The money market protocol for Waves Ecosystem

intra@vires.finance

July 21, 2021

Contents

1 Introduction

Vires.Finance is a peer-to-contract money market protocol built on Waves Blockchain: it implements pool-based strategy where loans do not need to be individually negotiated and matched(as in P2P-based strategy), but rather the conditions of lending and borrowing are determined by the protocol itself, algorithmically discovering rates("price of money") via the equilibrium between supply and demand.

2 The Protocol

Vires.Finance as a protocol describes the algorithm of borrowing assets by supplying other assets as collateral. In many aspects, it's similar to compound/aave lending protocols.

2.1 Supplying Assets

Assets supplied to a market are represented by "LP(liquidity provider) tokens", named vTokens, staked automatically upon deposit. As the money market accrues interest, which is a function of borrowing demand, vTokens become convertible into an increasing amount of the underlying asset, e.g. earning interest.

2.2 Borrowing Assets

Staked vTokens can be used as collateral to borrow from the protocol. Each market has a collateral factor, ranging from 0 to 1, that represents the portion of the underlying asset value that can be borrowed. The sum of the value of an account's underlying token balances, multiplied by the collateral factors, equals a user's borrowing capacity. Users are able to borrow up to, but not exceeding, their borrowing capacity.

2.3 Risk and Liquidation

If the value of an account's borrowing outstanding exceeds their borrowing capacity, a portion of the outstanding borrowing may be repaid in exchange for the user's staked vToken, at the current market price minus a liquidation discount. This incentives an ecosystem of arbitrageurs to quickly step in to reduce the borrower's exposure, and eliminate the protocol's risk. The proportion eligible to be closed, a close factor, is the portion of the borrowed asset that can be repaid, and ranges from 0 to 1, such as 25%. The liquidation process may continue to be called until the user's borrowing is less than their borrowing capacity(with regards to liquidation threshold).

2.4 Interest Rate Model

Borrowing interest rate I of a particular asset a is the function of it's utilisation U, which is parameterised for each asset:

$$U_a = TotalBorrows_a / TotalDeposit_a$$

$$I_a = f_a(U_a)$$

2.4.1 Market Dynamics

Each time a transaction occurs, the Interest Rate Index for the asset is updated to compound the interest since the prior index, using the interest for the period, denominated by r * t, calculated using a per-block interest rate:

$$Index_{a,n} = Index_{a,(n-1)} * (1 + r * t)$$

Accordingly,

$$\begin{aligned} TotalBorrows_{a,n} &= TotalBorrows_{a,(n-1)} * (1 + r * t) \\ collectedInterest_{a,n} &= TotalBorrows_{a,(n-1)} - TotalBorrows_{a,n} \\ &= TotalBorrows_{a,(n-1)} * r * t \end{aligned}$$

and

$$TotalDeposit_{a,n} = TotalDeposit_{(a,n-1)} + (1 - \lambda) * collectedInterest_{a,n}$$

So that λ, ranged from 0 to 1, represents `reserveFactor`, ensuring a portion of the accrued interest is retained (set aside) as reserves.

2.4.2 Liquidity Incentive

The profit from interest rate of borrowing is shared among vToken owners(and stakers). The interest rate model incentivises suppliers to provide more liquidity in periods of extreme demand for an asset, as when this occur, interest rates rise.

The unsused part of deposits which can be staked within their host protocols within Waves, are staked.

3 Implementation and Architecture

The described mechanisms are implemented as a system of interconnected smart contracts deployed over Waves blockchain, described on a high-level at Figure 1.

3.1 Borrow capacity

Whenever a user deposits funds to a token reserve, he can decide whether he wants to use the token deposit as collateral. The user's u borrow capacity is defined as weighted sum of all his assets, used as collateral:

$$BC_u = \sum (Ltv_a * C_{(u,a)} * Deposit_{(u,a)} * Price_a)$$

where

- Ltv is a percentage-denominated Loan-to-value ratio,
- $C_{(u,a)}$ is `use as collateral` option set by user,
- $Price_a$ is price of asset a provided by oracle;

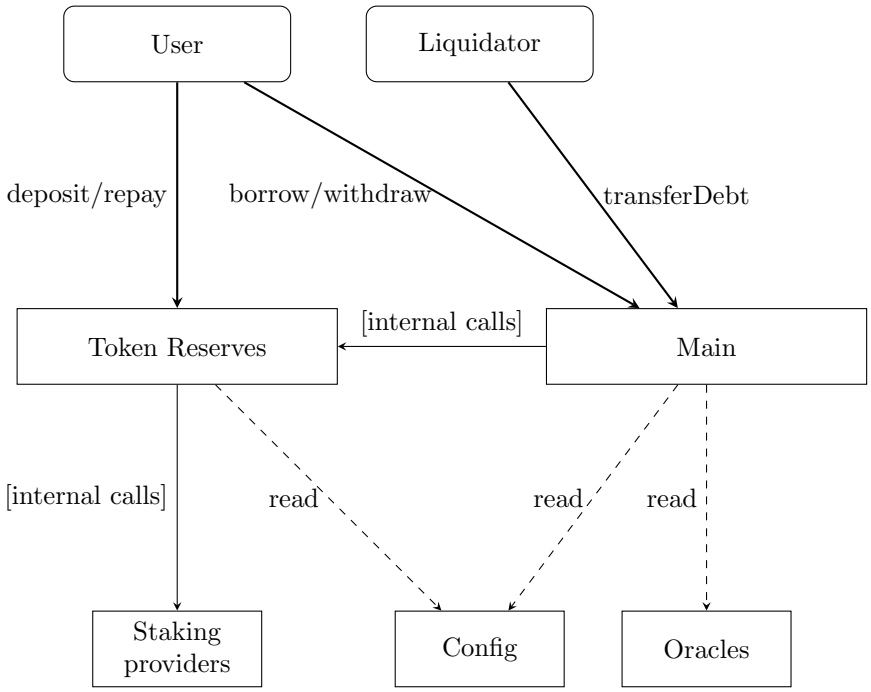

Figure 1: Smart contract architecture

3.2 Liquidation threshold

The user's u used borrow capacity(BCU_u) is defined as weighted sum of all his assets, used as collateral:

$$BCU_u = \sum((Borrow_{(u,a)} * Price_a)/LT_a)$$

where LT is liquidation threshold value for each asset, ranging from 0 to 1.

3.3 Health factor and Liquidation

Each user needs to keep an eye on the `health factor` of his portfolio. In essence, `health factor` is a ratio BC_u and BCU_u.

If a user's health factor drops below certain value, liquidators can step in and improve user's health by acquiring part of the unhealthy account's deposit and loan. This restores user's health factor, but, in order to incentivize the liquidator, maintaining overall system health, the `liquidation penalty` is applied(for example, 10%).

Formally, liquidation for a user becomes available when $BC_u \leq BCU_u$.

3.4 Interest-bearing tokens

If the asset is not used as collateral, user can mint interest-bearing vtokens, representing his share in total deposit of the asset, which grows in time as the debt. Apart from establisihing the secondary market for the deposits, vtokens

can be redeemed for that part of growing deposit(described in Section 2.4.1) and used for replenishing the user's account.