MOVEBIT
Securing the Move Ecosystem

AptoPad Aptos Contracts Audit Report

https://twitter.com/movebit_

contact@movebit.xyz

AptoPad Aptos Contracts Audit Report

1 Executive Summary

1.1 Project Information

Type	LaunchPad
Auditors	MoveBit
Timeline	2023-2-21 to 2023-2-24
Languages	Move
Methods	Architecture Review, Unit Testing, Formal Verification, Manual Review
Source Code	Repository: https://github.com/Aptopad-io/Aptopad-Coin Received Commit: 9d697e9aa21a339d777240cebf5e7ba46917a5be Last Reviewed Commit: 6e94b2e92d54d4c0039f2957d7f91d61c942d3b7
Updates	

1.2 Issue Statistic

Item	Count	Fixed	Pending	Confirmed
Total	2	1		1
Minor				
Medium	2	1		1

Major				
Critical				

1.3 Issue Level

- **Minor** issues are general suggestions relevant to best practices and readability. They don't post any direct risk. Developers are encouraged to fix them.
- **Medium** issues are non-exploitable problems and not security vulnerabilities. They should be fixed unless there is a specific reason not to.
- **Major** issues are security vulnerabilities. They put a portion of users' sensitive information at risk, and often are not directly exploitable. All major issues should be fixed.
- **Critical** issues are directly exploitable security vulnerabilities. They put users' sensitive information at risk. All critical issues should be fixed.

1.4 Issue Status

- **Fixed:** The issue has been resolved.
- **Pending:** The issue has been acknowledged by the code owner, but has not yet been resolved. The code owner may take action to fix it in the future.
- **Confirmed:** The issue has been acknowledged by the code owner, and the code owner confirms it's as designed, and decides to keep it.

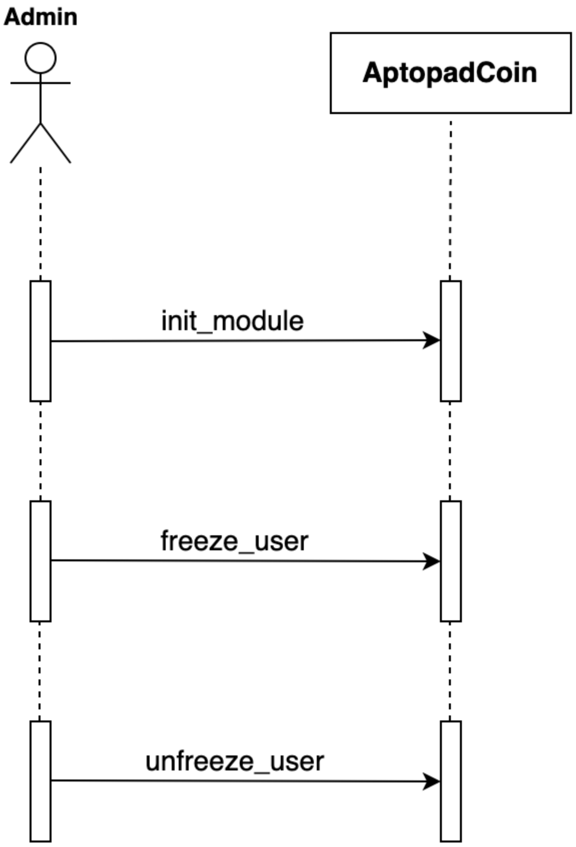
2 Summary of Findings

AptoPad is the best decentralized launchpad on the Aptos Network. With Aptos building the safest and most scalable Layer 1 blockchain for the million users, AptoPad is engineered from the ground up to empower Aptos project owners, by offering a strategized token launch experience with customized launch model, time period, accepted token types and auction algorithms. Our team read the design documents on https://www.aptopad.io/whitepaper.pdf and reviewed the code of the AptoPad project. The audit team mainly focused on reviewing the code security and normative. Our team has been in close contact with the developing team for the past few days. As a result, our team found a total of 2 issues. The teams have discussed these issues together, and the development team has addressed these issues.

The following are the main roles in the smart contract with their respective capabilities:

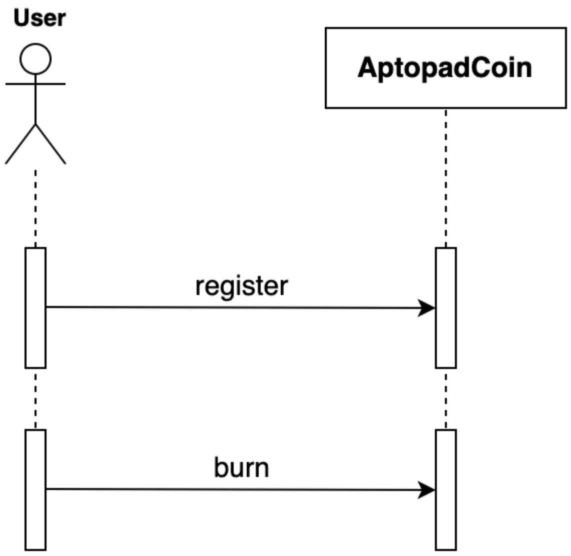
(1) Admin

- Admin can initialize the AptopadCoin module.
- Admin can freeze users.
- Admin can unfreeze users.



(2) User

- User can register APD coins.
- User can burn coins from self.



3 MoveBit Audit BreakDown

MoveBit aims to assess repositories for security-related issues, code quality, and compliance with specifications and best practices. Possible issues we looked for included (but are not limited to):

- Transaction-ordering dependence
- Timestamp dependence
- Integer overflow/underflow by bit operations
- Number of rounding errors
- Denial of service / logical oversights
- Access control
- Centralization of power
- Business logic contradicting the specification
- Code clones, functionality duplication
- Gas usage
- Arbitrary token minting
- Unchecked CALL Return Values
- The flow of capability
- Witness Type

4 Methodology

The security team adopted the "**Testing and Automated Analysis**", "**Code Review**" and "**Formal Verification**" strategy to perform a complete security test on the code in a way that is closest to the real attack. The main entrance and scope of security testing are in the conventions in the "Audit Objective", and that can expand to the context beyond the scope according to the actual testing needs. The main types of this security audit include:

(1) Testing and Automated Analysis

Items to check: state consistency / failure rollback / unit testing / value overflows / parameter verification / unhandled errors / boundary checking / coding specifications.

(2) Code Review

Code scope sees **Appendix 1**.

(3) Formal Verification

Perform formal verification for key functions with the Move Prover.

(4) Audit Process

- Carry out relevant security tests on the testnet or the mainnet;
- If there are any questions during the audit process, communicate with the code owner in time, and they should actively cooperate (which may include the latest stable source code, relevant deployment scripts or methods, transaction signature scripts, exchange docking schemes, etc.);
- The necessary information during the audit process will be well documented for both the audit team and the code owner in time.

5 Findings

5.1 The admin account can freeze any user's account

Severity: Medium

Status: Confirmed

Descriptions: The admin account can freeze any user's account. This means that the user can't withdraw or transfer their APD coins. And the admin account has large power. If its private key is lost, it can cause great damage.

Code Location: Aptopad-Coin-main/sources/aptopad.move, line 61, 70.

aptopad.move

```
    public entry fun freeze_user(account: &signer, user: address) acquires CoinCapabilities {
        let account_addr = signer::address_of(account);
        is_admin(account_addr);
        have_coin_capabilities(account_addr);

        let freeze_cap = &borrow_global<CoinCapabilities>(@admin).freeze_cap;
        coin::freeze_coin_store<APD>(user, freeze_cap);
    }

    public entry fun unfreeze_user(account: &signer, user: address) acquires CoinCapabilities {
        let account_addr = signer::address_of(account);
        is_admin(account_addr);
        have_coin_capabilities(account_addr);

        let freeze_cap = &borrow_global<CoinCapabilities>(@admin).freeze_cap;
        coin::unfreeze_coin_store<APD>(user, freeze_cap);
    }
```

Suggestion: Use a multi-signature account or set up a governance committee to manage the relevant accounts.

Confirmed: Communicated with the developer team, and they designed it in this way, and they already deployed the contract on Aptos mainnet, so they decided to keep this behavior to manage potential malicious users and avoid losses.

5.2 Change the rev dependency to the git version number

Severity: Medium

Status: Fixed

Descriptions: In the `Move.toml` file, the dependent third-party code version is the corresponding branch, and that branch may have ongoing development updates. Each time the current project is compiled and deployed, the third-party code it depends on may be different, so it is recommended to change it to the appropriate git commit version number.

Code Location: Aptopad-Coin-main/Move.toml line 6.

Move.toml

```
[dependencies.AptosFramework]
git = 'https://github.com/aptos-labs/aptos-core.git'
rev = 'devnet'
subdir = 'aptos-move/framework/aptos-framework'
```

Suggestion: Modify the `rev` to the git version number. The latest git version of AptosFramework on the mainnet branch is 62ce8809dbff3d9fcb75079c7540465cb664391a

Move.toml

```
[dependencies.AptosFramework]
git = 'https://github.com/aptos-labs/aptos-core.git'
rev = '62ce8809dbff3d9fcb75079c7540465cb664391a'
subdir = 'aptos-move/framework/aptos-framework'
```

Solved: Updated in 6e94b2e92d54d4c0039f2957d7f91d61c942d3b7.

Appendix 1 – Files in Scope

The following are the SHA1 hashes of the last reviewed files.

Files	SHA-1 Hash
Aptopad-Coin-main/sources/aptopad.move	4aed84f56b21596eca5186dc8c8d815c59ff3a04
Aptopad-Coin-main/Move.toml	8844cd6165e5a4324ae85c9707f0c09285d5bc55

Appendix 2 – Disclaimer

This report is based on the scope of materials and documents provided, with a limited review at the time provided. Results may not be complete and do not include all vulnerabilities. The review and this report are provided on an as-is, where-is, and as-available basis. You agree that your access and/or use, including but not limited to any associated services, products, protocols, platforms, content, and materials, will be at your own risk. A report does not imply an endorsement of any particular project or team, nor does it guarantee its security. These reports should not be relied upon in any way by any third party, including for the purpose of making any decision to buy or sell products, services, or any other assets. TO THE FULLEST EXTENT PERMITTED BY LAW, WE DISCLAIM ALL WARRANTIES, EXPRESS OR IMPLIED, IN CONNECTION WITH THIS REPORT, ITS CONTENT, RELATED SERVICES AND PRODUCTS, AND YOUR USE, INCLUDING BUT NOT LIMITED TO THE IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, NOT INFRINGEMENT.

MOVEBIT

Securing the Move Ecosystem

https://twitter.com/movebit_

contact@movebit.xyz