# Documentation for `Motivational Fund`

Ramil Amirov

September 23, 2024

## Contents

# 1 Introduction

This document provides comprehensive documentation for the MotivationalFund and FundExchange smart contracts. These contracts form the core of a decentralized finance (DeFi) system designed to manage a motivational fund that rewards certain users through a shares mechanism. The system is built on the Ethereum blockchain using Solidity and incorporates features such as rebasing tokens, profit distribution, and access control.

## 1.1 Project Overview

The project consists of two primary smart contracts:

a. MotivationalFund: An ERC20-compliant token with a rebasing mechanism that adjusts the total supply based on the performance of underlying investments. It includes a shares system that allows a **DEPOSITOR** to allocate shares to selected users, thereby providing them with additional benefits during profit distribution.

b. FundExchange: Acts as an interface between users and the MotivationalFund, handling deposits, withdrawals, and the periodic distribution of profits (payouts). It integrates with a PortfolioManager that manages investments into various strategies.

## 1.2 Key Concepts

- **Rebasing Tokens**: Tokens whose total supply can increase or decrease algorithmically. User balances adjust proportionally to maintain the same ownership percentage.
- **Shares**: A mechanism that allows the DEPOSITOR to allocate additional benefits to selected users. Shares are given to only a few users and entitle them to a portion of profits generated by the fund.
- totalDeposit: Represents funds deposited by the DEPOSITOR. Although these funds generate profit, the DEPOSITOR does not receive an increase in their funds within this contract. Instead, profits generated from totalDeposit are allocated to shareholding users.
- **Profit Distribution**: The mechanism by which profits (or losses) from investments are distributed among token holders and shareholding users.

# 2 Contract Descriptions

## 2.1 MotivationalFund Contract

The MotivationalFund contract is an ERC20 token with a rebasing mechanism. It includes additional features to manage shares and distribute profits accordingly.

### 2.1.1 Profit Distribution Mechanism

The profit distribution mechanism in MotivationalFund works as follows:

1. **Calculating Profit (delta)**:

$$\delta = \texttt{\_newTotalSupply} - \texttt{\_totalSupply} - \texttt{\_totalDeposit}$$

2. **Calculating baseDelta**:

$$\texttt{baseDelta} = \delta \times \frac{\texttt{\_totalDeposit}}{\texttt{\_totalSupply} + \texttt{\_totalDeposit}}$$

3. **Calculating teamDelta**:

$$\texttt{teamDelta} = \delta - \texttt{baseDelta}$$

4. **Updating Total Supply**:

$$\texttt{\_totalSupply} = \min(\texttt{\_totalSupply} + \texttt{teamDelta}, \texttt{MAX\_SUPPLY})$$

5. **Minting to Shareholding Users**:

$$\texttt{mintAmount} = \frac{\texttt{\_sharesBalances[curOwner]} \times \texttt{baseDelta}}{\texttt{\_totalShares}}$$

6. The function iterates over all shareholding users and mints `mintAmount` to each.

## 2.2 `FundExchange` Contract

The `FundExchange` contract serves as an interface between users and the `MotivationalFund`, handling the exchange of assets (e.g., USDC) and managing deposits, withdrawals, and payouts.

## 2.3 Interaction Between Contracts

- Users interact with `FundExchange` to deposit assets and receive `MotivationalFund` tokens.
- `FundExchange` transfers assets to the `PortfolioManager`, which invests them to generate returns.
- During payouts, `FundExchange` calculates profits or losses and calls `changeSupply` on `MotivationalFund` to adjust the total supply accordingly.
- Shareholding users receive additional tokens minted from profits generated by both user investments and `totalDeposit`.

# 3 Detailed Profit Distribution Mechanism

## 3.1 Calculations in `changeSupply`

The `changeSupply` function in `MotivationalFund` is critical for distributing profits or losses. Here's a step-by-step breakdown:

### Calculating Total Profit (`delta`)

$$\delta = \texttt{\_newTotalSupply} - \texttt{\_totalSupply} - \texttt{\_totalDeposit}$$

### Allocating Profit to `baseDelta` and `teamDelta`

$$\texttt{baseDelta} = \delta \times \frac{\texttt{\_totalDeposit}}{\texttt{\_totalSupply} + \texttt{\_totalDeposit}}$$

$$\texttt{teamDelta} = \delta - \texttt{baseDelta}$$

### Updating Total Supply

$$\texttt{\_totalSupply} = \min(\texttt{\_totalSupply} + \texttt{teamDelta}, \texttt{MAX\_SUPPLY})$$

### Recalculating Credits per Token

$$\texttt{\_rebasingCreditsPerToken} = \frac{\texttt{\_rebasingCredits}}{\texttt{\_totalSupply}}$$

**Minting Additional Tokens to Shareholding Users** For each shareholding user:

$$\texttt{mintAmount} = \frac{\texttt{\_sharesBalances[curOwner]} \times \texttt{baseDelta}}{\texttt{\_totalShares}}$$

**Impact on Different Roles**

- **Regular Token Holders**:
  - Benefit from the increase in `_totalSupply` through `teamDelta`.
  - Their token balances adjust proportionally due to the rebasing mechanism.
- **Shareholding Users**:
  - Receive additional tokens minted from `baseDelta`, increasing their balances.
  - Benefit both from `teamDelta` (like regular token holders) and from the shares mechanism.
- **DEPOSITOR**:
  - Does not receive an increase in funds within this contract.
  - `totalDeposit` generates profit, but this profit is allocated to shareholding users.

# 4 Roles and Permissions

## 4.1 DEPOSITOR

- Has the authority to assign shares to selected users via `giveShares`.
- Can remove shares from users via `burnShares`.
- Manages `totalDeposit`, which contributes to the fund's profitability but does not increase the DEPOSITOR's funds within the contract.

## 4.2 Shareholding Users

- Receive shares from the DEPOSITOR.
- Benefit from profit distributions both through rebasing and additional tokens minted from `baseDelta`.
- Are likely key team members or contributors incentivized to support the fund's success.

## 4.3 Regular Token Holders

- Hold `MotivationalFund` tokens obtained through deposits.
- Benefit from profit distributions via the rebasing mechanism.
- Do not receive additional tokens from the shares mechanism.

## 4.4 Access Control Modifiers

- `onlyAdmin`: Restricts functions to admin role.
- `onlyDepositor`: Restricts functions to the DEPOSITOR.
- `onlyExchanger`: Restricts functions to the exchanger role.
- `onlyPortfolioAgent`: Restricts functions to portfolio agents.
- `onlyUnit`: Restricts functions to a specific unit (used in `payout`).

# 5 Security Considerations

## 5.1 Reentrancy Protection

Both contracts use the `nonReentrant` modifier from OpenZeppelin's `ReentrancyGuard` to prevent reentrancy attacks during state-changing operations.

## 5.2 Pausable Mechanism

The contracts can be paused by authorized roles using the `pause` function, disabling certain functions during emergencies.

## 5.3 Flashloan Attack Prevention

The `_requireOncePerBlock` function in `FundExchange` ensures that only one mint or redeem transaction can occur per block when necessary, mitigating the risk of flashloan attacks.

## 5.4 Access Control

Roles are defined and enforced using modifiers to restrict access to critical functions, enhancing security.

# 6 Conclusion

The `MotivationalFund` and `FundExchange` contracts together create a sophisticated DeFi system that allows for dynamic profit distribution and incentivization of key participants. By incorporating a shares mechanism, the system provides additional rewards to selected users, aligning their interests with the fund's success. The design ensures that while the DEPOSITOR contributes capital to enhance profitability, the profits generated from `totalDeposit` are allocated to shareholding users, reflecting the project's strategic objectives.