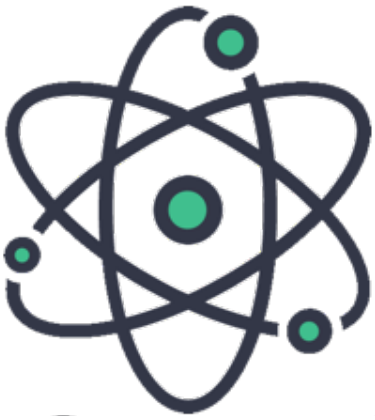


MetaDefender

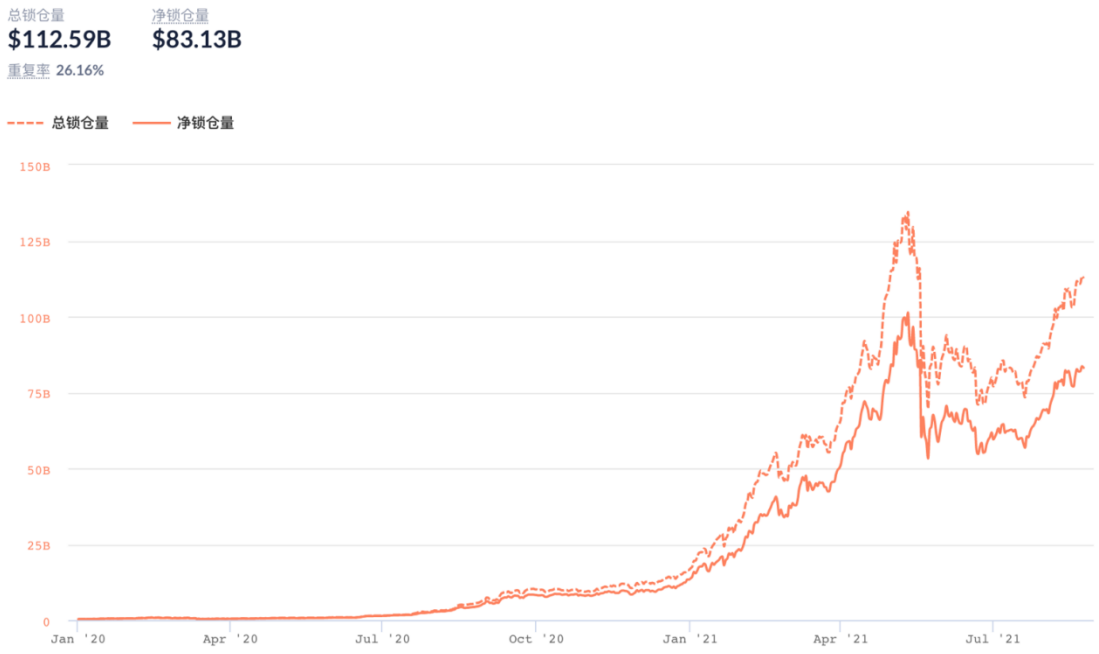
Metaverse 时代的去中心化数字资产保险

目录

引言

随着 web3.0 时代的到来，越来越多的人开始使用去中心化网络来存储、交流内容与价值。数字资产的概念从早期单纯的虚拟货币，逐渐扩大到链上非同质资产、声誉资产、链上身份及隐私、分布式存储的内容资产等领域，且仍在持续外延。

去中心化金融（DeFi）的发展大大丰富了区块链的生态，在过去的一年里创造了近 200 亿美元的总市值。但与此同时爆发的链上资产安全问题也不容忽视。截至 2021 年中旬，基于智能合约本身漏洞造成的数字资产损失事件已经遍及所有主要 DeFi 公链，金额累计超过 5000 万美金。其中大部分协议甚至经过了严格的第三方机构安全审计。由于区块链协议的开放性，很多攻击者在多个自身本无漏洞的合约之间跨域交互，让普通使用者蒙受巨大的损失。



DeFi 项目总锁仓量（美元）

Metaverse 作为互联网的终极形态，正在成为不可阻挡的趋势。未来以加密形态承载的价值将连接人类的生活、社交甚至工作。为加密货币以外更广义的数字资产提供保障将成为一种刚性需求。因此保险就显得尤为重要。

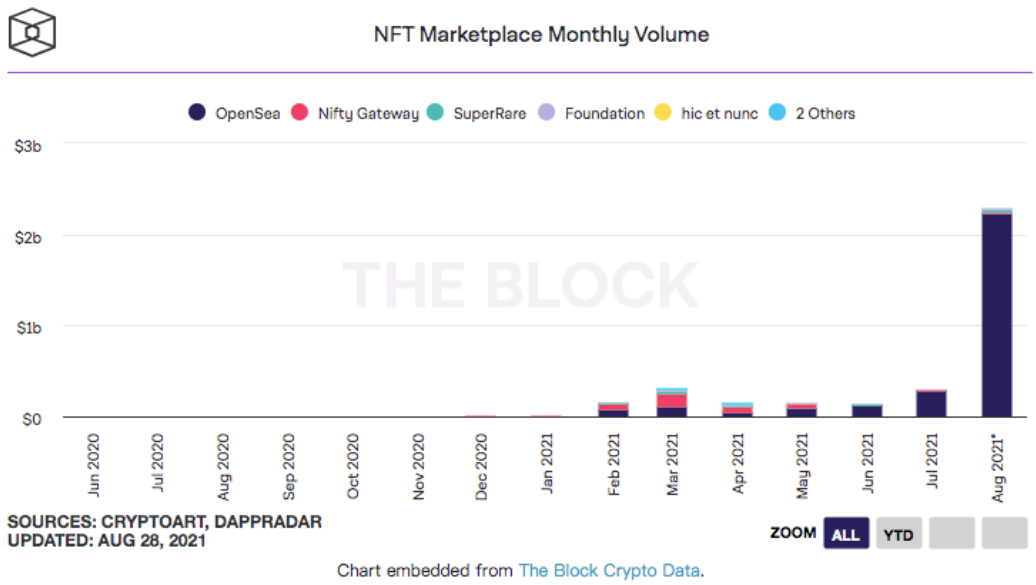
保险是一种有助于在整个社会重新分配风险的工具。但是承保风险需要大量的资本，因此这个行业就被寡头公司所垄断，这些公司有能力为潜在的索赔义务提供充足的资金保障。保险公司的盈利能力取决于保费收取的金额，尽管监管严格但是还存在大量问题，因为保险公司有拒绝索赔的权利。此外保险公司对于新的风险保障是存在缺口的，保险公司依赖于数据对风险作出评估，进而决定是否对新的风险提供保障。去中心化金融（DeFi）就是很好的例子。DeFi 的飞速发展和创新的流动性挖矿带来了链上资产总价值的大幅增长。流动性提供者为了利益愿意为 DeFi 产品提供资金，但是往往没有全面了解潜在的安全风险。很多项目虽然经过了安全审计，仍然是黑客攻击的目标，导致用户资产损失巨大。

下表为近年来著名的 DeFi 安全事件汇总：

序号	时间	协议	损失（百万美元）	漏洞描述
1	2019.7.30	Synthetix	8.1	预言机缺陷导致错误价格
2	2020.2.15	bZx	1	Flsh 贷款和预言机操纵
3	2020.2.18	bZx	0.64	预言机操纵
4	2020.3.12	Maker	9	人为操纵
5	2020.4.18	imBTC Uniswap Pool	0.20	ERC777 Token
6	2020.4.19	Lendf.me	25	ERC777 Token
7	2020.6.28	Balancer	0.5	预言机缺陷导致错误价格
8	2020.8.4	Opyn	0.37	双重消费攻击
9	2020.9.6	SYFI	0.25	软件漏洞
10	2020.9.14	bZx	8.1	智能合约代码漏洞
11	2020.10.26	Harvest	25.0	Flash 贷款攻击
12	2020.11.7	Origin Protocol	7.0	智能合约代码漏洞
13	2020.11.13	Akropolis	2.0	Flash 贷款攻击
14	2020.11.14	Value Protocol	6.0	Flash 贷款攻击
15	2020.11.12	Pickle Finance	20.0	智能合约代码漏洞

16	2020.11.26	Compound	3.55	预言机缺陷导致错误价格
17	2020.11.30	Sushiswap	0.015	智能合约代码漏洞
18	2020.12.1	Compounder.Finance	12.3	内部操作
19	2020.12.14	Nexus Mutual	8	钓鱼攻击
20	2020.12.18	Warp Finance	7.76	预言机缺陷导致错误价格
21	2020.12.28	Cover protocol	4350ETH	代币增发
22	2021.2	Alpha Homora	37	Flash 贷款攻击
23	2021.8.10	Poly Network	610	智能合约代码漏洞

简单来看，网络黑客攻击已经成为 DeFi 生态发展的最大威胁。除了解决这个问题通过技术手段，另外保险从本质上来看也是对这个风险的另外一种有效手段。经过深入调研之后，目前 DeFi 市场上保险赛道还是处于起步阶段。根据 Debank 数据，目前所有 DeFi 项目近 500 个项目中，保险赛道相关项目只有 6 个，其中较为关注的项目只有三个 NXM、Cover、Armor。



近期 NFT 项目数据增长

在过去的几个月里，围绕艺术和游戏的非同质代币（NFT）的热度开始升温，支持此类代币交易的市场活跃在交易者数量和交易量方面都达到顶峰。八月份

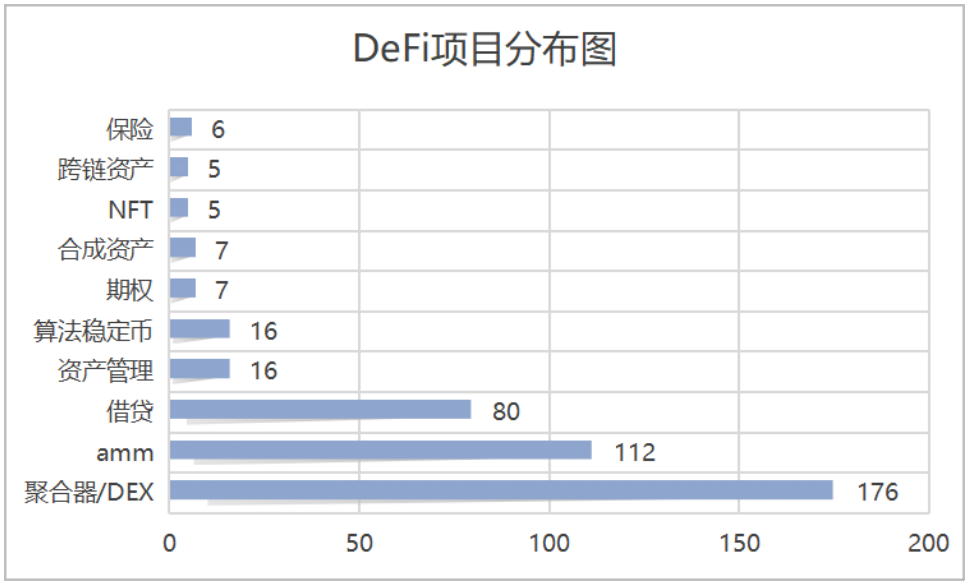
NFT 市场交易者数量急剧上升了 87%。最大的贡献者是 OpenSea 和 Rarible；占这一增长的 76%。NFT 将会是下一个增长点，从目前数据也可以直观看出。

MARKETPLACES

	MARKET	TRADERS	VOLUME
1	OpenSea ETH • Polygon	322,149	$4.086B
2	Axie Infinity ETH	500,611	$1.724B
3	CryptoPunks ETH	4,746	$1.166B
4	NBA Top Shot FLOW	434,055	$672.683M
5	Rarible ETH	70,766	$198.867M
6	SuperRare.co ETH	4,569	$104.769M
7	Sorare ETH	27,523	$97.421M
8	AtomicMarket WAX	659,370	$79.408M
9	Foundation ETH	15,250	$67.343M
10	PUNKS Comic ETH	2,379	$48.357M

NFT 赛道明星项目

飞速发展的 NFT 市场和元宇宙生态吸引了大量资金，但作为一个比 DeFi 更年轻的市场，合约的完备性和金融系统的安全性，都没有得到过时间的检验，蕴含的安全风险是不言而喻的。



从数据上来看，目前 DeFi 市场还是在高速发展之中，但是现有保险项目所覆盖的 DeFi TVL 总体水平还是很低，根据 Debank 最新数据显示，目前保险项目总锁仓量 194.8 Million，仅占全行业的 1%左右。自保险赛道的明星项目 Cover

被黑客攻击之后，锁仓量更是直线下滑。总体来看，生态的迅速发展催生了网络风险，市场上需要更多的保险产品来提供更为全面的风险安全保障。

MetaDefender 是第一个为去中心化 NFT 协议、区块链游戏资产、乃至 metaverse 中的数字资产提供合约安全保障的金融产品。在 MetaDefender 中，每一个市场的参与者都可以自由地投保或承保，并随时实现资本退出。

MetaDefender 实现了承保资金深度的聚合，且能够保证不同阶段承保人风险和收益的对等性。项目采用升级的恒定乘积模型 2.0 版，来完成被承保资产风险定价的发现。

MetaDefender 将可以支持数字资产的发行人自主选择保险费率、承保与理赔币种和承保事项范围，并支持一键式自建保险池。未来的安全预言机将致力于实现 dapp 的 API 监控，以实现理赔的完全去中心化。

第一章 保险模型设计

一套完备的、用户友好的去中心化保险机制，应该至少包括共识层、算法层、资本层和应用层，分别管理保险的基本逻辑、保单的风险定价、承保资本的进出和保障的生成。

由于不同的数字资产来自于相互独立的链上协议，我们认为，不同资产受到攻击或发生损失的概率，主要取决于其合约本身的安全性。因此，不同合约资产的风险定价是不同的，能够吸引承保资产的能力也不同。独立的项目应有独立的资本池。在确定了被承保项目之后，一份保单里应至少包含以下参数：

地址变量	保单受益人
数字变量	保单有效期
数字变量	保单到期日
数字变量	保单承保金额
状态变量	理赔状态

每个项目对应的资本池，具有不同的承保和偿付能力。参考欧盟保险公司偿付资本监管框架，借鉴巴塞尔协议的“三支柱”风控体系，每个开放的资本池应至少保证以下三个维度信息的公开可查：

第一支柱：定量要求	第二支柱：监管行为	第三支柱：市场纪律
准备金要求	内控和风险管理原则	披露
最低资本要求（MCR）	监管审查程序	透明度
偿付能力资本要求(SCR)		

最低资本要求，是指保险公司在遇到不利市场情况时，仍能够维持正常偿付能力的资本要求，主要限制保险公司对保费的吸纳；偿付能力资本要求，是指保险公司为应对重大不可预见损失，保证对保单持有人的赔付而持有的资本，主要用来规制保险公司的对外投资。

我们认为每个资本池应至少披露三项内容：

1、累计注入资本，代表单位资本可以捕获的保费收益；

2、当前在池资本，代表该资本池当前的整体承保能力；

3、当前可用资本，代表着该资本池目前的剩余承保能力，并将决定着保费的变化

保险经营的是风险与概率，因此应尽力避免单个被保险对象的保额过大，使风险丧失离散性。每个保单的保额上限应遵循以下公式：

$$C_{coverage} <= \eta \cdot (P_{inpool} - P_{occupied})$$

η为该保费池的资本离散系数。

每个保费池应允许任何人为其提供资本，成为承保人。承保人承担项目遭受攻击后的偿付责任风险（远期），并捕获保费收益（即期）。由于不同的承保人加入的先后顺序不同，保险机制应该确保每笔收益只能由为其承担风险的人获得。

资本的自由退出一直是去中心化金融的灵魂，但保险工具特有的属性似乎与之相矛盾。在投保-承保的关系中，缴纳保费-承保人获得收益，是即期且确定的；而发生风险-承保人履行义务，是远期且不确定的。而且随着加入资本池的承保人数量的增多，每单位资本能捕获的保费金额和对应分担的承保义务亦不同。

保险的以上特性要求我们必须维持承保资本池的相对稳定性，且只有不断扩大的资本池才能为 metaverse 参与者提供更好的承保深度。所以我们认为，进入资本池的承保资本应视为一级市场资本，资本池可将每个资本提供者（承保人）对应的资本份额二次代币化，并允许其转让流通。

第二章 项目代币经济模型

MetaDefender 项目拥有两种类型代币：

一是项目原生代币 MetaDefender Token（缩写为 MDF），是项目合约推荐的承保及理赔标的币种，以及本项目的治理代币。

二是承保代币构成某个项目的保险资本池后，所映射的资本凭证代币 stakedToken（简称 sMDF），可作为资本提供/收益捕获的凭证，在二级市场兑换回原承保代币，实现资本退出。

MDF 的发行总量是固定的，为了提供足够的流动性，我们将在 V1 版本中推荐使用它作为承保、投保的标的资产。

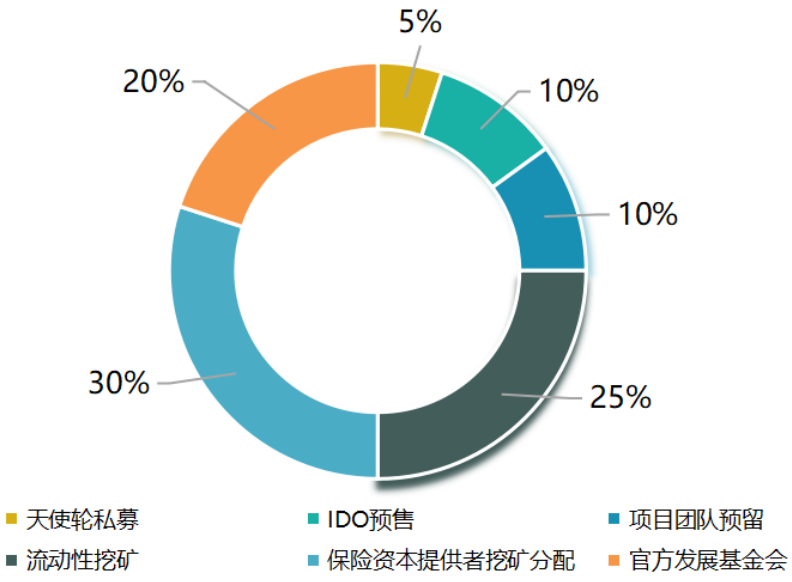
假设一名承保人希望为以太坊上的著名 NFT 交易所 opensea 承保，该承保人找到 opensea 的保费池，将 1MDF 注入其中；协议会铸造一枚名为 sMDF_opensea 的资本代币给他。

持有这枚 sMDF_opensea，承保人可以在此后该资本池收到每笔保费 W 之后，获得如下收益：

$$R = W/sMDF_{opensea}.totalSupply()$$

为了最小化链上处理成本，sMDF 持有人累计捕获的收益将会被储存在合约里，由持有人自行统一提取。

MDF 总供应量中，天使轮私募预售 5%，IDO 预售 10%，创始团队预留 10%；流动性挖矿分配 25%，保险资本提供者挖矿分配 30%，官方 metaverse 发展基金留存 20%。



代币释放规则如下：

天使轮私募和 IDO 份额：项目上线解锁 25%，剩余部分按季度两年内线性解锁；

创始团队份额：项目上线解锁 20%，剩余部分按季度两年内线性解锁；

Metaverse 基金会份额：项目运行早期，基金会义务为第一批保险项目添加流动性并锁定；MDF DAO 成立之后，基金会资金的使用权完全交付 DAO 投票管理。

同时，MDF 也是 MetaDefender 项目的治理代币。所有持币人都有权加入 MetaDefender 理事会，对基金金库使用、重大合约升级、重大争议事项进行投票表决。

第三章 保单的风险定价及保单生成

按照经典保险学的模型，保单的保费与保单保额的数学关系为：

$$\mathrm{Fee} = r \cdot \mathrm{C}_{coverage}$$

r 为保单的费率，代表了保单生成当前，被承保事项的风险定价。

在保险精算中，风险定价的底价，是根据历史上对承保事项出险概率的长期监测，得到的保险公司盈利是数学期望恰好为 0 时的保险费率：

$$\mathrm{R}_0 \cdot \Sigma \mathrm{C}_\mathrm{i} = \Sigma \mathrm{C}_{claimed}$$

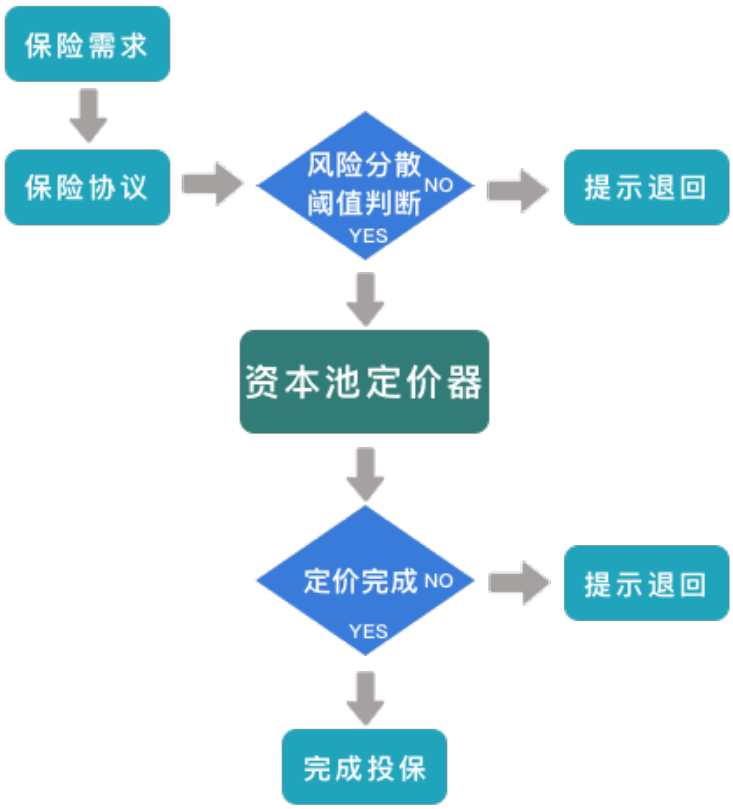
但我们需要意识到，去中心化网络乃至 metaverse 的实践周期和样本厚度，还远远未能达到经典保险模型要求的数量级。目前我们只能参考相似市场、相似产品的风险定价，作为 MetaDefender 协议的长尾风险定价。

目前 DeFi 领域最大的保险提供商 Nexus Mutual，对头部 DeFi 协议（如 uniswap、compound 等）给出的保费费率是 2.6%，基本代表了目前去中心化网络生态的风险底价。

MetaDefender 支持任何协议构建自身的保险池，并自定义初始风险定价。我们相信自由博弈的市场最终会让价格趋于中性。参考 Nexus Mutual 为我们做出的范例，我们会将第一批受保护协议的初始费率定为 3%。

另一方面，保费的高低也反映了保险的需求度。投保行为体现了保险需求，同时消耗了剩余可偿付资本。MetaDefender 使用了升级版的恒定乘积模型，来拟合两者的数学关系：

$$r \cdot (P_{inpool} - P_{occupied}) = K$$



显然，随着保险池中的资本不断被消耗，在新的资本提供者进入之前，保险费率会逐渐升高——因为源源不断的需求意味着市场对风险的共识。

当然，高费率也意味着资本提供者能够捕获更多的保费收益，吸引更多的资本提供者，将保险降低到合理水平。

我们认为，在保险中，风险是客观存在的，并不绝对随着承保资本深度的增加而可以被消除，尤其在一个相对早期的市场里，一定的风险底线是必要的。

因此，目前 MetaDefender 默认受保护协议纳入时的初始风险定价，是该协议的风险底价。当资本池深度增加，触及风险底价之后，K 的值会自动增大，亦即我们即将论述的弹性承保资本。

第四章 弹性承保资本

MetaDefender 允许任何人向任一承保资本池添加资本，参与捕获保费利润。为了增加资本利用效率，协议可以让高风险偏好者为所有受保护项目承保，以捕获全局利润。但相应地，任一项目出现风险也会导致资本受损。

资本的注入，或已占用资本的释放，会导致保险费率沿着恒定乘积曲线发生滑动。当触达最低风险定价之后，费率 r 不再下降，转而增大恒定乘积 K。

假设第 i 个资本提供者注入资本之前的恒定乘积为K_{i-1}，初始保费（即最低风险定价为r_0）：

$$r_{i-1} \cdot （P_{inpool} - P_{occupied}） = K_{i-1}$$

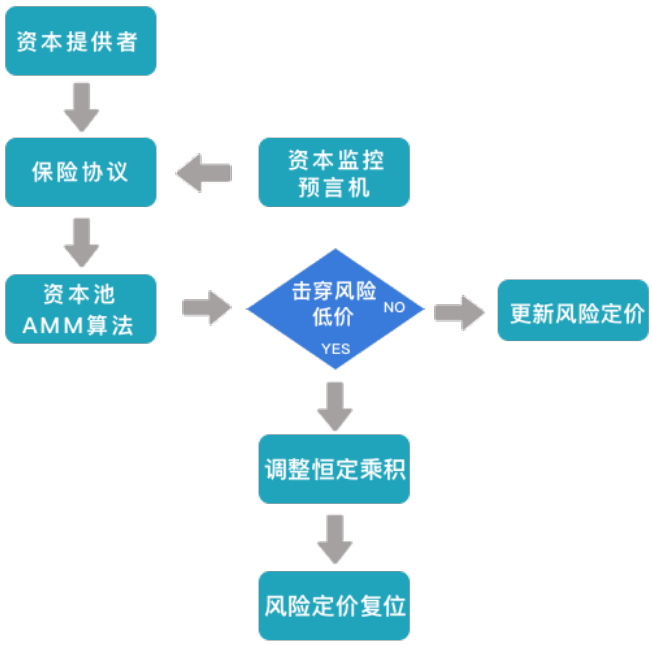
注入资本P_i后，可用资本变为$P_{inpool} - P_{occupied} + P_i$，协议试算：

$$r_{i-test} = K_{i-1}/P_{inpool} - P_{occupied} + P_i$$

当$r_{i-test} \geq r_0$，则恒定乘积维持K_{i-1}不变，费率$r_i = r_{i-test}$；若$r_{i-test} < r_0$，则：

$$r_i = r_0$$

$$K_i = r_0 \cdot （P_{inpool} - P_{occupied} + P_i）$$



即使没有新的资本流入，如果某一保费池所保护的项目长期未出现风险，大量保单到期，释放了可用资本，也会导致试算保费费率低于最低风险定价的情况。这种情形下，协议也会自动执行上述语句。

第五章 市场分析

我们对现有产品市场做了针对性调研分析，按照产品形态和项目方向大致可分为三类。一、互助性保险；二、点对点保险；三、金融衍生工具。

	互助性保险	点对点保险	金融衍生工具
产品	NXM	Cover	Opyn
资本与流动性			
共同资金池	是	否	否
完全抵押	否	是	是
流动资金	用户资金到资金池	双面市场	双面市场
灵活性			
新产品	高	底	高
风险覆盖率	高	底	高
索赔评估	投票	不投票	不投票
定价			
极限风险率	好	一般	一般
货币风险	一般	好	好

现有保险产品比较

经过比较研究，我们发现目前市场现存的保险项目主要存在以下短板：

（1）产品局限性

中心化定价：行业处在相对早期，缺乏风险数据支撑，保费定价基本由项目方决定。

KYC：部分协议针要求用户进行 KYC，阻挡了 10 多个国家的用户，这与区块链自由开放的精神矛盾。

缺少跨链协作：导致新兴公链上的项目普遍缺乏保障。

缺少针对 NFT 项目的保险：目前的保险协议普遍集中于 DeFi 合约安全领域，而更为广阔和多元的 NFT、metaverse 世界的异构资产，目前无人保障其安全。

（2）缺乏基本风险管理

风险管理是所有保险业务的核心，目前市场上 DeFi 保险产品有很大空间提升其自身风险控制能力。

保险协议自身的网络安全问题：目前市场上已经出现了保险协议自身被黑客攻击事件。例如 Cover 被攻击之后用户对保险自身网络安全问题产生了很大质疑。因此保险协议自身如何更好的维护自身网络安全是重中之重的问题。

索赔评估：现有的索赔评估过于粗略，没有对损失进行量化评估。

风险定价缺乏弹性：目前的链上保险协议，对风险的定价基本机械照搬了传统的保险数学模型，缺乏一种适应加密世界的机制。

（3）资本效率低下

资本效率是所有金融公司的重点，但是目前 DeFi 保险产品资本效率低是一个关键问题。

注入保险协议的资金，本质上属于长期资本，不应该随意移动。但也正因为如此，造成了巨额的资本闲置。由于整个行业处于早期，用户教育的不足导致保险业务量没有实质性的增长，承保资本能够捕获的收益低于同期二级市场收益，进一步造成资本外流和承保能力枯竭。

（4）承保流动性过于分散

主要表现为：完全代币化的承保资本，每一份资本能提供的保障期限和额度都是离散的，无法确保投保人每时每刻都能获得全额保障（不考虑保费的前提下）。例如 Cover 协议的承保人通过抵押稳定币而生成的承保资本，都有一个有效期，这个有效期完全取决于对应稳定币抵押的时间。因此用户长期保险的需求很难被满足，也缺乏一个集中的流动性聚合池，来为不同时间前来投保的用户提供统一的保障。

第六章 竞争优势

（1）财务信息透明

打造一个好的保险平台的一个关键因素是财务状态的健康，披露资金的分布情况以及是否有足够的保费浮动来支付潜在的索赔。由于区块链是一个分布式账

本，每个节点都有相同的链上数据记录抄本。当数据发生变化时，每个参保人都可以看到同步更新的数据，使每个基金的运作公开透明。因此，在 MDF 网站首页将有专门的模块来披露相关信息，并提供每季度准确的实时财务状况，例如风险因素、最低资本要求、代币价格历史数据、索赔评估摘要，以及锁定/流通代币的数量等相关重要财务信息。

（2）去中心化社区治理

未来会支持元宇宙项目运营者自主发布保险产品，自定义风险初始定价、理赔范围和赔付资产种类。

（3）产品升级

我们会根据市场反馈以及用户体验进行对产品的持续改进升级，推出更多核心产品，对更多的优质项目提供安全风险保障，满足更多用户的需求。我们希望随着项目、社群的持续发展，社群用户会持续积累，并为项目改进、产品升级提供宝贵意见。

（4）网络安全

DeFi 最大的风险就是面临的网络安全风险，保险存在的意义就是解决这些为用户带来损失的风险问题，为用户提供安全保障。作为风险管理的平台，自身的安全风险保障更为关键，不能让 Cover 事件重演。MDF 会定期邀请第三方独立审计公司对保险的智能合约进行安全审计，消除潜在的合约漏洞，公告审计结果；其次 MDF 有相关安全软件来检测网络的健康状态、链上活动、私钥管理等相关细节以增强平台的安全性。

（5）无 KYC

目前市场上最火的明星项目 NXM 由于自身的 KYC 问题，导致众多的用户无法准入。我们会用从用户角度出发，解除此类相关限制。

（6）提高资本效率

MetaDefender 支持同一份资本为所有被保险协议提供流动性支持，即所谓全局流动性提供者；

为单一保险池提供资本，并获得提供凭证 sMDF 的参与者，可以用 sMDF 参与资本挖矿，在不影响保险池资本稳定性的前提下，扩大资本收益。

（7）聚合的流动性

我们把所有资本提供者的资本聚合在了一个智能合约控制的聚合池中，池内的可用资本没有时间限制，用户可以在任意时间选择任意的投保期限，不会出现“没有合适的保险可买”的情况。

第七章 项目路线图

按照我们的计划，MetaDefender 的开发是一个系统工程，需要持续的努力和不断的改进，未来一年整个项目将按照以下计划进行。

2020 年 5 月项目团队组建，成员为区块链行业精英在相关领域深耕多年，来自与币安、火币等团队，有丰富的行业经验及市场预测能力。项目团队开发能力强，曾毕业于麻省理工、芝加哥大学、新加坡国立大学、清华大学。

2021 年 2 月项目设计完成，确定项目经济模型；保险算法；理赔机制及未来升级路径。

2021 年 9 月 IDO 开始。IDO 预计该项目首次融资 80 万美元，用于技术开发和市场开发。首批发布平台是 Cardstarter、Daomaker 和 Polkastarter。

2021 年 10 月产品内测。在 BSC 上发布产品内测版本并建立初始流动性；确定第一批受保护的协议；开启媒体与去中心化社区之间的全面合作。

2022 年 2 月多链部署。开放社区投票，扩大受保护协议的范围；根据项目进度，将我们的产品部署在以太坊主网、HECO、Polygon 等网络上；与专业的区块链安全公司合作；更多的媒体、社区和交易所合作。

2022 年 11 月产品升级。支持任何去中心化协议构建者自由发布自己的保险产品；提高保险事件的准确性；为 NFT 资产提供借贷、证券化和资本化等高级金融服务。

结语

MetaDefender 是首个利用区块链技术，为去中心化 NFT 资产协议、乃至 metaverse 时代泛数字资产提供保险服务的金融工具。我们首创了由弹性的承保资本决定风险定价的算法机制，并兼具了承保流动性的聚合性和资本进出的自由性，致力于成为 metaverse 时代保障数字资产安全的基础性金融设施。