区块链技术的激励相容

- **可以讲一讲第二点P+Epsilon攻击**

根据哈维茨（Hurwiez）创立的机制设计理论，在市场经济中每个理性经济人都会有自利的一面，其个人行为会按自利的规则行为行动。如果能有一种制度安排使行为人追求个人利益的行为，正好与企业实现集体价值最大化的目标相吻合，这一制度安排就是激励相容

“无组织”群体行动分为以下层次：第一是“非经济利益驱动”的群体行动，第二是“潜在经济利益驱动”的群体行动，第三是“明确经济利益驱动”的群体行动，也就是本文研究的加密经济的分布式协同作业

攻击vs协作

攻击主要发生在对新增区块进行验证和共识的过程中，最典型的方式是攻击者从某个区块开始构造一条秘密的区块链，当秘密构造的区块链比当前公开的区块链更长时，将其公开，其他节点将会视其为“正确”的链条，在该链条上继续工作和延长它，使被攻击区块包含的交易被撤销，制造“双花攻击”，从而破坏系统参与者原来达成的共识。

如何在“无组织”的群体中形成共识即是经典的“拜占庭将军问题”：在一个一致意见具有绝对必要性的系统里，如何在缺乏信任机制的情况下，通过一个可信的方法，将一个一致意见同步给所有人？或者说，诚实者如何战胜破坏者，形成一个多数一致的、可信的意见？

如何在“无组织”的群体中形成共识即是经典的“拜占庭将军问题”：在一个一致意见具有绝对必要性的系统里，如何在缺乏信任机制的情况下，通过一个可信的方法，将一个一致意见同步给所有人？或者说，诚实者如何战胜破坏者，形成一个多数一致的、可信的意见？

纳什均衡的表：

无激励，无惩罚-->均衡是（协作，协作）或者（攻击，攻击）

	协作	**攻击**
协作	(8,8)	(-2,6)
攻击	(6,-2)	(-1,-1)

有激励（coinbase reward，记账权，tx fee）-->均衡是（协作，协作）

	协作	**攻击**
协作	(11,11)	(1,6)
攻击	(6,1)	(-1,-1)

有惩罚（发言成本，攻击成本PoW机制）-->均衡是（协作，协作）

	协作	**攻击**
协作	(8,8)	(-2,3)
攻击	(3,-2)	(-4,-4)

毋庸置疑，若同时施加恰当的激励和惩罚机制，系统的安全性更能得到保障

PoW的安全隐患 P+Epsilon攻击

P+Epsilon攻击（感觉可以讲一下~）

P+Epsilon攻击由以太坊创始人VitalikButerin提出，它是一种贿赂攻击者模型，即攻击者进入系统，以可信的预算贿赂其他矿工们参与攻击，但事后却无须付出任何成本。以表1为例，假定攻击者给予矿工们一个可信的贿赂预期：当其他人选择“协作”时，如果你选择“攻击”，我将给予你比选择“协作”更高的收益

通过这样的贿赂，其他人选择“协作”，我选择“攻击”的收益由6变为8+ε。此时的纳什均衡解就变为（攻击，攻击），即所有矿工均选择“攻击”，各自的收益均为-1，事后，攻击者没有付出成本，因为所有人都选择了攻击，攻击者不用兑现贿赂承诺。也就是说，攻击者只要以可信的预算和承诺（例如将资金锁定在智能合约），就可零成本地实现对系统的攻击。

	协作	攻击
协作	(8,8)	(-2,8+epsilon)
攻击	(8+epsilon,-2)	(-1,-1)

区块链系统中矿池间的博弈问题及优化

- **可以尝试模拟这里面的11中决策** if possible

区块截留攻击

一些矿工会发送部分工作量证明（Partial Proof of Work，对产出几乎无帮助，只是证明干了活），抛弃完整工作量证明（Full Proofs of Work，收益来源）。

主要原因是：

- 区块链协议具有难度自适应的特征，会根据当前区块生成速度调整前导0 的个数，从而改变难度，控制区块生成速度保持不变。有矿工选择攻击会导致矿池有效算力减少，协议为了保持区块生成速度不变，自会降低挖矿难度，这样滥竽充数的矿工就会得到更多收益。
- 其次是因为，得到奖励的矿池会根据工作量证明按照矿池中每个矿工贡献算力的比例将所获奖励分配给每一个矿工。而完整的工作量证明很难生成，偷奸耍滑的矿工可以选择向开放矿池发送部分工作量证明来获得本该贡献实际算力才能得到的奖励。

11种策略

A 矿池派出的渗透算力为a，B 矿池的渗透算力为b，则对于A 矿池来说，面对B 矿池可以采取多种策略来应对

- P1--ALLC：All Cooperate，永远合作策略，无论对手采取何种策略，都选择合作，即令渗透算力a恒为0。
- P2--ALLD：All Defect，永远背叛策略，无论对手采取何种策略，都选择背叛，即令渗透算力a恒为最大。
- P3--TFT：Tit For Tat，一报还一报策略，第一次选择合作(即a=0) 此后，如果对手的渗透算力b大于某一阈值，则下一轮背叛（即a=max），否则合作（即a=0）。
- P4--Grim：冷酷策略，第一次选择合作(即a=0), 只要对手背叛一次，就不再合作，令a=max。
- P5--WSFS：Win Stay Fail Shift，赢存输变策略，第一次选择合作(即a=0)，之后每一轮如果收益高于某一值，就保持策略不变，否则采取相反的策略(即a=max)。
- P6--Random：离散型随机取值策略，a 以等概率取0 或max。
- P7--TFT_D：TFT_Defect， 类似于TFT， 区别在于第一次选择背叛(即a=max)。

- P8--Grim_D：Grim_Defect，同上，类似于Grim。
- P9--WSFS_D：WSFS_Defect，同上，类似于WSFS。
- P10-- 不定值策略（**论文提出的新策略**）：a 的取值在[0,max] 区间内均匀分布。
- P11-- 定值策略（**论文提出的新策略**）：第一次令a=0，若此后b一直取0，则a 继续取0，若某一轮b>0, 则a 继续取0,设本轮b 取值为b1，下一轮若b>0 则a 继续取0，b 取值为b2，依此类推

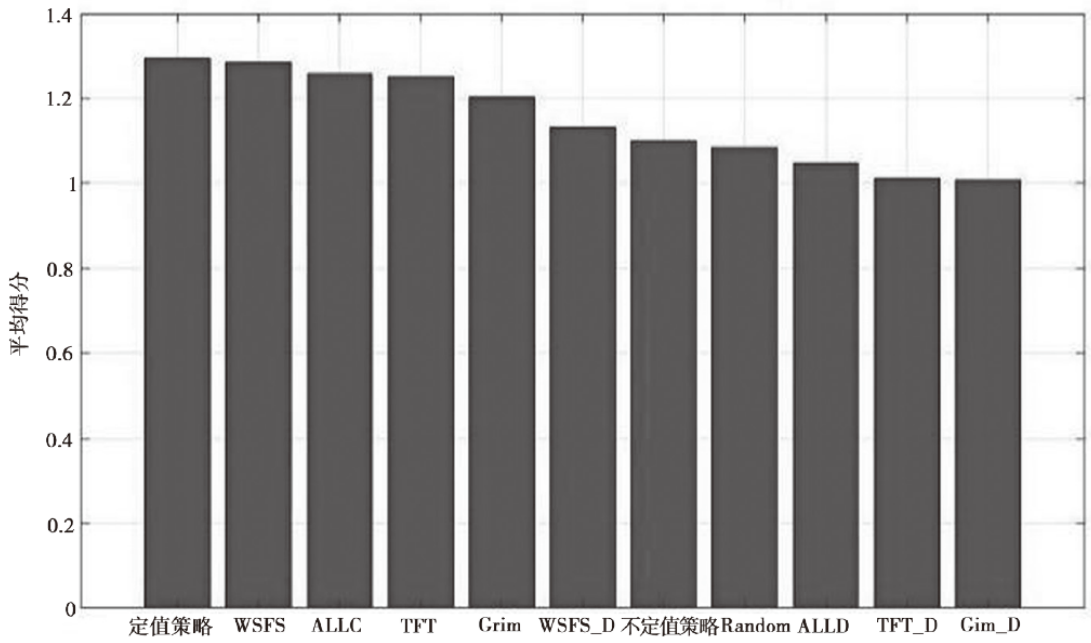

图 7　11 种策略的总体表现排名

模拟仿真结果

对上述仿真结果进行分析，归纳出该博弈模型的以下特点：

1. ALLD 策略在每一次博弈中都不吃亏，但在总体上却是一种很差的策略；
2. 一般而言，“善意”的策略表现要优于“贪心”的策略；
3. 第一次的选择非常重要，对整个策略的表现影响很大。
4. 传统IPD 中，TFT 策略和Grim 策略表现最佳。而在该区块链博弈模型中，定值策略和WSFS 策略表现最好，且定值策略较传统的WSFS 更胜一筹