



Melos Token 审计报告

版本：1.0.0

报告编号：2022021500011016

Fairyproof 发布

2022 年 2 月 15 日

01. 介绍

本报告包含了Fairyproof对Melos通证智能合约源码进行审计的结果。

审计开始时间:

2022年2月15日

审计结束时间:

2022年2月15日

通证名:

MELOS

通证符号:

MELOS

通证精度:

18

审计代码文件及目录结构:

审计结束时的代码文件名及对应的SHA-256哈希值为:

```
MELOS.sol      :  
0xea23cddfa849282be5c90f99a9502842c4718064c14de6c131929966ad6725b8
```

本次审计的目的是通过审阅MELOS通证发行合约，发现是否存在潜在的安全隐患，研究其设计、架构，并试图找到可能存在的漏洞。

我们全面阅读了上述代码，并仔细审阅了上述代码中可能出现的各种问题，对审计的合约源码给出了全面、综合的改进意见及评审结果。

本次审计仅针对授权方指定版本的代码、安装包及其它授权方提供的素材展开，其结论仅对相应版本的应用适用，一旦相关代码、配置、运营环境等发生变化，相应结论将不再适用。

— 免责声明

截至本报告发布之日，本报告所阐述的内容仅反映审计团队对当前所审计的代码安全进展及状况的理解。任何人在接触或使用与本报告相关的服务、产品、协议、平台、或任何物品时，自行承担一切可能产生的冲突、损失、利益及风险，本报告的审计团队概不负责。

本审计不涉及审计代码的编译器及任何超出代码编程语言的领域。如果所审计的代码为智能合约，则合约由引用链下信息或资源所导致的风险及责任不在本审计覆盖的范围之内。

本审计无法详尽查看每一个细节，也无法穷尽每一种可能，因此本报告的审计团队鼓励本项目的开发团队及任何相关利益方对所审计代码进行任何后续的测试及审计。

对任何第三方使用本报告中所提及或涉及的软件、源码、软件库、产品、服务、信息这一切事物所产生的冲突、损失、利益及风险，本审计团队不保证、不承诺也不承担任何责任。

本报告的内容、获取方式、使用以及任何其所涉及的服务或资源都不能作为任何形式的投资、税务、法律、监管及建议等的依据，也不产生相关的责任。

— 审计方式

审计MELOS通证智能合约源码是为了能清晰地理解该通证的实现方式及运行原理。审计团队对项目代码进行了深入的研究、分析和测试，并收集了详尽的数据。审计团队会在本报告中会详细列举所发现的每个问题、问题所在的源码位置、问题产生的根源以及对问题的描述，并对问题给出相应的改进建议。

Fairyproof审计的流程如下：

1. 背景研究。Fairyproof团队会阅读项目介绍、白皮书、合约源码等一切相关材料与信息，以确保Fairyproof团队理解项目的规模、范围及功能。
2. 自动化检测。此步骤主要用自动化工具扫描源码，找到常见的潜在漏洞。
3. 人工审阅项目代码。此步骤由工程师逐行阅读代码，找到潜在的漏洞。
4. 逻辑校对。此步骤审计工程师将对代码的理解与所提供的材料及信息相比较，检查代码的实现是否符合项目的定义及白皮书等信息中的描述。
5. 测试用例检测。此步骤包括三部分：
 - i. 测试用例设计。审计工程师将根据前述步骤对项目背景的理解及合约代码的理解，针对项目可能的执行逻辑及方式设计测试用例。
 - ii. 测试范围分析。该步骤会详细检查所设计的测试用例是否覆盖了合约代码的所有逻辑分支，并判断测试用例执行后，合约代码的逻辑是否能得到充分的执行及检查
 - iii. 符号执行。该步骤将运行测试用例以测试代码所有可能的执行路径。
6. 优化审查。该流程将根据合约的应用场景、调用方式及业界最新的研究成果从可维护性、安全性及可操作性等方面审查项目代码。

— 报告结构

本报告列举的每个问题都被设置了一个安全级别，这些安全级别根据其对项目的影响及安全隐患的大小而定。我们对每个问题都给出了相应的改进建议。为了便于读者阅读，我们分别按主题内容和安全级别这两种方式罗列了所有的问题，并提出了全面增强安全性的建议。

— 引用文档

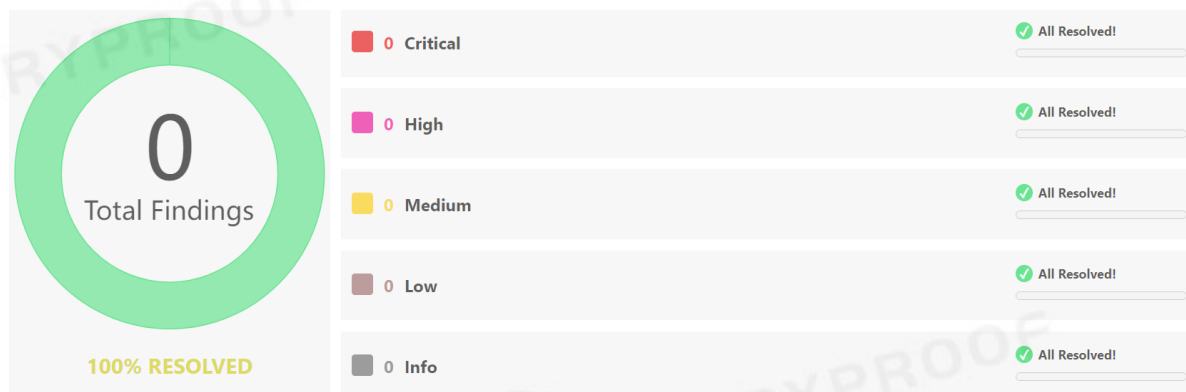
在审阅过程中，我们参考了与项目相关的文档以加深对审计通证合约逻辑、功能及应用的理解。本次报告参阅的文档资料如下：

合约源码

上述文档被视为审计通证合约的实现及功能的定义。

一 审计结果

审计编号	审计团队	审计时间	审计结果
2022021500011016	Fairyproof Security Team	2022.02.15 - 2022.02.15	通过



审计结论:

Fairyproof团队综合使用了自动化工具和人工方式审计了本项目，暂未发现风险。

02. Fairyproof介绍

[Fairyproof](#)是一家领先的区块链技术公司，公司为行业企业提供安全审计和咨询方面的服务。Fairyproof研发了自己的一系列合约编写和安全审计标准，为众多客户提供了周到、严谨的服务。

03. 审计代码的主要功能

被审计代码的主要功能为通证发行，细节如下：

通证名称：MELOS

通证符号：MELOS

代币精度：18

发行总量：1,000,000,000 枚

增发/燃烧：不可增发/可燃烧

暂停/冻结：不可暂停/不可冻结

是否通缩：否

其它事项：无

04. 风险种类

当前审计采用智能工具静态分析和人工审计相结合的方法，从以下多个风险种类方面对项目代码进行了全方位的审计。

- 重入攻击
- 重放攻击
- 重排攻击
- 矿工特权
- 回滚攻击
- 注入攻击
- 拒绝服务攻击
- 交易顺序依赖
- 条件竞争攻击
- 权限控制攻击
- 整数上溢/下溢攻击
- 时间戳依赖攻击
- Gas 使用
- 冗余的回调函数
- 函数状态变量的显式可见性
- 逻辑缺陷
- 未声明的存储指针
- 算术精度误差
- tx.origin 身份验证
- 假充值漏洞
- 变量覆盖
- 设计缺陷
- 潜在后门
- 代币发行
- 管理权限
- 代理升级
- 委托调用插槽共享
- 用户资金安全
- 迁移管理
- 代码优化
- 其它分类

05. 风险分级

本报告中的每个问题都被设置了一个安全等级，程度由高到低排列如下：

致命 风险及隐患需要立刻解决。

高危 风险及隐患将引发风险及问题，必须解决。

中度 风险及隐患可能导致潜在风险，最终仍然需要解决。

低 风险及隐患主要指各类处理不当或者会引发警告信息的细节，这类问题可以暂时搁置，但建议最终解决。

信息 一般不会引起风险问题，主要是代码的改进与优化。

06. 本审计关注的风险重点

根据所审计代码的功能及应用场景，我们着重审查了下列功能中可能潜藏的风险。

- 数值安全

我们检查了合约中的数值处理是否有算术溢出问题。常规的加减运算容易引起整数溢出，尤其是在处理通证金额或计算奖励金额时，本合约均使用了严谨的数学模块进行了处理。

经审查此功能暂未发现明显风险。

- 权限检查

我们检查了每一个能改变合约状态的函数是否具备合适的权限，重点检查那些必须管理员权限才能操作的函数。

经审查此功能暂未发现明显风险。

- 通证发行

我们检查了通证发行是否有不合规的增发接口，以保护投资者的利益和系统的稳定运行。

经审查此功能暂未发现明显风险。

- 不安全的状态更改

我们检查了合约创建时初始化的一些关键状态变量。在很多情况下，这些变量只应该初始化一次，运行后再更改可能会给整个合约运行带来意料不到的风险。

经审查此功能暂未发现明显风险。

- 资金安全与后门

我们重点检查了入金和出金函数是否存在用户资金不受控制的风险、是否可能导致用户资金受损的问题。

经审查此功能暂未发现明显风险。

- 其它

经审查其它功能暂未发现明显风险。

07. 基于风险等级的问题列表

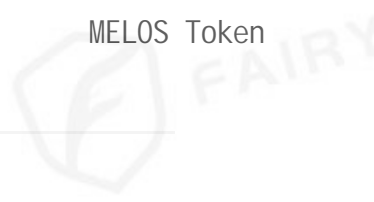
- 无

08. 问题详述

- 无

09. 增强建议

-无





-  <https://medium.com/@FairproofT>
-  <https://twitter.com/FairproofT>
-  <https://www.linkedin.com/company/fairproof-tech>
-  https://t.me/Fairproof_tech
-  [Reddit: https://www.reddit.com/user/FairproofTech](https://www.reddit.com/user/FairproofTech)

