dFed.finance: Decentralized Federal Reserve Board

that Enable Everyone to Issue Currency

team@dfed.finance

1. Overall: a brand-new finance mechanism full beyond CeFi

Archimedes had a prominent saying: give me a fulcrum and I can pry up the whole earth. In the economic world, borrowing and lending are the fulcrum. Borrowing and lending are based on collateral while the value of collateral is generated by a free and competitive market.

There have been several DeFi lending programs such as Compound and MakerDao that normally rely on oracles to evaluate collateral. However, without a fully competitive market, insolvency and bad debts turn up when collateral market price collapses, which leads to the instability of the economy. Moreover, it's also inevitable in the traditional CeFi world.

dFed.finance believes, borrowing and lending are effective only when collateral price is valid by being generated in a fully competitive market. dFed will establish a decentralized system that integrates market dealing, borrowing & lending, and currency-issuing. dFed will be a lending and currency-issuing market based on a decentralized exchange of **Liquidity Pool**. In dFed, we conduct loans and issue monetary currency backed by collaterals. Just as the nature of the US dollar is the national debt, the essence of dFed currency is a decentralized debt which is always guaranteed and can be liquidated with no bad debts invariably.

dFed will autonomously run on a decentralized blockchain permanently.

2. An efficient exchange: the foundation of decentralized lending

An efficient market is the foundation of all finance activities. Though absolute efficiency doesn't exist, still we can build a good-enough exchange where collaterals can be liquidated smoothly all the time.

Trading Pair

There are multiple trading pairs in the exchange. A trading pair is a Liquidity Pool (LP) consisting of two assets. Users can concurrently add or withdraw the two assets to the liquidity pool on a pro-rata basis.

Trading

Trading in the pair means users sell one asset to the Liquid Pool to withdraw the other asset. The product of the two assets will be constant in trading, which is:

In the trading pair of Asset A and Asset B, assuming that the amount of A is x and the amount of B is y, users sell the a amount of A and withdraw the b amount of B. After trading, the product of A and B remains unchanged,

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

Involving in the transaction fee rate p, commonly 0.3% in such exchanges, then,

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

Note that in other trading systems N will be larger after trading. The new $N = (x + a) \cdot (y - b)$, with transaction fee is put into the liquidity pool. dFed is similar but slightly different: N remains unchanged all the time.

The advantage of this kind of market (or exchange) is that, it runs efficiently and concisely by a decentralized protocol forever.

3. Lending: high-convenient borrowing and lending with any assets can be collaterals

In such an efficient all-day exchange above, we can build the borrowing and lending system. dFed first builds a DEX (Decentralized Exchange) and then add the lending function to it.

For the above A-B trading pair, users can mortgage the ***d*** amount of A to withdraw the ***e*** amount of B, as long as

$$(x + d) \cdot (y - \frac{E}{1 - p}) = xy = N$$

, where $E \geq e$. It guarantees that users can always get more than ***e*** amount of B by selling ***d*** amount of A.

The merit of this lending system is that it will certainly not generate any bad debts.

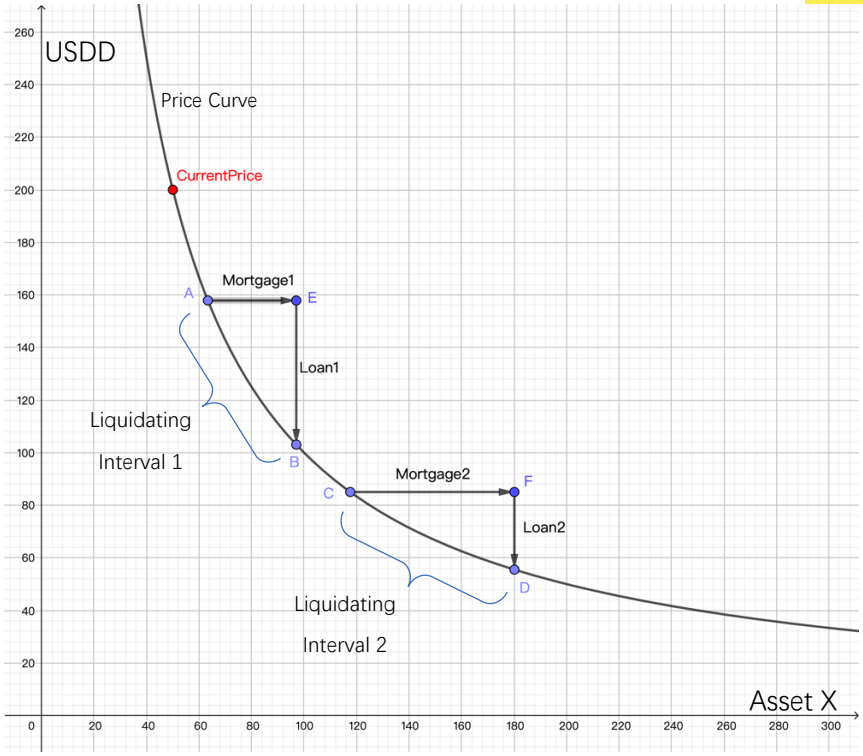
Moreover, consider the borrowing interests and time now. Assuming the interest rate per time unit is ***r*** and the time is ***t***, it needs to meet: $E \geq e \cdot (1 + r \cdot t)$, which we call **dFed Lending Necessary Condition**.

To return the loan is simply to repay the ***E*** amount of B (which we call Repayable Assets) and to withdraw the ***d*** amount of A.

4. Autonomous liquidating: a liquidating mechanism with no bad debts

As collateral price or liquidity decreases, impairment turns up. When the impairment is about to be unable to cover the repayable assets, the exchange needs to sell the collateral in time to get the repayable assets and achieve balance.

The key design of dFed is **autonomous liquidating**. When price or liquidity decreases caused by user operations, dFed will anticipate whether liquidating is required for the current reserve loans (which equals un-paid loans/un-liquidated loans). If so, the exchange will conduct the liquidating and user operating (trading or withdrawing the liquid pool) at the same time. The liquidating and user operating must be an atomic operation.



dFed liquidating must guarantee every mortgage cover its loan. As the collateral price is dynamic, there is certainly a tipping point at which the loan must be liquidated and the buy-back funds exactly equals the corresponding debts and fees. We define **Liquidating Interval** as the interval from the tipping point that triggers the liquidation, to the point where liquidation finishes. By analogy with traditional CeFi conductions, it's like there is a fixed order in the Liquidating Interval. When the price goes down, the order will be conducted autonomously. In dFed, the Liquidating Intervals of any two loans must not overlap, so as to guarantee that every liquidation is absolutely safe without generating any bad debts.

During liquidating, there might be multiple loans that need to be cleared at the same time. The goal is, after the conductions of liquidating and user operating, all the reserve loans must meet the **dFed Lending Necessary Condition** that is defined in Section 3.

Liquidating may not require the complete sale of all the collaterals. For example, if the ***d*** amount of Asset A is mortgaged, the $e \cdot (1 + r \cdot t)$ amount of Asset B should be repaid. In the liquidating, funds from selling d' A is enough to pay the debts ($d' < d$). The excess $d - d'$ A will be returned to the borrower.

5. Currency: a monetary currency everyone can issue

In dFed, the monetary currency is USDD, a stable digital cash one-to-one pegged to the US dollar. USDD is always one asset of a trading pair in dFed. USDD can only be issued by two modes：

1). issued by exchanging with other stable coins which are also one-to-one pegged to the US dollar.

2). issued by mortgaging assets.

In mode 1, dFed only supports USDT for now and will support more stable coins in the future. USDT and USDD are freely two-way exchangeable conducted by smart contracts.

In mode 2, as there is a trading pair of a certain asset and USDD, users can mortgage this asset to issue new USDD. The new-issued USDD value will not be greater than the value of the collateral. When the collateral price goes down and the mortgage is liquidated, or when the USDD is returned by the users, the exchange will burn the USDD it collects back.

The newly issued USDD in mode 2 can also be exchanged to USDT freely. As the USDD circulation is certainly no larger than the locked amount in the liquidity pool, exchanging will always be safe and smooth with no bank runs.

6. Governance and rewards: all belong to people

Currency issuing is based on mortgaging; mortgaging is based on efficient market; efficient market is based on abundant liquidity. Apparently, the activity of providing liquidity for dFed shall be rewarded.

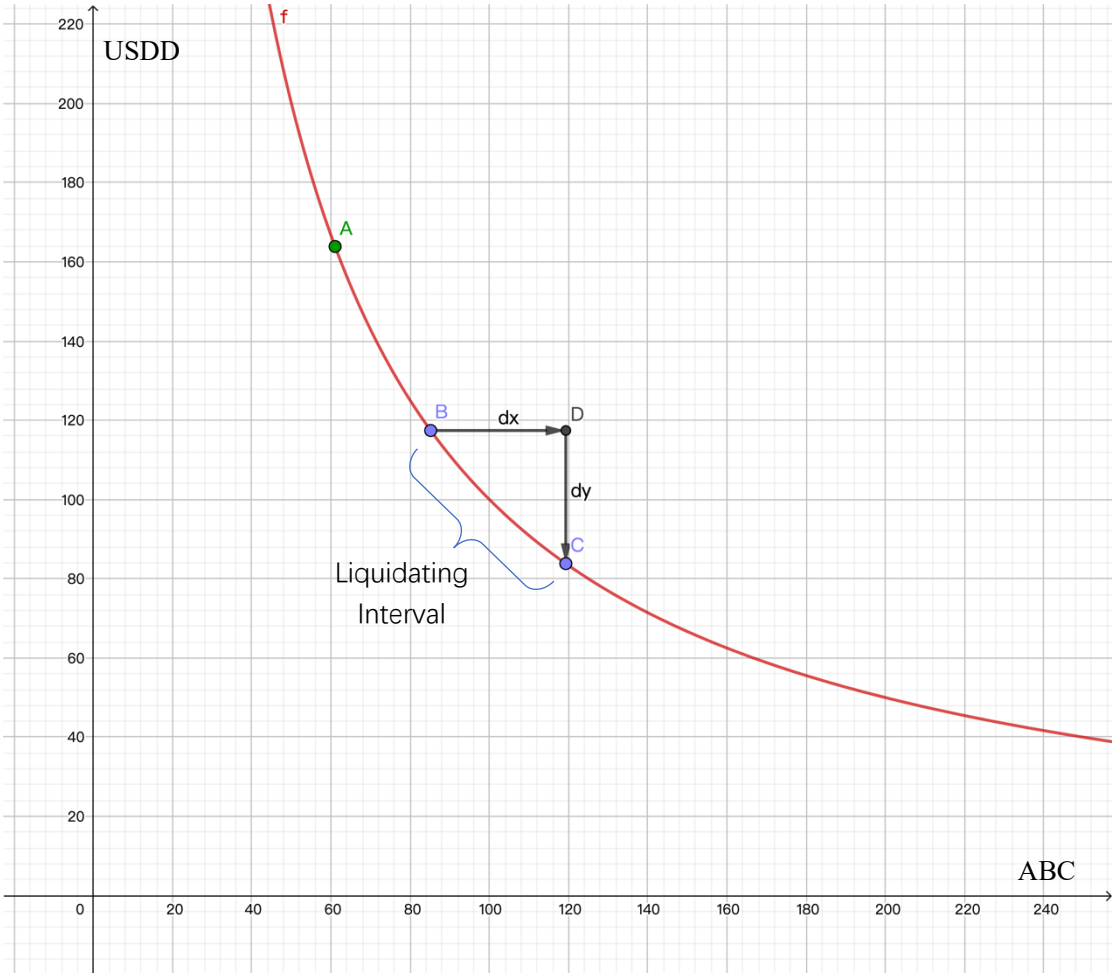
All the users that provide liquidity to the pool will be rewarded of the FED governance tokens, which is defined as **mining** in dFed. The more and the longer liquidity they provide, the more FED tokens they will get.

FED tokens only represent the governance rights without any other value or asset mapping. Users who hold FED tokens can participate in the governance of dFed.

Note that all the transaction fees are charged in USDD. In the FED-USDD trading pair, the transaction fees will be used to buy back and burn the FED tokens in the market. Buy-back is to distribute the transaction fees to all FED holders in essence.

Appendix:

1. Definition of Liquidating Interval

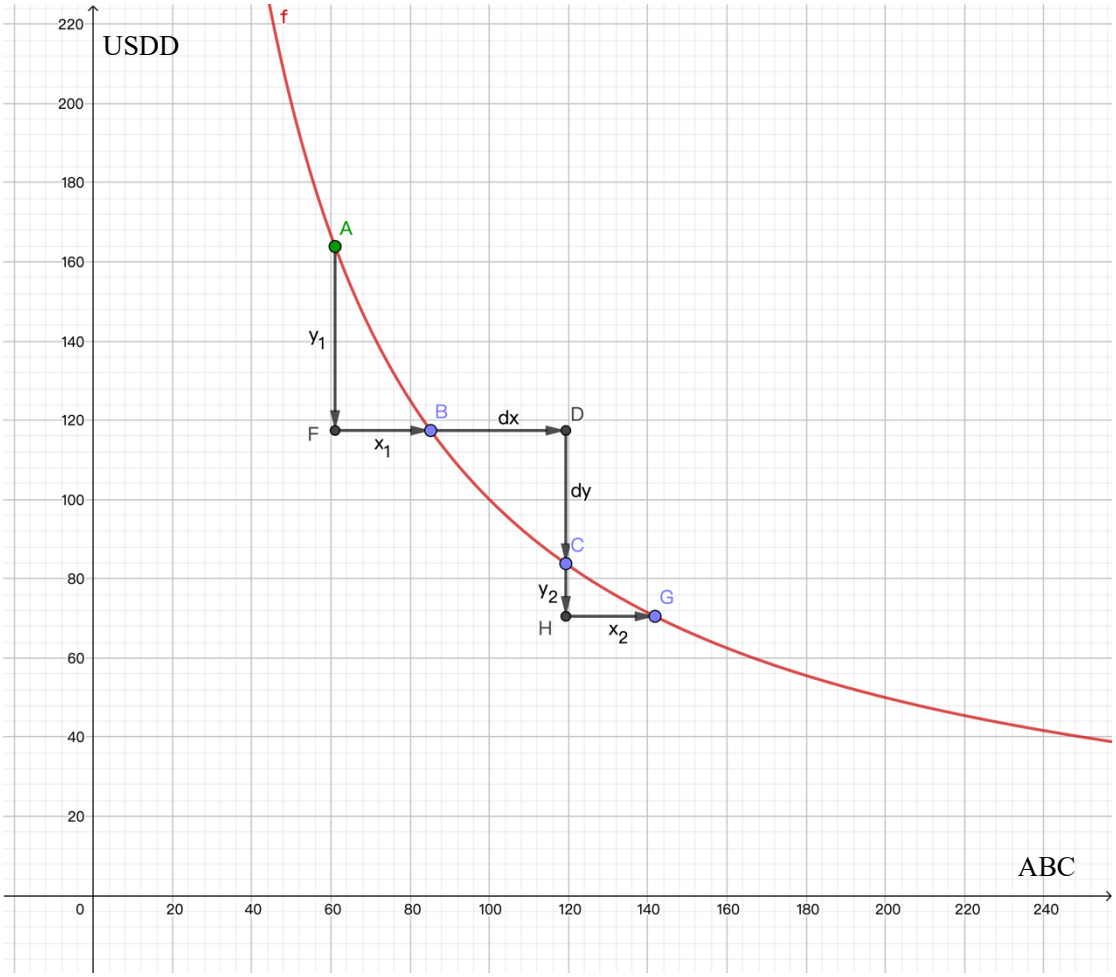


As shown in the figure, ***f*** is the trading curve of the ABC-USDD trading pair. X-axis is the amount of ABC. Y-axis is the amount of USDD. As the liquidity pool remains constant, for any point on curve ***f***, ***xy=N***. ***N*** is a constant. Point A is the current price.

For a loan, the ***dx*** amount of Asset ABC is mortgaged and the ***dy*** amount of USDD debts is generated. (For convenience, ***dy*** contains the interests and transaction fees.) Price B can be calculated from ***dx*** and ***dy***, at which this loan must be liquidated. After the liquidation, the price goes to C, where $C.x - B.x = dx$ and $B.y - C.y = dy$. That is, funds from selling ***dx*** amount of ABC is exactly enough to pay the debts of ***dy*** amount of USDD.

We define this interval between B and C as the **Liquidating Interval**.

2. Liquidating Caused by Selling Tokens

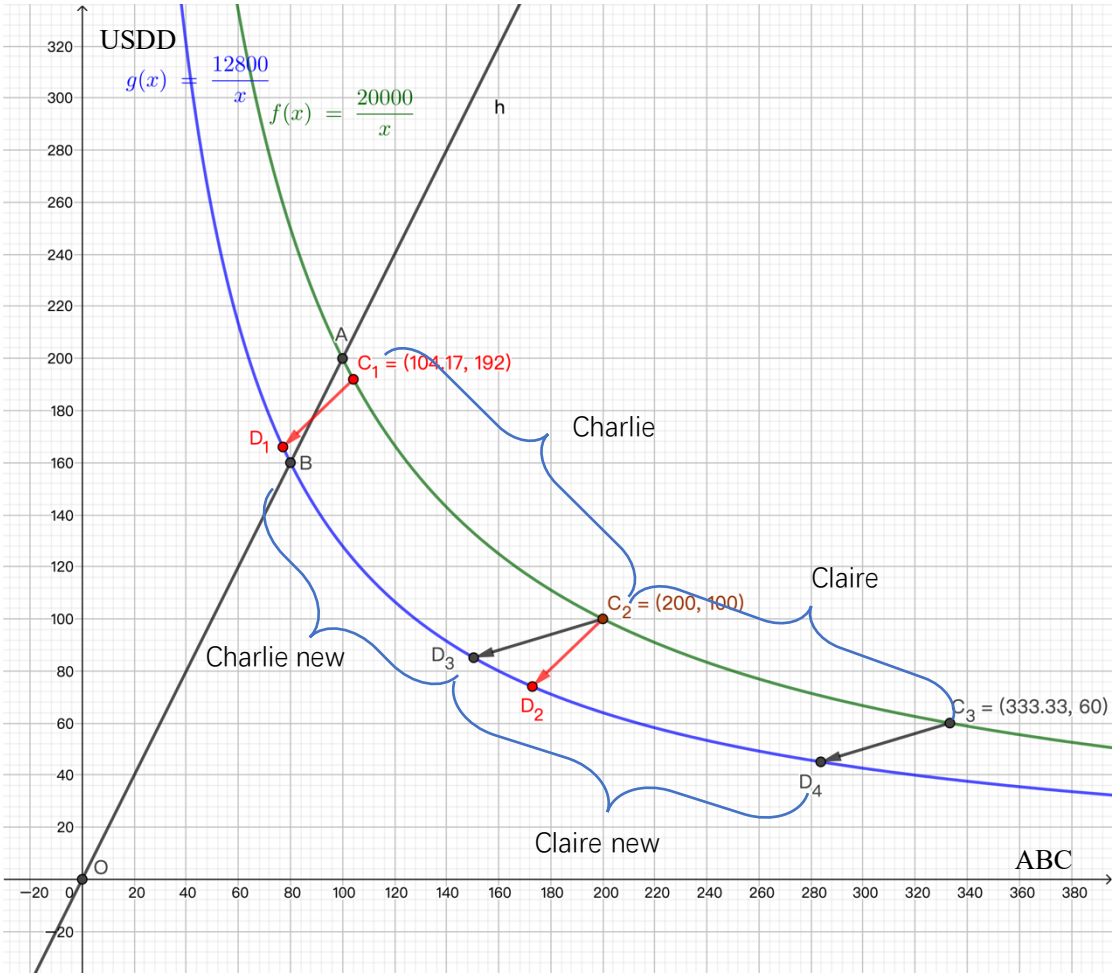


Still in the above figure, if we start to sell ABC from price A and sell more than ***x1*** amount, the price will go to the B point and the loan between B and C will be liquidated.

Assuming no more than x_1 ABC is sold, the sale logic is same as normal Uniswap in which there is no need to liquidate.

Assuming user Alex wants to sell more than x_1 ABC, it will trigger a liquidation caused by price decreasing. Let's say Alex is going to sell x ABC. To begin with, the first x_1 ABC he sells is exchanged to y_1 USDD. Then, dFed starts a liquidation in which dx ABC is sold to exchange for dy USDD to clear this loan. The liquidating is autonomous, independently of Alex's operation. And then, Alex continues to sell another x_2 ABC from price C and get y_2 USDD. Till now, the whole selling is finished while $x_1+x_2=x$ and Alex get y_1+y_2 USDD in the end.

3. Liquidating Caused by Removing Liquidity



When Alex is going to remove liquidity from the pool, things become a little complex.

Assume in the ABC-USDD trading pair, there are 100 ABC and 200 USDD totally. The trading cure is f(x)=20000/x (for 100*200=20000). The price is at point A. Alex holds 20% of the liquidity pool including 20 ABC and 40 USDD. He is going to withdraw.

Here comes the complexity. There were two liquidating intervals in the original cure f(x), that are Charlie's mortgage from C_1 to C_2 and Claire's mortgage from C_2 to C_3. The two intervals are fully adjacent. However, after the liquidity is removed, Charlie's liquidating interval C_1C_2 changes to D_1D_2 while Claire's C_2C_3 to D_3D_4. Two problems come up:

1. D_1 is beyond the current price B.
2. D_1D_2 and D_3D_4 are partly overlapped.

dFed solve the problems as following:

For problem 1, Alex needs to cover the exchange balance in the interval BD_1, which is, Alex pay $D_1.y - B.y$ USDD from his withdraw funds and get $B.x - D_1.x$ ABC in return. In other words, Alex needs to liquidate the BD_1 interval to guarantee that the collateral value can balance the loan in the remaining mortgage. In this way, the interval D_1D_2 is cut to BD_2.

For problem 2, to liquidate the overlap, following the principle that the mortgage with higher price (higher pledge rate) is liquidated first, Charlie's interval BD_2 needs to cut off the overlap, remaining only BD_3. In this way, the original intervals C_1C_2 and C_2C_3 become BD_3 and D_3D_4.

Then, how to conduct the cropped interval D_3D_2? This interval represents a loan of $D_3.y - D_2.y$ USDD and a collateral of $D_2.x - D_3.x$ ABC. If this part of the pledge was also exchanged by Alex, he could maliciously liquidate other's mortgage for arbitrage, for he could buy ABC at a lower price (as price D_2 and D_3 are lower than price B). dFed will remove $D_2.x - D_3.x$ ABC from this mortgage and lock $D_3.y - D_2.y$ USDD correspondingly. Alex won't be able to withdraw this amount of USDD temporarily. We record this money as Alex's credit which he can retrieve in the future. There will be two circumstance for retrieving. The one is, when Charlie repays his loan， Alex can get the corresponding USDD back. The other is, when Charlie's mortgage BD_3 is liquidated, Alex can only get the corresponding ABC to recover his credit under this circumstance.