Moremoney: Decentralized borrowing protocol for liquid and illiquid tokens

October 29, 2021

Abstract

The Moremoney protocol offers collateralized debt positions (CDP) with liquid and illiquid collateral at a 0% interest rate, allowing users to extract value from their assets by borrowing *USDm*, a USD-pegged stablecoin. Upon depositing, collateral assets are diverted to partner protocols where these tokens earn yield. Harvested yield is either converted to USDm and distributed back to depositors, automatically repaying their debt or compounded into the collateral token.

1 Introduction

Moremoney is a decentralized protocol uniting key pillars of the DeFi ecosystem:

- NFTs, AMM liquidity provision, and other valuable illiquid assets
- Stablecoins and overcollateralized lending
- Yield farming

Moremoney presents a further iteration in the compounding value chain of functionality, fungibility, and yield. Users of Moremoney can deposit their (potentially illiquid) assets as collateral to mint USDm, the stablecoin of the Moremoney Protocol. The collateral is then forwarded to yield generating protocols like compound, yearn or other vetted platforms and automatically repays the loan, by converting harvested yield to USDm.

1.1 Core characteristics of the Moremoney protocol

- Interest-free lending to borrowers
- Liquid and illiquid, fungible and non-fungible assets as collateral
- Flexible collateralization ratio
- Yield earned on collateral as self-repaying loans
- DeFi insurance layer
- Extensible architecture to support growth

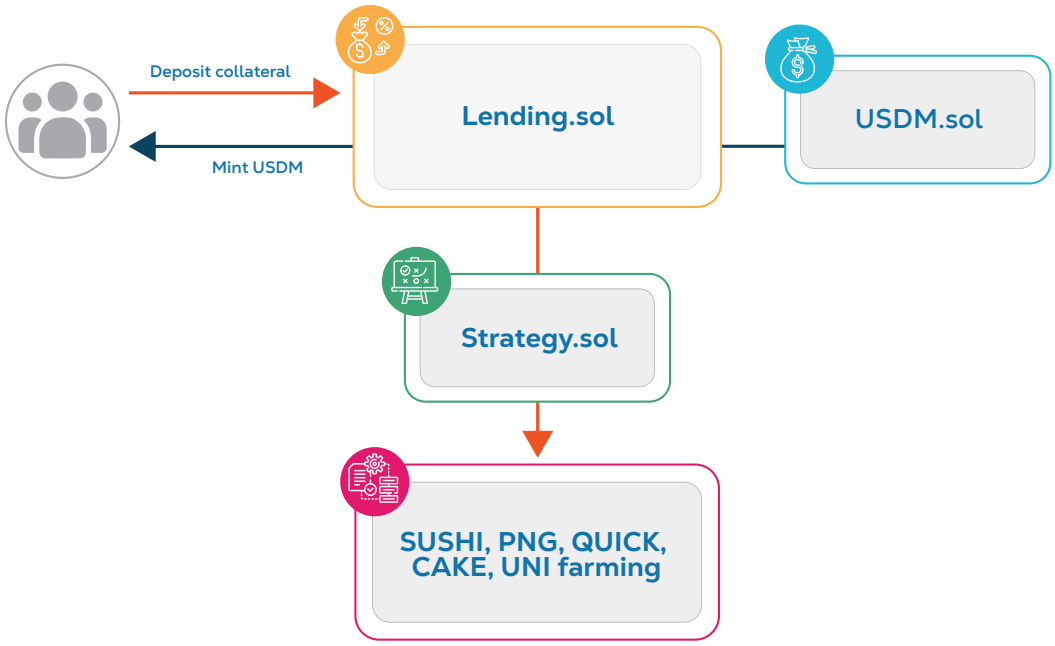

Figure 1: Depositing and borrowing

1.2 Example workflow

1.2.1 Depositing and borrowing

1. Alice holds Liquidity Pool Tokens in a supported pair.
2. She deposits these tokens into the Moremoney lending contract for that LP token and requests a loan in USDm.
3. The lending contract withdraws the LPT from her wallet and deposits it into a yield-earning contract, such as an incentive contract run by the DEX.
4. The contract checks the collateralization ratio for Alice's account using a price oracle.
5. Alice receives USDm, and is charged a minting fee.
6. She can trade her USDm on exchanges, add liquidity to farm *MORE* or provide it as collateral for margin trading, etc.

1.2.2 Yield harvesting

1. Bob has a significant collateral position in the same LPT and wishes to realize gains generated in his account.

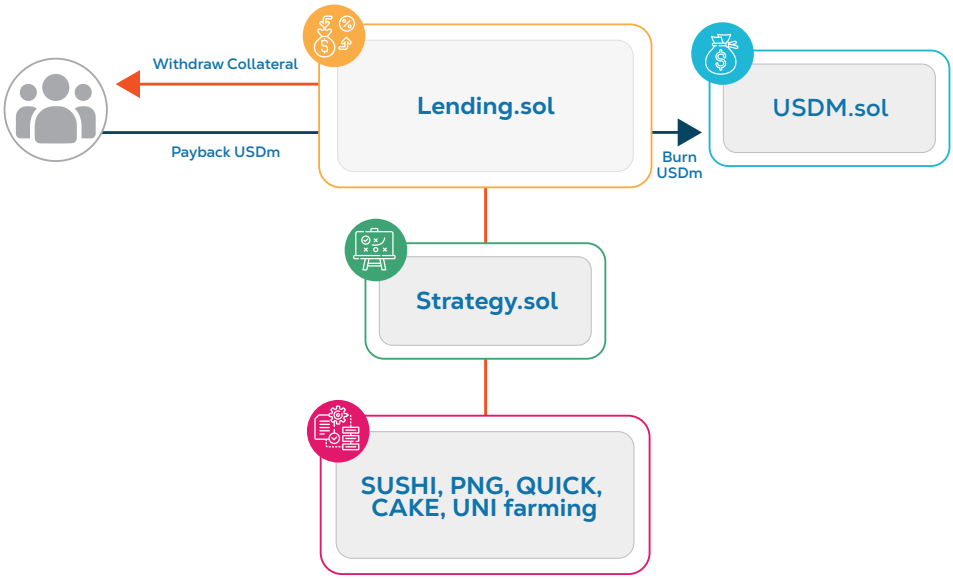

Figure 2: Yield harvesting

2. He submits a transaction requesting that the lending contract for the LPT harvest yield that has accumulated.
3. The harvested yield (in some other currency) gets converted into USDm using open market transactions.
4. The total amount of harvest in USDm is recorded for future distribution.
5. Alternatively to explicit calls, other Moremoney calls harvest yield regularly, distributing and extinguishing users' debt.

1.2.3 Withdrawing collateral

1. Alice re-acquires USDm in the amount of her outstanding debt.
2. She requests a withdrawal of collateral and extinguishing of her loan by depositing USDm.
3. The lending contract first applies any yield credits that Alice's account may be eligible for, diminishing her USDm loan.
4. Her debt is extinguished in the amount of her deposited USDm and the deposited tokens are burnt.
5. Alice's requested collateral is disbursed to her wallet.
6. If any debt remains, the contract checks the collateralization ratio.

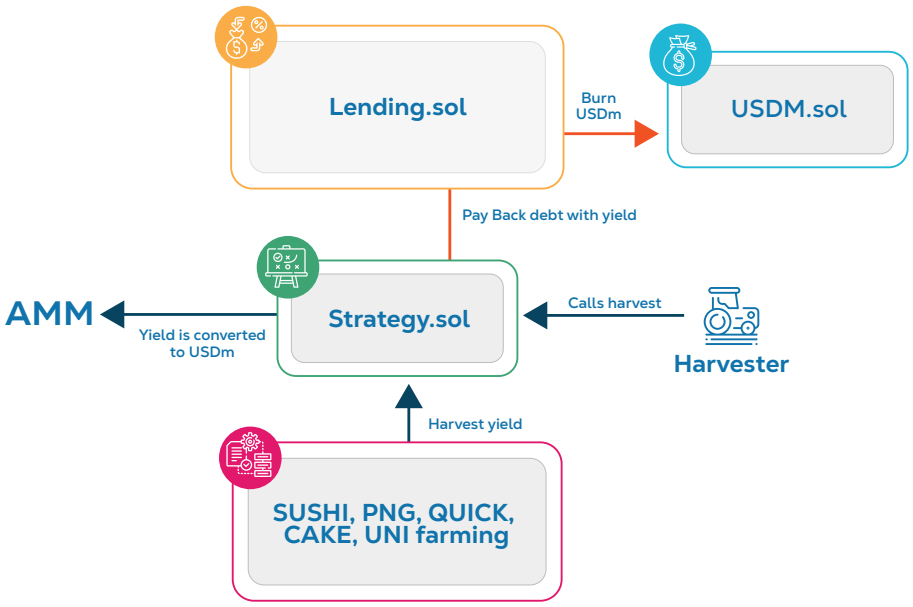

Figure 3: Withdrawing collateral

1.2.4 Borrowing against an NFT

1. Aice holds a valuabel NFT.
2. She deposits the NFT into the Moremoney NFT lending contract and specifies how much she is looking to borrow maximally and minimally, as well as the duration of the loan.
3. If her NFT is whitelisted to have an on-chain oracle of value, she can already mint and withdraw a fraction of the NFT's ultimate value in USDm.
4. If her NFT is compatible with some yield generating platform (be it royalties or some incentive scheme), her NFT is forwarded to generate yield.
5. An auction process is initialized where USDm holders can deposit bids to liquidate her NFT in the event that Alice does not return her loan in time to unlock her NFT. Bob has the winning bid to liquidate Alice.
6. In case Alice's NFT is not whitelisted, her ability to borrow is limited to Bob's highest liquidation bid, maximally.
7. After her lock-in period is over, Alice can return her loan plus fees and a liquidator premium to unlock her NFT.
8. If Alice fails to do so within a grace period, Bob can liquidate the debt position and withdraw the NFT.

Optionally, Bob's winning bid itself can be tokenized as an NFT, which in turn could be submitted to the above process, repeating the cycle of lending as often as is expedient and attractive.

1.3 Related work in Decentralized Finance

Decentralized finance(DeFi) is a form of finance that does not rely on central intermediaries such as brokerages, exchanges, or banks to offer traditional financial instruments, instead utilizing smart contracts on blockchains. DeFi platforms offer price-setting exchanges, lending, and borrowing of funds, derivatives, and other forms of price speculation movements on a range of assets using derivatives, insurance instruments, and interest-yielding accounts.

1.3.1 Lending

Overcollateralized lending was popularized by the Compound protocol [LH19], where token holders wishing to participate in financial interactions denominated in a different currency from the one they hold can do so without relinquishing their original holding. They deposit their token as collateral and then borrow up to a certain threshold against its current value, but always less than what they deposited, risking liquidation in the case of extreme price swings. MakerDAO [Tea17] pioneered minting a stablecoin 'DAI' for lending against the deposited asset.

1.3.2 Yield Farming

Yield farming protocols bundle and optimize resource allocation across a wide variety of yield generation opportunities. They have gained widespread popularity in DeFi, following the successful example of secure, distributed yield aggregators such as Yearn. Many yield farming protocols incentivize contribution and interaction with their platform by offering protocol governance tokens.

1.3.3 On-chain illiquid assets

A variety of valuable yet illiquid asset classes have been gaining importance in the DeFi ecosystem:

Liquidity Pool Tokens (LPT): Automated Market Makers (AMMs) such as Uniswap [AZS+21] have tokenized ownership of liquidity within a pair. These tokens provide access to fees earned and represent a certain amount of value via the underlying asset. Nevertheless, they mostly cannot be traded on decentralized or centralized exchanges nor used as collateral in other contexts. Effectively, the act of re-representing the value of the underlying assets renders it incompatible with the rest of the DeFi ecosystem.

Non Fungible Tokens: Popular in the art world as well as in consolidated liquidity AMMs such as Uniswap v3, these assets provide a store of value which is prima facie indivisible and unique, but in some instances can be estimated effectively, on-chain.

Synthetic Assets: Synthetic and representative tokens like xSUSHI or bBADGER are issued when SUSHI or BADGER is staked. These tokens mostly have no liquidity on any market but the underlying assets they represent are very liquid.

2 Protocol structure

The protocol is implemented as a collection of smart contracts on ethereum-compatible networks. At the core of the protocol lie two tokens: the governance token and a mintable stablecoin. They are flanked by a family of lending contracts, each with a different collateral class or yield generation strategy. The whole protocol is supported by ancillary contracts for roles management and handling protocol funds.

When applicable, we shall use Liquidity Pool Tokens as a running example of a characteristic collateral class, though a wider variety of collateral will be accepted by the protocol.

2.1 Lending stable against collateral

2.1.1 Collateralization ratio

A user can borrow stablecoin up to a certain percentage threshold, set to be strictly less in value than the value of the deposited collateral.

Definition 2.1. Collateralization ratio $rc_{A,u}$ for an asset A and user u is defined as:

$$rc_A = \mathcal{V}_A(D_u)/L_u$$

Where $\mathcal{V}_A$ is the valuation oracle for asset A, mapping amounts of A to *USD*.

Collateralization ratios can be set per asset, by governance, according to the risk profile of the collateral class, ranging from 105% to 200%.

2.1.2 Price oracle

The Moremoney protocol is designed to handle assets that may not be liquid or have a direct oracle price feed associated with them, but allow for calculating accurately based on price feeds for other, underlying assets. Where possible, the protocol relies on Chainlink price feeds to anchor these calculations. If such price feeds are not available the protocol can also fall back on price feeds derived from on-chain exchanges, such as the TWAP price tracking, which is built into Uniswap pairs.

Definition 2.2. Price oracle calculation for LPT: Liquidity Pool Tokens are a prime example of an illiquid asset bearing a uniquely defined exchange value, as derived from the value of their underlying assets. The protocol provides overcollateralized loans based on these valuations.

The USD value of an LPT is calculated as:

$$\mathcal{V}_{lpt}(x) = x \cdot \frac{reserve_{t0} \cdot \mathcal{V}_{t0}(reserve_{t0}) + reserve_{t1} \cdot \mathcal{V}_{t1}(reserve_{t1})}{totalSupply(LPT)}$$

Given price oracles $\mathcal{V}_{t0}$ and $\mathcal{V}_{t1}$ for both constituent tokens in the trading pair, as well as their reserve amounts held by the trading pair.

Price oracles for NFTs: NFTs representing concentrated liquidity positions, bonds, or otherwise tied to assets with clear valuation are valued similarly to the above.

Accurately and securely pricing NFTs representing art is a very new and dynamic branch of a new and dynamic market. The Moremoney protocol will be committed to following developments closely and moving forward with new functionality in a circumspect manner, as reliable solutions become available.

When valuing NFTs based on sales prices on an NFT exchange, special care must be taken to defend against Sybil attacks. The protocol can whitelist individual tokens and adopt rating services to provide price data. In the case of somewhat comparable tokens such as generative art, uniform minimum valuations can be derived from their issuance price or snapshot minimum prices across the NFT class.

2.1.3 Liquidation

User accounts are flagged as below the liquidation threshold if their colleralization ratio falls below a governance-defined minimum. Their collateral assets can then be bought out in exchange for USDm, using an auction-style process.

Any participant can place a bid on buying out accounts falling below the liquidation threshold. If their bid is higher than the previous highest bid, their bid amount is placed in escrow for a specified number of blocks, after which the winning bidder can execute the transfer of collateral to their account.

Ensuring that liquidation will be incentivized, a minimum initial loan threshold can be set, which broadly speaking ensures that the commensurate collateral is valuable enough to warrant liquidation. The auction approach also allows for low bids to account for transaction costs.

Liquidation for NFTs: In the case of NFTs, liquidation bids happen at the start of the lending process and provide additional collateral backing for a premium. Since NFT loans are fixed term, the winning liquidation bid can simply withdraw the NFT in question after the term expires if the borrower does not repay.

2.2 Harvesting yield for loan repayment

Harvested funds automatically pay off loans made in the protocol. To this end, every lending contract avails itself of a conversion path via an AMM to convert the harvest back into protocol stablecoin. These stables are then burnt and every account is credited their share, proportional to their deposited amount of collateral. This credit is realized in a gas-efficient manner, notionally conforming to the following formula:

Definition 2.3.

$$yield_u([t_0, t_{now}]) = \int_{t_0}^{t_{now}} harvest(t)\ dt \cdot \int_{t_0}^{t_{now}} \frac{collateral_u(t)}{totalCollateral(t)}\ dt$$

$$totalCollateral(t) = \sum_{\hat{u}\ \in\ Users} collateral_{\hat{u}}(t)$$

Where u is the user in question, $[t_0, t_{now}]$ defines the time interval in which we re querying, $harvest(t)$ is the yield harvested at time t, denominated in *USDm* and $collateral_u(t)$ is the amount of collateral attributed to user u at time t.

In the interest of gas efficiency, the distribution takes on the following form:

1. The protocol tracks the running sum of harvested stable divided by the integral of the $totalCollateral$ function up to that point.
2. All acocunts track the checkpoint of this running sum, at which they last recieved harvest distribution (or were initialized).
3. Before taking action in an account, any eligible harvested yield gets credited to the account, according to the above formula.

2.3 Avoiding harvesting sandwich attacks

The above formula takes into account the amount of time a collateral was locked, in order to determine the fair share of distribution to a user. As such, an attacker cannot overwhelm the distribution of yield by briefly depositing a large amoutn of collateral using flash loans or similar instruments.

In order to prevent sandwich attacks on trading pairs while converting harvested yield into USDm, the lending contract requires that the value of generated yield in the origin token is no less than the value of the USDm it converts to (minus a slippage parameter, where slippage is relative to the true 1 USD value of USDm). This approach prioritizes simplicity and safity, with the ability for governance to step in as a backstop in case system availability is impaired.

3 Tokens

Two tokens power the Moremoney protocol

USDm: The value extracting stablecoin, minted from liquid / illiquid assets

MORE: The protocol's governance token

3.1 USDm – The value extracting stablecoin

USDm is a stablecoin that is pegged to USD and collateralized by various tokens (both liquid and illiquid). The total amount of USDm that can be minted is based on multiple factors:

- The total value of the underlying collateral deposited by a borrower.
- The Maximum mint/debt ceiling for USDm, which can be changed by governance.
- Minting allowance for a particular contract/asset, which is set when a new asset is allowed to be used as collateral or when a new contract is granted the power to mint USDm.

3.1.1 Maintaining the USDm–USD peg

The protocol's stablecoin is backed by the value of the collateral that users deposit, as well as funds held by the protocol's treasury. It can be traded for other stable and non-stable assets using decentralized and centralized exchanges.

USDm is designed to maintain parity with USD. Since loans including minting fees are in excess of the amount withdrawn by the user, loan repayment (either manual or automatic) serves as a steady stream of demand for the stablecoin, providing support for the price via market mechanics beyond the backing value.

In case 1 USDm $<$ 1 USD it becomes attractive for users to buy USDm from the open market to close their CDPs by repaying their debts. Arbitrageurs also ensure that the dollar peg is maintained by buying up USDm in the market when it is below peg and reselling when the peg is regained. The opposite incentive to sell is in effect when USDm rises above the 1 USD peg. USDm can also be minted with other stables as collateral, making it very attractive to open CDP using other stables when the price exceeds 1 USD.

3.1.2 Minting and burning

Minting and burning of tokens is controlled by overcollateralized lending contracts, which charge a minting fee, denominated in the stablecoin. Minting fees can vary according to the risk of the collateral provided.

For Liquidity Pool Tokens the minting fee will initially be set to 1% of the amount borrowed.

3.2 MORE – The governance token

MORE is the governance token for the Moremoney protocol. It allows holders to vote on changes to the Protocol. MORE holders can also allocate funds from the fees accumulated in the treasury to pay contributors, instate bug bounties, even sponsor research and more.

MORE is required to vote and decide on the outcome of proposals through Moremoney Improvement Proposals (MIPs).

At the early stage, the Protocol will be managed by a Foundation and eventually transition to a Decentralized Autonomous Organization (DAO). As part of the DAO, holders of the MORE token will be able to initiate proposals and vote on issues that will steer the direction of the Protocol.

3.3 Protocol Revenue Generation

The Moremoney protocol can draw on a variety of revenue sources. These include but are not limited to[1]:

1. USDm minting fees (varying by collateral asset)
2. 10% of harvested yield
3. MORE Liquidity farming fees

[1] More details will be provided in Gitbook documentation.

4 Conclusion

We have introduced Moremoney, a collateralized debt protocol that unwinds the inherent liquidity in illiquid and liquid assets.

Viewed from a bird's eye perspective, at the center of DeFi lies a complete re-imagination of the principles and financial mechanics underpinning fractional reserve banking. The analogy is striking: Collateralization ratios correspond to reserve ratios and yield plays a similar role in both realms. Nevertheless, the mechanisms and outcomes are strikingly different.

In DeFi, every step of the depositing, lending, and yield generation value chain is represented in token form, posing unique challenges, while promising key benefits: As instruments of extracting value are layered on top of each other, it becomes apparent that in DeFi the lion's share of value extracted accrues to the user, instead of any institution.

The Moremoney protocol presents a natural conclusion of this process of layered value extraction and is designed from the ground up to take the dynamic of empowering users seriously. Moremoney collates the entire stack of value extraction, adding an additional layer, and optimizes for maximum return at every level.

References

[AZS+21] Hayden Adams, Noah Zinsmeister, Moody Salem, River Keefer, and Dan Robinson. Uniswap v3 core. Technical report, Tech. rep., Uniswap, 2021.

[LH19] Robert Leshner and Geoffrey Hayes. Compound: The money market protocol. *White Paper*, 2019.

[Tea17] The Maker Team. The dai stablecoin system. *White Paper*, 2017.