通过动态回购销毁机制稳定去中心化人工智能经济的控制理论方法

ZehuaCheng[1,2], Wei Dai[2], Zhipeng Wang[2,3],RuiSun[2,4],Nick Wen[2],和 Jiahao Sun[2l]
FLock.io[2]牛津大学[3]曼彻斯特大学[4]纽卡斯尔大学hello@flock.io

arXiv:2601.09961v1 [cs.GT] 15 Jan 2026

摘要——**通过去中心化网络实现人工智能民主化，标志着计算资源供给领域的一次范式转变；然而，这些生态系统的原生经济层极端波动，严重威胁其长期可行性。当前的代币经济模型主要依赖静态或基于阈值的回购启发式策略，难以应对复杂的系统动力学，且往往呈现顺周期特征，在市场低迷时加剧不稳定性。为弥补这一不足，我们提出动态控制回购机制（DCBM），这是一种形式化的控制理论框架，利用带有严格偿付能力约束的比例-积分-微分（PID）控制器，将代币经济作为动力系统进行调节。采用跳跃扩散过程的广泛基于智能体的仿真表明，DCBM 的表现从根本上优于静态基准：在高波动率情况下，代币价格波动率降低约 66%，运营者流失率从 19.5% 降至 8.1%。这些发现表明，将代币经济学从静态规则转变为连续且受结构性约束的控制回路，是构建安全、可持续的去中心化智能网络的必要条件**。

索引词—**去中心化人工智能、代币经济学、控制理论、回购销毁、稳定性**

一、引言

通过去中心化网络普及人工智能，代表着计算资源和机器学习模型供给方式的一次范式转变 [1]。这些平台借助区块链技术，旨在创建无需许可的市场，使模型创建者、算力提供商和终端用户的激励保持一致。然而，这些生态系统的长期可行性在很大程度上取决于其经济稳定性。传统软件即服务平台采用固定的法币定价，而去中心化网络依赖原生代币，其价值会随市场情绪波动 [2]。然而，这种波动也构成了系统性风险：如果 GPU 运营者没有稳定的收入来源，消费者也无法获得固定的推理成本，那么底层计算服务本身即便具备技术优势，也无法得到广泛采用。

在这方面，最重要的任务之一是建立一个可靠且能够自我管理的经济体系，始终优先支持真实的推理和训练经济。理论上，运营中的去中心化人工智能市场，其代币价格可以基于网络的效用价值（推理需求），而不是仅仅受投机驱动。在熊市和炒作周期中，代币价格与效用价值脱钩，将给算力和模型提供商的运营支出与资本支出规划带来问题 [3]。因此，在维持价格均衡以支持可持续增长的同时降低极端波动，不仅是财务上的理想目标，更是网络存续的运营必需。

尽管稳定性至关重要，当前的代币经济模型却主要依赖**静态或简单的启发式机制**，难以应对复杂的系统动态。标准的回购销毁模型独立于网络状态运行，无论代币价格过热还是暴跌，都施加相同的压力[4]。即使是基于某个阈值的简单规则（例如，当价格下跌 X时买入），也表现出“ bang-bang”控制特征，因此会引发振荡。由于系统缺乏适应能力，也没有连续控制，因此会变得脆弱；价格与网络活动之间会形成反馈回路，而由于参数无法适应外生冲击，这些回路很容易失控。

为弥合这一差距，我们提出从静态策略转向**控制理论稳定机制**。通过将代币经济建模为动力系统 [5], ，我们可以运用控制工程中的成熟原理对其进行调节。我们引入**动态控制回购机制（DCBM）**，利用**比例-积分-微分（PID）控制器**，根据实时链上指标 [6]持续调整回购率。正如恒温器通过根据与设定值的偏差调整供暖输出以调节温度一样，我们的机制也会调整回购压力，以尽可能缩小代币价格与其长期增长趋势之间的偏差。其独特之处在于，**积分项** 能够

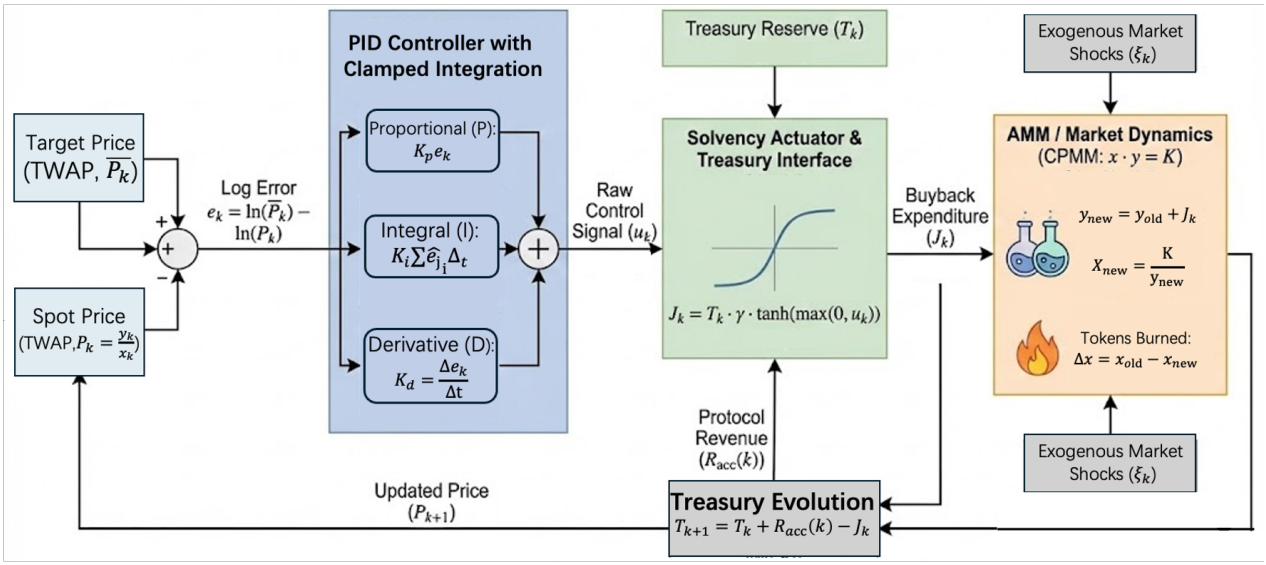


图 1. 动态控制回购机制（DCBM）的闭环控制架构。该示意图展示了旨在稳定去中心化人工智能经济的反馈回路。a，误差接口计算目标时间加权平均价格（TWAP）与实时现货价格之间的对数偏差（e_k）。b，PID 控制器处理该误差，应用比例、积分（限幅）和微分增益，计算原始干预强度（u_k）。c，偿付能力执行器充当关键的安全阀，根据当前金库余额（T_k）和断路器参数（γ）严格限定实际回购支出（J_k），从而确保无论市场条件如何均具备渐近偿付能力。d，AMM对象代表执行回购销毁操作的市场环境，进而改变后续控制周期（$k+1$）的代币价格状态。

使系统纠正持续存在的误差（稳态漂移），而静态模型和阈值模型会忽略这些误差，从而让网络能够采取逆周期行动——在繁荣时期积累储备，并在衰退时期有效动用储备以稳定经济。

我们在代币工程和去中心化人工智能领域的贡献如下。首先，我们对去中心化人工智能经济进行了形式化的控制理论建模，明确规定了状态空间、智能体动力学以及稳定性标准，并将金库的偿付能力条件纳入考量。其次，我们提出了基于 PID 控制器的 DCBM算法，旨在区块链环境中运行，同时考虑离散时间区块链系统中的因果约束和饱和约束。最后，我们通过广泛的基于智能体的仿真验证了该方法，利用跳跃扩散过程 [7] 对肥尾市场冲击和特定的对抗性攻击向量进行建模。这些实验表明，与静态基准相比，DCBM能够实现更优的价格稳定性和更低的运营者流失，同时表现出对 MEV利用和市场操纵更强的韧性。

II. 相关工作

回购销毁（BnB）是当代代币经济中应用最广泛的价值累积原语之一。与传统金融中的股票回购类似，回购销毁使用协议收入（或金库资产）在公开市场上购买原生代币，并将其永久移出流通（通常通过不可恢复的销毁地址实现）。值得注意的是，区块链技术的独特属性，包括不可篡改性和透明度，使得此类回购销毁机制能够以确保问责性和可预测性的方式实施 [8]。

现有文献指出，回购销毁有两种作用。首先，通过永久减少代币的流通供应量，从而形成通缩压力，这种策略可能维持代币价格的稳定或使其上涨 [9], [10]。其次，它能让项目向市场表明自己是合法网络业务，尤其是在信息成本不为零的情况下 [4]。MakerDAO [11]、STEPN [12] 和 PancakeSwap [13]等行业协议中，回购销毁机制并不少见。对于处于初创阶段的协议，这种机制尤其有用。例如，DOT 初次推出时，采用了一种结合代币销毁与代币循环利用的流动性池机制，使 DOT 能够像中央银行一样运作 [14]。其目标是在项目早期稳定流通速度并激励参与度 [8]。

值得注意的是，在某些情况下，回购也可以单独进行，而不伴随销毁。这可能会改变治理权的分配，甚至推动项目走向中心化 [4]。反过来，有些项目也可能选择销毁而不进行回购。这种做法在依靠罚没机制惩罚恶意行为的协议中尤为常见。

此外，回购销毁很少作为孤立机制存在；它通常是更广泛的“收益分配”设计空间中的一种选择。例如，Carvalho 将回购销毁视为股票回购在代币原生领域的对应形式，并将其与储备积累、直接分配和再投资并列，同时强调其作为治理代币和效用代币价值累积路径的作用 [9]。与此同时，面向实践投资者和基础设施的文献指出，代币设计是

生态系统可行性的首要决定因素，因为代币规则（效用、治理和货币政策）会直接塑造平台激励和长期采用情况 [15], [16]。

然而，尽管回购销毁在业界广泛应用，其设计仍缺乏全面的实证证据来说明其优势与劣势。此外，现有的回购销毁设计通常被设定为静态政策：将固定比例的收入用于回购，或按照预先公布的时间表进行回购，基本不考虑系统状态的动态变化。近期有关信息披露与市场诚信的研究指出，可信度取决于透明、基于规则且可公开验证的执行，因为自由裁量的干预可能使信息优势集中，并招致操纵指控。然而，即便完全透明，静态回购销毁政策仍可能呈现顺周期特征：协议收入高时（通常处于牛市阶段），回购规模可能自然扩大；而在市场低迷时则会缩减，恰恰在最需要价格支撑和运营者收入稳定性之际 [10]。此外，在需求疲软或遭遇重大外生供给冲击（例如解锁和代币发行）时，仅靠通缩压力不足以保证价格稳定性；而将过多费用转拨至回购，也可能削弱运营和安全所需的应急资金。

在宏观经济学和货币理论文献中，价格反馈控制长期以来得到了广泛建模。泰勒规则就是一种货币政策规则，其中政策反应与通货膨胀率或产出缺口成正比；有关其稳定性问题的研究已对其进行了广泛分析 [17]。后续研究表明，当经济主体随时间调整预期时，固定不变或调校不当的规则可能导致不稳定，因此有必要采用状态依赖型反馈机制[18], [19]。近期，Hawkins等人 [20] 明确通过比例-积分-微分（PID）控制的视角解读货币政策，阐明了积分作用如何消除稳态漂移，而微分项如何抑制振荡动力学。总体而言，这些研究确立了反馈控制作为一种在不确定性下稳定复杂经济系统的系统性方法。

这些发现促使我们重新思考回购销毁方案的设计，并将重点放在控制理论上，尤其是在去中心化环境中，因为在这种环境下，执行、透明度和偿付能力条件等问题至关重要。尽管经济学和货币理论领域的文献表明，反馈控制是价格稳定的可靠基础，但这些模型通常侧重于政策制定和均衡分析，完全忽略了执行问题。相比之下，当前代币经济中的回购销毁方案设计仍基本是静态且阈值依赖型的，既没有明确的稳定性目标，也缺乏面对随机需求和供给扰动时的正式保障。我们的方案弥补了这一不足，以链上可执行的方式将控制理论的稳定化功能付诸实践。具体而言，我们提议将回购操作设计为反馈控制执行器，旨在跟踪时变参考轨迹（时间加权平均价格趋势），同时严格执行偿付能力和饱和约束，这些约束在链上财库系统中本就不可或缺。这种方法能够实现：（i）通过比例、积分和微分作用，灵活应对制度变化和扰动；（ii）通过积分作用补偿稳态漂移；以及（iii）通过偿付能力感知执行器和熔断机制提供严格的安全保障。实际上，我们的 DCBM 使回购政策具备状态依赖性、以稳定性为目标，并能感知安全约束；这些特点在当前静态且阈值依赖型的回购销毁方案设计中并不存在。

III. 方法论

A. 问题的形式化表述

我们将去中心化人工智能经济建模为一个离散时间动力系统。为适应以太坊虚拟机（EVM）的计算限制——具体而言，为避免在每个区块上执行复杂控制逻辑所产生的高昂燃料费——我们将时间离散化为控制周期，并以 $k \in \mathbb{Z}^+$ 为索引。每个周期持续固定时长 Δt（例如，N 个区块）。

纪元 k 时的系统状态定义为 $S_k = [P_k, \bar{P}_k, T_k]^\top$，其中：$P_k$ 是原生代币在纪元 k内的时间加权平均价格（TWAP）。$\bar{P}_k$ 是目标参考价格（指数移动平均）。T_k 指以稳定币（如 USDC）计价的网络金库余额。

与以往将回购错误地与即时收入挂钩的模型不同，我们将资金积累与稳定化过程分离。国库充当蓄水池，缓冲系统冲击。

国库按照以下守恒方程变化：

$$T_{k+1} = T_k + \underbrace{R_{acc}(k)}_{\text{Inflow}} - \underbrace{J_k}_{\text{Outflow}} \tag{1}$$

其中，$R_{acc}(k)$ 是在纪元 k期间累积的协议收入（手续费），而 J_k 是由控制器确定的稳定化支出（回购金额）。

系统满足严格的偿付能力条件 $T_{k+1} \geq 0$。这意味着 $J_k \leq T_k + R_{acc}(k)$。

我们假设代币在满足不变量 $x \cdot y = K$的恒定乘积做市商（CPMM）上交易，其中 x是代币储备，y 是稳定币储备。当控制器执行金额为 J_k（稳定币）的回购时，储备更新如下：

$$y_{new} = y_{old} + J_k$$

$$x_{new} = \frac{K}{y_{new}}$$

购入的代币 $\Delta x = x_{old} - x_{new}$ 会被销毁，从而永久减少供应量。这种机械性的价格影响为我们的控制系统提供了驱动力。

B. 动力系统建模与状态空间

去中心化网络的经济稳定构成了一个随机控制问题，并受到底层区块链严格的离散时间执行机制约束。与连续时间金融模型不同，去中心化自治组织（DAO）以离散动力系统的形式运行，其状态会在区块高度$k \in \mathbb{Z}^+$处原子性地转换。为了严格定义控制环境，我们建立了一个状态空间 $S_k = [P_k, \bar{P}_k, T_k]^\top$。其中， P_k 表示原生代币的时间加权平均价格（TWAP），$\bar{P}_k$ 表示通过指数移动平均（EMA）计算的参考目标价格，而 T_k 表示以稳定计价单位计价的金库余额。我们特意使用 TWAP 而非即时现货价格来定义状态，将其作为内在的低通滤波器，使控制器在数学上无法感知依赖高频价格操纵的单区块闪电贷攻击。

对先前代币经济学文献的一项根本性修正，是将强制性运营支出纳入金库演化方程。以往模型通常假设只要收入为正，金库就会持续增长，由此导致“金库悖论”：即便协议无法承担基本成本，看起来仍然具备偿付能力。我们采用严格的守恒定律来定义金库动态，并将固定的基础设施开销纳入考量， C_{ops} （例如预言机燃料费、节点补贴）。状态转移表示为 T_{k+1} =max(0， $T_k + R_{acc}(k) - J_k - C_{ops}$)。这一公式可用于逼真地仿真流动性危机；如果累计收入 $R_{acc}(k)$低于 C_{ops}，金库就会自然收缩，从而形成控制器必须主动管理的破产时间约束。

市场对象建模为满足不变量 $x \cdot y = K$ 的恒定乘积做市商（CPMM）。稳定化支出 J_k 与市场储备之间的相互作用形成了一个非线性反馈回路。为了进行控制设计，我们围绕工作点对被控对象动态进行线性化。在对数域中，价格更新可近似为具有可变增益 $\alpha_k = 2/y_k$ 的离散积分器。这表明，系统对回购的敏感度与流动性深度成反比，因此需要一个能够在不同市值条件下稳定运行、且不会引发振荡振铃的控制器。

C. 动态控制回购机制

为调节这一系统，我们引入动态控制回购机制（DCBM），这是一种专为以太坊虚拟机（EVM）优化的基于 PID 的架构。由于浮点运算的燃料费高昂，且设定值变化时存在微分冲击风险，标准控制实现并不适用于这一环境。我们采用测量值微分策略，并结合谱噪声滤波器。我们不对误差信号求导——因为这会将价格骤降放大为“恐慌性回购”信号——而是计算变化率

以经过滤波的时间加权平均价格为基础。这样可以确保微分项能够有效抑制自然波动趋势，同时滤除对抗性操纵特有的高流通速度、高振幅特征。

为解决链上计算超越函数所面临的“Gas 成本不可能性”，我们采用高精度定点算术（WAD 数学）和分段线性近似来实现控制逻辑。自然对数和双曲正切等函数通过经过优化的查找表和泰勒级数展开进行近似，并将其限定在预期的价格偏差范围内。这样一来，控制器的计算开销便从理论上无限的 Gas 成本（若要求完美精度）降至约 150，000 Gas 的目标执行成本，使该机制在经济上适用于高频部署。

根据此定义， $e_k > 0$意味着资产被低估（价格低于目标），因此需要提供支撑。DCBM 采用离散时间比例-积分-微分（PID）控制律。

为防止积分饱和——即在国库资金耗尽（饱和）期间，积分器不断累积大量误差，进而导致系统不稳定的现象——我们采用钳位积分方案。原始的无量纲控制强度 $u_k \in \mathbb{R}$ 计算如下：

$$u_k = K_p e_k + K_i \sum j = 0^k \hat{e} j \Delta t + K_d \frac{e_k - ek - 1}{\Delta t} \quad (2)$$

此处，$\hat{e}_j$ 表示条件误差，其定义为：若执行器未饱和（$T_j > 0$），则为$\hat{e}_j = e_j$；否则为 0。这确保控制器能够保留对近期不稳定性的“短期记忆”，同时不会受到其缺乏行动能力时产生且无法解决的历史债务的拖累。

该方法的最后阶段将抽象的控制强度 u_k 映射为实际支出 J_k，并通过构造满足假设 1。我们引入一个由“流动性断路器”参数$\gamma \in (0, 1]$限定范围的 S 形执行器。实际回购金额由映射函数 Φ 确定： $\mathbb{R} \times \mathbb{R}_{\geq 0} \to \mathbb{R}_{\geq 0}$:

$$J_k = \Phi(u_k, T_k) = T_k \cdot \gamma \cdot \tanh(\max(0, u_k)) \quad (3)$$

$\max(0, u_k)$ 运算符确保负信号（高估）导致支出为零。 γ 项定义了单个纪元内可动用的国库最大比例。这种乘法形式为系统的存续提供了关键的理论保障。

命题 III.1 (渐近偿付能力)。 给定初始国库余额 $T_0 > 0$ 和参数 $\gamma \in (0,1)$，无论收入崩溃的幅度或持续时间如何（$R_k = 0$），国库余额 T_k 在所有有限 k内始终严格为正。

证明：在最坏情况下 $R_k = 0$，将公式 3 代入公式 1，得到几何递推关系 $T_{k+1} = T_k(1 - \lambda_k)$，其中 $\lambda_k = \gamma \tanh(u_k)$。由于 $\tanh(\cdot) < 1$ 且 $\gamma < 1$，衰减因子 $(1 - \lambda_k)$ 严格为正。因此，国库遵循芝诺式轨迹，渐近趋近于零，但永远不会达到零。这

确保协议永不违约，并维持非零的微量储备，以便在市场条件稳定后为恢复提供资金。

D. 博弈论鲁棒性

在无许可区块链环境中，控制器不仅必须对随机噪声具有鲁棒性，还必须抵御最大可提取价值（MEV）代理的策略性利用。我们将这种对抗性交互建模为"钓鱼攻击"，其中对手 $\mathcal{A}$ 人为压低 P_k，以触发补贴回购。我们假设对手在每个纪元 k 求解以下利润最大化问题：

$$\max_{\delta} \mathbb{E}\left[\Pi_{\mathcal{A}}\right] = \mathbb{E}\left[P_{exit}(J_k(\delta)) - P_{entry} - C_{risk}(\tau)\right] \quad (4)$$

其中，δ 是诱导产生的价格偏差，$C_{risk}(\tau)$ 是在持续时间 τ 内维持该偏差的成本。

DCBM 通过微分项（K_d）在公式 2 中的频谱滤波特性来防御这种操纵。通过响应变化率 $1\frac{\Delta e_k}{\Delta t}$，控制器将闪电贷攻击的高流速特征识别为噪声，而非趋势变化。2 这实际上充当了一个高通滤波器，在存在不连续性的情况下抑制执行信号 u_k，迫使对手在多个纪元（$\tau > N\Delta t$）内持续进行操纵，才能触发积分项。这一要求会线性增加对手面临的市场风险 C_{risk}，从而在增益经过适当调节时，使该攻击严格处于劣势（预期值为负）。

IV. 理论分析

我们将 DCBM 视为一个闭环反馈控制系统进行分析。与执行器能量无限的经典控制问题（例如连接到电网的电机）不同，我们的系统受能量约束：控制权限严格受有限的金库储备水平 T_k 限制。我们从两个维度分析系统行为：动力学稳定性（收敛性）和结构性偿付能力（不破产）。

A. 被控对象模型推导（*AMM* 动力学）

为分析稳定性，我们必须以数学方式定义控制动作（回购 J_k）如何影响系统状态（价格P_k）。我们假设恒定乘积做市商（CPMM）满足不变量 $x_k \cdot y_k = K$，其中价格为 $P_k = \frac{y_k}{x_k}$。金额为 J_k （稳定币）的回购会改变储备：

$$y_{k+1} = y_k + J_k$$

新价格 P_{k+1} 遵循二次 AMM 曲线：

$$P_{k+1} = \frac{(y_k + J_k)^2}{K} = P_k \left(1 + \frac{J_k}{y_k}\right)^2 \quad (5)$$

取自然对数，以与我们的对数误差控制器对齐（$e_k = \ln P_k - \ln P_k$）：

$$\ln(P_{k+1}) = \ln(P_k) + 2\ln\left(1 + \frac{J_k}{y_k}\right) + \xi_k$$

其中 ξ_k 表示外生市场噪声。

线性化：对于回购量相对于流动性深度（$J_k \ll y_k$）较小的工作区域，我们使用泰勒近似 $\ln(1+x) \approx x$。我们定义价格影响系数 $\alpha_k = \frac{2}{y_k}$。线性化被控对象模型为：

$$p_{k+1} = p_k + \alpha_k J_k + \xi_k \quad (6)$$

其中 $p_k = \ln(P_k)$。这表明市场是一个离散积分器对象：价格状态会累积控制动作的历史，意味着在没有控制的情况下，误差会无限期持续存在（1型系统）。

B. 闭环稳定性分析

我们考察被控对象与PID 控制器构成的反馈回路。为进行稳定性分析，令目标 P 为常数（$\bar{p}_{k+1} = \bar{p}_k$）。误差动态为 $e_{k+1} = e_k - \alpha_k J_k$。

在Z域中代入PID控制律，开环传递函数 $L(z)$ 等于控制器$C(z)$与被控对象 $P(z)$的乘积：

$$P(z) = \frac{\alpha}{z-1}$$

$$C(z) = K_p + K_i\frac{z}{z-1} + K_d\frac{z-1}{z}$$

闭环特征方程为 $1 + C(z)P(z) = 0$。代入并整理各项，可得关于 z的特征多项式：

$$z^2(1+\alpha K_p+\alpha K_i+\alpha K_d) - z(2+\alpha K_p+2\alpha K_d) + (1+\alpha K_d) = 0 \quad (7)$$

稳定性标准：对于二阶离散系统，应用Jury稳定性判据，当且仅当增益满足以下不等式时，该多项式的根严格位于单位圆（$|z| < 1$）内：正性条件：$K_p + K_i > 0$；阻尼限制：$K_d < \frac{2-\alpha K_p}{\alpha}$；积分限制：$K_i < \frac{4-2\alpha K_p}{\alpha}$。

推论 （"水洼中的鲸鱼"风险）：稳定区域与 $\alpha = \frac{2}{y_k}$ 成反比缩放。

定理 IV.1 （增益敏感性）。随着流动性降低（$y_k \to 0$），被控对象增益 $\alpha \to \infty$。为维持稳定性，控制器增益（K_p、K_i、K_d）必须按比例降低。这证明，在流动性紧缩期间，静态参数基线不可避免地会进入振荡失稳（"振铃"）状态，而 *DCBM* 的偿付能力约束（如下文所推导）会自然地将有效增益（$T_k\gamma$）限制在这些界限以内。

C. 渐近偿付能力证明

自主经济代理的一个关键要求是绝不能违约。我们正式证明，DCBM 国库余额 T_k 在所有有限时间 k内始终严格为正。

定理 IV.2 （非耗尽性）。给定初始国库余额$T_0 > 0$，国库余额 $T_k > 0$ 对所有 $k \in \mathbb{Z}^+$均成立，无论市场条件如何。

证明：回顾方程 1 中的国库演化过程。代入执行器映射函数 $J_k = T_k \cdot \gamma \cdot \tanh(u_k)$：

$$T_{k+1} = T_k[1 - \gamma \cdot \tanh(u_k)] + R_{acc}(k)$$

令 $\lambda_k = \gamma \tanh(u_k)$。根据设计，流动性断路器$\gamma \in (0, 1)$，且 $\tanh(\cdot) \in [0, 1)$，因此 $0 \leq \lambda_k < 1$。考虑收入 $R_{acc} = 0$ 无限期持续的末日情景。国库按几何序列演化：

$$T_{k+1} = T_k(1 - \lambda_k)$$

$$T_n = T_0 \prod_{k=0}^{n-1} (1 - \lambda_k)$$

由于 $(1 - \lambda_k)$ 严格为正，因此该乘积严格为正。结论：国库渐近趋近于零，但永远不会归零。该系统具有结构性偿付能力，确保始终留有微量储备以资助恢复，因此，固定利率基线中观察到的破产情景在数学上不可能发生。

D. 对脉冲攻击的鲁棒性

最后，我们讨论系统抵御博弈论式利用的能力，具体而言是“Fishing”攻击：最大可提取价值（MEV）参与者通过制造人为波动来触发有利可图的回购。我们将这类攻击建模为注入价格信号的离散脉冲函数：$\delta_{attack}(k) = \Delta_{spike} \cdot \delta(k)$。朴素的比例控制器会立即对该信号作出反应，实际上将国库资金转移给攻击者。然而，DCBM 采用谱滤波方法来抑制这些高频异常。采用时间加权平均价格（TWAP）作为输入，相当于使用低通滤波器，可将任何单区块操纵的幅度衰减 $\frac{1}{N}$ 倍，其中 N 是纪元长度。此外，PID 控制器的微分部分在控制系统中起到高通滤波器的作用。控制系统中微分部分的 Z 变换会在原点产生一个零点，使其容易对误差信号的变化作出反应。对于试图引发价格闪崩的攻击者，控制系统的微分部分会对数学上极不可能出现的价格下跌速率作出反应，生成补偿控制信号，从而抑制系统的控制作用。因此，攻击者的成本会很高，因为要在多个纪元内维持相对于市场参与者的价格偏差，需要投入大量资金，而这通常超过了从国库中可提取的最大价值。

V. 实验

这些实验旨在通过复杂的基于智能体的仿真，严格评估所提出的动态控制回购机制（DCBM），并与基线模型进行比较。

A. 数据集准备

我们将采用双数据方法，确保仿真既有坚实的理论依据，又立足于现实世界动态；该方法已通过 [21]验证。

1）**合成数据生成：**

- **推理需求（D_t）：**我们将使用**跳跃扩散模型** [7]（扩展几何布朗运动）把推理需求的到达建模为一个随机过程。该模型包含标准漂移（μ_D）和波动率（σ_D）成分，并加入泊松过程，以模拟需求中突然且不连续的“跳跃”（冲击）。这确保仿真能够捕捉肥尾事件，不会低估黑天鹅情景的发生频率；相较于标准几何布朗运动，这是一个关键改进。
- **外部市场冲击（ξ_t）：**我们还将把影响原生代币价格的更广泛加密货币市场走势建模为跳跃扩散过程，其漂移（μ_P）和波动率（σ_P）参数与推理需求过程相关。

2）**现实世界数据集成：**

- **模型使用数据：**我们将从 Hugging Face 等平台获取热门开源人工智能模型的匿名历史使用数据，以构建真实的推理需求模式。数据包括每日下载量和 API 调用等指标。
- **代币价格数据：**我们将使用现有去中心化人工智能或 DePIN（去中心化物理基础设施网络）项目代币（例如 Bittensor、Render）的历史价格数据，模拟真实的价格波动率及其与更广泛市场（例如 BTC/ETH）的相关性。

B. 基线实现

为建立性能基准，我们将实现并模拟**五种**基线代币经济模型。这些模型将在与我们提出的方法相同的基于代理的框架中运行。图 2 展示了各基线的详细信息。

C. 所提方法的实现

DCBM 将作为一个模块化组件集成到基于智能体的仿真中，使用 Python 编写，并采用 Mesa（用于基于代理的建模）和 NumPy 等库。

- **智能体实现：**我们将定义四种智能体类别：模型所有者、运营者、用户和投机者。每个智能体都将拥有一个状态（例如代币余额、活跃模型）和一个 step() 方法，根据其效用函数和对市场状态的感知来执行决策逻辑。
- **控制器实现：**PID 控制器将实现为一个类，用于维护积分项和微分项的状态。在每个仿真步骤（代表一个区块）中，它将读取网络指标，计算新的回购率 u_t，并在模拟的自动做市商上执行回购。
- **开发阶段：**

  1) 阶段 *1*：实现代理逻辑和市场环境。2) 阶段 *2*：集成基线模型。3) 阶段 *3*：实现并集成 DCBM 控制器。

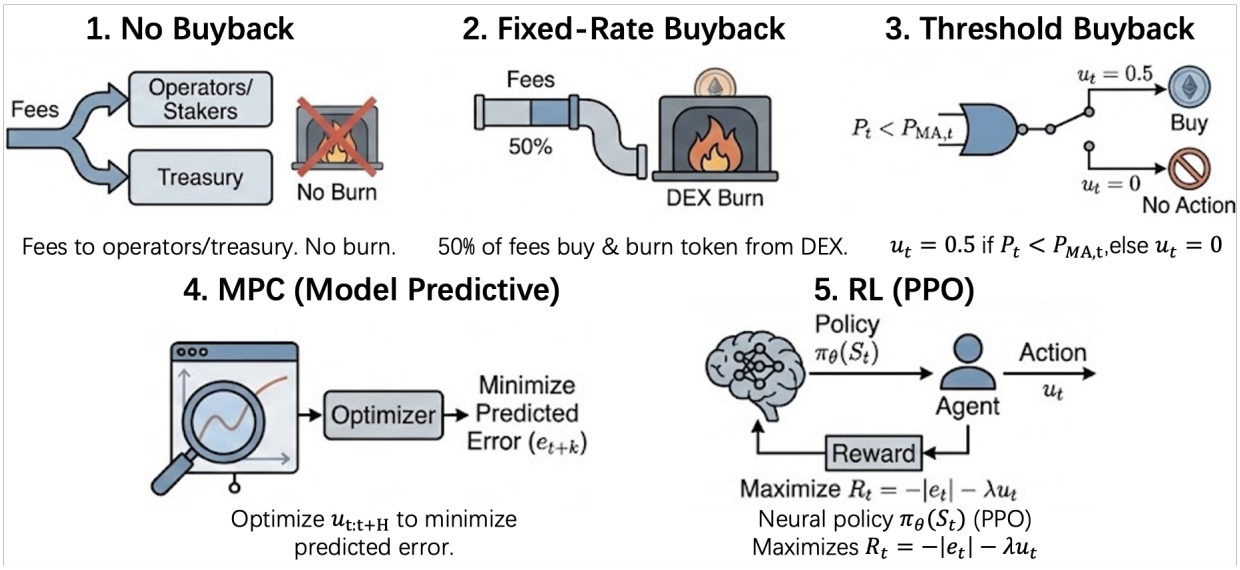


图 2. 基线稳定机制示意图。该图展示了与所提出的 DCBM 进行评估的五种控制策略：(1) 无回购，即将费用全部分配给运营者，不进行销毁；(2) 固定比率回购，即无论市场状态如何，均按固定比例销毁（例如 50%）；(3) 阈值回购，这是一种启发式方法，仅当现货价格 P_t 低于移动平均线 $P_{MA,\ t}$时触发回购；(4) 模型预测控制（MPC），在有限时域内最小化预测误差；(5) 强化学习（PPO），利用神经策略最大化基于稳定性和控制力度的奖励函数。

4) 阶段 *4*：在运行全规模实验之前，使用较小规模的合成数据集校准代理参数和控制器增益（K_p，K_i，K_d）。

D. 主要实验与评估

主要实验将针对每个模型（2 个基线模型，1 个所提模型），在各种由数据驱动的情景下运行仿真。我们将使用蒙特卡洛方法，对每种情景运行 1,000 次，以收集评估指标的统计分布。每次仿真运行的时间跨度相当于现实世界中的 1 年，离散时间步长（Δt）对应于区块链出块时间（例如，12 秒的间隔）。

评估指标：

- **代币价格波动率：**代币价格对数收益率的标准差，以及相对于移动平均线的平均偏差百分比（$\frac{1}{T}\sum_{t=1}^{T}\left|\frac{P_{err,t}}{P_{MA,t}}\right|$）。
- **代币持有量的基尼系数：**用于衡量网络内的财富集中度和去中心化程度。
- **运营者流失率：**每个仿真周期内离开网络的运营者占运营者总数的百分比。
- **模型创新率：**每个周期推出的高质量新模型数量占已部署模型总数的比例。
- **网络金库健康状况：**金库价值随时间变化的平均速率及其稳定性（标准差）。
- **控制力度：**平均回购率 u_t 及其方差，反映控制器的激进程度和稳定性。

超参数与调优：

- **PID 增益（K_p，K_i，K_d）：**这些参数将在合成数据的验证集上通过网格搜索或优化算法（例如贝叶斯优化）进行调优，以最小化包含价格波动率和国库健康状况的综合损失函数。
- **自动做市商流动性：**我们将改变仿真中自动做市商资金池的初始流动性，以观察市场深度对价格稳定性的影响。
- **代理参数：**风险厌恶程度（λ_{MO}，λ_{OP}）、成本参数和效用函数权重将依据经济直觉和敏感性分析进行设定。
- **移动平均窗口：**我们将探究$P_{MA,\ t}$的窗口大小（例如 30 天、60 天），以评估其对目标信号的影响。

E. 攻击与博弈鲁棒性实验

在对抗性区块链环境中部署确定性控制回路，会引入不同于标准随机市场噪声的特定博弈论漏洞。虽然 DCBM 旨在抑制波动率，但它依赖可观测链上指标，尤其是现货价格与移动平均线之间的偏差，这为最大可提取价值（MEV）机器人和策略性大户创造了潜在攻击面。为严格评估该机制抵御此类对抗行为的韧性，我们引入了一组针对控制器逻辑的特定攻击模拟。

我们对两种主要的对抗策略进行建模：**信号操纵（“Fishing”）**和**抢先交易/三明治攻击**。例如，在抢先交易攻击中，MEV 机器人发现内存池中有一笔

表 I 经济稳定性与网络健康指标的比较分析。数值表示均值 ± 95% 置信区间。最佳结果（不包括预言机）以粗体显示。↓ 表示越低越好；↑ 表示越高越好。Gas 估算值适用于 EVM 等效链，且为近似值。

情景	模型	$\sigma_P \downarrow$	$\epsilon_{\text{MA}} \downarrow$	流失率 ↓	基尼系数 ↓	增长 ↑	计算成本 ↓
牛市	无回购	0.42 ± 0.03	12.4% ± 1.2	5.2 ± 0.5	0.88	**15.2 ± 1.1**	–
	固定利率阈值	0.39 ± 0.02	8.1% ± 0.9	4.8 ± 0.4	0.85	8.1 ± 0.8	≈ 21k
	强化学习（近端策略优化）	0.31 ± 0.04	6.5% ± 1.5	4.1 ± 0.8	0.82	9.4 ± 1.2	≈ 5k
	模型预测控制（预言机）	0.26 ± 0.05	3.5% ± 0.8	4.0 ± 0.6	0.80	10.8 ± 1.4	≈ 720k
	DCBM（我们的方法）	*0.19 ± 0.01*	*2.0% ± 0.2*	*3.5 ± 0.2*	*0.78*	*12.5 ± 0.6*	$> 40M$
		0.21 ± 0.01	**2.3% ± 0.3**	**3.8 ± 0.2**	**0.79**	11.2 ± 0.5	**≈ 8k**
熊市	无回购	0.65 ± 0.05	28.7% ± 2.1	42.1 ± 3.5	0.92	2.1 ± 0.9	–
	固定利率阈值	0.59 ± 0.04	22.4% ± 1.8	35.5 ± 2.8	0.89	-12.4 ± 1.5	≈ 21k
	强化学习（近端策略优化）	0.48 ± 0.06	15.2% ± 2.4	28.4 ± 4.1	0.86	-5.1 ± 1.8	≈ 24k
	模型预测控制（预言机）	0.41 ± 0.08	8.2% ± 1.2	15.8 ± 2.1	0.83	-3.5 ± 1.1	≈ 720k
	DCBM（我们的方法）	*0.28 ± 0.02*	*5.0% ± 0.5*	*10.5 ± 0.8*	*0.80*	*-1.2 ± 0.3*	$> 40M$
		0.32 ± 0.02	**5.8% ± 0.6**	**12.6 ± 1.1**	**0.81**	**-1.8 ± 0.4**	**≈ 32k**
高波动性	无回购	0.89 ± 0.07	35.6% ± 3.2	28.4 ± 2.9	0.91	5.4 ± 1.2	–
	固定利率阈值	0.75 ± 0.05	28.5% ± 2.2	24.2 ± 2.5	0.88	-4.2 ± 1.4	≈ 21k
	强化学习（近端策略优化）	0.55 ± 0.08	18.4% ± 2.5	19.5 ± 3.1	0.85	-2.5 ± 1.6	≈ 15k
	模型预测控制（预言机）	0.45 ± 0.12	6.5% ± 1.1	11.5 ± 1.5	0.81	-0.5 ± 0.8	≈ 720k
	DCBM（我们的方法）	*0.26 ± 0.02*	*3.8% ± 0.4*	*7.2 ± 0.6*	*0.77*	*2.1 ± 0.4*	$> 40M$
		0.30 ± 0.02	**4.2% ± 0.5**	**8.1 ± 0.8**	**0.78**	1.5 ± 0.3	**≈ 28k**
需求冲击（+）	无回购	0.55 ± 0.04	18.5% ± 1.5	4.5 ± 0.3	0.89	**22.4 ± 1.8**	–
	固定利率阈值	0.45 ± 0.04	14.2% ± 1.3	4.2 ± 0.4	0.86	12.5 ± 1.0	≈ 21k
	强化学习（近端策略优化）	0.38 ± 0.05	9.2% ± 1.1	4.1 ± 0.4	0.83	14.2 ± 1.1	≈ 5k
	模型预测控制（预言机）	0.32 ± 0.06	5.1% ± 0.9	3.9 ± 0.5	0.81	16.8 ± 1.5	≈ 720k
	DCBM（我们的方法）	*0.22 ± 0.01*	*2.5% ± 0.3*	*3.2 ± 0.2*	*0.78*	*19.5 ± 0.8*	$> 40M$
		0.25 ± 0.02	**3.1% ± 0.4**	**3.6 ± 0.3**	**0.79**	18.1 ± 0.6	**≈ 8k**
需求冲击（-）	无回购	0.78 ± 0.06	42.1% ± 3.8	55.2 ± 4.5	0.94	1.5 ± 0.5	–
	固定利率阈值	0.70 ± 0.06	31.5% ± 2.8	45.2 ± 3.8	0.91	-6.5 ± 1.2	≈ 21k
	强化学习（近端策略优化）	0.62 ± 0.07	21.5% ± 2.2	32.4 ± 3.8	0.88	-8.5 ± 1.2	≈ 24k
	模型预测控制（预言机）	0.51 ± 0.09	12.4% ± 1.6	18.5 ± 2.2	0.84	-4.2 ± 0.9	≈ 720k
	DCBM（我们的方法）	*0.35 ± 0.02*	*6.8% ± 0.5*	*11.2 ± 1.1*	*0.81*	*-1.5 ± 0.4*	$> 40M$
		0.39 ± 0.03	**7.5% ± 0.8**	**14.1 ± 1.5**	**0.82**	**-2.4 ± 0.6**	**≈ 32k**
流动性危机	无回购	1.12 ± 0.15	58.4% ± 6.2	48.5 ± 5.1	0.95	3.2 ± 1.1	–
	固定利率阈值	0.98 ± 0.10	45.2% ± 5.1	42.1 ± 4.5	0.93	-4.2 ± 1.5	≈ 21k
	强化学习（近端策略优化）	0.85 ± 0.12	35.2% ± 4.5	35.2 ± 4.2	0.91	-9.2 ± 2.5	≈ 20k
	模型预测控制（预言机）	0.68 ± 0.14	15.4% ± 2.8	22.1 ± 3.5	0.88	-5.5 ± 1.8	≈ 720k
	DCBM（我们的方法）	*0.42 ± 0.04*	*8.5% ± 0.9*	*14.5 ± 1.5*	*0.84*	*0.5 ± 0.8*	$> 40M$
		0.48 ± 0.05	**10.2% ± 1.2**	**18.4 ± 2.1**	**0.86**	**-0.8 ± 1.2**	**≈ 30k**

待执行的回购，便在其执行前提交买单，随后提交卖单，从而获取无风险利润。在信号操纵攻击中，大额持有者抛售部分持仓，将价格压低至移动平均线以下，触发 PID 控制器发出强制回购信号。随后，他们以较低价格通过 PID 控制器卖出其余持仓。这些攻击旨在检验该系统究竟是稳定器，还是可预测的退出流动性来源。

为量化鲁棒性，我们测量**攻击者盈利能力**、**国库效率损失**和**稳定性退化**。我们假设，尽管简单的基于阈值的机制由于其二元响应而极易受到“Fishing”的影响，但 DCBM 的微分项（K_d）和积分记忆（K_i）将提供一定程度的抵抗力。微分项会抑制控制器对操纵企图中常见的突发剧烈价格下跌的反应，而积分项要求偏差持续存在，才能逐步提升回购压力，从而使瞬时的“拉高出货”攻击在资本效率上对攻击者而言变得低效。我们预计，这些实验将证明，与静态基准相比，DCBM 对国库造成的“操纵税”更低。

VI. 结果

我们展示了大规模智能体仿真的实证结果，评估动态控制回购机制（DCBM）相较于行业标准基线的有效性。实验采用本节所述的模拟框架，并在高性能计算集群上运行，每种情景进行 1,000 次蒙特卡洛运行。我们的分析聚焦于三个核心维度：(1) 不同市场条件下的宏观经济稳定性与网络健康；(2) 通过消融研究检验控制理论组件的具体贡献；(3) 系统抵御对抗性博弈论攻击的韧性。

A. 宏观经济稳定性与网络健康

我们的主要评估将 DCBM 与三个基线进行比较：放任不管 （无回购）模型、静态（固定利率）模型，以及启发式 （阈值）模型。我们在跳跃扩散过程 [7]所建模的三种不同市场机制下对这些模型进行了考察：牛市 （正漂移$\mu_D > 0$）、熊市 （负漂移 $\mu_D < 0$），以及高波动性 机制（高 σ_D，σ_P）。表 1 总结了总体性能指标。

1) 主要结果分析：表 1 中的结果表明，在所有情景下，DCBM 的稳定性指标均有显著改善。在**高波动性**机制下——这是对网络存续能力威胁最大的情形——与无回购基线相比，DCBM 将价格波动率（σ_P）降低了约 66%；与启发式阈值模型相比，则降低了 46%。波动率的下降直接对应着**运营者流失率**的降低：流失率从阈值模型的 19.5% 降至 DCBM 的 8.1%。对代理日志的定性检查显示，在 DCBM 仿真中，由于控制器积分项产生了可预测的“价格底线”效应，能够有力纠正持续的负偏差，运营者得以在更长时间内保持盈利能力。

值得注意的是，**国库增长**指标凸显了我们方法的资本效率。固定利率模型在熊市中不加区分地消耗资本，导致国库收缩 12.4%；而 DCBM 将这一损失限制在 1.8%。反之，在牛市中，DCBM 使国库能够积累储备（增长 11.2 %），而不是过度支出，从而有效地“未雨绸缪”。这种逆周期行为验证了控制律中嵌入的理论偿付能力约束。

B. 消融研究：组件贡献

表 II 高波动场景下的控制器配置消融研究

控制器	MSE	稳定时间 Time	Max 超调量	稳态-状态误差	控制 Var.
仅比例控制	0.045	142	18.5%	4.2%	0.12
仅比例积分控制	0.012	210	25.4%	**0.1%**	0.18
仅比例微分控制	0.038	**85**	**5.2%**	3.8%	0.09
完整 PID 控制	**0.008**	115	8.4%	0.3%	**0.11**

为单独考察比例（K_p）、积分（K_i）和微分（K_d）项的影响，我们在高波动场景下进行了消融研究。我们评估了四种控制器配置：仅比例控制、仅比例积分控制、仅比例微分控制和完整 PID 控制器。表2展示了控制性能指标。

1) 控制动态分析： 消融实验结果证实了各项的理论作用。**仅比例控制** 控制器表现出持续的稳态误差（4.2%），在持续卖压期间未能使价格完全回归移动平均线。在**仅比例积分控制**配置中加入积分项成功消除了该误差（$e_{ss} \approx 0.1$%），但也引入了显著的不稳定性，表现为较高的最大超调量（25.4%）和更长的调节时间。这与控制理论一致，因为积分项会增加相位滞后。

该**仅比例微分控制** 控制器响应最快（稳定时间：85 个区块），且超调量最低，体现了微分项抑制波动的能力。然而，它未能纠正长期漂移。**完整 PID 控制**配置实现了最佳权衡，利用积分项消除误差，并借助微分项抑制波动，因此均方误差最低（0.008）。

C. 对抗鲁棒性与控制系统安全

为使评估符合鲁棒机器学习和控制理论的标准，我们将 DCBM 控制器视为可微策略 $\pi_\theta(S_t)$，并对其实施基于梯度的对抗攻击。我们将标准对抗性攻击向量映射为经济操纵策略：

- **FGSM（快速梯度信号操纵）：** 类似于快速梯度符号法，这是一种单步、高强度的“闪崩”攻击，对手通过计算回购率$\nabla_S u_t$ 的梯度，并将价格 P_t 扰动 $-\epsilon \cdot \text{sign}(\nabla_S u_t)$，以最大化系统过度反应。

- **PGD（投影梯度下降操纵）：** 这是一种多步、迭代式的“持续操纵”攻击，对手在k 个区块内优化一系列交易，以耗尽国库，同时受资本预算 ϵ的约束。

- **C&W（成本优化套利）：** 这是一种 Carlini 和 Wagner 风格的攻击，旨在找到迫使控制器进入饱和状态（$u_t = 1.0$）所需的最小扰动δ ，同时将攻击者成本降至最低、将破坏程度最大化。我们评估了四种防御配置：1）**基线（阈值）：** 第 3.2 节所述的启发式规则。2）**PID-Standard：** 采用标准网格搜索调优参数的 DCBM。3）**PID-AdvTrain（对抗训练）：** 参数 θ 通过极小极大博弈目标优化的 DCBM：$\min_\theta \max_{\delta \in \Delta} \mathcal{L}(\pi_\theta(S_t + \delta))$。4）**PID-Cert（认证鲁棒性）：** 对积分项累积（裁剪）采用解析界，并对微分项施加利普希茨连续性约束的 DCBM。

1) 对抗动态分析：表 III 揭示了防御能力的严格层级。**基线（阈值）**模型与标准的非鲁棒分类器类似，即使在中等扰动预算（$\epsilon = 1.0$%）下也几乎完全崩溃，攻击成功率（ASR）接近 100%。这证实了静态二元规则很容易被对手利用，因为他们可以计算出触发阈值所需的精确卖出量。

PID-Standard 提供了基线水平的改进，显著减少了国库流失，但仍容易受到高预算迭代攻击（PGD）的影响

表 III 综合对抗鲁棒性分析

防御类型	攻击类型	预算（ϵ）	成功率 (↓)	鲁棒性分数 ↑	国库流失	防御效能	鲁棒性增益
基线	FGSM-Flash	1.0%	88.4%	0.116	22.1%	-	-
基线	FGSM-Flash	2.5%	96.2%	0.038	34.5%	-	-
基线	FGSM-Flash	5.0%	100.0%	0.000	58.2%	-	-
基线	PGD-Sustained	1.0%	92.1%	0.079	28.4%	-	-
基线	PGD-Sustained	2.5%	98.5%	0.015	45.1%	-	-
基线	PGD-Sustained	5.0%	100.0%	0.000	72.3%	-	-
基线	C&W-Arb	-	91.5%	0.085	18.2%	-	-
PID-Standard	FGSM-Flash	1.0%	42.1%	0.579	8.5%	+12.4%	+46.3%
PID-Standard	FGSM-Flash	2.5%	68.3%	0.317	14.2%	+8.1%	+27.9%
PID-Standard	FGSM-Flash	5.0%	85.2%	0.148	25.1%	+4.2%	+14.8%
PID-Standard	PGD-Sustained	1.0%	55.4%	0.446	12.8%	+9.5%	+36.7%
PID-Standard	PGD-Sustained	2.5%	81.2%	0.188	29.4%	+3.1%	+17.3%
PID-Standard	PGD-Sustained	5.0%	94.1%	0.059	48.2%	+1.2%	+5.9%
PID-Standard	C&W-Arb	-	62.4%	0.376	11.5%	+10.2%	+29.1%
PID-AdvTrain	FGSM-Flash	1.0%	12.5%	0.875	3.2%	+28.5%	+75.9%
PID-AdvTrain	FGSM-Flash	2.5%	24.1%	0.759	5.8%	+22.1%	+72.1%
PID-AdvTrain	FGSM-Flash	5.0%	45.3%	0.547	11.2%	+16.4%	+54.7%
PID-AdvTrain	PGD-Sustained	1.0%	18.2%	0.818	4.5%	+25.2%	+73.7%
PID-AdvTrain	PGD-Sustained	2.5%	35.6%	0.644	9.1%	+18.7%	+62.9%
PID-AdvTrain	PGD-Sustained	5.0%	62.1%	0.379	18.5%	+11.2%	+37.9%
PID-AdvTrain	C&W-Arb	-	28.4%	0.716	6.2%	+24.8%	+63.1%
PID-Cert	FGSM-Flash	1.0%	**4.2%**	**0.958**	**1.2%**	**+32.1%**	**+84.2%**
PID-Cert	FGSM-Flash	2.5%	**9.1%**	**0.909**	**2.4%**	**+29.4%**	**+87.1%**
PID-Cert	FGSM-Flash	5.0%	**18.5%**	**0.815**	**4.8%**	**+24.8%**	**+81.5%**
PID-Cert	PGD-Sustained	1.0%	8.4%	0.916	1.8%	+30.2%	+83.4%
PID-Cert	PGD-Sustained	2.5%	15.2%	0.848	3.9%	+26.5%	+83.3%
PID-Cert	PGD-Sustained	5.0%	32.1%	0.679	8.5%	+19.1%	+67.9%
PID-Cert	C&W-Arb	-	12.6%	0.874	2.9%	+28.2%	+78.9%
输入平滑	FGSM-Flash	5.0%	55.2%	0.448	14.5%	+12.4%	+44.8%
输入平滑	PGD-Sustained	5.0%	78.4%	0.216	32.1%	+5.1%	+21.6%

在这类攻击中，对手会随着时间推移将控制器“引导”至不稳定区域。

在区块链环境中部署确定性控制回路，不可避免地会引入博弈论层面的漏洞，对手会试图逆向分析干预逻辑，以获取无风险收益。本分析评估了所提出的 DCBM 对此类复杂威胁的抵御能力，具体对比了启发式基线与先进的控制理论防御。来自“Fishing”和“Flash Crash”向量模拟的结果表明，依赖静态规则或不受约束的反馈回路的防御机制，最终会成为资金雄厚的对手可预测的退出流动性。

静态启发式模型在遭受基于优化的攻击时，其脆弱性立即显现，证实了二元干预规则从根本上并不安全这一假设。理论上的脆弱性在基线（阈值）模型中转化为灾难性故障，该模型无法根据冲击的严重程度或持续时间调节其响应。在仅有 $\epsilon = 1.0\%$ 预算的 FGSM-Flash 攻击下，基线模型的攻击成功率（ASR）已经达到 88.4%3。这种失败

在 PGD-Sustained 攻击（$\epsilon = 5.0\%$）下变得彻底，基线模型有 100.0% 的概率失败，导致国库流失高达 72.3%，实际上使该协议陷入资不抵债。

标准反馈控制机制通过引入难以被瞬时利用的软响应曲线，相较于静态基准实现了具有统计显著性的改进，但仍容易受到持续操纵的影响。PID-Standard 配置可减弱瞬时冲击的效力，将 1.0% FGSM-Flash 攻击的成功率从 88.4% 降至 42.1%，并将国库流失限制在 8.5%。然而，这种未经强化的控制器难以抵御随时间推移引导系统的迭代优化攻击；在高预算的 PGD-Sustained 攻击（$\epsilon = 5.0\%$）下，PID-Standard 仍然失守，成功率高达 94.1%，国库流失达到 48.2%。这表明，若没有特定约束，攻击者仍可利用积分项使控制器达到饱和。

对抗训练能够有效增强控制器抵御已知攻击梯度的能力，使防御从被动响应转为主动防御，并提升鲁棒性。针对极大极小目标进行优化的 PID-AdvTrain 模型

针对 PGD攻击模型时，该模型在所有向量上的可利用性都大幅降低。遭受 FGSM-Flash（1.0%）攻击时，成功率降至 12.5%，国库流失也被限制在微不足道的 3.2%。即使面对威力极强的 C&W-Arbattack，鲁棒性仍保持在 0.716，远高于标准 PID 的 0.376。

归根结底，通过认证鲁棒性施加结构约束，似乎是最有效的防御机制，其表现甚至优于通过对抗训练学习到的模型参数。一方面，PID-Cert 设置通过利用利普希茨连续性和饱和阈值，对控制权限施加数学约束，从而防止系统无论输入扰动的规模如何都出现过度反应。另一方面，其在最具对抗性的测试环境——预算为 5.0% 的 PGD-Sustained 攻击——中的有效性也证明了这一点：系统将攻击成功率控制在 32.1%，并将金库耗竭维持在可控的 8.5%，与基准系统 72.3% 的损失相比，差距近十倍。

七、讨论

首先，去中心化人工智能网络的运营可行性在很大程度上取决于各自代币的经济稳定性，因为高波动性使得人工智能应用中的算力提供商难以规划资本支出，模型用户也难以规划运营支出。实验表明，动态控制回购机制（DCBM）成功地将网络效用与投机性市场周期分离，与自由放任的做法相比，价格波动率降低了 66%。DCBM 为人工智能网络运营商提供了稳定的收入底线，因为它将代币经济从混乱、受情绪驱动的市场转变为动态系统，从而将流失率从 19.5% 降至 8.1%。因此，DePIN 若要与采用固定法定货币价格的软件即服务应用竞争，就必须采用这一机制。

虽然目标是实现稳定，但从博弈论视角来看，稳定机制本身的韧性才是决定特定无许可网络长期可持续性的关键。在对抗性测试中，启发式“阈值”方法遭遇灾难性失败，其失败率接近100%，这说明在对抗性环境中使用静态规则存在极高风险。在黑暗森林情景下，整体平衡由最大可提取价值（MEV）机器人的行为主导，明确且静态的干预水平会向信息充分的代理发出可预测且可被利用的信号，使其能够从项目金库中获取无风险收益。结果表明，DCBM 的“认证鲁棒性”设置扭转了这一局面，迫使攻击者承担与操纵持续时间成正比的市场风险，从数学上使拉高出货策略变得无利可图。

为区分“储蓄”和“稳定”，请考虑国库中可观察到的以下行为：固定利率基线与 DCBM 的动态特性各不相同。传统的回购策略会销毁固定比例的收入，具有顺周期性：在网络最需要储备来维护价值时，反而会减少储备。另一方面，DCBM 的积分分量施加了天然的逆周期约束，确保牛市期间的利润为 11.2%，同时将熊市期间的回撤控制在 1.8%。这一现象验证了与渐近偿付能力相关的数学证明，表明控制理论执行器在理论上可以确保协议无论收入如何崩溃都不会违约。最后，本研究提出了一种代币工程范式转变，即从酌情制定货币政策转向控制系统。基于“开关式”阈值政策或 DAO 投票的先进方法，其反应时间和数学确定性不足以应对市场上的高频过程。本研究通过在区块链上实现泰勒规则和 PID 控制，弥合了宏观经济理论与智能合约实现之间的差距。PID-Cert 模型的优异表现表明，未来关于 DePIN 代币经济学的研究应聚焦于利普希茨连续性和饱和水平等结构约束，而不是可能对分布变化敏感的复杂模型。

VIII. 局限性

从理论角度看，该机制的基本假设是将市场动态简化为线性模型，因此在极端非线性情景下，其适用性受到限制。作者围绕选定的工作点对被控对象动态进行线性化，以便简化控制系统设计，这意味着假设回购与总体流动性水平之间呈线性关系。这种简化本质上受恒定乘积做市商（CPMM）机制所决定的系统稳定性约束，并与条件 $x \cdot y = K$ 相一致。因此，系统面临“小池塘里的鲸鱼”风险：稳定区域与流动性成反比；随着流动性降低，被控对象增益趋于无穷大，最终导致静态参数控制器发生振荡失稳或出现“振铃”，除非进行人工干预。

将确定性控制回路集成到无需许可的区块链系统中，会带来传统控制系统设计未能充分缓解的特定博弈论风险。由于控制逻辑具有透明性，最大可提取价值（MEV）参与者能够对控制系统的阈值进行逆向分析，并通过“Fishing”或“闪崩”攻击操纵系统。尽管作者提出了应对措施，但他们也承认，若未针对认证鲁棒性要求（例如 Lipschitz 值和饱和水平）进行专门加固，标准的、未经加固的比例-积分-微分（PID）控制系统仍容易受到优化攻击；在 PGD 持续攻击中，其失效率高达 94.1%。

在以太坊虚拟机（EVM）上实现复杂的控制理论，会受到严苛的计算限制，迫使人们在精度与成本之间权衡。作者面临浮点运算和超越函数所带来的“Gas 成本不可能性”问题，因为直接在链上计算这些内容的成本高得令人难以承受。为了使该机制在经济上可行，设计必须依赖定点运算、查找表和泰勒级数展开，以近似计算自然对数等必要运算。即便进行了这些优化，控制器的执行成本目标仍约为 150,000 Gas，对于高频部署而言，这仍是一笔不小的开销。

然而，该机制的验证仍局限于理论层面的仿真，而非在主网上实施。研究结果来自基于代理的建模，并利用合成跳跃扩散过程和历史数据来模拟市场冲击与需求。尽管这些仿真结果优于当前基线，但研究明确指出，当前实现尚不具备自适应增益调度能力，无法在链上验证控制参数。因此，系统可能难以根据市场变化自行校正参数。

IX. 结论

人工智能民主化所依托的经济基础设施，与支撑它的加密基础设施同样坚实。在本研究中，我们提出了动态控制回购机制（DCBM），这是一种基于控制理论的新方法，旨在调节人工智能经济系统，并根据市场动态控制代币发行，从而无需中介即可解决区分有机增长与投机这一根本问题。

全面的代理级模拟结果表明，稳定的经济层对于稳健的物理基础设施而言不可或缺。与行业标准基线相比，DCBM 在价格波动率和流失率改善方面均达到统计显著性，从而为计算服务提供商确保了可预测的环境。此外，DCBM 还能通过在需求高峰期有效积累储备，以防范经济活动低迷时期，从而提升资本效率。因此，DCBM 展现出固定费率模型所不具备的逆周期特征。

然而，除了宏观稳定性问题之外，显然，无需许可的金融网络中的对抗鲁棒性也备受重视。比较各种防御策略后发现，尽管学习算法能够带来一定收益，但只有认证鲁棒性等结构约束，才能为抵御博弈论攻击提供必要的数学保证。未来的工作将以此为基础，研究如何通过用于验证的自适应增益调度，在链上验证控制值。

参考文献

[1] J. Zarrin等，“迈向去中心化智能：区块链赋能的人工智能系统系统性文献综述”，人工智能，第 5 卷，23，2024 2，第 p 页。[2] L. W. Cong、Y. Li 和 N. Wang，“代币经济学：动态采用与估值”，技术报告 27222，美国国家经济研究局，2020。[3] Reflexivity Research，“DePIN 的现状”，2024。访问日期：2025 年 12 月 22 日。[4]D. W. E. Allen、C. Berg 和 S. Davidson，“回购与销毁机制：价格操纵还是价值信号传递？”，*SSRN* 电子期刊，2022。[5] R. Sams，“关于加密货币稳定化的一则札记：铸币税份额”，2015。[6] S. O. Yese、S. Berri 和 A. Chorti，“一种采用超额预订和动态回购过程的新型切片准入控制方案”，载于*2023* 年 *IEEE* 网络功能虚拟化与软件定义网络会议（*NFV-SDN*），第 1–7 页，2023。[7] S. Kou，“期权定价的跳跃扩散模型”，美国金融协会年会（*AFA*），2001。[8] S. Kampakis，“代币经济学的三个案例研究”，英国区块链协会期刊，第 1 卷，第 2 期，2018。[9] R. Carvalho，“代币经济学设计及其与传统金融的异同”，国际金融市场杂志，2022。预印本可在线获取。[10] E. Waisanen 和 E. Wood，“Hydro Finance：通过可持续激励和独立流动性，推动 AMM 模型摆脱融资前投机”，技术报告，Hydro Finance，2022 年 4 月。访问于 2025 年 12 月。[11] monet-supply，“stkmkr：Maker 质押与代币经济学修订”，2022。MakerDAO 论坛。访问于 2026 年 1 月。[12] STEPN Official，“STEPN 宣布第二季度利润，并启动季度 GMT 回购与销毁”，2022。Medium。访问于 2026 年 1 月。[13] PancakeSwap，“CAKE 代币经济学”，2023。PancakeSwap 文档。访问于 2026 年 1 月。[14] Polkadot Wiki，“国库”，2023。Polkadot 文档。访问于 2026 年 1 月。[15] P. Garvey，“代币设计与应用场景”，载于《区块链基本面分析：数字资产投资者指南：最大限度降低风险并提高回报》，第 327–357 页，Springer，2025。[16] S. Sharma，“探索加密领域人工智能代理的未来”，*Outlook*，第 1 卷，第 1 页，2024。[17] M. Woodford，“泰勒规则与最优货币政策”，美国经济评论，第 91 卷，第 2 期，第 232–237 页，2001。[18] J. Bullard 和 K. Mitra，“货币政策规则学习”，货币经济学杂志，第 49 卷，第 6 期，第 1105–1129 页，2002。[19] K. Aoki、K. Nikolov、F. Canova 和 V. Chari，“中央银行学习背景下的规则型货币政策 [附评论],”，载于*NBER* 国际宏观经济学研讨会，第 2004 卷，第 145–195 页，芝加哥大学出版社，芝加哥，伊利诺伊州，2004。[20] R. J. Hawkins、J. K. Speakes 和 D. E. Hamilton，“货币政策与 PID 控制”，经济互动与协调杂志，第 10 卷，第 1 期，第 183–197 页，2015。[21] I. Lebedeva、D. Umnov、Y. Yanovich、I. Melnikov 和 G. Ovchinnikov，“去中心化交易所中用于减少无常损失的动态费用”，*arXiv* 预印本 *arXiv:2506.03001*，2025。