smart state

Web3 security easier than ever

DOGEN

Token audit report

October 08, 2024

Table of contents

Methodology

- Best code practices

- Manual code analysis

- Arithmetic Overflows / Underflows

- Hidden Malicious Code

- Code with no effects

- Floating points and numerical precision

- Race conditions / front running

- Use of deprecated functions

- Re-entrancy

- Unused vars

- Logical bugs & code logic issues

- Using components with known vulnerabilities

- Weak PRNG / Random number generators issues

- Denial of service (DOS)

- Solana account confusions

- External program validation failure

- Insufficient SPL Token Account verification

- Missing signer check

- Missing ownership check

- Signed invocation of unverified program

- Delegate call

- Default Visibilities

- Unchecked call return method

- External contract

- Entropy illusion

- Block timestamp manipulation

- Short address / Parameter attack

Summary

DOGEN token is a fungible meme token on the Solana network.

This audit encompasses the examination of the DOGEN token parameters.

Disclaimer

This is a final public security audit report version and does not include vulnerabilities that might have been found and addressed during the audit process.
An audit does not provide any warranties regarding the code security. We presume that a single audit cannot be considered totally sufficient and always recommend several independent audits and a public bug bounty program to ensure code security.
Please do not consider this report as investment and / or financial advice of any kind.

Vulnerabilities found by type

INFO	2
LOW	0
MEDIUM	0
HIGH	0
CRITICAL	0
Total	2

1. About

DOGEN token is a fungible meme token on the Solana network created using the Solana token program.

Token address:

B7xavrAozTa1msQxu8YAcvPftf76x1fJYyLrYdTnbrah

Current basic on-chain data (as of October 08, 2024):

```
SPL Token Mint
  Address: B7xavrAozTa1msQxu8YAcvPftf76x1fJYyLrYdTnbrah
  Program: TokenkegQfeZyiNwAJbNbGKPFXCWuBvf9Ss623VQ5DA
  Supply: 10000000000000000
  Decimals: 6
  Mint authority: (not set)
  Freeze authority: (not set)
```

2. Token Distribution

Token distribution refers to the token allocation and / or dispersion among the holders. As is customary for the Solana Token Program, all initially minted tokens were transferred to the owner's account.

DOGEN token (mint) address:

B7xavrAozTa1msQxu8YAcvPftf76x1fJYyLrYdTnbrah

DOGEN token authority:

65zEawtiqL6wo4Q4mursdbV33YZQne5GZJ3spvzrL8vC

Initial mint:

10,000,000,000.000000 DOGEN token

Minted / Transferred to:

Wallet account:

B1Ey1uokrtsx2UHQJFma6pqeG7Cut2LTqRggfHRyH9KT

Token account:

CD59sCM4VemF9QJqqYtXRnoN7b2RhbRoNV1gCYyJY4C8

TX:

5yH1SZKJT91DmqHcHdfCYZmU9Exi2Unt13PvZCQJ7iqzsyXR2fdw97RGCK612djS7abP7Uhd8uBzps1PRsLexstr

Current DOGEN token supply (as of October 08, 2024):

10,000,000,000.000000 DOGEN token

3. Minting Authority

A minting authority is a designated address or entity that has been granted the authority to generate tokens within the token ecosystem.

According to the on-chain analysis, the minting authority is **currently undefined**, implying that no new tokens can be created beyond the existing token supply.

4. Freeze Authority

A freeze authority is a control mechanism in SPL token ecosystems that enables a designated entity to halt the transfer of tokens for certain accounts.

According to the on-chain analysis, the freeze authority is **currently undefined**, indicating that there are no restrictions possible on the transfer of tokens for specific accounts.

5. Token Metadata

Token Metadata provides additional detailed token information such as token name, symbol (ticker) etc.

Metaplex Metadata

```
▼"root" : { 10 items
  "key" : int 4
  "updateAuthority" : string "65zEawtiqL6wo4Q4mursdbV33YZQne5GZJ3spvzrL8vC"
  "mint" : string "B7xavrAozTa1msQxu8YAcvPftf76x1fJYyLrYdTnbrah"
  ▼"data" : { 5 items
    "name" : string "DOGEN"
    "symbol" : string "DOGEN"
    "uri" : string "https://arweave.net/6pv9hkTWpFdaFzV20hp1aceF_E91W3c-LP9UM5JcKf4"
    "sellerFeeBasisPoints" : int 0
    "creators" : undefined
  }
  "primarySaleHappened" : int 0
  "isMutable" : int 0
  "editionNonce" : int 254
  "tokenStandard" : int 2
  "collection" : undefined
  "uses" : undefined
}
```

isMutable is set to 0 (False) which means DOGEN token Metadata cannot be further modified.

6. Token Extensions

DOGEN token has **no extensions.**

7. Token External Dependencies

The DOGEN token used **SPL (Solana Program Library) token program** to generate fungible tokens.

SPL token program address:
TokenkegQfeZyiNwAJbNbGKPFXCWuBvf9Ss623VQ5DA

8. Findings

8.1 NON-UNIQUE TOKEN NAMING DATA

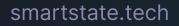| **Status**: Acknowledged	INFO
Type: Other	
DOGEN token utilizes a non-unique name / ticker, which may potentially lead to phishing / defacement.	

8.2 CENTRALIZED INITIAL TOKEN DISTRIBUTION

Status: Acknowledged	INFO
Type: Centralization	
Upon contract deployment, all DOGEN tokens are transferred to a single account. This poses a potential risk of centralization, as the account has the ability to distribute tokens without community consensus. If the account holding undistributed tokens is compromised, the attacker could potentially steal and sell the tokens on the market, which could significantly harm the project.	

Verification data

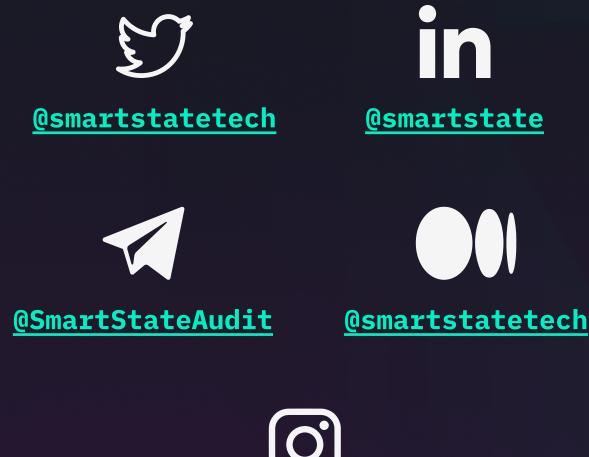| Token	Address on block explorer	
DOGEN	https://explorer.solana.com/address/B7xavrAozTa1msQxu8YAcvPftf76x1fJYyLrYdTnbrah https://solscan.io/token/B7xavrAozTa1msQxu8YAcvPftf76x1fJYyLrYdTnbrah	

Project evaluation

9/10

Get in touch 👋

@smartstatetech

@smartstate

@SmartStateAudit

@smartstatetech

@smartstate.tech

View this report on Smartstate.tech

info@smartstate.tech

smartstate.tech