Six Network

Definix Core Contracts

Security Assessment

March 29th, 2021

Audited By:
Alex Papageorgiou @ CertiK
alex.papageorgiou@certik.org
Reviewed By:
Camden Smallwood @ CertiK
camden.smallwood@certik.org

Disclaimer

CertiK reports are not, nor should be considered, an "endorsement" or "disapproval" of any particular project or team. These reports are not, nor should be considered, an indication of the economics or value of any "product" or "asset" created by any team or project that contracts CertiK to perform a security review.

CertiK Reports do not provide any warranty or guarantee regarding the absolute bug-free nature of the technology analyzed, nor do they provide any indication of the technologies proprietors, business, business model or legal compliance.

CertiK Reports should not be used in any way to make decisions around investment or involvement with any particular project. These reports in no way provide investment advice, nor should be leveraged as investment advice of any sort.

CertiK Reports represent an extensive auditing process intending to help our customers increase the quality of their code while reducing the high level of risk presented by cryptographic tokens and blockchain technology.

Blockchain technology and cryptographic assets present a high level of ongoing risk. CertiK's position is that each company and individual are responsible for their own due diligence and continuous security. CertiK's goal is to help reduce the attack vectors and the high level of variance associated with utilizing new and consistently changing technologies, and in no way claims any guarantee of security or functionality of the technology we agree to analyze.

What is a CertiK report?

- A document describing in detail an in depth analysis of a particular piece(s) of source code provided to CertiK by a Client.
- An organized collection of testing results, analysis and inferences made about the structure, implementation and overall best practices of a particular piece of source code.
- Representation that a Client of CertiK has completed a round of auditing with the intention to increase the quality of the company/product's IT infrastructure and or source code.

Overview

Project Summary

Project Name	Six Network - Definix Core Contracts
Description	The core DEX contracts of the Definix implementation based on Uniswap.
Platform	Ethereum; Solidity, Yul
Codebase	GitHub Repository
Commits	1. fbcee365914d1eeea933a058ba2f82d3fb3160e6

Audit Summary

Delivery Date	March 29th, 2021
Method of Audit	Static Analysis, Manual Review
Consultants Engaged	1
Timeline	March 26th, 2021 - March 29th, 2021

Vulnerability Summary

Total Issues	1
Total Critical	0
Total Major	0
Total Medium	1
Total Minor	0
Total Informational	0

Executive Summary

We were tasked with auditing the Definix DEX implementation that is based on PancakeSwap which in turn is based on Uniswap.

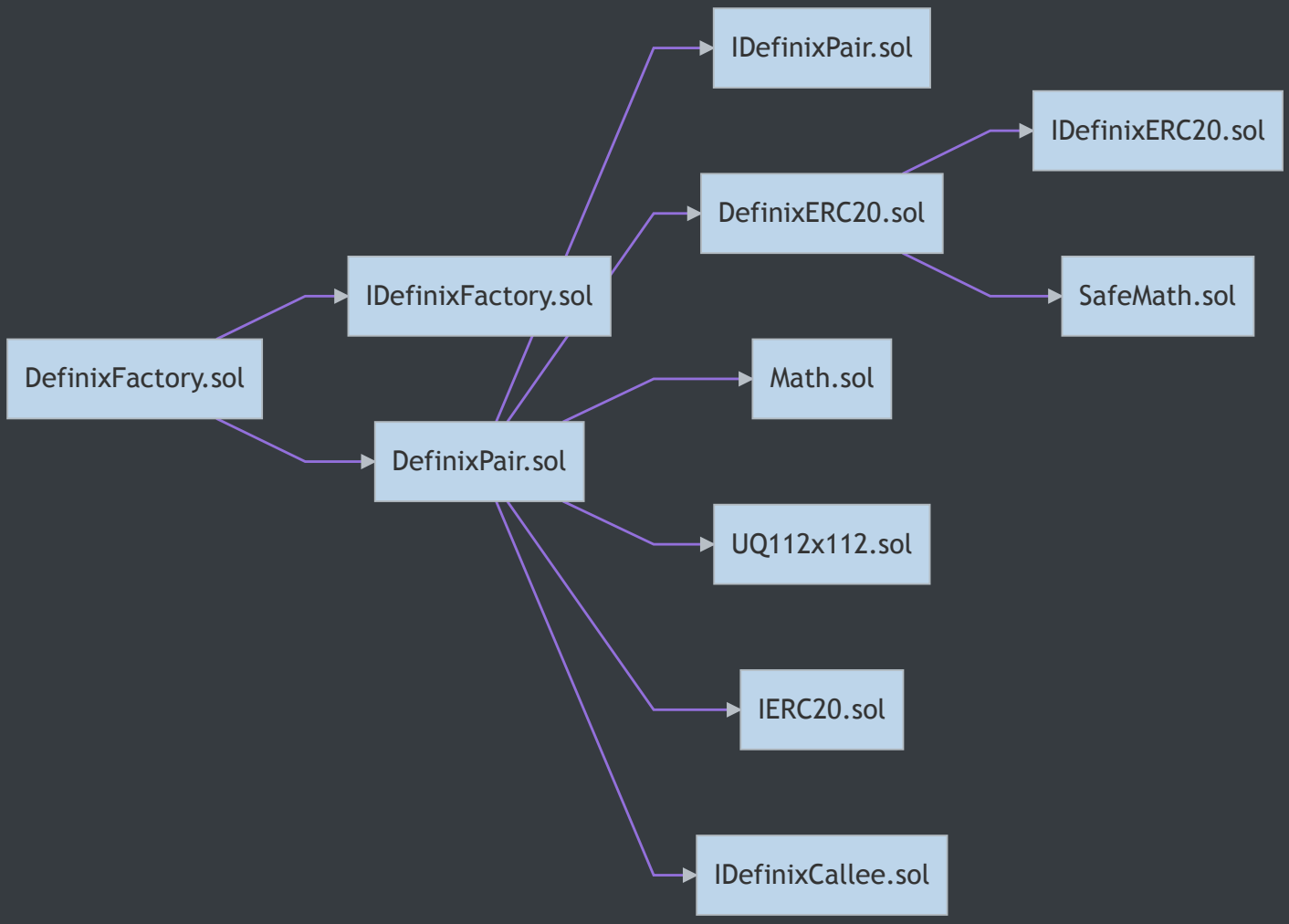
There were no changes introduced to the Definix codebase from the PancakeSwap implementation, however, we should note that the PancakeSwap implementation deviates from the Uniswap implementation in that it imposes a 0.2% fee on trades instead of a 0.3% fee and continues to split that fee in a final resulting 0.05% fee towards the fee address of the protocol.

A single finding was identified that is a well known issue with regards to the usage of a domain separator that we advise the Definix team to fix to ensure no issues may arise in a consequent fork of the chain the project deploys to.

Files In Scope

ID	Contract	Location
DER	DefinixERC20.sol	contracts/DefinixERC20.sol
DFY	DefinixFactory.sol	contracts/DefinixFactory.sol
DPR	DefinixPair.sol	contracts/DefinixPair.sol
IDC	IDefinixCallee.sol	contracts/interfaces/IDefinixCallee.sol
IDE	IDefinixERC20.sol	contracts/interfaces/IDefinixERC20.sol
IDF	IDefinixFactory.sol	contracts/interfaces/IDefinixFactory.sol
IDP	IDefinixPair.sol	contracts/interfaces/IDefinixPair.sol
IER	IERC20.sol	contracts/interfaces/IERC20.sol
MAT	Math.sol	contracts/libraries/Math.sol
SMH	SafeMath.sol	contracts/libraries/SafeMath.sol
UQ2	UQ112x112.sol	contracts/libraries/UQ112x112.sol

File Dependency Graph



Manual Review Findings

ID	Title	Type	Severity	Resolved
DER-01	Cross-Chain Replay Attack	Logical Issue	Medium	

DER-01: Cross-Chain Replay Attack

Type	Severity	Location
Logical Issue	Medium	DefinixERC20.sol L29-L37

Description:

The `DOMAIN_SEPARATOR` used by the contract is only computed once during its `constructor` whereby the current `chainid` is evaluated once.

Recommendation:

We advise it to be re-computed each time on the `permit` function instead as calculating the separator once causes cross-chain replay attacks to be possible whereby the chain the contract is deployed in forks, contains a different `chainid` but due to the separator being assigned once utilizes the main chain's `chainid` thus enabling a single permit to be used on both chains.

Alleviation:

The Six Network team has stated that their contracts are already live and as such, it is not possible to remediate this particular exhibit. The security vulnerability that arises from this exhibit would only manifest if the Binance chain the contracts are deployed in forks and produces a satellite chain on which the signatures could be replayed.

Appendix

Finding Categories

Logical Issue

Logical Issue findings are exhibits that detail a fault in the logic of the linked code, such as an incorrect notion on how `block.timestamp` works.