bridge.

Bridge mutual v1.0

技术白皮书

Bridge Mutual

Bridge Mutual 是一个无需许可的、去中心化的、DAO治理的可自由选择的，为稳定币、中心化交易所、智能合约和其他加密服务提供承保的风险管理平台。 平台允许用户购买保单以保护其资产，提供承保以赚取利润和收益，以及对索赔及赔付进行投票，通过公平评估获得补偿。

Bridge Mutual 平台允许任何人随时为任何智能合约、交易所或服务创建保险池。 然后，其他用户可以购买承保协议，以保护自己免受因可能的黑客、 薅羊毛 (rug pull) 或漏洞利用导致永久性资金损失的侵害；稳定币也可承保。稳定币的承保范围包括一切使稳定币脱离1美元挂钩的事件而造成的任何价值损失。 Bridge Mutual 将由成千上万个风险池组成，每个池代表行业中每个平台、交易所和稳定币资产的承保范围。

前言

我们的业务模型的某些方面已更改或推迟，以加快开发和产品发行的速度。 因此，v1.0 中的某些功能将在v2.0及更高版本中改进或更改。 随着我们发布平台的更新版本，我们将更新此技术白皮书。

在本白皮书中讨论的任何将在v2.0中启动的功能，都明确标记为 (V2)。

v1.0 专注于智能合约的承保，不包括稳定币或中心化交易所 (及托管) 的承保范围。

词汇定义

有效保单 - 保单持有人针对特定风险池购买的所有保单的累积价值，以DAI表示。

上诉 - 重新评估已被裁决的索赔的程序。在上诉程序中，仅由那些信誉分数高 (因投票而获得) 的受信任投票人对索赔进行评估。

bmiDAI质押合同 - 用于存储 bmiDAIx 的智能合约池，并根据项目X风险池的利用率，为质押用户提供额外的BMI奖励。

BMI质押合同 - 允许用户质押BMI的智能合约。进行BMI质押的用户将获得 stkBMI，这些 stkBM 会累积BMI质押奖励，并有资格在DAO中投票。

资金池 - 管理存放在生态系统所有项目保险池和再保险池中的DAI的智能合约。通过DeFi协议产生收益。

索赔人 - 提交了索赔申请的保单持有人。

索赔额 - 索偿人要求得到补偿的金额。该金额应由索赔人提供的证据支持，且不能超过保单金额的最大值。

承保 - 当承保事件发生时，保单持有人有提出索赔的权利。如果获得投票人的批准，则索赔人可以获得不超过保单最高金额的补偿。

承保事件 - 指保单涵盖的任何事件，可使保单持有人有资格提出索赔并对损失获得补偿。

保险池 - 由智能合约控制的资金池，专门为某特定项目或平台提供保险而设立。

承保人/保险提供人 - 为特定保险池提供资金的用户。

承保人收益 - 承保人赚取的收益，作为承担特定的项目保险池的风险并提供流动性的回报，占保费的80%。

未结开放索赔 - 正在投票流程中的索赔申请。 投票人会评估保单持有人提供的证据，并决定索赔的有效性。

保单持有人 - 在由承保人提供资金作为储备的特定保险池中购买保险的用户。

保费 - 为获得承保，保单持有人支付的或被要求支付的特定保险单的金额。

项目X - 在 Bridge Mutual 协议中具有保险池的任何项目 (X代表项目名称)。

项目X保险池 - 为项目X设立的保险池 (见以上项目X定义)。

协议 - 一般指 Bridge Mutual 平台和系统。

协议费 - 无论在哪里产生和支付的，都会累积在再保险池中的费用 (通常是名义金额)。

再保险池 - 从协议费和资金池的收入中积累，以提高协议的资本效率。在下一代协议的交互中，再保险池将为生态系统中的保险池提供资本 (从而获得收益并影响保费价格)。

Defi 收益产生聚合器 – 用于管理存放在生态系统内所有项目池中的DAI，并生成转移到再保险池的收益的智能合约。

信誉分数 - 用户在 Bridge Mutual 系统的信誉级别，该级别根据用户对索赔的评估的准确性而增加或减少。信誉分数从 1.0x 开始，最高可以达到3.0x。

奖励池 - 一个将奖励分配给的相关的网络参与者，进行某些有益于协议生态系统的活动的智能合约。

护盾挖矿 - 项目X通过以项目X代币的形式给承保人额外奖励作为激励措施的程序。将代币作为额外的奖励分发给项目X 保险池的承保人。代币将作为额外奖励分发给项目X 保险池的承保人。

受信任投票人 - 活跃投票人中信誉得分最高的15%。

利用率 - 有效保单已使用的保险池资金除以该保险池中可用的保险资金总额。利用率越高，保单价格越贵。如果某个保险池中有1,000个 DAI 的承保资金可用，有效保单已占用了其中的500 DAI 作为储备金，则该保险池的利用率为50%。

投票人 - 质押 BMI 代币以对索赔进行投票的用户。

投票权 - 等于 vBMI 数量乘以信誉得分。

代币词汇定义

BMI 代币- Bridge Mutual 生态系统的平台币。用户将其BMI质押后，会收到代替的 stkBMI 代币。

stkBMI 代币 - 作为存储和质押了 BMI 的证明而发行的代币。stkBMI 的价值不断增长，代表持有用户从协议的奖励池中累积的奖励。为参与索赔投票而质押的 BMI，用户会收到替代的 vBMI 代币。

vBMI 代币 - 作为存储和质押了 stkBMI 的证明而发行的代币。 vBMI 在投票流程中使用，用户在对索赔和 DAO 治理提案进行投票时使用。

bmiDAIx 代币 - 作为在任何项目X保险池中存入 DAI 的证明而发行的代币 (例如: bmiDAIsushi 或 bmiDAIcompound)。bmiDAIx 是一种收益和承担风险的代币，每当有用户购买保单而支付保费，就会被动地累积 DAI 作为承保人的收益。

承保人可以将其 bmiDAIx 代币在 bmiDAIx 质押合同中锁定固定的一段时间，以换取额外的奖励。当质押 bmiDAIx 后，用户会收到可转让的 NFT 债券。发行此 NFT 的目的是在不从生态系统中取出 DAI 的情况下，为用户提供流动性；持有人可以在公开市场上出售该 NFT，购买该 NFT 的用户将获得该 NFT 所对应的质押的 bmiDAIx 的所有权。

BMI NFT Bond - 作为在质押合同中的质押了 bmiDAIx 的所有权证明的不可替代债券而发行的代币。 该 Bond 可完全转让，可以在任何 NFT 市场上出售。

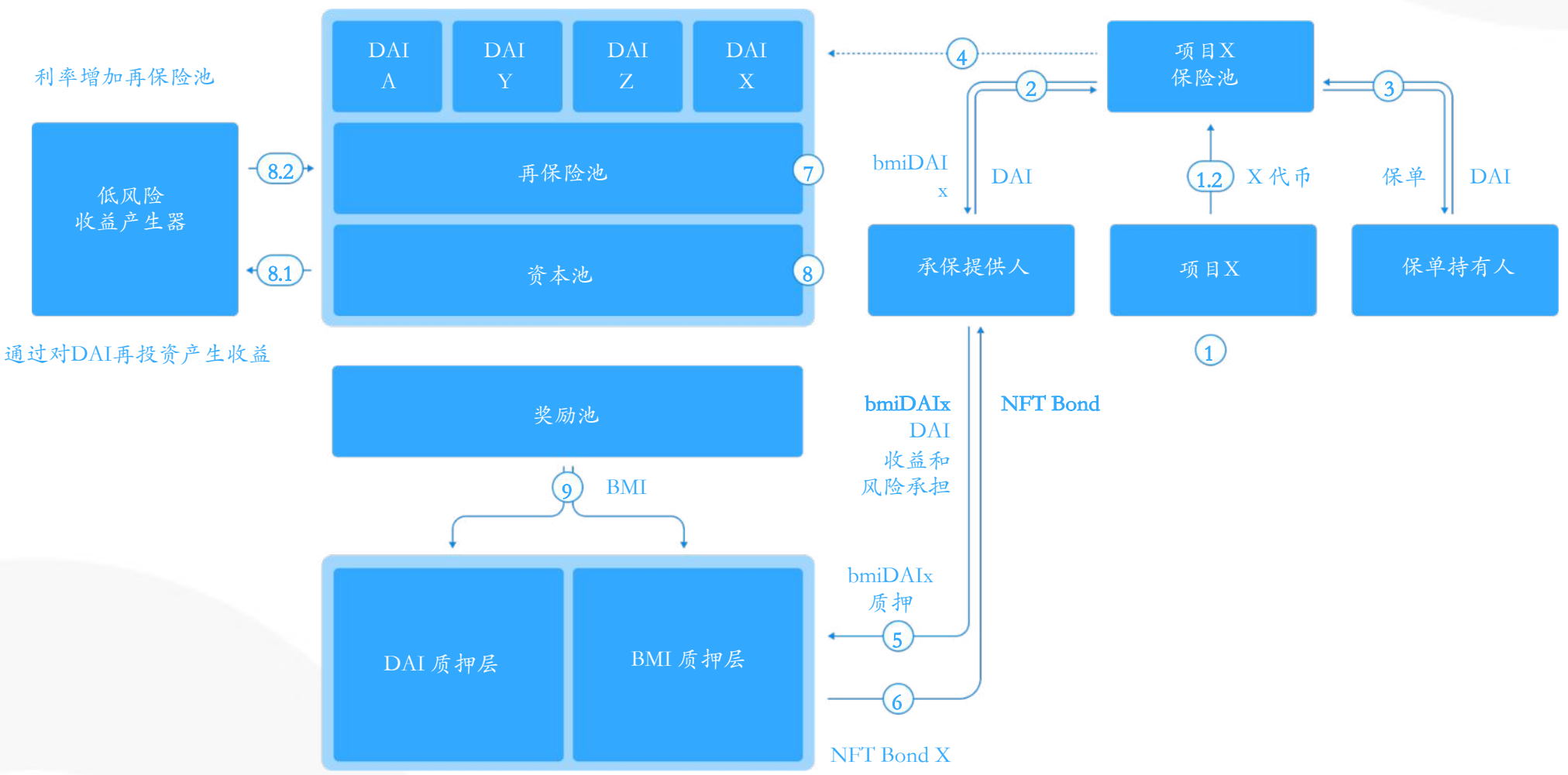
ETH/BMI LP token - 为交换用户向 Uniswap 提供 BMI 流动性，而发行的流动性池代币。 用户可以在 Bridge Mutual 的 Launch App 平台上质押 ETH/BMI LP token，以获得相应的奖励。

平台概要

1. 任何人都可以通过选择兼容的网络 (以太坊、币安智能链、波卡等)，输入项目X代币的合同地址，并存入初始资金DAI来简单地在协议上创建新的项目保险池。
2. 对自己的安全性有信心的项目可以通过提供项目X代币作为额外奖励来激励承保人，这些奖励将分发给流动性提供者 (这称为护盾挖矿)。 护盾挖矿是增加项目保险池可承保额度的好方法。
3. 任何地方的任何人都可以购买所需时间和金额的保险。没有KYC的要求。
4. 项目X保单持有人所支付保费的大部分 (80%) 作为收益分配给承保人。保费的一部分分配给投票人，其它部分存入再保险池。
5. 保险池中的大部分资金都转移到资金池中。资本池将这些资金通过其他DeFi服务产生收益，然后将此收益存储到再保险池中，以提高V1协议的整体资本效率。
6. 再保险池从资本池以及所购买的每份保单的保费的一小部分中累积收入，用于提高资本效率。
7. 一小部分保费被存入到再保险池中，用于为项目自身提供保险，并提供更具价格竞争力的保费。
8. 如果发生承保事件，保单持有人可以通过提交相关证据来支持索赔，以证明保单持有人因承保事件遭受了永久损失。索赔主张的有效性由投票人 (或受信任投票人) 通过盲投的方式，以及建立在博弈论基础上的投票系统决定。根据投票结果，可以部分或全部批准索赔请求。
9. 投票给得票多数一方的投票人将获得代币奖励，并且信誉分数得到提高，从而进一步增加其投票权。投票给得票少数一方的投票人将被降低信誉分数，在极端情况下 (如1:99)，甚至可能会失去部分质押代币。
10. 其索赔请求被拒绝的保单持有人，可以上诉并再次提交索赔。 上诉程序只有受信任的投票人有权投票。
11. 协议提供了多种不同和具有协同效力的质押选项。用户可以同时作为承保提供者或流动性提供者，同时赚取质押收益以及获得投票奖励。
12. 随着项目的发展，Bridge Mutual 将过渡到完全的去中心化的自治组织 (DAO)。 DAO完全由代币持有人控制；代币持有人可以对协议提出建议，进行表决，并对协议治理实施改进和更改。

0. 系统模型概览

商业模式图



该模型的各个组成部分已在上面编号，并将在后面具体说明。

1. 为项目创建一个保险池，这称为项目X保险池(由于系统是无需许可的，因此任何用户都可以在平台上为任何项目创建任何池）。

    1.1. 创建项目X保险池的用户必须存入初始资本(DAI)

    1.2. 通过将任意数量的X代币存入其指定的护盾挖矿池中(V2)，项目X提供额外的奖励，以激励用户为其保险池提供资金；该X代币奖励与其它收益一起分配给承保提供者，从而提高了APY。

2. 保险提供人/承保人

2.1. 负责衡量将资本投入到项目X 保险池，为其提供保险的风险。

2.2. 押注该项目不太可能发生承保事件

2.3. 每当保单持有人购买保险时，从所收取保费中获得利润分成 (请参阅第2章 (f)(iii) - (v) 节)

2.4. 如果项目X参加了护盾挖矿 (V2)，则可以收取项目X代币

2.5. 每当有对其提供承保的项目保险池的成功索赔时，则与其他承保提供人一起按比例损失部分或全部资本；

2.6. 承保人获得 bmiDAIx (其中x代表项目名称)：

2.6.1. bmiDAIx 证明用户已将DAI存入项目X 保险池

2.6.2. bmiDAIx 是一种收益承担资产。有人购买保单，则 bmiDAIx 的价值将增加。

2.6.3. bmiDAIx 也是一种风险承担资产。如果对项目X提出成功索赔，则 bmiDAIx 的价值将减少。

2.6.4 如果对项目X提出成功索赔，则1bmiDAIx 的价值可能少于1DAI。

示例:

- 项目X的保险池中有10,000个DAI
- 发行10,000个bmiDAIx代表10,000 个DAI 。1 bmiDAIx = 1 DAI + 所获得的收益
- 后来，对项目X保险池成功索赔2,000 DAI
- 支付赔偿后，项目X保险池内还剩8,000 DAI
- 现在，1 bmiDAIx = 0.8 DAI + 所获的收益

2.6.5. 索赔的有效性和赔付由投票人决定 (该程序在本文的第4部分 “保单索赔” 部分进行说明)。

3. 保单持有人

3.1. 为项目X发生可能导致项目X资金损失的承保事件支付保费。保费数额由项目X保险池的利用率决定。

3.2. 利用率由有效保单价值除以项目X保险池中DAI的价值来决定。如果有金额为10个DAI的有效保单，而在项目X保险池中共有100个DAI，则利用率为10%。

3.3. 承保事件发生时 (例如，黑客攻击、漏洞利用、薅羊毛等)，保单持有人必须提交索赔申请才能获得赔偿 (要求赔偿的金额不能超过保单的承保金额)。

3.4. 保单期满后7天内提出索赔，但承保事件必须发生在保单有效期间内。

4. 项目X保险池

4.1. 存放在项目X保险池中的DAI存储在资本池中，用于为BMI质押人和协议产生被动收入。这适用于所有保险池。

4.2. 保单持有人购买保险协议所支付的总费用 (保费) 分配如下：

4.2.1. 80％作为收益分配给承保人；

4.2.2. 20％作为协议费进入再保险池。

5. 承保人可以将bmiDAIx质押到bmiDAI质押合同池中，以获得额外的BMI奖励。奖励是按区块分配的。

6. 在bmiDAI抵押合同池中质押bmiDAIx的承保人将获得BMI NFT Bond，代表所投入DAI的金额。

6.1. BMI NFT Bond 是一种收益和风险承担的资产，代表承保人存储在保险池中的DAI。

6.2. BMI NFT Bond 可交易，可以在任何 NFT 交易市场上出售。

7. 再保险池

7.1. 存储保单持有人支付所保费的20％;

7.2. 存储资本池产生的所有收入;

7.3. 再保险库中的资金用于向项目X 保险池提供流动性，以提高资本效率，赚取额外收入，优化生态系统(V2)。

8. 资本池汇总项目X资金池的DAI，以便为协议产生额外的收入

8.1. 资本池将DAI发送到低风险收益生成平台 (V2)

8.2. DAO 决定收入的支出方式 (V2+)

9. 平台启动后的24个月内，从奖励池中分配一部分BMI，用于激励bmiDAIx质押和BMI质押，除非DAO对此做出更改。

9.1. 可以将BMI质押在质押协议中，获得BMI奖励;

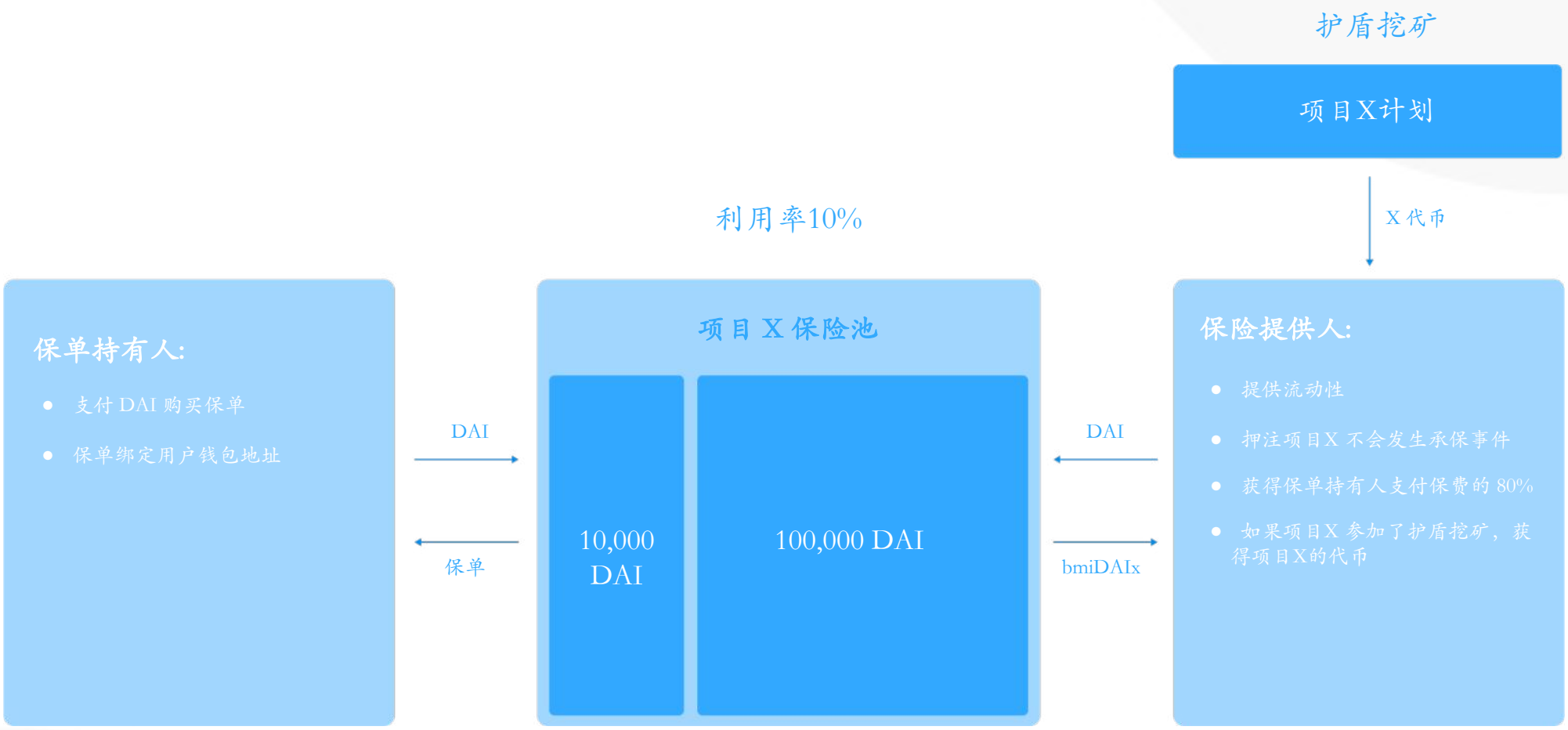
9.2. BMI质押，奖励会自动计入本金。

9.3. BMI质押不能立即解除；用户解除质押需要等待8天。

9.4. 向用户发行stkBMI作为存储BMI的证明。

1. 提供承保

项目 X 保险池示意图



系统参与者

保单持有人:

1. 愿意为项目X可能发生的对项目产生影响的承保事件承保的保单支付费用 (保费) 的用户。
2. 保费的20%直接存入再保险池，80%分配给承保人;
3. 保单持有人用稳定币DAI购买保单
4. 保单的价格基于:
    - 4.1. 承保期间 - 1至52周
    - 4.2. 项目X保险池的利用率
        - 4.2.1. 有效保单的金额;
        - 4.2.2. 保险池的资本额;

        如果有效保单额为100 DAI，池中的总资本额为1,000 DAI，则利用率为10%。
    - 4.3. 参与项目对应的再保险池功能 (V2)

承保人/保险提供人:

1. 可以是任何人，甚至是项目本身。
2. 为项目X保险池的风险承担一方提供DAI。
3. 共同分享保单持有人购买X项目保险池的保单而支付的全部保费的80%，作为向项目X 保险池提供资金的交换。 承保人的获得的奖励与提供给项目X保险池的资金数额成正比。
4. 成功索赔后，索赔人将从承保人提供的资金中获得补偿，最高可达其购买保单的最高额。 承保人应按其向项目X保险池中存入的金额，按比例分担损失。

关于保单和收益

承保人:

1. 每个池的APY都会清楚显示在平台上。 APY最多包含3种不同的资产： Bridge Mutual token (BMI)，DAI (稳定币) 和项目X的token (并非每个池都有)；
2. 收益每天分配给承保人；
3. 每个池的APY与其利用率成正比。例如：
    - 3.1. 项目X保险池的利用率为10%；
    - 3.2. 保费的年度费用为10%；
    - 3.3. 某随机用户想要购买$1,000保额的保单，为期12周；
    - 3.4. 他必须支付100 DAI *（12/52周），即23 DAI。
    - 3.5. 23 DAI 将在12周内分发给该池的承保人 (减去任何协议费)；
    - 3.6. 假设池中有1000个DAI，则APY为10%。
4. 收益是在用户将其bmiDAIx交换为DAI的当天实现的。例如：
    - 4.1. 随机用户将100 DAI存入APY为20%的池中；
    - 4.2. 他收到100 bmiDAIx 作为交换，这代表他存入的资产；
    - 4.3. 12周后，他想撤回他的 bmiDAIx，当时的价值为105 DAI (由于20%的APY)。
    - 4.4. 他在平台上销毁100个bmiDAIx，取回105个DAI。
5. 承保人从以DAI支付的保费中取得的收益，在每个区块 (或每个纪元/epoch) 中都添加到池中，从而增加了项目X保险池中DAI的余额。
6. 收益是复利的，这增加了项目X 保险池的深度。
7. 资金池使用项目X 保险池中的DAI为协议生成收益 (V2)。

存入DAI

> #bmiDAIx = 用户质押DAI取得bmiDAIx的数量
> TSbmIDAIx = 未撤回的bmiDAIx总额
> DAIb = 项目x保险池中的DAI 余额
> #DAId = 存储在项目x保险池中 DAI 的数量

当用户将DAI存入项目x保险池时，协议会生成bmiDAIx作为交换。
如果项目 x 保险池是空时，则：

> **#bmiDAIx = #DAId**

如果项目x保险池不是空时，则：

> $$\#bmiDAIx = \frac{TSbmiDAIx * \#DAId}{DAIb}$$

承保人收益，即以DAI所支付保费的80%，被添加到池中每一个区块(或每一个时期/epoch)，从而增加了项目X 保险池 (DAIb) 中DAI的余额。

承保人收益

当收到保费后，将所收取保费的80%在保单的承保期间内分配。

例如，如果购买为期30天的保单，则承保人的收益将以每天3.33%的比例进行分配。

> $DAIb_{n+1}$ = 每天结束时项目X保险池中的DAI余额
> Pc_x = 用户x向项目X保险池支付的新保费费用
> Ppool = 在承保人收益奖励池中累计的保费

> $$DAIb_{n+1} = DAIb_n + 3.33\% * (Ppool + \sum_{1}^{x} Pc_x)$$

示例:

在DAIb中 有1,000 USD， 在Ppool中100 以每天3.33%分配

> DAIb = 1,000 USD
> Ppool = 100 USD
> **每天的奖励** = 3.33 USD

因 此:

$$DAIb_{n+1} = 1{,}000\ USD + 3.33USD$$
$$DAIb_{n+1} = 1{,}003.33\ USD$$

目 前 的APY 为:

$$APY = \frac{3.33\ USD * 365}{1{,}000\ USD}$$

$$APY = 121\%$$

第二天，一个新用户进入并购买了保单，他在Pc_n支付了100 USD

那 么:

$$DAIb = 1{,}003.33\ USD$$
$$Ppool = 196.66\ USD$$
$$每天的奖励 = 6.54\ USD$$

$$DAIb_{n+1} = 1{,}003.33\ USD + 6.54\ USD$$
$$DAIb_{n+1} = 1{,}009.87\ USD$$

现在的APY 为:

$$APY = \frac{6.54USD * 365}{1{,}003.33\ USD}$$

$$APY = 237\%$$

从质押池中取出DAI

#DAIw = 用户从项目X保险池中取出的DAI的 数额
#bmiDAIxb = 为取出DAI，用户销毁的bmiDAIx的数额

$$\#DAIw = \frac{DAIb * \#bmiDAIxb}{TSbiDAIx}$$

为了确保池中有足够的流动性来支付所有未结的保单，在承保人提交撤回请求后，必须等待8天 (冷却期)，才可以取出其DAI。

- 承保范围提供者提交提款请求后，议定书仍然可以使用其资金来支付对该集合的成功索偿。
- 经过8天冷却期后，承保人有48小时的时间提取资金。 如果没有在期限内提取，则必须再次提交提款请求，并再等待8天。

保单购买和计价

- 保费由承保期限、金额和项目X保险池的当前利用率决定。
- 承保期限最短1周，最多长52周。这可能会在以后的版本中更改，或者可能在不同的保险池有所不同。
- 保单期限以 epochs 衡量，其中一个epochs为1周。所有epochs都带有时间戳，并在日历年度的特定日期开始和结束。用户可以购买保险的最短时间为1个epochs ，最大时间为52个epochs 。
    - 实际上，如果购买是在epochs的中间或末期进行的，则用户可以购买实际时长少于一个整周的保单。这意味着最长保单期间 (52周) 始终等于或小于一个整年。
- 利用率越高，保费越高。
- 利用率极低的池会设置一个年度最低保费； 在启动时，此最低值为3%，但可能通过治理更改。
- 较高的利用率反映了对保单的高需求，这意味着项目X被视为具有较高风险，因此价格更高。
- 应用程序上显示的所有保费均按年计算。

> MC = 最低保单费用 (保费) (以 %表示)
>
> Pc = 投入到再保险池的用户支付的费用 (协议费) 的百分比 (以 %表示)
>
> TMCC = 当资产不被视为风险资产时的目标最高保单费用(保费) (以 %表示)
>
> URRp = 当资产被视为风险资产时定价模型的利用率 (以 %表示)
>
> MCC = 当利用率等于100% (以 %表示) 时的最高保单费用 （溢价） (以 %表示)
>
> UR = 利用率 (以 %表示)
>
> %CoC = 保单费用 (保费) 相对于保单金额大小的百分比 (以 %表示)
>
> %CoC final = 最终保单费用 (保费)相对于保单金额大小的百分比 (以 %表示)
>
> $PoC = 年度化保单价格 (保费) 百分比 (以 %表示)

$$利用率 = \frac{保单持有人一侧池里的DAI + 保单大小}{承保人一侧池里的DAI}$$

$$如果\ UR < URRp \Rightarrow \%\ CoC = \frac{UR}{URRp} * TMCC$$

$$如果\ UR > URRp \Rightarrow \%\ CoC = TMCC + \frac{UR - URRp}{100\% - URRp} * (MCC - TMCC)$$

$$\%CoC\ final = \max\{\%\ Col, MC\}$$

$$\$PoC = 保单大小 * \%CoC\ final$$

支付给承保人的资金:

> 作为收益支付给承保人的资金 = $PoC final · (1- Pc)

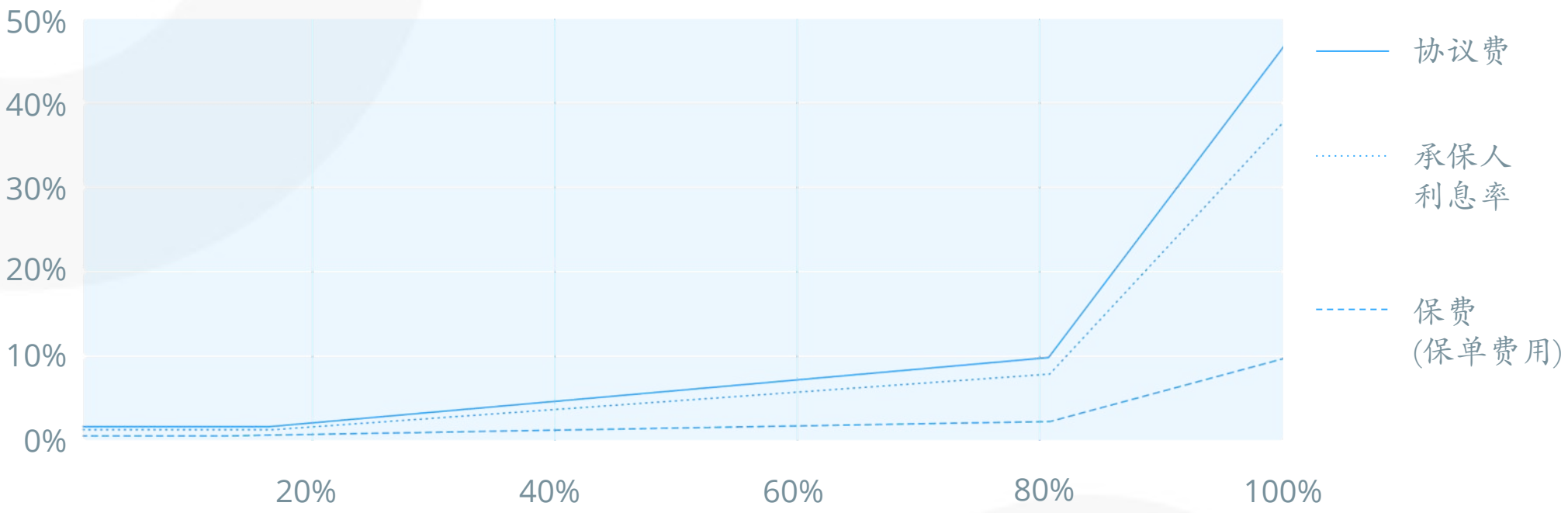
协议费:

> 作为协议费进入再保险池的资金 = $PoI final *Pc

启动时变量:

> MC = 2%
> Pc = 20%
> TMCC = 10%
> URRp = 80%
> MCC = 50%

保费、承保人利息率、协议费 vs 利用率



示例 1:

用户想购买金额为100,000 USD的项目X的保险;
保险池中已经有10,000,000 USD的可用保险;
其他用户已经购买了5,000,000 USD的保单。

$$利用率 = \frac{5{,}000{,}000 + 100{,}000}{10{,}000{,}000} \qquad 利用率 = 51\%$$

$$如果UR < URRp \Rightarrow \%\ CoC = \frac{51\%}{80\%} * 10\%$$

$$\%\ CoC = 5.10\%$$

$$\$PoC = 100{,}000\ USD * 5.10\%$$
$$\$PoC = 5{,}100\ USD$$

作为收益支付给承保人的资金 = 5,100 USD - (5,100 *20%)
作为收益支付给承保人的资金 = 4,080 USD

作为协议费存入再保险池的资金 = 5,100 *20%
作为协议费存入再保险池的资金 = 1,020 USD

示例 2:

用户想购买金额为4,000,000 USD的项目X的保险;
保险池中已有10,000,000 USD的可用保险;
其他用户已经购买了5,000,000 USD的保单。

$$利用率 = \frac{5{,}000{,}000 + 4{,}000{,}000}{10{,}000{,}000} \qquad 利用率 = 90\%$$

$$如果UR > URRp \Rightarrow \%\ CoC = 30\% + \frac{90\% - 80\%}{100\% - 80\%} * (50\% - 10\%)$$

$$\%\ CoC = 30\%$$

$$\$PoC = 4{,}000{,}000\ USD * 30\%$$
$$\$PoC = 1{,}200{,}000\ USD$$

作为收益支付给承保人的资金 = 5,100 USD - (5,100 *20%)
作为收益支付给承保人的资金 = 4,080 USD

作为协议费存入再保险池的资金 = 5,100 *20%
作为协议费存入再保险池的资金 = 1,020 USD

示例 3:

用户想购买金额为100,000 USD 的项目X的保险;
保险池中已经有10,000,000 USD的可用保险;
其他用户已经购买了5,000,000 USD的保单。

$$利用率 = \frac{500{,}000 + 100{,}000}{10{,}000{,}000} \qquad 利用率 = 6\%$$

$$如果\ UR < URRp \Rightarrow \quad \%\ CoC\ = \frac{6\%}{80\%} * 20\%$$

$$\%\ CoC\ = 1.50\%$$

$$\%CoC\ \ final = \max\{\%\ Col, MC\}$$

$$\%CoC\ \ final = MC = 2\%$$

$$\$PoC\ = 100{,}000\ USD * 2\%$$

$$\$PoC\ = 2{,}000\ USD$$

作为收益支付给承保人的资金 = 2,000 USD - (2,000 USD *20%)
作为收益支付给承保人的资金 = 1,600 USD

作为协议费存入再保险池的资金 = 2,000 USD *20%
作为协议费存入再保险池的资金 = 400 USD

保险池 & 护盾挖矿的设立

- 任何人都可以在应用程序上轻松设置保险池。只要用户提供确定的网络和智能合约地址，并存入1,000或更多DAI作为初始流动性资金，就可以创建一个新保险池。 其他用户将能够立即看到已创建的池。

- 用户 (任何人) 都可以为护盾挖矿提供代币 (V2)。
  - 用户可以在护盾挖矿池中存入任意数量的X代币
  - 用户可以自定义将x代币奖励分发给承保人的持续时间 (最少1个月)
  - 代币将线性且按比例分配给承保人

- 承保人可以随时免费提取护盾挖矿代币，没有提现延迟 (无需8天冷却期)。
- 护盾挖矿池可以随时由任何人补充或重新填充。

2. DEFI层 & 再保险池

再保险池

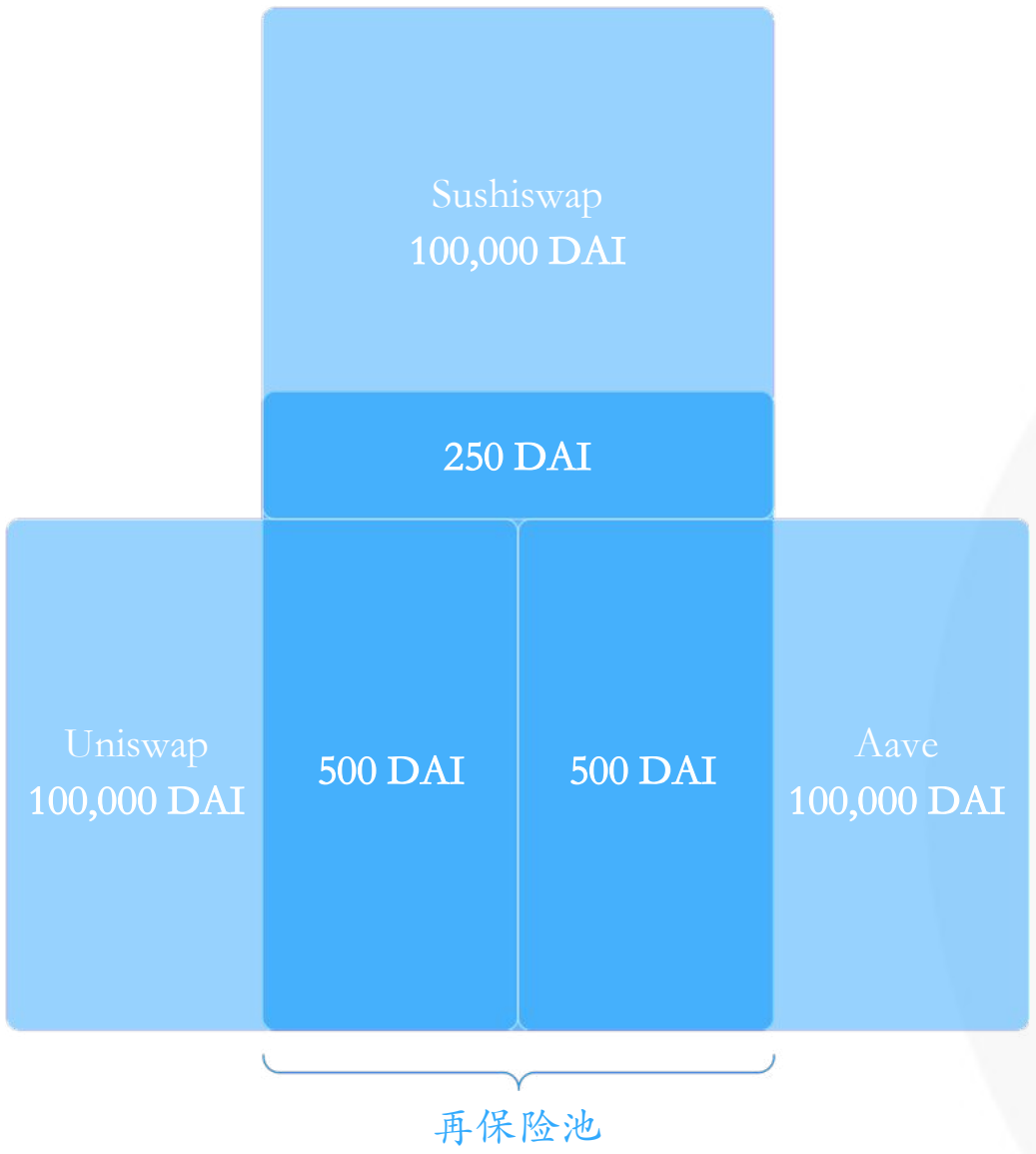
再保险池由协议拥有的资金组成，用于提高协议的整体资本效率，并通过增加资金池的利用率降低保费的价格。 再保险池的算法将在V2中发布。

利用率的效应

- 再保险池将作为承保人参加多个保险池。
- 再保险池资金可在许多不同的保险池中多次使用 (本质上是利用再保险库中的DAI)，因此降低了利用率，从而降低了用户的保费价格。
- 即使再保险池资金被多次使用，也不能 (通过杠杆DAI) 获得额外收益。从本质上讲，它在保持承保人收益的同时降低了协议的风险。
- 保险池的风险状况由DAO确定。

以下是潜在风险状况的示例：

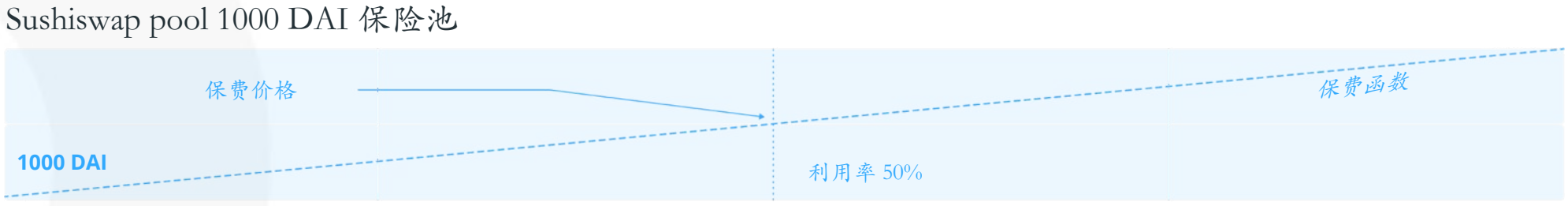
1. Uniswap (低风险), AAVE (低风险) and Sushiswap (中等风险)。
2. 每个池有 1,000 DAI，500 DAI 的有效保单，因此，每个池的率用率为 50%.
3. 再保险池有 1,000 DAI。
4. 再保险池按以下方式向保险池提供 DAI:
    - 4.1. 在Uniswap投入500 DAI (400真实的DAI + 100杠杠DAI) ，使Uniswap保险池规模变为1,500 DAI;
    - 4.2. 在AAVE投入500 DAI (400真实的DAI + 100杠杠DAI) ，使AAVE保险池规模变为1,500 DAI;
    - 4.3. 在Sushiswap投入250 DAI (200真实的DAI + 50杠杠DAI)，使Sushiswap保险池规模变为1,250 DAI。



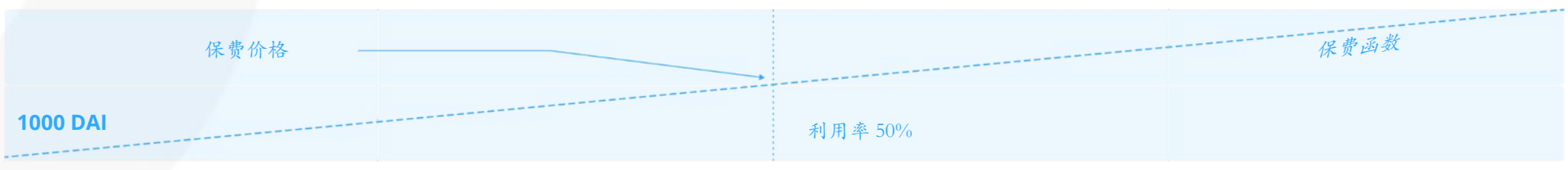
5. 再保险池共投入1,250 DAI 到三个保险池：AAVE (500 DAI), Uniswap (500 DAI) 和 Sushiswap (250 DAI).
6. 由于上述设计，利用率已经降低 (也因此降低了保费)。新的利用率分别为：
    - 6.1. Uniswap 33%
    - 6.2. AAVE 33%
    - 6.3. Sushiswap 40%

没有利用再保险池时:

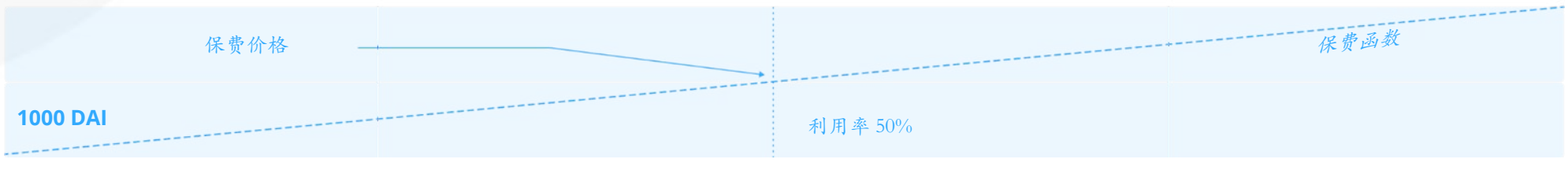
Sushiswap pool 1000 DAI 保险池



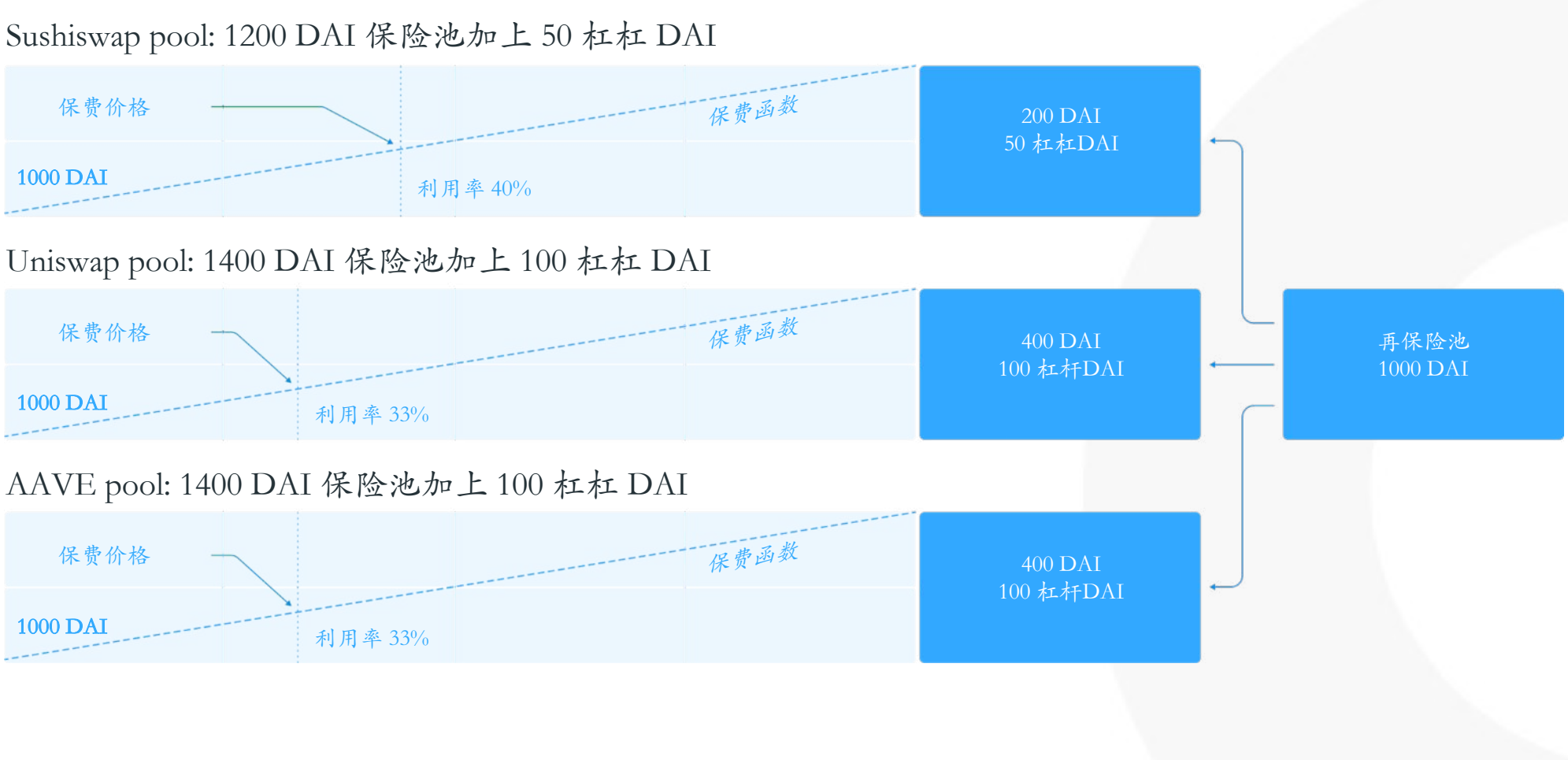
Uniswap pool 1000 DAI 保险池



AAVE pool 1000 DAI 保险池



使用了再保险池:



上述方法降低了利用率和保费。

示例:

没有使用再保险池时:

- 池中有1000 DAI;
- 有人以20%的保费购买了100 DAI 的保险;
- 承保人可获得 20 DAI;
- 承保人的收益是 20%。

使用再保险池时:

- 池中有1500 DAI;
- 再保险池提供了400 DAI 和100 个杠杠DAI;
- 有人以20%的保费购买了100 DAI 的保险;
- 在池中所有非杠杠DAI，即 20 DAI 被分配;
- 承保人收益仍然是 14.29% (1000/1400*20) ，在保险池收益为 5.71% (400/1400*20)。
- 池中有1500 DAI (1400 真实+100 杠杠)，但收益只分配真实的 DAI。

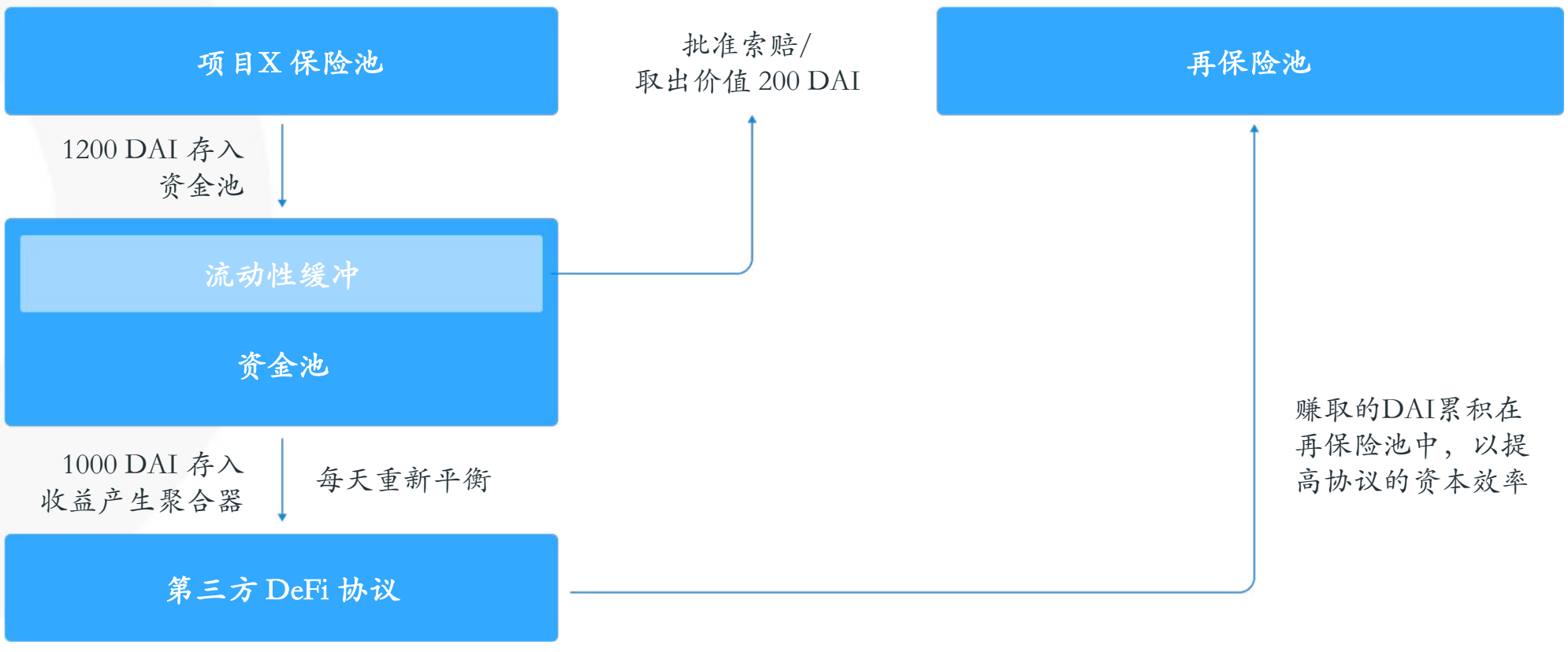
资金池

在早期版本中，资本池将主要作用于增加再保险池的规模，以提高协议的资本效率并降低保费。 DAO可以自由更改产生收益的分配 (通过第三方DeFi协议)。

1. 不需要用于即将到来的赔付/提款的DAI，会用来为资金池产生收入。
    1.1. 用户将DAI存入项目X保险池
    1.2. DAI 从项目X保险池转移到资金池
    1.3. 资金池保持流动性缓冲 (用于即将到来的赔付和提款)，并每天进行重新平衡。
    1.4. 除流动性缓冲外，资金池中的所有资金均分配给多个低风险收益产生协议。
    1.5. 每天都会进行小规模的重新平衡，而当分配与目标值显着不同时，就会触发重大的重新平衡。

2. 为了从项目X保险池中取回DAI，用户必须提交提款申请，并等待8天。
3. 经过8天的等待期后，用户需在48小时内提款 – 如未在提款期限内提出，则需要重新提交提款请求。
4. 在协议的第一个迭代中，由资本池产生的收入存储到再保险池中；在以后的迭代中，DAO可能会对此进行更改。

项目X池规模 = 1200 DAI



3. 质押和奖励

BMI 质押/staking

- 任何人都可以在BMI质押合同中购买并质押BMI。
- 奖励根据所质押的BMI数量按比例分配给质押人。
- BMI 奖励会自动计入本金。
- 用户从BMI质押合同中取出BMI，需在提交提款请求后等待8天。

当用户将BMI存入BMI质押合同时，协议将向该用户发行stkBMI代币，代表用户在质押合同中的资产。

> #stkBMI = 用户因质押BMI，所得的stkBMI的数量
> TSstkBMI = 已发行stkBMI的全部供应
> #BMIb = BMI质押合同中的BMI余额
> #BMId = 用户存储在池中的BMI数量

当BMI质押合同是空时:

> #stkBMI = #BMI

当BMI质押合同不是空时:

$$\#stkBMI = \frac{TSstkBMI * \#BMId}{\#BMIb}$$

奖励是按区块计算的，并使用线性函数“增加”质押押池 (#BMIb) 中的BMI余额。

预定量的BMI将在每个块中添加到#BMIb中。

> #BMIb = 用户存入的BMI + 每个区块的BMI* 目前的区块

从质押池中取出BMI

#BMIw = 用户从BMI质押合同中取出BMI数额
#stkBMIb = 为取出BMI，用户需销毁的stkBMI的数量

$$\#BMIw = \frac{BMIb * \#stkBMIb}{TSstkBMI}$$

bmiDAIx质押

1. 每个承保人都会获得bmiDAIx代币 (其中x是协议名称)。
2. bmiDAIx是收益和风险承担的资产，代表在项目X保险池中DAI的权利 (V2+)。
    2.1. bmiDAIx价值将根据特定的项目X保险池的收益率和成功索赔的数量，按比例调整。
3. 承保人可以将列入白名单的bmiDAIx存入bmiDAI质押合同中，以获得额外的BMI奖励。
    3.1. 通过DAO投票选择项目池列入白名单 (V2+)
4. 只有列入白名单的项目才能从bmiDAIx质押中受益，从而避免对协议的经济利用。
5. 奖励池中的大部分奖励将分配给bmiDAIx质押人。
    5.1. 发行 BMI NFT 债券给承保人，BMI NFT 债券代表他们在保险池中的权益，并赋予他们索回同等金额的 bmiDAIx 的权利。
    5.2. 但是，BMI NFT债券可立即从bmiDAI抵押合同中获得BMI奖励。
    5.3. BMI NFT债券是不可替代代币，由以下元数据组成：
        5.3.1. 可主张的bmiDAIx数量
        5.3.2. 可以从bmiDAI质押合同中获得BMI奖励（可以随时要求支付）。
        5.3.3. 这些NFT的所有人有权随时取出bmiDAIx和BMI代币，也可以在任何NFT市场上出售该NFT。

奖励池中BMI的分配

较低的利用率也意味着项目X保险池的奖励倍数较低。 利用率较高的项目被认为具有较高的风险，因此平台鼓励用户通过增加奖励来为这些池提供额外的保险。

基于风险的奖励倍数

风险评估:

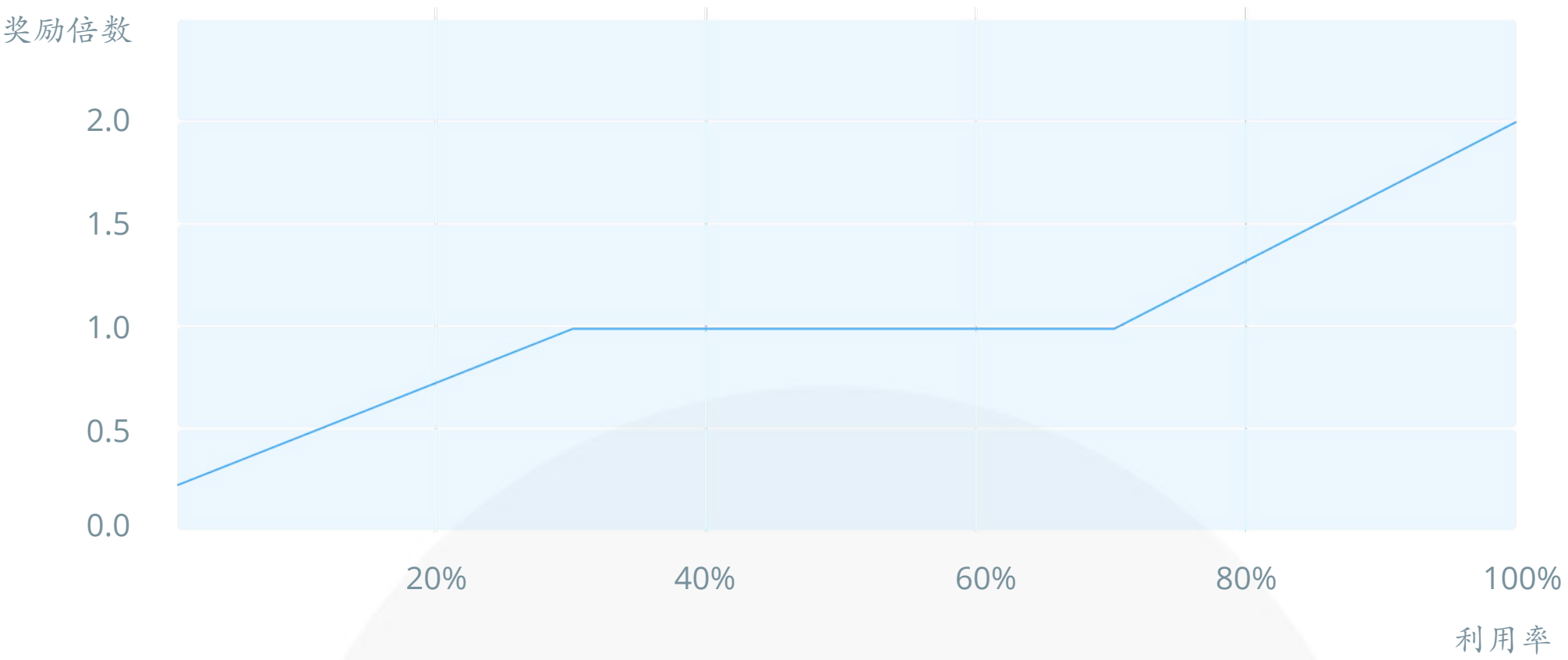
MinRm = 最低奖励倍数 (目前是 0.15x)
MaxRm = 最高奖励倍数 (目前是 2x)
BaseRm = 基本奖励倍数 (目前是 1x)
URRr = 当资产被认为是风险资产时，奖励模型的利用率 (以 %表示)
URRm = 当资产被认为是中等风险资产时，奖励模型的利用率 (以 %表示)
UR = 利用率 (以 %表示)
RMx = 项目X保险池的奖励倍数

$$\text{if UR} < \text{UURm} \Rightarrow \text{RMx} = \frac{\text{UR-1\%}}{\text{URRm}} * (\text{BaseRm} - \text{MinRm}) + \text{MinRm}$$

$$\text{if UR} > \text{UURm} \Rightarrow \text{RMx} = \text{BaseRm}$$

$$\text{if UR} > \text{UURm} \Rightarrow \text{RMx} = \text{BaseRm} + \frac{(\text{MaxRm-BaseRm})*(\text{UR-URRr})}{100\% - \text{URRr}}$$

奖励倍数 vs 利用率



DPIPx = DPIPx= 项目X保险池中的 bmiDAIx
PPR = 项目X奖励分配的比例

$$\%PPR = BaseRm + \frac{RM_x * DPIP_x}{\sum_{1}^{n}(RM_1 * DPIP_1 + RM_n * DPIP_n)}$$

此时的项目奖励 = %PPR * #R

MinRm = 0.15x
MaxRm = 2x
BaseRm = 1x
URRr = 70%
URRm = 50%
UR = 利用率 (以 %表示)
RMx = 项目X保险池的奖励倍数

示例 1:
保险池中有10,000,000 USD，5,000,000 USD 的保单已被购买。

利用率 = 5,100,000/10,000,000
利用率 = 51%

if UR > UURm ⇨ **RMx** = BaseRm
RMx = 1

示例 2:
保险池中有 10,000,000 USD，9,000,000 USD 的保单已被购买。

利用率 = 9,000,000/10,000,000
利用率 = 90%

$$\text{if UR} > \text{UURm} \Rightarrow RMx = BaseRm + \frac{(MaxRm-BaseRm)*(UR-URRr)}{100\% - URRr}$$

$$RMx = 1 + \frac{(2-1)*(90\%-70\%)}{100\% - 70\%}$$

$$RMx = 1.66(6)$$

示例 3:

保险池中有 10,000,000 USD，600,000 USD 的保单已被购买/预留。

> **利用率** = 600,000/10,000,000
> **利用率** = 6%
>
> $$\text{if UR} < \text{UURm} \Rightarrow \quad \text{RMx} = \frac{\text{UR-1\%}}{\text{URRm}} * (\text{BaseRm - MinRm}) + \text{MinRm}$$
>
> $$\text{RMx} = \frac{6\%-1\%}{50\%} * (1 - 0.15) + 0.15$$
>
> $$\text{RMx} = \text{RMx}=0.171$$

BMI奖励的再质押/Re-staking

BMI 奖励会自动累积到 BMI 质押合同的本金，这意味着奖励实际上是免费再质押的。

BMI奖励的提取

用户可以随时要求取回所获得的100%的奖励，但必须提交提款请求并等待8天。 8天过后，会有一个48小时的窗口，用户可以在该期间取出所有奖励。 如果用户未能在此窗口期间取回奖励，则必须重新提交另一个提款请求。

或者，用户可以立即取回80%的奖励，但其他20%将重新分配给所有 bmiDAIx 质押人。 该惩罚是为了减少bmiDAIx池的波动性。

3. 投票

提出索赔

- 如果用户要提出索赔，则需要锁定价值其要求赔偿额的1%的BMI - 这是为了防止轻率和欺诈性的索赔。
  - 如果索赔请求被拒绝，则将该锁定的BMI分配给投票人；
  - 如果索赔请求得到支持，则将该BMI退还给索赔人，投票人的奖励将从再保险池中支付；
- 如果索赔被认定为有效，则向索赔人支付DAI。
- 如果索赔请求被拒绝，则索赔人可以另外锁定价值索赔金额的1%的BMI，来提出上诉。

索赔流程

- 必须将索赔结果从智能合约中拉出来，才能显示投票结果。
- 为了避免未揭露索偿结果的情况，我们设计了一个模型，允许任何人揭示索偿结果并触发奖励分配。
  - 索赔未揭示的时间越长，触发奖励分配的人可获得的奖励就越多。
- 索赔评估程序完成后，索赔人有排他的3天时间单击按钮以查看投票结果。他将获得所有奖励的3%。
- 3天后，任何人都可以单击此按钮查看投票结果。
- 未公布索赔投票结果的3天后的每1天，给揭示投票结果的人的奖励将增加1%，最高可达100%的奖励分配给揭示投票结果的“点击按钮者”。

7 天提出索赔期

- 潜在的索赔人在其保单期满后有7天的时间对该保单提出索赔。
- 如果索赔被拒绝，则从拒绝之日算起，索赔人有7天的时间提出上诉。
- 在对一项索赔进行表决过程中，索赔人无法针对同一项目X保险池 购买额外的保单。
- 为了使索赔有效，承保事件必须在保单期间的最后一个epoch结束之前发生。 否则，索赔将被拒绝。

投票

- 只有vBMI (质押的stkBMI) 持有者才有资格投票 (以避免有偏见的DAI质押人)。
- 要获得vBMI，用户必须质押stkBMI。
- vBMI代币不可交易。
- 投票占多数的投票者获得奖励。
- 奖励根据用户持有的vBMI数量及其信誉分数来分配。

决定索赔的有效性

- 每个质押了stkBMI的用户都可以在应用程序的“索赔评估”选项中看到开放的索赔申请，并且可以打开索赔，查看索赔人上传的证据。
- 投票是匿名的。
- 投票人必须打开证据才能获得对索赔的投票权。
- 投票人可以对多个索赔进行投票，然后一起成批提交所有索赔投票，这是为了节省时间和汽油费。
- 如果投票人认为索赔无效，则应予以拒绝，则他们应输入“0”作为补偿索赔人的DAI金额。 提交“0”与投票“否”同义，表示拒绝该索赔主张。
- 投票大于“0”的任何值都等于投票 “是”，这意味着该索赔是有效的。 该值还代表投票人认为索赔人应得到的赔付金额。

示例:
交易所遭到黑客攻击，各种保单持有人提交了三个索赔申请。为了简单起见，他们所有人都请求同等的1.000 DAI的索赔金额。
在审查了证据之后，一名投票人得出以下结论:

- 索赔1有效，但仅适用于500 DAI，因此投票人输入 500 DAI;
- 索赔2有效，对全部1.000 DAI 的索赔有效，因此投票人输入 1,000 DAI;
- 索赔3是欺诈，因此无效，投票人输入 0 DAI。

用户按下“投票”按钮，该按钮将在一次交易中提交所有3个投票，从而节省了汽油费。

- 投票流程结束后，裁定给索赔人的最终赔付金额由vBMI代币的加权平均值及其投票结果决定。
- 一个索赔需要通过66%的多数同意，否则索赔将被拒绝。
- 投票占多数的投票人获得信誉分数，并参与奖励的分配。
- 投票占少数的投票人失去信誉分数（如果少数投票人的比例不超过10%，那么少数投票人也将失去部分质押）。
- 投票权 = 质押的vBMI x 信誉分数
- 如果索赔被拒绝，则索赔人可以提出上诉。
  - 要提出上诉，上诉人必须另外锁定其上诉价值的1%的stkBMI

上诉和受信任的投票人

- 只有“受信任的投票人”才能对上诉进行投票。
- 受信任的投票人是信誉系统中所有活跃投票人 (他们至少多数投票过一次) 分数最高的15%。
- 要成为受信任的投票人，您必须：
  - 信誉分数在系统中的前15%
  - 信誉值高于2.0x
- 在所有其他方面，上诉以与普通索赔流程相同的方式处理。
- 上诉不能再次上诉，其结果是最终的。 索赔人可以提出新的索赔，即使其在上诉阶段被拒绝，其保单也不会消失。

信誉系统

信誉改变投票权。

- Every每个用户的信誉分数的起始值是1.0x
- 信誉可以低至0.1x，高至3.0x
- 当用户投票占多数时，他们将获得信誉;
- 当用户投票占少数时，他们将失去信誉;
- 少数投票人比例越小，少数投票人失去的信誉就越多。例如，如果投票结果2%投“是”，98% 投“否”，则损失的信誉将是严重的。
- 无论多数投票者比例多大或多小，多数投票者总会获得线性信誉值的增加。

信誉评分系统

#vBMIvoting yes = 用于投票“是”的vBMI的数量
#vBMIvoting no = 用于投票“否”的vBMI的数量
VY = 用户投票为“是”的比例
VN = 用户投票为“否”的比例
%VMA = 多数投票用户的百分比 (%)
%VMI = 少数投票的用户的百分比 (%)

$$VY = \frac{\text{vBMI voting yes}}{\text{vBMI voting no} + \text{vBMI voting yes}}$$

$$VN = 1 - VY$$

比较“no”投票数和“yes”投票数

如果投票人投票“yes”占多数，则：

> %VMA = VY IF VY >= 50%
> %VMI = VY IF VY < 50%

如果投票人投票“no”占多数，则：

> %VMA = VN IF VN >= 50%
> %VMI = VN IF VN < 50%

用户信誉

> URx_{n+1} = 在投票n之后投票人x的信誉分数
> URxn = 当投票n时，投票人x的信誉分数
> %VMI = 投票人投票为少数时的百分比 (%)
> %VMA = 投票人投票为多数时的百分比 (%)

如果投票人的投票为少数

> $$URx_{n+1} = URxn - \frac{(1- (\%VMI * 2))^2}{2}$$
>
> URx_{n+1} 不能低于 0.1

如果投票人的投票为多数

> $$URx_{n+1} = URxn + \frac{\%VMA}{20}$$
>
> URx_{n+1} 不能高于 3

示例：

- 投票结果 = 45% yes / 55% no
  - 多数投票人: $URx_{n+1} = URxn + 0.0275$
  - 少数投票人: $URx_{n+1} = URx - 0.005$
- 投票结果 = 30% yes / 70% no
  - 多数投票人: $URx_{n+1} = URxn + 0.035$
  - 少数投票人: $URx_{n+1} = URx - 0.08$
- 投票结果 = 1% yes / 99% no
  - 多数投票人: $URx_{n+1} = URxn + 0.0495$
  - 少数投票人: $URx_{n+1} = URx - 0.48$

投票惩罚

为了有资格进行投票，用户需要使用stkBMI代币，并将其锁定在投票合同中，以换取vBMI投票代币。

当投票人的投票占**极少数票数**时， 将失去他们锁定BMI的一部分。

当投票人投票占比不超过10%时，属于极少数票数 。

> **如果 %VMI < PT 适用惩罚**
> **PT =** 以百分比 (%) 表示的惩罚门槛
> **PT** = 11%
>
> **投票惩罚 = PT - %VMI**

示例1
投票结果 = 1% yes / 99% no

投票惩罚 = 11% - 1%
投票惩罚 = 10%

用于投票的10％ vBMI，将被没收并添加到再保险池中。

示例 2
投票结果 = 90 % yes / 10% no

投票惩罚 = 11% - 10%
投票惩罚 = 1%

用于投票的1％ vBMI，将被没收并添加到再保险池中。

示例 3
PT = 21 %
投票结果 = 85% yes / 15% no

投票惩罚 = 21% - 15%
投票惩罚 = 6%

用于投票的6％ vBMI，将被没收并添加到再保险池中。

投票奖励的数额

- 要提出索赔，索赔人必须存入请求的索赔价值的1%。
- 每个索赔分配的投票奖励等于索赔人锁定的BMI (索赔价值的1%) 或Pc。

  Pc = 存入到再保险池的协议费 (以%表示)
- 如果索赔人的索赔成功，则将所存入的1%BMI退还给索赔人，用 Pc 向投票人奖励。 如果索赔人的请求失败，则将索赔人锁定的1%BMI 作为奖励分给投票人。

示例

1. **第一阶段**
   - 1.1. 提出了1,000,000 USD 的索赔
   - 1.2. 当索赔人支付保单费用时，他支付了4%的保费 (40,000 USD) - Pc等于20%，即8,000 USD。
   - 1.3. 用户必须锁定价值10,000 USD的BMI以开始索赔 (索赔价值的1%)
   - 1.4. 如果用户的索赔请求被批准，则将退还其锁定的 10,000美元的BMI，投票人的奖励为 8,000 DAI (Pc)。
   - 1.5. 如果用户的索赔请求被拒绝，则没收其锁定的10,000美元的BMI，其中的8,000美元作为奖励分给投票人 (以BMI形式)，其中的2,000美元分配给质押人 (以BMI形式) 。
2. **上诉阶段**
   - 2.1. 索赔人开始第二阶段 (上诉阶段)
   - 2.2. 索赔人必须另外锁定其请求的索赔金额的1%，即价值10,000美元的BMI
   - 2.3. 上诉阶段的其余部分与第一阶段的操作相同

投票人奖励的计算

> **#BMIvr** = 在特定阶段分配的BMI投票奖励代币数量
> **#BMIPc** = 在缴纳保费时，以Pc形式收取的BMI数量
> **#BMIlock** = 索赔人开始索赔时锁定的BMI数量
>
> **#BMIvr** = min(#BMIPc , #BMIlock)

成功索赔支出的计算

FA = 支付给索赔人的最终金额
APTVx = 投票人x 提出的赔偿金额
VRx = 投票人x 信誉分数
vBMIx = 投票人x 在投票中使用的vBMI

$$FA = \sum_{1}^{n} \left(\frac{URx * BMIx * APTVx}{\sum_{1}^{n} (UR_1 * vBMI_1 + UR_n * vBMI_n)} \right)$$

投票占多数的投票人的奖励分配

奖励分配给投票占多数的投票人。分配基于投票人的信誉得分和他们用来投票的vBMI数量。

VRx = 投票人 x 的信誉分数
vBMIx = 投票人x 在投票中所使用的vBMI
%VPR = 投票人x参与投票奖励分配的百分比%
#BMIvr = 在特定阶段用来分配的BMI 投票奖励代币的数量
0xVx = 分配给0x地址所有人(投票人x) 的BMI代币

$$\%UPR = \left(\frac{URx * vBMIx}{\sum_{1}^{n} (UR_1 * vBMI_1 + UR_n * vBMI_n)} \right)$$

0xUx = #BMIvr * %UPR

bridge.

联系我们

www.bridgemutual.io

bridgemutual.medium.com

twitter.com/bridge_mutual

t.me/bridge_mutual