CLARIFICATION ON TOKEN SMC IMPROVEMENT

1. Reason for improvement

→ Existing SMC information:
https://bscscan.com/token/0x26d32da27e6f9f1ca2c9b227e9a75782c30fcd36#balances

In the existing smart contract version, we have fixed centralization risks based on suggestion from report of Certik. A part of the audit report has been shown below:

ID	Title	Category	Severity	Status
IHI-01	Centralization Related Risks	**Centralization / Privilege**	**Major**	Acknowledged
IHI-02	Missing Emit Events	Coding Style	Informational	Resolved
IHI-03	No Restrictions On Functions	Logical Issue	Informational	Resolved
IVI-01	Centralization Related Risks	**Centralization / Privilege**	**Major**	Acknowledged
IVI-02	Variables that could be declared as immutable	Gas Optimization	Informational	Resolved
IVR-01	Missing emit events	Coding Style	Informational	Resolved
IVR-02	Unlocked compiler version	Language Specific	Informational	Resolved

2. Improvement

→ Updated SMC information:
https://bscscan.com/address/0x059ca11ba3099683Dc2e46f048063F5799a7f34c#code

The current version removes privilege of single admin managing smart contract which is manipulated in decentralization mechanism with multi-signer's addresses. The more signers contract has, the more security it is. Furthermore, creation of token is controlled by a double checking technique which ensures that released token follows our vesting schedule.

Proof of improvement:

In the following solidity code, we highlight modification which strengthens security ability of our smart contract described in the description section.

```
**
   *@dev require total vote for pause or unpause > 50% minter.
   */
  modifier mintEnoughVotes(uint256 id) {
    require(
      getMintVoteCount(id)
 >= getRequired(),
      "IvirseToken Contract: Not enough votes!"
    );
    _;
  }
  /**
   *@dev require sender accept for mint request.
   */
  modifier mintAccepted(uint256 id) {
    address sender = _msgSender();
    require(mintVotes[id][sender], "IvirseToken Contract: Rejected!");
    _;
  }
  /**
   *@dev require sender does not accept for mint request.
   */
  modifier mintRejected(uint256 id) {
    address sender = _msgSender();
    require(!mintVotes[id][sender], "IvirseToken Contract: Accepted!");
    _;
  }
  /**
   *@dev require mint request actived.
   */
  modifier notMint(uint256 id) {
    require(!mints[id].used, "IvirseToken Contract: Minted!");
    _;
  }
```

From IVIRSE team