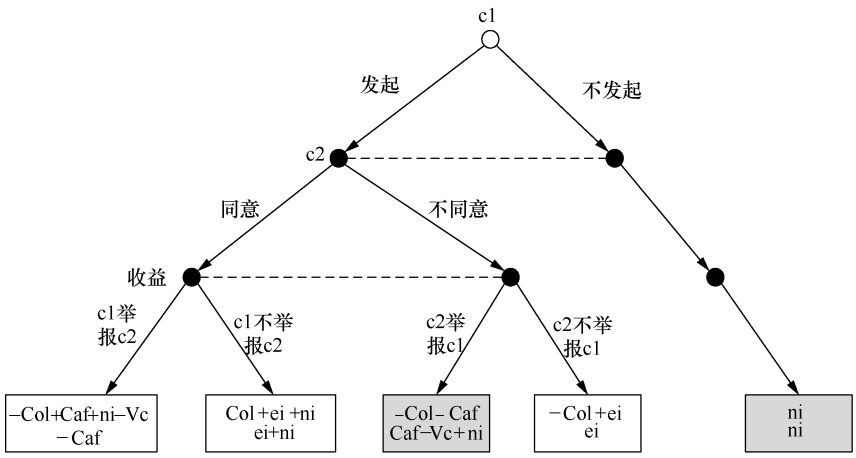

图 6　共谋双方的博弈树
Figure 6　Conspiracy the game tree of both parties

优策略。

每个节点最终都是为了自己的利益最大化，当一个节点发起共谋时，根据博弈树中的线路必定最后会被另一方举报，这时双方就会形成囚徒困境。它的效用函数为

$$E(c1) = -\text{col} - \text{caf} \tag{29}$$

所以，任何节点都不会选择共谋策略，即 c1 和 c2 之间都不共谋，它们的效用都为 ni 。

可以看出，图 7、图 8 中对于 c1 和 c2 不存在均衡点，只有图 9 中的（不发起共谋，不同意共谋）才是两者的最优策略，此时两者的效用函数都为 ni 。

博弈矩阵		c2(同意)
c1(发起共谋)	举报 c2	−col+caf+ni − vc， −caf
	不举报 c2	−col+ei+ni， ei+ni

图 7　c1 发起共谋后 c2 同意的效用函数
Figure 7　The utility function c2 agrees to after c1 initiates a conspiracy

博弈矩阵	c2(不同意)	
	举报 c1	不举报 c1
c1(发起共谋)	−col − caf， caf − vc+ni	−col+ni， ni

图 8　c1 发起共谋后 c2 不同意的效用函数
Figure 8　The utility function that c2 disagrees with after c1 initiates a conspiracy

博弈矩阵	c2(不同意共谋)
c1(不发起共谋)	ni ,ni

图 9　c1 和 c2 不共谋的效用函数
Figure 9　c1 and c2 are not collusive utility functions

3　安全性分析

3.1　抗 DDoS 和 Eclipse attacks 攻击

在 GRCACAGT 共识算法中，矿池中节点分为提议者、发起者、验证者和其他，其中发起者和验证者身份的匿名保证了共识算法的安全性，如果发起者和验证者身份暴露，则很可能发生 DDoS 攻击和 Eclipse attacks 攻击[19]，这两种攻击都需要事先知道验证发起者和验证者，提出的共识协议中，用智能合约和加权随机函数实现发起者和验证者的随机化，并保证节点之间的身份匿名，从而防止 DDoS 攻击和 Eclipse attacks 攻击。

3.2　抗 1/3 节点共谋攻击

利用博弈论分析容错类的共识算法中得到，该类共识算法每轮投票都需要保证正确节点多于错误节点的 3 倍，当大于 1/3 节点发生共谋则最终达成的共识结果不可信。对于该问题，在 GRCACAGT 共识算法中利用智能合约和博弈论方法设计了共谋合约，当有节点发起共谋时，理性地接收节点最终会选择举报共谋而获得收益，而对于共谋发起者来说这种策略是对其损失最大的策略，因此对于矿池中理性的矿工节点不会选择发起共谋，从而防止了 1/3 节点共谋攻击。

3.3　信誉动态更新增强共识算法的正确性

一个人的信誉是变化的，并且一个人的不诚实概率等于信誉的对立。因此，本文利用构建的信誉模型对节点信誉进行更新，利用提议者的信誉值代替提议者的不诚实概率能够使本文的共识算法更加高效，同时验证者的数量更加准确，提高共识算法正确性。

4　实验分析

容错类共识算法中共谋攻击的概率是不可以忽略的。本文对基于拜占庭容错的共识算法进行 7 次共识实验，分别进行 20 次、50 次、80 次、110 次、140 次、170 次、200 次共识过程。

在假设所有节点被选择的概率相等下得到最后 1/3 节点共谋攻击成功的次数和每次共谋成功的概率为 0.436 4，如图 10 所示。

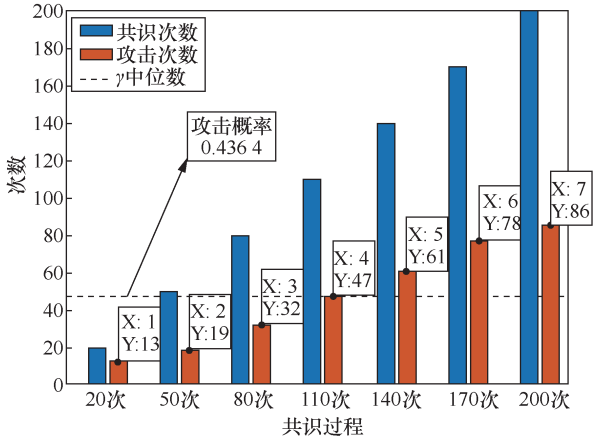

图 10　1/3 节点共谋攻击情况分析
Figure 10　Analysis of conspiracy attack of 1/3 nodes

实际情况是，节点为了更大概率地实现攻击会选择概率大的节点进行共谋，因此实现共谋攻击的概率大于 0.436 4。本文通过建立共谋合约制止节点之间的这种共谋。

接下来分析该共识算法的时间开销、吞吐量等指标[20]。假设 T_{RS} 表示每次加权随机选择节点的时间开销，T_{Ver} 表示验证节点合法性的时间开销，T_{Vote} 表示每个阶段所有节点投票的时间开销，T_{Update} 表示信誉更新的时间开销，T_{Black} 表示区块产生的时间，发起者 T_L、验证者 T_V、投票确认者 T_P、产生区块 T_{Block}、假设验证者个数为 k。

发起者开销为

$$T_L = 4T_{\mathrm{RS}} + T_{\mathrm{Ver}} + 4T_{\mathrm{Upadate}} \tag{30}$$

验证者确认的时间开销为

$$T_V = k \cdot T_{\mathrm{RS}} + T_{\mathrm{Ver}} + k \cdot T_{\mathrm{Update}} \tag{31}$$

投票者确认阶段时间开销

$$T_V = k \cdot T_{\mathrm{Vote}} \tag{32}$$

总的时间开销为

$$\begin{aligned} T_{\mathrm{Sum}} &= T_L + T_V + T_P = 4T_{\mathrm{RS}} + T_{\mathrm{Ver}} + 4T_{\mathrm{Update}} + \\ & k \cdot T_{\mathrm{RS}} + T_{\mathrm{Ver}} + k \cdot T_{\mathrm{Update}} + k \cdot T_{\mathrm{Vote}} = \\ & (4+k)\left(T_{\mathrm{RS}} + T_{\mathrm{Update}}\right) + 2T_{\mathrm{Ver}} + k \cdot T_{\mathrm{Vote}} \end{aligned} \tag{33}$$

通过对比 PoW、PoS、True Decentralization 和 GRCACAGT 性能指标（如表 3 所示），发现 GRCACAGT 相对 PoW 和 PoS 在 TPS、时延、交易确认时间、交易不可更改时间、资源消耗方面具有优势，相对 True Decentralization 具有更高的安全性。

表 3　PoW, PoS, True Decentralization, GRCACAGT 性能指标

Table 3　Performance indicator of the PoW, PoS, True Decentralization and GRCACAGT

算法	每秒交易数	时延	交易确认时间/min	交易不可更改时间/h	资源消耗	时间复杂度
PoW	<7	分钟级	10	1	high	$O(n^2)$
PoS	5~10	分钟级	10	1	a little high	$O(n^2)$
True Decentralization	800	秒级	<1	not	low	$O(nm)$
GRCACAGT	700	秒级	<1	not	lower	$O(nm)$

吞吐量是衡量系统单位时间内处理交易的能力。本文使用每秒交易数（TPS，transaction per second）来表示吞吐量，比较了 True Decentralization 和 GRCACAGT 两种共识机制的吞吐量，区块链网络中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，计算如下：

$$\mathrm{TPS}_{\Delta t} = \mathrm{Sum\ Transactions}_{\Delta t} \tag{34}$$

其中，Δt 为交易产生到区块被确认的时间间隔，$\mathrm{Transactions}_{\Delta t}$ 为在时间间隔内被确认区块中包含的交易总数。取 Δt 分别为 50 s、60 s、100 s、300 s 等不同的时间间隔，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 11 所示。

由图 11 可知。当 $\Delta t \prec 60$ 时，GRCACAGT 相比 True Decentralization 的 TPS 小一点，但当 $\Delta t \succ 60$ 时，GRCACAGT 和 True Decentralization 的 TPS 基本相等，所以 GRCACAGT 相对 True Decentralization 在提高安全性和效率的情况下对 TPS 的影响不大。

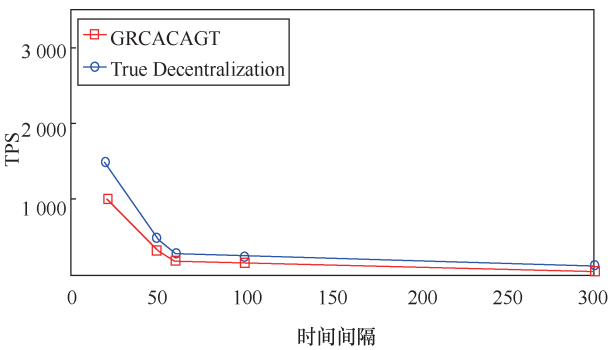

图 11　True Decentralization 和 GRCACAGT 吞吐量比较

Figure 11　Comparison of throughput with True Decentralization and GRCACAGT

运行两个共识协议 30 次后对比两者的运行时间，True Decentralization 和 GRCACAGT 一轮验证时间对比如图 12 所示。

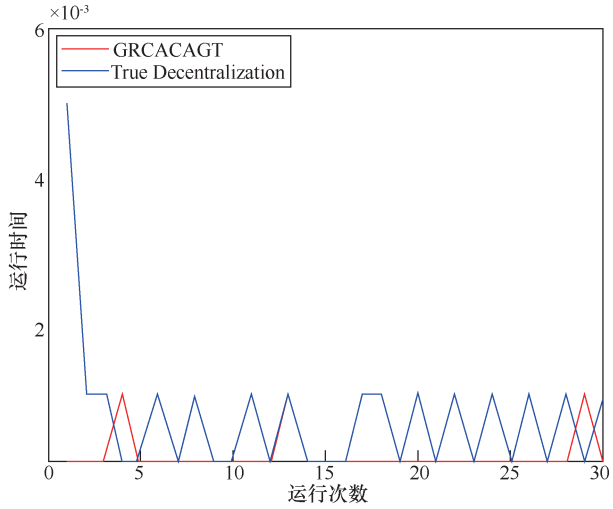

图 12　True Decentralization 和 GRCACAGT 运行时间对比
Figure 12　Run time comparison of True Decentralization and GRCACAGT

通过图 12 能够清楚地知道，GRCACAGT 在时间上相比 True Decentralization 更有优势。

5　结束语

本文利用博弈论、映射函数和加权随机函数，提出了 GRCACAGT。GRCACAGT 主要解决容错类算法中节点的全局随机化问题，并利用博弈论分析发现这类算法中存在共谋攻击，然后构建共谋合约解决这类共谋攻击从而实现该类算法的高安全性。安全性分析表明，GRCACAGT 抗 DDoS、Eclipse attacks、不诚实节点贿赂和与 1/3 节点共谋等攻击。实验分析对比了 GRCACAGT 和相似的一些共识算法的吐量、交易完成时间、时间开销等性能。实验结果表明，GRCACAGT 在安全性和效率性方面得到了很大的提高。本文在选择验证节点时通过不放回抽样的方法避免节点被重复选中，但是该方法使协议的效率变低。并且，在信誉的动态更新模型中，本文没有具体设置模型的参数，对于影响信誉大小的元素没有具体构造出来。因此，高效地实现节点不被重复选择和信誉更新模型具体的构建是下一步工作的方向。

参考文献：

[1] TILBORGH C A, JAJIDIA S. Encyclopedia of cryptography and security[M]. US：Springer, 2011.
[2] GANESH C, ORLANDI C, TSCHUDI D. Proof-of-stake protocols for privacy-aware blockchains[C]//Advances in Cryptology – EUROCRYPT 2019, 2019
[3] KIAYIAS A, RUSSELL A, DAVID B, et al. Ouroboros: a provably secure proof-of-stake blockchain protocol[C]//Advances in Cryptology – CRYPTO 2017.
[4] KERBER T, KIAYIAS A, KOHLWEISS M, et al. Ouroboros crypsinous: privacy-preserving proof-of-stake[C]//Proceedings of 2019 IEEE Symposium on Security and Privacy. 2019: 157-174.
[5] FAN X X, CHAI Q. Roll-DPoS: a randomized delegated proof of stake scheme for scalable blockchain-based Internet of things systems[C]//Proceedings of the 15th EAI International Conference on Mobile and Ubiquitous Systems: Computing, Networking and Services. 2018.
[6] BUCHMAN E, KWON J, MILOSEVIC Z. The latest gossip on BFT consensus[EB].
[7] ALZAHRANI N, BULUSU N. Towards true decentralization: a blockchain consensus protocol based on game theory and randomness[C]//Decision and Game Theory for Security, 2018.
[8] BENTOV I, LEE C, MIZRAHI A, et al. Proof of activity[J]. ACM SIGMETRICS Performance Evaluation Review, 2014, 42(3): 34-37.
[9] CHEPURNOY A. Interactive proof-of-stake[EB].
[10] SABZMAKAN A, MIRTAHERI S L. An improved distributed access control model in cloud computing by blockchain[C]// Proceedings of 2021 26th International Computer Conference, Computer Society of Iran (CSICC). 2016: 1-4.
[11] GILAD Y, HEMO R, MICALI S, et al. Algorand: scaling Byzantine agreements for cryptocurrencies[C]//Proceedings of the 26th Symposium on Operating Systems Principles. 2017.
[12] OMAR M, CHALLAL Y, BOUABDALLAH A. Reliable and fully distributed trust model for mobile ad hoc networks[J]. Computers & Security, 2009, 28(3/4): 199-214.
[13] ZHAN Y, WANG B C, LU R X, et al. DRBFT: Delegated randomization Byzantine fault tolerance consensus protocol for blockchains[J]. Information Sciences, 2021, 559: 8-21.
[14] DONG C Y, WANG Y L, ALDWEESH A, et al. Betrayal, distrust, and rationality: smart counter-collusion contracts for verifiable cloud computing[EB].
[15] CHEN H, LAINE K, PLAYER R. Simple encrypted arithmetic library - SEAL v2.1[M]. Berlin:Springer, 2016.
[16] ANDERW M, YU X, KUYLE C, et al. The Honey badger of BFT Protocols[R]. 2016.
[17] JALALZAI M, BUSCH C, JII G R. Proteus: a scalable bft consesus protocol for blockchains[C]//CORR .2019.
[18] LESSMANN S, BAESENS B, SEOW H V, et al. Benchmarking state-of-the-art classification algorithms for credit scoring: an update of research[J]. European Journal of Operational Research, 2015, 247(1): 124-136.
[19] 王缵，田有亮，岳朝跃，等. 基于门限密码方案的共识机制[J].

计算机研究与发展, 2019, 56(12): 2671-2683.
WANG Z, TIAN Y L, YUE C Y, et al. Consensus mechanism based on threshold cryptography scheme[J]. Journal of Computer Research and Development, 2019, 56(12): 2671-2683.

[20] YU Y L, CHEN T S. An efficient threshold group signature scheme[J]. Applied Mathematics and Computation, 2005, 167(1): 362-371.

[作者简介]

张宝（1995− ），男，贵州毕节人，贵州大学硕士生，主要研究方向为密码学、区块链网络和共识算法。

田有亮（1982− ），男，贵州盘州人，博士，贵州大学教授、博士生导师，主要研究方向为算法博弈论、密码学与安全协议、大数据安全与隐私保护、区块链与电子货币等。

高胜（1987− ），男，湖北黄冈人，博士，中央财经大学副教授，主要研究方向为数据安全与隐私保护、区块链技术及应用。