KEEN（ODK）稳定币协议白皮书

V1.0

最新更新：2023 年 4 月 26 日

作者：KEEN.ODK

摘要

KEEN 稳定币协议，与 MakerDao 协议类似，是一个构建在以太坊平台上，使用智能合约实现的一个稳定币协议，它继承了 MakerDao 的一些特性，例如基于超额的多担保品抵押、软锚定美元的 ERC20 代币、用于去中心化治理和激励的 ERC20Token 等。与 MakerDao 不同的是，KEEN 协议借鉴了 compound 的双向借贷模型，使得本协议拥有了许多优秀特性。

首先，由于使用了双向借贷模型，提高了抵押资产的利用率，也间接降低了铸造稳定币的成本；其次，协议实现了自动利率目标，因此不再需要 DSR 机制来激励稳定币的持有者，也不需要人为调整铸造费率(从而避免了人为治理的非理性因素)，这一切都由市场自动完成；最后，本协议使用了更为成熟的第三方价格预言机来取代弱中心化的喂价系统，使得协议本身更为轻量级，也更具鲁棒性。

介绍

价格波动催生加密稳定货币

以比特币为首的加密数字货币是去中心化的、支持点对点交易的资产，底层技术是区块链。加密数字货币无须经过银行等传统金融机构就可以实现价值转移，速度快且成本较低，因而在发行之后就得到广泛关注。但加密数字货币交易价格普遍表现出很高的波动性,日波幅甚至达到 10%以上，受到一部分风险爱好者的追逐。

在价格剧烈波动且缺乏法币定价的数字货币市场中， 需要一种价值相对稳定的加密数字货币发挥资金避险、交易中介、支付结算等功能。稳定币的最终目的是通过锚定美元等资产来增强加密货币的稳健性，打消用户对加密货币大幅波动的担忧，建立并不断增强用户对加密货币的信心，以期提供更加稳定的价值以及实现更加快捷和廉价的结算。

稳定币现状

稳定币的本质是通过区块链技术和比特币的设计理念来缔造一种价格相对稳定的支付工具。大多稳定币借鉴了各种传统外汇市场的“货币稳定机制”，以试图来试验出最佳策略组合。下面我们简单介绍最为知名的两种稳定币。

MakerDAO 作为最早的去中心化自治组织之一，为以太坊提供稳定币 Dai。Dai 通过抵押债仓（CDP）智能合约发行，当用户存入抵押品如 ETH 时，CDP 会自动铸造一定比例的新 Dai 币。抵押品价格往往高度波动，因此 CDP 智能合约要求用户“超额抵押”，即用户获取的 Dai 稳定币的价值必须远远低于用户作为抵押品存入的 ETH 的总价值。当 CDP 中的抵押品价值下降到协议指定的阈值以下时，CDP 智能合约通过拍卖存放的抵押品获取 Dai 并销毁，以保持流通中的 Dai 足额抵押。

不得不提的是，MakerDAO 作为 Dai 的发行组织，对 Dai 的各类参数甚至发行规模均有决策权限。在 Dai 模式中，足额的抵押保证了 Dai 足够稳定，但也存在许多问题，例如：协议中没有实现价格自动稳定的良好算法以至于人为调整整个系统的所有参数往往导致目标价格稳定机制失效、单向抵押借出稳定币导致资金利用率低、系统决策效率低下导致系统对外部金融市场变化反映迟钝，等等。

2014 年， 注册在马恩岛和香港的 Tether 公司发行了第一个稳定币 TetherUSD， 简称 USDT（中文名称为泰达币），也是目前规模最大的稳定币。Tether 公司宣称，用户可以通过 SWIFT 电汇美元至 Tether 公司提供的银行账户或通过 Bitfinex 交易所换取 USDT。赎回美元时，反向操作即可。Tether 公司“承诺”严格遵守 1:1 的准备金保证,并有定期审计。

从类型来看,USDT 属于典型的链下资产抵押型稳定币。由于 USTD 由独立公司进行运作，关于 USDT 的信任问题一直不绝于耳,例如关于 USDT 过度增发和财务存在问题的质疑之声早已有之。

迄今为止，Tether 只披露了两次项目审计结果，但都存在问题，非政府中心化机构发行稳定币的弱点暴露无疑。

KEEN 的优势

KEEN 协议尽可能的保持简洁，去除一切不必要的冗余模块，例如 MakerDao 中的 DSR、人工调整铸造费率以及弱中心化的喂价模块，简洁的协议有助于提升去中心化特性和健壮性。
去中心化的稳定币协议作为一个底层协议，我们不认为它需要支持储蓄功能，储蓄是更上层的应用需要考虑的事情， 上述所说的底层协议与上层应用的关系类似中央银行与商业性银行，因此我们抛弃了 MakerDao 中的 DSR。
KEEN 的双向借贷模型把抵押铸造稳定币和存款生息两个独立的功能合并成一个模块，并产生一个自由的借贷市场，利率会随时响应市场的变化，供需双方在一个合理的利率水平上达成平衡，这种自动平衡的利率比人工调整的更为精准，也减少了社区争议和分裂的可能性。

MakerDao 协议的治理代币 MKR 的主要作用是调控稳定币价格和协议治理，在激励方面的效果就比较弱，仅仅当系统产生一定量的债务或盈余时，才会通过拍卖机制进行增发和回购，对于系统的主要贡献者，即抵押者或借款者并没有有效的激励。

KEEN 则通过流动性挖矿机制实时的对系统的贡献者进行激励，每当协议的使用者存入或者借出资产时，都会产生贡献值，这个贡献值我们也可以称之为算力，算力越高，获得协议奖励的治理代币则越多。

由于稳定币协议的简洁性，使用者对系统的主要贡献是可以量化的，因此流动性挖矿在稳定币协议中将会是一个比较完美的激励机制。

最后，本协议使用了更为成熟的第三方价格预言机取代弱中心化的喂价系统，使得协议本身更为轻量级，也更具鲁棒性。

协议概览

ODK 稳定币

ODK 是 KEEN 协议中软锚定美元的与 ERC-20 兼容的稳定加密货币，部署在类似以太坊的公有链平台之上，通过智能合约控制其发行权，因此是去中心化、无需许可的，可以在全世界范围内通过加密数字货币钱包使用。

任何人都可以通过以下途径获取 ODK：

- 可以通过 KEEN 协议的客户端抵押 ETH 或 BTC(跨链资产)铸造 ODK，在下文中我们也称之为从市场中借出 ODK；
- 任何人可以通过 Uniswap 这类去中心化交易所购买 ODK；
- 通过别人的转账，比如支付或捐赠等；
- 通过类似于 compound 的借贷市场中借出；
- 通过中心化的交易所购买后再提取到去中心化的加密数字货币钱包。

通过以上途径获得的 ODK 都是无差别的，均可以在全世界自由流通。流通中的每个 ODK 都由超额资产背书，担保物的价值总是高于 ODK 债务的价值，一切都是公开透明并且可以进行证明的，这是公有链提供的独特价值。

ODK 的目标价格是 1USD，即 1ODK=1USD，其发行量没有上限，与合约中用于担保的资产量相关，随着使用者增加担保资产而增发，随着使用者偿还而销毁。KEEN 协议的设计目标是使 ODK 在频繁高波动的加密货币市场中能保持价格稳定，可以用于价值贮藏、交易媒介以及记账单位。

借贷市场

KEEN 的市场与现有的部分借贷货币市场类似，如 compound，但 compound 市场中的代币均为第三方项目的代币，KEEN 协议则天然的内置了一个原生代币市场，即 ODK 市场。在初始化的时候系统作为贷款人为市场供应了第一笔 ODK，这笔 ODK 的数量将用于计算资金使用率和存款利率。需要注意的是，系统的存款行为不会产生贡献值，即不会参与治理代币的分配。

供应资产

用户使用协议的第一步是存入担保资产，也称之为增加供应。用户可以供应 ETH 以及 ERC-20 兼容的数字资产，系统会等按照一定比例兑换为协议内部资产，即 kToken。当用户拥有了 kToken 之后，才可以进行借款或铸造稳定币，我们可以把铸造稳定币视作一种特化的借出操作，这有助于理解本协议，也就是说用户也可以选择借出其他资产，比如 WBTC、renBTC 等（前提是 KEEN 协议增加了这些资产的借贷市场，并且有其他人供应该资产）。

赎回资产

用户想要退出协议的时候，可以通过 redeem 接口将持有的 kToken 兑换为相应的外部 ERC-20 资产。用户供应和取回资产时，并不总是按照 1:1 的比率进行兑换，这个兑换率是浮动的，我们会在下一小节详细描述这个兑换率，在本节，我们只需要知道，kToken 和基础资产原 Token 之间的价格（兑换率）会秩序上涨，因为随着借款的增加及时间的积累，系统的利息总是在增长。

借入资产

用户供应资产之后，协议会根据每项资产的担保率计算出用户的 accountliquidity，并以此数值判断用户可以借出多少资产。担保率一般是小于 1 的，严格来说是小于 0.9，信用、市值规模、影响力越高的资产的担保率越高。用户的 accountliquidity=sum(supplyasset*factor)-totalBorrows。当 accountliquidity 小于 0 时，用户将无法借款。

偿还资产

根据公式，用户可以通过偿还借款来提高 accountliquidity，从而提高借款额度，同时也可以避免因为担保资产的波动性导致被清算的风险。用户可以偿还自己的借款，也可以为其他用户偿还。

清算

当用户的 accountliquidity 为负数时，任何用户可以调用协议对该账户的 CDP 进行清算，即通过偿还部分或全部该 CDP 中的借款额，以一个折扣价格获得该 CDP 的担保资产，这个折扣价格是对清算者的激励。KEEN 协议希望通过对清算者的激励来第一时间降低系统潜在的债务风险。

但这个措施无法避免黑天鹅事件，当担保资产的价格暴跌时，清算者将获得超过 CDP 中担保资产的数量，此时系统将产生负债，我们会在风险控制一节说明 KEEN 协议如何处理系统负债。在 MakerDao 协议中，CDP 的清算是通过拍卖的方式，出价更高者可以获得担保资产，但可能会造成偿还的 Dai 低于借款的数额，这会造成 Dai 的债务而不是担保资产的债务，这一点与 KEEN 协议有所区别。

利率模型

在 MakerDao 协议中，用户抵押资产进行铸币时，需要支付固定的费用，用户获得 Dai 之后可以存入合约中获取固定的利息，这个利息的来源就是部分铸币费用或者称作稳定费用，稳定费率和存款利率在短期是固定的，虽然可以通过社区投票的方式来调整，但这种方式是笨重和低效的，甚至可能会造成社区的分裂。KEEN 协议的利率分为借款利率和存款利率，借款利率决定了存款利率，借款利率是浮动的和实时计算的，因此存款利率也是浮动和实时计算的。KEEN 的借款利率公式如下：

$$utilizationRate=totalBorrows/(totalCash+totalBorrows-totalReserves)borrowRate=baseRate+utilizationRate*multiplier$$

从公式中可以看出，借款利率随着总借款额的增长而增长，当然我们也可以通过调整系统储备金来对借款利率进行微调。

存款利率或者供应利率则通过 kToken 与底层资产的兑换率来体现：

$$exchangeRate=(totalCash+totalBorrows-totalReserves)/totalSupply$$

也就是说在协议实现中,并不需要为用户的存款计算利息或者进行结算,随着借款额的增加，exchangeRate 会逐渐变大，用户存入的 kToken 在未来总能兑换更多的底层资产，这之间的差值与时间的比率与通过借款利率计算的供应利率是大致相同的：

$$supplyRate=borrowRate*(1-reserveFactor)*utilizationRate$$

流动性挖矿和治理代币： KDS

KDS 是 KEEN 协议中的治理代币，其主要职责是作为社区成员对协议细节产生变更或进行重大决策的凭证。KDS 总量恒定为 2100 万枚，其中一小部分用于赠送给早期的支持者和贡献者，大部分则用于激励协议的使用者。每当用户发生供应、存款、偿还、清算、kToken 转账等行为时，用户的供应数额和借款数额均会发生变化，当用户增加供应或借款时，KDS 的分配合约将提升用户的算力，当用户减少供应或贷款时，算力也将被降低，算力越高，用户单位时间内获得的奖励 KDS Token 越多，用户可以随时领取这些奖励。KDS 的通胀模型与比特币类似，但减半周期缩短为一年，协议一旦发布，该发行策略不再改变。

治理

尽管 KEEN 协议与 MakerDao 相比已经轻量许多，但仍然有许多可以调整和改进的空间，我们不希望它像比特币一样是一个一成不变的系统，只能通过分叉来解决争议和进行变革，同时我们也要防范集权带来的风险。KEEN 协议采取的方案是渐进式去中心化方案，在系统的初期，我们可能会对系统的部分参数和策略进行频繁调整，因此采用的是管理员治理机制，随着系统的逐步稳定,协议将过度到多重签名账户的治理机制,最终协议将采用民主投票制度，成为一个真正去中心化的协议。但无论是哪种治理机制，所有的变更内容或决策过程都是在链上进行的，所有人都可以进行监督。

风险控制

采用超额担保机制的稳定币协议在大多数情况下都是可靠的,但仍然需要考虑黑天鹅事件的出现可能性。比如，在担保资产价格暴跌一定幅度，所有的担保资产都不足以偿还借款时，会发生两种情况，一种是系统禁止继续清算(compound 采用的策略)，另一种是系统允许清算者以更低的价格偿还借款从而获得担保资产(MakerDao 的策略)。

KEEN 采用的策略是始终允许清算者进行套利，系统会使用储备金来弥补这个差价，这种策略也会导致系统储备金不足甚至为负数，进而影响到供应利率，这时候就只能通过链上结合链下的治理机制来解决这一问题，社区将会组织募捐 KDS，并将 KDS 在交易所兑换为相应的资产再偿还系统债务。

技术概览

kTOKEN 合约

在 KEEN 协议中,资产有三种类型,他们分别是 underlyingasset,wrappedasset,anchorasset。例如,用户在使用 KEEN 协议前就在钱包中持有的资产成为 underlyingasset,例如 ETH、WBTC、renBTC、ODK、KDS 等，用户将 underlyingasset 存入 KEEN 后，将按比例兑换成相应的 wrappedasset，也叫 kToken，类似 compound 中的 cToken，aave 中的 aToken。

wrappedasset 都以 k 字母开头,例如 kETH,kODK,kWBTC 等,anchorasset 是 underlyingasset 所锚定的资产,例如 ODK 对应的是 USD,renBTC 对应的是 BTC,KEEN 并不真正存储 anchorasset，仅仅为 kToken 标记一个锚定资产的符号，用于向预言机询价。kToken 合约的功能包括：underlyingasset 与 wrappedasset 之间的兑换，提供借款、偿还、清算等借贷市场的用户操作接口，另外还包括存入和提取储备金、调整储备金率等管理员操作接口。

kToken 合约本身也是 ERC-20 兼容的，存储着 wrappedasset 的余额账本，允许用户自由转移 wrappedasset，并且由于 wrappedasset 有预期的利息回报，第三方应用可以基于此构建一种债券期货市场，但这只是一种可能性，并不是 KEEN 协议本身要考虑的内容。

市场控制者

Marketcontroller 是 KEEN 协议的核心组件，几乎所有的算法、控制策略都通过该合约进行调用，例如借款利率的计算、accountliquidity 的计算、预言机价格的查询、新的担保资产的支持等。

与 kToken 合约类似，Marketcontroller 提供了一些管理员接口，比如设置资产的抵押率、清算者的激励系数等，当系统出现紧急问题短期无法处理时，可以通过 Makertcontroller 合约的管理员账户进行紧急关停，当然我们会通过 Governance 合约对这一特权进行限制，由社区成员投票进行决策。

发行人

Distributor 合约负责记录用户的算力账本以及 KDS 代币的分配，distributor 使用 TokenPool 数据结构来存储用户的算力和代币分配信息。

KEEN 协议中存在两种类型的 TokenPool，一种是永久存在的主矿池，大部分的 KDS 在这个 pool 中分配，另一种叫做 LiquidityProviderPool,这种 pool 是通过治理合约临时创建的，主要用途是为了在早期激励那些在 dex 中为 KEEN 协议中的代币提供流动性的用户，LiquidityProviderPool 一般会指定一个分配总量和分配起止区块数，在起止区块之内将 dex 的流动性代币转入 Distributor 合约中，则可以进行 KDS 代币的分配，需要注意的是 LiquidityProviderPool 中的算力与主矿池中的算力会单独核算。

Distributor 使用的分配算法完全在链上运行，该算法的复杂度为 O(1)，该分配算法的关键在于两个参数：rewardIndex 和 mask，rewardIndex 表示单位算力可分配的代币数，mask 表示用户增加算力时当前区块应忽略不计的那部分算力份额，只要在用户算力变更时更新这两个参数，Distributor 即可随时以常数复杂度计算任何用户在任何时间点可以获得的奖励。

价格预言机

协议在初期采用预言机提供的价格信息(pricefeed)，但并不意味着 KEEN 要永远依赖预言机，KEEN 协议对预言机接口进行了抽象，可以在必要时通过治理系统平滑的更换更合适的预言机实现。预言机的每种资产的价格信息都要通过不同的合约进行查询，而 KEEN 的借贷市场所支持的资产类型是可以动态增删的，因此，我们在预言机代理中需要提供一个接口来设置新增加的资产在预言机中对应的合约地址。

维护与治理

KEEN 绝不是一个一旦发布就万事大吉的系统，它需要持续的调整、维护和升级以不断适应需求，这些工作需要整个社区成员共同完成，我们在合约预留了一些接口来帮助社区完成这些工作，这些接口包括：

```
-kToken::setReserveFactor-kToken::reduceReserves-KErc20::addReserves-MarketCont
roller::supportMarket-MarketController::setLiquidationIncentive-MarketControlle
r::setCollateralFactor-MarketController::setBorrowPaused-PriceOracle::_setPrice
FeedAddress
```

Governance 合约中实现了提案发起和投票的功能，任何满足条件(比如持有 KDS 超过一定量)的用户可以发起提案，请求执行上述合约的管理员接口，当提案得到一定数量的投票支持后，管理员接口会被调用，KEEN 协议完成了变更和调整。

可升级性代理

软件系统的设计者不可能考虑到所有可能发生变化的情况，在上一节提到的预留的管理员接口是远远不足以覆盖到 KEEN 协议各种升级和变化的可能性的，我们使用了 upgradeabilityproxy 技术来解决这一问题。

我们通过 proxy 来解耦模块之间的依赖关系，当某个合约的算法发生重大变化或出现漏洞时，我们可以部署一个新的合约，然后将新合约的地址注册到代理合约中，即可在保持旧合约存储数据的同时应用新的合约算法或逻辑。

未来

随着参与 KEEN 协议的用户不断增多，ODK 的流通规模将逐步扩大，ODK 将在更多市场中发挥价值贮藏、交换媒介、记账单位等重要功能，成为加密世界去中心化金融生态的基石。

扩展货币市场

KDS 持有者也许愿意创建基于新的资产的货币市场，这些资产也将受到 ODK 的风险要求、参数和自动利率目标的约束。

- **允许创建基于合成资产的货币市场。**在区块链世界中，合成资产存在的必要性显而易见，因为总有人无法或不愿意持有初始资产，合成资产满足了更多样的需求且合成资产往往比原始资产具有更多金融属性。
- **允许创建基于跨链的货币市场。**将无智能合约功能的区块链资产（如比特币）移植到具有智能合约功能的区块链（如以太坊）的跨链资产，在去中心化金融中生态中，正在发挥越来越重要的作用。

潜在市场

更多样的金融工具。以随着 KEEN 系统的逐步稳定，ODK 资产的规模扩大，平台可以为用户提供更多元的获利工具，例如存币生息、现实资产抵押等。

- **商业收据、跨境交易和汇款:**ODK 可以降低外汇的波动性并免去对中介的需求，这意味着跨国交易的成本会大幅降低。
- **慈善机构和非政府组织:**它们可以使用 ODK 透明的分布式账本技术。

- **游戏业:**对于区块链游戏开发者来说，ODK 是一种理想的货币之选。整合了 ODK 之后，游戏开发者得到的不仅是一种货币，还有一整个经济系统。有了 ODK 的可组合性，游戏开发者可以基于去中心化金融构建新的玩家行为机制。
- **等等**

去中心化治理

去中心化社区治理探索空间仍大，目前在去中心化的社区治理方面的探索仍然有更多的提升空间，这是由于目前一些探索机制尚未落地，仍然需要实践来证明进而改进。例如如何在保持整体去中心化的同时兼顾公平，效率问题，需要多方权衡。

KEEN 协议采取的方案是渐进式去中心化方案，随着系统的逐步稳定，协议将逐渐过度到多重签名账户的治理机制，最终协议将采用民主投票制度，成为一个真正去中心化的协议。

总结

KEEN 是一个去中心化的稳定币协议，它使用超额担保资产为稳定币的价值背书，与中心化的 USTD 相比，KEEN 协议中产生的 ODK 是一种无需许可、一视同仁的、价格稳定的、且不会发生挤兑风险的加密数字货币，可用于价值贮存，交易媒介等，在世界任何一个可以联网地方都可以使用。

与最主流的去中心化稳定币协议 MakerDao 相比，KEEN 做出了多项创新，例如双向借贷模型的引入和市场化的利率调整使得系统更加自动化和智能化，通过流动性挖矿的引入使得系统对于贡献者的激励更加公平和有效，通过去除技术落后的弱中心化喂价系统，使得协议更为去中心化且更具鲁棒性。

随着主流加密数字资产市值的进一步提升，基于超额担保机制的去中心化稳定币必将取代中心化发行的稳定币，成为加密世界去中心化金融生态的基石。

参考文献

1. Compound:TheMoneyMarketProtocol.https://compound.finance
2. TheEthereumBlockchainWhitepaper.https://ethereum.org/
3. TheMakerProtocol:MakerDAO'sMulti-CollateralDai(MCD)System.https://makerdao.com/en/whitepaper/#emergency-shutdown
4. CryptocurrencyMarketCapitalizations.https://coinmarketcap.com/
5. ETHLendWhitePaper.https://github.com/ETHLend