dFed.finance: 去中心化联邦储备银行，使每个人都能发行货币

team@dfed.finance

1. 总览：超越中心化金融的全新金融机制

阿基米德曾有句著名的话：″给我一个支点，我就可以撬起整个地球。″在经济世界中，借贷就是支点。借贷是基于抵押品，而抵押品的价值是由自由竞争的市场产生的。

已经有一些 DeFi 借贷合约，例如 Compound 和 MakerDao，这些合约通常依靠预言机来评估抵押品。然而，如果没有完全竞争的市场，当抵押品市场价格暴跌时，破产和坏帐就会增加，这会导致经济不稳定。此外，在传统的中心化金融世界中这也是不可避免的。

dFed.finance 认为，只有在完全竞争的市场中产生的抵押品价格可用时，借贷才是有效的。dFed 将建立一个去中心化的系统，该系统将市场交易，借贷和货币发行整合在一起。dFed 将是基于**去中心化流动性交换**的借贷和货币发行市场。在 dFed 中，我们进行抵押贷款并发行货币货币。就像美元的性质是国债一样，dFed 货币的本质是去中心化的债务，这种债务总是有担保的，可以被清算而没有坏账。

dFed 将永久在去中心化的区块链上自动运行。

2. 一个高效的交易所：去中心化借贷的基础

有效市场是所有金融活动的基础。尽管不存在绝对的效率，但我们仍然可以建立足够好的交易所，使抵押品可以一直平稳地清算。

交易对

交易所中有多个交易对。交易对是由两个资产组成的流动资金池（LP）。用户可以按比例同时将这两种资产添加到流动性池中或从中移除流动性。

交易

交易对交易意味着用户将一项资产出售给流动资金池以提取另一项资产。

这两种资产的乘积在交易中将是恒定的，即：

在资产 A 和资产 B 的交易对中，假设 A 的数量为 x，B 的数量为 y，则用户出售 A 的 a 数量，取走 B 的 b 数量。交易后，A 和 B 的乘积保持不变，

$$(x + a) \cdot (y - b) = xy = N$$

由于涉及交易费率 $\boldsymbol{p}$，在此类交易所通常为 0.3%，因此，

$$[x + (1 - p) \cdot a] \cdot (y - b) = xy = N$$

请注意，在其他交易系统中，交易后 N 会更大。新的N =（x+a）•（y−b），再加上被放入流动资金池中交易费。dFed 类似但略有不同：N 始终保持不变。

这种市场（交易所）的优势在于，它通过去中心化的协议高效而简洁地永久运行。

3. 借贷：任何资产都可以作为抵押品的高效借贷

在如此高效的全天候交易所中，我们可以构建借贷系统。dFed 首先构建一个 DEX（去中心化交易所），然后向其添加借贷功能。

对于上述的 A-B 交易对，用户可以抵押 A 的 d 数量来提取 B 的 e 数量，只要

$$[x + (1 - p) \cdot E] \cdot (y - d) = xy = N$$

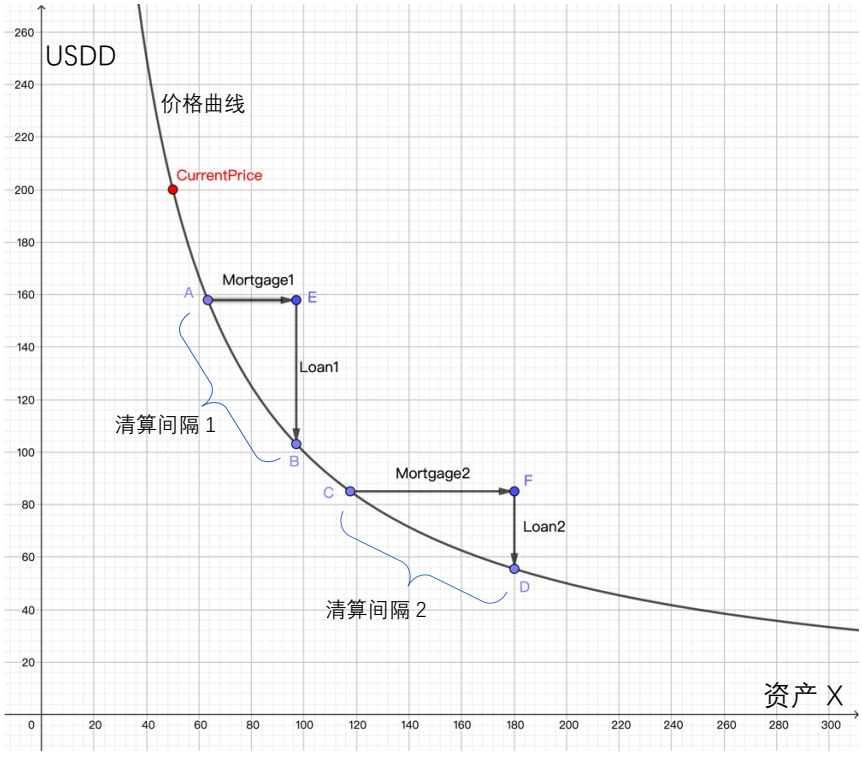
，需 $E \geq e$。它保证了用户通过出售 d 数量的 A 总是可以获得比 e 数量更多的 B。此贷款系统的优点在于，它肯定不会产生任何坏账。

更多的，考虑上借入利息和时间。假设每个时间单位的利率为 r 并且时间为 t，则需要满足：$E \geq e$（1 $+r \cdot t$），我们将其称为 **dFed 放贷必要条件**。退还贷款仅是偿还 B 的 E 数量（我们称为可偿还资产）并提取 A 的 d 数量。

4. 自动清算：没有坏账的清算机制

随着抵押品价格或流动性的降低，减值会上升。当减值将无法偿还可偿还资产时，交易所需要及时出售抵押品以获取可偿还资产并达到平衡。

dFed 的关键设计是**自动清算**。当由于用户操作而导致价格或流动性下降时，dFed 将预计是否需要清算当前准备金贷款（=未付贷款/未清算贷款）。如果是这样，交易所将同时进行清算和用户操作（交易或撤回流动资金池）。清算和用户操作必须是原子操作。



dFed 清算必须保证每个抵押贷款都能偿还其贷款。由于抵押品价格是动态的，因此肯定有一个临界点，必须清算贷款，回购资金恰好等于相应的债务和手续费。我们将

清算间隔定义为从触发清算的转折点到清算结束的价格区间。与传统金融的传导机制类似，清算间隔中有固定的顺序。价格下降时，订单将自动执行。在 dFed 中，任何两笔贷款的清算间隔不得重叠，以确保每次清算绝对安全，且不会产生任何坏账。

清算期间，可能需要同时清算多笔贷款。目标是，在进行清算和用户操作后，所有储备贷款必须满足第 3 节中定义的 dFed 贷款必要条件。

清算可能不需要完全出售所有抵押品。例如，如果资产 A 的 d 数量已抵押，则应偿还资产 B 的$e\cdot(1+r\cdot t)$数量。在清算中，出售 d' 数量的 A 以偿还债务（$d'<d$）。超出的部分将退还给借款人。

5. 货币：每个人都可以发行的货币

在 dFed 中，货币是 USDD，一种稳定的数字货币，与美元一对一固定。USDD 始终是 dFed 中交易对的其中一项资产。USDD 只能通过两种方式发行：

1）通过与美元一对一兑换的其他稳定币交换而发行。

2）通过抵押资产发行。

在方式 1 中，dFed 目前仅支持 USDT，将来将支持更稳定的稳定币。USDT 和 USDD 可通过智能合约自由进行双向交换。

在方式 2 中，由于存在特定资产和 USDD 的交易对，因此用户可以抵押该资产以发行新的 USDD。新发行的 USDD 值将不大于抵押品的价值。当抵押品价格下降且抵押贷款被清算时，或者当用户退还 USDD 时，交易所将烧掉所收取的 USDD。

方式 2 中新发行的 USDD 也可以自由兑换为 USDT。由于 USDD 的流通量肯定不大于流动资金池中的锁定数量，因此交换将始终安全，顺畅，不会被挤兑。

6. 治理和激励：全部属于民众

货币发行基于抵押；抵押是基于有效的市场；有效的市场是建立在充足的流动性基础上的。显然，为 dFed 提供流动性的活动应得到回报。

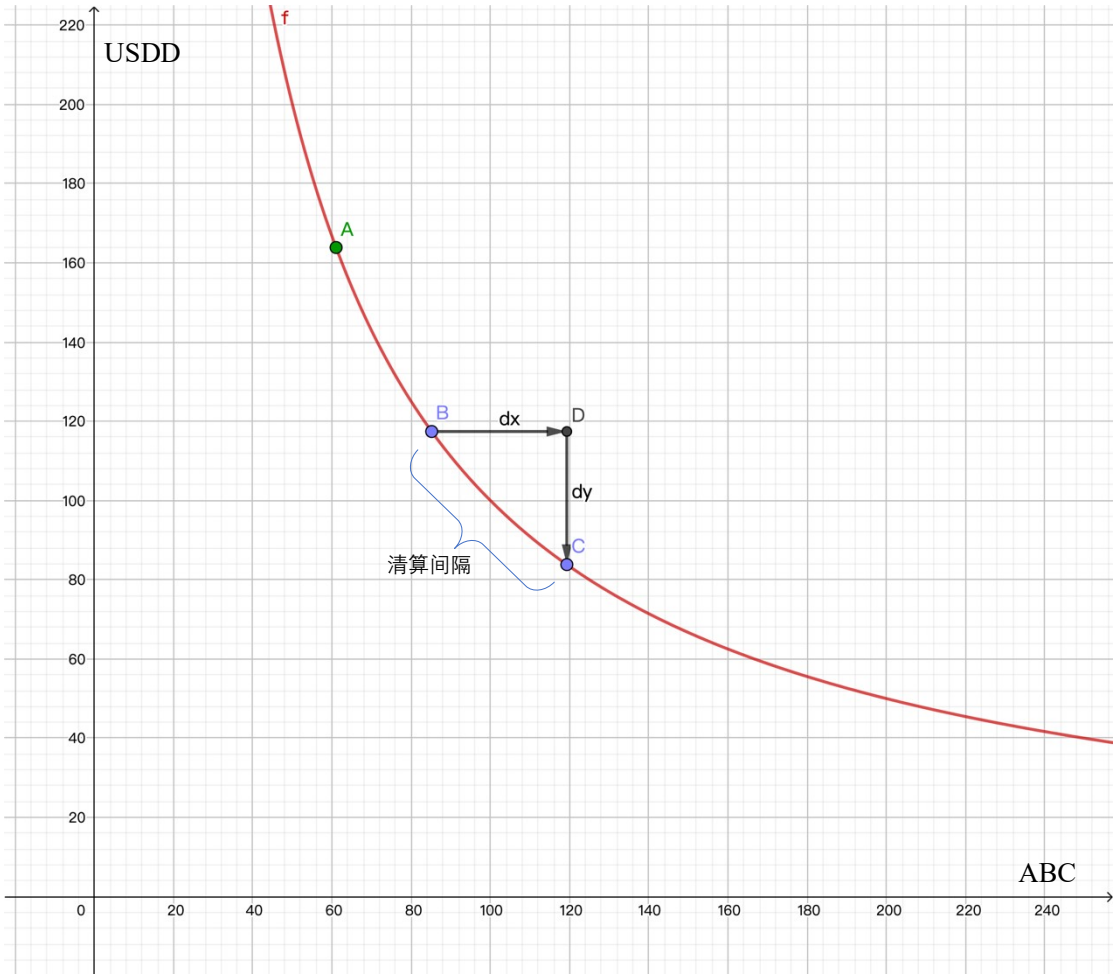
向流动资金池提供流动性的所有用户都将获得 FED 治理令牌的奖励，该令牌被定义为 dFed 中的挖矿。他们提供的流动性越多和时间越长，他们将获得的 FED 代币越多。

FED 代币仅代表治理权，没有任何其他价值或资产映射。持有 FED 令牌的用户可以参与 dFed 的治理。

请注意，所有交易费用均以 USDD 收取。在 FED-USDD 交易对中，交易费用将用于在市场上回购和燃烧 FED 代币。回购实质上是将交易费分配给所有 FED 持有人。

附录:

1. **清算间隔的定义**

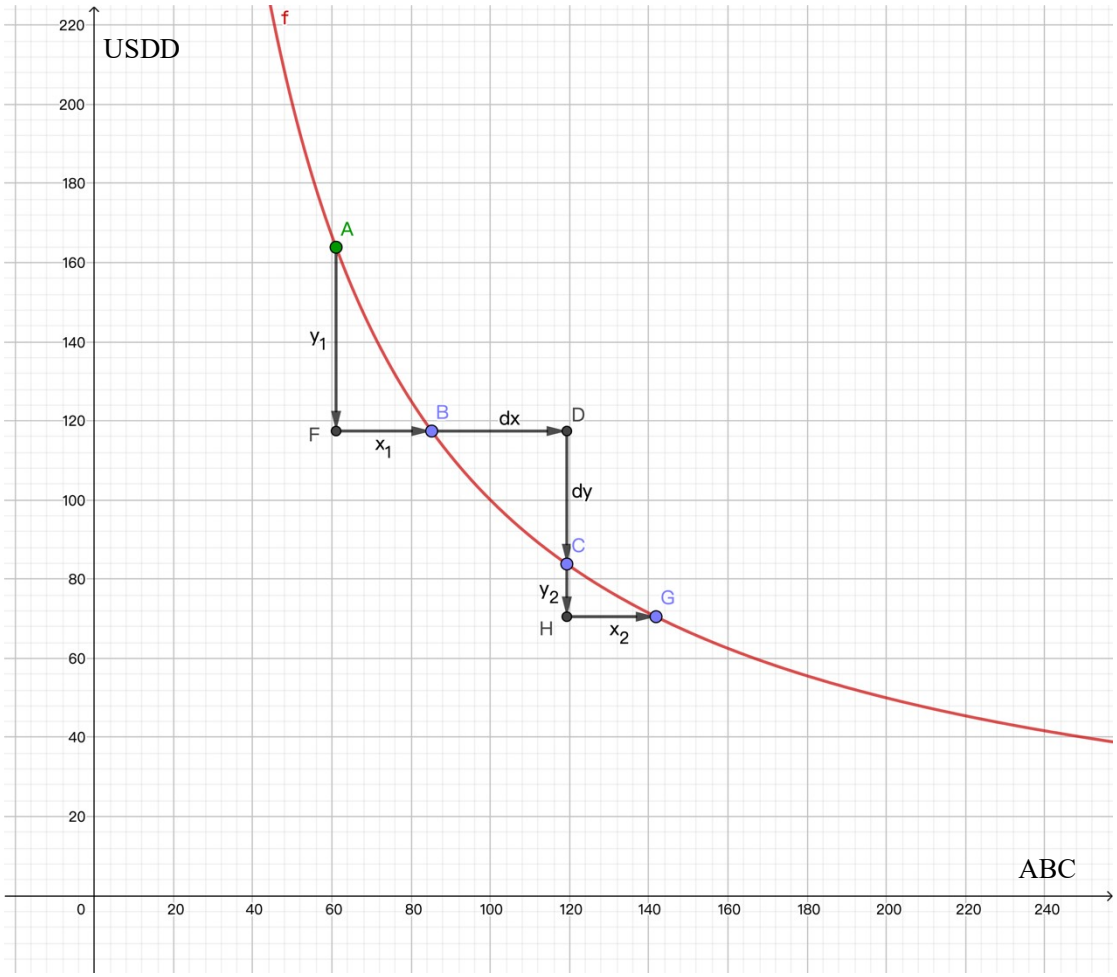


如图所示，f 是 ABC-USDD 交易对的交易曲线。X 轴是 ABC 的数量。Y 轴是 USDD 的数量。由于流动资金池保持恒定，因此对于曲线 f 上的任何点，xy = N。N 是一个常数。点 A 是当前价格。

对于贷款，将资产 ABC 的 dx 数量抵押，并生成 dy USDD 数量的债务。（为方便起见，dy 包含利息和交易费用。）价格 B 可以根据 dx 和 dy 计算，这笔贷款必须可被清算。清算后，价格变成 C，$Cx\text{-}Bx{=}dx$和$By\text{-}Cy = dy$. 也就是说，出售 dx 数量的 ABC 的资金正好足以偿还 dy 数量的 USDD 的债务。

我们将 B 和 C 之间的间隔定义为**清算间隔**。

2. 卖出代币造成的清算

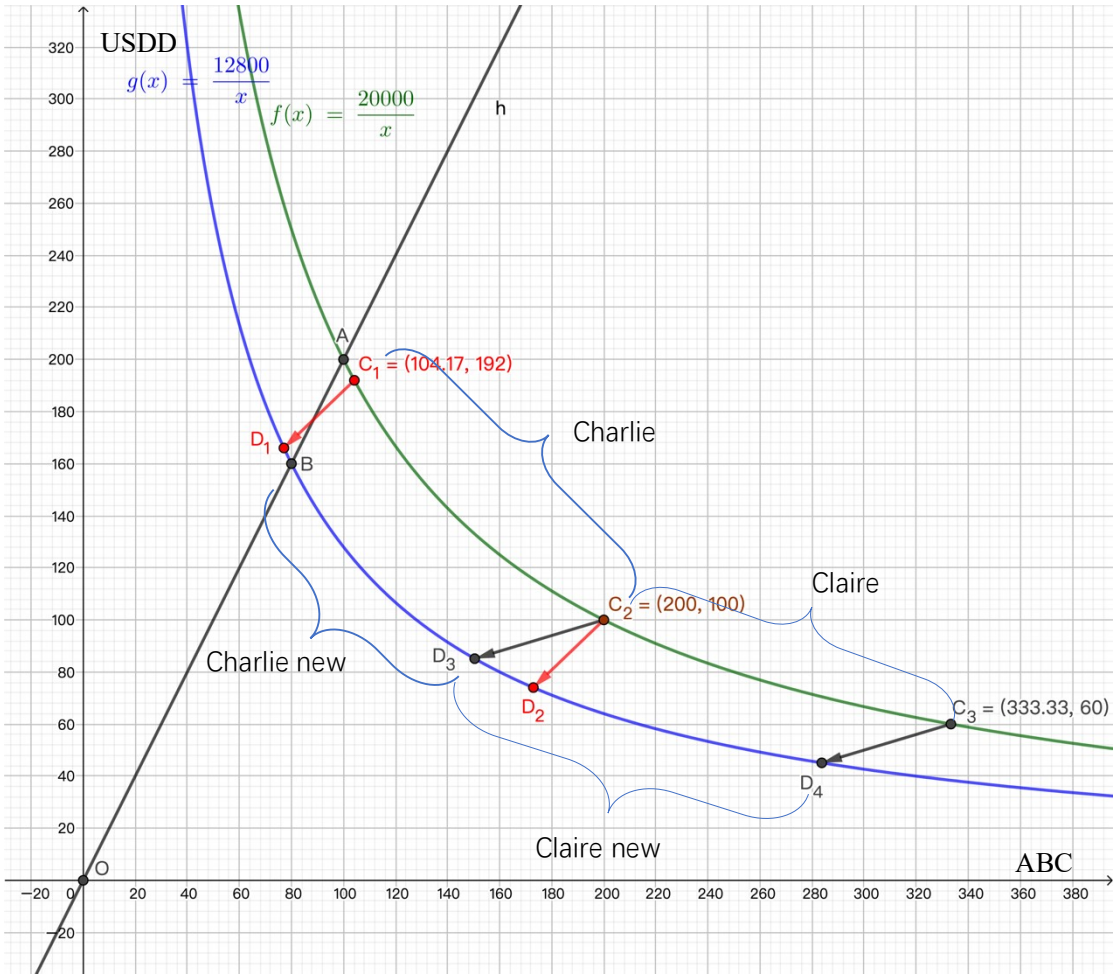


还是上图，如果我们开始从价格 A 卖出 ABC 并卖出多于 x_1 的数量，那么价格将达到 B 点，B 和 C 之间的贷款将被清算。

假设出售的 ABC 数量不超过 x_1，则卖出逻辑与普通的 Uniswap（无需清算）相同。

假设用户 Alex 想要出售多于 x_1 的 ABC，它将触发价格下跌导致的清算。假设 Alex 要卖出 x 个 ABC。首先，他出售的第一笔 x_1 个 ABC 交换为 y_1 个 USDD。然后，dFed 开始清算，出售 d_x 个 ABC 以换取 d_y 个 USDD 来清算这笔抵押贷款。清算是自动的，与 Alex 的操作无关。然后，Alex 继续从价格 C 卖出另一笔 x_2 个 ABC，得到 y_2 个 USDD。到现在为止，整个卖出结束，$x_1 + x_2 = x$，Alex 最终得到 $y_1 + y_2$ 个 USDD。

3. 移除流动性导致的清算



当 Alex 要从流动资金池中移除流动性时，事情变得有些复杂。

假设在 ABC-USDD 交易对中，总共有 100 个 ABC 和 200 个 USDD。交易曲线为 f（x）= 20000 / x（对于 100 * 200 = 20000）。价格在 A 点。Alex 持有 20%的流动资金池，包括 20 个 ABC 和 40 个 USDD。他要提币。

复杂的地方来了。原始曲线 f（x）中有两个清算间隔，分别是 Charlie 从 C_1 到 C_2 的抵押和 Claire 从 C_2 到 C_3 的抵押。这两个间隔完全相邻。但是，在移除流动性后，Charlie 的清算间隔 C_1C_2 更改为 D_1D_2，而 Claire 的 C_2C_3 更改为 D_3D_4。这会出现两个问题：

1. D_1 超出当前价格 B。
2. D_1D_2 和 D_3D_4 部分重叠。

dFed 是这样解决的：

对于问题 1，Alex 需要向交易所支付 BD_1 间隔的余额，即 Alex 从他的提币中支付 D_1y-By 个 USDD 并获得 Bx-D_1x 个 ABC 作为回报。换句话说，Alex 需要清算 BD_1 间隔以保证抵押物价值可以平衡剩余的抵押贷款。这样，间隔 D_1D_2 被切成 BD_2。

对于问题 2，为了清算重叠部分，遵循首先清算价格较高（质押率更高）的抵押贷款的原则，Charlie 的区间 BD_2 需要切断重叠部分，而仅保留 BD_3。以这种方式，原始间隔 C_1C_2 和 C_2C_3 变为 BD_3 和 D_3D_4。

然而，如何裁剪间隔 D_3D_2？此间隔表示以 D_2x-D_3x 个 ABC 抵押 借 D_3y-D_2y 个 USDD。如果 Alex 交易了担保的这一部分，他可能会恶意清算其他人的抵押贷款进行套利，因为他可以以较低的价格购买 ABC（因为价格 D_2 和 D_3 低于价格 B）。dFed 将从这笔抵押贷款中移除 D_2x-D_3x 个 ABC，并相应锁定 D_3y-D_2y 个 USDD。Alex 将暂时无法提取这笔 USDD。我们将这笔钱记录为 Alex 的贷记，以后可以取回资金取回有两种情况。一种是，当 Charlie 偿还贷款时，Alex 可以取回相应的美元。另一种是，在 Charlie 的抵押贷款 BD_3 清算后，Alex 只能在这种情况下获得相应的 ABC 来收回其贷记。