SMART CONTRACT AUDIT REPORT

for

Antimatter Finance

Prepared By: Yiqun Chen

PeckShield

September 8, 2021

Document Properties

Client	Antimatter Finance
Title	Smart Contract Audit Report
Target	Antimatter Finance
Version	1.0
Author	Xiaotao Wu
Auditors	Xiaotao Wu, Xuxian Jiang
Reviewed by	Yiqun Chen
Approved by	Xuxian Jiang
Classification	Public

Version Info

Version	Date	Author(s)	Description
1.0	September 8, 2021	Xiaotao Wu	Final Release
1.0-rc	September 7, 2021	Xiaotao Wu	Release Candidate #1

Contact

For more information about this document and its contents, please contact PeckShield Inc.

Name	Yiqun Chen
Phone	+86 183 5897 7782
Email	contact@peckshield.com

Contents

1 Introduction

Given the opportunity to review the design document and related source code of the `Antimatter Finance` protocol, we outline in the report our systematic approach to evaluate potential security issues in the smart contract implementation, expose possible semantic inconsistencies between smart contract code and design document, and provide additional suggestions or recommendations for improvement. Our results show that the given version of smart contracts can be further improved due to the presence of several issues related to either security or performance. This document outlines our audit results.

1.1 About Antimatter Finance

The `Antimatter Finance` protocol aims to decide whether a particular cryptocurrency is bullish or bearish by using a financial derivative: perpetual options. A perpetual option is a non-standard option that can be exercised any time without expiration. `Antimatter Finance` achieves this by tokenizing perpetual options, so that investor can generate, redeem, and trade these tokens. `Antimatter Finance` users can judge based on two facts: the market price of the asset and the cost of generating tokens.

The basic information of audited contracts is as follows:

Table 1.1: Basic Information of Antimatter Finance

Item	Description
Name	Antimatter Finance
Website	https://antimatter.finance/
Type	Ethereum Smart Contract
Platform	Solidity
Audit Method	Whitebox
Latest Audit Report	September 8, 2021

In the following, we show the MD5 hash value of the related file with the contracts used in this audit.

- MD5 (PerpetualOption.sol) = be5d5ea6abc69ef7f6742e323886f8dd

1.2 About PeckShield

PeckShield Inc. [8] is a leading blockchain security company with the goal of elevating the security, privacy, and usability of current blockchain ecosystems by offering top-notch, industry-leading services and products (including the service of smart contract auditing). We are reachable at Telegram (https://t.me/peckshield), Twitter (http://twitter.com/peckshield), or Email (contact@peckshield.com).

Table 1.2: Vulnerability Severity Classification

Impact \ Likelihood	*High*	*Medium*	*Low*
High	Critical	High	Medium
Medium	High	Medium	Low
Low	Medium	Low	Low

1.3 Methodology

To standardize the evaluation, we define the following terminology based on OWASP Risk Rating Methodology [7]:

- Likelihood represents how likely a particular vulnerability is to be uncovered and exploited in the wild;
- Impact measures the technical loss and business damage of a successful attack;
- Severity demonstrates the overall criticality of the risk.

Likelihood and impact are categorized into three ratings: *H*, *M* and *L*, i.e., *high*, *medium* and *low* respectively. Severity is determined by likelihood and impact, and can be accordingly classified into four categories, i.e., *Critical*, *High*, *Medium*, *Low* shown in Table 1.2.

To evaluate the risk, we go through a list of check items and each would be labeled with a severity category. For one check item, if our tool or analysis does not identify any issue, the contract is considered safe regarding the check item. For any discovered issue, we might further

Table 1.3: The Full List of Check Items

Category	Check Item
Basic Coding Bugs	Constructor Mismatch
	Ownership Takeover
	Redundant Fallback Function
	Overflows & Underflows
	Reentrancy
	Money-Giving Bug
	Blackhole
	Unauthorized Self-Destruct
	Revert DoS
	Unchecked External Call
	Gasless Send
	Send Instead Of Transfer
	Costly Loop
	(Unsafe) Use Of Untrusted Libraries
	(Unsafe) Use Of Predictable Variables
	Transaction Ordering Dependence
	Deprecated Uses
Semantic Consistency Checks	Semantic Consistency Checks
Advanced DeFi Scrutiny	Business Logics Review
	Functionality Checks
	Authentication Management
	Access Control & Authorization
	Oracle Security
	Digital Asset Escrow
	Kill-Switch Mechanism
	Operation Trails & Event Generation
	ERC20 Idiosyncrasies Handling
	Frontend-Contract Integration
	Deployment Consistency
	Holistic Risk Management
Additional Recommendations	Avoiding Use of Variadic Byte Array
	Using Fixed Compiler Version
	Making Visibility Level Explicit
	Making Type Inference Explicit
	Adhering To Function Declaration Strictly
	Following Other Best Practices

deploy contracts on our private testnet and run tests to confirm the findings. If necessary, we would additionally build a PoC to demonstrate the possibility of exploitation. The concrete list of check items is shown in Table 1.3.

In particular, we perform the audit according to the following procedure:

- Basic Coding Bugs: We first statically analyze given smart contracts with our proprietary static code analyzer for known coding bugs, and then manually verify (reject or confirm) all the issues found by our tool.

- Semantic Consistency Checks: We then manually check the logic of implemented smart contracts and compare with the description in the white paper.

- Advanced DeFi Scrutiny: We further review business logics, examine system operations, and place DeFi-related aspects under scrutiny to uncover possible pitfalls and/or bugs.

- Additional Recommendations: We also provide additional suggestions regarding the coding and development of smart contracts from the perspective of proven programming practices.

To better describe each issue we identified, we categorize the findings with Common Weakness Enumeration (CWE-699) [6], which is a community-developed list of software weakness types to better delineate and organize weaknesses around concepts frequently encountered in software development. Though some categories used in CWE-699 may not be relevant in smart contracts, we use the CWE categories in Table 1.4 to classify our findings. Moreover, in case there is an issue that may affect an active protocol that has been deployed, the public version of this report may omit such issue, but will be amended with full details right after the affected protocol is upgraded with respective fixes.

1.4 Disclaimer

Note that this security audit is not designed to replace functional tests required before any software release, and does not give any warranties on finding all possible security issues of the given smart contract(s) or blockchain software, i.e., the evaluation result does not guarantee the nonexistence of any further findings of security issues. As one audit-based assessment cannot be considered comprehensive, we always recommend proceeding with several independent audits and a public bug bounty program to ensure the security of smart contract(s). Last but not least, this security audit should not be used as investment advice.

Table 1.4: Common Weakness Enumeration (CWE) Classifications Used in This Audit

Category	Summary
Configuration	Weaknesses in this category are typically introduced during the configuration of the software.
Data Processing Issues	Weaknesses in this category are typically found in functionality that processes data.
Numeric Errors	Weaknesses in this category are related to improper calculation or conversion of numbers.
Security Features	Weaknesses in this category are concerned with topics like authentication, access control, confidentiality, cryptography, and privilege management. (Software security is not security software.)
Time and State	Weaknesses in this category are related to the improper management of time and state in an environment that supports simultaneous or near-simultaneous computation by multiple systems, processes, or threads.
Error Conditions, Return Values, Status Codes	Weaknesses in this category include weaknesses that occur if a function does not generate the correct return/status code, or if the application does not handle all possible return/status codes that could be generated by a function.
Resource Management	Weaknesses in this category are related to improper management of system resources.
Behavioral Issues	Weaknesses in this category are related to unexpected behaviors from code that an application uses.
Business Logics	Weaknesses in this category identify some of the underlying problems that commonly allow attackers to manipulate the business logic of an application. Errors in business logic can be devastating to an entire application.
Initialization and Cleanup	Weaknesses in this category occur in behaviors that are used for initialization and breakdown.
Arguments and Parameters	Weaknesses in this category are related to improper use of arguments or parameters within function calls.
Expression Issues	Weaknesses in this category are related to incorrectly written expressions within code.
Coding Practices	Weaknesses in this category are related to coding practices that are deemed unsafe and increase the chances that an exploitable vulnerability will be present in the application. They may not directly introduce a vulnerability, but indicate the product has not been carefully developed or maintained.

2 Findings

2.1 Summary

Here is a summary of our findings after analyzing the design and implementation of the `Antimatter Finance` smart contracts. During the first phase of our audit, we study the smart contract source code and run our in-house static code analyzer through the codebase. The purpose here is to statically identify known coding bugs, and then manually verify (reject or confirm) issues reported by our tool. We further manually review business logics, examine system operations, and place DeFi-related aspects under scrutiny to uncover possible pitfalls and/or bugs.

Severity	# of Findings	
Critical	0	
High	0	
Medium	1	■
Low	1	■
Informational	2	■ ■
Total	4	

We have so far identified a list of potential issues: some of them involve subtle corner cases that might not be previously thought of, while others refer to unusual interactions among multiple contracts. For each uncovered issue, we have therefore developed test cases for reasoning, reproduction, and/or verification. After further analysis and internal discussion, we determined a few issues of varying severities need to be brought up and paid more attention to, which are categorized in the above table. More information can be found in the next subsection, and the detailed discussions of each of them are in Section 3.

2.2 Key Findings

Overall, these smart contracts are well-designed and engineered, though the implementation can be improved by resolving the identified issues (shown in Table 2.1), including 1 medium-severity vulnerability, 1 low-severity vulnerability, and 2 informational recommendations.

Table 2.1: Key Audit Findings

ID	Severity	Title	Category	Status
PVE-001	Informational	Meaningful Events For Important State Changes	Coding Practices	Confirmed
PVE-002	Informational	Unused/Commented-out Code Removal	Coding Practices	Confirmed
PVE-003	Medium	Trust Issue of Admin Keys	Security Features	Confirmed
PVE-004	Low	Accommodation of Non-ERC20-Compliant Tokens	Business Logic	Fixed

Beside the identified issues, we emphasize that for any user-facing applications and services, it is always important to develop necessary risk-control mechanisms and make contingency plans, which may need to be exercised before the mainnet deployment. The risk-control mechanisms should kick in at the very moment when the contracts are being deployed on mainnet. Please refer to Section 3 for details.

3 Detailed Results

3.1 Meaningful Events For Important State Changes

- ID: PVE-001
- Severity: Informational
- Likelihood: N/A
- Impact: N/A
- Target: Factory
- Category: Coding Practices [5]
- CWE subcategory: CWE-563 [3]

Description

In Ethereum, the event is an indispensable part of a contract and is mainly used to record a variety of runtime dynamics. In particular, when an event is emitted, it stores the arguments passed in transaction logs and these logs are made accessible to external analytics and reporting tools. Events can be emitted in a number of scenarios. One particular case is when system-wide parameters or settings are being changed. Another case is when tokens are being minted, transferred, or burned.

In the following, we use the Factory contract as an example. While examining the events that reflect the Factory dynamics, we notice there is a lack of emitting related event that reflect important state changes. Specifically, when the feeRate and config[_feeTo_] are being changed, there is no corresponding event being emitted to reflect the changes of feeRate and config[_feeTo_] (line 1990 and line 1991).

```
1988    function setFee(uint feeRate_, address feeTo) public governance {
1989        require(feeRate_ <= MAX_FEE_RATE);
1990        feeRate = feeRate_;
1991        config[_feeTo_] = uint(feeTo);
1992    }
```

Listing 3.1: Factory::setFee()

Recommendation Properly emit the related SetFee event when the feeRate and config[_feeTo_] are being changed.

Status The issue has been confirmed.

3.2 Unused/Commented-out Code Removal

- ID: PVE-002
- Severity: Informational
- Likelihood: N/A
- Impact: N/A
- Target: `Multiple contracts`
- Category: Coding Practices [5]
- CWE subcategory: CWE-563 [3]

Description

While reviewing the implementation of `PerpetualOption`, we observe the inclusion of certain commented-out code or the presence of unnecessary redundancies that can be safely removed. Take the `calc()` routine of the `Factory` contract as an example, the code in lines 2657 through 2659 are commented out and can be safely removed.

```
2654     function calc(uint priceFloor, uint priceCap, uint totalCall, uint totalPut) public
             pure returns (uint totalUnd, uint totalCur) {
2655         if(totalCall == 0 && totalPut == 0)
2656             return (0, 0);
2657         //uint temp = totalCall.mul(totalPut).div(totalCall.add(totalPut)).mul(priceCap.
                 sub(priceFloor)).div(1e18).mul(2);      // V1
2658         //totalUnd = temp.mul(totalCall).div(totalCall.mul(priceFloor).add(totalPut.mul(
                 priceCap)).div(1e18));
2659         //totalCur = temp.mul(totalPut).div(totalCall.add(totalPut));
2660
2661         totalCur = Math.sqrt(totalCall.mul(totalCall).add(totalPut.mul(totalPut)));
2662         totalUnd = totalCall.mul(totalCall).div(totalCur).mul(priceCap.sub(priceFloor)).
                 div(Math.sqrt(priceCap.mul(priceFloor)));
2663         totalCur = totalPut.mul(totalPut).div(totalCur).mul(priceCap.sub(priceFloor)).
                 div(1e18);
2664     }
```

Listing 3.2: `Factory::calc()`

In the `Antimatter Finance` protocol, there are also a number of commented-out functions. Take the `upgradeCallPut()` routine of the `Factory` contract as an example, the entire implementation of this function is commented out and will not be used. Therefore, we suggest to remove this redundant code.

```
    //function upgradeCallPut(address implCall, address implPut) external governance {
    //    __ReentrancyGuard_init_unchained();
    //    for(uint i=0; i<allCalls.length; i++) {
    //        address call = allCalls[i];
    //        address put  = allPuts [i];
    //        Call(call).withdraw_(put,  IERC20(Call(call).underlying()).balanceOf(call)
        );
    //        Put( put ).withdraw_(call, IERC20(Put (put ).currency()  ).balanceOf(put )
        );
```

```
//     }
//     productImplementations[_Call_] = implCall;
//     productImplementations[_Put_]  = implPut;
//}
```

Listing 3.3: `Factory::upgradeCallPut()`

Recommendation Consider the removal of the commented-out code with a simplified, consistent implementation.

Status The issue has been confirmed.

3.3 Trust Issue of Admin Keys

- ID: PVE-003
- Severity: Medium
- Likelihood: Low
- Impact: High
- Target: `Multiple contracts`
- Category: Security Features [4]
- CWE subcategory: CWE-287 [2]

Description

In the `Antimatter Finance` protocol, there are certain privileged accounts, i.e., `governor`, `admin` and `authority`. When examining the related contracts, i.e., `Governable`, `Configurable` and `Factory`, we notice inherent trust on these privileged accounts. To elaborate, we show below the related functions.

Firstly, the `transferGovernorship()` function allows for the `admin` or `governor` to transfer the `governor` role to the `newGovernor`.

```
/**
 * @dev Allows the current governor to transfer control of the contract to a
     newGovernor.
 * @param newGovernor The address to transfer governorship to.
 */
function transferGovernorship(address newGovernor) public governance {
    _transferGovernorship(newGovernor);
}

/**
 * @dev Transfers control of the contract to a newGovernor.
 * @param newGovernor The address to transfer governorship to.
 */
function _transferGovernorship(address newGovernor) internal {
    require(newGovernor != address(0));
    emit GovernorshipTransferred(governor, newGovernor);
    governor = newGovernor;
```

```
    }
```

Listing 3.4: `Governable::transferGovernorship()/_transferGovernorship()`

Secondly, the `setConfig()`, `setConfigI()` and `setConfigA()` functions allow for the `admin` or `governor` to set the key parameters for the `Antimatter Finance` protocol.

```
    function setConfig(bytes32 key, uint value) external governance {
        _setConfig(key, value);
    }
    function setConfigI(bytes32 key, uint index, uint value) external governance {
        _setConfig(bytes32(uint(key) ^ index), value);
    }
    function setConfigA(bytes32 key, address addr, uint value) public governance {
        _setConfig(bytes32(uint(key) ^ uint(addr)), value);
    }
```

Listing 3.5: `Configurable::setConfig()/setConfigI()/setConfigA()`

Lastly, the `transferAuth_()` function allows for the `authority` to transfer the `Call`/`Put` tokens from the `Antimatter Finance` users without restriction.

```
    function transferAuth_(address callOrPut, address sender, address recipient, uint256
         amount) external {
        require(getConfigA(_isAuthority_, _msgSender()) != 0, 'Not Authority');
        Call(callOrPut).transfer_(sender, recipient, amount);
    }
```

Listing 3.6: `Factory::transferAuth_()`

We understand the need of the privileged function for contract operation, but at the same time the extra power to the `governor/admin/authority` may also be a counter-party risk to the contract users. Therefore, we list this concern as an issue here from the audit perspective and highly recommend making these privileges explicit or raising necessary awareness among protocol users.

Recommendation Make the list of extra privileges granted to `governor/admin/authority` explicit to `Antimatter Finance` users.

Status The issue has been confirmed.

3.4 Accommodation of Non-ERC20-Compliant Tokens

- ID: PVE-004
- Severity: Low
- Likelihood: Low
- Impact: Low
- Target: `VanillaVirtualAccount`
- Category: Coding Practices [5]
- CWE subcategory: CWE-1126 [1]

Description

Though there is a standardized ERC-20 specification, many token contracts may not strictly follow the specification or have additional functionalities beyond the specification. In this section, we examine the `approve()` routine and analyze possible idiosyncrasies from current widely-used token contracts.

In particular, we use the popular stablecoin, i.e., `USDT`, as our example. We show the related code snippet below. On its entry of `approve()`, there is a requirement, i.e., `require(!((_value != 0) && (allowed[msg.sender][_spender] != 0)))`. This specific requirement essentially indicates the need of reducing the allowance to 0 first (by calling `approve(_spender, 0)`) if it is not, and then calling a second one to set the proper allowance. This requirement is in place to mitigate the known `approve()/transferFrom()` race condition (https://github.com/ethereum/EIPs/issues/20#issuecomment-263524729).

```
    /**
    * @dev Approve the passed address to spend the specified amount of tokens on behalf
        of msg.sender.
    * @param _spender The address which will spend the funds.
    * @param _value The amount of tokens to be spent.
    */
    function approve(address _spender, uint _value) public onlyPayloadSize(2 * 32) {

        // To change the approve amount you first have to reduce the addresses`
        //  allowance to zero by calling `approve(_spender, 0)` if it is not
        //  already 0 to mitigate the race condition described here:
        //  https://github.com/ethereum/EIPs/issues/20#issuecomment-263524729
        require(!((_value != 0) && (allowed[msg.sender][_spender] != 0)));

        allowed[msg.sender][_spender] = _value;
        Approval(msg.sender, _spender, _value);
    }
```

Listing 3.7: USDT Token **Contract**

Because of that, a normal call to `approve()` with a currently non-zero allowance may fail. In the following, we use the `Router::_transfer()` routine as an example. This routine will approve a specific amount of `undOrCur` token for `factory` contract if `vol > 0` (line 3090). To accommodate the specific idiosyncrasy, there is a need to `approve()` twice: the first one reduces the allowance to 0; and the second one sets the new allowance.

```
    function _transfer(address sender, address[] memory path, int vol, int max) internal {
        address WETH_ = WETH;
        address undOrCur = path[0];
        uint fee = Math.abs(vol).mul(Factory(factory).feeRate()).div(1e18);
        vol = vol.add_(fee);
        if(vol > 0) {
            IERC20(undOrCur).approve(factory, uint(vol));
            vol = vol.sub_(int(IERC20(path[path.length-1]).balanceOf(address(this))));
        }
        uint v = Math.abs(vol);
        if(vol < 0) {
            if(path.length <= 1) {
                require(vol <= max, _slippage_too_high_);
                if(path[path.length-1] != WETH_ && sender != address(this))
                    IERC20(undOrCur).safeTransfer(sender, v);
            } else
                _routeOut(v, (max < 0 ? uint(-max) : 0), path, path[path.length-1] ==
                    WETH_ ? address(this) : sender);
        } else if(vol > 0) {
            if(path.length <= 1) {
                require(vol <= max, _slippage_too_high_);
                IERC20(undOrCur).safeTransferFrom(sender, address(this), v);
            } else
                _routeIn(sender, v, (max > 0 ? uint(max) : 0), _revertPath(path),
                    address(this));
        }
```

Listing 3.8: `Router::_transfer()`

Moreover, it is important to note that for certain non-compliant ERC20 tokens (e.g., USDT), the `transfer()` function does not have a return value. However, the `IERC20` interface has defined the `transfer()` interface with a `bool` return value. As a result, the call to `transfer()` may expect a return value. With the lack of return value of `USDT`'s `transfer()`, the call will be unfortunately reverted.

Because of that, a normal call to `transfer()` is suggested to use the safe version, i.e., `safeTransfer()`, In essence, it is a wrapper around ERC20 operations that may either throw on failure or return false without reverts. Moreover, the safe version also supports tokens that return no value (and instead revert or throw on failure). Note that non-reverting calls are assumed to be successful. Similarly, there is a safe version of `approve()/transferFrom()` as well, i.e., `safeApprove()/safeTransferFrom()`.

Recommendation Accommodate the above-mentioned idiosyncrasy about ERC20-related `approve()`.

Status The issue has been fixed.

4 Conclusion

In this audit, we have analyzed the `Antimatter Finance` design and implementation. `Antimatter Finance` aims to decide whether a particular cryptocurrency is bullish or bearish by using a financial derivative: perpetual options. The current code base is well structured and neatly organized. Those identified issues are promptly confirmed and addressed.

Meanwhile, we need to emphasize that `Solidity`-based smart contracts as a whole are still in an early, but exciting stage of development. To improve this report, we greatly appreciate any constructive feedbacks or suggestions, on our methodology, audit findings, or potential gaps in scope/coverage.

References

[1] MITRE. CWE-1126: Declaration of Variable with Unnecessarily Wide Scope. https://cwe.mitre.org/data/definitions/1126.html.

[2] MITRE. CWE-287: Improper Authentication. https://cwe.mitre.org/data/definitions/287.html.

[3] MITRE. CWE-563: Assignment to Variable without Use. https://cwe.mitre.org/data/definitions/563.html.

[4] MITRE. CWE CATEGORY: 7PK - Security Features. https://cwe.mitre.org/data/definitions/254.html.

[5] MITRE. CWE CATEGORY: Bad Coding Practices. https://cwe.mitre.org/data/definitions/1006.html.

[6] MITRE. CWE VIEW: Development Concepts. https://cwe.mitre.org/data/definitions/699.html.

[7] OWASP. Risk Rating Methodology. https://www.owasp.org/index.php/OWASP_Risk_Rating_Methodology.

[8] PeckShield. PeckShield Inc. https://www.peckshield.com.