BEOSIN
Web3 Security & Compliance

JP Gold Coin

Smart Contract Security Audit

No. 202506261010

Jun 26th, 2025

SECURING BLOCKCHAIN ECOSYSTEM

WWW.BEOSIN.COM

Contents

Summary of Audit Result

After auditing, 1 Low risk item was identified in the JP Gold Coin project. Specific audit details will be presented in the Findings section. Users should pay attention to the following aspects when interacting with this project:

Low	Fixed : 1

Business overview

1. Basic Token Information

Token name	JP Gold Coin
Token symbol	JPGC
Decimals	8
Current supply	10,576,000
Token type	SPL Token

Table 1 JPGC token info

JP Gold Coin (JPGC) is a token based on the SPL protocol, with 8 decimal places of precision and a current total supply of 10,576,000 tokens. The SPL Token includes essential functionalities for tokens, with key instructions such as `InitializeAccount`, `InitializeAccount2`, and `InitializeAccount3` for creating and initializing token accounts. The `CloseAccount` instruction is used to close accounts and reclaim SOL, while `InitializeMultisig` and `InitializeMultisig2` are for creating and initializing multisig accounts. The `Transfer` and `TransferChecked` instructions facilitate token transfers, and `Approve` and `ApproveChecked` handle authorization management. Additionally, `MintTo` and `MintToChecked` are used for minting tokens, and `Burn` and `BurnChecked` are for token destruction.

2. Token Metadata


```
{
  "key": 4,
  "updateAuthority": "5UgJaGp1SYipxixJXfSo3cuN2EAXu66zmrBUFCeyFR9D",
  "mint": "JPGCPKWfGCEMRraSKhsCcn1qvs7qVaLjmq6ihveXn62",
  "data": {
    "name": "JP Gold Coin",
    "symbol": "JPGC",
    "uri": "https://meta.jpgoldcoin.app/",
    "sellerFeeBasisPoints": 0
  },
  "primarySaleHappened": 0,
  "isMutable": 1,
  "editionNonce": 250,
  "tokenStandard": 2
```

```
}
```

3. Distribution of tokens

The current total supply of JPGC tokens is 10,576,000, the main allocation is as follows:

Account	Quantity	Percentage
EXaAZb6fmaCL3V3SXKLJZE6ZnBJABF4tucgkqHe8YBr3	10,556,000	99.81%
5UgJaGp1SYipxixJXfSo3cuN2EAXu66zmrBUFCeyFR9D	13,999.9	0.13%
B5j8iMBe5vVPbeuVHcFRuAys9bHsycqhTviT3T7bNk3G	6,000	0.05673%
AaDuSSpQ4MaxRP6XpdRAMT7wK7a3sXdXkPnHQErEsngm	0.1	$0.0_{6}9456\%$

1 Overview

1.1 Project Overview

Project Name	JP Gold Coin
Project Language	Rust
Platform	Solana
Contract Address	JPGCPKWfGCEMRraSKhsCcn1qvs7qVaLjmq6ihveXn62

1.2 Audit Overview

Audit work duration: Jun 10, 2025, Jun 26, 2025

Audit team: Beosin Security Team

1.3 Audit Method

The audit methods are as follows:

1. Formal Verification

Formal verification is a technique that uses property-based approaches for testing and verification. Property specifications define a set of rules using Beosin's library of security expert rules. These rules call into the contracts under analysis and make various assertions about their behavior. The rules of the specification play a crucial role in the analysis. If the rule is violated, a concrete test case is provided to demonstrate the violation.

2. Manual Review

Using manual auditing methods, the code is read line by line to identify potential security issues. This ensures that the contract's execution logic aligns with the client's specifications and intentions, thereby safeguarding the accuracy of the contract's business logic.

The manual audit is divided into three groups to cover the entire auditing process:

The Basic Testing Group is primarily responsible for interpreting the project's code and conducting comprehensive functional testing.

The Simulated Attack Group is responsible for analyzing the audited project based on the collected historical audit vulnerability database and security incident attack models. They identify potential attack vectors and collaborate with the Basic Testing Group to conduct simulated attack tests.

The Expert Analysis Group is responsible for analyzing the overall project design, interactions with third parties, and security risks in the on-chain operational environment. They also conduct a review of the entire audit findings.

3. Static Analysis

Static analysis is a method of examining code during compilation or static analysis to detect issues. Beosin-VaaS can detect more than 100 common smart contract vulnerabilities through static analysis, such as reentrancy and block parameter dependency. It allows early and efficient discovery of problems to improve code quality and security.

2 Findings

Index	Risk description	Severity level	Status
JP Gold Coin-01	Centralization Risk	Low	Fixed

Finding Details:

[JP Gold Coin-01] Centralization Risk

Severity Level	Low
Type	Business Security
Description	The Solana SPL token's mint authority, freeze authority, and update authority are all controlled by a single entity 5UgJaGp1SYipxixJXfSo3cuN2EAXu66zmrBUFCeyFR9D, granting the token issuer centralized control over critical token functions.This centralized control introduces several critical risks: 1) The issuer retains the mint authority, enabling them to create additional tokens at any time. This poses a risk of unplanned supply inflation or unequal distribution, potentially undermining token value and holder trust. 2) The presence of the freeze authority allows the issuer to arbitrarily freeze token accounts. This could be used to restrict user access to funds or halt token transfers, which may impact token liquidity and usability. 3) With control over the update authority, the issuer can modify token metadata such as the token name, symbol, or URI. Such changes could lead to confusion, impersonation risks, or misalignment with what users expect from the token. This centralization introduces a single point of failure, where a compromise, misuse, or mismanagement of these authorities could disrupt token operations. The concentration of all critical authorities in one entity creates a significant centralization risk. If this entity is compromised, acts maliciously, or mismanages these powers, the token's integrity and operations could be severely disrupted.
Recommendation	It is recommended that the project team first allocate all tokens according to the planned distribution, then review the business logic and relinquish the mint authority by setting it to null, ensuring no further tokens can be minted and safeguarding the token's supply integrity.The freeze authority and update authority should be revoked or transferred to a decentralized governance mechanism, to prevent unilateral restrictions on token transfers and enhance user autonomy.
Status	**Fixed.**

3 Appendix

3.1 Vulnerability Assessment Metrics and Status in Smart Contracts

3.1.1 Metrics

In order to objectively assess the severity level of vulnerabilities in blockchain systems, this report provides detailed assessment metrics for security vulnerabilities in smart contracts with reference to CVSS 3.1(Common Vulnerability Scoring System Ver 3.1).

According to the severity level of vulnerability, the vulnerabilities are classified into four levels: "critical", "high", "medium" and "low". It mainly relies on the degree of impact and likelihood of exploitation of the vulnerability, supplemented by other comprehensive factors to determine of the severity level.

Likelihood \ Impact	Severe	High	Medium	Low
Probable	Critical	High	Medium	Low
Possible	High	Medium	Medium	Low
Unlikely	Medium	Medium	Low	Info
Rare	Low	Low	Info	Info

2.1.2 Degree of impact

- **Critical**

Critical impact generally refers to the vulnerability can have a serious impact on the confidentiality, integrity, availability of smart contracts or their economic model, which can cause substantial economic losses to the contract business system, large-scale data disruption, loss of authority management, failure of key functions, loss of credibility, or indirectly affect the operation of other smart contracts associated with it and cause substantial losses, as well as other severe and mostly irreversible harm.

- **High**

High impact generally refers to the vulnerability can have a relatively serious impact on the confidentiality, integrity, availability of the smart contract or its economic model, which can cause a greater economic loss, local functional unavailability, loss of credibility and other impact to the contract business system.

- **Medium**

Medium impact generally refers to the vulnerability can have a relatively minor impact on the confidentiality, integrity, availability of the smart contract or its economic model, which can cause a small amount of economic loss to the contract business system, individual business unavailability and other impact.

- **Low**

Low impact generally refers to the vulnerability can have a minor impact on the smart contract, which can pose certain security threat to the contract business system and needs to be improved.

2.1.3 Likelihood of Exploitation

- **Probable**

Probable likelihood generally means that the cost required to exploit the vulnerability is low, with no special exploitation threshold, and the vulnerability can be triggered consistently.

- **Possible**

Possible likelihood generally means that exploiting such vulnerability requires a certain cost, or there are certain conditions for exploitation, and the vulnerability is not easily and consistently triggered.

- **Unlikely**

Unlikely likelihood generally means that the vulnerability requires a high cost, or the exploitation conditions are very demanding and the vulnerability is highly difficult to trigger.

- **Rare**

Rare likelihood generally means that the vulnerability requires an extremely high cost or the conditions for exploitation are extremely difficult to achieve.

2.1.4 Fix Results Status

Status	Description
Fixed	The project party fully fixes a vulnerability.
Partially Fixed	The project party did not fully fix the issue, but only mitigated the issue.
Acknowledged	The project party confirms and chooses to ignore the issue.

3.2 Audit Categories

No.	Categories	Subitems
1	Coding Conventions	SPL Token Standards
		Visibility Specifiers
		Lamport Check
		Account Check
		Signer Check
		Program Id Check
		Deprecated Items
		Redundant Code
2	General Vulnerability	Integer Overflow/Underflow
		Reentrancy
		Pseudo-random Number Generator (PRNG)
		Transaction-Ordering Dependence
		DoS (Denial of Service)
		Function Call Permissions
		Returned Value Security
		Replay Attack
		Overriding Variables
		Third-party Protocol Interface Consistency
3	Business Security	Business Logics
		Business Implementations
		Manipulable Token Price
		Centralized Asset Control
		Asset Tradability
		Arbitrage Attack

Beosin classified the security issues of smart contracts into three categories: Coding Conventions, General Vulnerability, Business Security. Their specific definitions are as follows:

- **Coding Conventions**

Audit whether smart contracts follow recommended language security coding practices. For example, smart contracts developed in Solidity language should fix the compiler version and do not use deprecated keywords.

- **General Vulnerability**

General Vulnerability include some common vulnerabilities that may appear in smart contract projects. These vulnerabilities are mainly related to the characteristics of the smart contract itself, such as integer overflow/underflow and denial of service attacks.

- **Business Security**

Business security is mainly related to some issues related to the business realized by each project, and has a relatively strong pertinence. For example, whether the lock-up plan in the code match the white paper, or the flash loan attack caused by the incorrect setting of the price acquisition oracle.

*Note that the project may suffer stake losses due to the integrated third-party protocol. This is not something Beosin can control. Business security requires the participation of the project party. The project party and users need to stay vigilant at all times.

3.3 Disclaimer

The Audit Report issued by Beosin is related to the services agreed in the relevant service agreement. The Project Party or the Served Party (hereinafter referred to as the "Served Party") can only be used within the conditions and scope agreed in the service agreement. Other third parties shall not transmit, disclose, quote, rely on or tamper with the Audit Report issued for any purpose.

The Audit Report issued by Beosin is made solely for the code, and any description, expression or wording contained therein shall not be interpreted as affirmation or confirmation of the project, nor shall any warranty or guarantee be given as to the absolute flawlessness of the code analyzed, the code team, the business model or legal compliance.

The Audit Report issued by Beosin is only based on the code provided by the Served Party and the technology currently available to Beosin. However, due to the technical limitations of any organization, and in the event that the code provided by the Served Party is missing information, tampered with, deleted, hidden or subsequently altered, the audit report may still fail to fully enumerate all the risks.

The Audit Report issued by Beosin in no way provides investment advice on any project, nor should it be utilized as investment suggestions of any type. This report represents an extensive evaluation process designed to help our customers improve code quality while mitigating the high risks in blockchain.

3.4 About Beosin

Beosin is the first institution in the world specializing in the construction of blockchain security ecosystem. The core team members are all professors, postdocs, PhDs, and Internet elites from world-renowned academic institutions. Beosin has more than 20 years of research in formal verification technology, trusted computing, mobile security and kernel security, with overseas experience in studying and collaborating in project research at well-known universities. Through the security audit and defense deployment of more than 2,000 smart contracts, over 50 public blockchains and wallets, and nearly 100 exchanges worldwide, Beosin has accumulated rich experience in security attack and defense of the blockchain field, and has developed several security products specifically for blockchain.

BEOSIN
Web3 Security & Compliance

Official Website
https://www.beosin.com

Telegram
https://t.me/beosin

X
https://x.com/Beosin_com

Email
service@beosin.com

LinkedIn
https://www.linkedin.com/company/beosin/