



版本 3.0

## 项目说明

### 项目的简要介绍

Coinversation Protocol 是一个基于波卡合约链的合成资产发行协议与合约交易平台，用本项目发行的代币 CTO 和波卡 DOT 作为抵押，通过智能合约和预言机来合成出任何加密货币或者股票、债券、黄金等链下资产。用户通过抵押 CTO 或 DOT 可以铸造出某种合成资产，比如美元，就自动成为该资产的多头。用户也可以通过交易平台将铸造的资产转换成其他资产，从而实现做空该资产，做多其他资产的目的。用户铸造的资产即整个系统所对应的负债，每个用户负债的比例在抵押时就已经确定，由此可以计算出各自的盈利。因为这样的抵押池模型不需要交易对手，完美解决了 DEX 所存在的流动性和交易深度的问题。

### 项目代币 CTO

总发行量：100,000,000

本项目代币为 CTO，发行硬顶上限为 1 亿，在项目上线时发行一部分，剩余部分由流动性挖矿产生。

持有 CTO 主要有两大作用。第一是通过抵押 CTO 产生合成资产，并且赚取合约交易费用。CTO 持有人可以用 CTO 作为抵押来生成合成资产，并且按抵押的 CTO 数量可以计算出占总体的抵押比例。而合约交易所产生的费用会划入费用池，按比例奖励给抵押了 CTO 的用户。第二 CTO 同时

也是项目的治理代币。本项目所涉及到的所有参数，包括抵押物的增减、抵押比例的调整、合成资产的种类等，都可以通过 CTO 持有人投票决定。

整个系统主要的功能模块有：用抵押铸造合成资产、去中心化合约交易所、抵押池、费用池、预言机、流动性挖矿。

## 抵押铸造合成资产

整个系统所产生的合成资产，全部由用户抵押一定的抵押物产生。初期的抵押物包括 CTO 和 DOT，抵押比例分别为 800%和 500%。未来可通过社区治理对抵押物和抵押比例进行调整。用户抵押锻造合成资产时，即产生了对应的债务。当用户希望解锁抵押物时，则必须偿还抵押物，也即销毁之前生成的合成资产。

## cUSD

目前规定由抵押物直接铸造合成的资产为本项目的稳定币 cUSD。也即用户抵押 CTO 或者 DOT 后，直接生成的合成资产为 cUSD，而其他合成资产需要用户通过合约交易产生。cUSD 的价格在整个系统中始终定义为\$1。全部用户生成的所有 cUSD 即为整个系统的总负债，以 cUSD 计价。

通过合约交易，cUSD 可以转换成任意系统支持的合成资产，例如 cBTC、cETH，甚至挂钩股票、黄金等传统资产的 cAAPL、cXAU 等，并且支持做多或做空。合成资产的种类可以由社区治理添加。需要注意，如果用户铸造 cUSD 之后只是简单持有，那相当于自动做空系统内的所有其他资产。

## 去中心化交易所

即提供不同合成资产转换，合约交易的交易所。由于本项目的设计特性，此 DEX 不需要交易对手，也没有交易深度的问题。用户的盈亏计算，通过以下的例子来说明。

举例一：假设 A 和 B 两个用户，各生成\$50,000 的 cUSD，各自债务比例是 50%，系统总负债\$100,000 cUSD。现 A 把全部 cUSD 转换成 cBTC，B 仍然简单持有 cUSD。假设 BTC 价格上涨 50%，因此 A 持有的 cBTC 价值变为\$75,000，而 B 持有的 cUSD 价值仍然是\$50,000，此时系统总负债变成\$75,000+\$50,000=\$125,000。注意，因为债务比例并没有变，所以 A 的

负债是 $\$125,000 \times 50\% = \$62,500$ ，同理 B 的负债也是 $\$62,500$ 。因此可以计算出 A 的盈亏是 $\$75,000 - \$62,500 = \$12,500$ ，而 B 的盈亏为 $\$50,000 - \$62,500 = -\$12,500$ 。整个系统所有用户盈亏总和为 0，类似于传统合约交易系统。要注意，虽然 B 生成 cUSD 之后什么也没干，但他/她还是因为 BTC 的价格上涨而亏损了。这是因为生成 cUSD，即默认等效于成为美元的多头（在本例中也相当于 BTC 的空头）！

## 抵押池

抵押池即所有用户产生的合成资产的总和，以 cUSD 计价。根据各个用户生成的合成资产数量，抵押池也记录了每个用户占系统债务的比例。每当有新的合成资产产生时，系统的债务比例都要重新计算。举例如下。

举例二：假设接着举例一中的假设，现在 A 持有 $\$75,000$  的 cBTC，B 持有 $\$50,000$  的 cUSD。现假设有一个新用户 C，又生成了 $\$50,000$  cUSD，计算新的债务比例。注意，现在 A 和 B 的总债务已经是 $\$125,000$ ，而不是初始状态的 $\$100,000$  了！因此，C 操作之后，系统的总债务变为 $\$175,000$ 。A 的比例为 $\$62,500 / \$175,000 = 35.71\%$ ，B 的比例为 $\$62,500 / \$175,000 = 35.71\%$ ，C 的比例为 $\$50,000 / \$175,000 = 28.57\%$ 。

## 费用池

用户在去中心化交易所交易或转换合成资产会产生交易费用，费用比例暂定 0.3%，这些费用全部进入费用池。费用以 cUSD 收取，并且把全部费用按债务比例分配奖励给用户。系统规定只有抵押物为 CTO 的用户才能或者奖励，以此作为 CTO 持有人的激励。因为 CTO 价格有波动，因此规定只有符合抵押比例的用户才有资格获得奖励。

## 预言机

由于合约交易的价格都需要从外部读取，预言机是本项目中非常关键的一环。初期，系统会采用项目组提供的中心化预言机，未来会引入更安全的去中心化预言机。

## 流动性挖矿

本项目剩余的 50%代币 CTO 由流动性挖矿产生，即 5000 万个。

其产生数量为 4 年减半一次，而每 4 年的期间内随时间线性发行。也即项目上线后的第 1 到 4 年产生 2500 万个 CTO，第 5-8 年产生 1250 万个 CTO，第 9-12 年产生 625 万个 CTO，以此类推。

流动性挖矿的质押物和合成资产的抵押池保持一致，也即目前为 CTO 和 DOT，未来也可以增加其他资产。为了保障项目代币 CTO 持有人的利益，规定流动性挖矿产生的 CTO 的 75% 分配给质押 CTO 的用户，25% 分配给质押 DOT 的用户。这一比例未来可通过社区治理以及质押物的增加而调整。

为了增加合成资产抵押池的流动性，做出如下两条规定：

(1) 参与流动性挖矿用户必须拿出至少 20% 的代币参与合成资产的发行。例如用户用 4 个 CTO 参与流动性挖矿，那他/她至少要在合成资产的抵押池中存入 1 个 CTO。

(2) 由流动性挖矿产生得到的 CTO，其中的 20% 也必须参与合成资产的发行，进入合成资产的抵押池。

流动性挖矿是 CTO 代币的发放模块。用户可以在此锁仓 CTO 或 DOT，从而获得 CTO 的收益，锁仓 CTO 或 DOT 获得的收益比例不同。并规定，锁仓进行流动性挖矿的用户，必须同时在债务池抵押对应比例的 CTO 或 DOT 生成合成资产，从而为整个系统提供更多流动性。

## 系统核心产品

1、Coinpro.MintC——铸造和销毁 cUSD 的铸币中心

MintC 支持的操作包括：铸造和销毁 cUSD、管理抵押率、查看账户余额和 MintC 历史账本、解锁抵押的 CTO 或 DOT 等。

2、Coinpro.Exchange——交易合成资产的去中心化交易所

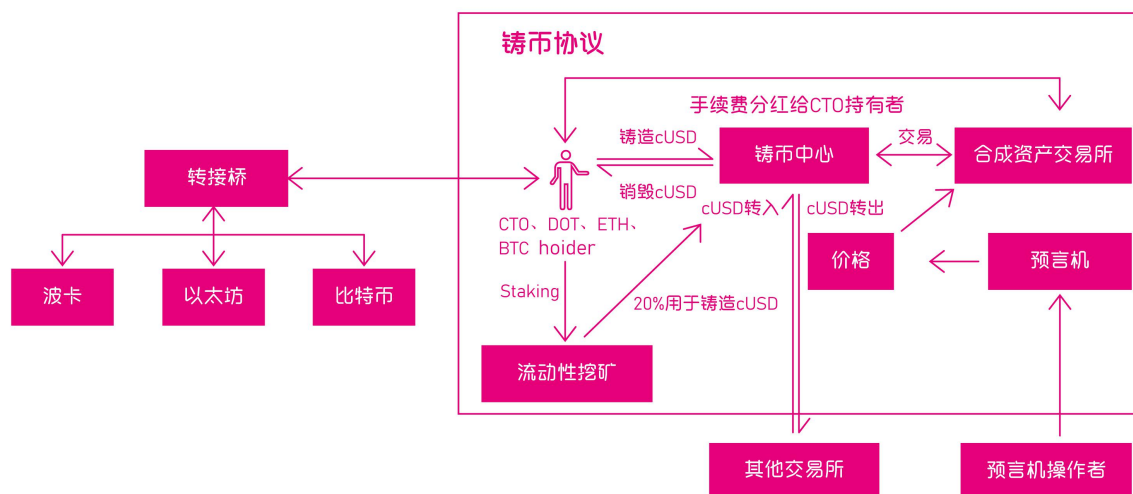
无限的流动性：没有订单簿，无需担心流动性或滑点。

点对合约交易：在各种合成资产之间无缝交易。

分布式抵押池：交易资产由分布式加密抵押池支持，可以抵御审查。

## 系统工作流程

合成资产的生命周期可以分为铸造-交易-销毁三个阶段，流程图如下所示。



## 一、铸造

用户通过在 Coinpro.MintC 中抵押 CTO 或 DOT 来铸造系统默认的稳定本位币 cUSD。CTO 的抵押比例为 800%（暂定），DOT 的抵押比例为 500%（暂定），即价值\$800 的 CTO 或\$500 的 DOT 可以铸造\$100 的 cUSD。用户的抵押比例应尽量高于这一规定的比例，即当抵押物价格下跌时，抵押比例有可能会不足，此时用户应补充抵押物或者归还（销毁）一部分 cUSD。系统规定，大于等于规定抵押比例的用户将获得费用池中的交易费用的分红作为激励。

## 二、交易

cUSD 是一种合成资产，也是整个系统的本位币，即所有债务都转换成 cUSD 计算。同时，cUSD 也是稳定币，在系统中的价值始终定义为\$1。cUSD 可以在 Coinpro.Exchange 中转换成其他合成资产，例如 cBTC、cETH、cDOT 等加密货币，欧元、日元、人民币等外汇，甚至黄金和各种股票，同时支持买多和卖空。所有这些资产都是系统合成的，并非真实资产，其转换汇率由预言机提供的外部真实价格确定。此转换过程不需要交易对手，用户总是可以把自己全部的 cUSD 转换成任意的系统所支持的合成资产。

在 Coinpro.Exchange 中进行合成资产转换（即交易）时，用户需缴 0.3%（暂定）的手续费，这些手续费进入系统费用池。费用池每两周（暂定）向整个系统符合规定抵押比例的用户进行分红，分红比例按债务比例确定。对于新用户，需持有债务一定天数以上或累积使用一定天数以上（待定），方有资格获得费用池分红。

本系统中所有合成资产的价格或转换汇率，由预言机读取外部交易所数据提供，未来规划可引入去中心化预言机。

### 三、销毁

当抵押 CTO 或 DOT 的用户想要退出系统或减少债务并解锁抵押的 CTO 或 DOT 时，必须首先偿还债务。比如用户通过抵押 CTO 铸造了\$100 的 cUSD，那么就需要销毁\$100 的 cUSD 才能解锁被锁定的 CTO。

需要注意的是，系统中全部用户各自的债务比例，由抵押 CTO 或 DOT 铸造 cUSD 的时候确定，而且和转换之后的其他合成资产的价格无关。只有在用户铸造或销毁 cUSD 时，债务比例才会改变。所有用户债务的总和即抵押池，因为资产价格的变动，会造成债务的变动，通过不变的债务比例，可以计算每个用户的盈利。

## 未来规划

本项目未来仍然有很大的上升空间，包括：

第一、目前项目的合成资产种类由项目方或者社区治理决定。未来计划升级到不同投资者可以自主在本系统上签订任意类型的合约。

第二、目前项目产生的稳定币 cUSD 或其他合成资产都只局限于系统内部。待未来波卡链上有类似于以太坊 ERC-20 的标准化代币时，本项目的合成资产都可以以标准化代币的形式在系统外部流通，甚至进入其他交易所。其中 cUSD 更是可以成为波卡生态中一大重要的稳定币。

## 项目目标

实现一个去中心化的虚拟资产发行平台和合约交易平台，长期不仅可替换各大中心化交易所的永续/期货合约功能，甚至可以在该协议上发行任意类型的资产，在传统金融市场占有一席之地。

## 项目优势

中心化的合约交易所暴露出来的问题越来越多，整个行业需要一个去中心化合约交易所的解决方案。本项目的去中心化合约交易方案，不仅具备了一般 DEX 公开透明、抗审查、不需要 KYC 等特点，而且因为本项目中无需交易对手，完美解决了一般 DEX 在交易深度和流动性上的问题。因此，我们认为本项目的前景非常广大，是真正的 DEX 解决方案。

## 开发路线图

### 一、2020 Q4

- (1) 确定第一批合成资产种类。
- (2) 确定合成资产的数据源，建立白名单机制，实现数据采集。
- (3) 完成预言机功能。
- (4) 实现抵押 DOT 和 CTO，铸造合成资产功能，包括 cUSD、cBTC、cETH、cAAPL、cXAU 等。

### 二、2021 Q1

- (1) 实现抵押池功能：当用户新生成或销毁 cUSD 时，重新确定债务比例，并且根据资产价格变动来计算用户的盈利。
- (2) 实现费用池功能：交易费用划入费用池，完成持 CTO 用户的利益分配。
- (3) 实现去中心化合约交易所 v1.0 版：
  - 1) 实现 Web 端的交易功能，让用户可以自由交易各种合成资产。
  - 2) 方便用户抵押 DOT 和 CTO 铸造 cUSD，以及销毁 cUSD 等操作。
  - 3) 允许用户查看债务比例、系统总债务、个人合成资产的余额、分红收益等。