

03 产品设计方案

主题：尝试协议设计与 Tokenomics 架构

一、任务目标 (Objective)

- 学员在已有研究基础上，尝试模拟协议 + Tokenomics 架构设计。
 - 通过课堂分组讨论与设计，理解：
 1. 如何定义问题与目标用户；
 2. 如何构建协议的功能逻辑；
 3. 如何设计代币经济模型，让代币有真实价值捕获；
 4. 如何识别并规避风险。
 - 最终目标：让学员不仅能研究项目，还能思考如果自己是创始人，会如何设计。
-

二、小组流程设计 (Process)

阶段 1：明确问题与目标

- 先回答：我们的协议解决什么痛点？目标用户是谁？
- 示例痛点：DEX 流动性不足、借贷抵押率过高、DAO 治理低效、链上保险覆盖不足。

阶段 2：设计协议逻辑

- 定义协议类型（DEX / 借贷 / 衍生品 / Restaking / 钱包 / RWA / 保险 …）。
- 拆解模块（如资金池、抵押模块、清算模块、保险赔付模块）。
- 用流程图展示用户如何与协议交互。

阶段 3：设计 Tokenomics 架构

- 代币类型：单代币还是双代币？
- 功能定位：治理 / 激励 / 费用捕获 / 风险分担。
- 分配机制：团队、投资人、社区、生态激励、基金会。
- 释放机制：Cliff + 线性解锁。
- 价值捕获：代币与协议的绑定方式（手续费回购、抵押需求、质押分红）。

阶段 4：风险与改进

- 协议风险：技术漏洞、黑天鹅事件。
- Tokenomics 风险：过度通胀、代币失去需求。
- 改进措施：多签治理、保险基金、动态通胀模型。

三、产品设计模版 (Template)

以下是小组完成方案时的基础骨架，每组需要逐项填充：

1. 协议概述

- 协议名称：_____
- 解决的痛点：_____
- 目标用户：_____

2. 协议逻辑

- 协议类型：DEX / 借贷 / 衍生品 / 保险 / 其他
- 核心功能模块：
 - 模块 1：_____
 - 模块 2：_____

- 模块 3: _____

- 用户交互流程 (附流程图)

3. Tokenomics 架构

- 代币类型: 单代币 / 双代币
- 功能: 治理 / 激励 / 费用捕获
- 分配比例: 团队 ____%、投资人 ____%、社区激励 ____%、基金会 ____%
- 释放机制: Cliff ____月 + 线性释放 ____年
- 价值捕获: 手续费分配、回购销毁、质押收益等

4. 风险与改进

- 协议风险: _____
 - Tokenomics 风险: _____
 - 改进方案: _____
-

四、模拟产品设计案例

1. 链上保险协议 InsurFi

下面以“链上保险”为例，完整演示一个模拟设计。

1. 协议概述

- 协议名称: InsurFi
- 解决的痛点: 当前 DeFi 用户面临智能合约漏洞、跨链桥被黑、稳定币脱锚等风险，但传统保险产品覆盖不足，赔付流程慢。
- 目标用户:
 - 普通 DeFi 投资者: 想要为质押/流动性挖矿买一份“风险保障”。
 - 项目方: 希望为自己的协议提供背书，吸引用户时能提供“保险保障”。

2. 协议逻辑

- 协议类型: 去中心化保险 (Insurance Protocol)

- **核心功能模块：**
 - 风险资金池**：用户缴纳保费形成保险资金池。
 - 风险评估模块**：由 DAO 或预言机提供风险等级（例如，跨链桥风险高于主流借贷协议）。
 - 理赔模块**：触发条件（如合约被攻击，或稳定币价格长期低于锚定值）→ DAO 投票或自动触发赔付。
 - **用户交互流程：**
 - 用户存入资产 → 选择要投保的协议/资产 → 支付保费。
 - 一旦触发赔付条件，用户可申请理赔 → 审核通过 → 从保险池赔付。
 - 资金池的流动性提供者（LP）可分享保费收益，但承担一定风险。
-

3. Tokenomics 架构

- **代币类型：**双代币模型
 - **INS（治理代币）**：治理、投票、价值捕获。
 - **iUSD（保险凭证）**：代表保险资金池份额，LP 存入资产可获得 iUSD。
- **功能：**
 - **INS：**
 - 治理（DAO 投票）
 - 费用捕获（部分保费回购销毁）
 - 抵押保障（质押 INS 参与风险分担）
 - **iUSD：**
 - 表示保险资金池份额
 - 可赎回本金 + 收益
 - 可能被扣减（黑天鹅事件赔付）
- **分配比例（INS）：**
 - 团队：15%（4 年线性释放）
 - 投资人：15%（2 年线性释放）
 - 社区激励：40%（保险参与奖励 + 流动性激励）
 - 基金会：20%（用于安全基金和合作伙伴）
 - 储备金：10%

- **释放机制：**

- 团队和投资人：12 个月 cliff，之后线性释放
- 社区激励：前两年释放 60%，后期逐渐递减

- **价值捕获：**

- 保费的 50% 用于回购销毁 INS
 - 30% 分配给 iUSD LP
 - 20% 进入 DAO 储备金，用于未来极端赔付
-

4. 风险与改进

- **协议风险：**

- 预言机攻击：如果风险数据被篡改，可能导致错误赔付。
- DAO 作恶：治理被鲸鱼操纵，导致滥用赔付。

- **Tokenomics 风险：**

- INS 通胀过高 → 没有足够的价值捕获支撑 → 代币价格下跌。
- iUSD 大规模赎回 → 保险资金池流动性不足。

- **改进方案：**

- 引入多重预言机与人工审核机制 → 提高理赔准确性。
 - 设置 DAO 投票门槛与时间锁 → 降低治理攻击风险。
 - 动态保费机制 → 风险越高的协议保费越高，保障代币价值。
-

2. 多链跨链桥协议 ChainLinker

1. 协议概述

- **协议名称：**ChainLinker

- **解决的痛点：**

- 多链生态快速发展（Ethereum、Solana、Aptos、Sui 等），但资产跨链效率低、安全风险高。
- 现有跨链桥问题：被黑事件频发（如 Wormhole、Ronin） 、流动性碎片化、用户体验差。

- **目标用户：**

- 想在多链间转移资产的普通用户（例如，把 ETH 从以太坊跨到 Arbitrum，用于 DeFi）。

- 需要多链资产支持的 dApp 和协议（如多链 DEX、借贷协议）。
 - 跨境金融和机构用户（希望有更安全合规的跨链基础设施）。
-

2. 协议逻辑

- **协议类型：**跨链桥（Cross-chain Bridge）
- **核心功能模块：**
 - 锁仓与铸造模块：**用户在源链锁定资产（如 ETH），目标链上铸造对应包装资产（如 cETH）。
 - 验证与共识模块：**采用多签 + MPC 技术保障交易验证，避免单点风险。
- **清算与赎回模块：**用户可随时赎回原链资产（销毁包装资产，释放源链资产）。
- **流动性池模块：**提供流动性池模式，用户可直接用 LP 资金池实现跨链兑换，无需等待验证（类似 Stargate 机制）。
- **用户交互流程：**
 - 用户在 ChainLinker 前端选择跨链方向（如 ETH → Solana）。
 - 协议在源链上锁仓 ETH，验证节点确认交易。
 - 在目标链上铸造等值 cETH（包装资产），或者从流动性池直接发放。
 - 用户可随时把 cETH 销毁 → 在源链取回 ETH。

5. Tokenomics 架构

- **代币类型：**单代币模型（CLINK）
- **功能：**
 - **治理：**DAO 投票（跨链费用、支持新链、验证人管理）。
 - **激励：**质押 CLINK 可成为跨链验证节点并获得手续费分成。
 - **费用捕获：**用户跨链需支付少量手续费（如 0.1%），一部分回购 CLINK。
- **分配比例（CLINK）：**
 - 团队：15%（3 年线性释放）
 - 投资人：10%（2 年线性释放）
 - 验证人/节点激励：40%（用于质押奖励）
 - 社区激励：25%（空投、流动性挖矿）

- 基金会：10%（跨链安全基金）
- **释放机制：**
 - 节点奖励逐年递减（前3年高激励，后续逐步减少）。
 - 团队和投资人锁定期 + Cliff，避免早期抛压。

- **价值捕获机制：**
 - 跨链手续费（0.1%）分配：
 - 40% 给验证节点
 - 30% 回购销毁 CLINK
 - 20% 注入跨链安全基金
 - 10% DAO 库房
-

6. 风险与改进

- **协议风险：**
 - 验证人作恶：如果验证节点被攻击或串谋，可能导致跨链资产被盗。
 - 流动性不足：资金池流动性枯竭，用户无法快速完成跨链兑换。
 - 跨链延迟：多链确认机制导致等待时间长，影响体验。
- **Tokenomics 风险：**
 - 早期抛压：投资人和团队代币解锁可能带来卖压。
 - 激励过度：高节点奖励可能导致通胀。
 - 价值捕获不足：如果跨链手续费过低，代币回购力度有限。
- **改进方案：**
 - a. **技术层面：**采用 MPC + TEE 双重验证机制，提升节点安全。
 - b. **经济层面：**动态手续费（跨链需求高时费率提升，帮助积累更多基金）。
 - c. **治理层面：**DAO 监督节点，若节点作恶，可没收其质押代币。
 - d. **生态层面：**与主流 DE
 - e. X、借贷协议合作，推动 CLINK 成为多链抵押资产。