Bytom2.0 Security Audit Report

Contents

11. Executive Summary

On August 20, 2021, the SlowMist security team received the Bytom team's security audit application for Bytom2.0, developed the audit plan according to the agreement of both parties and the characteristics of the project, and finally issued the security audit report.

The SlowMist security team adopts the strategy of "black, grey box lead, white box assists" to conduct a complete security test on the project in the way closest to the real attack.

SlowMist blockchain system test method:

Black box testing	Conduct security tests from an attacker's perspective externally.
Grey box testing	Conduct security testing on code module through the scripting tool, observing the internal running status, mining weaknesses.
White box testing	Based on the open source code, non-open source code, to detect wether there are vulnerabilities in programs suck as nodes, SDK, etc.

SlowMist blockchain risk level:

Critical vulnerabilities	Critical vulnerabilities will have a significant impact on the security of the blockchain, and it is strongly recommended to fix the critical vulnerabilities.
High-risk	High-risk vulnerabilities will affect the normal operation of blockchain. It is

vulnerabilities	strongly recommended to fix high-risk vulnerabilities.
Medium-risk vulnerablities	Medium vulnerability will affect the operation of blockchain. It is recommended to fix medium-risk vulnerabilities.
Low-risk vulnerabilities	Low-risk vulnerabilities may affect the operation of blockchain in certain scenarios. It is suggested that the project party should evaluate and consider whether these vulnerabilities need to be fixed.
Weaknesses	There are safety risks theoretically, but it is extremely difficult to reproduce in engineering.
Enhancement Suggestions	There are better practices for coding or architecture.

2. Project Background (Context)

2.1 Project Introduction

Project Website: https://bytom.io

Coin Symbol: BTM

Project source code: https://github.com/Bytom/bytom

Audit version: v2.0.4

2.2 Scope of Audit

The main types of security audit include:

(other unknown security vulnerabilities are not included in the scope of responsibility of this audit)

No.	Audit Category	Audit Result
1	Random Number Generation Algorithm Audit	PASSED
2	Keystore Audit	PASSED
3	Cryptographic Component Call Audit	PASSED
4	Encryption Strength Audit	PASSED
5	Length Extension Attack Audit	PASSED
6	Transaction Malleability Attack Audit	PASSED
7	Replay Attack Audit	PASSED
8	Top-up Program Audit	PASSED
9	RPC Permission Audit	PASSED

3. Code Overview

3.1 Infrastructure

Bytom2.0 is based on PoS + BBFT consensus algorithm, based on UTXO transaction model.

3.2 Random Number Generation Algorithm Audit

The generation of the private key seed is based on the `crypto/rand` standard library, and the entropy value is secure.

- bytom/crypto/randentropy/rand_entropy.go

```
func GetEntropyCSPRNG(n int) []byte {
mainBuff := make([]byte, n)
_, err := io.ReadFull(crand.Reader, mainBuff)
if err != nil {
panic("reading from crypto/rand failed: " + err.Error())
}
return mainBuff
}
```

3.3 Keystore Audit

Use the keystore to encrypt the storage, and the password strength is not verified. Weak passwords such as `123456` can be used in the test, which can be easily cracked.

3.4 Cryptographic Component Call Audit

Signature algorithm: Ed25519, based on Golang standard library crypto/ed25519.

Hash algorithm: SHA256, based on Golang standard library crypto/sha256.

No security risks have been found.

3.5 Encryption Strength Audit

Weak hash functions such as md5 and sha1 are not used.

3.6 Length Extension Attack Audit

In cryptography and computer security, a length extension attack is a type of attack where an attacker can use Hash(message1) and the length of message1 to calculate Hash(message1 ‖ message2) for an attacker-controlled message2, without needing to know the content of message1. Algorithms like MD5, SHA-1, and SHA-2 that are based on the Merkle－Damgard construction are susceptible to this kind of attack. The SHA-3 algorithm is not susceptible.

No error calls were found.

3.7 Transaction Malleability Attack Audit

The ECDSA algorithm generates two large integers r and s combined as a signature, which can be used to verify transactions. And r and BN-s can also be used as signatures to verify transactions. In this way, the attacker gets a transaction, extracts the r and s of inputSig, uses r, BN-s to generate a new inputSig, and then forms a new transaction with the same input and output, but different TXID. Attacker Can successfully generate legal transactions at almost no cost without having the private key.

Bytom2.0 uses the ed25519 algorithm to sign, in the algorithm design of ED25519, by using a cryptographic hash function to replace the pseudo-random number generator, it avoids the security problems that the users of the signature algorithm use because the random number generator used is not random enough. In addition to the generation of the private key, the implementation of ED25519 has completely departed from the dependence on the random number generator, avoiding the leakage and security problems of the key due to the randomization problem.

No error calls were found.

Reference：https://en.bitcoinwiki.org/wiki/Transaction_Malleability

3.8 Transaction Replay Attack Audit

The account transaction mechanism designed based on UTXO model, the transaction depends on the unspent transaction. When we repeatedly submit a transaction, we can see that the UTXO that has been spent cannot be repeatedly spent:

```
$ ./bytomcli build-transaction --alias testacc BTM 1 --type spend --receiver
0014cc993c76335b9ec61e43d45e3390ca932d6e0be4
{"allow_additional_actions":false,"fee":20000000,"raw_transaction":"070100010161015f994d3009931a783392d84778d8f
a09558708cf8628fe7b79cc4a87fb4b20bec6ffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffff80c8afa0250101160014cf7c
95ad9faaf5ff2e493ce9c2813385582ae5d30001000201003effffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffedea96250
1160014cf7c95ad9faaf5ff2e493ce9c2813385582ae5d3000001003affffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffff0101
160014cc993c76335b9ec61e43d45e3390ca932d6e0be40000","signing_instructions":[{"position":0,"witness_components
":[{"keys":[{"derivation_path":["2c000000","99000000","01000000","00000000","01000000"],"xpub":"9bdc265cf79afce1b
3db948ee988d8d8e066ed1d09abd6c533c79af98edfa1069409912ce54d1777b98f62c3bf19eca7def5e176c248a28d6f1
bccd1532bb541"}],"quorum":1,"signatures":null,"type":"raw_tx_signature"},{"type":"data","value":"0c8d89a673af6c7a582e0
b71b680479c4fd0567f4d32e1a4d945b854f3c988e6"}]}]}
$ ./bytomcli sign-transaction
'{"allow_additional_actions":false,"fee":20000000,"raw_transaction":"070100010161015ff7346b6dcc5b0720e7e54e7f29c
2031724433ca7892426abaaa6c61df69e5a3affffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffff80c8afa0250101160014cf7
c95ad9faaf5ff2e493ce9c2813385582ae5d30001000201003effffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffedea9625
01160014cf7c95ad9faaf5ff2e493ce9c2813385582ae5d3000001003affffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffff010
1160014cc993c76335b9ec61e43d45e3390ca932d6e0be40000","signing_instructions":[{"position":0,"witness_component
s":[{"keys":[{"derivation_path":["2c000000","99000000","01000000","00000000","01000000"],"xpub":"9bdc265cf79afce1b
3db948ee988d8d8e066ed1d09abd6c533c79af98edfa1069409912ce54d1777b98f62c3bf19eca7def5e176c248a28d6f1
bccd1532bb541"}],"quorum":1,"signatures":null,"type":"raw_tx_signature"},{"type":"data","value":"0c8d89a673af6c7a582e0
b71b680479c4fd0567f4d32e1a4d945b854f3c988e6"}]}]}' --password 123456
$ curl -X POST http://localhost:9888/submit-transaction -d
'{"raw_transaction":"070100010161015ff7346b6dcc5b0720e7e54e7f29c2031724433ca7892426abaaa6c61df69e5a3afff
ffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffff80c8afa0250101160014cf7c95ad9faaf5ff2e493ce9c2813385582ae5d3006
302406349ea08682c4a4d5313bb7ee68fdc031a7812f1dec6e2636d82bb4ca509a1c56880739bfee2c78f058950c7d3a4
1eecba8e15ace2668aac6d8d5c4bc8849b06200c8d89a673af6c7a582e0b71b680479c4fd0567f4d32e1a4d945b854f3c9
88e60201003effffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffedea962501160014cf7c95ad9faaf5ff2e493ce9c281338
5582ae5d3000001003affffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffff0101160014cc993c76335b9ec61e43d45e3390c
a932d6e0be40000"}'
{"status":"success","data":{"tx_id":"bc2b5f4a8b9c8a874c41f1637fd76965ade719e18c4413ce8ba37c4dce96480d"}}
Send repeatedly:
{"status":"fail","code":"BTM712","msg":"Transaction input UTXO not found","error_detail":"finalize can't find transaction input
utxo"}
```

The same UTXO does not exist between different chains, so there is no replay attack problem for transactions between different chains.

3.9 Top-up Program Audit

View a normal transfer transaction:


```
$ curl -X POST http://localhost:9888/get-transaction -d '{"tx_id":
"bc2b5f4a8b9c8a874c41f1637fd76965ade719e18c4413ce8ba37c4dce96480d"}'
{
    "status": "success",
    "data":
    {
        "tx_id": "bc2b5f4a8b9c8a874c41f1637fd76965ade719e18c4413ce8ba37c4dce96480d",
        "block_time": 1629887940000,
        "block_hash": "653d4fba08cb6014d53852f5b29b7734be0df8a003120bf9ce003c68fe8dbc58",
        "block_height": 31405,
        "block_index": 1,
        "block_transactions_count": 2,
        "inputs": [
        {
            "type": "spend",
            "asset_id": "ffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffff",
            "asset_alias": "BTM",
            "asset_definition":
            {
                "decimals": 8,
                "description": "Bytom Official Issue",
                "name": "BTM",
                "symbol": "BTM"
            },
            "amount": 10000000000,
            "control_program": "0014cf7c95ad9faaf5ff2e493ce9c2813385582ae5d3",
            "address": "tn1qea7fttvl4t6l7tjf8n5u9qfns4vz4ewn0sfahk",
            "spent_output_id": "ed444b679953d360669bee9b8424549ac9618a45f8ed13e8f1b62ba90eca1582",
            "account_id": "1869f184-42f2-4fe5-a4ca-8a82a804bb66",
            "account_alias": "testacc",
            "input_id": "7668eb0cbbf7e31f44d67370624a491e66e5b29f51cd81bf22b07ceb06372730",
            "witness_arguments":
["6349ea08682c4a4d5313bb7ee68fdc031a7812f1dec6e2636d82bb4ca509a1c56880739bfee2c78f058950c7d3a41eec
```

```
ba8e15ace2668aac6d8d5c4bc8849b06",
"0c8d89a673af6c7a582e0b71b680479c4fd0567f4d32e1a4d945b854f3c988e6"],
            "sign_data": "65d9afa3038336b8602cadb98423b95ed5e0f4ffd9fcebec12e54d0ee77bd523"
        }],
        "outputs": [
        {
            "type": "control",
            "id": "4b2608f49aed2376b4490be281b3fb483caf5875503518ddb1bc1e67aff4f6f7",
            "position": 0,
            "asset_id": "ffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffff",
            "asset_alias": "BTM",
            "asset_definition":
            {
                "decimals": 8,
                "description": "Bytom Official Issue",
                "name": "BTM",
                "symbol": "BTM"
            },
            "amount": 9979999999,
            "account_id": "1869f184-42f2-4fe5-a4ca-8a82a804bb66",
            "account_alias": "testacc",
            "control_program": "0014cf7c95ad9faaf5ff2e493ce9c2813385582ae5d3",
            "address": "tn1qea7fttvl4t6l7tjf8n5u9qfns4vz4ewn0sfahk"
        },
        {
            "type": "control",
            "id": "d87fc9875a3091b561799b4c26f96fc050abf7d399b8394fb3188d974621523f",
            "position": 1,
            "asset_id": "ffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffff",
            "asset_alias": "BTM",
            "asset_definition":
            {
                "decimals": 8,
                "description": "Bytom Official Issue",
                "name": "BTM",
                "symbol": "BTM"
            },
            "amount": 1,
            "account_id": "5f8787b1-9ed2-48c8-b26c-963655507c04",
            "account_alias": "test",
            "control_program": "0014cc993c76335b9ec61e43d45e3390ca932d6e0be4",
            "address": "tn1qejvnca3ntw0vv8jr630r8yx2jvkkuzlyj9n5gx"
```

```
        }],
        "size": 332
    }
}
```

When the exchange retrieves the recharge transaction, it needs to strictly verify the `status` equal to "success" and the value of asset_id, amount, control_program, and address in the outputs to avoid false top-up vulnerability .

3.10 RPC Permission Audit

RPC has a wallet function, there are RPC "Black Valentine's Day Vulnerabilities", which can lead to node privacy disclosure or asset theft.

Vulnerability reference: https://mp.weixin.qq.com/s/Kk2IsoQ1679Gda56Ec-zJg

4. Audit Result

4.1 Low-risk Vulnerabilitys

- Weak passwords can be used in the keystore, which can be easily cracked.

4.2 Enhancement Suggestions

- It is recommended to open RPC ports locally.

4.3 Exchange Suggestions

- The exchange should check all relevant fields in the transaction, and real-time reconciliation with the total balance of the account. If an abnormality occurs, it needs to be manually checked before processing the entry to prevent "false top-up attacks."

- It is forbidden to open the RPC interface to the WAN to prevent node privacy leakage or asset theft.
- The main chain natively supports multiple assets, and the exchange should pay attention to distinguishing asset_id when depositing funds.

4.4 Conclusion

Audit result: PASSED

Audit No. : BCA002108260001

Audit date: August 26, 2021

Audit team: SlowMist security team

Summary conclusion: After correction, all problems found have been fixed and the above risks have been eliminated by Bytom2.0. Comprehensive assessed, Bytom2.0 has no risks above already.

5. Statement

SlowMist issues this report with reference to the facts that have occurred or existed before the issuance of this report, and only assumes corresponding responsibility base on these.
For the facts that occurred or existed after the issuance, SlowMist is not able to judge the security status of this project, and is not responsible for them. The security audit analysis and other contents of this report are based on the documents and materials provided to SlowMist by the information provider till the date of the insurance this report (referred to as "provided information"). SlowMist assumes: The information provided is not missing, tampered with, deleted or concealed. If the information provided is missing, tampered with, deleted, concealed, or inconsistent with the actual situation, the SlowMist shall not be liable for any loss or adverse effect resulting therefrom. SlowMist only conducts the agreed security audit on the security situation of the project and issues this report. SlowMist is not responsible for the background and other conditions of the project.

Official Website
www.slowmist.com

E-mail
team@slowmist.com

Twitter
@SlowMist_Team

Github
https://github.com/slowmist