SOLIDIKEY
TECHNOLOGY
LIMITED

SECURITY AUDIT

ARK **PULSE**

Website:: https://Arkpulse.xyz

Contract: ARK.sol , Square.sol, Circle.sol

Approved: 27 October 2023

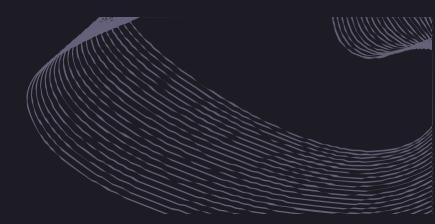SOLIDIKEY

Table of Contents

CRITICAL ISSUES
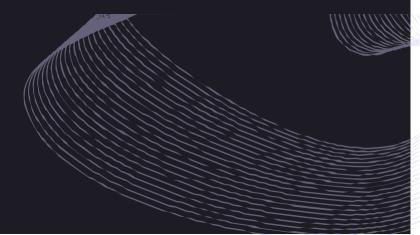
(critical, high severity): 0

Critical and harmful access for owners, user block ability, Bugs, and vulnerabilities that enable theft of funds, lock access to funds without possibility to restore it or lead to any other loss of funds to be transferredto any party.

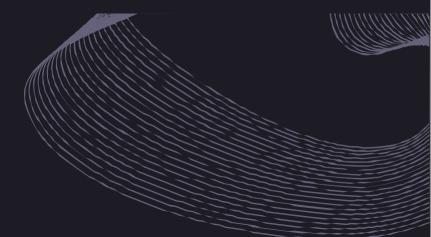# ERRORS, BUGS AND WARNINGS

(medium, low severity): 0

Bugs can negatively affect the usability of a program, errors that can trigger a contract failure, Lack of necessary security precautions, other warnings for owners and users, warning codes that are valid code but the compiler thinks are suspicious.
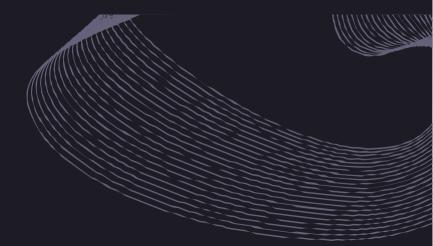
OPTIMIZATION

(low severity): 0

Methods to decrease the cost of transactions in Smart-Contract.

RECOMMENDATIONS

(very low severity): 0

Hint and tips to improve
contract functionality and
trustworthiness.

CONCLUSION

In the ARKPULSE Smart-Contract were found no vulnerabilities, nobackdoors, and no scam scripts.
The code was tested with compatible compilers and simulated manually reviewed for all commonly known and specific vulnerabilities.
So ARKPULSE Smart-Contract is safe for use in the PULSECHAIN network.

INDEPENDENT DESCRIPTION OF THE SMART–CONTRACT FUNCTIONALITY

- The report has been prepared for ARK PULSE. The Pulse Rate project is a Tomb Finance fork, allowing users to acquire $ARK(pegged to 1 PLS) and $SQUARE(share token) tokens. Both ARK and SQUARE tokens are ERC20 standard tokens, ARK has privileged account allowed to mint. SQUARE reward pool (SQUARERewardPool contract) may charge a fee of up to 2% for each deposit.
  Contracts checked

ARK.sol
SQUARE.sol
CIRCLE.sol
boardroom.sol
SQUARERewardPool.sol
treasury.sol
oracle.sol

Procedure

We perform our audit according to the following procedure:
Automated analysis
    Scanning the project's smart contracts with several publicly available automated Solidity analysis tools Manual verification (reject or confirm) all the issues found by the tools

Manual audit
    Manually analyze smart contracts for security vulnerabilities Smart contracts' logic check

Known vulnerabilities checked

Title	Check result
Unencrypted Private Data On-Chain	passed
Code With No Effects	passed
Message call with hardcoded gas amount	passed
Typographical Error	passed
DoS With Block Gas Limit	passed
Presence of unused variables	passed
Incorrect Inheritance Order	passed
Requirement Violation	passed
Weak Sources of Randomness from Chain Attributes	passed
Shadowing State Variables	passed
Incorrect Constructor Name	passed
Block values as a proxy for time	passed
Authorization through tx.origin	passed
DoS with Failed Call	passed
Delegatecall to Untrusted Callee	passed
Assert Violation	passed
State Variable Default Visibility	passed
Reentrancy	passed

Owner capabilities (Centralization risks):
The project is fully centralized.
ARK token is open for minting by operator account, which is assigned by the owner, other contracts are highly dependent on the owner's account.
Recommendation: Renounce ownership wherever possible and/or secure owner's account.
Unlimited deposit fee (squareRewardPool.sol):
Each pool has individual deposit fee which can be set from 0 to 2% (up to 2% in the updated version) during pool creation. However, the operator can update pool parameters after creation without any restrictions on the depositFeeBP parameter.

DISCLAIMER

This audit is only to the Smart-Contract code at the specified address. Solidikey technology limited is a 3rd party auditing company that works on audits based on client requests. And as a professional auditing firm, we check on the contract for any vulnerabilities, backdoors, and/or scam scripts.
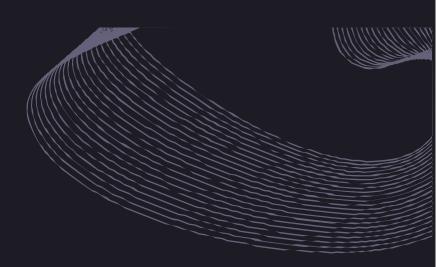
Therefore:

We are not financial advisors nor do we partner with the contract owners

Operations and website administration is fully on the client's side

We do not have influence over client operations, which can lead to website changes, withdrawal function closes, etc. One always has the option to do this through the contract.

Any concerns about the project themselves need to be raised directly to the project owners and not through Solidikey technology limited.

Investors are not in any way obliged, coerced or influenced to invest in projects audited by Solidikey technology limited.

We are not responsible for your funds or guarantee you profits.We highly recommend that investors do their own research and gain crypto experience before investing.

SOLIDIKEY
TECHNOLOGY
LIMITED

Questions? Contact us.

Solidikey.us

Hello@Solidikey.us

https://twitter.com/solidikey2