CERTIK

Security Assessment

BAS

May 24th, 2022

Table of Contents

Summary

This report has been prepared for BAS to discover issues and vulnerabilities in the source code of the BAS project as well as any contract dependencies that were not part of an officially recognized library. A comprehensive examination has been performed, utilizing Static Analysis and Manual Review techniques.

The auditing process pays special attention to the following considerations:

- Testing the smart contracts against both common and uncommon attack vectors.
- Assessing the codebase to ensure compliance with current best practices and industry standards.
- Ensuring contract logic meets the specifications and intentions of the client.
- Cross referencing contract structure and implementation against similar smart contracts produced by industry leaders.
- Thorough line-by-line manual review of the entire codebase by industry experts.

The security assessment resulted in findings that ranged from critical to informational. We recommend addressing these findings to ensure a high level of security standards and industry practices. We suggest recommendations that could better serve the project from the security perspective:

- Enhance general coding practices for better structures of source codes;
- Add enough unit tests to cover the possible use cases;
- Provide more comments per each function for readability, especially contracts that are verified in public;
- Provide more transparency on privileged activities once the protocol is live.

Overview

Project Summary

Project Name	BAS
Description	BSC Application Sidechain
Platform	EVM Compatible
Language	Golang
Codebase	https://github.com/Ankr-network/bas-template-bsc/tree/e5ac3a4a037a350873306ce93f5778fb7bdc0843/
Commit	e5ac3a4a037a350873306ce93f5778fb7bdc0843

Audit Summary

Delivery Date	May 24, 2022 UTC
Audit Methodology	Static Analysis, Manual Review

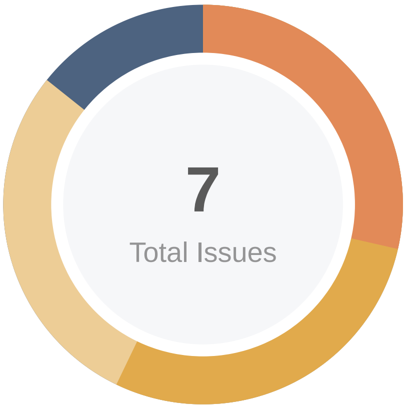
Vulnerability Summary

Vulnerability Level	Total	Pending	Declined	Acknowledged	Mitigated	Partially Resolved	Resolved
● Critical	0	0	0	0	0	0	0
● Major	2	0	0	2	0	0	0
● Medium	2	0	0	2	0	0	0
● Minor	2	0	0	2	0	0	0
● Informational	1	0	0	1	0	0	0
● Discussion	0	0	0	0	0	0	0

Audit Scope

ID	File	SHA256 Checksum
ERR	systemcontract/error.go	90050d2a5ab8eb0fd5cbdce40fc2aa00f8570f677c90f10e2cdbb84b28446cf7
COT	contracts.go	71ab48d3048066f5c5aa299ea22741bafc67694b705d7e97d09285a47a5a0fa7
EVM	evm.go	462255a596b95b62a347541adffa327101aad8bafe078625a44866dcecc11e98
TYP	systemcontract/types.go	21b567ac5e1df7bcf38914ceee088099bb8e73af9addafbd7a937e615d1b4a34
UPG	systemcontract/upgrade.go	ce369c4d363173603600343b6bc1c766f557d6775cffc7bade6260373ce2a2d3
ABI	abi.go	622802d232ca767abd77ada9bdf00fe0eaf41177f7be61c936104234fc02cb6e
CON	const.go	7af8375760f60790cec571c3079fca5d51720a76725f0ba7f59d51da6db85023
FAC	systemcontract/factory.go	1823c1de1f69e0fd2857948d96ecf7d62f44fc325cd2a994e3d3d33b87861c77

Findings



🟥 **Critical**	**0** (0.00%)
🟧 **Major**	**2** (28.57%)
🟨 **Medium**	**2** (28.57%)
▨ **Minor**	**2** (28.57%)
🟦 **Informational**	**1** (14.29%)
🟩 **Discussion**	**0** (0.00%)

ID	Title	Category	Severity	Status
CON-01	`TokenManagerContract` Is Missing In `systemContracts` Map	Logical Issue	● Medium	ⓘ Acknowledged
E5A-01	Redundant Definition Of `runtimeUpgradeContract`	Logical Issue	● Minor	ⓘ Acknowledged
EVM-01	Unused Function `CreateWithAddress()` And Meaningless Opcode `STOP`	Logical Issue	● Minor	ⓘ Acknowledged
UPG-01	The Situation Of Deploying New System Contracts Is Not Handled Properly	Logical Issue	● Major	ⓘ Acknowledged
UPG-02	For Upgrading Existing System Contracts, Deployment Code Must Be Run To Get The Final Code	Logical Issue	● Major	ⓘ Acknowledged
UPG-03	It Is Very Dangerous To Allow RuntimeUpgrade System Contract To Upgrade Itself	Logical Issue	● Medium	ⓘ Acknowledged
UPG-04	New Version And Old Version Of System Smart Contracts Must Have Compatible Storage Layout	Logical Issue	● Informational	ⓘ Acknowledged

CON-01 | `TokenManagerContract` Is Missing In `systemContracts` Map

Category	Severity	Location	Status
Logical Issue	● Medium	const.go (common/systemcontract): 19, 41~50	ⓘ Acknowledged

Description

`TokenManagerContract` is defined as one of BSC contracts. But it is missing in the `systemContracts` map. The code should make it clear whether it is enabled in BAS.

Recommendation

We recommend adding `TokenManagerContract` to the `systemContracts` map.

E5A-01 | Redundant Definition Of `runtimeUpgradeContract`

Category	Severity	Location	Status
Logical Issue	● Minor	const.go (common/systemcontract): 28, 36; systemcontract/upgrade.go (core/vm): 44	ⓘ Acknowledged

Description

The `runtimeUpgradeContract` address is defined in both `common/systemcontract/const.go` and `core/vm/systemcontract/upgrade.go`. It may lead to potential inconsistency in future changes.

Recommendation

We recommend removing `runtimeUpgradeContract` in `core/vm/systemcontract/upgrade.go`.

EVM-01 | Unused Function `CreateWithAddress()` And Meaningless Opcode `STOP`

Category	Severity	Location	Status
Logical Issue	● Minor	evm.go (core/vm): 571~575	ⓘ Acknowledged

Description

The function `CreateWithAddress()` is not used at all in the project. And it does not make any sense to use the opcode `STOP` for creating new contract.

Recommendation

We recommend removing the function `CreateWithAddress()`.

Alleviation

From BAS team: `CreateWithAddress()` is used in another project `create genesis`. Now we also use this function for the new system contract deployment.

UPG-01 | The Situation Of Deploying New System Contracts Is Not Handled Properly

Category	Severity	Location	Status
Logical Issue	● Major	systemcontract/upgrade.go (core/vm): 64	ⓘ Acknowledged

Description

Based on the example RuntimeUpgrade system smart contract at `https://github.com/Ankr-network/bas-genesis-config/blob/devel/contracts/RuntimeUpgrade.sol`, the RuntimeUpgrade evm hook can be used to deploy new system contracts. In such case, `StateDb.SetCode()` is not enough at all, many other actions like `Create a new account on the state`, `run the deployment code to get the final code`, `revert when deployment code fails`, etc must also be performed. Otherwise, deploying new system contracts will malfunction.

Recommendation

We recommend referencing the function `create()` in `https://github.com/Ankr-network/bas-template-bsc/blob/devel/core/vm/evm.go` for creating new system contracts.

Alleviation

From BAS team: Agree, in this case we might not be able to use constructor and init function after deployment will always skip calling ctor due to empty state. I'm adding new deployTo method that allows to deploy smart contract with constructors.

UPG-02 | For Upgrading Existing System Contracts, Deployment Code Must Be Run To Get The Final Code

Category	Severity	Location	Status
Logical Issue	● Major	systemcontract/upgrade.go (core/vm): 64	ⓘ Acknowledged

Description

The solidity compiler generates both deployment byte code and deployed byte code from source code. If the `upgradeTo()` parameter is deployment code, then the deployment code needs to be run in blockchain context to get the final contract byte code(deployed code) which is used as the 2nd parameter of function `StateDb.SetCode()`. No matter if the parameter is deployment code or deployed code, there must be NO immutables in system contracts. Otherwise, deployed code may NOT work.

Recommendation

We recommend handling the mentioned situation properly.

Alleviation

From BAS team: Try to bring compatibility with openzeppelin’s upgradable smart contracts. If upper solutions don’t work then make sure that we don’t lose any immutable private fields after the runtime upgrade

UPG-03 | It Is Very Dangerous To Allow RuntimeUpgrade System Contract To Upgrade Itself

Category	Severity	Location	Status
Logical Issue	● Medium	systemcontract/upgrade.go (core/vm): 56	ⓘ Acknowledged

Description

Upgrading system contract is dangerous action, especially for RuntimeUpgrade system contract itself. If there is any bug in the new version of RuntimeUpgrade system contract, the whole runtime upgrading system may stop working forever. Ideally the RuntimeUpgrade system contract should be kept minimal, simple, clear and bug free such that it does not need upgrade at all.

Recommendation

We recommend making RuntimeUpgrade system contract code immutable.

UPG-04 | New Version And Old Version Of System Smart Contracts Must Have Compatible Storage Layout

Category	Severity	Location	Status
Logical Issue	● Informational	systemcontract/upgrade.go (core/vm): 60	ⓘ Acknowledged

Description

New version and old version of system smart contracts must have compatible storage layout. Otherwise, the contract will malfunction and may be stuck in an unrecoverable state. And system contracts must avoid using immutables(better also avoid initializing state variables in field declarations and constructor(constructor must be empty)), otherwise deployed byte code will not work or deployment byte code may overwrite existing storage data and cause unrecoverable error. See https://docs.openzeppelin.com/upgrades-plugins/1.x/writing-upgradeable and https://github.com/bnb-chain/bsc-genesis-contract/tree/master/contracts.

Recommendation

We recommend reviewing new version and old version of system smart contracts before upgrade to make sure their storage layouts are absolutely compatible, avoiding immutables and keeping field declarations and constructor empty.

Alleviation

From BAS team: Try to bring compatibility with openzeppelin’s upgradable smart contracts

Appendix

Finding Categories

Logical Issue

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

Checksum Calculation Method

The "Checksum" field in the "Audit Scope" section is calculated as the SHA-256 (Secure Hash Algorithm 2 with digest size of 256 bits) digest of the content of each file hosted in the listed source repository under the specified commit.

The result is hexadecimal encoded and is the same as the output of the Linux "sha256sum" command against the target file.

Disclaimer

This report is subject to the terms and conditions (including without limitation, description of services, confidentiality, disclaimer and limitation of liability) set forth in the Services Agreement, or the scope of services, and terms and conditions provided to you (“Customer” or the “Company”) in connection with the Agreement. This report provided in connection with the Services set forth in the Agreement shall be used by the Company only to the extent permitted under the terms and conditions set forth in the Agreement. This report may not be transmitted, disclosed, referred to or relied upon by any person for any purposes, nor may copies be delivered to any other person other than the Company, without CertiK’s prior written consent in each instance.

This report is not, nor should be considered, an “endorsement” or “disapproval” of any particular project or team. This report is 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 assessment. This report does 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.

This report should not be used in any way to make decisions around investment or involvement with any particular project. This report in no way provides investment advice, nor should be leveraged as investment advice of any sort. This report represents an extensive assessing 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.

The assessment services provided by CertiK is subject to dependencies and under continuing development. 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. Cryptographic tokens are emergent technologies and carry with them high levels of technical risk and uncertainty. The assessment reports could include false positives, false negatives, and other unpredictable results. The services may access, and depend upon, multiple layers of third-parties.

ALL SERVICES, THE LABELS, THE ASSESSMENT REPORT, WORK PRODUCT, OR 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, CERTIK HEREBY DISCLAIMS ALL WARRANTIES, WHETHER EXPRESS, IMPLIED, STATUTORY, OR OTHERWISE WITH RESPECT TO THE SERVICES, ASSESSMENT REPORT, OR OTHER MATERIALS. WITHOUT LIMITING THE FOREGOING, CERTIK SPECIFICALLY DISCLAIMS ALL IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, TITLE AND NON-INFRINGEMENT, AND ALL WARRANTIES ARISING FROM COURSE OF DEALING, USAGE, OR TRADE PRACTICE. WITHOUT LIMITING THE FOREGOING, CERTIK MAKES NO WARRANTY OF ANY KIND THAT THE SERVICES, THE LABELS, THE ASSESSMENT REPORT, WORK PRODUCT, OR OTHER MATERIALS, OR ANY PRODUCTS OR RESULTS OF THE USE THEREOF, WILL MEET CUSTOMER'S OR ANY OTHER PERSON'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. WITHOUT LIMITATION TO THE FOREGOING, CERTIK PROVIDES NO WARRANTY OR UNDERTAKING, AND MAKES NO REPRESENTATION OF ANY KIND THAT THE SERVICE WILL MEET CUSTOMER'S REQUIREMENTS, ACHIEVE ANY INTENDED RESULTS, BE COMPATIBLE OR WORK WITH ANY OTHER SOFTWARE, APPLICATIONS, SYSTEMS OR SERVICES, OPERATE WITHOUT INTERRUPTION, MEET ANY PERFORMANCE OR RELIABILITY STANDARDS OR BE ERROR FREE OR THAT ANY ERRORS OR DEFECTS CAN OR WILL BE CORRECTED.

WITHOUT LIMITING THE FOREGOING, NEITHER CERTIK NOR ANY OF CERTIK'S AGENTS MAKES ANY REPRESENTATION OR WARRANTY OF ANY KIND, EXPRESS OR IMPLIED AS TO THE ACCURACY, RELIABILITY, OR CURRENCY OF ANY INFORMATION OR CONTENT PROVIDED THROUGH THE SERVICE. CERTIK WILL ASSUME NO LIABILITY OR RESPONSIBILITY FOR (I) ANY ERRORS, MISTAKES, OR INACCURACIES OF CONTENT AND MATERIALS OR FOR ANY LOSS OR DAMAGE OF ANY KIND INCURRED AS A RESULT OF THE USE OF ANY CONTENT, OR (II) ANY PERSONAL INJURY OR PROPERTY DAMAGE, OF ANY NATURE WHATSOEVER, RESULTING FROM CUSTOMER'S ACCESS TO OR USE OF THE SERVICES, ASSESSMENT REPORT, OR OTHER MATERIALS.

ALL THIRD-PARTY MATERIALS ARE PROVIDED "AS IS" AND ANY REPRESENTATION OR WARRANTY OF OR CONCERNING ANY THIRD-PARTY MATERIALS IS STRICTLY BETWEEN CUSTOMER AND THE THIRD-PARTY OWNER OR DISTRIBUTOR OF THE THIRD-PARTY MATERIALS.

THE SERVICES, ASSESSMENT REPORT, AND ANY OTHER MATERIALS HEREUNDER ARE SOLELY PROVIDED TO CUSTOMER AND MAY NOT BE RELIED ON BY ANY OTHER PERSON OR FOR ANY PURPOSE NOT SPECIFICALLY IDENTIFIED IN THIS AGREEMENT, NOR MAY COPIES BE DELIVERED TO, ANY OTHER PERSON WITHOUT CERTIK'S PRIOR WRITTEN CONSENT IN EACH INSTANCE.

NO THIRD PARTY OR ANYONE ACTING ON BEHALF OF ANY THEREOF, SHALL BE A THIRD PARTY OR OTHER BENEFICIARY OF SUCH SERVICES, ASSESSMENT REPORT, AND ANY ACCOMPANYING MATERIALS AND NO SUCH THIRD PARTY SHALL HAVE ANY RIGHTS OF CONTRIBUTION AGAINST CERTIK WITH RESPECT TO SUCH SERVICES, ASSESSMENT REPORT, AND ANY ACCOMPANYING MATERIALS.

THE REPRESENTATIONS AND WARRANTIES OF CERTIK CONTAINED IN THIS AGREEMENT ARE SOLELY FOR THE BENEFIT OF CUSTOMER. ACCORDINGLY, NO THIRD PARTY OR ANYONE ACTING ON BEHALF OF ANY THEREOF, SHALL BE A THIRD PARTY OR OTHER BENEFICIARY OF SUCH REPRESENTATIONS AND WARRANTIES AND NO SUCH THIRD PARTY SHALL HAVE ANY RIGHTS OF CONTRIBUTION AGAINST CERTIK WITH RESPECT TO SUCH REPRESENTATIONS OR WARRANTIES OR ANY MATTER SUBJECT TO OR RESULTING IN INDEMNIFICATION UNDER THIS AGREEMENT OR OTHERWISE.

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

About

Founded in 2017 by leading academics in the field of Computer Science from both Yale and Columbia University, CertiK is a leading blockchain security company that serves to verify the security and correctness of smart contracts and blockchain-based protocols. Through the utilization of our world-class technical expertise, alongside our proprietary, innovative tech, we’re able to support the success of our clients with best-in-class security, all whilst realizing our overarching vision; provable trust for all throughout all facets of blockchain.

CERTIK