知道创宇

密级 ★ | 项目组公开

智能合约审计报告

安全状态

低危

★ ★ ★ ★ ★

版本说明

修订人	修订内容	修订时间	版本号	审阅人
罗逸锋	**编写文档**	**2020/9/22**	**V1.0**	**徐昊杰**

文档信息

文档名称	文档版本号	文档编号	保密级别
SMinter 合约审计报告	V1.0	【SMinter-DMSJ-20200922】	项目组公开

版权声明

目录

1. 综述

本次报告有效测试时间是从 2020 年 9 月 19 日开始到 2020 年 9 月 22 日结束，在此期间针对 SMinter 智能合约代码的安全性和规范性进行审计并以此作为报告统计依据。

此次测试中，知道创宇工程师对智能合约的常见漏洞（见第三章节）进行了全面的分析，发现了重入攻击、事务顺序依赖、拒绝服务攻击、增发代币风险，故综合评定为低危。

本次智能合约安全审计结果：通过

由于本次测试过程在非生产环境下进行，所有代码均为最新备份，测试过程均与相关接口人进行沟通，并在操作风险可控的情况下进行相关测试操作，以规避测试过程中的生产运营风险、代码安全风险。

本次测试的目标信息：

模块名称	内容
Token 名称	SMinter
代码类型	代币代码
代码语言	solidity

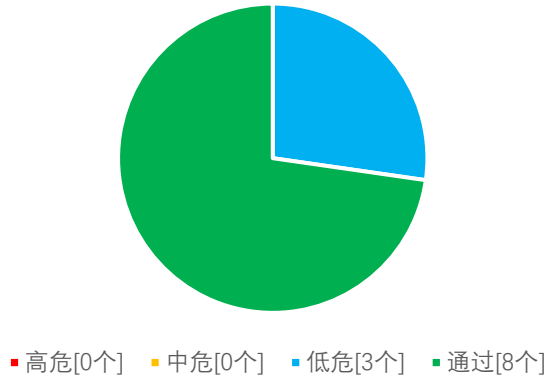
2. 代码漏洞分析

2.1. 漏洞等级分布

本次漏洞风险按等级统计:

漏洞风险等级个数统计表			
高危	中危	低危	通过
0	0	3	8

风险等级分布图



2.2. 审计结果汇总

审计结果			
测试项目	测试内容	状态	描述
智能合约	重入攻击检测	低危	检查 call.value()函数使用安全
	数值溢出检测	通过	检查 add 和 sub 函数使用安全
	访问控制缺陷检测	通过	检查各操作访问权限控制
	未验证返回值的调用	通过	检查转币方法看是否验证返回值
	错误使用随机数检测	通过	检查是否具备统一的内容过滤器
	事务顺序依赖检测	低危	检查是否存在事务顺序依赖风险
	拒绝服务攻击检测	通过	检查代码在使用资源时是否存在资源滥用问题
	逻辑设计缺陷检测	通过	检查智能合约代码中与业务设计相关的安全问题
	假充值漏洞检测	通过	检查智能合约代码中是否存在假充值漏洞
	增发代币漏洞检测	低危	检查智能合约中是否存在增发代币的功能
	冻结账户绕过检测	通过	检查转移代币中是否存在未校验冻结账户的问题

3. 代码审计结果分析

3.1. 重入攻击检测【低危】

重入漏洞是最著名的以太坊智能合约漏洞，曾导致了以太坊的分叉（The DAO hack）。

Solidity 中的 call.value()函数在被用来发送 Ether 的时候会消耗它接收到的所有 gas，当调用 call.value()函数发送 Ether 的操作发生在实际减少发送者账户的余额之前时，就会存在重入攻击的风险。

检测结果：经检测，智能合约代码中存在相关 call 外部合约调用。

```
*/
function sendValue(address payable recipient, uint256 amount) internal {
    require(address(this).balance >= amount, "Address: insufficient balance");

    // solhint-disable-next-line avoid-low-level-calls, avoid-call-value
    (bool success, ) = recipient.call{ value: amount }("");
    require(success, "Address: unable to send value, recipient may have reverted");
}
```

安全建议：

（1）尽量使用 send()、transfer() 函数。

（2）如果使用像 call() 函数这样的低级调用函数时，应该先执行内部状态的更改，然后再使用低级调用函数。

（3）编写智能合约时尽量避免外部合约的调用。

3.2. 数值溢出检测【通过】

智能合约中的算数问题是指整数溢出和整数下溢。

Solidity 最多能处理 256 位的数字（2^256-1），最大数字增加 1 会溢出得到 0。同样，当数字为无符号类型时，0 减去 1 会下溢得到最大数字值。

整数溢出和下溢不是一种新类型的漏洞，但它们在智能合约中尤其危险。溢出情况会导致不正确的结果，特别是如果可能性未被预期，可能会影响程序的可靠性和安全性。

检测结果：经检测，智能合约代码中不存在该安全问题。

安全建议：无。

3.3. 访问控制检测【通过】

访问控制缺陷是所有程序中都可能存在的安全风险，智能合约也同样会存在类似问题，著名的 Parity Wallet 智能合约就受到过该问题的影响。

检测结果：经检测，智能合约代码中不存在该安全问题。

安全建议：无。

3.4. 返回值调用验证【通过】

此问题多出现在和转币相关的智能合约中，故又称作静默失败发送或未经检查发送。

在 Solidity 中存在 transfer()、send()、call.value()等转币方法，都可以用于向某一地址发送 Ether，其区别在于： transfer 发送失败时会 throw，并且进行状态回滚；只会传递 2300gas 供调用，防止重入攻击；send 发送失败时会返回 false；只会传递 2300gas 供调用，防止重入攻击；call.value 发送失败时会返回 false；传递所有可用 gas 进行调用（可通过传入 gas_value 参数进行限制），不能有效防止重入攻击。

如果在代码中没有检查以上 send 和 call.value 转币函数的返回值，合约会继

续执行后面的代码，可能由于 Ether 发送失败而导致意外的结果。

检测结果：经检测，智能合约代码中不存在相关漏洞。

安全建议：无。

3.5. 错误使用随机数【通过】

智能合约中可能需要使用随机数，虽然 Solidity 提供的函数和变量可以访问明显难以预测的值，如 block.number 和 block.timestamp，但是它们通常或者比看起来更公开，或者受到矿工的影响，即这些随机数载一定程度上是可预测的，所以恶意用户通常可以复制它并依靠其不可预知性来攻击该功能。

检测结果：经检测，智能合约代码中不存在该问题。

安全建议：无。

3.6. 事务顺序依赖【低危】

由于矿工总是通过代表外部拥有地址（EOA）的代码获取 gas 费用，因此用户可以指定更高的费用以便更快地开展交易。由于以太坊区块链是公开的，每个人都可以看到其他人未决交易的内容。这意味着，如果某个用户提交了一个有价值的解决方案，恶意用户可以窃取该解决方案并以较高的费用复制其交易，以抢占原始解决方案。

检测结果：经检测，智能合约代码中存在相关漏洞。

```
 */
function _approve(address owner, address spender, uint256 amount) internal virtual {
    require(owner != address(0), "ERC20: approve from the zero address");
    require(spender != address(0), "ERC20: approve to the zero address");

    _allowances[owner][spender] = amount;
    emit Approval(owner, spender, amount);
}
```

安全建议：

1.限制 approve 函数在将配额从 N 修改为 M 时，只能先从 N 修改为 0，再从 0 修改为 M：require((_value == 0) || (allowance[msg.sender][_spender] == 0));

2.使用 increaseApproval 函数和 decreaseApproval 函数来代替 approve 函数

3.7. 拒绝服务攻击【通过】

在以太坊的世界中，拒绝服务是致命的，遭受该类型攻击的智能合约可能永远无法恢复正常工作状态。导致智能合约拒绝服务的原因可能有很多种，包括在作为交易接收方时的恶意行为，人为增加计算功能所需 gas 导致 gas 耗尽，滥用访问控制访问智能合约的 private 组件，利用混淆和疏忽等等。

检测结果：经检测，智能合约代码中不存在此类漏洞。

安全建议：无

3.8. 逻辑设计缺陷【通过】

检测智能合约代码中与业务设计相关的安全问题。

检测结果：经检测，智能合约代码中不存在相关漏洞。

安全建议：无。

3.9. 假充值漏洞【通过】

在代币合约的 transfer 函数对转账发起人(ABBT.sender)的余额检查用的是 if 判断方式，当 balances[ABBT.sender] < value 时进入 else 逻辑部分并 return

false，最终没有抛出异常，我们认为仅 if/else 这种温和的判断方式在 transfer 这类敏感函数场景中是一种不严谨的编码方式。

检测结果：经检测，智能合约代码中不存在相关漏洞。

安全建议：无。

3.10. 增发代币漏洞【低危】

检测在初始化代币总量后，代币合约中是否存在可能使代币总量增加的函数。

检测结果：经检测，智能合约代码中存在相关漏洞。

```
 */
function _mint(address account, uint256 amount) internal virtual {
    require(account != address(0), "ERC20: mint to the zero address");

    _beforeTokenTransfer(address(0), account, amount);

    _totalSupply = _totalSupply.add(amount);
    _balances[account] = _balances[account].add(amount);
    emit Transfer(address(0), account, amount);
}
```

安全建议：该问题不属于安全问题，但部分交易所会限制增发函数的使用，具体情况需根据交易所的要求而定。

3.11. 冻结账户绕过【通过】

检测代币合约中在转移代币时，是否存在未校验代币来源账户、发起账户、目标账户是否被冻结的操作。

检测结果：经检测，智能合约代码中不存在该问题。

安全建议：无。

4. 附录 A：合约代码

```
// SPDX-License-Identifier: MIT

pragma solidity ^0.6.0;
//pragma experimental ABIEncoderV2;

import "./SToken.sol";
import "./Governable.sol";

import "./TransferHelper.sol";


interface Minter {
    event Minted(address indexed recipient, address reward_contract, uint minted);

    function token() external view returns (address);
    function controller() external view returns (address);
    function minted(address, address) external view returns (uint);
    function allowed_to_mint_for(address, address) external view returns (bool);

    function mint(address gauge) external;
    function mint_many(address[8] calldata gauges) external;
    function mint_for(address gauge, address _for) external;
    function toggle_approve_mint(address minting_user) external;
}

interface LiquidityGauge {
    event Deposit(address indexed provider, uint value);
    event Withdraw(address indexed provider, uint value);
    event UpdateLiquidityLimit(address user, uint original_balance, uint
original_supply, uint working_balance, uint working_supply);

    function user_checkpoint (address addr) external returns (bool);
    function claimable_tokens(address addr) external view returns (uint);
    function claimable_reward(address addr) external view returns (uint);
    function integrate_checkpoint()       external view returns (uint);

    function kick(address addr) external;
    function set_approve_deposit(address addr, bool can_deposit) external;
    function deposit(uint _value) external;
    function deposit(uint _value, address addr) external;
    function withdraw(uint _value) external;
    function withdraw(uint _value, bool claim_rewards) external;
    function claim_rewards() external;
    function claim_rewards(address addr) external;

    function minter()                     external view returns (address);
    function crv_token()                  external view returns (address);
    function lp_token()                   external view returns (address);
    function controller()                 external view returns (address);
    function voting_escrow()              external view returns (address);
    function balanceOf(address)           external view returns (uint);
    function totalSupply()                external view returns (uint);
    function future_epoch_time()          external view returns (uint);
    function approved_to_deposit(address, address)  external view returns (bool);
    function working_balances(address)    external view returns (uint);
    function working_supply()             external view returns (uint);
    function period()                     external view returns (int128);
    function period_timestamp(uint)       external view returns (uint);
    function integrate_inv_supply(uint)   external view returns (uint);
    function integrate_inv_supply_of(address) external view returns (uint);
    function integrate_checkpoint_of(address) external view returns (uint);
    function integrate_fraction(address)  external view returns (uint);
    function inflation_rate()             external view returns (uint);
    function reward_contract()            external view returns (address);
    function rewarded_token()             external view returns (address);
    function reward_integral()            external view returns (uint);
    function reward_integral_for(address) external view returns (uint);
    function rewards_for(address)         external view returns (uint);
    function claimed_rewards_for(address) external view returns (uint);
}
```

```
contract SSimpleGauge is LiquidityGauge, Configurable {
    using SafeMath for uint;
    using TransferHelper for address;

    address override public minter;
    address override public crv_token;
    address override public lp_token;
    address override public controller;
    address override public voting_escrow;
    mapping(address => uint) override public balanceOf;
    uint override public totalSupply;
    uint override public future_epoch_time;

    // caller -> recipient -> can deposit?
    mapping(address => mapping(address => bool)) override public approved_to_deposit;

    mapping(address => uint) override public working_balances;
    uint override public working_supply;

    // The goal is to be able to calculate ∫(rate * balance / totalSupply dt) from 0
till checkpoint
    // All values are kept in units of being multiplied by 1e18
    int128 override public period;
    uint256[1000000000000000000000000000000] override public period_timestamp;

    // 1e18 * ∫(rate(t) / totalSupply(t) dt) from 0 till checkpoint
    uint256[1000000000000000000000000000000] override public integrate_inv_supply;  //
bump epoch when rate() changes

    // 1e18 * ∫(rate(t) / totalSupply(t) dt) from (last_action) till checkpoint
    mapping(address => uint) override public integrate_inv_supply_of;
    mapping(address => uint) override public integrate_checkpoint_of;

    // ∫(balance * rate(t) / totalSupply(t) dt) from 0 till checkpoint
    // Units: rate * t = already number of coins per address to issue
    mapping(address => uint) override public integrate_fraction;

    uint override public inflation_rate;

    // For tracking external rewards
    address override public reward_contract;
    address override public rewarded_token;

    uint override public reward_integral;
    mapping(address => uint) override public reward_integral_for;
    mapping(address => uint) override public rewards_for;
    mapping(address => uint) override public claimed_rewards_for;


     uint public span;
     uint public end;

     function initialize(address governor, address _minter, address _lp_token) public
initializer {
        super.initialize(governor);

        minter     = _minter;
        crv_token  = Minter(_minter).token();
        lp_token   = _lp_token;
        IERC20(lp_token).totalSupply();        // just check
     }

    function setSpan(uint _span, bool isLinear) virtual external governance {
       span = _span;
       if(isLinear)
          end = now + _span;
       else
          end = 0;
    }

    function kick(address addr) virtual override external {
       _checkpoint(addr, true);
    }

    function set_approve_deposit(address addr, bool can_deposit) virtual override
external {
```

```
        approved_to_deposit[addr][msg.sender] = can_deposit;
    }

    function deposit(uint amount) virtual override external {
        deposit(amount, msg.sender);
    }
    function deposit(uint amount, address addr) virtual override public {
        require(addr == msg.sender || approved_to_deposit[msg.sender][addr], 'Not
approved');

        _checkpoint(addr, true);

        _deposit(addr, amount);

        balanceOf[addr] = balanceOf[addr].add(amount);
        totalSupply = totalSupply.add(amount);

        emit Deposit(addr, amount);
    }
    function _deposit(address addr, uint amount) virtual internal {
        lp_token.safeTransferFrom(addr, address(this), amount);
    }

    function withdraw() virtual  external {
        withdraw(balanceOf[msg.sender], true);
    }
    function withdraw(uint amount) virtual override external {
        withdraw(amount, true);
    }
    function withdraw(uint amount, bool claim_rewards) virtual override public {
        _checkpoint(msg.sender, claim_rewards);

        totalSupply = totalSupply.sub(amount);
        balanceOf[msg.sender] = balanceOf[msg.sender].sub(amount);

        _withdraw(msg.sender, amount);

        emit Withdraw(msg.sender, amount);
    }
    function _withdraw(address to, uint amount) virtual internal {
        lp_token.safeTransfer(to, amount);
    }

    function claimable_reward(address) virtual override public view returns (uint) {
        return 0;
    }

    function claim_rewards() virtual override public {
        return claim_rewards(msg.sender);
    }
    function claim_rewards(address) virtual override public {
        return;
    }
    function _checkpoint_rewards(address, bool) virtual internal {
        return;
    }

    function claimable_tokens(address addr) virtual override public view returns (uint
amount) {
        if(span == 0 || totalSupply == 0)
            return 0;

        amount = SMinter(minter).quotas(address(this));
        amount = amount.mul(balanceOf[addr]).div(totalSupply);

        uint lasttime = integrate_checkpoint_of[addr];
        if(end == 0) {                                                  // isNonLinear,
endless
            if(now.sub(lasttime) < span)
                amount = amount.mul(now.sub(lasttime)).div(span);
        }else if(now < end)
            amount = amount.mul(now.sub(lasttime)).div(end.sub(lasttime));
        else if(lasttime >= end)
            amount = 0;
    }

    function _checkpoint(address addr, uint amount) virtual internal {
```

```
        if(amount > 0) {
            integrate_fraction[addr] = integrate_fraction[addr].add(amount);

            address teamAddr = address(config['teamAddr']);
            uint teamRatio = config['teamRatio'];
            if(teamAddr != address(0) && teamRatio != 0)
                integrate_fraction[teamAddr] =
integrate_fraction[teamAddr].add(amount.mul(teamRatio).div(1 ether));
        }
    }

    function _checkpoint(address addr, bool _claim_rewards) virtual internal {
        uint amount = claimable_tokens(addr);
        _checkpoint(addr, amount);
        _checkpoint_rewards(addr, _claim_rewards);

        integrate_checkpoint_of[addr] = now;
    }

    function user_checkpoint(address addr) virtual override external returns (bool) {
        _checkpoint(addr, true);
        return true;
    }

    function integrate_checkpoint() override external view returns (uint) {
        return now;
    }
}

contract SExactGauge is LiquidityGauge, Configurable {
    using SafeMath for uint;
    using TransferHelper for address;

    bytes32 internal constant _devAddr_       = 'devAddr';
    bytes32 internal constant _devRatio_      = 'devRatio';
    bytes32 internal constant _ecoAddr_       = 'ecoAddr';
    bytes32 internal constant _ecoRatio_      = 'ecoRatio';

    address override public minter;
    address override public crv_token;
    address override public lp_token;
    address override public controller;
    address override public voting_escrow;
    mapping(address => uint) override public balanceOf;
    uint override public totalSupply;
    uint override public future_epoch_time;

    // caller -> recipient -> can deposit?
    mapping(address => mapping(address => bool)) override public approved_to_deposit;

    mapping(address => uint) override public working_balances;
    uint override public working_supply;

    // The goal is to be able to calculate ∫(rate * balance / totalSupply dt) from 0
till checkpoint
    // All values are kept in units of being multiplied by 1e18
    int128 override public period;
    uint256[100000000000000000000000000000] override public period_timestamp;

    // 1e18 * ∫(rate(t) / totalSupply(t) dt) from 0 till checkpoint
    uint256[100000000000000000000000000000] override public integrate_inv_supply;  //
bump epoch when rate() changes

    // 1e18 * ∫(rate(t) / totalSupply(t) dt) from (last_action) till checkpoint
    mapping(address => uint) override public integrate_inv_supply_of;
    mapping(address => uint) override public integrate_checkpoint_of;

    // ∫(balance * rate(t) / totalSupply(t) dt) from 0 till checkpoint
    // Units: rate * t = already number of coins per address to issue
    mapping(address => uint) override public integrate_fraction;

    uint override public inflation_rate;

    // For tracking external rewards
    address override public reward_contract;
    address override public rewarded_token;
```

```
    uint override public reward_integral;
    mapping(address => uint) override public reward_integral_for;
    mapping(address => uint) override public rewards_for;
    mapping(address => uint) override public claimed_rewards_for;

     uint public span;
     uint public end;
     mapping(address => uint) public sumMiningPerOf;
     uint public sumMiningPer;
     uint public bufReward;
     uint public lasttime;

     function initialize(address governor, address _minter, address _lp_token) public
initializer {
         super.initialize(governor);

         minter     = _minter;
         crv_token  = Minter(_minter).token();
         lp_token   = _lp_token;
         IERC20(lp_token).totalSupply();              // just check
     }

    function setSpan(uint _span, bool isLinear) virtual external governance {
        span = _span;
        if(isLinear)
            end = now + _span;
        else
            end = 0;
        lasttime = now;
    }

    function kick(address addr) virtual override external {
        _checkpoint(addr, true);
    }

    function set_approve_deposit(address addr, bool can_deposit) virtual override
external {
        approved_to_deposit[addr][msg.sender] = can_deposit;
    }

    function deposit(uint amount) virtual override external {
        deposit(amount, msg.sender);
    }
    function deposit(uint amount, address addr) virtual override public {
        require(addr == msg.sender || approved_to_deposit[msg.sender][addr], 'Not
approved');

        _checkpoint(addr, true);

        _deposit(addr, amount);

        balanceOf[msg.sender] = balanceOf[msg.sender].add(amount);
        totalSupply = totalSupply.add(amount);

        emit Deposit(msg.sender, amount);
    }
    function _deposit(address addr, uint amount) virtual internal {
        lp_token.safeTransferFrom(addr, address(this), amount);
    }

    function withdraw() virtual external {
        withdraw(balanceOf[msg.sender], true);
    }
    function withdraw(uint amount) virtual override external {
        withdraw(amount, true);
    }
    function withdraw(uint amount, bool _claim_rewards) virtual override public {
        _checkpoint(msg.sender, _claim_rewards);

        totalSupply = totalSupply.sub(amount);
        balanceOf[msg.sender] = balanceOf[msg.sender].sub(amount);

        _withdraw(msg.sender, amount);

        emit Withdraw(msg.sender, amount);
    }
```

```
    function _withdraw(address to, uint amount) virtual internal {
        lp_token.safeTransfer(to, amount);
    }

    function claimable_reward(address addr) virtual override public view returns (uint)
{
        addr;
        return 0;
    }

    function claim_rewards() virtual override public {
        return claim_rewards(msg.sender);
    }
    function claim_rewards(address) virtual override public {
        return;
    }
    function _checkpoint_rewards(address, bool) virtual internal {
        return;
    }

    function claimable_tokens(address addr) virtual override public view returns (uint)
{
        return _claimable_tokens(addr, claimableDelta(), sumMiningPer,
sumMiningPerOf[addr]);
    }
    function _claimable_tokens(address addr, uint delta, uint sumPer, uint lastSumPer)
virtual internal view returns (uint amount) {
        if(span == 0 || totalSupply == 0)
            return 0;

        amount = sumPer.sub(lastSumPer);
        amount = amount.add(delta.mul(1 ether).div(totalSupply));
        amount = amount.mul(balanceOf[addr]).div(1 ether);
    }
    function claimableDelta() virtual internal view returns(uint amount) {
        amount = SMinter(minter).quotas(address(this)).sub(bufReward);

        if(end == 0) {                                          // isNonLinear,
endless
            if(now.sub(lasttime) < span)
                amount = amount.mul(now.sub(lasttime)).div(span);
        }else if(now < end)
            amount = amount.mul(now.sub(lasttime)).div(end.sub(lasttime));
        else if(lasttime >= end)
            amount = 0;
    }

    function _checkpoint(address addr, uint amount) virtual internal {
        if(amount > 0) {
            integrate_fraction[addr] = integrate_fraction[addr].add(amount);

            addr = address(config[_devAddr_]);
            uint ratio = config[_devRatio_];
            if(addr != address(0) && ratio != 0)
                integrate_fraction[addr] =
integrate_fraction[addr].add(amount.mul(ratio).div(1 ether));

            addr = address(config[_ecoAddr_]);
            ratio = config[_ecoRatio_];
            if(addr != address(0) && ratio != 0)
                integrate_fraction[addr] =
integrate_fraction[addr].add(amount.mul(ratio).div(1 ether));
        }
    }

    function _checkpoint(address addr, bool _claim_rewards) virtual internal {
        if(span == 0 || totalSupply == 0)
            return;

        uint delta = claimableDelta();
        uint amount = _claimable_tokens(addr, delta, sumMiningPer,
sumMiningPerOf[addr]);

        if(delta != amount)
            bufReward = bufReward.add(delta).sub(amount);
        if(delta > 0)
            sumMiningPer = sumMiningPer.add(delta.mul(1 ether).div(totalSupply));
```

```
        if(sumMiningPerOf[addr] != sumMiningPer)
            sumMiningPerOf[addr] = sumMiningPer;
        lasttime = now;

        _checkpoint(addr, amount);
        _checkpoint_rewards(addr, _claim_rewards);
    }

    function user_checkpoint(address addr) virtual override external returns (bool) {
        _checkpoint(addr, true);
        return true;
    }

    function integrate_checkpoint() override external view returns (uint) {
        return lasttime;
    }
}


contract SNestGauge is SExactGauge {
     address[] public rewards;
     mapping(address => mapping(address =>uint)) public sumRewardPerOf;     //
recipient => rewarded_token => can sumRewardPerOf
     mapping(address => uint) public sumRewardPer;                          //
rewarded_token => can sumRewardPerOf

     function initialize(address governor, address _minter, address _lp_token, address
_nestGauge, address[] memory _moreRewards) public initializer {
        super.initialize(governor, _minter, _lp_token);

        reward_contract = _nestGauge;
        rewarded_token  = LiquidityGauge(_nestGauge).crv_token();
        rewards         = _moreRewards;
        rewards.push(rewarded_token);
        address rewarded_token2 = LiquidityGauge(_nestGauge).rewarded_token();
        if(rewarded_token2 != address(0))
        rewards.push(rewarded_token2);

        LiquidityGauge(_nestGauge).integrate_checkpoint();     // just check
        for(uint i=0; i<_moreRewards.length; i++)
            IERC20(_moreRewards[i]).totalSupply();            // just check
     }

    function _deposit(address from, uint amount) virtual override internal {
        super._deposit(from, amount);                                    //
lp_token.safeTransferFrom(from, address(this), amount);
        lp_token.safeApprove(reward_contract, amount);
        LiquidityGauge(reward_contract).deposit(amount);
    }

    function _withdraw(address to, uint amount) virtual override internal {
        LiquidityGauge(reward_contract).withdraw(amount);
        super._withdraw(to, amount);                          // lp_token.safeTransfer(to,
amount);
    }

    function claim_rewards(address to) virtual override public {
        if(span == 0 || totalSupply == 0)
            return;

        uint[] memory bals = new uint[](rewards.length);
        for(uint i=0; i<bals.length; i++)
            bals[i] = IERC20(rewards[i]).balanceOf(address(this));

        Minter(LiquidityGauge(reward_contract).minter()).mint(reward_contract);
        LiquidityGauge(reward_contract).claim_rewards();

        for(uint i=0; i<bals.length; i++) {
            uint delta = IERC20(rewards[i]).balanceOf(address(this)).sub(bals[i]);
            uint amount = _claimable_tokens(msg.sender, delta, sumRewardPer[rewards[i]],
sumRewardPerOf[msg.sender][rewards[i]]);

            if(delta > 0)
                sumRewardPer[rewards[i]] = sumRewardPer[rewards[i]].add(delta.mul(1
ether).div(totalSupply));
            if(sumRewardPerOf[msg.sender][rewards[i]] != sumRewardPer[rewards[i]])
                sumRewardPerOf[msg.sender][rewards[i]] = sumRewardPer[rewards[i]];
```

```
            if(amount > 0) {
                rewards[i].safeTransfer(to, amount);
                if(rewards[i] == rewarded_token) {
                    rewards_for[to] = rewards_for[to].add(amount);
                    claimed_rewards_for[to] = claimed_rewards_for[to].add(amount);
                }
            }
        }
    }

    function claimable_reward(address addr) virtual override public view returns (uint)
{
        uint delta = LiquidityGauge(reward_contract).claimable_tokens(address(this));
        return _claimable_tokens(addr, delta, sumRewardPer[rewarded_token],
sumRewardPerOf[addr][rewarded_token]);
    }

    function claimable_reward2(address addr) virtual public view returns (uint) {
        uint delta = LiquidityGauge(reward_contract).claimable_reward(address(this));
        address reward2 = LiquidityGauge(reward_contract).rewarded_token();
        return _claimable_tokens(addr, delta, sumRewardPer[reward2],
sumRewardPerOf[addr][reward2]);
    }

}


contract SMinter is Minter, Configurable {
    using SafeMath for uint;
    using Address for address payable;
    using TransferHelper for address;

     bytes32 internal constant _allowContract_   = 'allowContract';
     bytes32 internal constant _allowlist_       = 'allowlist';
     bytes32 internal constant _blocklist_       = 'blocklist';

    address override public token;
    address override public controller;
    mapping(address => mapping(address => uint)) override public minted;
// user => reward_contract => value
    mapping(address => mapping(address => bool)) override public allowed_to_mint_for;
// minter => user => can mint?
    mapping(address => uint) public quotas;                                    //
reward_contract => quota;

    function initialize(address governor, address token_) public initializer {
        super.initialize(governor);
        token = token_;
    }

    function setGaugeQuota(address gauge, uint quota) public governance {
      quotas[gauge] = quota;
    }

    function mint(address gauge) virtual override public {
        mint_for(gauge, msg.sender);
    }

    function mint_many(address[8] calldata gauges) virtual override external {
        for(uint i=0; i<gauges.length; i++)
            mint(gauges[i]);
    }

    function mint_for(address gauge, address _for) virtual override public {
        require(_for == msg.sender || allowed_to_mint_for[msg.sender][_for], 'Not
approved');
        require(quotas[gauge] > 0, 'No quota');

        require(getConfig(_blocklist_, msg.sender) == 0, 'In blocklist');
        bool isContract = msg.sender.isContract();
        require(!isContract || config[_allowContract_] != 0 || getConfig(_allowlist_,
msg.sender) != 0, 'No allowContract');

        LiquidityGauge(gauge).user_checkpoint(_for);
        uint total_mint = LiquidityGauge(gauge).integrate_fraction(_for);
        uint to_mint = total_mint.sub(minted[_for][gauge]);
```

```
        if(to_mint != 0) {
            quotas[gauge] = quotas[gauge].sub(to_mint);
            token.safeTransfer(_for, to_mint);
            minted[_for][gauge] = total_mint;

            emit Minted(_for, gauge, total_mint);
        }
    }

    function toggle_approve_mint(address minting_user) virtual override external {
        allowed_to_mint_for[minting_user][msg.sender]
= !allowed_to_mint_for[minting_user][msg.sender];
    }
}

/*
// helper methods for interacting with ERC20 tokens and sending ETH that do not
consistently return true/false
library TransferHelper {
    function safeApprove(address token, address to, uint value) internal {
        // bytes4(keccak256(bytes('approve(address,uint256)')));
        (bool success, bytes memory data) =
token.call(abi.encodeWithSelector(0x095ea7b3, to, value));
        require(success && (data.length == 0 || abi.decode(data, (bool))),
'TransferHelper: APPROVE_FAILED');
    }

    function safeTransfer(address token, address to, uint value) internal {
        // bytes4(keccak256(bytes('transfer(address,uint256)')));
        (bool success, bytes memory data) =
token.call(abi.encodeWithSelector(0xa9059cbb, to, value));
        require(success && (data.length == 0 || abi.decode(data, (bool))),
'TransferHelper: TRANSFER_FAILED');
    }

    function safeTransferFrom(address token, address from, address to, uint value)
internal {
        // bytes4(keccak256(bytes('transferFrom(address,address,uint256)')));
        (bool success, bytes memory data) =
token.call(abi.encodeWithSelector(0x23b872dd, from, to, value));
        require(success && (data.length == 0 || abi.decode(data, (bool))),
'TransferHelper: TRANSFER_FROM_FAILED');
    }

    function safeTransferETH(address to, uint value) internal {
        (bool success,) = to.call{value:value}(new bytes(0));
        require(success, 'TransferHelper: ETH_TRANSFER_FAILED');
    }
}
*/
// SPDX-License-Identifier: MIT

pragma solidity ^0.6.0;

/**
 * @title Initializable
 *
 * @dev Helper contract to support initializer functions. To use it, replace
 * the constructor with a function that has the `initializer` modifier.
 * WARNING: Unlike constructors, initializer functions must be manually
 * invoked. This applies both to deploying an Initializable contract, as well
 * as extending an Initializable contract via inheritance.
 * WARNING: When used with inheritance, manual care must be taken to not invoke
 * a parent initializer twice, or ensure that all initializers are idempotent,
 * because this is not dealt with automatically as with constructors.
 */
contract Initializable {

  /**
   * @dev Indicates that the contract has been initialized.
   */
  bool private initialized;

  /**
   * @dev Indicates that the contract is in the process of being initialized.
   */
```

```
  bool private initializing;

  /**
   * @dev Modifier to use in the initializer function of a contract.
   */
  modifier initializer() {
    require(initializing || isConstructor() || !initialized, "Contract instance has
already been initialized");

    bool isTopLevelCall = !initializing;
    if (isTopLevelCall) {
      initializing = true;
      initialized = true;
    }

    _;

    if (isTopLevelCall) {
      initializing = false;
    }
  }

  /**
   * @dev Modifier to use in the initializer function of a contract when upgrade EVEN
times.
   */
  modifier initializerEven() {
    require(initializing || isConstructor() || initialized, "Contract instance has
already been initialized EVEN times");

    bool isTopLevelCall = !initializing;
    if (isTopLevelCall) {
      initializing = true;
      initialized = false;
    }

    _;

    if (isTopLevelCall) {
      initializing = false;
    }
  }

  /// @dev Returns true if and only if the function is running in the constructor
  function isConstructor() private view returns (bool) {
    // extcodesize checks the size of the code stored in an address, and
    // address returns the current address. Since the code is still not
    // deployed when running a constructor, any checks on its code size will
    // yield zero, making it an effective way to detect if a contract is
    // under construction or not.
    address self = address(this);
    uint256 cs;
    assembly { cs := extcodesize(self) }
    return cs == 0;
  }

  // Reserved storage space to allow for layout changes in the future.
  uint256[50] private ______gap;
}


contract Governable is Initializable {
    address public governor;

    event GovernorshipTransferred(address indexed previousGovernor, address indexed
newGovernor);

    /**
     * @dev Contract initializer.
     * called once by the factory at time of deployment
     */
    function initialize(address governor_) virtual public initializer {
        governor = governor_;
        emit GovernorshipTransferred(address(0), governor);
    }

    modifier governance() {
```

```
        require(msg.sender == governor);
        _;
    }

    /**
     * @dev Allows the current governor to relinquish control of the contract.
     * @notice Renouncing to governorship will leave the contract without an governor.
     * It will not be possible to call the functions with the `governance`
     * modifier anymore.
     */
    function renounceGovernorship() public governance {
        emit GovernorshipTransferred(governor, address(0));
        governor = address(0);
    }

    /**
     * @dev Allows the current governor to transfer control of the contract to a
newGovernor.
     * @param newGovernor The address to transfer governorship to.
     */
    function transferGovernorship(address newGovernor) public governance {
        _transferGovernorship(newGovernor);
    }

    /**
     * @dev Transfers control of the contract to a newGovernor.
     * @param newGovernor The address to transfer governorship to.
     */
    function _transferGovernorship(address newGovernor) internal {
        require(newGovernor != address(0));
        emit GovernorshipTransferred(governor, newGovernor);
        governor = newGovernor;
    }
}


contract Configurable is Governable {

    mapping (bytes32 => uint) internal config;

    function getConfig(bytes32 key) public view returns (uint) {
        return config[key];
    }
    function getConfig(bytes32 key, uint index) public view returns (uint) {
        return config[bytes32(uint(key) ^ index)];
    }
    function getConfig(bytes32 key, address addr) public view returns (uint) {
        return config[bytes32(uint(key) ^ uint(addr))];
    }

    function _setConfig(bytes32 key, uint value) internal {
        if(config[key] != value)
            config[key] = value;
    }
    function _setConfig(bytes32 key, uint index, uint value) internal {
        _setConfig(bytes32(uint(key) ^ index), value);
    }
    function _setConfig(bytes32 key, address addr, uint value) internal {
        _setConfig(bytes32(uint(key) ^ uint(addr)), value);
    }

    function setConfig(bytes32 key, uint value) external governance {
        _setConfig(key, value);
    }
    function setConfig(bytes32 key, uint index, uint value) external governance {
        _setConfig(bytes32(uint(key) ^ index), value);
    }
    function setConfig(bytes32 key, address addr, uint value) external governance {
        _setConfig(bytes32(uint(key) ^ uint(addr)), value);
    }
}
// SPDX-License-Identifier: MIT

pragma solidity ^0.6.0;

/*
 * @dev Provides information about the current execution context, including the
```

```
 * sender of the transaction and its data. While these are generally available
 * via msg.sender and msg.data, they should not be accessed in such a direct
 * manner, since when dealing with GSN meta-transactions the account sending and
 * paying for execution may not be the actual sender (as far as an application
 * is concerned).
 *
 * This contract is only required for intermediate, library-like contracts.
 */
abstract contract Context {
    function _msgSender() internal view virtual returns (address payable) {
        return msg.sender;
    }

    function _msgData() internal view virtual returns (bytes memory) {
        this; // silence state mutability warning without generating bytecode - see
https://github.com/ethereum/solidity/issues/2691
        return msg.data;
    }
}


/**
 * @dev Wrappers over Solidity's arithmetic operations with added overflow
 * checks.
 *
 * Arithmetic operations in Solidity wrap on overflow. This can easily result
 * in bugs, because programmers usually assume that an overflow raises an
 * error, which is the standard behavior in high level programming languages.
 * `SafeMath` restores this intuition by reverting the transaction when an
 * operation overflows.
 *
 * Using this library instead of the unchecked operations eliminates an entire
 * class of bugs, so it's recommended to use it always.
 */
library SafeMath {
    /**
     * @dev Returns the addition of two unsigned integers, reverting on
     * overflow.
     *
     * Counterpart to Solidity's `+` operator.
     *
     * Requirements:
     *
     * - Addition cannot overflow.
     */
    function add(uint256 a, uint256 b) internal pure returns (uint256) {
        uint256 c = a + b;
        require(c >= a, "SafeMath: addition overflow");

        return c;
    }

    /**
     * @dev Returns the subtraction of two unsigned integers, reverting on
     * overflow (when the result is negative).
     *
     * Counterpart to Solidity's `-` operator.
     *
     * Requirements:
     *
     * - Subtraction cannot overflow.
     */
    function sub(uint256 a, uint256 b) internal pure returns (uint256) {
        return sub(a, b, "SafeMath: subtraction overflow");
    }

    /**
     * @dev Returns the subtraction of two unsigned integers, reverting with custom
message on
     * overflow (when the result is negative).
     *
     * Counterpart to Solidity's `-` operator.
     *
     * Requirements:
     *
     * - Subtraction cannot overflow.
     */
```

```
    function sub(uint256 a, uint256 b, string memory errorMessage) internal pure
returns (uint256) {
        require(b <= a, errorMessage);
        uint256 c = a - b;

        return c;
    }

    /**
     * @dev Returns the multiplication of two unsigned integers, reverting on
     * overflow.
     *
     * Counterpart to Solidity's `*` operator.
     *
     * Requirements:
     *
     * - Multiplication cannot overflow.
     */
    function mul(uint256 a, uint256 b) internal pure returns (uint256) {
        // Gas optimization: this is cheaper than requiring 'a' not being zero, but the
        // benefit is lost if 'b' is also tested.
        // See: https://github.com/OpenZeppelin/openzeppelin-contracts/pull/522
        if (a == 0) {
            return 0;
        }

        uint256 c = a * b;
        require(c / a == b, "SafeMath: multiplication overflow");

        return c;
    }

    /**
     * @dev Returns the integer division of two unsigned integers. Reverts on
     * division by zero. The result is rounded towards zero.
     *
     * Counterpart to Solidity's `/` operator. Note: this function uses a
     * `revert` opcode (which leaves remaining gas untouched) while Solidity
     * uses an invalid opcode to revert (consuming all remaining gas).
     *
     * Requirements:
     *
     * - The divisor cannot be zero.
     */
    function div(uint256 a, uint256 b) internal pure returns (uint256) {
        return div(a, b, "SafeMath: division by zero");
    }

    /**
     * @dev Returns the integer division of two unsigned integers. Reverts with custom
message on
     * division by zero. The result is rounded towards zero.
     *
     * Counterpart to Solidity's `/` operator. Note: this function uses a
     * `revert` opcode (which leaves remaining gas untouched) while Solidity
     * uses an invalid opcode to revert (consuming all remaining gas).
     *
     * Requirements:
     *
     * - The divisor cannot be zero.
     */
    function div(uint256 a, uint256 b, string memory errorMessage) internal pure
returns (uint256) {
        require(b > 0, errorMessage);
        uint256 c = a / b;
        // assert(a == b * c + a % b); // There is no case in which this doesn't hold

        return c;
    }

    /**
     * @dev Returns the remainder of dividing two unsigned integers. (unsigned integer
modulo),
     * Reverts when dividing by zero.
     *
     * Counterpart to Solidity's `%` operator. This function uses a `revert`
     * opcode (which leaves remaining gas untouched) while Solidity uses an
```

```
     * invalid opcode to revert (consuming all remaining gas).
     *
     * Requirements:
     *
     * - The divisor cannot be zero.
     */
    function mod(uint256 a, uint256 b) internal pure returns (uint256) {
        return mod(a, b, "SafeMath: modulo by zero");
    }

    /**
     * @dev Returns the remainder of dividing two unsigned integers. (unsigned integer
modulo),
     * Reverts with custom message when dividing by zero.
     *
     * Counterpart to Solidity's `%` operator. This function uses a `revert`
     * opcode (which leaves remaining gas untouched) while Solidity uses an
     * invalid opcode to revert (consuming all remaining gas).
     *
     * Requirements:
     *
     * - The divisor cannot be zero.
     */
    function mod(uint256 a, uint256 b, string memory errorMessage) internal pure
returns (uint256) {
        require(b != 0, errorMessage);
        return a % b;
    }

     function sqrt(uint x)public pure returns(uint y) {
        uint z = (x + 1) / 2;
        y = x;
        while (z < y) {
            y = z;
            z = (x / z + z) / 2;
        }
    }
}


/**
 * @dev Collection of functions related to the address type
 */
library Address {
    /**
     * @dev Returns true if `account` is a contract.
     *
     * [IMPORTANT]
     * ====
     * It is unsafe to assume that an address for which this function returns
     * false is an externally-owned account (EOA) and not a contract.
     *
     * Among others, `isContract` will return false for the following
     * types of addresses:
     *
     *  - an externally-owned account
     *  - a contract in construction
     *  - an address where a contract will be created
     *  - an address where a contract lived, but was destroyed
     * ====
     */
    function isContract(address account) internal view returns (bool) {
        // This method relies in extcodesize, which returns 0 for contracts in
        // construction, since the code is only stored at the end of the
        // constructor execution.

        uint256 size;
        // solhint-disable-next-line no-inline-assembly
        assembly { size := extcodesize(account) }
        return size > 0;
    }

    /**
     * @dev Replacement for Solidity's `transfer`: sends `amount` wei to
     * `recipient`, forwarding all available gas and reverting on errors.
     *
     * https://eips.ethereum.org/EIPS/eip-1884[EIP1884] increases the gas cost
```

```
     * of certain opcodes, possibly making contracts go over the 2300 gas limit
     * imposed by `transfer`, making them unable to receive funds via
     * `transfer`. {sendValue} removes this limitation.
     *
     * https://diligence.consensys.net/posts/2019/09/stop-using-soliditys-transfer-
now/[Learn more].
     *
     * IMPORTANT: because control is transferred to `recipient`, care must be
     * taken to not create reentrancy vulnerabilities. Consider using
     * {ReentrancyGuard} or the
     * https://solidity.readthedocs.io/en/v0.5.11/security-considerations.html#use-the-
checks-effects-interactions-pattern[checks-effects-interactions pattern].
     */
    function sendValue(address payable recipient, uint256 amount) internal {
        require(address(this).balance >= amount, "Address: insufficient balance");

        // solhint-disable-next-line avoid-low-level-calls, avoid-call-value
        (bool success, ) = recipient.call{ value: amount }("");
        require(success, "Address: unable to send value, recipient may have reverted");
    }

    /**
     * @dev Performs a Solidity function call using a low level `call`. A
     * plain`call` is an unsafe replacement for a function call: use this
     * function instead.
     *
     * If `target` reverts with a revert reason, it is bubbled up by this
     * function (like regular Solidity function calls).
     *
     * Returns the raw returned data. To convert to the expected return value,
     * use https://solidity.readthedocs.io/en/latest/units-and-global-
variables.html?highlight=abi.decode#abi-encoding-and-decoding-functions[`abi.decode`].
     *
     * Requirements:
     *
     * - `target` must be a contract.
     * - calling `target` with `data` must not revert.
     *
     * _Available since v3.1._
     */
    function functionCall(address target, bytes memory data) internal returns (bytes
memory) {
      return functionCall(target, data, "Address: low-level call failed");
    }

    /**
     * @dev Same as {xref-Address-functionCall-address-bytes-}[`functionCall`], but
with
     * `errorMessage` as a fallback revert reason when `target` reverts.
     *
     * _Available since v3.1._
     */
    function functionCall(address target, bytes memory data, string memory
errorMessage) internal returns (bytes memory) {
        return _functionCallWithValue(target, data, 0, errorMessage);
    }

    /**
     * @dev Same as {xref-Address-functionCall-address-bytes-}[`functionCall`],
     * but also transferring `value` wei to `target`.
     *
     * Requirements:
     *
     * - the calling contract must have an ETH balance of at least `value`.
     * - the called Solidity function must be `payable`.
     *
     * _Available since v3.1._
     */
    function functionCallWithValue(address target, bytes memory data, uint256 value)
internal returns (bytes memory) {
        return functionCallWithValue(target, data, value, "Address: low-level call with
value failed");
    }

    /**
     * @dev Same as {xref-Address-functionCallWithValue-address-bytes-
uint256-}[`functionCallWithValue`], but
```

```
     * with `errorMessage` as a fallback revert reason when `target` reverts.
     *
     * _Available since v3.1._
     */
    function functionCallWithValue(address target, bytes memory data, uint256 value,
string memory errorMessage) internal returns (bytes memory) {
        require(address(this).balance >= value, "Address: insufficient balance for
call");
        return _functionCallWithValue(target, data, value, errorMessage);
    }

    function _functionCallWithValue(address target, bytes memory data, uint256
weiValue, string memory errorMessage) private returns (bytes memory) {
        require(isContract(target), "Address: call to non-contract");

        // solhint-disable-next-line avoid-low-level-calls
        (bool success, bytes memory returndata) = target.call{ value: weiValue }(data);
        if (success) {
            return returndata;
        } else {
            // Look for revert reason and bubble it up if present
            if (returndata.length > 0) {
                // The easiest way to bubble the revert reason is using memory via
assembly

                // solhint-disable-next-line no-inline-assembly
                assembly {
                    let returndata_size := mload(returndata)
                    revert(add(32, returndata), returndata_size)
                }
            } else {
                revert(errorMessage);
            }
        }
    }
}


/**
 * @dev Interface of the ERC20 standard as defined in the EIP.
 */
interface IERC20 {
    /**
     * @dev Returns the amount of tokens in existence.
     */
    function totalSupply() external view returns (uint256);

    /**
     * @dev Returns the amount of tokens owned by `account`.
     */
    function balanceOf(address account) external view returns (uint256);

    /**
     * @dev Moves `amount` tokens from the caller's account to `recipient`.
     *
     * Returns a boolean value indicating whether the operation succeeded.
     *
     * Emits a {Transfer} event.
     */
    function transfer(address recipient, uint256 amount) external returns (bool);

    /**
     * @dev Returns the remaining number of tokens that `spender` will be
     * allowed to spend on behalf of `owner` through {transferFrom}. This is
     * zero by default.
     *
     * This value changes when {approve} or {transferFrom} are called.
     */
    function allowance(address owner, address spender) external view returns (uint256);

    /**
     * @dev Sets `amount` as the allowance of `spender` over the caller's tokens.
     *
     * Returns a boolean value indicating whether the operation succeeded.
     *
     * IMPORTANT: Beware that changing an allowance with this method brings the risk
     * that someone may use both the old and the new allowance by unfortunate
```

```
     * transaction ordering. One possible solution to mitigate this race
     * condition is to first reduce the spender's allowance to 0 and set the
     * desired value afterwards:
     * https://github.com/ethereum/EIPs/issues/20#issuecomment-263524729
     *
     * Emits an {Approval} event.
     */
    function approve(address spender, uint256 amount) external returns (bool);

    /**
     * @dev Moves `amount` tokens from `sender` to `recipient` using the
     * allowance mechanism. `amount` is then deducted from the caller's
     * allowance.
     *
     * Returns a boolean value indicating whether the operation succeeded.
     *
     * Emits a {Transfer} event.
     */
    function transferFrom(address sender, address recipient, uint256 amount) external
returns (bool);

    /**
     * @dev Emitted when `value` tokens are moved from one account (`from`) to
     * another (`to`).
     *
     * Note that `value` may be zero.
     */
    event Transfer(address indexed from, address indexed to, uint256 value);

    /**
     * @dev Emitted when the allowance of a `spender` for an `owner` is set by
     * a call to {approve}. `value` is the new allowance.
     */
    event Approval(address indexed owner, address indexed spender, uint256 value);
}


/**
 * @dev Implementation of the {IERC20} interface.
 *
 * This implementation is agnostic to the way tokens are created. This means
 * that a supply mechanism has to be added in a derived contract using {_mint}.
 * For a generic mechanism see {ERC20PresetMinterPauser}.
 *
 * TIP: For a detailed writeup see our guide
 * https://forum.zeppelin.solutions/t/how-to-implement-erc20-supply-mechanisms/226[How
 * to implement supply mechanisms].
 *
 * We have followed general OpenZeppelin guidelines: functions revert instead
 * of returning `false` on failure. This behavior is nonetheless conventional
 * and does not conflict with the expectations of ERC20 applications.
 *
 * Additionally, an {Approval} event is emitted on calls to {transferFrom}.
 * This allows applications to reconstruct the allowance for all accounts just
 * by listening to said events. Other implementations of the EIP may not emit
 * these events, as it isn't required by the specification.
 *
 * Finally, the non-standard {decreaseAllowance} and {increaseAllowance}
 * functions have been added to mitigate the well-known issues around setting
 * allowances. See {IERC20-approve}.
 */
contract ERC20 is Context, IERC20 {
    using SafeMath for uint256;
    using Address for address;

    mapping (address => uint256) public _balances;

    mapping (address => mapping (address => uint256)) internal _allowances;

    uint256 public _totalSupply;

    string internal _name;
    string internal _symbol;
    uint8 internal _decimals;

    /**
     * @dev Sets the values for {name} and {symbol}, initializes {decimals} with
```

```
     * a default value of 18.
     *
     * To select a different value for {decimals}, use {_setupDecimals}.
     *
     * All three of these values are immutable: they can only be set once during
     * construction.
     */
    constructor (string memory name, string memory symbol) public {
        _name = name;
        _symbol = symbol;
        _decimals = 18;
    }

    /**
     * @dev Returns the name of the token.
     */
    function name() public view returns (string memory) {
        return _name;
    }

    /**
     * @dev Returns the symbol of the token, usually a shorter version of the
     * name.
     */
    function symbol() public view returns (string memory) {
        return _symbol;
    }

    /**
     * @dev Returns the number of decimals used to get its user representation.
     * For example, if `decimals` equals `2`, a balance of `505` tokens should
     * be displayed to a user as `5,05` (`505 / 10 ** 2`).
     *
     * Tokens usually opt for a value of 18, imitating the relationship between
     * Ether and Wei. This is the value {ERC20} uses, unless {_setupDecimals} is
     * called.
     *
     * NOTE: This information is only used for _display_ purposes: it in
     * no way affects any of the arithmetic of the contract, including
     * {IERC20-balanceOf} and {IERC20-transfer}.
     */
    function decimals() public view returns (uint8) {
        return _decimals;
    }

    /**
     * @dev See {IERC20-totalSupply}.
     */
    function totalSupply() public view virtual override returns (uint256) {
        return _totalSupply;
    }

    /**
     * @dev See {IERC20-balanceOf}.
     */
    function balanceOf(address account) public view virtual override returns (uint256)
{
        return _balances[account];
    }

    /**
     * @dev See {IERC20-transfer}.
     *
     * Requirements:
     *
     * - `recipient` cannot be the zero address.
     * - the caller must have a balance of at least `amount`.
     */
    function transfer(address recipient, uint256 amount) public virtual override
returns (bool) {
        _transfer(_msgSender(), recipient, amount);
        return true;
    }

    /**
     * @dev See {IERC20-allowance}.
     */
```

```
    function allowance(address owner, address spender) public view virtual override
returns (uint256) {
        return _allowances[owner][spender];
    }

    /**
     * @dev See {IERC20-approve}.
     *
     * Requirements:
     *
     * - `spender` cannot be the zero address.
     */
    function approve(address spender, uint256 amount) public virtual override returns
(bool) {
        _approve(_msgSender(), spender, amount);
        return true;
    }

    /**
     * @dev See {IERC20-transferFrom}.
     *
     * Emits an {Approval} event indicating the updated allowance. This is not
     * required by the EIP. See the note at the beginning of {ERC20};
     *
     * Requirements:
     * - `sender` and `recipient` cannot be the zero address.
     * - `sender` must have a balance of at least `amount`.
     * - the caller must have allowance for ``sender``'s tokens of at least
     * `amount`.
     */
    function transferFrom(address sender, address recipient, uint256 amount) public
virtual override returns (bool) {
        _transfer(sender, recipient, amount);
        _approve(sender, _msgSender(), _allowances[sender][_msgSender()].sub(amount,
"ERC20: transfer amount exceeds allowance"));
        return true;
    }

    /**
     * @dev Atomically increases the allowance granted to `spender` by the caller.
     *
     * This is an alternative to {approve} that can be used as a mitigation for
     * problems described in {IERC20-approve}.
     *
     * Emits an {Approval} event indicating the updated allowance.
     *
     * Requirements:
     *
     * - `spender` cannot be the zero address.
     */
    function increaseAllowance(address spender, uint256 addedValue) public virtual
returns (bool) {
        _approve(_msgSender(), spender,
_allowances[_msgSender()][spender].add(addedValue));
        return true;
    }

    /**
     * @dev Atomically decreases the allowance granted to `spender` by the caller.
     *
     * This is an alternative to {approve} that can be used as a mitigation for
     * problems described in {IERC20-approve}.
     *
     * Emits an {Approval} event indicating the updated allowance.
     *
     * Requirements:
     *
     * - `spender` cannot be the zero address.
     * - `spender` must have allowance for the caller of at least
     * `subtractedValue`.
     */
    function decreaseAllowance(address spender, uint256 subtractedValue) public virtual
returns (bool) {
        _approve(_msgSender(), spender,
_allowances[_msgSender()][spender].sub(subtractedValue, "ERC20: decreased allowance
below zero"));
        return true;
```

```
    }

    /**
     * @dev Moves tokens `amount` from `sender` to `recipient`.
     *
     * This is internal function is equivalent to {transfer}, and can be used to
     * e.g. implement automatic token fees, slashing mechanisms, etc.
     *
     * Emits a {Transfer} event.
     *
     * Requirements:
     *
     * - `sender` cannot be the zero address.
     * - `recipient` cannot be the zero address.
     * - `sender` must have a balance of at least `amount`.
     */
    function _transfer(address sender, address recipient, uint256 amount) internal
virtual {
        require(sender != address(0), "ERC20: transfer from the zero address");
        require(recipient != address(0), "ERC20: transfer to the zero address");

        _beforeTokenTransfer(sender, recipient, amount);

        _balances[sender] = _balances[sender].sub(amount, "ERC20: transfer amount
exceeds balance");
        _balances[recipient] = _balances[recipient].add(amount);
        emit Transfer(sender, recipient, amount);
    }

    /** @dev Creates `amount` tokens and assigns them to `account`, increasing
     * the total supply.
     *
     * Emits a {Transfer} event with `from` set to the zero address.
     *
     * Requirements
     *
     * - `to` cannot be the zero address.
     */
    function _mint(address account, uint256 amount) internal virtual {
        require(account != address(0), "ERC20: mint to the zero address");

        _beforeTokenTransfer(address(0), account, amount);

        _totalSupply = _totalSupply.add(amount);
        _balances[account] = _balances[account].add(amount);
        emit Transfer(address(0), account, amount);
    }

    /**
     * @dev Destroys `amount` tokens from `account`, reducing the
     * total supply.
     *
     * Emits a {Transfer} event with `to` set to the zero address.
     *
     * Requirements
     *
     * - `account` cannot be the zero address.
     * - `account` must have at least `amount` tokens.
     */
    function _burn(address account, uint256 amount) internal virtual {
        require(account != address(0), "ERC20: burn from the zero address");

        _beforeTokenTransfer(account, address(0), amount);

        _balances[account] = _balances[account].sub(amount, "ERC20: burn amount exceeds
balance");
        _totalSupply = _totalSupply.sub(amount);
        emit Transfer(account, address(0), amount);
    }

    /**
     * @dev Sets `amount` as the allowance of `spender` over the `owner`s tokens.
     *
     * This is internal function is equivalent to `approve`, and can be used to
     * e.g. set automatic allowances for certain subsystems, etc.
     *
     * Emits an {Approval} event.
```

```
     *
     * Requirements:
     *
     * - `owner` cannot be the zero address.
     * - `spender` cannot be the zero address.
     */
    function _approve(address owner, address spender, uint256 amount) internal virtual
{
        require(owner != address(0), "ERC20: approve from the zero address");
        require(spender != address(0), "ERC20: approve to the zero address");

        _allowances[owner][spender] = amount;
        emit Approval(owner, spender, amount);
    }

    /**
     * @dev Sets {decimals} to a value other than the default one of 18.
     *
     * WARNING: This function should only be called from the constructor. Most
     * applications that interact with token contracts will not expect
     * {decimals} to ever change, and may work incorrectly if it does.
     */
    function _setupDecimals(uint8 decimals_) internal {
        _decimals = decimals_;
    }

    /**
     * @dev Hook that is called before any transfer of tokens. This includes
     * minting and burning.
     *
     * Calling conditions:
     *
     * - when `from` and `to` are both non-zero, `amount` of ``from``'s tokens
     * will be to transferred to `to`.
     * - when `from` is zero, `amount` tokens will be minted for `to`.
     * - when `to` is zero, `amount` of ``from``'s tokens will be burned.
     * - `from` and `to` are never both zero.
     *
     * To learn more about hooks, head to xref:ROOT:extending-contracts.adoc#using-
hooks[Using Hooks].
     */
    function _beforeTokenTransfer(address from, address to, uint256 amount) internal
virtual { }

}


contract SfgToken is ERC20 {

    constructor(address SfgFarm) ERC20("Stable Finance Governance Token", "SFG")
public {
        uint8 decimals = 18;
        _setupDecimals(decimals);

        _mint(SfgFarm,  21000000 * 10 ** uint256(decimals));      // 100%, 21000000
    }
}

contract SfyToken is ERC20 {

    constructor(address SfyFarm) ERC20("Stable Finance Yield Token", "SFY") public {
        uint8 decimals = 18;
        _setupDecimals(decimals);

        _mint(SfyFarm,  21000000 * 10 ** uint256(decimals));      // 100%, 21000000
    }
}
pragma solidity ^0.6.0;

// helper methods for interacting with ERC20 tokens and sending ETH that do not
consistently return true/false
library TransferHelper {
    function safeApprove(address token, address to, uint value) internal {
        // bytes4(keccak256(bytes('approve(address,uint256)')));
        (bool success, bytes memory data) =
token.call(abi.encodeWithSelector(0x095ea7b3, to, value));
        require(success && (data.length == 0 || abi.decode(data, (bool))),
```

```
'TransferHelper: APPROVE_FAILED');
    }

    function safeTransfer(address token, address to, uint value) internal {
        // bytes4(keccak256(bytes('transfer(address,uint256)')));
        (bool success, bytes memory data) =
token.call(abi.encodeWithSelector(0xa9059cbb, to, value));
        require(success && (data.length == 0 || abi.decode(data, (bool))),
'TransferHelper: TRANSFER_FAILED');
    }

    function safeTransferFrom(address token, address from, address to, uint value)
internal {
        // bytes4(keccak256(bytes('transferFrom(address,address,uint256)')));
        (bool success, bytes memory data) =
token.call(abi.encodeWithSelector(0x23b872dd, from, to, value));
        require(success && (data.length == 0 || abi.decode(data, (bool))),
'TransferHelper: TRANSFER_FROM_FAILED');
    }

    function safeTransferETH(address to, uint value) internal {
        (bool success,) = to.call{value:value}(new bytes(0));
        require(success, 'TransferHelper: ETH_TRANSFER_FAILED');
    }
}
```

5. 附录 B：漏洞风险评级标准

智能合约漏洞评级标准	
漏洞评级	**漏洞评级说明**

高危漏洞	能直接造成代币合约或用户资金损失的漏洞，如：能造成代币价值归零的数值溢出漏洞、能造成交易所损失代币的假充值漏洞、能造成合约账户损失 ETH 或代币的重入漏洞等； 能造成代币合约归属权丢失的漏洞，如：关键函数的访问控制缺陷、call 注入导致关键函数访问控制绕过等； 能造成代币合约无法正常工作的漏洞，如：因向恶意地址发送 ETH 导致的拒绝服务漏洞、因 gas 耗尽导致的拒绝服务漏洞。
中危漏洞	需要特定地址才能触发的高风险漏洞，如代币合约拥有者才能触发的数值溢出漏洞等；非关键函数的访问控制缺陷、不能造成直接资金损失的逻辑设计缺陷等。
低危漏洞	难以被触发的漏洞、触发之后危害有限的漏洞，如需要大量 ETH 或代币才能触发的数值溢出漏洞、触发数值溢出后攻击者无法直接获利的漏洞、通过指定高 gas 触发的事务顺序依赖风险等。

6. 附录 C：漏洞测试工具简介

6.1. MaABBTicore

MaABBTicore 是一个分析二进制文件和智能合约的符号执行工具，MaABBTicore 包含一个符号以太坊虚拟机（EVM），一个 EVM 反汇编器/汇编器以及一个用于自动编译和分析 Solidity 的方便界面。它还集成了 Ethersplay，用于 EVM 字节码的 Bit of Traits of Bits 可视化反汇编程序，用于可视化分析。 与二进制文件一样，MaABBTicore 提供了一个简单的命令行界面和一个用于分析 EVM 字节码的 Python API。

6.2. OyeABBTe

OyeABBTe 是一个智能合约分析工具，OyeABBTe 可以用来检测智能合约中常见的 bug，比如 reeABBTrancy、事务排序依赖等等。更方便的是，OyeABBTe 的设计是模块化的，所以这让高级用户可以实现并插入他们自己的检测逻辑，以检查他们的合约中自定义的属性。

6.3. securify.sh

Securify 可以验证以太坊智能合约常见的安全问题，例如交易乱序和缺少输入验证，它在全自动化的同时分析程序所有可能的执行路径，此外，Securify 还具有用于指定漏洞的特定语言，这使 Securify 能够随时关注当前的安全性和其他可靠性问题。

6.4. Echidna

Echidna 是一个为了对 EVM 代码进行模糊测试而设计的 Haskell 库。

6.5. MAIAN

MAIAN 是一个用于查找以太坊智能合约漏洞的自动化工具，Maian 处理合约的字节码，并尝试建立一系列交易以找出并确认错误。

6.6. ethersplay

ethersplay 是一个 EVM 反汇编器，其中包含了相关分析工具。

6.7. ida-evm

ida-evm 是一个针对以太坊虚拟机（EVM）的 IDA 处理器模块。

6.8. Remix-ide

Remix 是一款基于浏览器的编译器和 IDE，可让用户使用 Solidity 语言构建以太坊合约并调试交易。

6.9. 知道创宇渗透测试人员专用工具包

知道创宇渗透测试人员专用工具包，由知道创宇渗透测试工程师研发，收集和使用，包含专用于测试人员的批量自动测试工具，自主研发的工具、脚本或利用工具等。

知道创宇

北京知道创宇信息技术股份有限公司

咨询电话 +86(10)400 060 9587

邮　　箱 sec@knownsec.com

官　　网 www.knownsec.com

地　　址 北京市 朝阳区 望京 SOHO T2-B座-2509