# Compound:货币市场协议

**Version 0.4**

June 2018

**Autftors**

Robert Leshner, Geoffrey Hayes

<https://compound.finance>

# 摘要

在本文中，我们引入了一种去中心协议，该协议建立了根据供需关系利用算法设定利率的货币市场，允许用户无摩擦地交换以太坊资产的时间价值。

# 1.介绍

加密货币和数字区块链资产市场已发展成为一个充满投资者，投机者和交易者的充满活力的生态系统，在其中数以千计[1]的区块链资产在交易。不幸的是，遵循金融市场的复杂性没有展现出来：因为参与者几乎没有能力去交易资产的时间价值。

利率填补了无法使用剩余资产和没有资产的人（资产指具有生产性或投资用途）之间的差距;交易资产的时间价值使双方受益，并创造非零和(non-zero-sum)财富。对于区块链资产，现在主要存在两个缺陷：

●借贷机制极为有限，导致资产错误定价（例如“scamcoins”不可估值，因为没有办法缩减库存）。

●区块链资产的收益率为负，这是由于存储成本和风险（包括交易所和场外交易）造成的，但却没有自然利率来抵消这些成本。这会造成波动，因为持有是不利和亏损资产的。

集中交易（包括Bitfinex，Poloniex ......）允许客户以保证金交易区块链资产，通过在交易所内置“借入市场”。这些是基于信任的系统（你必须相信交易所不会被黑客攻击，不会卷走你的资产和不会错误地关闭你的账户），仅限于某些客户群体，并且仅限于少数（最多主流）资产。最后，余额和账户是虚拟的;你不能在链上移动账户，例如在智能合约或ICO中使用借来的Ether或代币会使得这些组织无法访问dApps[2]。

点对点协议（包括ETHLend，Ripio，Lendroid，dYdX ......）直接促进市场参与者之间的抵押和无抵押贷款。不幸的是，权力下放会给用户带来巨大的成本和冲突;在审查的每个协议中，贷方都需要发布，管理和（如果是抵押贷款）监督贷款协议和正在活跃的贷款，同时履行贷款通常是缓慢和不同步的（需要时间筹集或整理贷款用的资金）[3-6]。

在本文中，我们引入了一个去中心系统，用于无冲突地借用以太坊代币，它不存在现行手段的缺点，使货币市场能够正常运作，并创建一种安全的正收益率方法来存储资产。

# Compound 协议

Compound是以太坊区块链上的一个协议，它建立货币市场，这是基于代币的供需使用算法衍生利率的代币池。资产的供应商（和借款人）直接与协议交互，赚取（并支付）浮动利率，而无需与同行或交易对手协商诸如到期日，利率或抵押品等条款。

每个货币市场对ERC-20代币都是独有的（例如，代币化的Ether，诸如DAI的稳定币，或诸如Golem之类的实用代币），并且包含完全透明且可公开检查的余额信息，其中记录了所有交易和历史利率。

## 2.1代币供应 Supplying Tokens

与交易所或点对点平台不同，这里用户的代币被匹配并借给另一个用户，Compound协议汇聚整合每个用户的供应; 当用户提供代币时，它就成为一种可替代的资源。这种方法提供了完整的流动性：用户可以随时撤回其代币，而无需等待特定贷款到期。

货币市场中的余额根据该资产特有的供应利率产生利息。用户可以实时查看其余额（包括应计利息）; 当用户进行更新余额（提供，转移或取出代币）的交易时，应计利息将转换为本金并支付给用户。

### 2.1.1主要用例

长期投资Ether和代币（“HODLers”）的个人可以使用Compound货币市场作为其额外投资回报的来源。 例如，拥有OmiseGo的用户可以将其代币提供给Compound协议，并获得利息（以OmiseGo计价），而无需管理其资产，履行贷款请求或承担投机风险。

具有代币余额的dApps，机构和交易所可以使用Compound协议通过“清理”余额作为代币增量回报的来源; 这有可能为以太坊生态系统解锁全新的商业模式。

## 2.2 代币借入 Borrowing Tokens

Compound允许用户使用抵押信贷额度从协议中无摩擦地借用代币，以便在以太坊任何地方使用。与点对点协议不同，从Compound中借用代币只需要用户指定所需的资产;而不需要谈判条款，到期日或筹集时间;借款是即时和可预测的。与资产供应类似，每个货币市场都有一个由市场力量设定的浮动利率，这决定了每种资产的借贷成本。

我们设立了一项规则，即每个帐户的余额必须超过未偿还借款金额，我们将此称为**抵押比率**，并且账户无法采取任何行动（例如借入或取款）能够使其价值低于我们期望的比率;为了增加（或重置）抵押品比率，用户可以随时全部或部分偿还借入的资产。即使在用作抵押品时，在Compound中持有的余额通常会继续产生利息。

### 2.2.1风险与清算 Risk and Liquidation

如果用户提供的资产的价值除以其未偿还借款的价值低于抵押比率，则用户的抵押品可以按当前市场价格减去**清算折扣**购买（使用借入的资产）; 这可以激励套利者迅速介入，以减少借款人的风险，并消除协议的风险。

拥有借入资产的任何以太坊地址可以全部或部分地调用清算职能，将其资产与借款人的抵押品进行交换。由于用户，资产和价格都包含在Compound协议中，清算是无摩擦的也不依赖于任何外部系统或订单簿。

### 2.2.2主要用例

无缝持有新资产（无需出售或重新安排组合资产）的能力为dApp消费者，交易者和开发者提供了新的空间和可能性：

●无需等待订单填写或需要链外行为，dApp可以借用代币在以太坊中使用，例如在Golem网络上购买计算能力；

●交易者可以使用现有的组合资产作为抵押借入Ether，为新的ICO投资提供资金；

●想要卖空代币的交易者可以借入它，将其发送到交易所并卖出代币，从被高估代币的价格下跌中获利（即做空）；

## 2.3 分类系统 Ledger System

Compound保留了一份完整且可审计的余额记录和分类账本，包括所有交易。对于每个货币市场a：

*Casha + Borrowsa = Supplya + Equitya*

每笔交易使用国际会计标准生成两个会计分录（借方和贷方）：

|  |  |  |
| --- | --- | --- |
| 事件 | 借 | 贷 |
| 存入代币 | 现金 | 供给 |
| 提取代币 | 供给 | 现金 |
| 借出代币 | 借款 | 现金 |
| 偿还代币 | 现金 | 借款 |
| 清算（借款人） | 供给（抵押） | 借款（资产） |
| 清算 (清算人) | 现金（资产） | 供给（抵押） |
| 利率增长（供给） | 抵押净值 | 供给 |
| 利率增长(贷） | 借款 | 抵押净值 |

## 2.4利率模型 Interest Rate Model

在Compound协议中并不是单个供应商或借款人必须就条款和费率进行谈判，而是利用利率模型，在每个货币市场中，基于个别资产的供需来实现有效的利率均衡。 货币市场***a***的利用率***U***将供给和需求统合为一个变量：

*Ua = Borrowsa / (Casha + Borrowsa)*

根据经济理论，利率（货币的“价格”）应随需求而增加; 当需求低时，利率应该低，在需求高的时候反之亦然。需求曲线通过治理编制（并由首席经济学家更新），解释为有效的函数。例如，借款利率可能如下：

*Borrowing Interest Ratea = 10% + Ua \* 30%*

为使协议具有可持续性并能承受经济攻击（通过在同一货币市场上供应和借入），供应商的利息总额必须小于借款人的利息产品总价值。供给利率是借款利率的函数，包括一个差价***S***（如0.10），代表了协议的经济利润：

*Supply Interest Ratea = Borrowing Interest Ratea \* Ua \* (1 − S)*

# 3实现与架构

Compound货币市场的核心是一个分类账本，允许以太坊账户提供应或借入代币，同时计算利息。该协议的智能合约将可公开访问，对于机构组织，dApp和人类完全免费。

## 3.1货币市场合约 MoneyMarket Contract

货币市场合约存储每个账户的当前余额。 在最简单的情形下，货币市场的行为类似于ERC-20代币，为每个账户资产保留余额。 随着时间的推移，货币市场中的余额会产生利息，我们将在下面介绍一种实现这些余额更新的低gas消耗方法。

作为协议的客户供应或借入资产，货币市场合约更新相应资产的余额信息。 此外，我们使用此余额信息计算上文第2.4节所述的供应和借入代币的当前利率。

## 3.2利率机制 Interest Rate Mechanics

Compound货币市场由一对现行利率（供给和借入利率）定义，适用于所有用户，随着供需关系的变化而随时间调整。

每个货币市场的每个利率历史由利率指数捕获，利率指数是，早用户供给，提取，借入，偿还或清算资产导致的每次利率变化时计算的。用户的余额（包括应计利息）只是当下指数除以用户余额最后一次检查时指数的比率。

货币市场中每个帐户地址的余额存储为账户检查点。账户检查点是一个Solidity元组<uint256 balance，uint256 interestIndex>。此元组描述上次该账户利率被阴影时的余额。目前的利率指数也存储在全局范围内。

每次交易发生时，资产的供应和借入利率指数都会通过先前的指数和每个区块的利率r\*t计算得到。

*Indexa,n = Indexa,(n−1) \* (1 + r \* t)*

## 3.3 借入 Borrowing

希望借入并且具有足够余额存储在Compound中的用户可以在货币市场合约上调用Borrow（address asset，uint amount）。此函数调用检查用户的帐户余额，并给予足够的抵押品，更新用户的借入额度，将代币转移到用户的以太坊地址，并更新货币市场的浮动利率。

借款与3.2中计算的余额利息完全相同的方式产生利息;借款人有权随时通过调用函数“repayBorrow(address asset, uint amount）“来偿还未偿还的贷款。

如果用户的整体账户价值由于他或她的抵押品价值变化（例如，用户持有ZRX，并作为借入Ether的抵押品且ZRX的价值在明显下降）而低于清算比率，那么我们就有一个公共函数`liquidateMarketBorrow （address customer, address collateralAsset, address borrowAsset, uint collateralAmount）`用于以略高于市场的价格交易借用者抵押的用户资产。

价格预言机（Price Oracle）维持每种资产的当前汇率;Compound协议将设置资产价值的能力委托给一个委员会，该委员会从十大交易所汇集整理价格。这些汇率用于确定借款能力和抵押要求，以及所有需要计算账户价值的功能。

## 3.4市场状况 Market Status

每个由资产定义的市场可以处于Compound货币市场中的三个状态之一：不受认可，受认可或暂停。每个市场都将以不受认可的状态开始，并可能（根据管理员的操作）转换为受认可的状态。一旦市场被认可，任何用户都可以如上所述从市场供应或借入。

如果出于任何原因，必须关闭市场，只有管理员才有能力将受认可的市场转移到暂停状态。Compound治理委员会将在暂停市场之前为用户提供重要的缓冲时间。暂停的市场不允许用户继续供应或借入资产（尽管用户仍可以撤回或关闭借入的账户）。

如果一个市场无限期暂停，必须保证所有借款都已偿还;否则，协议将没有足够的现金偿还给所有优秀供应商。因此，一旦市场暂停，无论借款人的抵押品健康状况如何，该资产的所有借款都可以按标准折扣进行清算。

## 3.5 治理 Governance

Compound将从协议的集中控制开始（例如选择每个资产的利率模型），并且随着时间的推移，将转变为社区和利益相关者控制。 协议中的以下权利由管理员或治理委员会控制：

●选择新的管理员，例如DAO

●为每个市场设置利率模型

●认可，暂停或解冻市场的能力

●委派实体作为价格预言机

●取出协议的产权（收入）

随着时间的推移，Compound希望将这些权利转移到由社区控制的DAO。 DAO将采用以太坊合约的形式，通过提案和投票，调用与上述能力相关的功能。 由于管理员（或DAO）可能会选择新的管理员，因此随着时间DAO将根据利益相关者的决策而发展。

## 3.6 合约接口 Contract Interface

|  |  |
| --- | --- |
| 函数 ABI | 行动 |
| supply(address asset, uint256 amount) | 转移一个ERC-20代币到货币市场和标记消息发送者(msg.sender)更新后的余额。  更新利率模型； |
| withdraw(address asset, uint256 amount) | 如果资金可用，转移一个ERC-20代币到消息发送者  更新利率模型； |
| borrow(address asset, uint amount) | 检查消息发送者的抵押价值，如果足够，更新借款余额信息和转移ERC-20代币给消息发送者  更新利率模型； |
| repayBorrow(address asset, uint amount) | 转移一个ERC-20代币到货币市场和减少消息发送者的借款余额  更新利率模型； |
| liquidate(address customer,address collateralAsset, address borrowAsset,uint borrowAmount) | 调整借款人的利息，然后将ERC-20令牌转移到货币市场以偿还借入债务。  消息发送者以折扣价收到借款人的抵押品。  只有在借款人违反抵押比率时才能调用此功能。  更新利率模型； |
| setAssetPrice(address asset, uint256 value) | 给特定资产设定价格预言机，由指定预言机地址才能调用 |

Table 1. 区块链上的ABI和货币市场函数总结

# 4.Summary

●Compound为以太坊资产创造了正常运作的货币市场

●每个货币市场的利率由相关资产的供需决定

●用户可以向货币市场提供代币以赚取利息，而无需依赖中央机构

●用户可以使用协议中的余额作为抵押品借用代币（用于使用，出售或再出借）

# References

[1]Cryptocurrency Market Capitalizations. https://coinmarketcap.com/

[2]Bitfixex Margin Funding Guide. https://support.bitfinex.com/

[3]ETHLend White Paper. https://github.com/ETHLend

[4]Ripio White Paper. https://ripiocredit.network/

[5]Lendroid White Paper. https://lendroid.com/

[6]dYdX White Paper. https://whitepaper.dydx.exchange/