



一种基于智能合约的  
去中心化杠杆借贷协议

**RooLend . Finance**

RooLend.Finance Team

2021/05/20

# 目录

## 一、概述

|                       |    |
|-----------------------|----|
| 1.1 去中心化金融 .....      | 01 |
| 1.2 去中心化金融的不同形式 ..... | 02 |
| 1.3 去中心化借贷协议 .....    | 03 |

## 二、Roolend.Finance

|              |    |
|--------------|----|
| 2.1 存币 ..... | 04 |
| 2.2 借币 ..... | 05 |
| 2.3 取回 ..... | 06 |
| 2.4 偿还 ..... | 07 |
| 2.5 利率 ..... | 08 |

## 三、清算和风控

|                 |    |
|-----------------|----|
| 3.1 清算和风控 ..... | 09 |
|-----------------|----|

## 四、协议架构

|                |    |
|----------------|----|
| 4.1 协议架构 ..... | 10 |
|----------------|----|

## 五、治理通证

|                |    |
|----------------|----|
| 5.1 治理通证 ..... | 11 |
|----------------|----|

## 六、附录

|                |    |
|----------------|----|
| 6.1 名词解释 ..... | 12 |
|----------------|----|

# 1.1 去中心化金融

DeFi是去中心化金融的缩写，也称为开放式金融。它实际上是指用于构建开放式金融系统的去中心化协议，该协议旨在使世界上任何人都可以随时随地进行金融活动。

在现有的金融体系中，金融服务主要是由中央组织控制和调节，并且是社会最基本的服务，例如存款、取款、借贷和衍生工具。DeFi试图通过分布式开源协议建立透明、可访问的点对点金融系统，以最大程度地降低信任风险，并使参与者更轻松、便捷地获得金融服务。

与传统的集中式金融系统相比，这些DeFi平台具有三大优势：

- A.** 个人无需信任任何中介机构即可在计算机和代码上重建新的信任；
- B.** “无许可”参与，任何人都可以创建DeFi应用，任何人都可以使用它们。与当今的金融不同，没有门卫或冗长的账户。用户直接通过其加密货币钱包与智能合约进行交互。每个人都有访问的权利。
- C.** 所有协议都是开源的，因此任何人都可以在协议上合作以开发新的金融产品并在网络效应下加速金融创新。

DeFi是一个相对笼统的概念，包括：货币发行、交易和结算、借贷，交易、投资和融资等。

## 1.2 去中心化金融的不同形式

就像存在许多不同的去中心化应用一样，也存在许多不同的去中心化金融应用，包括：

- 1、支付——支付类型的去中心化金融应用一般有自己的数字货币，用户可以使用它们进行交易，也会提供钱包地址让用户持有这些数字货币。
- 2、借贷——去中心化借贷是尝试让经济去中心化的一个核心应用。不像现在这样，人们得去银行获取房贷，去中心化借贷目标旨在允许人们能从更多资金出借人那里获得贷款，民主化整个借贷过程。
- 3、稳定币——稳定币是一种具有价格稳定特性的资产，因此适用于诸如交易媒介、记账单位和价值存储的功能。相比诸如比特币、以太坊以及其他波动性较大的数字资产，稳定币因为价格稳定的特性在数字资产领域得到越来越多的关注。
- 4、去中心化交易所——去中心化交易所允许用户交易比特币和以太坊等数字资产。去中心化交易所是为了解决中心化交易所问题而产生，在中心化交易所用户不拥有自己的私钥，所以无法掌控自己的财产。

目前，DeFi项目已有数千个，除了以上四种类型，还有去中心化钱包、保险平台、预测市场、身份认证等都是属于 DeFi 的范畴。我们可以看到一个全新行业的早期阶段，整个 DeFi 生态系统正在蓬勃发展时期。

## 1.3 去中心化借贷协议

在 DeFi 世界，去中心化借贷系统是一个极其重要的赛道，也是整个 DeFi 体系里面的基石系统，它能够模拟现实世界里的金融系统，了解不同用户的资金需求，并提供用户间相互资金融通的平台；它能够无边际成本的支持符合同质化代币标准的所有加密资产之间的借贷，并能够根据市场供需，自动化的计算与调整市场的借贷利率。

借贷的实质是促使参与者具有交易资产时间价值的能力，交易资产的时间价值对双方都有利并创造非零和财富。对于区块链数字资产，当今存在两个主要缺陷：

- 1) 借贷机制极为有限，这会导致资产定价错误。
- 2) 区块链资产由于巨大的风险而产生负收益，但没有自然利率来抵消这些费用。

中心化交易所允许客户交易区块链资产，并在交易所中内置了“借贷市场”，这些是基于中心化系统的信任（您必须相信交易所不会被黑客入侵，潜入您的资产或被错误地关闭您的头寸），并且仅限于少数（最主流）资产。最后，余额和头寸是虚拟的；您无法在链上移动头寸，例如无法用这些头寸来访问 DApp。

P2P市场协议促进了市场之间的抵押贷款和无抵押贷款直接参加。不幸的是，权力下放迫使产生大量成本和摩擦；在每个经过审查的协议中，贷方都必须发布、管理和（如果抵押贷款）监督贷款报价和有效贷款，而还款通常很慢，并且是异步的（贷款需要资金，而这需要时间）。

基于以太坊公链，目前主要是两个借贷协议，Compound 和 AAVE。Compound 是以太坊区块链上的协议，允许用户借用和借出加密代币。其利率是根据每种资产的供求通过算法设置的。贷方和借方直接与协议交互，赚取（并支付）浮动利率，而无需与对等方或对手方协商期限，利率或抵押品等条款。Aave的起源可以追溯到2017年Stani Kulechov和一个开发团队于2017年11月在首次代币发行（ICO）中发布了ETHlend。AAVE是基于以太坊上的加密资产抵押借贷协议，在借贷类产品中排名前三，允许来自全世界的人公开透明的使用安全的借贷功能，享受区块链去中心化金融的服务。不仅首创无抵押借贷产品“闪电贷”为行业带来新兴动力，而且还整合了Uniswap市场中的交易对资产。

RooLend.Finance是基于智能合约的去中心化杠杆借贷平台，支持多个虎符公链上市种的质押借贷，用户通过在RooLend上进行借贷即可获得激励通证 ROO 奖励。ROO 将作为 RooLend 平台的枢纽，通过支持虎符生态链上资产相互通融的质押借贷，实现虎符生态资产间的相互通融与价值传递。

## 2.1 存币

存币指用户将其数字货币存入借贷平台，获取存款利息和流动性挖矿产出（ROO）。用户的存币可被其他用户借出，也可抵押存入的数字货币，借出其他数字货币。

假设，Alice首先存入其中一项资产，例如USDT，存入资金后，已存入的USDT将被添加到合并基金中，这称为总流动资金。该总流动性计算如下：

$$\text{总流动性} = \text{总可用流动资金} + \text{总借入资产}$$

总可用流动资金是指该资产可供借款人借入或贷出的可用流动性。总借入资产是借贷总额和累计借贷额的总和。总借入资产的计算如下：

$$\text{总借入资产} = \text{借入资产} + \text{利息}$$

Alice将收到rTokens，例如rUSDT，代表她存入总流动资金的USDT份额。rToken是用户贷款头寸的代币表示，是一种计息方式，这意味着rToken可以随着时间的推移会变得更价值。

## 2.2 借币

用户将资产存入并开启质押后，即可将存入资产作为抵押物，借贷任意BTC、ETH等主流资产，当用户借出其他资产后，需要支付借款利息，并且可以同时获得ROO挖矿收益。

在用户可以借贷之前，他们必须先将其一些可用于抵押的资产存入协议。存入此类资产后，用户会收到rToken，代表用户在资产池有份额。请注意，某些资产不被接受作为抵押，以保护协议的安全。即使这些rToken被用作抵押品，用户仍然会从中获得存款利息，因为其他用户正在从资金池借入标的资产，并向协议支付利息。

当用户借入并收到借入金额时，协议将计算借入份额占比，分担借入金额。借入资产份额代表用户借入金额的份额，此比值意义是已借入份额在总可借份额的占比。

## 2.3 取回

取回的操作与用户存入的操作是反向的，即用户向合约系统归还存款凭证代币 rToken或其他，并获得原始的存入资产。用户只有在有足够的总可用流动资金可提取的情况下才能提取该金额。要提取部分或全部存入金额，协议将会计算可提取份额，燃烧等于提款份额数量的rToken，然后向用户转移相应金额。

$$\text{可取回份额} = \text{可取回金额} * \text{总rToken} / \text{总流动性}$$

由于总流动资金因应计利息增加了时间，因此提款金额会随着时间的推移变得较小，因此消耗更少的代币来赎回相同的提款数量。如果用户提取所有存款金额，则用户将收到一笔提取金额。



## 2.4 偿还

为了偿还部分或全部借入金额，协议根据偿还额计算偿还份额，将还款额转入池中，并通过还款份额减少借入份额。偿还份额计算如下：

$$\text{偿还份额} = \text{偿还金额} * \text{总借入份额} / \text{总借入资金}$$

由于总借入资金会随着应计借贷利息的增加而增加，因此相同的还款额将等于随着时间的推移较小的还款份额，从而使借入份额减少。如果用户偿还所有借入的金额，用户将支付比原始金额更多的款项。

## 2.5 利率

借款方和贷款方的利率由利用率决定。

$$\text{利用率} = \text{借入资金} / \text{总流动性}$$

由于利用率反映了借用资产的需求，因此较高的利用率对应借贷成本或借贷利率较高。每项资产都有自己的基本借贷利率和最优使用率。因为累计的借贷利息将添加到总流动性中，贷方收到的rToken代表总流动资金的份额，较高的借贷利率对应较高的存款利率，可以计算为：

$$\text{存款利率} = \text{借贷利率} * \text{利用率}$$

产品简化利率模型，不设定浮动的借款利率，不考虑盈利，只保证账目借贷平衡，有：

- 借款总额为零（没有人进行借款），此时没有营收产生，存款利率为零；
- 借款总额增大，产生营收增多，存款利率也会提高；
- 借款总额不变（营收不变），存款总额增大，存款利率降低。

所以利率随着借款总额和存款总额的变动而变动。

## 3.1 清算和风控

清算过程涉及到 DeFi 借贷系统中重要的概念，即账户的健康因子（又称：健康指数），前面有提到到存款权益的确权是基于凭证的，而健康因子则与账户的借款额、抵押物相关，具体用公式表述为：

$$\text{健康因子} = (1 - (\text{借款额} + \text{借款利息}) / \Sigma(\text{抵押物} * \text{清算阈值})) * 100\%$$

当健康因子 接近0 时，将触发 DeFi 借贷系统对该用户账户抵押物的清算，清算个别用户是为了避免系统性金融风险的发生，因此借款人将受到系统的惩罚，而清算人则会获得一定的奖励。

加密数字货币市场波动大，借贷协议若不做足风险控制，将给协议及用户带来损失。

风控体系 3 层框架如下：

### 资产治理框架

市场中的资产须在 HSC公链上的 DEX 或 Hoo中有足够的交易深度，可以被清算的资产才可以被质押。

### 协议治理框架

参考 Hoo 来调整每个资产的质押率，且平均质押率均低于市场头部前三交易所和头部 DeFi 借贷协议。

### 清算治理框架

清算市场完全开放，代码开源，文档开放，任何链上清算合约均可以在规则内进行清算，让市场充分竞争，清算过程顺畅，避免风险。

# 4.1 协议架构

## 4.1 借贷池

借贷池是协议的核心合约。该合约管理所有状态并处理用户与借贷池的互动。互动包括存款，借贷，还款，提款和清算。

## 4.2 借贷池配置器

借贷池配置器提供了借贷池的配置功能，并实现了代币的配置。配置包括资金池配置和利率计算。

## 4.3 rToken

rToken合约管理rToken的铸造和烧毁。rToken代表用户的贷款头寸或存入金额占该资产总流动性的份额。

## 4.4 价格预言机

预言机合约负责查询资产的最新价格。

## 4.5 手续费规则

- 平台只在借款时收取0.25%手续费；
- 手续费收入用于回购代币、添加流动性。

## 5.1 RooLend.Finance 治理通证

ROO将充当产品组合（包括抵押，奖励）中的核心实用工具通证，通过为协议提供流动性或保护协议以及治理程序来获得。通证将致力于成为调整激励措施的主要工具，创建一个强大的DeFi社区，共同帮助推动RooLend生态系统向前发展。

### 通证分配

- 80%用于借贷挖矿、流动性挖矿激励
- 5%用于 DAO 风险准备金+社区治理
- 5%用户市场运营推广
- 3%项目早期投资者
- 7%用于激励团队持续开发
- 分配随着挖矿产生

### 代币产出周期

- 每个区块 2个代币
- 每30天减产 9%，减产到每个区块 0.2个代币不再减产
- 总量 2100 万个
- 代币分发 4 年完成

# 6.1 附录

## 名词解释

在使用借贷业务前，用户可以先了解以下名词：

### 抵押率

代表该资产最大可用作抵押来借其他资产的比例。针对不同资产的流动性情况 and 安全性，被授予不同的质押率。各类资产的质押率可查见《各类资产抵押率》。

### 借款额度

指根据用户抵押品的授信价值计算出的可贷资金额度，是按账户所有资产合并计算的。用户将存款转为质押以后，可以增加其贷款额度。例如：用户存入抵押100U的USDT 和100U的BTC，则他的安全借款额为： $(100 * \text{<抵押率>\%} + 100 * \text{<抵押率>\%})$

### 借款额度使用率

$\text{借款额度使用率} = \text{借贷资产} / \text{最大可借资产} * 100\%$  请用户密切关注借款额度使用率，若使用率接近100%，则账户将面临被清算风险。

### 安全线

当用户借款额度使用了100%时，就会触发资产清算，为了避免币价日常波动造成资产被清算，系统设置了<安全线>的安全线。安全线是针对一个账户内的所有资产的。

例如：用户存入抵押100U的USDT 和100U的BTC，则他的安全借款额为： $(100 * \text{<抵押率>\%} + 100 * \text{<抵押率>\%}) * \text{<安全线>\%}$ 。

### 借贷规则

用户将资产存入RooLend中，即可获得存款收益和Roo挖矿收益；

开启质押后，即可将存入资产作为抵押物，借贷BTC等资产，当用户借出其他资产后，需要支付借款利息，并且可以同时获得Roo挖矿收益。

## 利率规则

Roolend的存款利率和借款利率是浮动的，会根据资金使用率情况进行浮动，资金使用率越高则利率越高，资金使用率越低则利率越低。因此，每一个区块存款利率和借款利率都可能不同。

## 利率公式

出借人每个块可以收到借出利息的<百分比>，然后均分给池子里面所有的出借人。

当某币种流动性持续不足时，将会触发利率上限调整机制。

## 利率上调规则

APY为存款年收益/利息，例如M币种存款APY为100%，则表示用户A存入100个M币种，一年的总收益为100个M币种，利息收益将会自动增加在存款中。

## 清算规则

当用户借出的资产价值 > 可借资产价值（借款额度使用率 > 100%）时，用户将触发清算条件。此时任意用户均可作为清算执行人调用合约对借款额度使用率大于100%的借款用户进行清算。清算执行人将会帮清算用户进行还款，并同时获得清算用户的抵押资产，清算执行人可以从待清算账户中挑选任意资产进行清算。

用户可关注以下导致清算的事例：

借出资产价格上涨：当借出资产价格上涨导致借出资产的总价值上涨时，可能会导致借款额度使用率 > 1

抵押资产价格下跌：当抵押资产价格下跌时，那么可借资产价值就会变小，可能会导致借款额度使用率 > 100

长期不归还：用户借款是有一定利息的，借出什么币种，那么他的利息就是对应的币种，本文中的其它地方说的借出资产包含了需要还的利息部分，当借出的币+需要还的利息增加的时候也可能导致借款额度使用率 > 1，所以即使是单币种，抵押借贷，随着利息的增加也可能导致清算的发生。

## 挖矿收益

存入或借出资产任何代币都可获得挖矿收益。挖矿产出中的45%ROO会分配给资产提供者，55%ROO分配给借款人，合约根据用户资产在所在市场内占比获得相应ROO。相应的市场每个区块的产出速度由当前市场借款额的比例决定。