

	01	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
00000010																	
00000020																	
00000030																	
00000040																	
00000050																	
00000060																	
00000070																	
00000080																	
00000000																	
000000A0																	
000000B0																	
00000000																	
000000D0																	
000000E0																	
000000F0																	
00000100																	
00000110																	
00000000																	
oooo Dis	_	_															
00000020	6.1	6.5	36														
000000 Coo	le Au	ıdit															
0000 M^C	<b>)</b> Cod	ordi	nati	on l	laye	r fo	r pe	rmis	ssion	ed i	insti	tutio	onal	act	ors	to g	enerate \$M 🛛
00000050																65	
00000060																	
00000070																	5400bfb1bcd
00000080															34		
00000090							31	64		31							fff0001d01e
000000A0		31		31								31					01010000000
000000B0																	
00000000																	
00000000								30					30				
00000E0										30			66		66	66	$\bigcirc$
																	55550715550
00000F0	66		66	66		37	30	34	66	66	66	66	30	30	31	64	ffff074fff0
000000F0 00000100	66 30	66 31	66 30	66 34	30 66	37 66	30 66	34 66	66 66	66 66	66 66	66 66	3 0 3 0	30 31	31 30	64 30	0104fffffff
00000100		31		34	66	66		66	66	66	66	66		31		30	0104ffffff
00000100 00000110	3 <b>0</b> 6 6	31 32	3 O 3 O	34 35	66 32	66 61	66 30	66 31	66 30	66 30	66 30	66 30	3 0 3 0	31 30	30 34	3 <del>0</del>	0104fffffff f2052a01000
00000100 00000110 00000120	30 66 34	31 32 31	3 0 3 0 3 0	34 35 34	66 32 39	66 61 36	66 30 62	66 31 35	66 30 33	66 30 38	66 30 65	66 30 38	30 30 35	31 30 33	30 34 35	30 33 31	0104fffffff f2052a01000 4104946b538
00000100 00000110 00000120 00000130	30 66 34 39	<ul><li>31</li><li>32</li><li>31</li><li>63</li></ul>	30 30 30 37	34 35 34 32	66 32 39 36	66 61 36 61	66 30 62 32	<ul><li>66</li><li>31</li><li>35</li><li>63</li></ul>	66 30 33 39	66 30 38 31	66 30 65 65	66 30 38 36	30 30 35 31	31 30 33 65	30 34 35 63	30 33 31 31	0104fffffff f2052a01000 4104946b538 9c726ac91e6
00000100 00000110 00000120 00000130 00000140	30 66 34 39 31	31 32 31 63 36	30 30 30 37 30	34 35 34 32 30	66 32 39 36 61	66 61 36 61 65	66 30 62 32 31	<ul><li>66</li><li>31</li><li>35</li><li>63</li><li>33</li></ul>	66 30 33 39	66 30 38 31 30	66 30 65 65 38	66 30 38 36 31	30 30 35 31 33	31 30 33 65 61	30 34 35 63 36	30 33 31 31 32	0104fffffff f2052a01000 4104946b538 9c726ac91e6 16000ae1390
00000100 00000110 00000120 00000130 00000140 00000150	30 66 34 39 31 37	31 32 31 63 36 63	30 30 30 37 30 36	34 35 34 32 30 36	66 32 39 36 61 66	66 61 36 61 65 62	66 30 62 32 31 38	66 31 35 63 33 62	66 30 33 39 39 65	66 30 38 31 30 37	66 30 65 65 38 39	66 30 38 36 31 34	30 30 35 31 33	31 30 33 65 61 62	30 34 35 63 36 65	30 33 31 31 32 36	0104fffffff f2052a01000 4104946b538 9c726ac91e6 16000ae1390 7c66fb8be79
00000100 00000110 00000120 00000130 00000140 00000150 00000160	30 66 34 39 31 37 33	31 32 31 63 36 63 63	30 30 30 37 30 36 35	34 35 34 32 30 36 32	66 32 39 36 61 66 64	66 61 36 61 65 62 61	66 30 62 32 31 38 37	66 31 35 63 33 62 35	66 30 33 39 39 65 38	66 30 38 31 30 37 39	66 30 65 65 38 39 33	66 30 38 36 31 34 37	30 30 35 31 33 37 39	31 30 33 65 61 62 35	30 34 35 63 36 65 31	30 33 31 31 32 36 35	0104fffffff f2052a01000 4104946b538 9c726ac91e6 16000ae1390 7c66fb8be79 3c52da73589
00000100 00000110 00000120 00000130 00000140 00000150 00000160 00000170	30 66 34 39 31 37 33 64	31 32 31 63 36 63 63 34	30 30 30 37 30 36 35 65	34 35 34 32 30 36 32 30	66 32 39 36 61 66 64 61	66 61 36 61 65 62 61 36	66 30 62 32 31 38 37 30	66 31 35 63 33 62 35 34	66 30 33 39 39 65 38 66	66 30 38 31 30 37 39 38	66 30 65 65 38 39 33 31	66 30 38 36 31 34 37 34	30 30 35 31 33 37 39 31	31 30 33 65 61 62 35 37	30 34 35 63 36 65 31 38	30 33 31 31 32 36 35 31	0104fffffff f2052a01000 4104946b538 9c726ac91e6 16000ae1390 7c66fb8be79 3c52da73589 d4e0a646381
00000100 00000110 00000120 00000130 00000140 00000150 00000160 00000170 00000180	30 66 34 39 31 37 33 64 65	31 32 31 63 36 63 63 34 36	30 30 30 37 30 36 35 65 32	34 35 34 32 30 36 32 30 32	66 32 39 36 61 66 64 61 39	66 61 36 61 65 62 61 36 34	66 30 62 31 38 37 30 37	66 31 35 63 33 62 35 34 32	66 30 33 39 39 65 38 66 31	66 30 38 31 30 37 39 38 31	66 30 65 65 38 39 33 31 36	66 30 38 36 31 34 37 34 36	30 30 35 31 33 37 39 31 62	31 30 33 65 61 62 35 37 66	30 34 35 63 36 65 31 38 36	30 33 31 31 32 36 35 31 32	0104fffffff f2052a01000 4104946b538 9c726ac91e6 16000ae1390 7c66fb8be79 3c52da73589 d4e0a646381 e6224947321

### **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.

	01	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
00000010																	
00000020																	
00000030																	
00000040																	
00000050																	
000000000																	
000000000																	
00000070																	
000000000																	
000000A0																	
000000B0																	
00000000																	
000000D0																	
000000E0																	
000000F0																	
00000100																	
00000110																	
00000000		_	_		30												
00000 Ta	ble	Ot															
Coc	te Ai	dit															
00000030	200	31	35	61	30	38 r fa.	39	63	36	38	64	36	31	39	30	30	e15a089c638
M''C						1301	pe	et Biblis								10 ge	enerate \$M 820
00000050																	
00000060																	
0000070																	5400bfb1bcd
00000080															34		
00000090							31	64		31							fff0001d01e
000000A0		31		31													
000000B0																	01010000000
00000000																	
00000000																	
000000D0																	
$\bigcirc$								3 0 3 0 3 0					30 30 30				
00000000 00000E0								30 30 30 30		30 30 30 30			30 30 30 66		30 30 30 66	30 30 30 66	
00000000 000000E0 00000F0	30 30 66		30 30 30 66	30 30 30 66		30 30 30 30 30	30 30 30 30 30	30 30 30 30 30	30 30 30 30 66	30 30 30 30 66	30 30 30 30 66	30 30 30 30 66	30 30 30 66 30	30 30 30 66 30	30 30 30 66 31	30 30 30 66 64	00000000000000000000000000000000000000
00000000 000000E0 000000F0 00000100	3 0 3 0 6 6 3 0	30 30 66 31	30 30 30 66 30	30 30 30 66 34	30 30 30 30 30 30	30 30 30 30 37 66	30 30 30 30 30 30	30 30 30 30 34 66	30 30 30 30 66 66	30 30 30 30 66 66	30 30 30 30 66 66	30 30 30 30 66 66	30 30 30 66 30	30 30 30 66 30 31	30 30 30 66 31 30	30 30 30 66 64 30	00000000000000000000000000000000000000
000000D0 00000E0 00000F0 0000110	30 30 66 30 66	30 30 66 31 32	30 30 30 66 30	30 30 30 66 34 35	30 30 30 30 30 30 66 32	30 30 30 30 37 66 61	30 30 30 30 30 30 66	30 30 30 30 34 66 31	30 30 30 30 66 66 30	30 30 30 30 66 66 30	30 30 30 30 66 66 30	30 30 30 30 66 66 30	30 30 30 66 30 30	30 30 30 66 30 31 30	30 30 30 66 31 30 34	30 30 30 66 64 30 33	00000000000000000000000000000000000000
000000D0 00000E0 00000F0 00000100 00000110 00000120	30 30 66 30 66 34	30 30 66 31 32 31	30 30 30 66 30 30	30 30 30 66 34 35 34	30 30 30 30 30 30 66 32 39	30 30 30 30 37 66 61 36	30 30 30 30 30 30 66 30 62	30 30 30 30 34 66 31 35	30 30 30 30 66 66 30 33	30 30 30 30 66 66 30 38	30 30 30 30 66 66 30 65	30 30 30 30 66 66 30 38	30 30 30 66 30 30 30 35	30 30 30 66 30 31 30 33	30 30 30 66 31 30 34 35	30 30 30 66 64 30 33 31	00000000000000000000000000000000000000
000000D0 00000E0 00000F0 00000100 00000110 00000120 00000130	30 30 66 30 66 34 39	30 30 66 31 32 31 63	30 30 30 66 30 30 30 37	30 30 30 66 34 35 34 32	30 30 30 30 30 66 32 39 36	30 30 30 30 37 66 61 36	30 30 30 30 30 66 30 62 32	30 30 30 30 34 66 31 35 63	30 30 30 30 66 66 30 33	30 30 30 30 66 66 30 38 31	30 30 30 30 66 66 30 65 65	30 30 30 30 66 66 30 38 36	30 30 30 66 30 30 30 35 31	30 30 30 66 30 31 30 33 65	30 30 30 66 31 30 34 35 63	30 30 30 66 64 30 33 31	00000000000000000000000000000000000000
000000D0 00000E0 00000F0 00000100 00000110 00000120 00000130 00000140	30 30 66 30 66 34 39 31	30 30 66 31 32 31 63 36	30 30 30 66 30 30 30 37 30	30 30 30 66 34 35 34 32 30	30 30 30 30 30 66 32 39 36 61	30 30 30 30 37 66 61 36 61 65	30 30 30 30 30 66 30 62 32 31	30 30 30 34 66 31 35 63 33	30 30 30 66 66 30 33 39	30 30 30 30 66 66 30 38 31 30	30 30 30 30 66 66 30 65 65 38	30 30 30 30 66 66 30 38 36 31	30 30 30 66 30 30 35 31 33	30 30 30 66 30 31 30 33 65 61	30 30 30 66 31 30 34 35 63 36	30 30 30 66 64 30 33 31 31	00000000000000000000000000000000000000
000000D0 00000E0 00000F0 00000100 00000120 00000130 00000140 00000150	30 30 66 30 66 34 39 31 37	30 30 66 31 32 31 63 36 63	30 30 30 66 30 30 30 37 30 36	30 30 30 66 34 35 34 32 30 36	30 30 30 30 30 66 32 39 36 61 66	30 30 30 37 66 61 36 61 65 62	30 30 30 30 30 66 30 62 31 38	30 30 30 34 66 31 35 63 33 62	30 30 30 30 66 66 30 33 39 65	30 30 30 30 66 66 30 38 31 30 37	30 30 30 30 66 66 30 65 65 38 39	30 30 30 30 66 66 30 38 36 31 34	30 30 30 66 30 30 35 31 33 37	30 30 30 66 30 31 30 33 65 61 62	30 30 30 66 31 30 34 35 63 36	30 30 30 66 64 30 33 31 31 32 36	00000000000000000000000000000000000000
000000D0 00000E0 00000F0 00000100 00000120 00000130 00000140 00000150 00000160	30 30 66 30 66 34 39 31 37	30 30 66 31 32 31 63 36 63 34	30 30 30 66 30 30 30 37 30 36 35	30 30 30 66 34 35 34 32 30 36 32	30 30 30 30 30 66 32 39 36 61 66 64	30 30 30 37 66 61 36 61 65 62 61	30 30 30 30 30 66 30 62 31 38 37	30 30 30 34 66 31 35 63 33 62 35	30 30 30 30 66 66 30 33 39 65 38	30 30 30 30 66 66 30 38 31 30 37 39	30 30 30 30 66 66 30 65 65 38 39 33	30 30 30 30 66 66 30 38 36 31 34 37	30 30 30 66 30 30 35 31 33 37	30 30 30 66 30 31 30 33 65 61 62 35	30 30 30 66 31 30 34 35 63 36 65 31	30 30 30 66 64 30 33 31 31 32 36 35	00000000000000000000000000000000000000
000000D0 00000E0 00000F0 00000100 00000120 00000130 00000140 00000150 00000160 00000170	30 30 66 30 66 34 39 31 37 33 64	30 30 66 31 32 31 63 36 63 34	30 30 30 66 30 30 37 30 36 35 65	30 30 30 66 34 35 34 32 30 36 32 30	30 30 30 30 30 66 32 39 36 61 66 64 61	30 30 30 37 66 61 36 61 65 62 61 36	30 30 30 30 30 66 30 62 31 38 37 30	30 30 30 34 66 31 35 63 33 62 35 34	30 30 30 66 66 30 33 39 65 38 66	30 30 30 30 66 66 30 38 31 30 37 39 38	30 30 30 30 66 66 30 65 65 38 39 33 31	30 30 30 30 66 66 30 38 36 31 34 37 34	30 30 30 66 30 30 35 31 33 37 39 31	30 30 30 66 30 31 30 33 65 61 62 35 37	30 30 30 66 31 30 34 35 63 36 65 31 38	30 30 30 66 64 30 33 31 32 36 35 31	00000000000000000000000000000000000000
00000000 0000000000000000000000000000	30 30 66 30 66 34 39 31 37 33 64 65	30 30 66 31 32 31 63 36 63 34 36	30 30 30 66 30 30 37 30 36 35 65 32	30 30 30 66 34 35 34 32 30 36 32 30 32	30 30 30 30 30 66 32 39 36 61 66 64 61 39	30 30 30 37 66 61 36 61 65 62 61 36 34	30 30 30 30 30 66 30 62 31 38 37 30 37	30 30 30 34 66 31 35 63 33 62 35 34 32	30 30 30 30 66 66 30 33 39 65 38 66 31	30 30 30 30 66 66 30 38 31 30 37 39 38 31	30 30 30 30 66 66 30 65 65 38 39 33 31 36	30 30 30 30 66 66 30 38 36 31 34 37 34 36	30 30 30 66 30 30 35 31 33 37 39 31 62	30 30 30 66 30 31 30 33 65 61 62 35 37	30 30 30 66 31 30 34 35 63 36 65 31 38 36	30 30 30 66 64 30 33 31 32 36 35 31 32	00000000000000000000000000000000000000

### Table of Contents

Disclaimer	3
Summary	7
Scope	9
Methodology	11
Project Dashboard	13
Code Maturity Evaluation	16
Findings	19
3S-M^0-L01	19
3S-M^0-L02	20
3S-M^0-N01	21
3S-M^0-N02	22

00000000	01	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
00000010																	
99999929																	
00000030																	
00000040																	
00000050																	
00000060																	
00000070																	
00000080																	
00000090																	
000000A0																	
000000B0																	
00000000																	
00000000																	
000000E0																	
000000F0																	
00000100																	
00000110																	
0000000																	
00000 <b>Su</b>	61	65	<b>y</b> 36														
00000 Coc																	
00000050	31	65	34	62	aye	37	34	34	62 62	62 i	62	65	36	38	30	65	enerate \$M 820 1e4ba7445bb
00000060																	
00000070																	5400bfb1bcd
00000080															34		
00000090							31	64		31							fff0001d01e
000000A0		31		31								31					01010000000
000000B0																	
00000000																	
00000000								30					30				
000000E0										30			66			66	$\bigcirc$
000000F0	66		66	66		37	30	34	66	66	66	66	30	30	31	64	ffff074fff0
00000100		31		34	66	66		66	66	66	66	66		31		30	0104ffffff
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
	35	38	65	65	61	63	30	30	30	30	30	30	30	30			58eacc00000
000001A0									_					-			

# Summary

Three Sigma audited M<sup>0</sup> in a 3 day engagement. The audit was conducted from 17-07-2024 to 19-07-2024.

### **Protocol Description**

A neutral value transmission framework able to permissionlessly mint currencies under decentralized governance. The purpose of \$M is to become a superior building block for value representation, by combining the convenience of digital money with the risk profile of physical cash.

00000000	01	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
00000010																	
00000020																	
00000030																	
00000040																	
00000050																	
00000060																	
00000070																	
00000080																	
00000090																	
000000A0																	
000000B0																	
00000000																	
000000D0																	
00000E0																	
000000F0																	
00000100																	
00000110																	
0000000																	
99999 Sc																	
00000020	61	65															
00000 Coc																	
00000050	31	65	34	62	61	37	34	34	62	62	62	65	36	38	30	65	generate \$M 820 1e4ba7445bb
00000060																	
00000070																	5400bfb1bcd
00000080															34		
00000090							31	64		31							fff0001d01e
000000A0		31		31								31					01010000000
000000B0																	
00000000																	
00000000								30					30				
00000E0										30			66		66	66	$\bigcirc$
00000F0	66		66	66		37	30	34	66	66	66	66	30	30	31	64	ffff074fff0
00000100		31		34	66	66		66	66	66	66	66		31		30	0104ffffff
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			58eacc00000
00000000	30	31	30	30	30	30	30	30	34	38	36	30	65	62	31	38	01000000486

# Scope

Filepath	nSLOC
src/libs/IndexingMath.sol	46
src/Migratable.sol	20
src/Proxy.sol	31
src/WrappedMToken.sol	239
Total	336

000000000	01	00	00	00	00	00	00	(0) (0)	00	00	00	(0) (0)	00	00	00	00	
00000010																	
00000020																	
00000030																	
00000040																	
00000050																	
000000000																	
00000070																	
000000070																	
000000000																	
000000A0																	
000000B0																	
00000000																	
000000D0																	
000000E0																	
000000F0																	
00000100																	
00000110																	
	30																
0000 M∈	etho	ode	OIC	gy	62												
00000M^C	<b>)</b> Cod	ordi	nati	on I	laye	r fo	r pe	rmi	ssion	ed i	insti	tutio	onal	act	tors	to ge	enerate \$M <sup>820</sup> 1e4ba7445bb
00000060																	
0000070																	5400bfb1bcd
00000080																	
00000090							31	64									fff0001d01e
000000A0		31										31					01010000000
000000B0																	
00000000																	
00000000								30					30				
00000E0										30			66		66	66	$\bigcirc$
00000F0	66		66	66		37	30	34	66	66	66	66	30	30	31	64	ffff074fff0
00000100		31		34	66	66		66	66	66	66	66		31		30	0104fffffff
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			58eacc00000
			30	20	30	30	30	30	2.4	38	20	30	СЕ	60	2.1	~ ~	01000000486

## 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 <a href="immunefi.com/severity-updated/">immunefi.com/severity-updated/</a>. 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	LOW MEDIUM H							
NONE		None							
LOW		Low							
MEDIUM	Low	Medium	Medium						
HIGH	Medium	High	High						
CRITICAL	High	Critical	Critical						

08000080	00000000	0.1	00	00	00	00	00	00	00	0.0	00	0.0	00	00	00	00	66	
98889838																		
988689848																		
98989848																		
98989868 91 91 91 90 98 98 91 98 98 98 98 98 98 98 98 98 98 98 98 98																		
989898689																		
989090979 98 98 98 98 98 98 98 98 98 98 98 98 98																		
98989888																		
99999999																		
000000000																		
00000000																		
00000000																		
00000000																		
0000000E0																		
00000000																		
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 00 00 00 01 01 01 0000000 000000																		
00000110 8A 4C 70 2B 6B F1 1D 5F AC 00 00 00 00 00 00 00 01 01 01 0000000 000000																		
00000000																		
000000																		
000000 Code Audit 35 61 30 38 39 63 36 64 36 31 39 30 30 e15a089c6 000000 M^O Coordination layer for permissioned institutional actors to generate \$M8 00000050 31 65 34 62 61 37 34 34 62 62 62 65 36 38 30 65 1e4ba7445 00000000 31 66 65 65 31 34 36 37 37 62 61 31 61 33 63 33 1fee14563 00000000 35 34 30 62 66 37 62 31 63 64 62 36 30 36 65 38 5400bfb1k 00000000 35 37 32 33 33 65 30 65 36 31 62 63 36 36 34 39 57233e0e6 00000000 66 66 66 66 63 0 30 31 64 30 31 65 33 36 32 39 39 fff0001d6 00000000 30 31 30 31 30 30 30 30 30 30 30 30 30 30 30 30 30	00000 <b>P</b> ro	siec	<b>`</b> ‡6I	Da	gh	ho	ar	ďž.										
000000 Code Audit 35 61 30 38 39 63 36 38 64 36 31 39 30 30 e15a08966 000000 M^O Coordination layer for permissioned institutional actors to generate \$M8 00000050 31 65 34 62 61 37 34 34 62 62 62 65 36 38 30 65 1e4ba7445 00000060 31 66 65 65 31 34 36 37 37 62 61 31 61 33 63 33 1fee14563 00000070 35 34 30 62 66 37 62 31 63 64 62 36 30 36 65 38 5400bfb18 00000080 35 37 32 33 33 65 30 65 36 31 62 63 36 36 36 34 39 57233e0e6 00000000 66 66 66 66 66 30 30 30 31 64 30 31 65 33 36 32 39 39 fff000100 00000000 30 31 30 31 30 31 30 30 30 30 30 30 30 30 30 30 30 30 30	0000004010	7 <b>76</b> 0	65	36	33 314	66	37	34										
000000 M^O Coordination layer for permissioned institutional actors for generate \$M8 00000050 31 65 34 62 61 37 34 34 62 62 62 65 36 36 38 30 65 1e4ba 7445 600000060 31 66 65 65 31 34 36 37 37 62 61 31 61 33 63 33 1fee14563 00000070 35 34 30 62 66 37 62 31 63 64 62 36 30 36 65 38 5400bfbl 00000080 35 37 32 33 33 65 30 65 36 31 62 63 36 36 34 39 57233e0e6 00000090 66 66 66 66 30 30 31 64 30 31 65 33 36 32 39 39 fff0001d6 000000000 30 31 30 31 30 30 30 30 30 30 30 30 30 30 30 30 30																		
000000060																		
000000060			orai	nan	on i	iaye	1-101	r pe	ererni:	ssion	ea	ınsıı	TUH	onai	acı	ors	to ge	enerate pivi
000000070																		
00000080																		
000000000																		
0000000A0 30 31 30 31 30 30 30 30 30 30 30 30 30 30 30 30 30																		
0000000B0       30			~ ~															
0000000C0       30																		
0000000D0       31       64       fffff074ff       60       60       66       66       66       66       66       66       66       66       66       66       66       66       66       30       31       30       30       90       90       90       90       90       30       31       30       30       30       30       30       30       30       30       30       30       30       30       30       30       30       30       30       30																		
000000E0 30 30 30 30 30 30 30 30 30 30 30 30 30																		
000000F0 66 66 66 66 30 37 30 34 66 66 66 66 66 30 30 31 64 ffff074ff 00000100 30 31 30 34 66 66 66 66 66 66 66 66 66 66 30 31 30 30 0104fffff 00000110 66 32 30 35 32 61 30 31 30 30 30 30 30 30 34 33 f2052a016 00000120 34 31 30 34 39 36 62 35 33 38 65 38 35 33 35 31 4104946b5 00000130 39 63 37 32 36 61 32 63 39 31 65 36 31 65 63 31 9c726ac91 00000140 31 36 30 30 61 65 31 33 39 30 38 31 33 61 36 32 16000ae13 00000150 37 63 36 36 66 62 38 62 65 37 39 34 37 62 65 36 7c66fb8b6 00000160 33 63 35 32 64 61 37 35 38 39 33 37 39 35 31 35 3c52da735 00000170 64 34 65 30 61 36 30 34 66 38 31 34 31 37 38 31 d4e0a6463														30				
00000100 30 31 30 34 66 66 66 66 66 66 66 66 66 66 30 31 30 30 0104fffff 00000110 66 32 30 35 32 61 30 31 30 30 30 30 30 30 34 33 f2052a016 00000120 34 31 30 34 39 36 62 35 33 38 65 38 35 33 35 31 4104946b5 00000130 39 63 37 32 36 61 32 63 39 31 65 36 31 65 63 31 9c726ac91 00000140 31 36 30 30 61 65 31 33 39 30 38 31 33 61 36 32 16000ae13 00000150 37 63 36 36 66 62 38 62 65 37 39 34 37 62 65 36 7c66fb8b6 00000160 33 63 35 32 64 61 37 35 38 39 33 37 39 35 31 35 3c52da735 00000170 64 34 65 30 61 36 30 34 66 38 31 34 31 37 38 31 d4e0a6463 00000180 65 36 32 32 39 34 37 32 31 31 36 36 62 66 36 32 e62249473														66			66	0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0
000000110 66 32 30 35 32 61 30 31 30 30 30 30 30 30 34 33 f2052a016 00000120 34 31 30 34 39 36 62 35 33 38 65 38 35 33 35 31 4104946b5 00000130 39 63 37 32 36 61 32 63 39 31 65 36 31 65 63 31 9c726ac91 00000140 31 36 30 30 61 65 31 33 39 30 38 31 33 61 36 32 16000ae13 00000150 37 63 36 36 66 62 38 62 65 37 39 34 37 62 65 36 7c66fb8b6 00000160 33 63 35 32 64 61 37 35 38 39 33 37 39 35 31 35 3c52da735 00000170 64 34 65 30 61 36 30 34 66 38 31 34 31 37 38 31 d4e0a6463 00000180 65 36 32 32 39 34 37 32 31 31 36 36 62 66 36 32 e62249473	000000F0	66		66	66		37	30	34	66	66	66	66	30	30	31	64	ffff074fff0
000000120       34       31       30       34       39       36       62       35       33       38       65       38       35       33       35       31       4104946b5       41	00000100		31		34	66	66		66	66	66	66	66		31		30	0104fffffff
000000130       39       63       37       32       36       61       32       63       39       31       65       36       31       65       63       31       9c726ac91         000000140       31       36       30       30       61       65       31       33       39       30       38       31       33       61       36       32       16000ae13         00000150       37       63       36       36       66       62       38       62       65       37       39       34       37       62       65       36       7c66fb8b6         000000160       33       63       35       32       64       61       37       35       38       39       33       37       39       35       31       35       3c52da735         00000170       64       34       65       30       61       36       30       34       66       38       31       34       31       37       38       31       d4e0a6463         00000180       65       36       32       32       39       34       37       32       31       31       36       36	00000110	66	32	30	35	32	61	30	31	30	30	30	30	30	30	34	33	f2052a01000
00000140 31 36 30 30 61 65 31 33 39 30 38 31 33 61 36 32 16000ae13 000000150 37 63 36 36 66 62 38 62 65 37 39 34 37 62 65 36 7c66fb8b6 00000160 33 63 35 32 64 61 37 35 38 39 33 37 39 35 31 35 3c52da735 00000170 64 34 65 30 61 36 30 34 66 38 31 34 31 37 38 31 d4e0a6463 00000180 65 36 32 32 39 34 37 32 31 31 36 36 62 66 36 32 e62249473	00000120	34	31	30	34	39	36	62	35	33	38	65	38	35	33	35	31	4104946b538
00000150       37 63 36 36 66 62 38 62 65 37 39 34 37 62 65 36       7c66fb8be         00000160       33 63 35 32 64 61 37 35 38 39 33 37 39 35 31 35       3c52da735         00000170       64 34 65 30 61 36 30 34 66 38 31 34 31 37 38 31       d4e0a6463         00000180       65 36 32 32 39 34 37 32 31 31 36 36 62 66 36 32       e62249473	00000130	39	63	37	32	36	61	32	63	39	31	65	36	31	65	63	31	9c726ac91e6
00000160       33       63       35       32       64       61       37       35       38       39       33       37       39       35       31       35       3c52da735       35         000000170       64       34       65       30       61       36       30       34       66       38       31       34       31       37       38       31       d4e0a6463         00000180       65       36       32       32       39       34       37       32       31       31       36       62       66       36       32       e62249473	00000140	31	36	30	30	61	65	31	33	39	30	38	31	33	61	36	32	16000ae1390
00000170 64 34 65 30 61 36 30 34 66 38 31 34 31 37 38 31 d4e0a6463 00000180 65 36 32 32 39 34 37 32 31 31 36 36 62 66 36 32 e62249473	00000150	37	63	36	36	66	62	38	62	65	37	39	34	37	62	65	36	7c66fb8be79
00000180 65 36 32 32 39 34 37 32 31 31 36 36 62 66 36 32 e62249473	00000160	33	63	35	32	64	61	37	35	38	39	33	37	39	35	31	35	3c52da73589
00000180 65 36 32 32 39 34 37 32 31 31 36 36 62 66 36 32 e62249473	00000170	64	34	65	30	61	36	30	34	66	38	31	34	31	37	38	31	d4e0a646381
		65	36	32	32	39	34	37	32	31	31	36	36	62	66	36	32	e6224947321
																		1e73a823cbf
000001A0 35 38 65 65 61 63 30 30 30 30 30 30 30 30 58eacc000				65								-						
																3 1	3.8	01000000486
	00000190 000001A0	31 35	65 38	37 65	33 65	61 61	38 63	32	63 30	62 30	66 30	32 30	33 30	34 30	32 30	63	38	1e73a823ck 58eacc0000

# **Project Dashboard**

## **Application Summary**

Name	M^0
Commit	0dd7b4553009e3d87298a2f9e6aec2a89ba308ad
Fix Commit	55896c2f37a13a39fae933d52a2b6687ff4c9408
Language	Solidity
Platform	Ethereum

## **Engagement Summary**

Timeline	17-07-2024 to 19-07-2024
№ of Auditors	1
Review Time	3 days

## Vulnerability Summary

Issue Classification	Found	Addressed	Acknowledged
Critical	0	0	0
High	0	0	0
Medium	0	0	0
Low	2	1	1



None	2	0	2

## Category Breakdown

Suggestion	4
Documentation	0
Bug	0
Optimization	0
Good Code Practices	0

000000000	0.1	66	00	คล	ดด	00	00	คล	66	00	00	00	00	ลล	00	00	
00000040																	
00000070																	
00000080																	
00000090																	
00000A0																	
000000B0																	
00000000																	
00000000																	
00000E0																	
00000F0																	
00000100																	
00000110																	
00000000																	
00000 <b>C</b> O	de	M	atu	ırit	1	Eva	alu	ıat	ion								
00000 <b>Co</b>	61	65	36	33	66	37	34	66	39								
00000 Cod																	
00000M^C	0.00	ordi	nati	on l	ave	r fo	r ne	rmi	ssion	ed i	insti	tätio	nnal	201	ors	to as	enerate \$M 820
00000050	31	65	34	62	61	37	34	34	62	62	62	65	36	38	30	65	enerate \$M 820 1e4ba7445bb
00000060																	
00000070																	5400bfb1bcd
00000080															34		
00000090							31	64		31							fff0001d01e
000000A0		31		31								31					01010000000
000000B0																	
00000000																	
000000D0								30					30				
000000E0										30			66			66	00000000000
000000F0			66	66		37	30	34		66	66	66	30	30	31	64	ffff074fff0
00000100		31		34	66	66		66	66	66	66	66		31		30	0104fffffff
00000110	66	32	30	35	32	61	30	31	30	30	30	30	30	30	34	33	f2052a01000
00000110	34	31	30	34	39	36	62	35	33	38	65	38	35	33	35	31	4104946b538
00000120	39	63	37	32	36	61	32	63	39	31	65	36	31	65	63	31	9c726ac91e6
00000130	31	36	30	30	61	65	31	33	39	30	38	31	33	61	36	32	16000ae1390
00000140	37	63	36	36	66		38	62	65	37	39	34	37			36	7c66fb8be79
00000150						62						37		62	65 31		3c52da73589
	33	63	35	32	64	61	37	35	38	39	33		39	35		35	
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			58eacc00000
0000000	30	31	30	30	30	30	30	30	34	38	36	30	65	62	31	38	01000000486

# **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. All access control is correctly implemented.
Arithmetic	Moderate. Some rounding errors were found.
Centralization	Satisfactory. No significant points of centralization were found.
Code Stability	Satisfactory. The code was stable throughout the audit.
Upgradeability	Satisfactory. The contracts are upgradeable.
Function Composition	Satisfactory. The code was correctly split into helper functions.
Front-Running	Satisfactory. No front-running issues were found.
Monitoring	Satisfactory. Most events are emitted.
Specification	Satisfactory. The code follows the specifications.
Testing and Verification	Satisfactory. The codebase implements unit and fuzz tests.

00000000	01	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
00000010																	
000000000																	
0000000A0																	
000000B0																	
000000000																	
000000D0																	
000000E0																	
000000F0																	
00000100																	
00000110																	
00000000	30	31	30														
000000: <del>F</del> ir	ıdın	ıgs	66														
00000 Coc																	e15a089c638
00000M^(	<b>)</b> Cod	ordi	nati	on l	laye	r foi	r pe	rmis	ssion	ed i	insti	tutio	onal	act	ors	to ge	nerate \$M 820 1e4ba7445bb
00000060																	
00000070																	5400bfb1bcd
00000080																	
00000090																	fff0001d01e
000000A0																	01010000000
000000B0																	
00000000								30					30				
00000E0													66		66	66	$\bigcirc$
00000F0	66		66	66		37	30	34	66	66	66	66	30	30	31	64	ffff074fff0
00000100		31		34	66	66		66	66	66	66	66		31			0104fffffff
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
00000130				C F	C 1	60	20	30	30	30	30	30	30	30			F000000
00000130	35	38	65	65	61	63	30	50	50	50	20	50	50	50			58eacc00000

## **Findings**

### 3S-M^0-L01

Anyone can stop earning \$M directly through

MToken::stopEarning(address account\_) increasing the

WrappedMToken balance without backing

Id	3S-M^0-L01
Classification	Low
Severity	Medium
Likelihood	Low
Category	Suggestion
Status	Acknowledged

#### Description

MToken allows an account to stop earning if it is not approved anymore in the Registrar. For this reason, when the WrappedMToken stops being approved, it must call stop earning in the MToken and store the last index, such that the correct balances can be calculated.

However, MToken::stopEarning(address account\_) is permissionless and enables sending the WrappedMToken address, stopping MToken from being accrued. However, as it is not called through WrappedMToken::disableEarning(), the

\_lastDisableEarningIndex() will not be immediately recorded, accruing artificial WrappedMToken balance that is not actually backed. Thus, users will be able to withdraw more MToken than what WrappedMToken holds, potentially leading to the last users not being able to withdraw, depending on the index mismatch.

#### Recommendation

The governance call to stop the WrappedMToken from being approved in the Registrar must be called atomically with a call to WrappedMToken::disableEarning(), such that the last index is correctly recorded.



### 3S-M^0-L02

\_subtractTotalEarningSupply() could not be in an unchecked block to prevent rounding errors from wrapping the supply

Id	3S-M^0-L02
Classification	Low
Severity	Low
Likelihood	Low
Category	Suggestion
Status	Addressed in #d6f4404.

#### Description

On WrappedMToken::\_addEarningAmount(), the principal of an account is set as IndexingMath.getPrincipalAmountRoundedDown(balance\_ + amount\_, index\_), but the added principal to \_principalOfTotalEarningSupply is

IndexingMath.getPrincipalAmountRoundedDown(amount\_, currentIndex\_), indicating
that there will be a mismatch between the sum of account principal and
\_principalOfTotalEarningSupply. Additionally, the added amount to
totalEarningSupply() can further round down in

WrappedMToken::\_setTotalEarningSupply() when calculating the index. In WrappedMToken\_::subtractEarningAmount(), the same happens as the balance of the account is updated with balance\_ - amount but the subtract principal is calculated on amount only, and the index calculation can again round down. Thus, we can expect the sum of the individual accounts principal and balance to deviate slightly (can be considered dust and dealt with using excess(), as long as the balance of MToken is bigger).

#### Recommendation

In WrappedMToken::\_subtractTotalEarningSupply(), remove the unchecked block as the mismatch can cause this operation to wrap around, leading to inflated total supplies.

### 3S-M^0-N01

Re-enabling, although not possible at the moment, will make a jump in the index, not accompanied by the \$M balance increase

Id	3S-M^0-N01
Classification	None
Category	Suggestion
Status	Acknowledged

#### Description

Firstly this bug is not possible at the moment because re-enabling is disabled, see <code>WrappedMToken::enableEarning()</code>. However, if it is allowed, when it is enabled again, it will use the current index from the <code>MToken</code>, which will be bigger than the past stored index in <code>WrappedMToken</code> while it was disabled. This will make a jump in everyone's <code>WrappedMToken</code> balance, but the actual <code>MToken</code> holdings will not match it. Thus, users would get instant profit while the last ones would not be able to withdraw.

#### Recommendation

A simple fix is not trivial. Perhaps when the new index is fetched, a multiplier can be applied that discounts the previous stored index.

### 3S-M^0-N02

WrappedMToken::\_lastDisableEarningIndex() assumes the index will be in position 1 when disabled, which may not be true in the future

Id	3S-M^0-N02
Classification	None
Category	Suggestion
Status	Acknowledged

#### Description

WrappedMToken::\_lastDisableEarningIndex() fetches index 1 from \_enableDisableEarningIndices to get the last stored index before disabling. However, this is only true if WrappedMToken is disabled once, but if the current code to stop re-enabling earning is removed, it will lead to a wrong index.

#### Recommendation

The correct index is **\_enableDisableEarningIndices.length - 1**. If for gas saving purposes 1 is kept, a comment should be added to ensure it is changed later in case the re-enabling is allowed in the future.