SOLIDProof
Bring trust into your projects

**Blockchain Security | Smart Contract Audits | KYC
Development | Marketing**

MADE IN GERMANY

Zera

AUDIT

SECURITY ASSESSMENT

05. February, 2026

FOR

ZERA

SolidProof_io

@solidproof_io

Introduction

SolidProof.io is a brand of the officially registered company Future Visions Deutschland. We're mainly focused on Blockchain Security, such as Smart Contract Audits and KYC verification for project teams.
Solidproof.io assesses potential security issues in the smart contracts implementations, reviews for potential inconsistencies between the code base and the whitepaper/documentation, and provides suggestions for improvement.

Disclaimer

SolidProof.io reports are not, nor should they be considered, an "endorsement" or "disapproval" of any particular project or team. These reports are not, nor should they be considered, an indication of the economics or value of any "product" or "asset" created by any team. SolidProof.io does not cover testing or auditing the integration with external contracts or services (such as Unicrypt, Uniswap, PancakeSwap, etc.).

SolidProof.io Audits do not provide any warranty or guarantee regarding the absolute bug-free nature of the technology analysed, nor do they provide any indication of the technology proprietors. SolidProof Audits should not be used in any way to make decisions around investment or involvement with any particular project. These reports in no way provide investment advice, nor should be leveraged as investment advice of any sort.

SolidProof.io Reports represent an extensive auditing process intending to help our customers increase the quality of their code while reducing the high level of risk presented by cryptographic tokens and blockchain technology. Blockchain technology and cryptographic assets present a high level of ongoing risk. SolidProof's position is that each company and individual are responsible for their own due diligence and continuous security. SolidProof in no way claims any guarantee of the security or functionality of the technology we agree to analyse.

Project Overview

Summary

Project Name	**Zera-Network**
Website	https://zera.net/
About the project	ZERA is a governance-first blockchain network redefining decentralization by giving the community direct and autonomous control over every aspect of the protocol. It eliminates the traditional gap between decision and action — when users vote, the network executes transactions autonomously through a self-enforcing governance engine.
Chain	Zera-Network
Language	C++
Codebase Link	https://github.com/zera-os/zera-network
Commit	7ba8ac9f2ce42a3f606036009659a11ae5305ced
Unit Tests	Not Provided

Social Medias

Telegram	https://t.me/zera_community
X (Twitter)	https://x.com/zera_net
Facebook	N/A
Instagram	https://www.instagram.com/zera_net
Github	N/A
Reddit	N/A
Medium	N/A
Discord	N/A
Youtube	N/A
TikTok	N/A
LinkedIn	N/A

Audit Summary

Version	Delivery Date	Changelog
v1.0	19. November 2025	• Layout Project • Automated- /Manual-Security Testing • Summary
V1.1	17. Dezember 2025	• Updated Findings
V.1.2	05. February 2026	• Updated Findings

Note - The following audit report presents a comprehensive security analysis of the smart contract utilized in the project that includes malicious outside manipulation of the contract’s functions. This analysis did not include functional testing (or unit testing) of the contract/s logic. We cannot guarantee 100% logical correctness of the contract as we did not functionally test it. This includes internal calculations in the formulae used in the contract.

Zera Network - Code Metrics

Overall Statistics

Metric	Value
Number of Files	207
Total Lines	65561
Code Lines	50704
Comment Lines	6537
Blank Lines	8320
Functions	2683
Classes/Structs	488
Comment Ratio	9.97%

Top 10 Directories (by lines)

Directory	Lines	Files
z_validator/headers	26571	33
z_validator/smart_contract/native_functions	6121	14
z_validator/util	3218	13
z_validator/block_process/custom	3196	11
z_validator/db	2414	10
z_validator/block_process	2011	10
z_validator/block_process/template	1977	12
z_validator/template	1977	12
z_validator/crypto	1781	5
z_validator/smart_contract	1769	1

File Overview

The Team provided us with the files that should be tested in the security assessment. This audit covered the following files listed below with an SHA-1 Hash.

File Name	SHA-1 Hash
CMakeLists.txt	6d9529b6eb98837039610555c3b2a9b44406dac3
setup.sh	ad06016d3d2ffefb5573167e2b70fad9b476d1bc
update-config.sh	507a2f60b9c4f775f8951197a59a98dc26fdc683
pre_process.cpp	144e1ab7cc48729fd33910693d20c531c29d7b85
process_txn.cpp	d24595b7835c20d663ffc47cf3122811595b4afc
store_txns.cpp	4e3dd9153798542f0f75cd15ef5bb785b8129243
block_process.h	7524c994017a7ca62461409d6f2ff4d393f42589
fees_simple.cpp	15b44c1de5418491491a244bbee6a4930a77c726
zera_manager.h	f916a7d4c314f24087bbb451afd8b92323fedb2e
fees.cpp	143a07721977156fb0ac75932d50ea4e9e76b111
block_timer.cpp	314837d6ac580938eacee8d5f6aff66266701434
process_revoke.cpp	7462a67ee1e30e004e54eeb62c1af2a204712eba
process_cur_equiv.cpp	27d2dad22af17334024bff27350f6ddf97faa535
process_fast_quorum.cpp	e6e703688337b012168c2be4bae2cd33ccd321bf
process_compliance.cpp	0ee08ac8bbf8d11cdb4076c772ee20d27de57e73
process_delegated_voting.cpp	e287adeb612fed38d03507d31a2cd8d3837f28a3
process_allowance.cpp	94952888bededa264b49d9f3d29e35ba431a8887
process_update_contract.cpp	b3e3e2026f16579eece7f3f629685efa5332a586

File Name	SHA-1 Hash
process_votes.cpp	63acb7febdb073927776c3cad45e3943792e5e11
process_sbt_burn.cpp	25aeff94646b9a674cdb4eeb5c66ca692ae74b46
process_contract.cpp	0ebde87999a18d5578ff28a6923ead913f3933b6
process_nft.cpp	1712e378822323726ef39bfa395dd4f8e75968b5
process_quash.cpp	05ba132f5f2c41860a4feae4b27ff0bc48990461
process_utils.cpp	815ae22cc7d621c60ca167510ba96c375e10fb25
fees.h	9bf30f3cfae0d6e259e73f9103068c7afe409a8d
process_item_mint.cpp	477134731932ff0f9565ef0d6cb0c25842674d8d
process_heartbeat.cpp	be94509a97dc06e5e24e576a7e71cf488f54d4e4
process_smart_contract_instantiate.cpp	5cda3f12a577c3036a64c4ef3753b25016c38d98
process_mint.cpp	a6e6b44ba51235e293577915d16e98e0f979ec18
process_proposal.cpp	d72d3d9d7a0a0ca8eb745dc7950c8203f5a73428
process_new_coin.cpp	70e492552f62faa99781e2ca23e2827085c48370
process_registration.cpp	a1ea2071081792343deee9cdb420eea830b00bfb
process_smart_contract_deploy.cpp	26ff24e80f5fda92d99b889c0cfc84ca73eecf7f
process_required_version.cpp	e5b9355308f6931ae54c4e668a6c0667bc11725b
process_expense.cpp	4caf74b6222aa2c4721ab73280c55d27d92aea85
process_smart_contract_execute.cpp	5d0f786123d3d6ceacd4730f54a2ad00b1a729a7
client_network_service.cpp	394a7b59d053857888ea647cd9911c8bc667b023
validator_api_client.cpp	93102ab614b6000f96516bfc431d4c60265fec89

File Name	SHA-1 Hash
contract.cpp	80bcf2588677328da02902226589cfe555a2a367
base_fee.cpp	f94a6fa80af0c5b636f84ee2d6a9574d0130358a
block.cpp	eb3600fb26e9cc03a77692df35e8b63e5935c8e5
smart_contract_activity.cpp	9bee895ed4cf1de526c6fbaddc519d872bd51f88
items.cpp	ffb89e760e5018c1d534a3123bb6fc4ab4dc8ffe
contract_fee.cpp	50edd89ee3f66b2768f6e2950def2c62e8a56329
nonce.cpp	103573165566dd4d47c0c06ad4c78fa60612655c
balance.cpp	94ca08d568874170511f5fe311f593597d4e68a8
ace_tokens.cpp	b2061374c14e05f25a93e157506bca4fb4ed589e
proposals.cpp	3c027e0bbd69ef80a12f8d31ff5462dbb5c93d26
denomination.cpp	7c03b09d22aa06ac0d08caea9dc9ff86253407dc
api_service.cpp	40486ad019179d145094672c56ec4ce7b3f019de
database.cpp	41539b7e21ec69ed50618ebf4862ecb6a60211ee
attestation_client.cpp	178312766484aa74c38d26f8b2015e417e69167f
validator_network_client.cpp	1db50e59551feeff7288ab4ceb99244e3de0c21b
gossip_client.cpp	9f35d284e98e003bdc8e5639ed88074ec546ff0a
block_sync_client.cpp	e2562ab8444c15004cffc7ce5c76efa1a753a291
nonce_service.cpp	0ef35060188a512e782753c787fb6faba08eec50
indexer_voting_service.cpp	8b0ba0d7d3420bc9644d224a2962c95f9f892ad4
balance_service.cpp	63fc8013ef4537230bc39f6453a8810ccf34105d

File Name	SHA-1 Hash
gossip_service.cpp	49a77e5146559ec9101113e060c10a68adf2527a
block_sync_service.cpp	ab2caacae4b849f4c9afa305bd0b4a4fd424c66c
broadcast_service.cpp	cfac80ac98fcef9acb827ce8a83d705dccf2d44b
attestation_service.cpp	5669645aa819d93e63bdfd2ee947893a2dbe7354
validator_network_service.cpp	03bfa2a8c33feb7687e1ffd12ef17ce682b36945
client_network_service.cpp	394a7b59d053857888ea647cd9911c8bc667b023
validator_api_client.cpp	93102ab614b6000f96516bfc431d4c60265fec89
logging.h	5f907f87477105ba6232ab7471f5a51685a96d27
logging.cpp	eae258a2cf88b931ee2d8e5f10ba7bc2fab5c01f
attestation_process.cpp	ef8bd4d6dfd2c3f30d519ab57ae4bf3a81afdf5b
attestation_process.h	bd51d1913e97c9d033217b796c0839fb11ee928e
zera-validator.cpp	bdec22b99f532f64cce2cde67820e20e8b0d7276
restricted_keys.cpp	ff3f648d8fad36c2a9b526e6a5ac58f1dae18a25
restricted_keys.h	ca72a8950f9356fb80311fbfe27a7340edf7d980
native_function_states.h	c00e67c7fd5a15b5874fcd38fa2ae0742c5d4091
txn.grpc.pb.cc	7d28131de980dc30b82d5112a7b2ba6fedb05971
lottery.h	b71782bcdcddc31d725678dc846e255b766a4f56
const.h	41b46cba5df25a4ea9964f2df5b0044a4abcab5d
verify_process_txn.h	584b1d88071c80ca764a358a9c7b4aa6ddbeca1b
rate_limiter.h	efc4a37827d43583ad01e4c446fd19f7124b9c0c

File Name	SHA-1 Hash
validator.pb.h	bad1e8c4bb15dbf56681c92499758b403f937f97
hex_conversion.h	0ca010c0c4db591f4ec2f82102373b055cc02ae6
test.h	81ec4589dc2a2a7e28f9fda65de42bf7a7aef237
native_function_db_store_single.h	a2690b8d7c13e070ef6670f66614d9e4ee8671e5
native_function_utils.h	5d9e247a6cbc92680affc2c0b455cac39cd23445
wallets.h	49573943b773ee552968eaf240f7b87a3fb7a837
validators.h	222f8a3cc3aa9dccd8b6454f6bfbecb10081efcc
native_function_get_ace.h	77fa7ca5afd28733db5ca3cf062efaecaa42ab2b
signatures.h	0adc0ba6f2db40328cacb3721e86f9c6f123c3d6
validator_api_client.h	0318bf6b2da31c50c89e1d568d1f8753b99e573b
debug.h	6a432bd3e7ff5fe6dd4f347b7857bde2515851ee
native_function_txns.h	d2b272ec20d841b0723a40aab6cfdc2d1f390f8f
client_network_service.h	d7e5cdc14d458e4d84f0501b0a25cd794ba0d2e1
utils.h	642781276ecd3c04d00b73ff529e168aee50b0bb
block_timer.h	afa96d87c0239fa6b79cdf8f619486fe3aad94b7
validator_network_client.h	dbac04acb7e8910c8ea29e803edf999cdbd200bb
proposer.h	4e20f0c8aa02a1584f04a66df7d95d7beebf688c
smart_contract_sender_data.h	83207bce91a4da4086273d80c8b4f3ffe03ac788
validator_api_service.h	0754170fe7babb0ad9bb6a0db4a529de717fec28
threadpool.h	f9def42a02e30d309f9941fb6376996c15861021

File Name	SHA-1 Hash
block.h	a028772906c09c29f28683effdf905ec30643de7
db_base.h	b9d3a8c3e4af0a9014af49675a88f30278a8b335
hashing.h	1d600be0966ae88d1206c212d0283d85ead86567
database.h	d97ff3c9a80fb678e6ea5e0eb2aad59280697f48
smart_contract_service.h	8b1be24020d26178fd2bc3258ad3fc5e661b5ee0
native_function_db_get_data.h	7e1426d94eddff0ffcc8416c963217442918a7c7
base58.h	b3f779e8045cf171817257077e86fa0aee8aa956
validator_network_service_grpc.h	4684c3613098869841ead4c3e4efbf0e1595c306
stopwatch.h	bfcc163cf072254da044812500b8e39fb5688017
base58.cpp	0691c7dd9fef459003f2d5464dffb763de315fb5
block.cpp	d4f62b8a9687ad09a16016d2744481d4ea0eefc1
startup_config.cpp	dfb75fa12b14ba06f0647a08e86ec48dd630d5d8
threadpool.cpp	cb487a18ffa218e6b3d1bf5d72bd49e2b3b1ac8d
validators.cpp	697bd107d62a730b533cb3576427156f1d00f7a6
hex_conversion.cpp	58bb281b4b56abc0c56d847de48bee2f46a0252a
block_timer.h	afa96d87c0239fa6b79cdf8f619486fe3aad94b7
validate_block.h	53c7e7786822ee7079d15fb8288cf506c93571e5
startup_config.h	7516ded1904d5acd5dc21fcc2add0ab8196015d6
utils.cpp	bd3121d5eda1a961ea2b38608942e1c615639990
validate_block.cpp	59554dd8cf9cee22e610138ad9760bdbb3984504

File Name	SHA-1 Hash
validator_config.cpp	07ede12c033bcbca9bbc51270e5accec6295c7bc
batch_contract.cpp	421889d44f46e77f23c69c1423e6c0be08ad1d0d
batch_validator.cpp	2d5c576587ad9a61fd3e302834697903d2e9fe97
batch_smart_contract.cpp	da288974db43824734ac2e6b9611f81aba3a9ed7
txn_batch.h	f160038c41e7e42c7acdd84dfe60d609767f91f3
batch_misc.cpp	aa781e9bfe3e3f7a972f181a4c1580e6fe1f5074
batch_item.cpp	2978f5ac8c400225061031edf6748299f4c3064d
batch_gov.cpp	0351cad67d4ae1aa938b492fbc907637c7bc0513
batch_proposals.cpp	e26983b5c7444b9e55f6124eccc931d02b6e261d
zera_api.proto	4867db4d27c130b9e1544f200535212b0167a12b
validator.proto	4e6569c2315d58f6891f9fe32bd7b2f235c6cb36
wallet.proto	ea530deb560606536aa0a31711378bcb54274fee
txn.proto	3ecfaf31b876e2ecc207f7e40f7aa07dad15b558
compliance.h	9acdba7e5caeea825fd95914083e670a28fd759a
compliance.cpp	782efd11ea2f87741246cabb4455033f59457e90
gov_process.h	5888a699bcd94679d8e608c85df9dcb56342cce1
gov_txn.cpp	da39a3ee5e6b4b0d3255bfef95601890afd80709
time_calc.cpp	73d206e685053540520509d579ab17796eda2d7e
time_calc.h	1cc7dbfa867d921e07a0434456603da1873a3477
gov_process.cpp	c477756052e36cc0e8525f52d127a52935d5d197

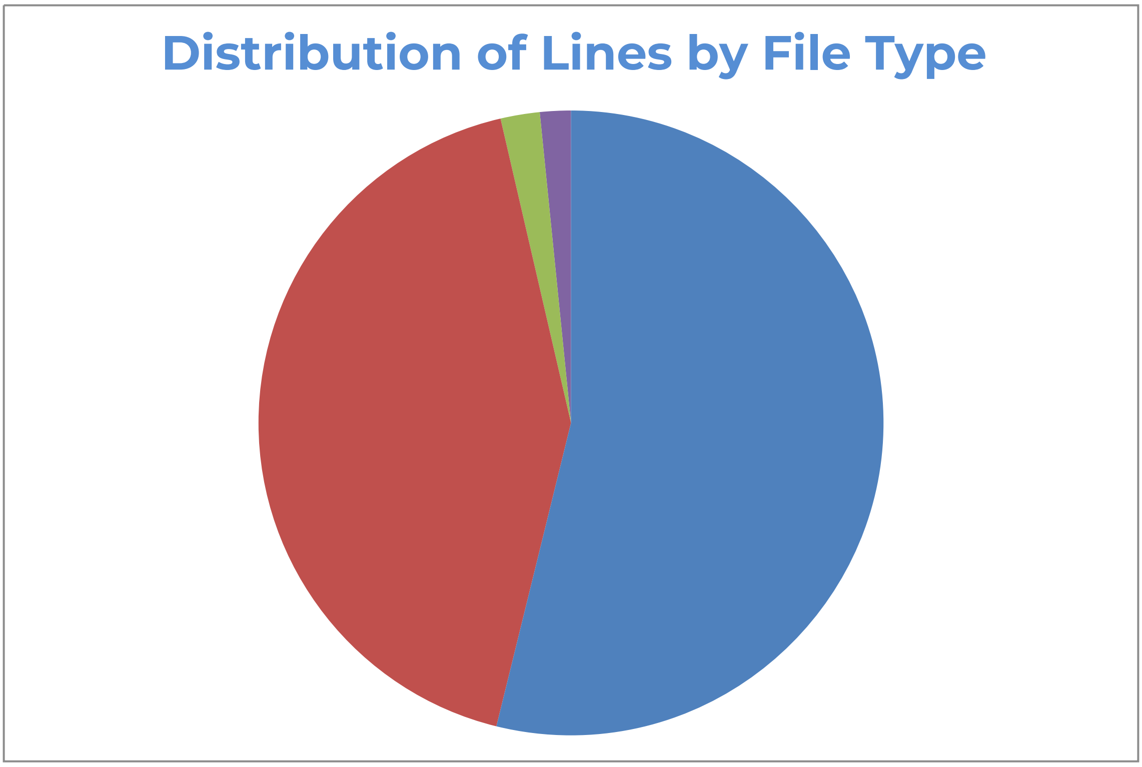
File Name	SHA-1 Hash
pre_process.cpp	937b41aeb05a67eb0a3970e4a863d91db840f47f
validator_balances.cpp	aa6e604b979a5b2527cf2ee05ee4642d57559d63
proposer.cpp	2f22eaf9e3556a63f26ac0d2945e4947db3e7a33
select_validators.cpp	9cc8d94ecbf5244c25deb494bc690b69aca3fd19
proposer_utils.cpp	9470afe09582b571ee225a7e58d669ba46fca06b
reg_process.cpp	365e35990cb1f481c2a202a53b02c47b270a878e
validate_block.cpp	6eeb14d16686d5dc5ea29e13f22f460a571cbcb4
vp_broadcast.cpp	c2e2a5892dee05917eb6e58ac62e933cef1d9c9d
verify_process.cpp	1daa29cc7db8e5256ae420b5275781b4f8bd482e
blake3.h	7452ab37649fe20f5f87975da22e4a9e0438c135
blake3.c	420588f2c94d0b33555f66937083bbeb62971202
blake3_portable.c	ec5dd78c0711e601ab9e29be6461a4cc5c7ce2b9
blake3_dispatch.c	3fef127f2bc808a5bf30b526322d30063944893b
blake3_impl.h	45ea99bded03b1c3073c133fcdc691c497256700
recieved_tracker.cpp	bf730e627360592a22dde89f5de055e8033845a0
proposer_tracker.cpp	4003b210b455a84ed1c9a8d27a4c8faf3229bbf6
nonce_tracker.cpp	1ac397e6aecd8bcb274a8c2d09f3cb4043f2684c
quash_tracker.cpp	acde82e2618d0667cd1b6ef58b5915b14b86d24c
txn_tracker.cpp	71ed960903dfbf29168e92742031d94e3fd2ca12
temp_data.h	53833eef0d9e6b186e3b5b064de3358d47fa6149

File Name	SHA-1 Hash
status_fee_tracker.cpp	9dbd843c807c58d3fb2ddb59ce681c7b8b648ce0
item_tracker.cpp	6a82018c20c6fed9a4a8789ddc466009f571cc1a
balance_tracker.cpp	9858cfaf57cd0a38de1e75b76f62781d7bd42713
supply_tracker.cpp	a727a582d33af6e8af37e78d9e87a05101d4ea46
contract_price_tracker.cpp	fc962ba6123eba37abffeb4c02bdd25179670a8f
sbt_burn_tracker.cpp	862f8d43f317402a586005cd9875aacf866801b8
txn_hash_tracker.cpp	1fa8ccf415d379b05271e32d45f9998ca27ffecb
allowance_tracker.cpp	499a0a35fab89ec7ad0c213b4b088415d5d37832
fast_quorum_tracker.cpp	2786f81411e61505f90a523fc26e53df322e9daf
process_revoke.cpp	7462a67ee1e30e004e54eeb62c1af2a204712eba
process_cur_equiv.cpp	27d2dad22af17334024bff27350f6ddf97faa535
process_fast_quorum.cpp	e6e703688337b012168c2be4bae2cd33ccd321bf
process_compliance.cpp	0ee08ac8bbf8d11cdb4076c772ee20d27de57e73
process_delegated_voting.cpp	e287adeb612fed38d03507d31a2cd8d3837f28a3
process_allowance.cpp	94952888bededa264b49d9f3d29e35ba431a8887
process_update_contract.cpp	b3e3e2026f16579eece7f3f629685efa5332a586
process_votes.cpp	63acb7febdb073927776c3cad45e3943792e5e11
process_sbt_burn.cpp	25aeff94646b9a674cdb4eeb5c66ca692ae74b46
process_contract.cpp	0ebde87999a18d5578ff28a6923ead913f3933b6
process_nft.cpp	1712e378822323726ef39bfa395dd4f8e75968b5

File Name	SHA-1 Hash
process_quash.cpp	05ba132f5f2c41860a4feae4b27ff0bc48990461
debug.cpp	8a2c96a989b031f2bd25cbbea04017172bc8b01b
test.cpp	f4d983eb1940c560bbfa652423e03ae9db3626d6
lottery.cpp	91f66aa69bd35a3c23b2f76068977f5ad2b137a0
merkle.cpp	02ad3bf28892f7344e2f0c06c8b359157c45cb65
merkle.h	8bbba30976c77f801859ed11cdcdd4bce87308b0
signatures.cpp	93eaa5acdbd579f9de8879783427d261c1366256
wallets.cpp	6bb0a91e31941e5fc6ceac2a610f7695d87c8fa6
db_block_headers.cpp	5efc64c175f6540cf0ee576f90719f6dccfef168
db_validators.cpp	e78758600bd492711c3ae34261ac5ebde6cf8a8b
reorg.cpp	48c7e701817918e96cd4ad0d48f4e94cad74a2ab
reorg.h	9923212be9cff21ce2b4e11b5510326b1bd1dca4
migrate_db.cpp	b1c4d600278b1133ce9055507151563c920b28d5
db_config.cpp	e0476e3dcd4aa696565f3b926f4962ece9971ef9
db_base.cpp	f561e9d88be33ee02cd156eb1065d81caf765c6e
migrate_db.h	e41bf6c0ca5d252783cc2353241c1ffe5fd6b24f
db_blocks.cpp	570261de529dc0e40344567314cade6bcdab3d44
database.cpp	6842f147dc02edb90512b01fb0167d8d578ba7cc
native_function_vote.cpp	08bdae4a1c36628a1251c2396914174a6ea2da2b
native_function_states.cpp	1134f9965cd6ed63870d06e1f9e3a6a0a3517cbf

File Name	SHA-1 Hash
native_function_mint.cpp	502c971bbea30f386d122b42dd1a8f63128c4b59
native_function_contract_bridge.cpp	58fbb382de275a4c79cfab95021c765c36669201
native_function_get_ace.cpp	680104bd3b48113e0887183e9806a57effdc908c
native_function_send.cpp	a36ba09a4884f39b6b0862717b2426ede7439a34
native_function_db_get_data.cpp	714071fff36cfb225f3b3e07c6456055a0a8c195
native_function_multi_send.cpp	c813f1133d8c7085a25c30b9b3e070ae0744f111
native_function_transfer.cpp	7f0df42090afca1934857a62f29a5be36a7c3568
native_function_db_store_single.cpp	4c00e9a2058bfa86e4452d6861fbb05ccafe6c2e
native_function_allowance.cpp	34c88700bd81a78311f43627fcec4c0f80cc5752
native_function_utils.cpp	16e5db9c7ea14c6034c9652fe6ddd77aaa8dc579
native_function_expense_ratio.cpp	819b7c49a53b20db6943b336f070ce729e3fdd6c
native_function_hold.cpp	c7840bf9e23c9de1c6fe70b334dbd1d6c4040a78
smart_contract_service.cpp	c9902a267a12b26436742793bddcb78762bf77b4

File Type	Files	Lines	Code	Comments
.cpp	147	35296	26742	3357
.h	53	27890	22107	2818
.proto	4	1328	1218	33
.c	3	1047	637	329



Please note: Files with a different hash value than in this table have been modified after the security check, either intentionally or unintentionally. A different hash value may (but need not) indicate a changed state or potential vulnerability that was not the subject of this scan.

Filename	Type	Lines	Functions	Classes	Comment Ratio
validator.pb.h	.h	23582	1675	310	9.07%
smart_contract_service.cpp	.cpp	1769	21	0	12.04%
native_function_allowance.cpp	.cpp	1087	17	0	1.93%
validate_block.cpp	.cpp	1058	21	0	1.61%
native_function_send.cpp	.cpp	1029	21	0	32.46%
db_base.cpp	.cpp	959	0	0	2.71%
gov_process.cpp	.cpp	924	21	0	2.27%
native_function_utils.cpp	.cpp	876	28	0	7.88%
signatures.cpp	.cpp	867	34	0	7.27%
process_new_coin.cpp	.cpp	823	16	0	2.79%
txn.proto	.proto	650	0	0	0.77%
balance_tracker.cpp	.cpp	618	14	0	3.72%
blake3.c	.c	616	0	0	31.01%
wallets.cpp	.cpp	609	28	0	3.12%
process_proposal.cpp	.cpp	586	6	0	3.07%
attestation_client.cpp	.cpp	523	12	0	12.81%
process_contract.cpp	.cpp	522	7	0	5.56%
process_contract.cpp	.cpp	522	7	0	5.56%
native_function_mint.cpp	.cpp	500	11	0	33.60%
restricted_keys.cpp	.cpp	499	14	0	6.81%
process_update_contract.cpp	.cpp	470	6	0	2.77%
validator_config.cpp	.cpp	470	68	0	1.28%
process_update_contract.cpp	.cpp	470	6	0	2.77%
native_function_states.cpp	.cpp	455	7	0	11.43%
fees.cpp	.cpp	439	11	0	4.33%
native_function_hold.cpp	.cpp	423	16	0	60.28%
store_txns.cpp	.cpp	421	11	0	4.28%
native_function_multi_send.cpp	.cpp	412	11	0	51.46%
validator_api_client.cpp	.cpp	405	21	0	6.42%
validator_api_client.cpp	.cpp	405	21	0	6.42%
validator.proto	.proto	404	0	0	4.21%
attestation_service.cpp	.cpp	403	7	0	15.88%
native_function_contract_bridge.cpp	.cpp	397	7	0	4.79%
utils.cpp	.cpp	388	17	0	4.90%
gossip_service.cpp	.cpp	380	8	0	9.21%
db_base.h	.h	378	0	57	3.17%
process_smart_contract_execute.cpp	.cpp	375	10	0	7.20%
migrate_db.h	.h	344	0	54	3.49%
native_function_transfer.cpp	.cpp	337	11	0	61.42%
proposer.cpp	.cpp	336	8	0	8.93%
validator_network_client.cpp	.cpp	335	3	0	3.28%
block_timer.cpp	.cpp	306	9	0	4.58%
proposer.h	.h	299	7	4	7.69%
process_registration.cpp	.cpp	294	4	0	2.38%
database.cpp	.cpp	294	13	0	3.74%
process_smart_contract_instantiate.cpp	.cpp	292	8	0	7.19%
startup_config.cpp	.cpp	290	11	0	18.62%
validator_network_client.h	.h	285	7	1	12.63%
block_sync_client.cpp	.cpp	278	6	0	12.23%

Filename	Type	Lines	Functions	Classes	Comment Ratio
proposer_utils.cpp	.cpp	273	2	0	1.10%
blake3_impl.h	.h	273	9	0	43.59%
base58.cpp	.cpp	271	9	0	9.96%
blake3_dispatch.c	.c	271	0	0	49.08%
validator_balances.cpp	.cpp	269	6	0	10.04%
verify_process.cpp	.cpp	267	1	0	1.87%
process_votes.cpp	.cpp	266	4	0	10.53%
process_votes.cpp	.cpp	266	4	0	10.53%
batch_contract.cpp	.cpp	263	3	0	4.18%
zera_api.proto	.proto	261	0	0	4.21%
rate_limiter.h	.h	258	16	5	9.30%
threadpool.cpp	.cpp	241	12	0	8.30%
validator_network_service_grpc.h	.h	239	7	1	17.57%
pre_process.cpp	.cpp	231	3	0	0.87%
select_validators.cpp	.cpp	229	5	0	3.93%
allowance_tracker.cpp	.cpp	224	6	0	7.14%
process_txn.cpp	.cpp	212	4	0	3.77%
reg_process.cpp	.cpp	210	2	0	2.38%
reorg.cpp	.cpp	206	4	0	4.85%
db_config.cpp	.cpp	206	3	0	1.94%
batch_misc.cpp	.cpp	203	4	0	6.90%
hashing.h	.h	202	2	2	12.87%
temp_data.h	.h	194	0	15	4.12%
process_item_mint.cpp	.cpp	192	2	0	5.73%
process_utils.cpp	.cpp	189	5	0	11.64%
process_mint.cpp	.cpp	188	2	0	10.11%
native_function_vote.cpp	.cpp	187	5	0	6.95%
pre_process.cpp	.cpp	183	2	0	8.20%
process_nft.cpp	.cpp	183	2	0	6.01%
process_nft.cpp	.cpp	183	2	0	6.01%
native_function_expense_ratio.cpp	.cpp	182	5	0	6.59%
merkle.cpp	.cpp	181	3	0	2.21%
process_quash.cpp	.cpp	171	1	0	2.92%
process_quash.cpp	.cpp	171	1	0	2.92%
validators.cpp	.cpp	166	4	0	21.69%
process_smart_contract_deploy.cpp	.cpp	164	2	0	29.27%
migrate_db.cpp	.cpp	164	0	0	7.32%
batch_proposals.cpp	.cpp	163	3	0	9.20%
client_network_service.h	.h	162	5	1	13.58%
time_calc.cpp	.cpp	162	12	0	2.47%
blake3_portable.c	.c	160	0	0	3.12%
compliance.cpp	.cpp	150	3	0	4.67%
validators.h	.h	149	0	2	12.75%
process_expense.cpp	.cpp	148	2	0	5.41%
broadcast_service.cpp	.cpp	144	7	0	20.83%
nonce_tracker.cpp	.cpp	142	11	0	6.34%
fees_simple.cpp	.cpp	133	2	0	14.29%
block.cpp	.cpp	129	7	0	11.63%
verify_process_txn.h	.h	128	4	1	19.53%
native_function_db_get_data.cpp	.cpp	127	4	0	15.75%

Filename	Type	Lines	Functions	Classes	Comment Ratio
database.cpp	.cpp	123	1	0	2.44%
gossip_client.cpp	.cpp	121	2	0	12.40%
validator_api_client.h	.h	120	0	3	32.50%
block_sync_service.cpp	.cpp	117	4	0	12.82%
lottery.cpp	.cpp	114	6	0	14.04%
contract_price_tracker.cpp	.cpp	111	4	0	2.70%
validator_api_service.h	.h	108	3	1	18.52%
test.cpp	.cpp	108	3	0	19.44%
vp_broadcast.cpp	.cpp	107	5	0	14.02%
smart_contract_activity.cpp	.cpp	106	2	0	6.60%
logging.cpp	.cpp	104	5	0	6.73%
batch_item.cpp	.cpp	104	2	0	5.77%
supply_tracker.cpp	.cpp	98	2	0	8.16%
validator_network_service.cpp	.cpp	95	22	0	1.05%
db_block_headers.cpp	.cpp	94	4	0	13.83%
batch_validator.cpp	.cpp	93	2	0	8.60%
process_delegated_voting.cpp	.cpp	92	4	0	6.52%
process_delegated_voting.cpp	.cpp	92	4	0	6.52%
db_blocks.cpp	.cpp	88	3	0	13.64%
client_network_service.cpp	.cpp	86	19	0	4.65%
client_network_service.cpp	.cpp	86	19	0	4.65%
process_heartbeat.cpp	.cpp	85	1	0	5.88%
quash_tracker.cpp	.cpp	74	3	0	2.70%
process_cur_equiv.cpp	.cpp	73	2	0	9.59%
process_cur_equiv.cpp	.cpp	73	2	0	9.59%
proposals.cpp	.cpp	70	1	0	4.29%
indexer_voting_service.cpp	.cpp	68	1	0	14.71%
threadpool.h	.h	66	0	2	31.82%
native_function_txns.h	.h	62	0	0	3.23%
block_process.h	.h	61	0	2	31.15%
signatures.h	.h	61	0	2	22.95%
process_allowance.cpp	.cpp	60	0	0	11.67%
process_sbt_burn.cpp	.cpp	60	0	0	11.67%
block.cpp	.cpp	60	1	0	3.33%
balance.cpp	.cpp	60	1	0	3.33%
native_function_utils.h	.h	60	0	0	6.67%
blake3.h	.h	60	0	1	36.67%
process_allowance.cpp	.cpp	60	0	0	11.67%
process_sbt_burn.cpp	.cpp	60	0	0	11.67%
api_service.cpp	.cpp	59	13	0	1.69%
native_function_get_ace.cpp	.cpp	58	1	0	22.41%
nonce_service.cpp	.cpp	57	1	0	17.54%
proposer_tracker.cpp	.cpp	57	4	0	5.26%
fees.h	.h	56	0	1	17.86%
attestation_process.cpp	.cpp	56	3	0	10.71%
const.h	.h	56	0	0	19.64%
block_timer.h	.h	56	4	1	10.71%
hex_conversion.cpp	.cpp	56	5	0	3.57%
block_timer.h	.h	56	4	1	10.71%
native_function_db_store_single.cpp	.cpp	51	1	0	27.45%

Filename	Type	Lines	Functions	Classes	Comment Ratio
process_required_version.cpp	.cpp	49	1	0	26.53%
validate_block.h	.h	49	2	1	48.98%
ace_tokens.cpp	.cpp	48	1	0	4.17%
nonce.cpp	.cpp	47	1	0	2.13%
txn_tracker.cpp	.cpp	47	2	0	6.38%
txn_hash_tracker.cpp	.cpp	47	6	0	4.26%
txn_batch.h	.h	46	1	1	13.04%
items.cpp	.cpp	45	1	0	2.22%
db_validators.cpp	.cpp	43	2	0	13.95%
batch_smart_contract.cpp	.cpp	41	2	0	12.20%
wallets.h	.h	39	0	1	15.38%
smart_contract_service.h	.h	38	1	1	13.16%
balance_service.cpp	.cpp	37	1	0	21.62%
stopwatch.h	.h	37	3	1	10.81%
contract_fee.cpp	.cpp	35	1	0	2.86%
smart_contract_sender_data.h	.h	35	0	1	14.29%
recieved_tracker.cpp	.cpp	35	3	0	2.86%
process_fast_quorum.cpp	.cpp	33	0	0	15.15%
contract.cpp	.cpp	33	1	0	18.18%
process_fast_quorum.cpp	.cpp	33	0	0	15.15%
sbt_burn_tracker.cpp	.cpp	30	2	0	6.67%
denomination.cpp	.cpp	28	1	0	3.57%
restricted_keys.h	.h	28	0	1	17.86%
block.h	.h	28	0	0	35.71%
database.h	.h	28	0	1	32.14%
test.h	.h	27	0	1	33.33%
time_calc.h	.h	27	0	1	18.52%
debug.cpp	.cpp	27	1	0	14.81%
process_compliance.cpp	.cpp	26	0	0	19.23%
process_compliance.cpp	.cpp	26	0	0	19.23%
item_tracker.cpp	.cpp	25	2	0	8.00%
status_fee_tracker.cpp	.cpp	24	2	0	16.67%
base_fee.cpp	.cpp	23	1	0	17.39%
process_revoke.cpp	.cpp	21	0	0	4.76%
process_revoke.cpp	.cpp	21	0	0	4.76%
native_function_states.h	.h	20	0	0	10.00%
utils.h	.h	20	0	0	20.00%
fast_quorum_tracker.cpp	.cpp	19	2	0	10.53%
zera-validator.cpp	.cpp	17	1	0	17.65%
hex_conversion.h	.h	17	0	1	41.18%
gov_process.h	.h	17	0	2	23.53%
reorg.h	.h	16	0	1	18.75%
base58.h	.h	13	0	0	23.08%
wallet.proto	.proto	13	0	0	0.00%
logging.h	.h	12	0	1	16.67%
zera_manager.h	.h	11	0	1	18.18%
lottery.h	.h	10	0	0	70.00%
merkle.h	.h	10	0	1	40.00%
attestation_process.h	.h	8	0	1	25.00%
native_function_db_get_data.h	.h	8	0	0	25.00%

Filename	Type	Lines	Functions	Classes	Comment Ratio
startup_config.h	.h	7	0	1	14.29%
compliance.h	.h	7	0	1	14.29%
native_function_get_ace.h	.h	6	0	0	33.33%
debug.h	.h	6	0	1	16.67%
validate_block.cpp	.cpp	6	0	0	83.33%
native_function_db_store_single.h	.h	5	0	0	40.00%
gov_txn.cpp	.cpp	0	0	0	0.00%

Imported packages

Used code from other Frameworks/Smart Contracts (direct imports).

Note for Investors: We only audited contracts mentioned in the scope above. All contracts related to the project apart from that are not a part of the audit, and we cannot comment on its security and are not responsible for it in any way

- gRPC
- Google Protocol Buffers
- RocksDB
- LevelDB
- libsodium
- WasmEdge Runtime

Audit Information

Vulnerability & Risk Level

Risk represents the probability that a certain source threat will exploit vulnerability and the impact of that event on the organization or system. The risk Level is computed based on CVSS version 3.0.

Level	Value	Vulnerability	Risk (Required Action)
Critical	9 - 10	A vulnerability that can disrupt the contract functioning in a number of scenarios, or creates a risk that the contract may be broken.	Immediate action to reduce risk level.
High	7 – 8.9	A vulnerability that affects the desired outcome when using a contract, or provides the opportunity to use a contract in an unintended way.	Implementation of corrective actions as soon aspossible.
Medium	4 – 6.9	A vulnerability that could affect the desired outcome of executing the contract in a specific scenario.	Implementation of corrective actions in a certain period.
Low	2 – 3.9	A vulnerability that does not have a significant impact on possible scenarios for the use of the contract and is probably subjective.	Implementation of certain corrective actions or accepting the risk.
Informational	0 – 1.9	A vulnerability that have informational character but is not effecting any of the code.	An observation that does not determine a level of risk

Auditing Strategy and Techniques Applied

Throughout the review process, care was taken to check the repository for security-related issues, code quality, and compliance with specifications and best practices. To this end, our team of experienced pen-testers and smart contract developers reviewed the code line by line and documented any issues discovered.

We check every file manually. We use automated tools only so that they help us achieve faster and better results.

Methodology

The auditing process follows a routine series of steps:

1. Code review that includes the following:

1.a. Review the specifications, sources, and instructions provided to SolidProof to ensure we understand the smart contract's size, scope, and functionality.

1.b. Manual review of the code, i.e., reading the source code line by line to identify potential vulnerabilities.

1.c. Comparison to the specification, i.e., verifying that the code does what is described in the specifications, sources, and instructions provided to SolidProof.

1. Testing and automated analysis that includes the following:

1.a. Test coverage analysis determines whether test cases cover code and how much code is executed when those test cases are executed.

1.b. Symbolic execution is analysing a program to determine what inputs cause each part of a program to execute.

2. Review best practices, i.e., smart contracts to improve efficiency, effectiveness, clarity, maintainability, security, and control based on best practices, recommendations, and research from industry and academia.

3. Concrete, itemized and actionable recommendations to help you secure your smart contracts.

Audit Results

Critical issues

No critical issues

High issues

1 # | Unsecure Random Number

File	Severity	Location	Status
smart_contract_service.cpp process_smart_contract_deploy.cpp	High	L442 L36	Fixed

Description – The use of rand() or srand() is insecure and predictable. Especially with a seed time(null)

Remediation – We recommend the usage of std::random_device or /dev/urandom on unix-like system.

2 # | Unsecure Random Number

File	Severity	Location	Status
smart_contract_service.cpp process_smart_contract_deploy.cpp	High	L442 L36	Fixed

Description – The use of rand() or srand() is insecure and predictable. Especially with a seed time(null)

Remediation – We recommend the usage of std::random_device or /dev/urandom on unix-like system.

Medium issues

1 # | Memory Leak in Key Generation

File	Severity	Location	Status
wallets.cpp	Medium	L575	Fixed

Description – The created pointer is not used, but memory got reserved. This could lead to an memory exhaustion.

Remediation – Remove unused code or make sure the occupied memory got released.

Low issues

1 # | Insecure Logging

File	Severity	Location	Status
logging.cpp	Low	L13	Fixed

Description – No rotation or size limits, possible disk filling.
Remedation – Implement a log rotation with limited sizes for the log files.

2 # | Missing Error Handling

File	Severity	Location	Status
db_base.cpp	Low	L803-840	Fixed

Description – Generic error handling, the database is reopend even on critical erros. This could lead to state inconsistency.
Remedation – Implement specific behavior, also try to implement a validation mechanism for the database state after an error occured.

3 # | Hardcoded Paths

File	Severity	Location	Status
process_smart_contract_deploy.cpp	Low	L10	Fixed

Description – Hardcoded relative paths could cause issues on portability and may fail on different systems.
Remedation – If hardcoded paths are needed, make sure they got created on initialization. Or implement a configuration for

Informational issues

1 # | „Hack“-Flag

File	Severity	Location	Status
validator_config.cpp gov_process.cpp	info	L24, L127-133 L217-221, L495-500	Fixed

Description – This flag set to true is a complete bypass of governance security mechanisms, which lead to an approval of every proposal. It also affects the proposal processing time by -10 days, which bypasses mandatory waiting times and a rushing through proposals.

Remediation – We assume this flag is only for testing purposes and must be removed before production. **There is no other way to resolve this is, than deleting this opportunity!**

Comment – This flag got accidentally in the audited code and was removed on the production code. This function would instantly validate every block, which is not possible in the mainnet version.

Legend for the Issue Status

Attribute or Symbol	Meaning
Open	The issue is not fixed by the project team.
Fixed	The issue is fixed by the project team.
Acknowledged(ACK)	The issue has been acknowledged or declared as part of business logic.

Solid Proofed

Blockchain Security | Smart Contract Audits | KYC Development | Marketing

MADE IN GERMANY