



Three Sigma

Code Audit



ORANGE

Orange Bridge Cross chain Bitcoin interoperability

Disclaimer

Code Audit

Orange Bridge Cross chain Bitcoin interoperability

Disclaimer

The ensuing audit offers no assertions or assurances about the code's security. It cannot be deemed an adequate judgment of the contract's correctness on its own. The authors of this audit present it solely as an informational exercise, reporting the thorough research involved in the secure development of the intended contracts, and make no material claims or guarantees regarding the contract's post-deployment operation. The authors of this report disclaim all liability for all kinds of potential consequences of the contract's deployment or use. Due to the possibility of human error occurring during the code's manual review process, we advise the client team to commission several independent audits in addition to a public bug bounty program.

Table of Contents

Code Audit

Orange Bridge Cross chain Bitcoin interoperability

Table of Contents

Disclaimer	3
Summary	7
Scope	9
Methodology	11
Project Dashboard	13
Code Maturity Evaluation	16
Findings	19
3S-OB-M01	19
3S-OB-M02	20
3S-OB-M03	21
3S-OB-L01	22
3S-OB-L02	23
3S-OB-L03	24
3S-OB-L04	25
3S-OB-L05	26
3S-OB-L06	27
3S-OB-L07	28
3S-OB-N01	29
3S-OB-N02	30
3S-OB-N03	31
3S-OB-N04	32
3S-OB-N05	33
3S-OB-N06	34
3S-OB-N07	35

00000000	01 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00
00000010	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00
00000020	00 00 00 00 3B A3 ED FD	7A 7B 12 B2 7A C7 2C 3E	;Eiÿz{.					
00000030	67 76 8F 61 7F C8 1B C3	88 8A 51 32 3A 9F B8 AA	gv.a.Ê.Ã~SQ					
00000040	4B 1E 5E 4A 29 AB 5F 49	FF FF 00 1D 1D AC 2B 7C	K.^J)«_Iyy.					
00000050	01 01 00 00 00 01 00 00	00 00 00 00 00 00 00 00						
00000060	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00						
00000070	00 00 00 00 00 00 FF FF	FF FF 4D 04 FF FF 00 1D	ÿÿÿÿ					
00000080	01 04 45 54 68 65 20 54	69 6D 65 73 20 30 33 2F	..EThe Tim					
00000090	4A 61 6E 2F 32 30 30 39	20 43 68 61 6E 63 65 6C	Jan/2009 CH					
000000A0	6C 6F 72 20 6F 6E 20 62	72 69 6E 6B 20 6F 66 20	lor on brin					
000000B0	73 65 63 6F 6E 64 20 62	61 69 6C 6F 75 74 20 66	second bail					
000000C0	6F 72 20 62 61 6E 6B 73	FF FF FF FF 01 00 F2 05	or banksÿÿÿÿ					
000000D0	2A 01 00 00 00 43 41 04	67 8A FD B0 FE 55 48 27	*....CA.gŠÿ					
000000E0	19 67 F1 A6 71 30 B7 10	5C D6 A8 28 E0 39 09 A6	.gñ q0·.\Ö"					
000000F0	79 62 E0 EA 1F 61 DE B6	49 F6 BC 3F 4C EF 38 C4	ybaê.ab¶IÖ%					
00000100	F3 55 04 E5 1E C1 12 DE	5C 38 4D F7 BA 0B 8D 57	óU.ã.Á.Þ\8M					
00000110	8A 4C 70 2B 6B F1 1D 5F	AC 00 00 00 00	ŠLp+kñ._~..					
00000000	30 31 30 30 30 30 30 30	36 66 65 32 38 63 30 61	01000000006f					
00000001	30 31 30 30 30 30 30 30	63 31 61 36 61 32 34 36	b6f1b3726c1					
00000002	61 65 36 33 66 37 34 66	39 33 31 65 38 33 36 35	ae63f7f4639					
00000003	35 61 30 38 39 63	36 38 64 36 31 39 30 30	e15a089c638					
00000004	30 30 30 30 30 30 30 30	30 30 30 30 30 30 30 30	000000009820					
00000005	31 65 34 62 61 37 34 34	62 62 62 65 36 38 30 65	1e4ba7445bb					
00000006	31 66 65 65 31 34 36 37	37 62 61 31 61 33 63 33	1fee1456376					
00000007	35 34 30 62 66 37 62 31	63 64 62 36 30 36 65 38	5400bfb1bcd					
00000008	35 37 32 33 33 65 30 65	36 31 62 63 36 36 34 39	57233e0e6bc					
00000009	66 66 66 66 30 30 31 64	30 31 65 33 36 32 39 39	fff0001d01e					
0000000A	30 31 30 31 30 30 30 30	30 30 30 31 30 30 30 30	01010000000					
0000000B	30 30 30 30 30 30 30 30	30 30 30 30 30 30 30 30	000000000000					
0000000C	30 30 30 30 30 30 30 30	30 30 30 30 30 30 30 30	000000000000					
0000000D	30 30 30 30 30 30 30 30	30 30 30 30 30 30 30 30	000000000000					
0000000E	30 30 30 30 30 30 30 30	30 30 30 30 66 66 66 66	000000000000					
0000000F	66 66 66 66 30 37 30 34	66 66 66 66 30 30 31 64	ffff074ffff0					
00000100	30 31 30 34 66 66 66 66	66 66 66 66 30 31 30 30	0104ffffffffff					
00000110	66 32 30 35 32 61 30 31	30 30 30 30 30 30 34 33	f2052a010000					
00000120	34 31 30 34 39 36 62 35	33 38 65 38 35 33 35 31	4104946b538					
00000130	39 63 37 32 36 61 32 63	39 31 65 36 31 65 63 31	9c726ac91e6					
00000140	31 36 30 30 61 65 31 33	39 30 38 31 33 61 36 32	16000ae1390					
00000150	37 63 36 36 66 62 38 62	65 37 39 34 37 62 65 36	7c66fb8be79					
00000160	33 63 35 32 64 61 37 35	38 39 33 37 39 35 31 35	3c52da73589					
00000170	64 34 65 30 61 36 30 34	66 38 31 34 31 37 38 31	d4e0a646381					
00000180	65 36 32 32 39 34 37 32	31 31 36 36 62 66 36 32	e6224947321					
00000190	31 65 37 33 61 38 32 63	62 66 32 33 34 32 63 38	1e73a823cbf					
000001A0	35 38 65 65 61 63 30 30	30 30 30 30 30 30	58eacc000000					
00000000	30 31 30 30 30 30 30 30	34 38 36 30 65 62 31 38	010000000486					

Summary

Three Sigma audited Orange Bridge in a 3 day engagement. The audit was conducted from 15-07-2024 to 17-07-2024.

Protocol Description

Orange Bridge is a cross-chain bridge that enables interoperability across the Bitcoin ecosystem and other blockchain networks. It effortlessly bridges tokens back and forth between the Bitcoin BRC20 and Ethereum ERC20 protocols.

Components:

- Orange Bridge Web DApp - The user interface that facilitates user interactions and blockchain services.
- Smart Contract - Manages the burning and minting of ERC20 tokens.
- EVM Event Listener - Listens for events on the Ethereum Virtual Machine (EVM) chain.
- Bitcoin BRC20 Event Listener - Listens for events on the Bitcoin chain related to BRC20 tokens.
- ERC20 Token Sending Service - Handles the sending of ERC20 tokens.
- BRC20 Token Sending Service - Manages the sending of BRC20 tokens.

00000000	01 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00
00000010	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00
00000020	00 00 00 00 3B A3 ED FD	7A 7B 12 B2 7A C7 2C 3E						
00000030	67 76 8F 61 7F C8 1B C3	88 8A 51 32 3A 9F B8 AA						
00000040	4B 1E 5E 4A 29 AB 5F 49	FF FF 00 1D 1D AC 2B 7C						
00000050	01 01 00 00 00 01 00 00	00 00 00 00 00 00 00 00						
00000060	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00						
00000070	00 00 00 00 00 00 FF FF	FF FF 4D 04 FF FF 00 1D						
00000080	01 04 45 54 68 65 20 54	69 6D 65 73 20 30 33 2F						
00000090	4A 61 6E 2F 32 30 30 39	20 43 68 61 6E 63 65 6C						
000000A0	6C 6F 72 20 6F 6E 20 62	72 69 6E 6B 20 6F 66 20						
000000B0	73 65 63 6F 6E 64 20 62	61 69 6C 6F 75 74 20 66						
000000C0	6F 72 20 62 61 6E 6B 73	FF FF FF FF 01 00 F2 05						
000000D0	2A 01 00 00 00 43 41 04	67 8A FD B0 FE 55 48 27						
000000E0	19 67 F1 A6 71 30 B7 10	5C D6 A8 28 E0 39 09 A6						
000000F0	79 62 E0 EA 1F 61 DE B6	49 F6 BC 3F 4C EF 38 C4						
00000100	F3 55 04 E5 1E C1 12 DE	5C 38 4D F7 BA 0B 8D 57						
00000110	8A 4C 70 2B 6B F1 1D 5F	AC 00 00 00 00						
00000000	30 31 30 30 30 30 30 30	36 66 65 32 38 63 30 61	01000000006f					
00000000	36 66 31 62 33 37 32	63 31 61 36 61 32 34 36	b6f1b3726c1					
00000020	61 65 36 33 66 37 34 66	39 33 31 65 38 33 36 35	ae63f7f4639					
00000000	35 61 30 38 39 63	36 38 64 36 31 39 30 30	e15a089c638					
00000000	30 30 30 30 30 30 30 30	30 30 30 30 30 30 30 30	000000009820					
00000050	31 65 34 62 61 37 34 34	62 62 62 65 36 38 30 65	1e4ba7445bb					
00000060	31 66 65 65 31 34 36 37	37 62 61 31 61 33 63 33	1fee1456376					
00000070	35 34 30 62 66 37 62 31	63 64 62 36 30 36 65 38	5400bfb1bcd					
00000080	35 37 32 33 33 65 30 65	36 31 62 63 36 36 34 39	57233e0e6bc					
00000090	66 66 66 66 30 30 31 64	30 31 65 33 36 32 39 39	fff0001d01e					
000000A0	30 31 30 31 30 30 30 30	30 30 30 31 30 30 30 30	01010000000					
000000B0	30 30 30 30 30 30 30 30	30 30 30 30 30 30 30 30	000000000000					
000000C0	30 30 30 30 30 30 30 30	30 30 30 30 30 30 30 30	000000000000					
000000D0	30 30 30 30 30 30 30 30	30 30 30 30 30 30 30 30	000000000000					
000000E0	30 30 30 30 30 30 30 30	30 30 30 30 66 66 66 66	000000000000					
000000F0	66 66 66 66 30 37 30 34	66 66 66 66 30 30 31 64	ffff074ffff0					
00000100	30 31 30 34 66 66 66 66	66 66 66 66 30 31 30 30	0104ffffffffff					
00000110	66 32 30 35 32 61 30 31	30 30 30 30 30 30 34 33	f2052a010000					
00000120	34 31 30 34 39 36 62 35	33 38 65 38 35 33 35 31	4104946b538					
00000130	39 63 37 32 36 61 32 63	39 31 65 36 31 65 63 31	9c726ac91e6					
00000140	31 36 30 30 61 65 31 33	39 30 38 31 33 61 36 32	16000ae1390					
00000150	37 63 36 36 66 62 38 62	65 37 39 34 37 62 65 36	7c66fb8be79					
00000160	33 63 35 32 64 61 37 35	38 39 33 37 39 35 31 35	3c52da73589					
00000170	64 34 65 30 61 36 30 34	66 38 31 34 31 37 38 31	d4e0a646381					
00000180	65 36 32 32 39 34 37 32	31 31 36 36 62 66 36 32	e6224947321					
00000190	31 65 37 33 61 38 32 63	62 66 32 33 34 32 63 38	1e73a823cbf					
000001A0	35 38 65 65 61 63 30 30	30 30 30 30 30 30	58eacc000000					
00000000	30 31 30 30 30 30 30 30	34 38 36 30 65 62 31 38	010000000486					

Scope

Components
orange-bridge-contract

Assumptions

External libraries are safe.

00000010	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	00000000	00 00 00 00 00 00 00 00
00000020	00 00 00 00 3B A3 ED FD	7A 7B 12 B2 7A C7 2C 3E	:Eiÿz{.	00000000
00000030	67 76 8F 61 7F C8 1B C3	88 8A 51 32 3A 9F B8 AA	gv.a.Ê.Ã~SQ	00000000
00000040	4B 1E 5E 4A 29 AB 5F 49	FF FF 00 1D 1D AC 2B 7C	K.^J)«_Iyy.	00000000
00000050	01 01 00 00 00 01 00 00	00 00 00 00 00 00 00 00		00000000
00000060	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00		00000000
00000070	00 00 00 00 00 00 FF FF	FF FF 4D 04 FF FF 00 1D	ÿÿÿÿ	00000000
00000080	01 04 45 54 68 65 20 54	69 6D 65 73 20 30 33 2F	..EThe Tim	00000000
00000090	4A 61 6E 2F 32 30 30 39	20 43 68 61 6E 63 65 6C	Jan/2009 CH	00000000
000000A0	6C 6F 72 20 6F 6E 20 62	72 69 6E 6B 20 6F 66 20	lor on brin	00000000
000000B0	73 65 63 6F 6E 64 20 62	61 69 6C 6F 75 74 20 66	second bail	00000000
000000C0	6F 72 20 62 61 6E 6B 73	FF FF FF FF 01 00 F2 05	or banksÿÿÿÿ	00000000
000000D0	2A 01 00 00 00 43 41 04	67 8A FD B0 FE 55 48 27	*....CA.gŠÿ	00000000
000000E0	19 67 F1 A6 71 30 B7 10	5C D6 A8 28 E0 39 09 A6	.gñ q0·.\Ö"	00000000
000000F0	79 62 E0 EA 1F 61 DE B6	49 F6 BC 3F 4C EF 38 C4	ybaê.ab¶IÖ%	00000000
00000100	F3 55 04 E5 1E C1 12 DE	5C 38 4D F7 BA 0B 8D 57	óU.ã.Á.Þ\8M	00000000
00000110	8A 4C 70 2B 6B F1 1D 5F	AC 00 00 00 00	ŠLp+kñ._~..	00000000
00000000	30 31 30 30 30 30 30 30	36 66 65 32 38 63 30 61	01000000006f	00000000
00000000	Methodology	62 33 37 32 63 31 61 36 61 32 34 36	b6f1b3726c1	00000000
00000020	61 65 36 33 66 37 34 66	39 33 31 65 38 33 36 35	ae63f7f4639	00000000
00000000	Code Audit	35 61 30 38 39 63 36 38 64 36 31 39 30 30	e15a089c638	00000000
00000000	Orange Bridge	Cross chain Bitcoin interoperability	000000009820	00000000
00000050	31 65 34 62 61 37 34 34	62 62 62 65 36 38 30 65	1e4ba7445bb	00000000
00000060	31 66 65 65 31 34 36 37	37 62 61 31 61 33 63 33	1fee1456376	00000000
00000070	35 34 30 62 66 37 62 31	63 64 62 36 30 36 65 38	5400bfb1bcd	00000000
00000080	35 37 32 33 33 65 30 65	36 31 62 63 36 36 34 39	57233e0e6bc	00000000
00000090	66 66 66 66 30 30 31 64	30 31 65 33 36 32 39 39	fff0001d01e	00000000
000000A0	30 31 30 31 30 30 30 30	30 30 30 31 30 30 30 30	01010000000	00000000
000000B0	30 30 30 30 30 30 30 30	30 30 30 30 30 30 30 30	000000000000	00000000
000000C0	30 30 30 30 30 30 30 30	30 30 30 30 30 30 30 30	000000000000	00000000
000000D0	30 30 30 30 30 30 30 30	30 30 30 30 30 30 30 30	000000000000	00000000
000000E0	30 30 30 30 30 30 30 30	30 30 30 30 66 66 66 66	000000000000	00000000
000000F0	66 66 66 66 30 37 30 34	66 66 66 66 30 30 31 64	ffff074ffff0	00000000
00000100	30 31 30 34 66 66 66 66	66 66 66 66 30 31 30 30	0104ffffffffff	00000000
00000110	66 32 30 35 32 61 30 31	30 30 30 30 30 30 34 33	f2052a010000	00000000
00000120	34 31 30 34 39 36 62 35	33 38 65 38 35 33 35 31	4104946b538	00000000
00000130	39 63 37 32 36 61 32 63	39 31 65 36 31 65 63 31	9c726ac91e6	00000000
00000140	31 36 30 30 61 65 31 33	39 30 38 31 33 61 36 32	16000ae1390	00000000
00000150	37 63 36 36 66 62 38 62	65 37 39 34 37 62 65 36	7c66fb8be79	00000000
00000160	33 63 35 32 64 61 37 35	38 39 33 37 39 35 31 35	3c52da73589	00000000
00000170	64 34 65 30 61 36 30 34	66 38 31 34 31 37 38 31	d4e0a646381	00000000
00000180	65 36 32 32 39 34 37 32	31 31 36 36 62 66 36 32	e6224947321	00000000
00000190	31 65 37 33 61 38 32 63	62 66 32 33 34 32 63 38	1e73a823cbf	00000000
000001A0	35 38 65 65 61 63 30 30	30 30 30 30 30 30	58eacc000000	00000000
00000000	30 31 30 30 30 30 30 30	34 38 36 30 65 62 31 38	010000000486	00000000

Methodology

To begin, we reasoned meticulously about the contract's business logic, checking security-critical features to ensure that there were no gaps in the business logic and/or inconsistencies between the aforementioned logic and the implementation. Second, we thoroughly examined the code for known security flaws and attack vectors. Finally, we discussed the most catastrophic situations with the team and reasoned backwards to ensure they are not reachable in any unintentional form.

Taxonomy

In this audit we report our findings using as a guideline Immunefi's vulnerability taxonomy, which can be found at immunefi.com/severity-updated/. The final classification takes into account the severity, according to the previous link, and likelihood of the exploit. The following table summarizes the general expected classification according to severity and likelihood; however, each issue will be evaluated on a case-by-case basis and may not strictly follow it.

Severity / Likelihood	LOW	MEDIUM	HIGH
NONE	None		
LOW	Low		
MEDIUM	Low	Medium	Medium
HIGH	Medium	High	High
CRITICAL	High	Critical	Critical

Orange Bridge

Project Dashboard

Application Summary

Name	Orange Bridge
Commit	cdc8ac673425e19909639fd6c689ab2635d7b8bd
Language	Solidity
Platform	Ethereum

Engagement Summary

Timeline	15-07-2024 to 17-07-2024
Nº of Auditors	1
Review Time	3 days

Vulnerability Summary

Issue Classification	Found	Addressed	Acknowledged
Critical	0	0	0
High	0	0	0
Medium	3	3	0
Low	7	6	0

None	7	6	1
------	---	---	---

Category Breakdown

Suggestion	7
Documentation	0
Bug	5
Optimization	5
Good Code Practices	0

00000010	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	00000000	00 00 00 00 00 00 00 00	00000000	00 00 00 00 00 00 00 00	00000000	00 00 00 00 00 00 00 00
00000020	00 00 00 00 3B A3 ED FD	7A 7B 12 B2 7A C7 2C 3E	00000000	00 00 00 00 00 00 00 00	00000000	00 00 00 00 00 00 00 00	00000000	00 00 00 00 00 00 00 00
00000030	67 76 8F 61 7F C8 1B C3	88 8A 51 32 3A 9F B8 AA	00000000	00 00 00 00 00 00 00 00	00000000	00 00 00 00 00 00 00 00	00000000	00 00 00 00 00 00 00 00
00000040	4B 1E 5E 4A 29 AB 5F 49	FF FF 00 1D 1D AC 2B 7C	00000000	00 00 00 00 00 00 00 00	00000000	00 00 00 00 00 00 00 00	00000000	00 00 00 00 00 00 00 00
00000050	01 01 00 00 00 01 00 00	00 00 00 00 00 00 00 00	00000000	00 00 00 00 00 00 00 00	00000000	00 00 00 00 00 00 00 00	00000000	00 00 00 00 00 00 00 00
00000060	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	00000000	00 00 00 00 00 00 00 00	00000000	00 00 00 00 00 00 00 00	00000000	00 00 00 00 00 00 00 00
00000070	00 00 00 00 00 00 FF FF	FF FF 4D 04 FF FF 00 1D	00000000	00 00 00 00 00 00 00 00	00000000	00 00 00 00 00 00 00 00	00000000	00 00 00 00 00 00 00 00
00000080	01 04 45 54 68 65 20 54	69 6D 65 73 20 30 33 2F	00000000	00 00 00 00 00 00 00 00	00000000	00 00 00 00 00 00 00 00	00000000	00 00 00 00 00 00 00 00
00000090	4A 61 6E 2F 32 30 30 39	20 43 68 61 6E 63 65 6C	00000000	00 00 00 00 00 00 00 00	00000000	00 00 00 00 00 00 00 00	00000000	00 00 00 00 00 00 00 00
000000A0	6C 6F 72 20 6F 6E 20 62	72 69 6E 6B 20 6F 66 20	00000000	00 00 00 00 00 00 00 00	00000000	00 00 00 00 00 00 00 00	00000000	00 00 00 00 00 00 00 00
000000B0	73 65 63 6F 6E 64 20 62	61 69 6C 6F 75 74 20 66	00000000	00 00 00 00 00 00 00 00	00000000	00 00 00 00 00 00 00 00	00000000	00 00 00 00 00 00 00 00
000000C0	6F 72 20 62 61 6E 6B 73	FF FF FF FF 01 00 F2 05	00000000	00 00 00 00 00 00 00 00	00000000	00 00 00 00 00 00 00 00	00000000	00 00 00 00 00 00 00 00
000000D0	2A 01 00 00 00 43 41 04	67 8A FD B0 FE 55 48 27	00000000	00 00 00 00 00 00 00 00	00000000	00 00 00 00 00 00 00 00	00000000	00 00 00 00 00 00 00 00
000000E0	19 67 F1 A6 71 30 B7 10	5C D6 A8 28 E0 39 09 A6	00000000	00 00 00 00 00 00 00 00	00000000	00 00 00 00 00 00 00 00	00000000	00 00 00 00 00 00 00 00
000000F0	79 62 E0 EA 1F 61 DE B6	49 F6 BC 3F 4C EF 38 C4	00000000	00 00 00 00 00 00 00 00	00000000	00 00 00 00 00 00 00 00	00000000	00 00 00 00 00 00 00 00
00000100	F3 55 04 E5 1E C1 12 DE	5C 38 4D F7 BA 0B 8D 57	00000000	00 00 00 00 00 00 00 00	00000000	00 00 00 00 00 00 00 00	00000000	00 00 00 00 00 00 00 00
00000110	8A 4C 70 2B 6B F1 1D 5F	AC 00 00 00 00 00 00 00	00000000	00 00 00 00 00 00 00 00	00000000	00 00 00 00 00 00 00 00	00000000	00 00 00 00 00 00 00 00
00000000	30 31 30 30 30 30 30 30	36 66 65 32 38 63 30 61	00000000	00 00 00 00 00 00 00 00	00000000	00 00 00 00 00 00 00 00	00000000	00 00 00 00 00 00 00 00
00000000	30 31 30 30 30 30 30 30	31 61 36 61 32 34 36	00000000	00 00 00 00 00 00 00 00	00000000	00 00 00 00 00 00 00 00	00000000	00 00 00 00 00 00 00 00
00000020	61 65 36 33 66 37 34 66	39 33 31 65 38 33 36 35	00000000	00 00 00 00 00 00 00 00	00000000	00 00 00 00 00 00 00 00	00000000	00 00 00 00 00 00 00 00
00000000	35 61 30 38 39 63 36 38	64 36 31 39 30 30	00000000	00 00 00 00 00 00 00 00	00000000	00 00 00 00 00 00 00 00	00000000	00 00 00 00 00 00 00 00
00000000	30 30 30 30 30 30 30 30	31 66 64	00000000	00 00 00 00 00 00 00 00	00000000	00 00 00 00 00 00 00 00	00000000	00 00 00 00 00 00 00 00
00000050	31 65 34 62 61 37 34 34	62 62 62 65 36 38 30 65	00000000	00 00 00 00 00 00 00 00	00000000	00 00 00 00 00 00 00 00	00000000	00 00 00 00 00 00 00 00
00000060	31 66 65 65 31 34 36 37	37 62 61 31 61 33 63 33	00000000	00 00 00 00 00 00 00 00	00000000	00 00 00 00 00 00 00 00	00000000	00 00 00 00 00 00 00 00
00000070	35 34 30 62 66 37 62 31	63 64 62 36 30 36 65 38	00000000	00 00 00 00 00 00 00 00	00000000	00 00 00 00 00 00 00 00	00000000	00 00 00 00 00 00 00 00
00000080	35 37 32 33 33 65 30 65	36 31 62 63 36 36 34 39	00000000	00 00 00 00 00 00 00 00	00000000	00 00 00 00 00 00 00 00	00000000	00 00 00 00 00 00 00 00
00000090	66 66 66 66 30 30 31 64	30 31 65 33 36 32 39 39	00000000	00 00 00 00 00 00 00 00	00000000	00 00 00 00 00 00 00 00	00000000	00 00 00 00 00 00 00 00
000000A0	30 31 30 31 30 30 30 30	30 30 30 31 30 30 30 30	00000000	00 00 00 00 00 00 00 00	00000000	00 00 00 00 00 00 00 00	00000000	00 00 00 00 00 00 00 00
000000B0	30 30 30 30 30 30 30 30	30 30 30 30 30 30 30 30	00000000	00 00 00 00 00 00 00 00	00000000	00 00 00 00 00 00 00 00	00000000	00 00 00 00 00 00 00 00
000000C0	30 30 30 30 30 30 30 30	30 30 30 30 30 30 30 30	00000000	00 00 00 00 00 00 00 00	00000000	00 00 00 00 00 00 00 00	00000000	00 00 00 00 00 00 00 00
000000D0	30 30 30 30 30 30 30 30	30 30 30 30 30 30 30 30	00000000	00 00 00 00 00 00 00 00	00000000	00 00 00 00 00 00 00 00	00000000	00 00 00 00 00 00 00 00
000000E0	30 30 30 30 30 30 30 30	30 30 30 30 66 66 66 66	00000000	00 00 00 00 00 00 00 00	00000000	00 00 00 00 00 00 00 00	00000000	00 00 00 00 00 00 00 00
000000F0	66 66 66 66 30 37 30 34	66 66 66 66 30 30 31 64	00000000	00 00 00 00 00 00 00 00	00000000	00 00 00 00 00 00 00 00	00000000	00 00 00 00 00 00 00 00
00000100	30 31 30 34 66 66 66 66	66 66 66 66 30 31 30 30	00000000	00 00 00 00 00 00 00 00	00000000	00 00 00 00 00 00 00 00	00000000	00 00 00 00 00 00 00 00
00000110	66 32 30 35 32 61 30 31	30 30 30 30 30 30 34 33	00000000	00 00 00 00 00 00 00 00	00000000	00 00 00 00 00 00 00 00	00000000	00 00 00 00 00 00 00 00
00000120	34 31 30 34 39 36 62 35	33 38 65 38 35 33 35 31	00000000	00 00 00 00 00 00 00 00	00000000	00 00 00 00 00 00 00 00	00000000	00 00 00 00 00 00 00 00
00000130	39 63 37 32 36 61 32 63	39 31 65 36 31 65 63 31	00000000	00 00 00 00 00 00 00 00	00000000	00 00 00 00 00 00 00 00	00000000	00 00 00 00 00 00 00 00
00000140	31 36 30 30 61 65 31 33	39 30 38 31 33 61 36 32	00000000	00 00 00 00 00 00 00 00	00000000	00 00 00 00 00 00 00 00	00000000	00 00 00 00 00 00 00 00
00000150	37 63 36 36 66 62 38 62	65 37 39 34 37 62 65 36	00000000	00 00 00 00 00 00 00 00	00000000	00 00 00 00 00 00 00 00	00000000	00 00 00 00 00 00 00 00
00000160	33 63 35 32 64 61 37 35	38 39 33 37 39 35 31 35	00000000	00 00 00 00 00 00 00 00	00000000	00 00 00 00 00 00 00 00	00000000	00 00 00 00 00 00 00 00
00000170	64 34 65 30 61 36 30 34	66 38 31 34 31 37 38 31	00000000	00 00 00 00 00 00 00 00	00000000	00 00 00 00 00 00 00 00	00000000	00 00 00 00 00 00 00 00
00000180	65 36 32 32 39 34 37 32	31 31 36 36 62 66 36 32	00000000	00 00 00 00 00 00 00 00	00000000	00 00 00 00 00 00 00 00	00000000	00 00 00 00 00 00 00 00
00000190	31 65 37 33 61 38 32 63	62 66 32 33 34 32 63 38	00000000	00 00 00 00 00 00 00 00	00000000	00 00 00 00 00 00 00 00	00000000	00 00 00 00 00 00 00 00
000001A0	35 38 65 65 61 63 30 30	30 30 30 30 30 30 30	00000000	00 00 00 00 00 00 00 00	00000000	00 00 00 00 00 00 00 00	00000000	00 00 00 00 00 00 00 00
00000000	30 31 30 30 30 30 30 30	34 38 36 30 65 62 31 38	00000000	00 00 00 00 00 00 00 00	00000000	00 00 00 00 00 00 00 00	00000000	00 00 00 00 00 00 00 00

Code Maturity Evaluation

Code Audit

Orange Bridge Cross chain Bitcoin interoperability

Code Maturity Evaluation

Code Maturity Evaluation Guidelines

Category	Evaluation
Access Controls	The use of robust access controls to handle identification and authorization and to ensure safe interactions with the system.
Arithmetic	The proper use of mathematical operations and semantics.
Centralization	The presence of a decentralized governance structure for mitigating insider threats and managing risks posed by contract upgrades
Code Stability	The extent to which the code was altered during the audit.
Upgradeability	The presence of parameterizations of the system that allow modifications after deployment.
Function Composition	The functions are generally small and have clear purposes.
Front-Running	The system's resistance to front-running attacks.
Monitoring	All operations that change the state of the system emit events, making it simple to monitor the state of the system. These events need to be correctly emitted.
Specification	The presence of comprehensive and readable codebase documentation.
Testing and Verification	The presence of robust testing procedures (e.g., unit tests, integration tests, and verification methods) and sufficient test coverage.

Code Maturity Evaluation Results

Category	Evaluation
Access Controls	Satisfactory. The codebase has a strong access control mechanism.
Arithmetic	Satisfactory. The codebase uses Solidity version >0.8.0 implementing safe arithmetic.
Centralization	Weak. The admins/owners of the protocol have significant privileges over the protocol.
Code Stability	Satisfactory. The codebase was stable during the course of the audit.
Upgradeability	Satisfactory. Orange Bridge is upgradeable.
Function Composition	Satisfactory. Functionality is well split into different helpers.
Front-Running	Satisfactory. No front-running issues were identified.
Monitoring	Satisfactory. Most state changes correctly emit events.
Specification	Satisfactory. The code matched the design specifications.
Testing and Verification	Satisfactory. Unit and integration tests were present for most functionality.

00000000	01 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00
00000010	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00
00000020	00 00 00 00 3B A3 ED FD	7A 7B 12 B2 7A C7 2C 3E	:Eiÿz{.				
00000030	67 76 8F 61 7F C8 1B C3	88 8A 51 32 3A 9F B8 AA	gv.a.Ê.Ã~SQ				
00000040	4B 1E 5E 4A 29 AB 5F 49	FF FF 00 1D 1D AC 2B 7C	K.^J)«_Iyy.				
00000050	01 01 00 00 00 01 00 00	00 00 00 00 00 00 00 00					
00000060	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00					
00000070	00 00 00 00 00 00 FF FF	FF FF 4D 04 FF FF 00 1D	ÿÿÿÿ				
00000080	01 04 45 54 68 65 20 54	69 6D 65 73 20 30 33 2F	..EThe Tim				
00000090	4A 61 6E 2F 32 30 30 39	20 43 68 61 6E 63 65 6C	Jan/2009 CH				
000000A0	6C 6F 72 20 6F 6E 20 62	72 69 6E 6B 20 6F 66 20	lor on brin				
000000B0	73 65 63 6F 6E 64 20 62	61 69 6C 6F 75 74 20 66	second bail				
000000C0	6F 72 20 62 61 6E 6B 73	FF FF FF FF 01 00 F2 05	or banksÿÿÿÿ				
000000D0	2A 01 00 00 00 43 41 04	67 8A FD B0 FE 55 48 27	*....CA.gŠÿ				
000000E0	19 67 F1 A6 71 30 B7 10	5C D6 A8 28 E0 39 09 A6	.gñ q0·.\Ö"				
000000F0	79 62 E0 EA 1F 61 DE B6	49 F6 BC 3F 4C EF 38 C4	ybaê.ab¶IÖ%				
00000100	F3 55 04 E5 1E C1 12 DE	5C 38 4D F7 BA 0B 8D 57	óU.ã.Á.Þ\8M				
00000110	8A 4C 70 2B 6B F1 1D 5F	AC 00 00 00 00	ŠLp+kñ._~..				
00000000	30 31 30 30 30 30 30 30	36 66 65 32 38 63 30 61	01000000006f				
00000001	66 31 62 33 37 32	63 31 61 36 61 32 34 36	b6f1b3726c1				
00000002	61 65 36 33 66 37 34 66	39 33 31 65 38 33 36 35	ae63f7f4639				
00000003	35 61 30 38 39 63	36 38 64 36 31 39 30 30	e15a089c638				
00000004	30 30 30 30 30 30 30 30	30 30 30 30 30 30 30 30	000000009820				
00000005	31 65 34 62 61 37 34 34	62 62 62 65 36 38 30 65	1e4ba7445bb				
00000006	31 66 65 65 31 34 36 37	37 62 61 31 61 33 63 33	1fee1456376				
00000007	35 34 30 62 66 37 62 31	63 64 62 36 30 36 65 38	5400bfb1bcd				
00000008	35 37 32 33 33 65 30 65	36 31 62 63 36 36 34 39	57233e0e6bc				
00000009	66 66 66 66 30 30 31 64	30 31 65 33 36 32 39 39	fff0001d01e				
0000000A	30 31 30 31 30 30 30 30	30 30 30 31 30 30 30 30	01010000000				
0000000B	30 30 30 30 30 30 30 30	30 30 30 30 30 30 30 30	000000000000				
0000000C	30 30 30 30 30 30 30 30	30 30 30 30 30 30 30 30	000000000000				
0000000D	30 30 30 30 30 30 30 30	30 30 30 30 30 30 30 30	000000000000				
0000000E	30 30 30 30 30 30 30 30	30 30 30 30 66 66 66 66	000000000000				
0000000F	66 66 66 66 30 37 30 34	66 66 66 66 30 30 31 64	ffff074ffff0				
00000100	30 31 30 34 66 66 66 66	66 66 66 66 30 31 30 30	0104ffffffff				
00000110	66 32 30 35 32 61 30 31	30 30 30 30 30 30 34 33	f2052a01000				
00000120	34 31 30 34 39 36 62 35	33 38 65 38 35 33 35 31	4104946b538				
00000130	39 63 37 32 36 61 32 63	39 31 65 36 31 65 63 31	9c726ac91e6				
00000140	31 36 30 30 61 65 31 33	39 30 38 31 33 61 36 32	16000ae1390				
00000150	37 63 36 36 66 62 38 62	65 37 39 34 37 62 65 36	7c66fb8be79				
00000160	33 63 35 32 64 61 37 35	38 39 33 37 39 35 31 35	3c52da73589				
00000170	64 34 65 30 61 36 30 34	66 38 31 34 31 37 38 31	d4e0a646381				
00000180	65 36 32 32 39 34 37 32	31 31 36 36 62 66 36 32	e6224947321				
00000190	31 65 37 33 61 38 32 63	62 66 32 33 34 32 63 38	1e73a823cbf				
000001A0	35 38 65 65 61 63 30 30	30 30 30 30 30 30	58eacc000000				
00000000	30 31 30 30 30 30 30 30	34 38 36 30 65 62 31 38	010000000486				

Findings

3S-OB-M01

Balance check in **Vault::withdraw()** does not take fees into account

Id	3S-OB-M01
Classification	Medium
Severity	High
Likelihood	Low
Category	Bug
Status	Addressed in #cdd25c9 .

Description

Vault::withdraw() transfers funds to an user if **address(this)).balance >= amount**, which may transfer funds resulting from fees.

Recommendation

Replace the check by **address(this)).balance - totalFees >= amount** to make sure fees can always be withdrawn.

3S-OB-M02

address.transfer is used in the codebase, which could lead to stuck funds

Id	3S-OB-M02
Classification	Medium
Severity	High
Likelihood	Low
Category	Bug
Status	Addressed in #252ae5e .

Description

Using **address.transfer** is not recommended as future gas cost changes can make it no longer work or users might use smart contract wallets. The reason is that it only forwards **2300** gas, which can lead to the 2 problems mentioned before.

Recommendation

Use **address.call{value: amount}("")** instead, [here](#) is an example implementation. If the gas usage of the target is a concern, [this](#) implementation can be used instead, setting the **_gas** to some amount that may be changed and **_maxCopy** and **_calldata** to 0.

3S-OB-M03

Equality check should be performed for fees, not $\geq$ as it can lead to users sending more fees than supposed

Id	3S-OB-M03
Classification	Medium
Severity	High
Likelihood	Low
Category	Bug
Status	Addressed in #2f47c6c .

Description

In **BRC20Factory::burn()**, **Vault::deposit()**, it is required that the fee is equal to or exceeds the **msg.value**. However, this could lead to loss of fees, as the fee can be lowered without users noticing (or frontrunning them), and users would lose this part of the fee. In the case of the **Vault**, these funds would be left untracked because the fees are tracked in **totalFees**, so the owner would not be able to withdraw these extra funds.

Recommendation

Replace the $\geq$ checks for $=$. The equality check should be performed for fees, not $\geq$ as it can lead to users sending more fees than supposed

3S-OB-L01

Ownership in **BRC20Factory** could be transferred using a 2 step procedure, similarly to **Vault**

Id	3S-OB-L01
Classification	Low
Severity	Low
Likelihood	Low
Category	Suggestion
Status	Addressed in #ee04c91 .

Description

It's recommended to change **owner** using a 2 step procedure to mitigate the risk of the contract losing ownership due to incorrect address.

Recommendation

Implement the 2 step ownership transfer procedure with a **pendingOwner** variable and **acceptOwnership()** function. [Here](#) is an example implementation.

3S-OB-L02

Token addresses are not validated in **BRC20Factory** and **Vault**, so users can use incorrect tokens

Id	3S-OB-L02
Classification	Low
Severity	Low
Likelihood	Low
Category	Bug
Status	Addressed in #1cd9410 .

Description

BRC20Factory::mint(), **BRC20Factory::burn()**, **Vault::deposit()** and **Vault::withdraw()** allow sending any token, which could lead to problems if the token is not a **BRC20**.

Recommendation

Validate the sent token was created by the factory. To do this an **isBRC20** mapping should be added to **BRC20Factory** which stores all the tokens that were created by it.

3S-OB-L03

BRC20Factory::burn() could validate the receiver length

Id	3S-OB-L03
Classification	Low
Severity	Low
Likelihood	Low
Category	Suggestion
Status	Addressed in #d5f3226 .

Description

BRC20Factory::burn() does not validate the **receiver**, which could lead to wasted funds. It's impossible to do a fail safe verification, but at least the length could be checked.

Recommendation

Revert if the length of the **receiver** is null.

3S-OB-L04

BRC20Factory::addSigner() and **Vault::addSigner()** must not allow adding the zero address as a signer

Id	3S-OB-L04
Classification	Low
Severity	Low
Likelihood	Low
Category	Suggestion
Status	Addressed in #4082cc6 .

Description

The signature verification in **BRC20Factory** and **Vault** does not check that the recovered address is not null, which means that if **address(0)** is added as a signer, it would be possible to forge signatures.

Recommendation

In **BRC20Factory::addSigner()** and **Vault::addSigner()**, revert if an **address(0)** account is sent as argument.

3S-OB-L05

Fee event is missing in the constructors of **BRC20Factory** and **Vault**

Id	3S-OB-L05
Classification	Low
Severity	Low
Likelihood	High
Category	Suggestion
Status	Addressed in #edbf47e .

Description

The fee is set in the constructors of **BRC20Factory** and **Vault**, but the event is not emitted.

Recommendation

Emit the **FeeChanged** event in the constructor of both contracts.

3S-OB-L06

BRC20Factory constructor is missing a duplicate check

Id	3S-OB-L06
Classification	Low
Severity	Low
Likelihood	Low
Category	Suggestion
Status	Addressed in #ea46e07 .

Description

BRC20Factory constructor does not check for duplicate signers, which would lead to problems as the index would be overridden.

Recommendation

Check for duplicate signers using the recommendation from [#4](#).

3S-OB-L07

Domain separator calculation is not fork safe

Id	3S-OB-L07
Classification	Low
Severity	Medium
Likelihood	Low
Category	Bug
Status	Addressed in #143cee8 .

Description

The domain separator is cached in the constructor of the contracts, which could lead to signature signing softwares in case of a hard fork. When a hard fork happens, **block.chainid** changes, which affects the domain separator, but as it is only computed in the constructor, it will be forever incorrect. Messages can still be signed but EIP712 will be broken.

Recommendation

The **EIP712 contract** from OpenZeppelin handles this by caching the original domain separator and recomputing it if **block.chainid** has changed.

3S-OB-N01

Checks effects interactions pattern is now always followed

Id	3S-OB-N01
Classification	None
Category	Suggestion
Status	Addressed in #2f47c6c .

Description

State changes should always be performed before interacting with an external contract, or it increases the risk of reentrancy attacks.

Recommendation

In `Vault::withdraw()` decrease `allowances[token]` before sending the funds.

In `Vault::withdrawFees()` set `totalFees` to `0` before transferring the funds.

3S-OB-N02

BRC20Factory and **Vault** do different checks when removing signers

Id	3S-OB-N02
Classification	None
Category	Suggestion
Status	Acknowledged

Description

BRC20Factory checks if the **account** is authorized and if its index stored in **indexes[account]** is smaller than the length of **signers**. **Vault** requires that the length of signers is bigger than 1 and the **account** is authorized.

Recommendation

The check that the index of the account is smaller than the length of **signers** is not required and can be removed. Also, decide if it makes sense to check if the length of the signers is bigger than 1 in the **BRC20Factory** or if this check is not required in both contracts.

3S-OB-N03

Storage variables can be cached to save gas

Id	3S-OB-N03
Classification	None
Category	Optimization
Status	Addressed in #68ce26f .

Description

Reading/writing from the same storage variable more than once should be avoided to save gas.

Recommendation

BRC20Factory::burn() can cache the [fee](#) (read twice).

Vault::deposit() cache the [fee](#) (read thrice).

Vault::acceptAdmin() can cache the [pendingAdmin](#) (read 4 times).

Vault::withdraw() can cache [signers.length](#) (read number of signers times).

3S-OB-N04

BRC20 parameters should be passed as arguments to the constructor of **BRC20** to save gas

Id	3S-OB-N04
Classification	None
Category	Optimization
Status	Addressed in #1fd3288 .

Description

BRC20Factory::createBRC20() creates new **BRC20** tokens by setting the **parameters** storage variable to the **name**, **symbol** and **decimals** of the new token, and then the **BRC20** token in the constructor fetching this storage variable.

Recommendation

Send the **name**, **symbol** and **decimals** in the constructor to save gas, as **create2** will work just as fine, but it becomes significantly cheaper to deploy the tokens.

3S-OB-N05

Signer duplicate check can be performed by requiring signers being sent ordered

Id	3S-OB-N05
Classification	None
Category	Optimization
Status	Addressed in #b03ca97 .

Description

Signers are checked for duplicates by creating a memory signers array and looping through this array for every new signer, which is inefficient.

Recommendation

Cache the last signer and assert that the current signer is bigger than the last, **require(signer > prevSigner, "duplicate")**. This is how Gnosis Safe does it, for example.

3S-OB-N06

authorized mapping is not required if the **indexes** mapping stores the **indexes + 1**

Id	3S-OB-N06
Classification	None
Category	Optimization
Status	Addressed in #dcd6efe .

Description

BRC20Factory and **Vault** store the **signers** array, the **authorized** and **indexes** mapping. The **authorized** mapping can be removed if the **indexes** mapping stores **index + 1** instead, so the check for existing signers can be made as **indexes[signer] != 0**.

Recommendation

Delete the **authorized** mapping, store the index as **index + 1** in the **indexes** mapping and check if the signer exists by doing **indexes[signer] != 0**.

3S-OB-N07

Reentrancy guard can be implemented with a **uint256** to save gas

Id	3S-OB-N07
Classification	None
Category	Optimization
Status	Addressed in #1cbaf62 .

Description

Storing a **uint256** instead of a bool saves gas as it is cheaper changing storage from non null to non null value.

Recommendation

Implement the guard with a **uint256**. [Here](#) is an example implementation from OpenZeppelin.