arXiv:2611.32389v1 [cs.CR] 24 Nov 2026

# AgentBank：基于区块链的智能体支付

Yuexin Xiang[1,2], Martin Perešíni[3], Yuchen Lei[4], Yuquan Li[5,2], Yuanzhe Zhang[6], Andreas Deppeler[7], TszHon Yuen[1], Shiping Chen[8], Qin Wang[2,8],和 Burkhard Stiller[3]

[1] 莫纳什大学信息技术学院，澳大利亚[2] 澳大利亚数字金融合作研究中心[3] 苏黎世大学信息学系通信系统组，瑞士[4] 武汉大学网络空间安全学院，中国[5] 墨尔本大学商业与经济学院，澳大利亚[6] 南洋理工大学数字信任中心，新加坡[7] 莫纳什大学商学院，马来西亚[8] 澳大利亚联邦科学与工业研究组织，悉尼，澳大利亚

**摘要。** 人工智能代理日益通过 x402 和 AP2 等协议为数据和计算付费，但独立出资的钱包会造成资金闲置，而且每笔支付都需要进行资产转移。我们提出 *AgentBank*，这是一种智能合约银行层，允许代理依据所有者签发的授权和链上支出限额使用银行负债。内部支付只更新账户余额，无需转移资产；资金池支持资金则在储备金与收益策略之间进行配置。我们对代理密钥遭攻陷造成的损失设定上限，并分析相关需求如何影响储备要求。实验表明，与每代理钱包相比，AgentBank 可将闲置流动性减少 52–77%，并降低批量内部支付的 Gas 成本。利用历史去中心化金融流动性数据，我们评估储备金政策在市场压力期间如何权衡资金库收益与支付可用性。我们还进一步探讨自动化挤兑的风险，并评估缓解这些风险的机制。

**关键词：** Ag entic 支付 · x402 · AP2 · 去中心化金融 · 流动性 · 金融

## 1 引言

人工智能代理越来越多地在几乎无需人工参与的情况下购买 API 调用、数据、推理服务以及其他代理提供的服务，而一系列不断扩大的协议也让它们能够授权支付：x402 让 HTTP 402 状态码重获新生，以支持按请求进行稳定币支付 [53], AP2 将用户授权传达给商家 [29], 而银行卡网络和支付处理商也发布了类似的框架 [59, 61]。在 Base 上，x402 在 280 天内记录了 1.367 亿笔结算，不过其中大多数只是虚构数据或运营方内部交易，并非独立需求 [46]。

这些系统共享一种金融抽象：钱包。代理的支付能力取决于为其注资的钱包余额，并且可能受到支出策略的约束 [16]。这种抽象带来了三项成本。首先，流动性被分散。每个钱包都必须按自身的需求峰值预先注资，而由任务驱动的代理需求具有突发性，因此各代理缓冲金的总和远超整体需求所需。其次，预充值余额处于闲置状态，无法产生收益。第三，每笔支付，即使发生在同一生态系统的代理之间，也要在链上转移结算资产。此外还存在安全隐患：如果代理受到提示词或记忆注入的操纵 [52] ，那么除非在模型底层强制执行额度限制，否则它就能花掉钱包中的所有资金。

银行从设计上就解决了前三项成本。银行余额是负债，而非对特定资产的所有权。账户之间的支付会重新分配负债，而不会移动储备金；银行只针对净流出持有流动性储备，并将其余资金用于生产性用途 [21, 39]。代币化存款将这种分离带到了可编程账本上 [4, 8, 25, 37]。同样的转变也带来了脆弱性：投入去中心化金融平台的支撑资产，在最需要时可能变得缺乏流动性。2026年4月18日发生 KelpDAO 漏洞利用事件后，以太坊上的 Aave v3 USDC 市场连续四天维持在 99.87% 的利用率，导致供应方持有的 18.9 亿美元无法提取 [45, 56]。部分准备金也会引发挤兑 [21, 28], ，而众所周知，链上透明度会加速挤兑 [2, 47], ；当存款人本身就是自动化代理时，这一问题便更加突出。

已部署的代理支付系统占据了设计空间的两个极端：一种是注资钱包，为每个代理持有足额储备；另一种是持有收益型代币的代理，将其全部余额用于投资。本文提出**AgentBank**，这是一种面向人工智能代理的智能合约银行层，位于两者之间：池化负债由储备金提供支撑，而储备金规模取决于策略选择。本文还研究了这一选择所带来的效率–韧性权衡。该问题将稳定币储备设计、委托策略管理和交易排序结合起来，且付款方与存款人均为机器。本文作出三项贡献。

**1.)** 我们设计了 AgentBank，这是一种智能合约银行架构，允许代理依据所有者签发的授权，在链上支出限额内使用银行负债。账户之间的支付通过内部结算完成，而汇集的支撑资产则在结算储备金与获准的收益策略之间分配，并受链上储备金约束和经折价调整的覆盖约束。未获覆盖的外部支付将进入到期队列。发生减值后，付款须遵循偿付能力约束下的赎回机制。扩展功能包括远期定价、epoch 结算和流动性费用。

**2.)** 我们证明了资产负债表守恒，并对遭泄露的代理密钥造成的损失进行了界定。我们表明，在需求相关的情况下，池化储备要求会收敛于单因子（Vasicek）极限；推导出适用于有限资金池的粒度调整；并说明传统的平方根法则为何会低估流动性要求。我们还表明，按面值顺序赎回会将损失集中到较晚赎回的存款人身上，而

在确认损失后，偿付能力条件赎回会消除这种先行者优势，前提是没有进一步的损失或清算成本。

**3.)** 我们将 Solidity 原型与 EIP-3009 和 ERC-4337 基准进行比较，以衡量委托支付的 Gas 成本。利用突发且相关的代理需求以及历史借贷池数据，我们量化了相较于每代理钱包 52–77% 的闲置流动性节省，并将其归因于所有者池化、银行池化和支付内部化。我们还分析了 2026年4月流动性冻结期间国库收益与支付可用性之间的权衡，估算了仅采用国库券策略时的储备要求，并测量自动化存款人耗尽储备金的速度。

## 2 背景与相关工作

**代理支付**。一项关于区块链上代理间支付的系统化研究，将支付生命周期分解为四个阶段，并指出意图绑定薄弱是一个尚待解决的问题 [63]。其分类体系未涵盖资金池式、类似银行的负债，而这正是本文的设计空间。已部署的协议将支付绑定到 HTTP 请求（x402，通过 EIP-3009 转移授权结算 [53]）、可验证的用户授权指令（AP2 [29]）或卡凭证 [59]。安全研究指出了 x402支付中的风险以及针对代理的上下文操纵攻击 [52, 60]。账户抽象和委托标准使账户具备可编程性、限定委托范围和定期额度，并注册代理身份。在所有这些

**表 1**。设计比较。

| 设计 | Par | No prefunding | Internal pay. | Yield | On-chain caps | Illiquidity |
|---|---|---|---|---|---|---|
| 注资型代理钱包 [53] | ✓ | ✗ | ✗ | ✗ | ○ | 不适用（已预留） |
| 智能账户，会话密钥 | ✓ | ○ | ✗ | ✗ | ✓ | 不适用（已预留） |
| 通道，会话 [61] | ✓ | ✗ | ○ | ✗ | ○ | 不适用（按配对） |
| TEE 净额结算 [14] | ✓ | ○ | ✓ | ✗ | ○ | 不适用（已预留） |
| 生息代币 | ✗ | ✗ | ✓ | ✓ | ✗ | 已阻止 |
| 链下托管账本 | ✓ | ✓ | ✓ | ○ | ✗ | 不透明 |
| **AgentBank** | ✓ | ✓ | ✓ | ✓ | ✓ | 储备金，队列 |

✓：已提供。○：部分提供。✗：未提供。不适用：不适用。预注资按代理分别进行。智能账户由每位所有者共享。

在这些系统中，授权背后的资金是获授权钱包或账户的余额。而 AgentBank 则将委托权限附加到一项<需要由其他方管理其支持资产的银行负债上。

**结算内部化**。支付通道会延后基础层结算 [22,51,55]，但会锁定各通道的流动性，并需要进行再平衡 [40]。面向代理的设计会批量处理或净额结算：Circle Gateway 在可信执行环境中对签名授权进行净额结算 [14],，A402 则通过基于 TEE 的金库汇总通道结算 [44]。这些设计会让付款方资金全额作为储备金闲置。在传统支付系统中，分层和节省流动性机制会降低流动性需求 [36, 38, 50],；对 CHAPS 分层机制的模拟表明，节省的流动性主要来自资金池化，而非内部化 [41],，正如我们的分解分析

对代理需求所做的分析。其根本作用是风险池化，经典形式是库存池化平方根法则 [23]。在需求相关或呈重尾分布时，池化收益会缩小 [7,17]。

**可编程银行业务**。 代币化存款在可编程账本上保留了账户负债与支撑资产之间的区别 [4,5,8,25],，且一家受监管银行已在公链上发行存款代币 [37]。稳定币在承压时的表现类似货币市场基金 [3],„ 链上透明度会加速挤兑 [47], ，信息披露对挤兑风险的影响尚不明确 [2],„ 赎回权限需要在价格稳定性与挤兑风险之间权衡 [48], ，而资本和流动性阈值是主要的监管杠杆 [27]。去中心化金融借贷池让存款能够产生收益，但提款受到未借出流动性的限制 [32,62],„ 而这种流动性在自我强化的情形中可能会消失 [12,42]。ERC-4626金库及其异步扩展 ERC-7540实现了份额记账和排队赎回的标准化。然而，金库份额的价值会浮动，策略损失也会转嫁给持有者。**表1** 将这些设计与AgentBank进行了对比。

## 3 AgentBank设计

AgentBank由两个核心智能合约 BankCore 和 TreasuryManager，以及每种获批投资策略对应的一个适配器构成。BankCore负责处理账户和支付。TreasuryManager通过适配器管理这些汇集的支撑资产。我们先介绍它们的组件，再说明它们如何实现银行的各项操作。

### 3.1 合约组件（图 1(a)）

每种结算资产都有各自的 BankCore 和 TreasuryManager。采用一种获批策略时，该部署包含三个 AgentBank 合约：

• **BankCore**。 接受存款、记录所有者余额和授权指令、验证签名支付意图，并持有流动性储备。它实现账户、授权与限额以及支付区块中的功能，包括内部转账、外部付款、先进先出队列和减值回收。

• **TreasuryManager**。 在 BankCore 和获批策略之间转移支撑资产。它实现储备分配并管理收益策略，在释放资金前检查储备下限和按折扣调整的覆盖率。

• **策略适配器**。位于收益策略之后，将 TreasuryManager 连接到一个外部场所。该原型的 ERC-4626适配器负责投资和提取资产，并报告头寸价值和可提取金额。

风险与控制模块将 BankCore 的结算规则与国库管理器的部署约束归为一组。

账户所有者存入资产，并授权代理从其账户中支出。多个代理可以共享同一所有者的余额。中继者提交已签名的

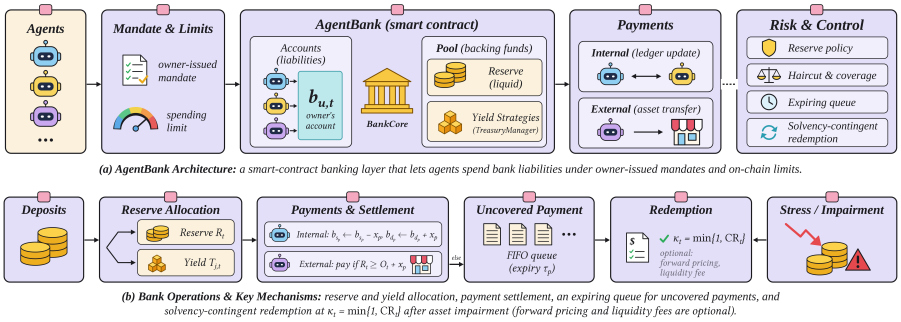


**图 1.** AgentBank：**(a)** 合约组件；**(b)** 操作流程。（ 存款与分配， 支付， 队， 减值。）

意图，外部收款方接收资产转账。银行运营方提供第一损失资本、批准策略并设定资金库参数，但无法修改账户余额。

我们假设已发布合约均能正确执行，且结算资产保持其名义价值。脱锚和发行方冻结不在模型范围内。攻击者可能危及代理的会话密钥，或诱使代理签署有害意图 [52]。他们可能审查、延迟或重新排序交易（中继者和区块构建者都能做到这一点） [19]，并在不同授权、部署实例或链之间重放意图。他们还可能导致策略损失或流动性不足，包括通过漏洞利用造成的损失 [26]。运营方的不当行为仅限于在链上资金库约束范围内选择参数和策略。参数变更应受时间锁约束。

**账户与支持资产**。 账户和资金池模块描述了银行资产负债表的两侧。BankCore 记录账户负债并持有储备金。适配器持有投资头寸，并通过 TreasuryManager 报告其价值。每个部署实例使用一种 ERC-20 结算资产，通常是法币计价稳定币，且不进行资产间转换。我们固定一种资产 $\sigma$，并令索引 $t$ 表示某项操作之前的即时合约状态。BankCore 维护一组账户 $\mathcal{U}$，其中 $b_{u,t} \geq 0$表示账户 $u \in \mathcal{U}$的余额。该余额是 AgentBank 的负债，而非对专用储备金的索取权。已接受但尚未结算的外部支付构成未偿义务 $O_t$，并存放在先进先出（FIFO）队列中。负债是

$$D_t = \sum_{u \in \mathcal{U}} b_{u,t}, \qquad L_t = D_t + O_t. \tag{1}$$

在资产方面， $R_t$ 是 BankCore 持有的结算储备金，$T_{j,t}$ 是获批策略 $j \in \{1, \ldots, J\}$ 中头寸的盯市价值。资产总额和权益为

$$A_t = R_t + \sum_j T_{j,t}, \qquad E_t = A_t - L_t, \tag{2}$$

运营方提供初始权益 $E_0 > 0$ 作为第一损失缓冲。每项策略都带有估值因子 $h_j \in [0, 1]$ （其中 $h_j = 1$ 表示无折价），

从而得出经折扣调整的有效资产和覆盖率

$$\begin{aligned} A_t^{\text{eff}} &= R_t + \textstyle\sum_j h_j T_{j,t}, \\ \text{CR}_t &= A_t^{\text{eff}} / L_t \qquad (L_t > 0). \end{aligned} \tag{3}$$

### 3.2 操作流程（图1(b)）

该流程涵盖从存款和分配到授权支付的全过程。队列处理用于应对流动性不足，而减值处理则会在发生资产损失后调整即时付款和排队付款。

● **存款与分配**。所有者将结算资产存入 BankCore，这会使所有者的账户余额及其储备金增加相同的金额。在储备金分配模块中，运营方可单独触发资金管理操作，自行选择投资或召回的时机及金额。对于将 $z > 0$ 单位投入策略 $j$ 的部署，TreasuryManager 仅在以下条件满足时才允许 BankCore 将这些资产转移至适配器：

$$\begin{aligned} R_t - z &\geq O_t + r_{\min} D_t, \\ A_t^{\text{eff}} - (1 - h_j)\, z &\geq \text{CR}_{\min} L_t. \end{aligned} \tag{4}$$

其中，$r_{\min} \in [0, 1]$ 为最低储备金率，$\text{CR}_{\min} \geq 1$ 为覆盖率下限。随后，适配器会投资所释放的资产。若要召回资金，TreasuryManager 会检查适配器的可提取金额，并指示其将资产返还至 BankCore，后者随即更新其储备金。在这些约束下，运营方将储备金目标设为 $R_t^* = O_t + B_t$，其中 $B_t$ 为应对新的外部需求而设置的缓冲金。固定 策略将 $B_t = r_{\text{base}} D_t$ 设为 $r_{\text{base}} \in [r_{\min}, 1]$。需求感知策略将

$$B_t = \max\{r_{\min} D_t,\ Q_\alpha(\mathcal{X}_{t,W})\}, \tag{5}$$

其中，$\mathcal{X}_{t,\ W}$ 包含此前 $W$ 天内观测到的请求外部流出（支付和提款）的滚动 $\Delta$ 小时总额。因此，$\Delta$ 是以小时计的规划期限，$W$ 是以天计的回溯时长，$Q_\alpha$ 是经验 $\alpha$分位数。需求估算在链下计算。**公式 4** 中的部署约束仍在链上强制执行。

覆盖并不意味着流动性充足：储备金以及能够及时召回的资产必须足以覆盖近期流出，如巴塞尔流动性覆盖率 [6]所示。借贷池资金召回取决于未借出流动性 [32]，而该流动性可能在数小时内接近于零。折价应反映压力情景下的可提取性和价格风险。

● **支付执行**。Payment $p$ 从授权的付款方账户$s_p \in \mathcal{U}$ 扣款，并指定模式 $q_p \in \{$ int，ext$\}$、收款方 $d_p$和金额 $x_p > 0$。

BankCore 首先检查授权与限额规则。所有者 $o$ 注册一条授权指令 $M = (\sigma,\ o,\ u,\ a,\ \Pi,\ n)$，允许代理密钥 $a$ 从账户 $u$中支出。同一账户可以由多个代理分别持有独立的授权指令。该策略$\Pi$ 规定单笔支付限额 $\ell_{\text{tx}}$、每个时间窗口的累计额度 $\ell_{\text{win}}$，以及

时长 $\omega$、有效期，以及可接受的结算模式与收款方组合（$q$， $d$）（明确列表或默克尔根）。只有 $o$ 可以注册或撤销 $M$。在该原型中，账户地址同时也是其所有者。授权随机数 $n$用于区分条款完全相同的授权。

标识符 id($M$) 是已注册授权条款（包括账户、代理、策略和授权随机数）的域分离 EIP-712 摘要。其域绑定链标识符和 BankCore 地址，从而确定结算资产。注册会将授权存储在该标识符下。撤销是最终性的，因此同一标识符无法再次注册。对于支付 $p$，代理使用相同的 EIP-712 域对$I_p$ =(id($M$) $q_p$， $d_p$， $x_p$， $n_p$， $\tau_p$)进行签名。其中， $n_p$是支付随机数，用于检查其是否在 id($M$)内被重复使用； $\tau_p$ 是意图的到期时间。BankCore 从所引用的授权中推导付款方，因此 $s_p = u$。该意图无法选择其他账户。

BankCore 仅在以下条件均满足时接受意图：授权已注册且未被撤销，签名可恢复为 $a$，随机数尚未使用，意图和授权均处于各自的有效期内，($q_p$， $d_p$)是可接受的， $x_p \le \ell_{\text{tx}}$，窗口许可额度未超出，以及 $b_{u,\ t} \ge x_p$。在扣除付款方资金之前，接受操作会消耗该授权内的支付随机数和额度；之后的取消不会恢复这些额度。所有状态更新均先于代币转账执行，且入口点受到防重入保护。由于意图不绑定交易发送方，中继者可以提交意图，并且多个意图可以在一笔交易中批量处理；每个意图都会根据其前置意图留下的状态进行验证（算法1）。

完成这些检查后，BankCore 通过支付区块结算已接受意图。内部支付要求 $d_p$ 是使用相同资产的 AgentBank 账户。BankCore 从 $s_p$ 扣款并向 $d_p$ 入账，使 $L_t$ 和所有资产保持不变。外部支付从 $s_p$ 扣款；如果

$$R_t \ge O_t + x_p, \tag{6}$$

这能保护流动性，确保较早产生的债务优先处理。提款采用外部支付路径。收款方成员资格的变更不会改变已签署的模式。

- **队列处理**。如果储备金条件不满足，BankCore 会将该笔支付追加到未覆盖支付区块中的先进先出队列，并将 $O_t$ 增加 $x_p$。任何地址都可以触发队列处理，按先进先出顺序处理数量有限的条目：如果债务 $k$ 的到期时间 $\tau_k$ （继承自其支付意图）已过，则取消该债务，并将其金额退还给付款方。否则，如果储备金足以支付其款项，则进行结算；处理会在遇到首笔未到期且无法结算的债务时停止。

- **减值处理**。赎回区块将支持资产估值与 BankCore 的外部付款连接起来。BankCore 读取其储备金和负债，并从 TreasuryManager 获取经折价调整的策略价值。违约规则按先进先出顺序处理排队义务，并根据报告的偿付能力调整每笔外部付款。对于 $L_t > 0$，回收率为 $\kappa_t$ =min$\{1,\text{CR}_t\}$：覆盖率至少为 1 时按面值结算，$\text{CR}_t < 1$ 时则进入减值模式。对于即时支付和排队

结算，BankCore 转移 $\kappa_t x$ 以换取名义债权 $x$ ，并消除 $x$ 负债。内部支付仅转移名义余额，不转移资产。默认设置没有通知期、分 epoch 批处理或清算费。在估值精确、没有折价且可无成本召回的情况下，它将 MakerDAO 紧急关闭中的按比例偿付机制延续到连续结算中 [49]。适配器必须报告保守且抗操纵的估值。延迟确认损失可能使早期赎回者按面值获得偿付。

该原型实现了这一违约规则。我们在模拟中分别评估了三项可选扩展。远期定价 按照 ERC-7540 的异步请求模型，将所有外部付款（包括提款）延迟至预先承诺的通知期结束，并采用结算时的回收率。*epoch* 结算 以每个 epoch 内对可用储备按比例分配取代先进先出优先级，从而消除该 epoch 内排序的价值 [9]。流动性费用 向赎回者收取因其付款需要清算策略头寸而产生的折价费用，类似于摆动定价 [35]。这些扩展分别应对估值滞后、交易优先级和清算成本问题。启用这些扩展时，其规则会预先固定，以避免与酌情赎回门槛相关的先发挤兑 [13, 43]。美国货币市场基金改革在 2023 [57] 中取消了赎回门槛。

## 4 分析

我们证明，AgentBank 通过所有者签发的授权保持资产负债表一致性，并限制被攻陷的代理密钥依据该授权造成的损失。我们推导了相关需求下的池化储备要求，并阐明顺序按面值赎回如何将损失集中于较晚的赎回者。我们还展示了偿付能力条件赎回何时能够消除这一劣势，以及延迟损失确认为何会限制其保护作用。完整证明见**第 C 节**。

**账户安全。** 内部支付只能在账户之间转移债权，而委托只能开放所有者授权许可的资金。以下结果将这两项要求形式化。

**引理1（守恒）。** 表***4*** 中的每项操作都满足 $\Delta A = \Delta L + \Delta E$。权益仅通过资本出资、国库损益或负债减记发生变化。内部支付保持 $D$, $O$, $R$ 和 $T$不变。

**命题1（有界委托损失）。** 设账户 $u$ 上的授权 $M$ 具有窗口许可额度 $\ell_{\text{win}}$ 和窗口长度 $\omega$，且其会话密钥从时间 $t_c$ 起由对手控制，直至所有者撤销于 $t_r$执行。那么，在 $[t_c, t_r]$ 期间，根据 $M$扣除的价值至多为 $\min\{b_u,\ \ell_{\text{win}}(\lceil (t_r - t_c)/\omega \rceil + 1)\}$，其中 $b_u$ 是在该时间段内 $u$ 中可用的总价值，每笔扣款支付的收款方均为 $\Pi_M$所允许的对象，且不会扣除其他账户的资金。

这一上限让所有者能够限制遭到入侵的代理所造成的风险敞口。设有支出策略的智能账户会对其资金执行相同的上限。AgentBank 在多个所有者的代理共享储备金时，也能做到这一点。

**储备要求**。资金池化之所以有帮助，是因为代理并非都需要同时使用资金。相关需求会限制这一优势：需求同时激增仍需要共同储备金。我们将在下文量化这两种效应。

命题 *2*（池化准备金）。设 $X_1, \ldots, X_N$ 是在补充周期内 $N$ 个代理的外部支付需求，且 $q_\alpha$ 为 $\alpha$ 分位数。*(i)* 若服务水平为 $\alpha$，单个代理的预先注资需要 $W_N = \sum_i q_\alpha(X_i)$；而池化准备金 $R_N = q_\alpha(\sum_i X_i)$ 以至少 $\alpha$ 的概率覆盖每个代理的需求。*(ii)* 若 $X_i$ 可交换，均值为 $m$、标准差为 $s$，两两相关系数为 $\varrho \geq 0$，且 $\sum_i X_i$ 近似服从高斯分布，则 $R_N / W_N \approx \big(m + z_\alpha s\sqrt{\varrho + (1-\varrho)/N}\big)/q_\alpha(X_1)$。*(iii)* 若给定共同因子 $Z$ 时，$X_i$ 条件独立同分布，$\mu(z) = \mathbb{E}[X_i \mid Z = z]$ 连续且严格递增，并且 $Z$ 的累积分布函数在 $q_\alpha(Z)$ 附近连续且严格递增，则当 $N \to \infty$ 时，$R_N/N \to \mu(q_\alpha(Z))$，因此 $R_N/W_N \to \mu(q_\alpha(Z))/q_\alpha(X_1)$。

第（ii）部分是库存池化平方根法则 [23]。第（iii）部分是巴塞尔内部评级公式 [30, 58] 背后的大投资组合极限：特异性需求会通过分散化消失，而共同成分必须按照其自身的 $\alpha$ 分位数进行储备。乘性共同因子会使总需求呈右偏的分布，因此高斯近似（ii）会低估所需储备。没有共同因子时，该比率趋于 $m/q_\alpha(X_1)$，对于突发性需求而言这一数值很小。对于有限的 $N$，对分位数进行二阶展开会加入信用投资组合模型中的粒度调整 [30, 31]：当 $\mu_N(z)$ 和 $v_N(z)$ 分别为给定 $Z = z$ 时 $\sum_i X_i$ 的均值和方差，且 $f_Z$ 为 $Z$ 的密度时，

$$
\begin{aligned}
R_N &\approx \mu_N(\zeta_\alpha) - \frac{1}{2 f_Z(\zeta_\alpha)} \, \frac{d}{dz}\Big[\frac{f_Z(z)\, v_N(z)}{\mu_N'(z)}\Big]_{z=\zeta_\alpha}, \\
\zeta_\alpha &= q_\alpha(Z).
\end{aligned}
\tag{7}
$$

其第二项不会随 $N$ 增长，并且要求有限条件方差。只有在接收者保留资金期间，内部化才能节省储备金。对于序列不相关收入以及每个周期的提款比例为 $\theta \in (0, 1]$，提款方差是收入方差的 $\theta/(2-\theta)$ 倍。

**赎回激励**。发生资产损失后，全额支付给早期赎回者会让等待者所得减少。损失一经确认，按比例偿付便会消除这一优势，但延迟估值仍为早期赎回留下了机会窗口。

**命题 3（顺序按面值赎回下的损失集中）**。设 $A$ 和 $L$ 分别表示初始真实资产和负债，且满足 $A < L$。假设总额仅因付款而变化，且策略召回无需成本。*(i)* 如果总价值为 $\pi L \leq A$ 的债务在处置前按面值结算，则可全额收回；而剩余债权可收回 $\gamma(\pi) = 1 - \frac{1 - A/L}{1 - \pi}$，该值随 $\pi$ 严格递减。*(ii)* 根据第 ***3.2*** 节的违约减值规则，在 $h_j = 1$ 且估值精确的情况下，无论赎回的顺序和时间如何，每笔债权均可收回 $A/L$。*(iii)* 如果银行在发生损失时满足资本充足率 $\geq 1$，而该损失

报告值仅反映稍后时点 $\tau$ 起的情况，则在 $\tau$ 之前进行的每笔结算均按面值支付，无论折价如何，因此 *(i)* 适用于在 $\tau$ 之前结算的债权。确认损失后，支付比率受当前真实比率 $A_t/L_t$ 的约束。

提前赎回的溢价（$1 - A/L$）/（$1 - \pi$）会随着赎回人数增加而上升，这正是银行挤兑背后的策略互补性 [21, 28]。在公共账本上，减值一经记录便成为共同知识，从而可以恢复多个均衡 [33], ；赎回请求在队列中的位置由交易排序决定，而区块构建者会出售这种排序权 [19]。**D 节**量化了由此产生的优先费竞赛。

根据命题3(iii)，折价无法在确认前关闭这一窗口：在覆盖率下限下，任何导致银行减值的损失都超过由权益支持的扣减缓冲。例如，借贷池份额价格只有在坏账被共同分担后才会反映出来。对于损失发生后提交的请求，当通知期超过确认滞后期时，远期定价会关闭这一窗口，因为下一净资产值定价消除了共同基金中的过时价格套利 [10, 64]。内部支付可以保持即时。所有外部付款都共享通知期，因此支付意图无法绕过该期限。

## 5 评估

我们探讨四个研究问题：

- **RQ1:** 受策略约束的委托会增加多少执行开销?
- **RQ2:** AgentBank 能节省多少闲置流动性？哪些机制对此有所贡献?

- **RQ3:** 在贷款资金池承压及国库券结算时间表的影响下，储备金政策如何平衡资金库收益与支付可用性?
- **RQ4:** 赎回规则和存款人速度如何影响减值损失?

### 5.1 方法论

**实现**。 我们使用 Solidity 0.8.34 实现了 BankCore、TreasuryManager 和一个 ERC-4626 策略适配器（基于 OpenZeppelin Contracts 5.4，共 466 行非注释代码），并遵循算法1中的违约规则。可选的赎回扩展通过模拟进行评估。Foundry 测试套件包含 38 项单元测试和模糊测试，其中一项针对命题1；此外，还通过 32,768 次随机调用检查了四项不变量（余额总和为 $D$，排队条目为 $O$， $R$ 等于持有的资产，且权益守恒）。Gas 数据取自 Anvil 在大阪规则下执行交易所得的回执。所有行均使用一种支持 EIP-3009 的六位小数代币，如 USDC，但不包含其代理合约和暂停检查。ERC-4337 基准使用 EntryPoint v0.7 和 SimpleAccount，其会话密钥通过与授权相同的策略进行绑定。

**工作负载**。除非另有说明，我们模拟 1,000 个代理，每位所有者 10 个。若 $\sqrt{\varrho}Z_t+\sqrt{1-\varrho}\,\varepsilon_{i,t}$ 超过某个阈值，则代理 $i$ 在第 $t$ 天处于活跃状态，其活跃概率为 $p_i$；该概率取自均值为 0.3、浓度参数为 5 的 Beta 分布。共同因子 $Z_t$ 的 AR(1) 持续性为 0.5，而 $\varrho$ 近似表示成对需求相关性。活跃代理发起的支付次数服从均值为 $\lambda_i e^{aZ_t-a^2/2}$ 的泊松分布，其中 $\lambda_i \sim 40\cdot$服从对数正态分布 LogNormal($-\frac{1}{2}$，1)。支付金额服从对数正态分布，中位数为 0.10 美元，对数尺度标准差为 1。每笔支付为内部支付的概率为 $\rho_{\text{in}} = 0.5$。接收者每天提取其余额的 $\theta = 0.2$，所有者则在一天后为账户补充资金。初始存款 $D_0$ 足以覆盖所有者 99% 的日常支付需求及接收者余额。

**借贷池轨迹**。国库将资金投资于以太坊上的 Aave v3 USDC市场。我们重放其从 2023 年 2 月 6 日至 2026年10月27日（1,360 天）的每日可用流动性和供应利率 [20], ，并按比例缩放银行，使其存款等于该市场可用流动性中位数的 10%；同时，我们限制银行每小时最多只能提取该市场的可用流动性。轨迹包含 KelpDAO 漏洞利用后发生的冻结：可用流动性从 2026年4月18日的 5.34 亿美元降至 4 月 19 日至 22 日的不足 25,000 美元，而供应利率则升至利率模型 12.6% 的上限。

**基准与指标**。我们将以下方案作为对照：(i) 普通钱包，持有结算资产但不赚取收益；(ii) 收益代币钱包，每个代理持有市场的生息代币，并在付款时赎回，但受可用流动性限制。我们报告 99% 日服务水平下的闲置流动性、正常运行期间的资产收益率（国库收入除以存款加权益），以及压力期间即时结算的付款价值占比和因超过 24 小时有效期仍未结算而失败的付款占比。每小时付款模拟采用先进先出结算，且不考虑资产损失，因此付款维持面值。运行实验将偿付能力条件赎回与其他方案进行比较。我们设定 $r_{\min} = 2\%$、$h_j = 0.98$、资本充足率$_{\min} = 1$和初始权益$E_0 = 0.02D_0$，每六小时再平衡一次，容差为 10%。结果取五个工作负载随机种子的平均值。

## 5.2 RQ1：委托开销

**表2**比较了 AgentBank、ERC-20、EIP-3009（x402）以及策略等价的 ERC-4337 转账在稳态下的 Gas 消耗。一次内部支付需要 61.4k Gas，其中 26.5k 用于在所有者的账本转账（34.8k）之上进行委托。这包括 EIP-712 哈希、签名恢复、四次授权读取、窗口和随机数更新，以及调用数据。针对 1,024 个收款目的地的证明会额外增加 8.3k。内部支付的成本低于 EIP-3009（后者会将每个随机数存储在新槽位中），并且仅为策略等价用户操作成本的 56%。批处理 $k = 50$ 可将成本降至 40.0k（为 ERC-20 转账的 1.17 倍）；相比之下，EIP-3009 为 46.6k，用户操作为 72.9k。

外部支付会增加 23.6k 的资产转移成本，以及 $\kappa_t$ 所需的策略估值成本 23.1k。批处理可将这项开销降至 11.1k。缓存的估值

**表2**。每笔支付的Gas消耗和单笔支付交易的calldata字节数。

| | 每笔支付的Gas消耗 | | | |
|---|---|---|---|---|
| **操作** | **单笔** | $k = 10$ | $k = 50$ | **字节** |
| **ERC-20** 代理钱包转移 | 34,313 | – | – | 68 |
| **EIP-3009**transferWithAuthorization（x402） | 65,222 | 48,524 | 46,587 | 292 |
| **ERC-4337** 会话密钥转账 | 109,771 | 75,840 | 72,929 | 900 |
| **AgentBank 内部支付** | 61,353 | 41,814 | 40,031 | 324 |
| 含目的地证明（1,024 个收款目的地） | 69,646 | – | – | 644 |
| **AgentBank 外部支付**，即时 | 108,095 | 55,797 | 51,111 | 324 |
| 不含策略估值（$J = 0$） | 84,955 | – | – | 324 |
| **AgentBank 外部支付**，排队 | 114,509 | 86,323 | – | 324 |
| **队列结算**，每条 | 77,921 | 22,719 | – | 36 |

只需一次存储读取，但在刷新前可支持按面值赎回（命题 3(iii)）。储备金不足时，排队支付的成本为 86–115k。

### 5.3 RQ2：流动性效率

**图 2**(a) 将代理数量从 1 变为 3,000，并将相关性设为$\varrho = 0$、0.05、0.1、0.2、0.3 和 0.5，以测量池化储备要求。在没有共同因子的情况下，该要求在 $N = 1,000$ 个代理时降至单个代理的预先注资的 22%，并趋近于极限 $m/q_\alpha(X_1) = 0.20$，与预测一致。在相关需求下，该要求更早达到平台期，且水平更高：对于 $\varrho = 0.05$，0.2 和 0.5，分别为单个代理的预先注资的 0.40、0.64 和 0.88。高斯近似低估了这些平台期，误差最高达 29%；而命题 2(iii) 的大池极限与模拟结果的误差在 1.5% 以内。对于有限资金池，**公式7** 使误差在 30 个同质代理或 100 个异质代理时降至 2% 以下。仅使用极限时，误差最高分别为 12% 和 8%（**表5**）。

**图 2**(b) 分解了异质代理带来的节省。让同一所有者的 10 个代理共用一个账户，便可将闲置流动性减少 23–46%。在所有所有者之间进行资金池化，可将其减少 32–76%；而内部化并留存收款方款项（$\theta = 0.2$）还能进一步降低 2–21 个百分点。因此，对于 $\varrho = 0$、0.1 和 0.3，AgentBank 所需的单个代理预先注资分别为 0.23、0.37 和 0.48，节省了 52–77%。与最强的基于钱包的替代方案——由同一所有者的代理共用一个智能账户——相比，节省幅度为 38–58%。与分层支付系统一样，[41],资金池化贡献了大部分节省。冲击相关性较高时，内部化的作用最大，因为留存余额能够平滑共同冲击。采用即时提现时（$\theta = 1$），它只能节省 1–9 个百分点。

采用 $\varrho = 0.1$ 时，将 $\rho_{\text{in}}$ 从 0 提高到 0.9，可使闲置流动性从单个代理的预先注资的 0.48 降至 0.31，并将每日代币转账量从约 12,200 笔降至 1,320 笔，因为内部支付无需转移任何资金，而 100 名接收者会提取汇总后的余额。接收者集中度使较高的 $\rho_{\text{in}}$ 成为可能：在 Base 上的 x402 中，最大的接收者获得 23% 的结算额，最大的三名接收者获得超过一半的结算额 [46]。在指数为 1 的齐夫定律下，对于 $10^4$ 名接收者，让最受欢迎的十名接收者接入系统可使 30% 的交易量实现内部化。接收者很少继续向外支付（互惠系数为 0.025 [46]），因此其提现率 $\theta$ 决定了内部化收益。重尾需求可将节省比例提高至 79–89%。

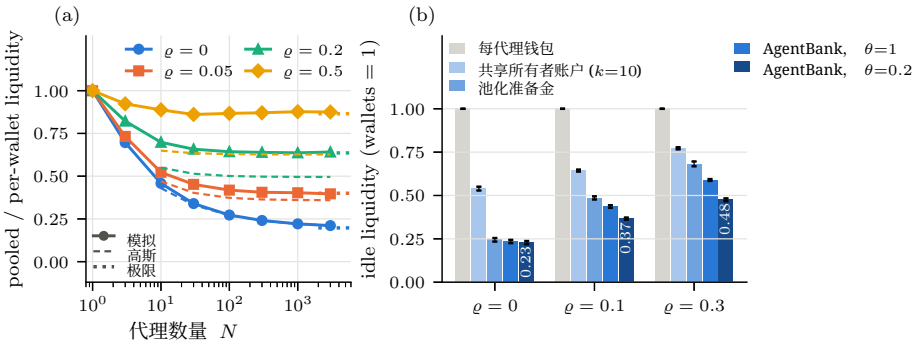


**图 2.** 流动性节省：**(a)** 准备金规模调整；**(b)** 资金池化与内部化。

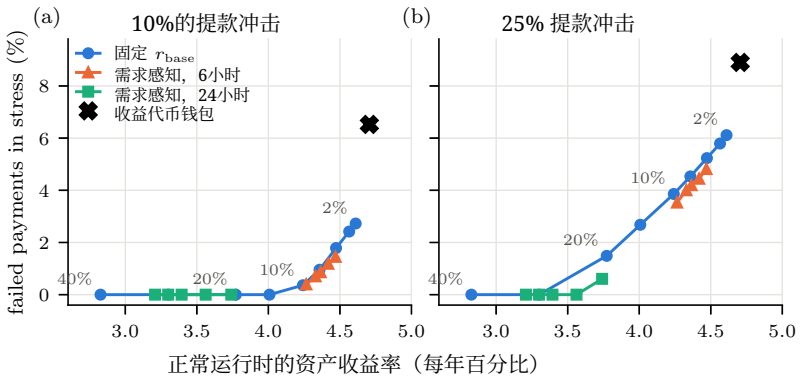


**图 3.** 在（**a**）10% 和（**b**）25% 提款冲击下的效率–韧性前沿。

### 5.4 RQ3：效率–韧性权衡

我们将 2–40% 的固定准备金比率与基于需求感知的策略进行比较，后者使用 0.5–0.99 的分位数、 $\Delta \in \{6, 24\}$ 小时的时间范围，以及 $W = 14$ 天的历史数据。在正常运行情况下，较低的准备金即可满足需求，因为国库每六小时可以召回流动性：在准备金率为 $r_{\text{base}} = 5\%$ 时，99.2% 的外部支付金额可即时结算，资产收益率为每年 4.47%，而平均供应利率为 4.71%。准备金率每额外提高 10 个百分点，收益率约降低 0.47 个百分点。

冻结改变了整体情况。我们评估了2026年4月18日至5月2日的情况：从4月18日中午起， $D_0$ 在24小时内陆续发生10%或25%的提款，所有者在5.5天内将追加资金减半，以反映避险行为（**图3**）。直接持有生息代币的代理可获得全部供应利率，但其支付金额中有6.5%（10%冲击）和8.9%（25%冲击）支付失败；即使没有冲击，在赎回受阻期间也有4.8%支付失败。AgentBank牺牲了部分收益率，以大幅减少故障：当 $r_{\text{base}} = 10\%$时，故障率降至0.4%和3.9%，收益率为4.24%。当 $r_{\text{base}} = 15\%$时，10%冲击下没有支付失败（收益率为4.01%），而 $r_{\text{base}} = 30\%$则可在

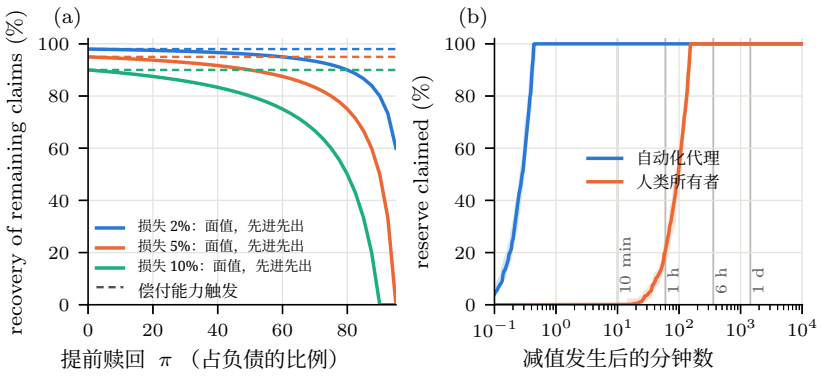


**图 4.** 赎回激励：**(a)** 剩余债权回收；**(b)** 储备金攫取。

25%冲击下消除故障（收益率为3.30%）。需求感知策略处于同一条前沿上。在24小时的时间范围内，它持有21–34%，几乎避免了所有故障，不过它只能看到AgentBank的资金流，无法预测外部冻结。

在冻结期间，收益代币钱包的故障在一天内影响的存款比例达到 18%，而 AgentBank 仍使用储备金和所有者的存款继续结算（**图 5**）：储备金将交易场所冻结转化为有界的排队延迟，其代价由运营方设定。

即使资金池的流动性被部分捕获、外部交易额翻倍、采用跨平台多元化策略，以及重现2022年6月的 Solend 冻结事件（**第 D 节**），这些结论依然成立。冻结事件屡次发生：自2022年以来，已有64个稳定币借贷池发生46次冻结，而2026年4月冻结波及七条区块链上的14个资金池。

**合规的国库资产**。GENIUS 法案允许将代币化美国国库券作为稳定币储备金，但禁止再抵押 [1], ，这就排除了借贷池。国库券基金不会冻结，但只能在营业日赎回，因此周末成为决定性压力情景（**图7**）：要即时结算99%的支付金额，固定储备金需从5%提高到20%；而要在一周中最不利的时点遭受10%冲击时，将故障率控制在0.05%以下，则需要30%的固定储备金（当日赎回）或40%的固定储备金（次日赎回），相应保留策略收益的72%或62%。因此，合规以日历风险换取交易场所风险。

### 5.5 RQ4：赎回规则与存款人速度

现在，我们从流动性冻结重放转向资产减值的存款人模型。**图 4**(a) 展示了命题 3(i)–(ii)。在资产损失为 5% 的情况下，如果存款人等待，且在他们之前已有一半负债按面值赎回，他们可收回 90%；如果已有 90% 的负债按面值赎回，则只能收回 50%。在数值精确、没有折价且没有清算成本的情况下，偿付能力条件赎回可让所有人获得 95%。

**图 4**(b) 说明了为什么赎回规则必须是机械执行的。鉴于反应延迟呈对数正态分布（自动化代理的中位数为一分钟，人类所有者为六小时），在减值公开后的 27 秒内，自动化存款人便会取出全部储备金

。人类所有者会在一小时内取出其中的 21%，并在 2.6 小时内取出全部储备金。因此，暂停提款等酌情响应往往要等到自动化挤兑完成后才会到来，而预先知晓的闸门会招致先发制人的赎回 [13, 43]。

在非均衡状态下，先进先出的面值结算会将损失留给人类所有者；或者，一旦自动化赎回请求超过资产，就会引发优先费竞赛，其成本甚至超过损失。若能及时确认损失并实现无成本清算，基于偿付能力条件的赎回便可消除挤兑，而基于周期的按比例结算则可消除同一周期内优先顺序的价值。

然而，如果 5% 的损失延迟一分钟才反映在报告值中，人类所有者只能收回 93.4%，而延迟 30 分钟后只能收回 90.2%；无论折价多少，结果都与先进先出相同。在损失信号私有且带有噪声的情况下，先进先出均衡是唯一的；在损失信号比面值挤兑会导致资不抵债的临界点提前约三个标准差时，挤兑便会开始。清算成本也会使不受偿付能力条件约束的赎回引发挤兑。流动性费用消除了这一模型中的均衡。

## 6 讨论

**经济设计**。 所有者池化降低了所有者必须存入的金额，而银行池化与内部化则减少了银行闲置持有的资金。后者的价值归于获得国库收益的一方；在所评估的方案中，运营方将其作为第一损失资本的补偿。将其中一部分转给存款人会提高采用率，但会收紧**图 3**所示的边界；更高的股本回报率也会增强减少储备金的动机 [27]。

**监管**。 AgentBank 接受存款并转换流动性，而这在大多数司法管辖区都受到监管：美国《GENIUS法案》要求持有类似现金的储备金，禁止对其进行再抵押，并禁止向持有人支付利息 [1], ；MiCA 禁止对电子货币代币支付利息 [24]。我们不对 AgentBank 余额究竟属于支付型稳定币、电子货币还是存款作出判断。无收益支付给持有人的国库券基金仍然可行，但除非通过全天候兑换设施 [15]衔接营业日，否则就需要更多储备金。另一种方案是由特许银行将 AgentBank 运营为代币化存款系统 [37] ，并提供可验证负债 [18, 34]。

**局限性**。 该原型未经审计，且测试使用了简化代币。工作负载为合成数据，因为实测 x402 活动主要由人为制造的结算构成 [46]。这些数据仅用于分析收款方集中度；我们的稳健性分析涵盖了更厚尾部 [7] ，但不涉及已部署代理的需求。流动性结果以比率表示，因此与支付金额无关。财资重放采用每日流动性。策略损失仅纳入挤兑模型；脱锚不在模型范围内；挤兑模型假设存款人为风险中性；减值模式之外的偿付不能力处置仍有待未来研究。

## 7 结论

我们提出 AgentBank，这是一种面向 AI代理支付的智能合约银行架构，将委托支出与汇集的支撑资产管理分离。该设计结合了所有者签发的授权、内部结算、受储备约束的财资分配，以及针对资产减值的明确赎回规则。我们界定了其支出界限和流动性要求，并通过 Solidity 原型和基于轨迹的评估，刻画资本效率与支付韧性之间的权衡。

# 参考文献

1. 美国第119届国会：《指导并确立美国稳定币国家创新法案》（GENIUS 法案）。公法119-27号，139 Stat. 419（2025年7月），https://
www.govinfo.gov/content/pkg/PLAW-119publ27/html/PLAW-119publ27.htm，于2025年7月18日颁布；参见§4(a)(1)、(a)(2)、(a)(11) 2. Ahmed, R., Aldasoro, I., Duley, C.：《公共信息与稳定币挤兑》。国际清算银行工作论文1164，国际清算银行（2024年），2025年1月修订 3. Anadu, K., Azar, P.D., Cipriani, M., Eisenbach, T.M., Huang, C., Landoni, M., La Spada, G., Macchiavelli, M., Malfroy-Camine, A., Wang, J.C.：《挤兑与避险转移：稳定币是否是新型货币市场基金？》工作人员报告1073，纽约联邦储备银行（2023 2024 4），修订于4月 . 国际清算银行：《未来货币体系蓝图：改进旧体系，赋能新体系》。载于：国际清算银行《2023年年度经济报告》，第3章（2023年）5. 国际清算银行：《下一代货币与金融体系》。载于：《2025年年度经济报告》，第III章（2025年6月），https://www.bis. org/publ/arpdf/ar2025e3.htm 6. 巴塞尔银行监管委员会：《巴塞尔协议III：流动性覆盖率与流动性风险监测工具》。技术报告BCBS 238，国际清算银行（国际清算银行（2013年1月）），https://www.bis.org/publ/bcbs238.htm 7. Bimpikis, K., Markakis, M.G.：《重尾需求下的库存合并》。《管理科学》**62**(6)（2016年）8. 国际清算银行创新中心：Agorá项目：用于批发跨境支付的共享可编程平台。项目报告，国际清算银行（2026年5月），
h
t
t
p
s://
www.bis.org/publications/project-agora-shared-programmable-platform-wholesale-cross-border-payments，由国际金融协会召集 9. Budish, E., Cramton, P., Shim, J.：《高频交易军备竞赛：频繁批量拍卖作为市场设计应对方案》。《经济学季刊》**130**(4)（2015年）10. Chalmers, J.M.R., Edelen, R.M., Kadlec, G.B.：《金融中介机构设定证券价格的风险：共同基金的万能选择权》。《金融学期刊》**56**(6)（2001年）11. Chen, Q., Goldstein, I., Jiang, W.：《收益互补性与金融脆弱性：来自共同基金资金流出的证据》。《金融经济学期刊》**97**(2)（2010年）12. Chiu, J., Ozdenoren, E., Yuan, K., Zhang, S.：《去中心化金融借贷的脆弱性》。工作人员工作论文2023-14，加拿大银行（2023年）13. Cipriani, M., Martin, A., McCabe, P.E., Parigi, B.M.：《赎回限制、费用与先发制人式挤兑》。金融与经济讨论系列2014-30，美联储理事会（2014年）14. Circle：《Circle Gateway驱动的纳支付现已在主网上线》。Circle博客（2026年4月），
https://circle.com/blog/nanopayments-powered-by-circle-gateway-is-now-live-on-mainnet 15. Circle Internet Financial：Circle宣布为BlackRock的BUIDL基金投资者提供用于转账的USDC智能合约。新闻稿（2024年4月），
h
t
t
p
s://
w
w
w.
c
i
r
cle.co
m/pressroom/circle-announces-usdc-smart-contract-for-transfers-by-blackrocks-buidl-fund-investors

16. Coinbase 开发者平台：CDP 智能体钱包（2026年），https://www.coinbase.com/developer-platform/products/agentic-wallets，产品与技术文档 17. Corbett, C.J., Rajaram, K.：《库存合并效应在非正态相关需求下的推广》。《制造与服务运营管理》**8(4)**（2006年）18. Dagher, G.G., Bünz, B., Bonneau, J., Clark, J., Boneh, D.：《Provisions：针对比特币交易所的隐私保护型偿付能力证明》。载于：ACM SIGSAC计算机与通信安全会议（CCS）（2015年）19. Daian, P., Goldfeder, S., Kell, T., Li, Y., Zhao, X., Bentov, I., Breidenbach, L., Juels, A.：《Flash Boys 2.0：去中心化交易所中的抢先交易、矿工可提取价值与共识不稳定性》。载于：IEEE安全与隐私研讨会（SP）（2020年）20. DefiLlama：DefiLlama收益率API：以太坊上Aave v3 USDC市场的每日历史数据（2026年），https://yields.llama.fi/chart/aa70268e-4b52-42bf-a116-608b370f9501，27 21 2023 02 06 2026 10 系列 - - 至 - - 。Diamond, D.W., Dybvig, P.H.：《银行挤兑、存款保险与流动性》。《政治经济学期刊》**91(3)**（1983年）22. Dziembowski, S., Eckey, L., Faust, S., Malinowski, D.：《Perun：基于加密货币的虚拟支付枢纽》。载于：IEEE安全与隐私研讨会（SP）（2019年）23. Eppen, G.D.：《注——集中化对多地点报童问题预期成本的影响》。《管理科学》**25(5)**（1979年）24. 欧洲议会和欧盟理事会：《2023年5月31日关于加密资产市场的《欧盟第2023/1114号条例》（MiCA）》。欧盟官方公报，L 150，2023年6月9日，第40–205页（2023年），https://eur-lex.europa.eu/eli/reg/202354 25111450 //oj，参见第和条。Garratt, R., Shin, H.S.：《稳定币与代币化存款：对货币统一性的影响》。国际清算银行公报73，国际清算银行（2023年）26. Gervais, A., Zhou, L.：《人工智能智能体智能合约漏洞利用生成》。载于：金融密码学与数据安全（FC）（2026 05558 27 2507），arXiv：. . Goel, T., Lewrick, U., Agarwal, I.：《如何让稳定币更稳定：监管能否有所助益？》国际清算银行工作论文1355，国际清算银行（2026年6月）28. Goldstein, I., Pauzner, A.：《活期存款合约与银行挤兑概率》。《金融学期刊》**60(3)**（2005年）29. Google 智能体商务：《智能体支付协议（AP2）规范》。协议规范，Google（2025年），https://ap2-protocol.org/ap2/specification/，版本0.2 30. Gordy, M.B.：《基于评级的银行资本规则的风险因子模型基础》。《金融中介期刊》**12(3)**（2003年）31. Gordy, M.B., Lütkebohmert, E.：《监管资本评估的粒度调整》。《国际中央银行期刊》**9(3)**（2013年）32. Gudgeon, L., Werner, S., Perez, D., Knottenbelt, W.J.：《可贷资金去中心化金融协议：利率、流动性与市场效率》。载于：ACM金融技术进展会议（AFT）（2020年）33. Hellwig, C.：《公共信息、私人信息与协调博弈均衡的多重性》。《经济理论期刊》**107(2)**（2002年）34. Ji, Y., Chalkias, K.：《广义负债证明》。载于：ACM SIGSAC计算机与通信安全会议（CCS）（2021年）35. Jin, D., Kacperczyk, M., Kahraman, B., Suntheim, F.：《摆动定价与开放式共同基金的脆弱性》。《金融研究评论》**35(1)**（2022年）

36. Johnson, K., McAndrews, J.J., Soramäki, K.：通过延迟结算机制节省流动性。纽约联邦储备银行《经济政策评论》**10**(3) (2004), https://www.newyorkfed.org/medialibrary/media/research/epr/04v 10n3/0412mcanpdf.pdf 37. J.P. Morgan Kinexys：J.P. Morgan Kinexys美元数字存款代币（JPMD）登陆Base。J.P. Morgan Payments新闻中心（2025年6月），https://www.jpmorgan.com/payments/newsroom/kinexys-usd-digital-deposit-tokens 38. Kahn, C.M., Roberds, W.：支付结算：私有与公共系统中的分层。《货币、信贷与银行杂志》**41**(5) (2009) 39. Kashyap, A.K., Rajan, R., Stein, J.C.：银行作为流动性提供者：对贷款与吸收存款并存现象的解释。《金融学期刊》**57**(1) (2002) 40. Khalil, R., Gervais, A.：Revive：链下支付网络的再平衡。载于：ACM SIGSAC计算机与通信安全会议（CCS）（2017）41. Lasaosa, A., Tudela, M.：大额支付分层结构的风险与效率提升：一种模拟方法。工作论文337，英格兰银行（2008）42. Lehar, A., Parlour, C.A.：去中心化市场中的系统性脆弱性。国际清算银行工作论文1062，国际清算银行（2022），https://www.bis.org/publ /work1062.pdf 43. Li, L., Li, Y., Macchiavelli, M., Zhou, X.：流动性限制、挤兑与中央银行干预：来自货币市场基金的证据。《金融研究评论》**34**(11) (2021) 44. Li, Y., Wang, L., Wang, K., Yang, Z., Wang, K., Guan, Z., Gao, J.：A402：将加密货币支付与代理式商业的服务执行绑定。arXiv预印本 arXiv:2603.01179（2026）45. Liao, G： [ARFC] 改善Aave v3以太坊核心上USDC的流动性缓冲：提高斜率2，降低最优利用率。Aave治理论坛（2026年4月），
h
t
t
p
s://
g
o
v
e
r
n
a
n
c
e.
a
ave.co
m/t/arfc-improve-liquidity-buffer-for-usdc-on-aave-v3-ethereum-core-raise-slope-2-lower-optimal-utilization/24684，发布于2026年4月22日；作者声明此为个人观点 46. Ling, S., Zhou, Y., Wu, L., Wang, C.：代理式商业的代理性究竟有多强？对x402采用情况及真实性的总体规模测量。arXiv预印本 arXiv:2607.12575（2026）47. Liu, J., Makarov, I., Schoar, A.：挤兑剖析：Terra Luna崩盘。工作论文31160，美国国家经济研究局（2023）48. Ma, Y., Zeng, Y., Zhang, A.L.：稳定币挤兑与套利中心化。NBER工作论文33882，美国国家经济研究局（2025年5月）49. MakerDAO：多抵押品Dai（MCD）的紧急关闭流程。Maker协议技术文档（2026），
h
t
t
ps://docs.
makerdao.com/smart-contract-modules/shutdown/the-emergency-shutdown-process-for-multi-collateral-dai-mcd，访问日期：2026年10月 50 - . Martin, A., McAndrews, J.：节省流动性机制的经济学分析。纽约联邦储备银行《经济政策评论》**14**(2) (2008) 51. Miller, A., Bentov, I., Bakshi, S., Kumaresan, R., McCorry, P.：Sprites与状态通道：比闪电网络更快的支付网络。载于：金融密码学与数据安全（FC）（2019）52. Patlan, A.S., Sheng, P., Hebbar, S.A., Mittal, P., Viswanath, P.：真实的人工智能代理，虚假的记忆：针对Web3代理的致命上下文操纵攻击。载于：金融密码学与数据安全（FC）（2026），arXiv:2503.16248

53. Reppel, E., Caspers, R., Leffew, K., Organ, D., Kim, D., Dalal, N.：x402：互联网原生支付开放标准。白皮书，Coinbase 开发者平台（2025年5月），https://www.x402.org/x402-whitepaper.pdf 54. Rochet, J.C., Vives, X.：协调失败与最后贷款人：Bagehot最终是对的吗？《欧洲经济协会杂志》**2**(6) (2004) 55. Sivaraman, V., Venkatakrishnan, S.B., Ruan, K., Negi, P., Yang, L., Mittal, R., Fanti, G., Alizadeh, M.：支付通道网络中的高吞吐量加密货币路由。载于：USENIX网络系统设计与实现研讨会（NSDI）（2020）56. Tcheyan, L.：KelpDAO/LayerZero漏洞利用导致2.9亿美元资金流失，去中心化金融市场被冻结。Galaxy Research（2026年4月），https://www.galaxy.com/insights/research/kelpdao-layerzero-exploit-defi，发布于2026年4月22日 57. 美国证券交易委员会：SEC通过货币市场基金改革及大型流动性基金顾问PF表格报告要求修正案。新闻稿2023-129（2023年7月），https://www.sec.gov/news/press-release/2023129 58-. Vasicek, O.：贷款组合价值的分布。《Risk》**15**(12) (2002) 59. Visa：可信代理协议。协议规范，Visa（2025），https://developer.visa.com/docs/trusted-agent-protocol/trusted-agent-protocol-specifications 60. Wang, Q., Yang, Y., Chen, Y., Ji, S., Payer, M.：HTTP 402遇上区块链：新兴x402支付的风险。载于：USENIX安全研讨会（USENIX Security）（2026 19545 61 2607），arXiv：. . Weinstein, J., Kaliski, S.：推出机器支付协议。Stripe博客（2026年3月），https://stripe.com/blog/machine-payments-protocol 62. Werner, S.M., Perez, D., Gudgeon, L., Klages-Mundt, A., Harz, D., Knottenbelt, W.J.：SoK：去中心化金融（DeFi）。载于：ACM金融技术进展会议（AFT）（2022）63. Zhang, Y., Xiang, Y., Lei, Y., Wang, Q., Qiu, T., Sun, Y., Zarkov, S., Yuen, T.H., Deppeler, A., Yu, J., Lam, K.Y.：SoK：区块链代理间支付。arXiv预印本 arXiv:2604.03733（2026）64. Zitzewitz, E.：谁关心股东？共同基金套利防护。《法律、经济学与组织杂志》**19**(2) (2003)

## 符号说明

**表 3.**符号说明。

| 符号 | 含义 | 符号 | 含义 |
|---|---|---|---|
| $\sigma$ | 结算资产 | $A_t^{\mathrm{eff}}$ | 有效资产 |
| $b_{u,t}$ | 账户余额 | $\mathrm{CR}_t$ | 覆盖率 |
| $D_t$，$O_t$ | 存款、排队义务 | $r_{\min}$，资本充足率$_{\min}$ | 储备下限，覆盖率下限 |
| $L_t$ | 负债总额 | $r_{\mathrm{base}}$ | 基准储备比率 |
| $R_t$ | 结算储备金 | $\alpha$ | 服务水平分位数 |
| $T_{j,t}$ | 策略头寸 | $W$ | 回看时长（天） |
| $A_t$，$E_t$ | 资产、权益 | $\Delta$ | 规划时域（小时） |
| $M$，$\Pi$ | 授权、策略 | $\mathrm{id}(M)$ | 授权标识符 |
| $I_p$，$\tau_p$ | 意图、到期时间 | $\rho_{\mathrm{in}}$ | 内部支付比例 |
| $\ell_{\mathrm{tx}}$ | 单笔支付限额 | $\varrho$ | 需求相关性 |
| $\ell_{\mathrm{win}}$，$\omega$ | 窗口许可额度，持续时间 | $\theta$ | 收款方提取比例 |
| $h_j$ | 估值因子 | $\kappa_t$ | 减值回收率 |

## B 算法

算法1总结了支付执行。除**表2**外，一笔所有者账本转账耗费 34,809 Gas。存款和提款分别耗费 58,430 和 82,294 Gas。授权注册和撤销分别耗费 118,209 和 28,256 Gas。国库部署和召回分别耗费 112,894 和 86,079 Gas。

**算法1** BankCore 支付执行与队列处理

**输入：** 资产 $\sigma$、意图 $I_p = (\mathrm{id}(M)\ q,\ d,\ x,\ n_p,\ \tau)$ 和签名。每次意图调用或队列处理调用都会为 $L > 0$ 设置 $\kappa = \min\{1, A^{\mathrm{eff}}/L\}$，然后才更改负债。转账会减少 $R$。此处省略状态索引。

**验证意图**

$M = (\sigma,\ o,\ u,\ a,\ \Pi,\ n) \leftarrow$ 所有者已注册的授权，ID 为 $(M)$
$s_p \leftarrow u$； $t \leftarrow$ 区块时间戳
**要求** $M$ 未被撤销；签名恢复为 $a$； $n_p$ 在 ID $(M)$ 下未使用
**要求** $t \le \tau$ 和 $t$ 均在 $\Pi$的有效期内
**要求** $(q,\ d)$ 在 $\Pi$ 下可接受；如果 $q =$ 是 int，则 $d$ 是 $\sigma$ 的账户
如果窗口已推进，则重置窗口使用量
**要求** $x \le \ell_{\mathrm{tx}}$，已使用 $+ x \le \ell_{\mathrm{win}}$，以及 $b_u \ge x$
标记 $n_p$ 在 id$(M)$ 下已使用；已使用 $\leftarrow$ 已使用 $+ x$； $b_u \leftarrow b_u - x$

**结算已接受意图**

**如果** $q =$意图 **则**
  $b_d \leftarrow b_d + x$
**否则**
  $D \leftarrow D - x$
  **如果** $R \ge O + x$ **则**
    转移 $\kappa x$ 的 $\sigma$ 至 $d$
  **else**
    $O \leftarrow O + x$
    $e \leftarrow (u, d, x, \tau)$
    将 $e$追加到队列
  **结束 if**
**结束 if**

**ProcessQueue**（$k$）（任意调用方）

**对于**最多 $k$ 个排队条目 **执行**
  $(u,\ d,\ x,\ \tau) \leftarrow$ 队列头
  **如果** $t > \tau$ **则**
    弹出队首； $O \leftarrow O - x$
    $b_u \leftarrow b_u + x$； $D \leftarrow D + x$
  **否则如果** $R \ge \kappa x$ **则**
    弹出头部； $O \leftarrow O - x$
    转移 $\kappa x$ 的 $\sigma$ 至 $d$
  **else**
    **中断**
  **结束 if**
**结束 for**

## C 证明

证明（引理*1*）。通过检查**表4**可知：在每一行中，$\Delta A = \Delta R + \Delta T$和 $\Delta L = \Delta D + \Delta O$，且其差值等于 $\Delta E$ 列中的条目。以回收率 $\kappa$ 结算名义债权 $x$ 会得到 $\Delta A = -\kappa x$、 $\Delta L = -x$以及$\Delta E = (1 - \kappa)\, x$。该减记在面值时消失。剩余的权益变动来自资本出资和国库损益。内部支付使两个余额分别变动 $\mp x$，因此 $D$ 及所有其他量均保持不变。□

**表4**。AgentBank 操作的资产负债表效应。

| 操作 | $\Delta D$ | $\Delta O$ | $\Delta L$ | $\Delta R$ | $\Delta T$ | $\Delta A$ | $\Delta E$ |
|---|---|---|---|---|---|---|---|
| **存款** | $+x$ | 0 | $+x$ | $+x$ | 0 | $+x$ | 0 |
| **资本出资** | 0 | 0 | 0 | $+x$ | 0 | $+x$ | $+x$ |
| **内部支付** | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| **外部支付，即时** | $-x$ | 0 | $-x$ | $-\kappa x$ | 0 | $-\kappa x$ | $(1-\kappa)x$ |
| **外部支付，排队** | $-x$ | $+x$ | 0 | 0 | 0 | 0 | 0 |
| **队列结算** | 0 | $-x$ | $-x$ | $-\kappa x$ | 0 | $-\kappa x$ | $(1-\kappa)x$ |
| **队列取消** | $+x$ | $-x$ | 0 | 0 | 0 | 0 | 0 |
| **资金部署/收回** | 0 | 0 | 0 | $\mp x$ | $\pm x$ | 0 | 0 |
| **国库收益/损失** | 0 | 0 | 0 | 0 | $\pm y$ | $\pm y$ | $\pm y$ |

$x$：名义操作价值。 $y$：国库收益或损失。 $T=\sum_j T_{j\circ}$ $\kappa$：结算前的回收率。 $\kappa=1$ 按面值。折价支付会核销负债的（$1-\kappa$）$x$，从而增加账面权益。

证明（命题*1*）。每个已接受意图都从由 id$(M)$ 标识的已注册授权中获取其付款方 $s_p=u$，并从该账户中扣款（算法1，第8行），因此不会从其他账户扣款；同时，可接受性检查将收款目的地限制为 $\Pi_M$。额度在接受时即被消耗，且不会恢复，因此每个窗口内的已接受价值最多为 $\ell_{\text{win}}$。长度为$t_r-t_c$ 的区间至多与 $\lceil (t_r-t_c)/\omega \rceil+1$ 个窗口相交。支付随机数在 id$(M)$ 内被消耗，而该授权无法重复注册；EIP-712 域则绑定了链和 BankCore 部署。因此，一个意图不可能被接受两次，也不可能在另一部署下被接受。最后，扣款金额绝不会超过 $u$的余额。□

证明（命题 *2*）。(i) 若 $\sum_i X_i \le R_N$，则时间范围内的每笔外部支付都满足 **方程 6**，因此在该事件中每个代理都能获得全额支付，而该事件发生的概率至少为 $\alpha$。(ii) $\mathrm{Var}(\sum_i X_i)=Ns^2(1+(N-1)\varrho)$，且高斯分位数为 $Nm+z_\alpha\sqrt{\mathrm{Var}(\sum_i X_i)}$。除以 $N$ 即得该表达式。(iii) 在给定 $Z$ 的条件下，强大数定律给出 $\frac{1}{N}\sum_i X_i \to \mu(Z)$ 几乎必然成立，因此也依分布收敛。关于 $\mu$ 的假设以及 $Z$ 的累积分布函数，使极限累积分布函数在 $q_\alpha(\mu(Z))=\mu(q_\alpha(Z))$ 附近连续且严格递增。因此，$\frac{1}{N}\sum_i X_i$ 的分位数收敛至该值 [30]。□

粒度调整。令 $\sum_i X_i=\mu_N(Z)+\varepsilon$ 为 $\mathbb{E}[\varepsilon \mid Z]=0$，且 $\mathrm{Var}(\varepsilon \mid Z)=v_N(Z)$。对 $\alpha$-分位数关于特质项进行二阶展开，得到 $q_\alpha(\sum_i X_i)\approx y_\alpha-\frac{1}{2g(y_\alpha)}\frac{d}{dy}[g(y)w(y)]_{y=y_\alpha}$，其中 $g$ 是 $\mu_N(Z)$的密度，$y_\alpha$是其 $\alpha$-分位数，而 $w(\mu_N(z))=v_N(z)$ [30,31]。由于 $\mu_N$递增，$y_\alpha=\mu_N(\zeta_\alpha)$，$g(\mu_N(z))=f_Z(z)/\mu_N'(z)$，且 $dy=\mu_N'(z)\,dz$，由此得到公式7。在我们的工作负载中，给定 $Z=z$，代理 $i$ 以概率$p_i(z)=\Phi\big((\sqrt{\varrho}z-c_i)/\sqrt{1-\varrho}\big)$ 处于活动状态，其活动阈值为 $c_i$；随后，它发起泊松分布的支付次数，其均值为 $\Lambda_i(z)B_i$，其中 $\Lambda_i(z)=\lambda_i e^{az-a^2/2}$，$B_i$ 是均值为 1 的突发乘数（$B_i=1$ 表示无突发），且支付规模为 $S$。因此，$\mu_N(z)=\sum_i p_i\Lambda_i\mathbb{E}[S]$且 $v_N(z)=\sum_i\big[p_i(\Lambda_i\mathbb{E}[S^2]+\Lambda_i^2\mathbb{E}[S]^2\mathbb{E}[B_i^2])-(p_i\Lambda_i\mathbb{E}[S])^2\big]$，仅当 $\mathbb{E}[B_i^2]<\infty$（Lomax 尾指数大于 2）时才有限。

证明（留存）。如果接收者每个周期提取其余额的 $\theta$，则接收者余额满足 $M_{t+1}=(1-\theta)M_t+I_t$，因此提款为

$W_t = \theta M_t = \theta \sum_{k\ge 0}(1-\theta)^k I_{t-1-k}$。对于序列不相关收入，

$$\mathrm{Var}(W_t) = \theta^2 \mathrm{Var}(I) \sum_{k\ge 0}(1-\theta)^{2k} = \frac{\theta^2}{1-(1-\theta)^2}\mathrm{Var}(I) = \frac{\theta}{2-\theta}\mathrm{Var}(I). \qquad \square$$

证明（命题 3）。（i）对 $\pi L$ 按面值结算后，负债 $A - \pi L \ge 0$ 对应的资产变为 $1-\pi$（$L$），从而得到 $\gamma(\pi)$。其关于 $\pi$ 的导数为 $-(1-A/L)/(1-\pi)^2 < 0$。（ii）在 $h_j = 1$ 且采用精确估值的减值模式下，$\kappa = A/L$，结算一项债权 $x$ 后变为 $(A-\kappa x)/(L-x) = \kappa$，因此该比率以及此后每一次支付的支付比率均保持不变。（iii）在 $\tau$之前，报告头寸保持损失发生前的数值，因此报告的有效资产 $\hat{A}^{\mathrm{eff}}$ 在损失发生时满足 $\hat{A}^{\mathrm{eff}} \ge L$。对 $x$ 按面值结算会使 $\hat{A}^{\mathrm{eff}}$ 和 $L$ 降低 $x$；从策略 $j$ 中召回$z$ 则会使 $\hat{A}^{\mathrm{eff}}$ 增加 $(1-h_j)\,z \ge 0$，因此在 $\tau$之前，无论 $h_j$如何，$\hat{A}^{\mathrm{eff}} - L \ge 0$ 和 $\kappa = 1$。所以，在 $\tau$ 之前结算的债权均按面值支付，如（i）所述。从 $\tau$起，估值是精确的，因此 $\hat{A}^{\mathrm{eff}}_t = R_t + \sum_j h_j T_j$、$_t \le A_t$ 和 $\kappa_t \le A_t/L_t$。结算债权 $x < L_t$ 后得到 $(A_t - \kappa_t x)/(L_t - x) \ge A_t/L_t$。因此，在上述假设下，当前真实资产覆盖率不会降低。最后，采用精确估值的资本充足率 $\ge 1$意味着 $E \ge \sum_j (1-h_j)\,T_j$，所以扣减缓冲内的损失会留下 $A \ge L$：任何导致银行减值的损失都超过该缓冲。□

## D 其他结果与稳健性

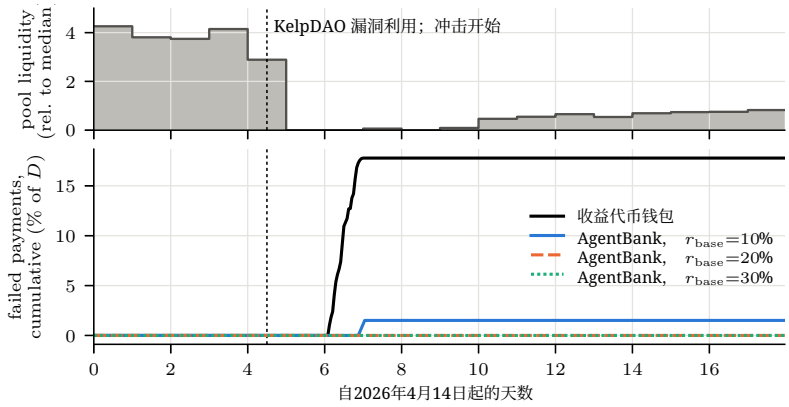


**图 5.** 2026年4月冻结：流动性（上）；累计支付失败（下）。

我们测试储备金估算、流动性压力和赎回激励。除非下文另有说明，设置均与主要评估一致。故障指的是发生 10% 提款冲击时的 2026年4月冻结。结果取五个工作负载随机种子的平均值；对于运行实验，则取 20 个总体的平均值。

**重尾需求。** 每日支付强度乘以相互独立、均值为 1 的 Lomax因子，其尾指数分别为 3、2 或 1.5。我们还将高斯共同因子创新替换为自由度为 5 或 3 的 Student-$t$创新

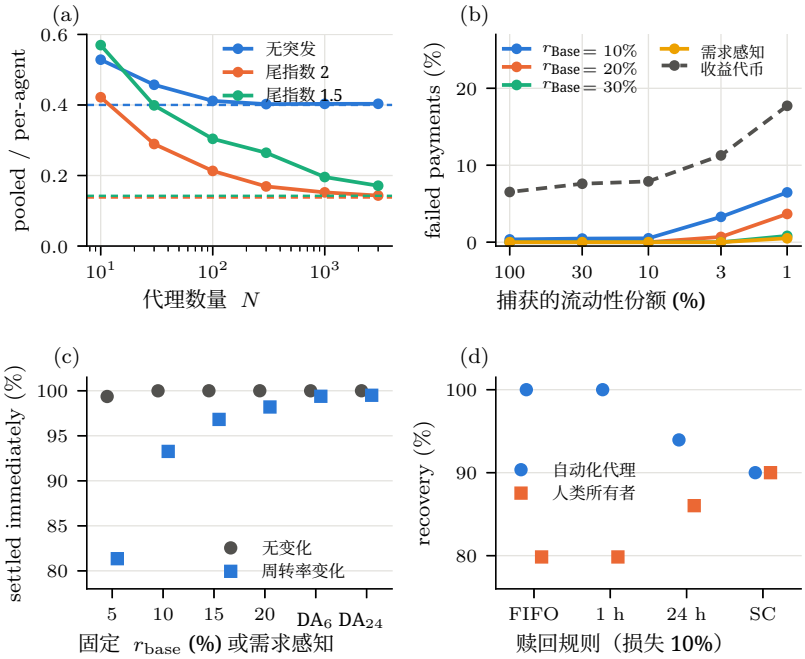


**图6**。 稳健性：（**a**）突发；（**b**）流动性捕获；（**c**）周转率；（**d**）赎回。

。在 $N = 1{,}000$ 时，以该因子自身的分位数评估的大池极限与模拟结果相差 0.6–5.5%，而高斯近似的误差为 $-25\%$ 至 $+15\%$。突发会使单个代理的预先注资从日均需求的 5.2 倍提高到约 15 倍，并使资金池化节省从 52–77% 提高到 79–89%。收敛速度较慢：当尾指数为 1.5 时，在 $N = 1{,}000$ 和 $N = 3{,}000$ 处，该极限分别低估储备金 27% 和 17%（**图6**(a)）。

**有限资金池储备规则**。**表5** 比较了大池极限与**公式7**中的粒度调整。在 $N = 100$，该调整将异质代理的误差从3–8%降至低于2%，并将尾指数为3的突发需求的误差从21%降至0.2%。在 $N = 10$ 附近，该调整会过度修正，并且需要有限条件方差。对于尾指数小于或等于2的情况，需求感知策略必须使用经验分位数。在部署中，条件矩将根据银行资金流和全市场活动指数进行估计。

**资金池流动性的部分捕获**。 基线允许访问所有可用的资金池流动性。模拟银行的按比例份额约占供给的1%。将捕获比例从100%降至1%后，在 $r_{\text{base}} = 15\%$ 时故障率从0升至5.1%，在30%时升至0.8%；而40%仍可避免故障（**图6**（b））。收益代币钱包的故障率为17.7%。24小时需求感知策略持有约三分之一的存款，故障率为0.5%。正常运营收益率保持不变。

**周转率变化**。 2025年1月1日，我们将内部份额从0.5降至0.2，并将 $\theta$ 从0.2提高至1，同时保持所有者的预先注资不变。存款下降

**表5.** 相对于模拟的99%分位数的准备金估计误差（%）。

| | 同质 | | | | 异质 | | | | 突发 | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | $\varrho = 0.05$ | | $\varrho = 0.2$ | | $\varrho = 0.05$ | | $\varrho = 0.3$ | | 尾部3 | | 尾部2.5 | |
| $N$ | 极限 | 粒度调整规则 | 极限 | GA | 极限 | 粒度调整规则 | 极限 | GA | 极限 | GA | 极限 | GA |
| 10 | −23.4 | 9.4 | −8.9 | 1.8 | – | – | – | – | −60.5 | 40.9 | **−64.3** | **78.1** |
| 30 | −11.5 | 1.1 | −3.3 | 0.4 | −18.4 | 5.7 | −4.1 | 0.8 | −41.7 | 8.3 | −47.3 | 23.0 |
| 100 | −4.4 | −0.3 | −1.1 | 0.1 | −7.7 | −0.3 | −3.0 | −1.6 | **−20.6** | **−0.2** | −25.3 | 4.6 |
| 300 | −1.4 | 0.0 | −0.5 | −0.1 | −3.5 | −0.5 | −1.1 | −0.6 | −8.7 | −0.8 | −12.2 | −0.5 |
| 1,000 | −0.7 | −0.3 | −0.1 | 0.0 | −1.3 | −0.1 | 0.3 | 0.5 | −3.1 | −0.7 | −3.9 | −0.1 |

极限：大池极限。GA：粒度调整规则。粗体配对显示了在 $N = 100$ （尾部3）时的改进，以及在 $N = 10$ （尾部2.5）时的超调。绝对误差越小越好。

至其初始水平的42%，外部周转率大约翻了一番。随后，固定储备金比例为5%、10%和15%时，即时结算率分别达到81%、93%和97%（**图6**(c)）。在 $r_{\text{base}} = 10$%时，冻结失败率从0.6%升至1.4%。6小时需求感知策略将储备金比例从10%提高至27%，并维持99.4%的即时结算率，收益率为2.7%，而固定10%策略的收益率为3.4%。24小时期限的储备金比例维持在75%，收益率为1.0%。自适应储备金能跟上更快的资金流出，但收益率较低。

**跨平台多元化**。 我们将资产等额分配到以太坊和 Base 上的 Aave v3、以太坊上的 Aave 和 Compound v3，或三者全部。在2024年3月10日至2026年10月27日期间，即使保留5%的储备金，每种分配方式在两种冲击下都能避免故障，收益率为4.27%–4.36%；相比之下，Aave 单独配置10%储备金时的收益率为4.30%。Base 曾冻结一天，而 Compound 未发生冻结。这些平台上的收益代币钱包也避免了故障。在此次事件中，多元化可以替代储备金，但相关性冻结和较小平台的流动性限制了这种保护作用。

**挤兑均衡**。**图6**(d)使用5,000名存款人，其余额服从对数正态分布（对数尺度标准差为1.5），其中一半为自动化存款人，另一半为人工存款人。对数正态反应延迟的对数尺度标准差为1，中位数分别为一分钟和六小时。发生损失 $\ell$后，当预期支付额减去1美元交易成本高于等待所能获得的回收率时，存款人会进行赎回。从“无人赎回”开始迭代最佳响应，可找到最小均衡。在 $\ell = 10$%的先进先出面值结算下，自动化代理的回收率为100%，人工存款人的回收率为79.8%，且20%的人工存款人损失超过其余额的一半。一个小时的结算周期不会带来任何变化，因为代理会填满第一个结算周期。24小时的结算周期将人工存款人的回收率提高至86.0%。偿付能力条件赎回不会发生挤兑，回收率为90%。将成本提高至20美元，回收率至多变化约一个百分点。在80%的存款人为自动化存款人且 $\ell = 5$%的情况下，人工存款人的先进先出回收率为75%。

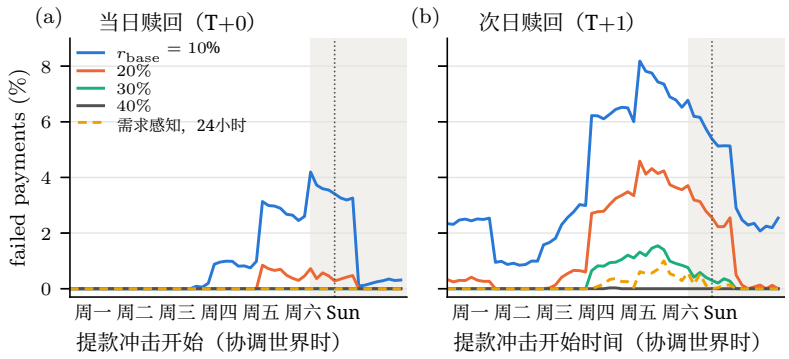


**图 7.** 国库券结算风险：（**a**）当日赎回和（**b**）次日赎回。

**国库券基金**。我们以符合GENIUS 法案 [1]储备金规则的代币化国库券基金替代借贷池。该基金没有流动性限制。T+0 在协调世界时18:00之前提出的请求，于该营业日21:00结算，之后的请求顺延。T+1提出的请求于下一个营业日结算。周末和美国联邦假日不计入。 在途资产累积收益率，并计入覆盖率。我们报告策略收益留存，其数值与假定的恒定收益率无关。即时赎回（全天候兑换设施所提供的服务） [15], 与无限流动性的Aave相匹配，不会发生故障。

在储备金为10%时，即时结算率从即时赎回时的99.99%降至93.0%（T+0）和85.1%（T+1）。最不利的冲击开始时间为周四晚间至周六清晨（**图7**）。周六中午冲击在储备金为10%时导致3.4%和5.4%的故障。将储备金提高至30%（T+0）或40%（T+1）后，在所有测试的开始时间下，10%冲击导致的故障率均保持在0.03%或以下，但25%的冲击仍会导致最高达2.4%和1.9%的故障（**表6**）。24小时需求感知策略可在T+0下控制住10%的冲击。72小时时间范围可避免所有故障，但为弥补结算缺口，需要持有约80%的存款。

**表 6.** 国库券基金表现（%）。

| | 已结算 立即 | | 保留的收益率 | | 故障 10%冲击 | | 故障 25%冲击 | |
|---|---|---|---|---|---|---|---|---|
| **准备金政策** | T+0 | T+1 | T+0 | T+1 | T+0 | T+1 | T+0 | T+1 |
| **固定 10%** | 93.00 | 85.13 | 92.6 | 94.1 | 4.20 | 8.18 | 8.45 | 11.33 |
| **固定 20%** | 99.80 | 99.32 | 82.3 | 83.7 | 0.84 | 4.59 | 5.08 | 7.82 |
| **固定 30%** | 100.00 | 99.99 | 72.0 | 73.1 | 0 | 1.54 | 2.42 | 4.52 |
| **固定 40%** | 100.00 | 100.00 | 61.5 | 62.5 | 0 | 0.03 | 0.30 | 1.87 |
| **需求感知，24 h** | 99.98 | 99.95 | 70.9 | 72.5 | 0 | 1.00 | 2.20 | 4.22 |
| **需求感知，72 h** | 100.00 | 100.00 | 20.8 | 22.3 | 0 | 0 | 0 | 0 |

结算和保留收益：正常运行。故障：不同冲击开始时间下的最坏情况。

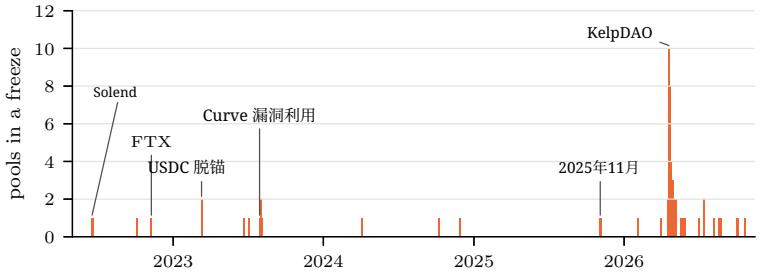


**图8.** 稳定币借贷池冻结。

**进一步冻结**。我们考察了64个DefiLlama稳定币池，这些资金池的报告价值等于可用流动性，且2026年10月的供给超过1,000万美元：涉及17条区块链、18个协议，以及自2022年5月以来的45,469个池日。冻结的定义是：流动性低于其过去30日中位数的5%（至少为500万美元），且供应利率至少为其中位数的1.5倍。**图8**显示了27个资金池中的46次冻结事件，平均每个资金池约每两年发生一次。其中21次持续超过一天。2026年4月影响了七条区块链上的14个资金池，单日最多影响10个，限制了单一协议内的多元化。该样本仅包含仍存续的资金池。

按照 RQ3 的设定，我们重演 2022年6月的 Solend 危机和 2023年7月30日的 Curve 漏洞利用：从每次冻结前一天中午开始施加冲击，并将规模调整为冻结前的资金池规模（**表7**）。Solend 的 USDC 流动性在三日冻结期间从 1.19 亿美元降至 1.2 万美元。在完全捕获的情况下，两种设计均不会发生故障。在 10% 或 1% 的捕获率下，收益代币钱包的故障率分别为 7.4% 和 16.7%；而 AgentBank 在储备金率为 20% 或 40% 时均可避免故障。一次为期一日的与 Curve 相关的 Aave 冻结，在 10% 冲击下不会导致故障。在 1% 捕获率下的 25% 冲击中，AgentBank 储备金率低于 10% 时，故障率最高达到 1.8%；而收益代币钱包可以避免故障，因为赎回每六小时发生一次。

**表7.** 10%提款冲击下的支付故障率（%）。

| 冻结 | 捕获 | 收益率代币钱包 | AgentBank，$r_{\text{base}}$ 10% | 20% | 30% | 40% | 已知，24 小时 |
|---|---|---|---|---|---|---|---|
| **KelpDAO 2026年**，Aave（5 天） | 100% | 7.76 | 0.51 | 0 | 0 | 0 | 0 |
| | 10% | 12.83 | 4.56 | 1.68 | 0 | 0 | 0 |
| | 1% | 28.24 | 8.05 | 5.34 | 2.45 | 0.06 | 1.80 |
| **Solend 2022年**，Solana（3 天） | 100% | 0 | 0 | 0 | 0 | 0 | 0 |
| | 10% | 7.38 | 1.24 | 0 | 0 | 0 | 0 |
| | 1% | 16.72 | 4.66 | 1.99 | 0.10 | 0 | 0.28 |
| **Curve 2023 年漏洞事件**，Aave（1 天）1–100% | | 0 | 0 | 0 | 0 | 0 | 0 |

Aave：以太坊上的 USDC。Solana：Solend USDC。捕获：可用资金池流动性的份额。

**优先费竞赛。** 当自动化代理在同一区块内作出反应时，优先费取代反应延迟，决定交易顺序 [19]。我们对挤兑研究中的存款人（平均余额为 2,000 美元）进行完全信息的一价拍卖建模。最大的未获服务余额决定每一位获得完整服务的自动化存款人所支付的价格。当自动化赎回请求超过资产时，竞赛便会开始，例如在自动化余额占比达到 95% 和 $\ell = 5\%$ 时。所有余额均实现自动化时，在损失率为 2%、5% 和 10% 的情况下，价格分别为 284 美元、526 美元和 900 美元。费用分别消耗存款的 10.1%、14.7% 和 18.6%，即损失的 1.9 至 5.0 倍，使总体回收率从 90–98% 降至 71–88%。余额最高的十分位组在扣除费用后可回收 92–98%，而 46–75% 的自动化存款人会损失超过一半的余额。完全信息意味着这些费用构成上限。一个覆盖自动化反应窗口的纪元会消除排序价值，并恢复 $A/L$ 回收率。偿付能力条件赎回同样可以消除这场竞赛。

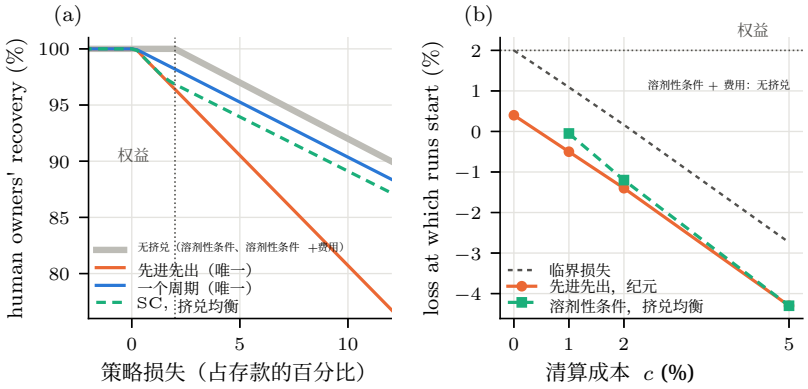


**图 9。** 含噪信号下的挤兑：**(a)** 人类所有者回收率；**(b)** 挤兑阈值。

**含噪信号。** 损失的共同知识允许存在多个挤兑均衡 [21]。遵循全球博弈模型 [28, 54],，存款人转而观测 $x = \ell + \eta\varepsilon$，其中 $\varepsilon$ 服从标准正态分布，并采用无信息先验。他们会在扣除 0.05% 余额成本后的预期支付超过等待所能获得的回收率时赎回。资本充足率为 $e = 2\%$，储备金为 $r = 10\%$，且一半的余额为自动化余额并优先得到服务。超出储备金的付款会以折价变现资产 $c$，从而形成策略互补性 [11]。我们分别从“无人赎回”和“人人赎回”开始迭代最佳响应。相交的极限确定了唯一的阈值均衡。

**图 9** 使用 $\eta = 0.5\%$。噪声为 0.25–2%、清算折价最高达 5% 时，也会出现相同的模式。先进先出迭代结果在网格分辨率范围内一致，挤兑开始时的信号比资不抵债阈值低 3.0–3.3 个标准差$e$–$(1-r)c/(1-c)$。在 $c = 2\%$ 时，该阈值接近零。3% 的损失使人工回收率降至 94.4%，而非 99%。一个周期不会改变阈值，但会使人工损失减半。如果清算没有成本，偿付能力条件赎回存在唯一的无挤兑均衡。对于 $c > 0$，早期赎回者可以规避由后续债权承担的成本，因此即使没有损失，也可能发生挤兑。对于所有经过测试的 $c$ 和 $\eta$，流动性费用都能消除挤兑。

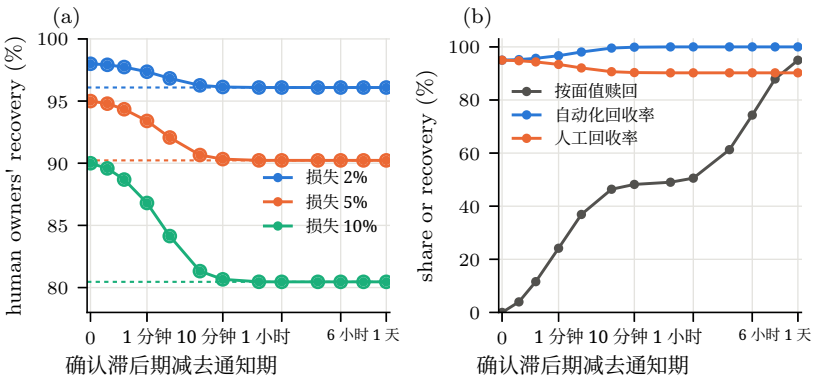


**图10.** 确认滞后期：（**a**）人工回收；（**b**）按面值赎回和回收率。

**确认滞后期**。我们按照 RQ4 中的反应延迟，推迟报告链下已知减值后的损失。所有资产均具有流动性。储备金为 10%，折价系数为 0.98、0.95 和 0.90 时，所需权益分别为存款的 2%、4.7% 和 10%。正如命题3(iii)所预测的，早期结算仍按面值进行。对于 5% 的损失，滞后一分钟会使人工回收率从 95.0% 降至 93.4%（**图10**）。滞后 30 分钟时，所有自动化代理都已按面值赎回，人工回收率降至 90.2%，与先进先出机制相符。滞后时间更长时，人工也会按面值赎回，六小时后提款达到余额的 74%。不同折价系数下的结果完全相同。远期定价会将每笔结算都推迟通知期的时长，从而缩短有效确认滞后。通知期长于滞后时间时，可恢复偿付能力或有结算。