WhatTheFork

Clean Code Review

Based Finance

twitter.com/WhatTheFork_xyz

discord.com/invite/V9quUUyYvQ

whatthefork.xyz

Rubik Finance

(Network => Fantom Opera)

Description:

An algorithmic stablecoin on the Fantom Opera blockchain, pegged to the price of 1 FTM
Rubik utilizes multiple bonding mechanisms at the DAO as well as seigniorage.

Contracts Reviewed:-

Rubik	:	0xA4Db7f3b07c7Bf1b5E8283Bf9e8aA889569fc2e7
RShare	:	0xf619D97e6Ab59E0B51A2154bA244D2E8157223Fe
RBond	:	0x7deCeb882539466D5F6a9C68c694915C469A4c37
Boardroom	:	0x00F41dEa8E0a8a0272B321E11448cd8B8c548A7f
RebateTreasury	:	0x74b0af515031598132D7455883c97846D5E3CfB8
Oracle	:	0x0E0d5e5F7411737AD598ad1553B7b811485822e5
Treasury	:	0x65767a3eb149FefB9AF0DC91D79983B7bb6a3Cb0
RShareRewardPool	:	0xf6b082B2ab9F4b17d2015F82342C3CA2843d524D
RubikGenesisRewardPool	:	0xEBf53aBf926e0942812fAa9538f9986fDdc3DC6E

Disclaimer

This review has been conducted to the best of our knowledge, it strictly checks for disparities bewteeen the project's contracts and that of Tomb.

In no way, shape or form is WhatTheFork attempting to promote the project neither is WhatTheFork suggesting finanical success by participating in it.

Rubik (0xA4Db7f3b07c7Bf1b5E8283Bf9e8aA889569fc2e7)

Rubik is highly similar the original tomb contract, apart from removal of a few function due to being unneeded Rubik Finance protocol, these include *exludeAddress*, *includeAddress* along with
the following taxation functions:

- *disableAutoCalculateTax*
- *enableAutoCalculateTax*
- *setBurnThreshold*
- *setTaxCollectorAddress*
- *setTaxOffice*
- *setTaxRate*
- *setTaxTiersRate*
- *setTaxTiersTwap*

Operator and owner status:

✅ Operator:Treasury - 0x65767a3eb149FefB9AF0DC91D79983B7bb6a3Cb0
✅ Owner :Renounced- 0x0000000000000000000000000000000000000000

Bshare (0xf619D97e6Ab59E0B51A2154bA244D2E8157223Fe)

Bshare does not contain any major disparties relative to Tshare.
The only differences include equal splitting of devFund into 4 different wallets, and *claimRewards* being able to be called only by the contract owner, this is likely done to act as a an additional safeguard against the Ripae Finance exploit.

Operator and owner status:

✅ Operator:Treasury - 0x65767a3eb149FefB9AF0DC91D79983B7bb6a3Cb0
✅ Owner :Deployer - 0xD9501f5C83344E38B6cfc3070CD08F99b537B5DC

RBond (0x7deCeb882539466D5F6a9C68c694915C469A4c37)

RBond does not show any differences relative to the original TBond contract.

Operator and owner status:

☑ Operator:Treasury - 0x65767a3eb149FefB9AF0DC91D79983B7bb6a3Cb0
☑ Owner :Treasury - 0x0000000000000000000000000000000000000000

Boardroom (0x00F41dEa8E0a8a0272B321E11448cd8B8c548A7f)

Rubik Finance's Boardroom does not show any disparities from Tomb Finance's Masonry contract.

Operator status:

☑ Operator:Treasury - 0x65767a3eb149fefb9af0dc91d79983b7bb6a3cb0

RebateTreasury(0x74b0af515031598132D7455883c97846D5E3CfB8)

The contract does not have any real differences relative to the original 3omb Finance's contract, a requirement related to *redeemAssetsForBuyback is* removed which restricts them from executing the function when above peg
Operator and owner status:

☑ Operator* :Deployer - 0xD9501f5C83344E38B6cfc3070CD08F99b537B5DC

Oracle (0x0E0d5e5F7411737AD598ad1553B7b811485822e5)

The Oracle does not have any real disparties from the original Tomb Finance Oracle contract.

Operator and owner status:

☑ Operator* :Deployer - 0xD9501f5C83344E38B6cfc3070CD08F99b537B5DC
☑ Owner* :Deployer - 0xD9501f5C83344E38B6cfc3070CD08F99b537B5DC
*Epoch periods can be modified to the need of the protocol, although, it can also be used for the contract owner's personal interests.
(This applies to tomb itself and mostly all tomb fork protocols.)

Treasury(0x65767a3eb149FefB9AF0DC91D79983B7bb6a3Cb0)

The Rubik Finance Treasury includes a few modifications:-

- *interface IBondTreasury* : This interface is present so that bond contract can be initiated and to call the totalVested function.

- *sendToBondTreasury* : The IBondTreasury interface is being used to get the amount vested to the treasury. If that amount is more than the treasury balance,that means that the vesting is done in that case, it just returns and does nothing.Otherwise, if the amount specified is greater than the unspent (Treasury Balance- Treasury vested), then more cash is minted.

- *setBondSupplyExpansionPercent* : By default, the expansion rate for the bond treasury each epoch is set to 5%. This function lets the expansion rate to be modified accordingly

Operator and owner status:

☑ Operator:Deployer- 0xfA1DCF8369fF71AFe0fc2b57e1d103Ab931766c7

BshareRewardPool(0xf6b082B2ab9F4b17d2015F82342C3CA2843d524D)

The contract has a function to set deposit fees, it is restricted to be modified to a maximum of 1%.

Operator and owner status:

☑ Operator:Deployer- 0xd9501f5c83344e38b6cfc3070cd08f99b537b5dc

BasedGenesisRewardPool(0x9Ec66B9409d4cD8D4a4C90950Ff0fd26bB39ad84)

The genesis pool contains a deposit fee which can be set to a maximum of 1% and has a 30 day governance recovery.

Operator status:

☑ *Operator :Deployer - 0xD9501f5C83344E38B6cfc3070CD08F99b537B5DC

*The deployer can add new pools, modify existing ones to the needs of the protocol, but, ghost pools can be added for the dev letting the dev farm with a large APR, although applies to a large number of tomb fork projects, along with Tomb itself.

Report Synopsis

RubikFinance's contracts do not show any signs of malice.

The only differences from the original Tomb Finance contracts include minor fine tuning in order to be more suitable to the protcol, including removal of tax functions from Rubik token and addition of bonding mechanism through the rebate treasury.

Few safety tips to keep in mind:

- Always ensure that the contract you're interacting with is the same one as mentioned in the contracts page.
- To check what contract your wallet is interacting with directly, you can find the contract address stated on the transaction screen right in the middle when approving tokens and on the top right while calling other functions.