VITAL BLOCK

Security Assessment

FENTURE FINANCE

Vital Block Verified on May 23th, 2023

@Vital-Block

@VB_Audit

info@vitalblock.org

www.vitalblock.org

PREPARED FOR:

FENTURE FINANCE

INTRODUCTION

Auditing Firm	**VITAL BLOCK SECURITY**
Client Firm	**FENTURE FINANCE**
Methodology	Automated Analysis, Manual Code Review
Language	Solidity
Contract	Fenture:Acoin: Fenture:Acoin lend: Fenture:Constants: Fentur:Interest_rate_module: Fenture::market: Fenture::oracle:
Language	**Move**
Centralization	Active ownership
Website	https://fenture.io/
Discord	http://discord.gg/3tftnwBS7u
Twitter	https://twitter.com/FentureFinance
GitHub	https://docs.fenture.io/
Prelim Report Date	May 22, 2023
Final Report Date	May 23 2023

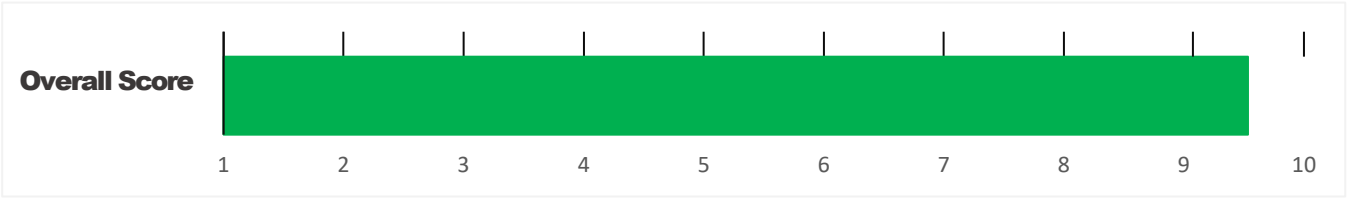
Verify the authenticity of this report on our GitHub Repo: https://www.github.com/vital-block

EXECUTIVE SUMMARY

FENTURE FINANCE has performed the automated and manual analysis of the FENTURE FINANCE Move code. The code was reviewed for common contract vulnerabilities and centralized exploits. Here's a quick audit summary:

Status	Critical !	Major "	Medium #	Minor $	Unknown %
Open	0	0	1	3	0
Acknowledged	0	0	1	3	0
Resolved	0	0	0	0	0
Noteworty onlyOwner Privileges	Set Taxes and Ratios, Airdrop, Set Protection Settings, Set Reward Properties, Set Reflector Settings, Set Swap Settings, Set Pair and Router				

FENTURE FINANCE Smart contract has achieved the following score: 95.0



Please note that smart contracts deployed on blockchains aren't resistant to exploits, vulnerabilities and/or hacks. Blockchain and cryptography assets utilize new and emerging technologies. These technologies present a high level of ongoing risks. For a detailed understanding of risk severity, source code vulnerability, and audit limitations, kindly review the audit report thoroughly.

Please note that centralization privileges regardless of their inherited risk status - constitute an elevated impact on smart contract safety and security.

TABLE OF CONTENTS

SCOPE OF WORK

Vital Block was consulted by FENTURE FINANCE to conduct the smart contract audit of its. Move source code. The audit scope of work is strictly limited to mentioned .Move file only:

- **FENTUREFINANCE.Move**

External contracts and/or interfaces dependencies are not checked due to being out of scope.

Verify audited contract's contract address and deployed link below:

Public Contract Code	
Acoin.move **Acoin lend.move** **Constants.move** **Interest_rate_module.move** **Market.move** **Oracle.move**	
Contract Name	**FENTURE FINANCE**
Token Symbol	**FFD**
Decimals	**8**

AUDIT METHODOLOGY

Smart contract audits are conducted using a set of standards and procedures. Mutual collaboration is essential to performing an effective smart contract audit. Here's a brief overview of Vital Block auditing process and methodology:

CONNECT

- **The onboarding team gathers source codes, and specifications to make sure we understand the size, and scope of the smart contract audit.**

AUDIT

- **Automated analysis is performed to identify common contract vulnerabilities. We may use the following third-party frameworks and dependencies to perform the automated analysis:**
  - **Remix IDE Developer Tool**
  - **Open Zeppelin Code Analyzer**
  - **SWC Vulnerabilities Registry**
  - **DEX Dependencies, e.g., Pancakeswap, Uniswap**
- **Simulations are performed to identify centralized exploits causing contract and/or trade locks.**
- **A manual line-by-line analysis is performed to identify contract issues and centralized privileges. We may inspect below mentioned common contract vulnerabilities, and centralized exploits:**

Centralized Exploits	○ **Token Supply Manipulation** ○ **Access Control and Authorization** ○ **Assets Manipulation** ○ **Ownership Control** ○ **Liquidity Access** ○ **Stop and Pause Trading** ○ **Ownable Library Verification**

Common Contract Vulnerabilities	○ Integer Overflow ○ Lack of Arbitrary limits ○ Incorrect Inheritance Order ○ Typographical Errors ○ Requirement Violation ○ Gas Optimization ○ Coding Style Violations ○ Re-entrancy ○ Third-Party Dependencies ○ Potential Sandwich Attacks ○ Irrelevant Codes ○ Divide before multiply ○ Conformance to Solidity Naming Guides ○ Compiler Specific Warnings ○ Language Specific Warnings

REPORT

- The auditing team provides a preliminary report specifying all the checks which have been performed and the findings thereof.
- The client's development team reviews the report and makes amendments to the codes.
- The auditing team provides the final comprehensive report with open and unresolved issues.

PUBLISH

- The client may use the audit report internally or disclose it publicly.

It is important to note that there is no pass or fail in the audit, it is recommended to view the audit

as an unbiased assessment of the safety of solidity codes.

RISK CATEGORIES

Smart contracts are generally designed to hold, approve, and transfer tokens. This makes them very tempting attack targets. A successful external attack may allow the external attacker to directly exploit. A successful centralization-related exploit may allow the privileged role to directly exploit. All risks which are identified in the audit report are categorized here for the reader to review:

Risk Type	Definition
Critical	These risks could be exploited easily and can lead to asset loss, data loss, asset, or data manipulation. They should be fixed right away.
Major	These risks are hard to exploit but very important to fix, they carry an elevated risk of smart contract manipulation, which can lead to high-risk severity.
Medium	These risks should be fixed, as they carry an inherent risk of future exploits, and hacks which may or may not impact the smart contract execution. Low-risk re-entrancy-related vulnerabilities should be fixed to deter exploits.
Minor	These risks do not pose a considerable risk to the contract or those who interact with it. They are code-style violations and deviations from standard practices. They should be highlighted and fixed nonetheless.
Unknown	These risks pose uncertain severity to the contract or those who interact with it. They should be fixed immediately to mitigate the risk uncertainty.

All statuses which are identified in the audit report are categorized here for the reader to review:

Status Type	Definition
Open	Risks are open.
Acknowledged	Risks are acknowledged, but not fixed.
Resolved	Risks are acknowledged and fixed.

CENTRALIZED PRIVILEGES

Centralization risk is the most common cause of cryptography asset loss. When a smart contract has a privileged role, the risk related to centralization is elevated.

There are some well-intended reasons have privileged roles, such as:

- **Privileged roles can be granted the power to** pause() **the contract in case of an external attack.**
- **Privileged roles can use functions like,** include(), **and** exclude() **to add or remove wallets from fees, swap checks, and transaction limits. This is useful to run a presale and to list on an exchange.**

Authorizing privileged roles to externally-owned-account (EOA) is dangerous. Lately, centralization-related losses are increasing in frequency and magnitude.

- **The client can lower centralization-related risks by implementing below mentioned practices:**
- **Privileged role's private key must be carefully secured to avoid any potential hack.**
- **Privileged role should be shared by multi-signature (multi-sig) wallets.**
- **Authorized privilege can be locked in a contract, user voting, or community DAO can be introduced to unlock the privilege.**
- **Renouncing the contract ownership, and privileged roles.**
- **Remove functions with elevated centralization risk.**

Understand the project's initial asset distribution. Assets in the liquidity pair should be locked. Assets outside the liquidity pair should be locked with a release schedule.

AUDIT SCOPE | FENTURE.FINANCE

ID	Repo	Comment	File	SHM211 Checksum
FTM	Fenture/Lending-Protocol	cC51D65	Move.toml	85f15802c6be0fd50f8632d8433cccc9db6f4b39f9e566d1fa78de54b84bddr54
FRY	Lending-Protocol/Source	cC51D53	fenture::acoin	8oippkjjjk96be0fd50f8632d8433cccc9db6f4b39f9e566d1yhhg8765fffckiuybb
FTV	Lending-Protocol/Source	cC51D61	fenture::acoin_lend	3666778uj908766362fvyga98jdkl88648yhfbqt37409owehbgwhuyyyg223738
FML	Lending-Protocol/Source	cC51D76	fenture::constants	98uuyriy399787390uhbiiuhghhdg7guu30oi7799u9359ydfgdgygeigi3ioueyy78
FTR	Lending-Protocol/Source	cC51D22	fenture::interest_rate_module	4566efgywqutfeuh87872t15378837983639293763hhegetgjfwjk89336668862
FOP	Lending-Protocol/Source	cC51D44	fenture::market	546363ttebnve88329973mvvdsggct478153ytgdfdxy792635fgdjgi1900990908
FDP	Lending-Protocol/Source	cC51D21	fenture::market_storage	835656990327hudbinnjntr6729dchjld0993ytyy3vq63235727879889073
FWY	Lending-Protocol/Source	cC51D97	fenture::oracle	cc089692343d1cc36eaf196046d7a528d153abd55ba20e82f1d57c22fcd92675
FKB	Lending-Protocol/Source	cC51D76	acoin.move	8448b3af42497f5f74e53424ee3e6c551f51356945108d22a893d608a7990542
FXY	Fenture-Finance/protocol/	cC51D23	acoin_lend.move	5c86aa1dd3889db5fcd17a80214b226fc784f268ab9db82df97c1d2459467831
FCB	Fenture-Finance/protocol/	cC51D63	constant.move	b8244da33db171e5533d77bef4a35703df1de2cebea5f35cb38ce6a26c778cf1
FWO	Fenture-Finance/protocol/	cC51D60	market.move	3d408b8f2cc56f9699a402b5151de90671de089c3007afc9e4fc867c04152e7c
FGT	Fenture-Finance/protocol/	cC51D54	oracle.move	9d751621c3501102e4b50005ca3314ec6e04e6ff8bbb30852d1c7edfff3f8cef
FDF	Fenture-Finance/protocol/	cC51D78	SafeMath.move	455687gfesadjknlppiuhhg774580vgfxrki9876dhgvb990lkjhde444566788

AUTOMATED ANALYSIS

Symbol	Definition
	Function modifies state
	Function is payable
	Function is internal
	Function is private
	Function is important

FENTURE FINANCE	Interface			
└	totalSupply	External		!	NO	
└	decimals	External		!	NO	
└	symbol	External		!	NO	
└	name	External		!	NO	
└	getOwner	External			NO	
└	balanceOf	External		!	NO	
└	transfer	External	"	!		NO	
└	allowance	External		!	NO	
└	approve	External	"	!		NO	
└	transferFrom	External	"		NO	

||||||

IFactoryV2	Interface				
└	getPair	External		NO	
└	createPair	External	"	NO	

||||||

IV2Pair	Interface				
└	factory	External		NO	
└	getReserves	External		NO	
└	sync	External	"	NO	

IRouter01	Interface		
└	factory	External	NO
└	Move	External	NO
└	addLiquidityAPT	External	# NO
└	addLiquidity	External	" NO
└	swapExactAPTForTokens	External	# NO
└	getAmountsOut	External	NO
└	getAmountsIn	External	NO
IRouter02	Interface	IRouter01	
└	swapExactTokensForAPTSupportingFeeOnTransferTokens	External	" NO
└	swapExactAPTForTokensSupportingFeeOnTransferTokens	External	# NO
└	swapExactTokensForTokensSupportingFeeOnTransferTokens	External	" ! NO
└	swapExactTokensForTokens	External	" NO
Protections	Interface		
└	checkUser	External	" ! NO
└	setLaunch	External	" NO
└	setLpPair	External	" NO
└	FFD	External	" NO
└	removeSniper	External	" NO
Cashier	Interface		
└	setRewardsProperties	External	" NO
└	tally	External	" NO
└	load	External	# NO
└	cashout	External	" NO
└	giveMeWelfarePlease	External	" NO
└	getTotalDistributed	External	NO
└	getUserInfo	External	NO
└	getUserRealizedRewards	External	NO

| └ | getPendingRewards | External ❗ | | |NO❗ |

| └ | initialize | External ❗ | " | |NO❗ |

| └ | getCurrentReward | External ❗ | | |NO❗ |

||||||

| **MOVE** | Implementation | **SafeMath** |||

| └ | <Constructor> | Public ❗ | | # |NO❗ |

| └ | transferOwner | External ❗ | " | | onlyOwner |

| └ | renounceOwnership | External ❗ | " | | NO❗|

| └ | setOperator | Public ❗ | " | |NO❗ |

| └ | renounceOriginalDeployer | External ❗ | " | |NO❗ |

| └ | <Receive Apt> | External ❗ | | # |NO❗ |

| └ | totalSupply | External ❗ | | |NO❗ |

| └ | decimals | External ❗ | | |NO❗ |

| └ | symbol | External ❗ | | |NO❗ |

| └ | name | External ❗ | | |NO❗ |

| └ | getOwner | External ❗ | | ❗ |NO❗ |

| └ | balanceOf | Public ❗ | | ❗ |NO❗ |

| └ | allowance | External ❗ | | ❗ |NO❗ |

| └ | approve | External ❗ | " | ❗ 🛑 |NO❗ |

| └ | _approve | Internal $ | " 🔒 🛑 | |

| └ | approveContractContingency | Public ❗ | " | ❗ 🛑 | onlyOwner |

| └ | transfer | External ❗ | " | |NO❗ |

| └ | transferFrom | External ❗ | " | |NO❗ |

| └ | setNewRouter | External ❗ | " | | onlyOwner |

| └ | setLpPair | External ❗ | " | | onlyOwner |

| └ | setInitializers | External ❗ | " | | onlyOwner |

| └ | isExcludedFromFees | External ❗ | | |NO❗ |

| └ | isExcludedFromDividends | External ❗ | | |NO❗ |

| └ | isExcludedFromProtection | External ❗ | | |NO❗ |

| └ | setDividendExcluded | Public ❗ | " | | onlyOwner |

| └ | setExcludedFromFees | Public ❗ | " | | onlyOwner |

FTV-02 POSSIBLE OVERFLOW

Category	Severity	Location	Status
Status Mathematical Operations	**Minor**	Lending-Protocol/acoin.move	Acknowledged

Description

In **updateForTaker** , the following equation is used inside an unchecked block

```
  public fun accrue_interest<CoinType>()
        {let current_block_number = timestamp::now_seconds();
       let accrual_block_number_prior = acoin::accrual_block_number<CoinType>();
if (current_block_number == accrual_block_number_prior) {
```

Where parameters. block_number Out Used is a this and override In is a this.
As these two are multiplied together in an unchecked block, they may overflow.

Recommendation

We recommend either checking for overflow in this case, or ensuring that the PairsIn is close enough it will never causean overflow

FZT-03 POSSIBLE OVERFLOW

Category	Severity	Location	Status
Status Mathematical Operations	**Minor**	Lending-Protocol/Market	Acknowledged

Description

In **updateForMinter** , the following equation is used inside an unchecked block

```
    } public fun mint_allowed<CoinType>(minter: address, _mint_amount: u64): u64 {
assert!(!storage::mint_guardian_paused<CoinType>(), EMINT_PAUSED);
```

Minter can not issue more **FFD** tokens indefinitely.
Note that as of the date of publishing, the above review reflects the current understanding of known security patterns as they relate to the FFD contract.

Recommendation

We recommend either checking for overflow in this case, or ensuring that the PairsIn is close enough it will never cause an overflow.

FZT-03 POSSIBLE OVERFLOW

Category	Severity	Location	Status
Inconsistency	**Informational**	Lending-Protocol/Oracle	Acknowledged

Description

In **updateForprice ,** the following equation is used inside an unchecked block

```
 public entry fun set_underlying_price_batch(price_feeder: &signer, coin_type_batch:
vector<String>, new_price_mantissa_batch: vector<u128>) acquires OracleStore {
only_price_feeder(price_feeder);        let index =
vector::length<String>(&coin_type_batch);        assert!(index ==
vector::length<u128>(&new_price_mantissa_batch), EINVALID_ARGS);  while (index > 0) {
```

The function price () does not have the override specifier. It should be noted that since price0 > a function that overrides only a single interface function does not require the override specifier (see doc). However, all other instances of this in the codebase contain the override specifier

Recommendation

We recommend either checking for overflow in this case, or ensuring that the PairsIn is close enough it will never cause an overflow.

OPTIMIZATIONS | FENTURE.FINANCE

ID	Title	Category	Status
FTV	**Logarithm Refinement Optimization**	Gas Optimization	Acknowledged
FOP	**Checks Can Be Performed Earlier**	Gas Optimization	Acknowledged
FDP	**Unnecessary Use Of SafeMath**	Gas Optimization	Acknowledged
FWY	**Struct Optimization**	Gas Optimization	Acknowledged
FGT	**Unused State Variable**	Gas Optimization	Acknowledged

General Detectors

Missing Zero Address Validation

Some functions in this contract may not appropriately check for zero addresses being used.

Attention Required

Incorrect Solidity Version

This contract uses an unconventional or very old version of Solidity

Attention Required

- No compiler version inconsistencies found
- No unchecked call responses found
- No vulnerable self-destruct functions found
- No assertion vulnerabilities found
- No old solidity code found
- No external delegated calls found
- No external call dependency found
- No vulnerable authentication calls found
- No invalid character typos found
- No RTL characters found
- No dead code found
- No risky data allocation found
- No uninitialized state variables found
- No uninitialized storage variables found
- No vulnerable initialization functions found
- No risky data handling found
- No number accuracy bug found
- No out-of-range number vulnerability found
- No map data deletion vulnerabilities found
- No tautologies or contradictions found
- No faulty true/false values found
- No innacurate divisions found
- No redundant constructor calls found
- No vulnerable transfers found
- No vulnerable return values found
- No uninitialized local variables found
- No default function responses found
- No missing arithmetic events found
- No missing access control events found
- No redundant true/false comparisons found
- No state variables vulnerable through function calls found
- No buggy low-level calls found
- No expensive loops found
- No bad numeric notation practices found
- No missing constant declarations found
- No missing external function declarations found
- No vulnerable payable functions found
- No vulnerable message values found

Vulnerability Scan

REENTRANCY

No reentrancy risk found

Severity	Minor
Confidence Parameter	Certain

Vulnerability Description

Not Mintable: A large amount of this token can not be minted by a private wallet or contract.

Scanning Line:

```
 public fun mint_allowed<CoinType>(minter:
address, _mint_amount: u64): u64 {
assert!(!storage::mint_guardian_paused<CoinType>
(), EMINT_PAUSED);        if
(!storage::is_listed<CoinType>()) {
return EMARKET_NOT_LISTED        };
update_fenturefinancedao_supply_index<CoinType>(
);
distribute_supplier_fenturefinancedao<CoinType>(
minter, false);        NO_ERROR    }    public
fun mint_verify<CoinType>(_minter: address,
_mint_amount: u64, _mint_tokens: u64) {
// currently nothing to do    }
```

Identifier	Definition	Severity
CEN-02	Initial asset distribution	Minor

```
public fun accrue_interest<CoinType>() {        let
current_block_number = timestamp::now_seconds();        let
accrual_block_number_prior = acoin::accrual_block_number<CoinType>();
if (current_block_number == accrual_block_number_prior) {
return        };        }
```

Description:

Floating point calculations can vary across different architectures.

Alleviation:

This exhibit was acknowledged and ultimately discarded by the **FENTURE FINANCE** team due to low severity. We consider the exhibit fully attended to as it doesn't impose any meaningful security concerns.

RECOMMENDATION

Project stakeholders should be consulted during the initial asset distribution process.

Repository:

https://github.com/Fenture-finance/

All Audited Files

Fenture:Acoin.Move
Fenture:Acoin lend.Move
Fenture:Constants.Move
Fentur:Interest_rate_module.Move
Fenture::market.Move
Fenture::oracle.Move

Contracts:

Contract :
Fenture::Acoin:
Fenture::Acoin_lend:
Fenture::Constants:
Fenture::Interest_rate_module:
Fenture::market:
Fenture::oracle:

Vulnerability Run check

Risk Analysis

Contract source code verified

This token contract is open source. You can check the contract code for details. Unsourced token contracts are likely to have malicious functions to defraud their users of their assets.

No Proxy

There is no proxy in the contract. The proxy contract means contract owner can modify the function of the token and possibly effect the price.

No mint function

Mint function is transparent or non-existent. Hidden mint functions may increase the amount of tokens in circulation and effect the price of the token.

No function to retrieve ownership

If this function exists, it is possible for the project owner to regain ownership even after relinquishing it.

Owner cant change balance

The contract owner does not have the authority to modify the balance of tokens at other addresses.

Honeypot Risk

This does not appear to be a honeypot

We are not aware of any code that prevents the sale of tokens.

No trading cooldown

The token contract has no trading cooldown function.If there is a trading cooldown function, the user will not be able to sell the token within a certain time or block after buying.

No Anti Whale

There is no limit to the number of token transactions. The number of scam token transactions may be limited (honeypot risk).

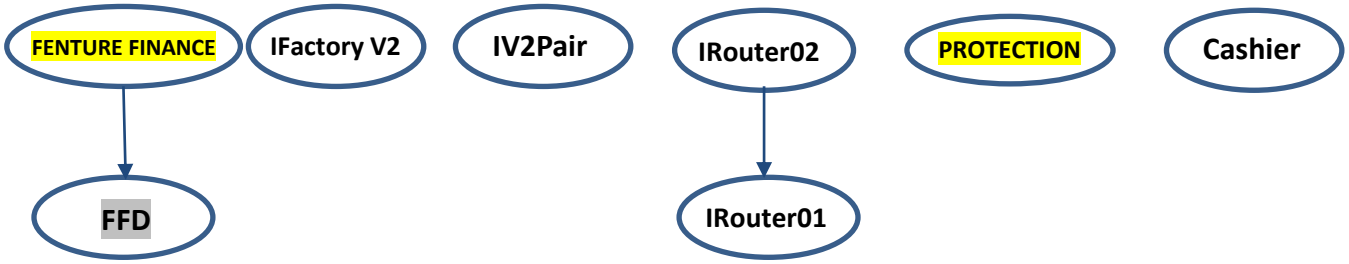
No blacklist function

No blacklist function is included.

No whitelist function

Whitelist function found

INHERITANCE GRAPH



Identifier	Definition	Severity
CEN-12	Centralization privileges of FENTURE FINANCE	Medium # 🟡

Vulnerability 0 : No important security issue detected.
Threat level: Low

```
Home  acoin_lend.move
}

public entry fun repay_all<CoinType>
(   payer: &signer,
    borrower: address,
) {
    accrue_interest<CoinType>();
    let repay_amount = acoin::borrow_balance<CoinType>(borrower);
    let coin = coin::withdraw<CoinType>(payer, repay_amount);
    repay_borrow<CoinType>(payer, borrower, coin);
}

public entry fun liquidate_borrow_entry<BorrowedCoinType, CollateralCoinType>(
    liquidator: &signer,
    borrower: address,
    repay_amount: u64,
) {
    let coin = coin::withdraw<BorrowedCoinType>(liquidator, repay_amount);
    let acoin = liquidate_borrow<BorrowedCoinType, CollateralCoinType>(liquidator, borrower, coin);
    deposit<CollateralCoinType>(liquidator, acoin);
}

listen on all transactions   Search with transaction hash or address
```

MANUAL REVIEW

FENTURE Finance: is a supercharged, autonomous DeFi protocol focused on venture capital investments, yield maximizing market strategies, and expanding the utility of the Web3 and DeFi ecosystem by building custom investment products and partnering with growing projects that lay foundations for the future.

Fenture Finance is a decentralized autonomous organization controlled by its governance token, FFD (Fenture Finance Dao). To participate in the DAO, users need to buy FFD tokens from the open market. These tokens can be used to vote on protocol proposals and direct the future of the project. They can also be staked in a revenue sharing contract to benefit from the treasury performance.

TOKEN NAME: FENTURE FINANCE
Ticker: FFD

Chain/Standard: APTOS & SUI

LAUNGUGE: Move

The FENTURE FINANCE Platform Is Launching On Aptos& Sui Chain

Fenture Finance Token (FFD)

Staking

Users can stake some of their FFD holdings and earn consistent rewards over time as passive income.

Bonding

With decentralized and non-custodial staking, bonding allows users to trade various crypto assets for FFD at a discounted price. In exchange to the bond sales, the treasury grows, providing stability to the protocol and yield generation opportunities for FFD holders.

Fully Mortgaged

FFD is fully mortgaged because it is backed by crypto assets on the chain in the scope of Fenture DAO. The intrinsic value of FFD is backed by the protocol's total asset under management.

Self- Learning Algorithm Control

When FFD trades at a premium, the protocol will mint FFD and sell it in the open market to increase supply and drive down prices. If FFD trades at a discounted price,the DAO will buy back tokens to reduce supply.

ISSUES CHECKING STATUS

	Issue Description	Checking Status
1.	Compiler errors.	PASSED
2.	Race Conditions and reentrancy. Cross-Function Race Conditions.	PASSED
3.	Possible Delay In Data Delivery.	PASSED
4.	Oracle calls.	PASSED
5.	Front Running.	PASSED
6.	Move Dependency.	PASSED
7.	Integer Overflow And Underflow.	PASSED
8.	DoS with Revert.	PASSED
9.	Dos With Block Gas Limit.	PASSED
10.	Methods execution permissions.	PASSED
11.	Economy Model of the contract.	PASSED
12.	The Impact Of Exchange Rate On the Move Logic.	PASSED
13.	Private use data leaks.	PASSED
14.	Malicious Event log.	PASSED
15.	Scoping and Declarations.	PASSED
16.	Uninitialized storage pointers.	PASSED
17.	Arithmetic accuracy.	PASSED
18.	Design Logic.	PASSED
19.	Cross-Function race Conditions	PASSED
20.	Save Upon Move contract Implementation and Usage.	PASSED
21.	Fallback Function Security	PASSED

AUDIT RESULT

PASSED

SMART CONTRACT AUDIT OF FENTURE FINANCE

Identifier	Definition	Severity
CEN-02	Initial asset distribution	Minor

All of the initially minted assets are sent to the contract deployer when deploying the contract. This can be an issue as the deployer and/or contract owner can distribute tokens without consulting the community.

```
    }

 public entry fun mint_entry<CoinType>(        minter: &signer,
 mint_amount: u64,    ) {        let coin = coin::withdraw<CoinType>(minter,
mint_amount);        let acoin = mint<CoinType>(minter, coin);
deposit<CoinType>(minter, acoin);
```

RECOMMENDATION

Project stakeholders should be consulted during the initial asset distribution process.

RECOMMENDATION

Deployer and/or contract owner private keys are secured carefully.

Please refer to PAGE-09 CENTRALIZED PRIVILEGES for a detailed understanding.

ALLEVIATION

The FENTURE FINANCE project team understands the centralization risk. Some functions are provided privileged access to ensure a good runtime behavior in the project

Identifier	Definition	Severity
COD-10	Third Party Dependencies	Minor

Smart contract is interacting with third party protocols e.g., Pancakeswap router, cashier contract, protections contract. The scope of the audit treats third party entities as black boxes and assumes their functional correctness. However, in the real world, third parties can be compromised, and exploited. Moreover, upgrades in third parties can create severe impacts, e.g., increased transactional fees, deprecation of previous routers, etc.

RECOMMENDATION

Inspect and validate third party dependencies regularly, and mitigate severe impacts whenever necessary.

CERTIFICATE BY VITAL BLOCK SECURITY

DISCLAIMERS

Vital Block provides the easy-to-understand audit of Solidity, Move and Raw source codes (commonly known as smart contracts).

The smart contract for this particular audit was analyzed for common contract vulnerabilities, and centralization exploits. This audit report makes no statements or warranties on the security of the code. This audit report does not provide any warranty or guarantee regarding the absolute bug-free nature of the smart contract analyzed, nor do they provide any indication of the client's business, business model or legal compliance. This audit report does not extend to the compiler layer, any other areas beyond the programming language, or other programming aspects that could present security risks. Cryptographic tokens are emergent technologies, they carry high levels of technical risks and uncertainty. You agree that your access and/or use, including but not limited to any services, reports, and materials, will be at your sole risk on an as-is, where-is, and as-available basis. This audit report could include false positives, false negatives, and other unpredictable results.

CONFIDENTIALITY

This report is subject to the terms and conditions (including without limitations, description of services, confidentiality, disclaimer and limitation of liability) outlined in the scope of the audit provided to the client. This report should not be transmitted, disclosed, referred to, or relied upon by any individual for any purpose without InterFi Network's prior written consent.

NO FINANCIAL ADVICE

This audit report does not indicate the endorsement of any particular project or team, nor guarantees its security. No third party should rely on the reports in any way, including to make any decisions to buy or sell a product, service or any other asset. The information provided in this report does not constitute investment advice, financial advice, trading advice, or any other sort of advice and you should not treat any of the report's content as such. This audit report should not be used in any way

to make decisions around investment or involvement. This report in no way provides investment advice, nor should be leveraged as investment advice of any sort.

FOR AVOIDANCE OF DOUBT, SERVICES, INCLUDING ANY ASSOCIATED AUDIT REPORTS OR MATERIALS, SHALL NOT BE CONSIDERED OR RELIED UPON AS ANY FORM OF FINANCIAL, TAX, LEGAL, REGULATORY, OR OTHER ADVICE.

TECHNICAL DISCLAIMER

ALL SERVICES, AUDIT REPORTS, SMART CONTRACT AUDITS, OTHER MATERIALS, OR ANY PRODUCTS OR RESULTS OF THE USE THEREOF ARE PROVIDED "AS IS" AND "AS AVAILABLE" AND WITH ALL FAULTS AND DEFECTS WITHOUT WARRANTY OF ANY KIND. TO THE MAXIMUM EXTENT PERMITTED UNDER APPLICABLE LAW, VITAL BLOCK HEREBY DISCLAIMS ALL WARRANTIES, WHETHER EXPRESSED, IMPLIED, STATUTORY, OR OTHERWISE WITH RESPECT TO SERVICES, AUDIT REPORT, OR OTHER MATERIALS. WITHOUT LIMITING THE FOREGOING, VITAL BLOCK SPECIFICALLY DISCLAIMS ALL IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, TITLE AND NON-INFRINGEMENT, AND ALL WARRANTIES ARISING FROM THE COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

WITHOUT LIMITING THE FOREGOING, VITAL BLOCK MAKES NO WARRANTY OF ANY KIND THAT ALL SERVICES, AUDIT REPORTS, SMART CONTRACT AUDITS, OR OTHER MATERIALS, OR ANY PRODUCTS OR RESULTS OF THE USE THEREOF, WILL MEET THE CLIENT'S OR ANY OTHER INDIVIDUAL'S REQUIREMENTS, ACHIEVE ANY INTENDED RESULT, BE COMPATIBLE OR WORK WITH ANY SOFTWARE, SYSTEM, OR OTHER SERVICES, OR BE SECURE, ACCURATE, COMPLETE, FREE OF HARMFUL CODE, OR ERROR-FREE.

TIMELINESS OF CONTENT

The content contained in this audit report is subject to change without any prior notice. Vital Block does not guarantee or warrant the accuracy, timeliness, or completeness of any report you access using the internet or other means, and assumes no obligation to update any information following the publication.

LINKS TO OTHER WEBSITES

This audit report provides, through hypertext or other computer links, access to websites and social accounts operated by individuals other than Vital Block. Such hyperlinks are provided for your reference and convenience only and are the exclusive responsibility of such websites and social accounts owners. You agree that Vital block Security is not responsible for the content or operation of such websites and social accounts and that Vital Block shall have no liability to you or any other person or entity for the use of third-party websites and social accounts. You are solely responsible for determining the extent to which you may use any content at any other websites and social accounts to which you link from the report.

ABOUT VITAL BLOCK

Vital Block provides intelligent blockchain Security Solutions. We provide solidity and Raw Code Review, testing, and auditing services. We have Partnered with 15+ Crypto Launchpads, audited 50+ smart contracts, and analyzed 200,000+ code lines. We have worked on major public blockchains e.g., Ethereum, Binance, Cronos, Doge, Polygon, Avalanche, Metis, Fantom, Bitcoin Cash, Aptos, Oasis, etc.

Vital Block is Dedicated to Making Defi & Web3 A Safer Place. We are Powered by Security engineers, developers, UI experts, and blockchain enthusiasts. Our team currently consists of 5 core members, and 4+ casual contributors.

Website: https://Vitalblock.org

Email: info@vitalblock.org

GitHub: https://github.com/vital-block

Telegram (Engineering): https://t.me/vital_block

Telegram (Onboarding): https://t.me/vitalblock_cmo

vital-block

info@vitalblock.org

www.Vitalblock.org

Vital Block Dedicated to securing Public and Private Blockchain Ecosystem