PALADIN
BLOCKCHAIN SECURITY

Smart Contract Security Assessment

Final Report

For SMTF Token

30 December 2021

paladinsec.co

info@paladinsec.co

Table of Contents

Disclaimer

Paladin Blockchain Security ("Paladin") has conducted an independent audit to verify the integrity of and highlight any vulnerabilities or errors, intentional or unintentional, that may be present in the codes that were provided for the scope of this audit. This audit report does not constitute agreement, acceptance or advocation for the Project that was audited, and users relying on this audit report should not consider this as having any merit for financial advice in any shape, form or nature. The contracts audited do not account for any economic developments that may be pursued by the Project in question, and that the veracity of the findings thus presented in this report relate solely to the proficiency, competence, aptitude and discretion of our independent auditors, who make no guarantees nor assurance that the contracts are completely free of exploits, bugs, vulnerabilities or deprecation of technologies. Further, this audit report shall not be disclosed nor transmitted to any persons or parties on any objective, goal or justification without due written assent, acquiescence or approval by Paladin.

All information provided in this report does not constitute financial or investment advice, nor should it be used to signal that any persons reading this report should invest their funds without sufficient individual due diligence regardless of the findings presented in this report. Information is provided 'as is', and Paladin is under no covenant to the completeness, accuracy or solidity of the contracts audited. In no event will Paladin or its partners, employees, agents or parties related to the provision of this audit report be liable to any parties for, or lack thereof, decisions and/or actions with regards to the information provided in this audit report.

Cryptocurrencies and any technologies by extension directly or indirectly related to cryptocurrencies are highly volatile and speculative by nature. All reasonable due diligence and safeguards may yet be insufficient, and users should exercise considerable caution when participating in any shape or form in this nascent industry.

The audit report has made all reasonable attempts to provide clear and articulate recommendations to the Project team with respect to the rectification, amendment and/or revision of any highlighted issues, vulnerabilities or exploits within the contracts provided. It is the sole responsibility of the Project team to sufficiently test and perform checks, ensuring that the contracts are functioning as intended, specifically that the functions therein contained within said contracts have the desired intended effects, functionalities and outcomes of the Project team.

Paladin retains full rights over all intellectual property (including expertise and new attack or exploit vectors) discovered during the audit process. Paladin is therefore allowed and expected to re-use this knowledge in subsequent audits and to inform existing projects that may have similar vulnerabilities. Paladin may, at its discretion, claim bug bounties from third-parties while doing so.

1 Overview

This report has been prepared for SmartFi's SMTF token on the Binance Smart Chain. Paladin provides a user-centred examination of the smart contracts to look for vulnerabilities, logic errors or other issues from both an internal and external perspective.

1.1 Summary

Project Name	SmartFi (SMTF Token)
URL	https://smartfi.com/
Platform	Binance Smart Chain
Language	Solidity

1.2 Contracts Assessed

Name	Contract	Live Code Match
SMTF	`0x11fd9ed04f1eb43ef9df6425a6990609f2468895`	MATCH

1.3 Findings Summary

Severity	Found	Resolved	Partially Resolved	Acknowledged (no change made)
High	0	0	-	-
Medium	0	0	-	-
Low	0	0	-	-
Informational	2	0	-	2
Total	**2**	**0**	**-**	**2**

Classification of Issues

Severity	Description
High	Exploits, vulnerabilities or errors that will certainly or probabilistically lead towards loss of funds, control, or impairment of the contract and its functions. Issues under this classification are recommended to be fixed with utmost urgency.
Medium	Bugs or issues with that may be subject to exploit, though their impact is somewhat limited. Issues under this classification are recommended to be fixed as soon as possible.
Low	Effects are minimal in isolation and do not pose a significant danger to the project or its users. Issues under this classification are recommended to be fixed nonetheless.
Informational	Consistency, syntax or style best practices. Generally pose a negligible level of risk, if any.

1.3.1 SMTF

ID	Severity	Summary	Status
01	INFO	Mint amount has too many digits	ACKNOWLEDGED
02	INFO	Total supply is minted to the deployer	ACKNOWLEDGED

2 Findings

2.1 SMTF

The SMTF token is an ERC-20 token. It has a total supply of 1,000,000,000 tokens, and the total supply is minted to the deployer when the contract is deployed. After which, no tokens can be minted.

2.1.1 Token Overview

Address	`0x11fd9ed04f1eb43ef9df6425a6990609f2468895`
Token Supply	1,000,000,000
Decimal Places	18
Transfer Max Size	No maximum
Transfer Min Size	No minimum
Transfer Fees	None

2.1.2 Issues & Recommendations

Issue #01	Mint amount has too many digits
Severity	INFORMATIONAL
Location	Line 485 `_mint(msg.sender, 1000000000 * 10 ** decimals());`
Description	Literals with many digits are difficult to read and review.
Recommendation	Consider changing the amount to be minted to something more readable such as `1_000_000_000`.
Resolution	ACKNOWLEDGED The team has acknowledged this issue as they will not be redeploying the contract.

Issue #02	Total supply is minted to the deployer
Severity	INFORMATIONAL
Description	The deployer of the token contract will have the full supply of the tokens. Depending on how the tokens are distributed after the initial mint, it could have some effects on the tokenomics of the project.
Recommendation	Communicate to the community how the token distribution will be allocated. If a huge allocation of tokens are to be stored in something like a treasury, ensure that a multisignature solution is used.
Resolution	ACKNOWLEDGED The team has acknowledged this issue as they will not be redeploying the contract.


PALADIN
BLOCKCHAIN SECURITY