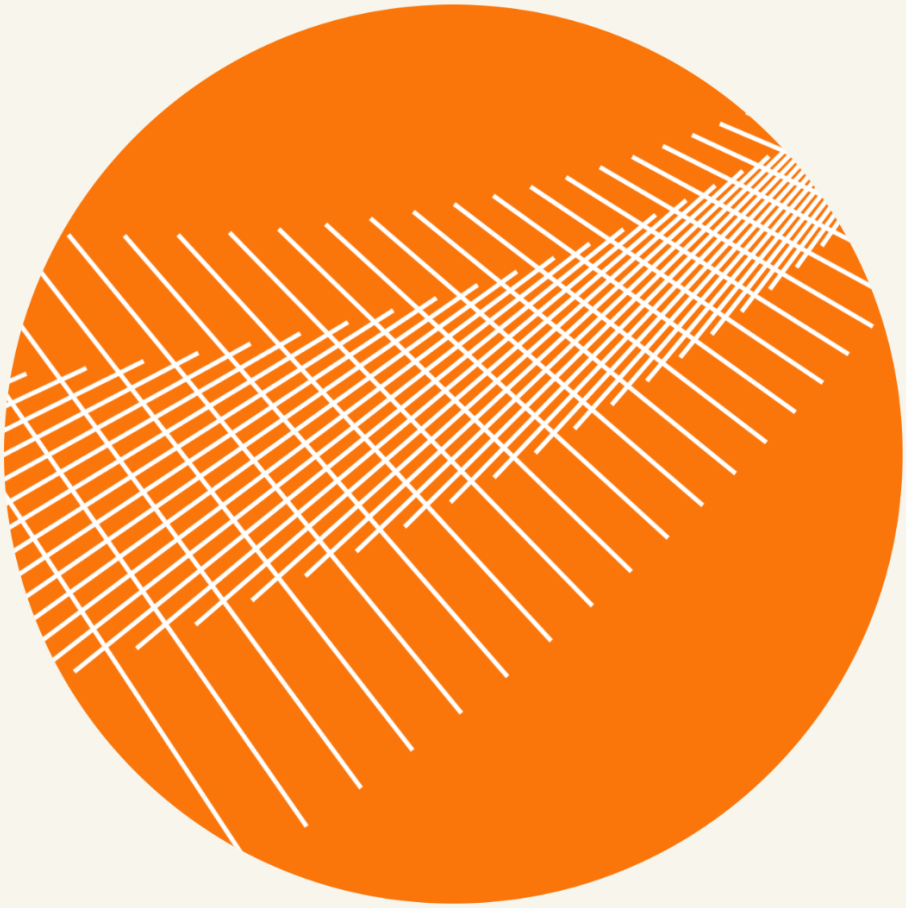
CTDSEC

YOU ARE PROTECTED



TERMS

Table of Contents

1.0 Introduction **3**

1.1 Project engagement 3

1.2 Disclaimer 3

2.0 Coverage **4**

2.1 Target Code and Revision 4

2.2 Attacks made to the contract 5

3.0 Security Issues **7**

3.1 High severity issues [0] 7

3.2 Medium severity issues [0] 7

3.3 Low severity issues [1] 7

4.0 Testing coverage **10**

5.0 Annexes **17**

6.0 Summary of the audit **18**

1.0 Introduction

1.1 Project engagement

During July of 2023, Bitrock team engaged CTDSec to audit smart contracts that they created. The engagement was technical in nature and focused on identifying security flaws in the design and implementation of the contracts. Bitrock provided CTDSec with access to their code repository and whitepaper.

1.2 Disclaimer

It should be noted that this audit is not an endorsement of the reliability or effectiveness of the contract, rather limited to an assessment of the logic and implementation. In order to ensure a secure contract that's able to withstand the network's fast-paced and rapidly changing environment, we at CTDSec recommend that Bitrock team put in place a bug bounty program to encourage further and active analysis of the smart contract.

2.0 Coverage

2.1 Target Code and Revision

Bitrock is a side chain on the Ethereum platform that utilizes the IBFT 2.0 Proof of Authority (PoA) consensus algorithm, offering users low fees and a fast block generation rate of 2 blocks per second. The node contributors in Bitrock are decentralized across various entities. Additionally, Bitrock is based on Hyperledger (Besu), an Ethereum client specifically tailored for public and private networks, keeping it enterprise-friendly. Moreover, Bitrock adheres to the industry best practices and standards set by Besu in its code. Finally, it is important to note that the Bitrock network is implemented in the Java programming language.

The following repository files are considered in-scope for the review:

https://github.com/BitrockChain/BitrockChain

2.2 Attacks made to the contract

In order to check for the security of the contract, we tested several attacks in order to make sure that the contract is secure and follows best practices.

All the tests were passed with no issues.

№	Issue description.	Checking status
1	Compiler warnings.	PASSED
2	Race conditions and Reentrancy. Cross-function race conditions.	PASSED
3	Possible delays in data delivery.	PASSED
4	Oracle calls.	PASSED
5	Front running.	PASSED
6	Timestamp dependence.	PASSED
7	Integer Overflow and Underflow.	PASSED
8	DoS with Revert.	PASSED
9	DoS with block gas limit.	PASSED
10	Methods execution permissions.	PASSED
11	Economy model. If application logic is based on an incorrect economic model, the application would not function correctly and participants would incur financial losses. This type of issue is most often found in bonus rewards systems, Staking and Farming contracts, Vault and Vesting contracts, etc.	PASSED
12	The impact of the exchange rate on the logic.	PASSED
13	Private user data leaks.	PASSED
14	Malicious Event log.	PASSED

15	Scoping and Declarations.	PASSED
16	Uninitialized storage pointers.	PASSED
17	Arithmetic accuracy.	PASSED
18	Design Logic.	PASSED
19	Cross-function race conditions.	PASSED
20	Safe Zeppelin module.	PASSED
21	Fallback function security.	PASSED
22	Overpowered functions / Owner privileges	PASSED

3.0 Security Issues

3.1 High severity issues [0]

No high severity issues found.

3.2 Medium severity issues [0]

No medium severity issues found.

3.3 Low severity issues [1]

1. Testing private keys leaked in the repository

We recommend to delete all the private keys used for testing:

config/src/main/resources/dev.json

```
23      },
24      "627306090abaB3A6e1400e9345bC60c78a8BEf57": {
25        "privateKey": "c87509a1c067bbde78beb793e6fa76530b6382a4c0241e5e4a9ec0a0f44dc0d3",
26        "comment": "private key and this comment are ignored.  In a real chain, the private key should NOT be stored",
27        "balance": "900000000000000000000000"
28      },
29      "f17f52151EbEF6C7334FAD080c5704D77216b732": {
```

config/src/main/resources/experimental.json

```
27      },
28      "627306090abaB3A6e1400e9345bC60c78a8BEf57": {
29        "privateKey": "c87509a1c067bbde78beb793e6fa76530b6382a4c0241e5e4a9ec0a0f44dc0d3",
30        "comment": "private key and this comment are ignored.  In a real chain, the private key should NOT be stored",
31        "balance": "900000000000000000000000"
32      },
33      "f17f52151EbEF6C7334FAD080c5704D77216b732": {
```

testutil/src/main/resources/fork-chain-data/genesis-outdated.json

```
27      },
28      "627306090abaB3A6e1400e9345bC60c78a8BEf57": {
29        "privateKey": "c87509a1c067bbde78beb793e6fa76530b6382a4c0241e5e4a9ec0a0f44dc0d3",
30        "comment": "private key and this comment are ignored.  In a real chain, the private key should NOT be stored",
31        "balance": "900000000000000000000000"
32      },
33      "f17f52151EbEF6C7334FAD080c5704D77216b732": {
```

Show 10 more matches

testutil/src/main/resources/fork-chain-data/genesis-upgraded.json

```
28      },
29      "627306090abaB3A6e1400e9345bC60c78a8BEf57": {
30        "privateKey": "c87509a1c067bbde78beb793e6fa76530b6382a4c0241e5e4a9ec0a0f44dc0d3",
31        "comment": "private key and this comment are ignored.  In a real chain, the private key should NOT be stored",
32        "balance": "900000000000000000000000"
33      },
34      "f17f52151EbEF6C7334FAD080c5704D77216b732": {
```

benchmark/config/caliper-networkconfig-offchain.json

```
5       "ethereum": {
6           "url": "ws://besu:8546",
7           "contractDeployerAddress": "0xD1cf9D73a91DE6630c2bb068Ba5fDdF9F0DEac09",
8           "contractDeployerAddressPrivateKey": "0x797c13f7235c627f6bd013dc17fff4c12213ab49abcf091f77c83f16db10e90b",
9           "fromAddressSeed": "0x3f841bf589fdf83a521e55d51afddc34fa65351161eead24f064855fc29c9580",
10          "transactionConfirmationBlocks": 1,
11          "chainId": 48122,
```

benchmark/config/caliper-networkconfig-onchain.json

```
7         "contractDeployerAddress": "0xD1cf9D73a91DE6630c2bb068Ba5fDdF9F0DEac09",
8         "contractDeployerAddressPrivateKey": "0x797c13f7235c627f6bd013dc17fff4c12213ab49abcf091f77c83f16db10e90b",
9         "fromAddressSeed": "0x3f841bf589fdf83a521e55d51afddc34fa65351161eead24f064855fc29c9580",
15                "privateFrom": "GGilEkXLaQ9yhhtbpBT03Me9iYa7U/mWXxrJhnbl1XY=",
16                "privateKey": "uTJGpd4ZEEtDPFSZM0+GT11xn5NFIr2KGP2Q4SdVPRM="
17            }
```

Show 2 more matches

benchmark/config/genesis.json

```
25        "balance": "0x200000000000000000000000000000000000000000000000000000000000000000000000",
26        "privatekey": "0x797c13f7235c627f6bd013dc17fff4c12213ab49abcf091f77c83f16db10e90b",
27        "derivation": "m/44'/60'/0'/0/0"
50        "balance": "0x200000000000000000000000000000000000000000000000000000000000000000000000",
51        "privatekey": "0x87abeb4c0230ca6fdf42f7d2cb2baa510856e42f039ab7670b13845e45dc3245",
52        "derivation": "m/44'/60'/5'/0/0"
```

config/src/main/resources/future.json

```
26    },
27    "627306090abaB3A6e1400e9345bC60c78a8BEf57": {
28      "privateKey": "c87509a1c067bbde78beb793e6fa76530b6382a4c0241e5e4a9ec0a0f44dc0d3",
29      "comment": "private key and this comment are ignored.  In a real chain, the private key should NOT be stored",
30      "balance": "90000000000000000000000"
31    },
32    "f17f52151EbEF6C7334FAD080c5704D77216b732": {
```

4.0 Testing coverage

During the testing phase, custom use cases were written to cover all the logic of contracts. *Check "5 Annexes" to see the testing code.*

Bitrock tests

Besu:

Test Summary

717 tests	0 failures	3 ignored	2m33.80s duration	100% successful

Ignored tests | **Packages** | Classes

Package	Tests	Failures	Ignored	Duration	Success rate
org.hyperledger.besu	25	0	0	1m5.62s	100%
org.hyperledger.besu.chainexport	8	0	0	0.040s	100%
org.hyperledger.besu.chainimport	16	0	0	5.370s	100%
org.hyperledger.besu.cli	434	0	3	1m6.08s	100%
org.hyperledger.besu.cli.config	6	0	0	0.126s	100%
org.hyperledger.besu.cli.converter	8	0	0	0.008s	100%
org.hyperledger.besu.cli.custom	8	0	0	0.174s	100%
org.hyperledger.besu.cli.operator	23	0	0	1.032s	100%
org.hyperledger.besu.cli.options	65	0	0	10.702s	100%
org.hyperledger.besu.cli.options.stable	3	0	0	0.075s	100%
org.hyperledger.besu.cli.rlp	13	0	0	0.416s	100%
org.hyperledger.besu.cli.subcommands.blocks	26	0	0	0.847s	100%
org.hyperledger.besu.cli.subcommands.storage	5	0	0	0.049s	100%
org.hyperledger.besu.cli.util	10	0	0	0.104s	100%
org.hyperledger.besu.controller	31	0	0	0.875s	100%
org.hyperledger.besu.services	25	0	0	0.156s	100%
org.hyperledger.besu.util	11	0	0	2.133s	100%

Besu_eth:

Test Summary

1573 tests	0 failures	33 ignored	5m24.04s duration

100% successful

Ignored tests | **Packages** | Classes

Package	Tests	Failures	Ignored	Duration	Success rate
org.hyperledger.besu.ethereum.eth	3	0	0	0.008s	100%
org.hyperledger.besu.ethereum.eth.manager	129	0	0	4.476s	100%
org.hyperledger.besu.ethereum.eth.manager.bounded	2	0	0	0.001s	100%
org.hyperledger.besu.ethereum.eth.manager.task	102	0	4	2.065s	100%
org.hyperledger.besu.ethereum.eth.messages	46	0	0	5.232s	100%
org.hyperledger.besu.ethereum.eth.messages.snap	8	0	0	0.162s	100%
org.hyperledger.besu.ethereum.eth.peervalidation	14	0	0	2.396s	100%
org.hyperledger.besu.ethereum.eth.sync	112	0	0	11.580s	100%
org.hyperledger.besu.ethereum.eth.sync.backwardsync	37	0	0	19.867s	100%
org.hyperledger.besu.ethereum.eth.sync.checkpointsync	11	0	0	10.451s	100%
org.hyperledger.besu.ethereum.eth.sync.fastsync	96	0	0	1m3.70s	100%
org.hyperledger.besu.ethereum.eth.sync.fastsync.worldstate	47	0	17	0.130s	100%
org.hyperledger.besu.ethereum.eth.sync.fullsync	53	0	0	1m18.59s	100%
org.hyperledger.besu.ethereum.eth.sync.snapsync	66	0	3	0.391s	100%
org.hyperledger.besu.ethereum.eth.sync.snapsync.request.heal	8	0	0	0.210s	100%
org.hyperledger.besu.ethereum.eth.sync.state	32	0	0	3.597s	100%
org.hyperledger.besu.ethereum.eth.sync.state.cache	5	0	0	0.090s	100%
org.hyperledger.besu.ethereum.eth.sync.tasks	276	0	1	1m1.77s	100%
org.hyperledger.besu.ethereum.eth.transactions	193	0	7	42.857s	100%
org.hyperledger.besu.ethereum.eth.transactions.layered	251	0	1	16.012s	100%
org.hyperledger.besu.ethereum.eth.transactions.sorter	82	0	0	0.468s	100%

Conensus_ibft:

Test Summary

207	0	0	23.494s
tests	failures	ignored	duration

100% successful

Packages Classes

Package	Tests	Failures	Ignored	Duration	Success rate
org.hyperledger.besu.consensus.ibft	39	0	0	16.280s	100%
org.hyperledger.besu.consensus.ibft.blockcreation	1	0	0	1.543s	100%
org.hyperledger.besu.consensus.ibft.jsonrpc.methods	28	0	0	2.538s	100%
org.hyperledger.besu.consensus.ibft.messagedata	16	0	0	0.694s	100%
org.hyperledger.besu.consensus.ibft.payload	10	0	0	0.217s	100%
org.hyperledger.besu.consensus.ibft.protocol	3	0	0	0.001s	100%
org.hyperledger.besu.consensus.ibft.statemachine	67	0	0	1.508s	100%
org.hyperledger.besu.consensus.ibft.validation	43	0	0	0.713s	100%

Algorithm:

Test Summary

116	0	0	2m15.72s
tests	failures	ignored	duration

100% successful

Packages Classes

Package	Tests	Failures	Ignored	Duration	Success rate
org.hyperledger.besu.crypto	55	0	0	2m9.49s	100%
org.hyperledger.besu.crypto.altbn128	61	0	0	6.236s	100%

eth_api_v1:

Test Summary

3429 tests	0 failures	5 ignored	6m38.25s duration	100% successful

Ignored tests | **Packages** | Classes

Package	Tests	Failures	Ignored	Duration	Success rate
org.hyperledger.besu.ethereum.api.graphql	94	0	0	17.244s	100%
org.hyperledger.besu.ethereum.api.graphql.scalar	36	0	0	0.382s	100%
org.hyperledger.besu.ethereum.api.jsonrpc	166	0	1	16.143s	100%
org.hyperledger.besu.ethereum.api.jsonrpc.authentication	39	0	0	4.072s	100%
org.hyperledger.besu.ethereum.api.jsonrpc.bonsai	1008	0	0	3m7.43s	100%
org.hyperledger.besu.ethereum.api.jsonrpc.context	3	0	0	0.002s	100%
org.hyperledger.besu.ethereum.api.jsonrpc.forest	1026	0	0	2m28.09s	100%
org.hyperledger.besu.ethereum.api.jsonrpc.health	10	0	0	0.025s	100%
org.hyperledger.besu.ethereum.api.jsonrpc.internal	4	0	1	0.491s	100%
org.hyperledger.besu.ethereum.api.jsonrpc.internal.filter	72	0	0	2.209s	100%
org.hyperledger.besu.ethereum.api.jsonrpc.internal.methods	311	0	0	5.507s	100%
org.hyperledger.besu.ethereum.api.jsonrpc.internal.methods.engine	135	0	2	1.932s	100%
org.hyperledger.besu.ethereum.api.jsonrpc.internal.methods.miner	16	0	0	0.069s	100%
org.hyperledger.besu.ethereum.api.jsonrpc.internal.methods.permissioning	82	0	0	0.057s	100%
org.hyperledger.besu.ethereum.api.jsonrpc.internal.parameters	43	0	0	0.118s	100%
org.hyperledger.besu.ethereum.api.jsonrpc.internal.privacy.methods	6	0	0	0.036s	100%
org.hyperledger.besu.ethereum.api.jsonrpc.internal.privacy.methods.eea	26	0	0	0.376s	100%

eth_api_v2:

org.hyperledger.besu.ethereum.api.jsonrpc.internal.privacy.methods.priv	85	0	0	0.716s	100%
org.hyperledger.besu.ethereum.api.jsonrpc.internal.privacy.methods.privx	3	0	0	0.009s	100%
org.hyperledger.besu.ethereum.api.jsonrpc.internal.processor	8	0	0	0.199s	100%
org.hyperledger.besu.ethereum.api.jsonrpc.internal.results	6	0	0	0.021s	100%
org.hyperledger.besu.ethereum.api.jsonrpc.internal.results.tracing.flat	3	0	0	0.107s	100%
org.hyperledger.besu.ethereum.api.jsonrpc.internal.results.transaction.pool	21	0	0	0.064s	100%
org.hyperledger.besu.ethereum.api.jsonrpc.ipc	5	0	0	0.484s	100%
org.hyperledger.besu.ethereum.api.jsonrpc.methods	14	0	0	0.107s	100%
org.hyperledger.besu.ethereum.api.jsonrpc.parameters	3	0	0	0.029s	100%
org.hyperledger.besu.ethereum.api.jsonrpc.timeout	3	0	0	0.124s	100%
org.hyperledger.besu.ethereum.api.jsonrpc.websocket	49	0	0	2.602s	100%
org.hyperledger.besu.ethereum.api.jsonrpc.websocket.methods	25	0	0	0.651s	100%
org.hyperledger.besu.ethereum.api.jsonrpc.websocket.subscription	24	0	1	5.018s	100%
org.hyperledger.besu.ethereum.api.jsonrpc.websocket.subscription.blockheaders	6	0	0	0.425s	100%
org.hyperledger.besu.ethereum.api.jsonrpc.websocket.subscription.logs	9	0	0	0.258s	100%
org.hyperledger.besu.ethereum.api.jsonrpc.websocket.subscription.pending	3	0	0	0.083s	100%
org.hyperledger.besu.ethereum.api.jsonrpc.websocket.subscription.request	22	0	0	0.018s	100%
org.hyperledger.besu.ethereum.api.jsonrpc.websocket.subscription.syncing	2	0	0	0.007s	100%
org.hyperledger.besu.ethereum.api.query	51	0	0	1.209s	100%
org.hyperledger.besu.ethereum.api.query.cache	5	0	0	1.934s	100%
org.hyperledger.besu.ethereum.api.tls	3	0	0	0.004s	100%
org.hyperledger.besu.ethereum.api.util	2	0	0	0.004s	100%

eth_block_creation:

Test Summary

66 tests	0 failures	0 ignored	25.825s duration	100% successful

Packages **Classes**

Class	Tests	Failures	Ignored	Duration	Success
org.hyperledger.besu.ethereum.blockcreation.AbstractMiningCoordinatorTest	14	0	0	3.024s	100%
org.hyperledger.besu.ethereum.blockcreation.BlockMinerTest	2	0	0	2.920s	100%
org.hyperledger.besu.ethereum.blockcreation.DefaultBlockSchedulerTest	4	0	0	0.029s	100%
org.hyperledger.besu.ethereum.blockcreation.HashRateMiningCoordinatorTest	4	0	0	3.035s	100%
org.hyperledger.besu.ethereum.blockcreation.IncrementingNonceGeneratorTest	2	0	0	0.166s	100%
org.hyperledger.besu.ethereum.blockcreation.LegacyFeeMarketBlockTransactionSelectorTest	12	0	0	3.246s	100%
org.hyperledger.besu.ethereum.blockcreation.LondonFeeMarketBlockTransactionSelectorTest	16	0	0	3.164s	100%
org.hyperledger.besu.ethereum.blockcreation.PoWBlockCreatorTest	8	0	0	5.121s	100%
org.hyperledger.besu.ethereum.blockcreation.PoWMinerExecutorTest	2	0	0	0.059s	100%
org.hyperledger.besu.ethereum.blockcreation.PoWMiningCoordinatorTest	2	0	0	5.061s	100%

eth_core:

Test Summary

950	0	127	45.690s
tests	failures	ignored	duration

100% successful

Ignored tests | **Packages** | Classes

Package	Tests	Failures	Ignored	Duration	Success rate
org.hyperledger.besu.ethereum	14	0	0	4.254s	100%
org.hyperledger.besu.ethereum.bonsai	60	0	6	2.903s	100%
org.hyperledger.besu.ethereum.bonsai.trielog	6	0	0	0.806s	100%
org.hyperledger.besu.ethereum.chain	30	0	0	14.569s	100%
org.hyperledger.besu.ethereum.core	16	0	0	0.091s	100%
org.hyperledger.besu.ethereum.core.encoding	19	0	0	3.302s	100%
org.hyperledger.besu.ethereum.core.feemarket	138	0	121	0.017s	100%
org.hyperledger.besu.ethereum.difficulty.fixed	1	0	0	0.007s	100%
org.hyperledger.besu.ethereum.forkid	70	0	0	0.322s	100%
org.hyperledger.besu.ethereum.mainnet	216	0	0	7.321s	100%
org.hyperledger.besu.ethereum.mainnet.feemarket	18	0	0	0.018s	100%
org.hyperledger.besu.ethereum.mainnet.headervalidationrules	94	0	0	3.196s	100%
org.hyperledger.besu.ethereum.mainnet.precompiles.privacy	22	0	0	0.928s	100%
org.hyperledger.besu.ethereum.privacy	92	0	0	0.505s	100%
org.hyperledger.besu.ethereum.privacy.markertransaction	2	0	0	0.034s	100%
org.hyperledger.besu.ethereum.privacy.storage	4	0	0	0.001s	100%
org.hyperledger.besu.ethereum.privacy.storage.migration	6	0	0	0.099s	100%
org.hyperledger.besu.ethereum.proof	8	0	0	0.030s	100%
org.hyperledger.besu.ethereum.storage.keyvalue	20	0	0	0.032s	100%
org.hyperledger.besu.ethereum.transaction	21	0	0	0.081s	100%
org.hyperledger.besu.ethereum.util	13	0	0	4.783s	100%
org.hyperledger.besu.ethereum.vm	42	0	0	0.994s	100%
org.hyperledger.besu.ethereum.worldstate	38	0	0	1.397s	100%

eth_p2p:

Test Summary

429	0	1	34.262s
tests	failures	ignored	duration

100% successful

Ignored tests | **Packages** | Classes

Package	Tests	Failures	Ignored	Duration	Success rate
org.hyperledger.besu.ethereum.p2p.config	2	0	0	0.052s	100%
org.hyperledger.besu.ethereum.p2p.discovery	44	0	0	14.908s	100%
org.hyperledger.besu.ethereum.p2p.discovery.internal	134	0	0	4.687s	100%
org.hyperledger.besu.ethereum.p2p.network	45	0	1	4.516s	100%
org.hyperledger.besu.ethereum.p2p.peers	100	0	0	2.626s	100%
org.hyperledger.besu.ethereum.p2p.permissions	13	0	0	0.083s	100%
org.hyperledger.besu.ethereum.p2p.plain	3	0	0	0.004s	100%
org.hyperledger.besu.ethereum.p2p.rlpx	26	0	0	0.309s	100%
org.hyperledger.besu.ethereum.p2p.rlpx.connections	6	0	0	0.074s	100%
org.hyperledger.besu.ethereum.p2p.rlpx.connections.netty	24	0	0	6.077s	100%
org.hyperledger.besu.ethereum.p2p.rlpx.framing	18	0	0	0.628s	100%
org.hyperledger.besu.ethereum.p2p.rlpx.handshake.ecies	5	0	0	0.262s	100%
org.hyperledger.besu.ethereum.p2p.rlpx.wire	3	0	0	0.035s	100%
org.hyperledger.besu.ethereum.p2p.rlpx.wire.messages	6	0	0	0.001s	100%

EVM:

Test Summary

3641	0	5	17.697s
tests	failures	ignored	duration

100% successful

Ignored tests | **Packages** | Classes

Package	Tests	Failures	Ignored	Duration	Success rate
org.hyperledger.besu.evm	1	0	0	1.465s	100%
org.hyperledger.besu.evm.code	2128	0	0	2.863s	100%
org.hyperledger.besu.evm.internal	22	0	0	0.219s	100%
org.hyperledger.besu.evm.log	1	0	0	0.521s	100%
org.hyperledger.besu.evm.operations	245	0	0	8.455s	100%
org.hyperledger.besu.evm.precompile	1232	0	5	4.150s	100%
org.hyperledger.besu.evm.processor	12	0	0	0.024s	100%

5.0 Annexes

The testing code for the Java-based repository was shared with the team in the form of a .zip file. This was necessary because there were numerous classes and lines of code to be included, which would have made it cumbersome to directly add them to the report.

BitrockBlockchain_testing.rar [SHA256]:

43d7d927321d4242eecf51efb58d281b1fb7dc7de93b8f801b4ddebc5ac0f2ac

6.0 Summary of the audit

All the tests executed to the main branch were 100% successful and 0 vulnerabilities were found.

*No high or medium criticality vulnerabilities were identified within the Bitrock Java code during the thorough security assessment. CTDSEC team also worked with the team to securize the infrastructure where the nodes and exposed &/OR internal services are running.

*To maintain the network as secure as possible, we will be implementing a continuous code review and infrastructure analysis, along with monitoring to detect potential bugs, errors, and threats.

*As the blockchain is based on Java code must be reviewed frequently to avoid additional bugs that can be added in new commits or new vulnerabilities that can appear with the code/infrastructure itself.