06 安全与合规审计

主题：解读 CertiK 报告、识别合约风险、理解监管趋势

一、导引

1. 为什么“安全 + 合规”是项目能否长期存在的根基？
2. 一份第三方审计（如 CertiK）报告能说明什么？又有哪些局限？
3. 非技术人员（小白）如何快速理解一份审计报告？
4. 常见的合约风险有哪些？如何做到最基础的识别？
5. 全球监管趋势如何影响项目未来的合规性与投资价值？

二、核心知识点讲解

1. **为什么要看审计报告？**

- 智能合约一旦上线，不能随意修改，漏洞就是永久风险。
- 第三方审计（CertiK、OpenZeppelin 等）相当于“体检”，帮助发现潜在问题。
- **注意**：审计不是“保险”，只是告诉你“哪些地方检查过 + 有哪些问题 + 是否已修复”。

---

2. **小白如何看审计报告？（三步法）**

- **看范围**：是只检查了部分代码，还是覆盖了主要逻辑？（范围越大越可信）
- **看严重等级**：Critical/Major 问题要重点关注。
- **看修复状态**：Fixed / Acknowledged / Not Fixed → 只“确认”但没修复的仍然是风险。

---

3. **常见合约风险**

- **权限问题**：某个地址能不能随意增发或更改参数？
- **逻辑漏洞**：奖励分配、清算机制是否可能被利用？
- **外部依赖**：依赖预言机/跨链桥，是否存在单点故障？

👉 快速记忆：**权限 + 逻辑 + 外部依赖** = 三大翻车点。

---

4. **如何做“快速安全印象分”？**

- 是否经过 1–2 家权威审计？
- 审计报告是否公开？
- 是否在 Immunefi 等平台挂漏洞赏金？
- 是否有过安全事故（如 Rekt.news 是否提过）？

👉 如果以上 4 点都能满足，说明项目安全性较好；如果大部分缺失，风险就很高。

---

5. **理解监管趋势（全球要点）**

- **三条主线：**

1. 稳定币监管：最严格，要求储备与托管（EU、UK、SG）。
2. 牌照制度：交易所、托管必须拿牌（HK、Dubai、Brazil）。
3. 资本市场接纳：美国批准以太坊现货 ETF，说明加密逐步进入传统金融体系。

全球/地区政策快览（2024–2025）

地区/国家	核心法规	监管重点	进展
欧盟	MiCA	稳定币资本金要求、牌照管理	2024 生效，2025 过
美国	证券法框架 + ETF	交易所/托管纳入监管，以太 ETF 获批	2024–2025，ETF 制度逐
英国	FCA 稳定币与托管框架	稳定币发行、托管须授权	2025 咨询与落地细则
新加坡	MAS DPT/稳定币规则	消费者保护、冲突管理	2024–2025 分步落
日本	FSA	交易所质押需牌照，AML 加强	2025 明确质押业务监管
香港	SFC VATP	平台牌照、代币准入、质押规则	2024–2025 快速许可
迪拜	VARA	VA 活动分类与许可、营销规范	2024–2025 牌照体系成
巴西	Law 14.478	央行主导，VASP 纳管	2025 央行细则推进
印度	税优先	30% 税 + 1% TDS，抑制投机	2025 继续维持高压税
澳大利亚	Token Mapping	功能映射 → 分阶段纳管	2023 咨询，2025 政策

👉 takeaway：不同国家监管差异大，投资前要搞清楚项目主要市场在哪、合规风险有多大。

三、实操案例

案例1：ORIGIN 项目（2024 年审计）

> 基于 CertiK 近期对 “ORIGIN 项目（在 BSC 和以太坊）” 的安全评估报告，时间点为 2024 年 4 月 22 日

背景介绍

- 项目名称：ORIGIN（BSC / Ethereum 环境）
- 审计时间：2024 年 4 月 22 日
- 审计平台：OpenZeppelin 安全评估

解读方法（“小白三步法”）

1. **审计范围**

- 报告涵盖了合约的主要功能模块，对项目核心逻辑进行了安全审查。

2. **问题等级概览**

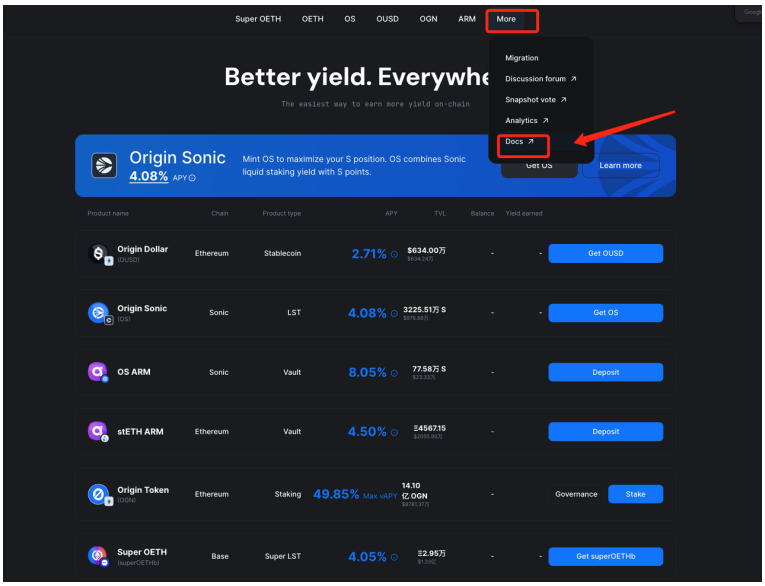
- CertiK 在本次审计中发现 **22 处安全问题**：包括 **4 个 Major（重大）问题** 和 **11 个 Medium（中等）问题** 。

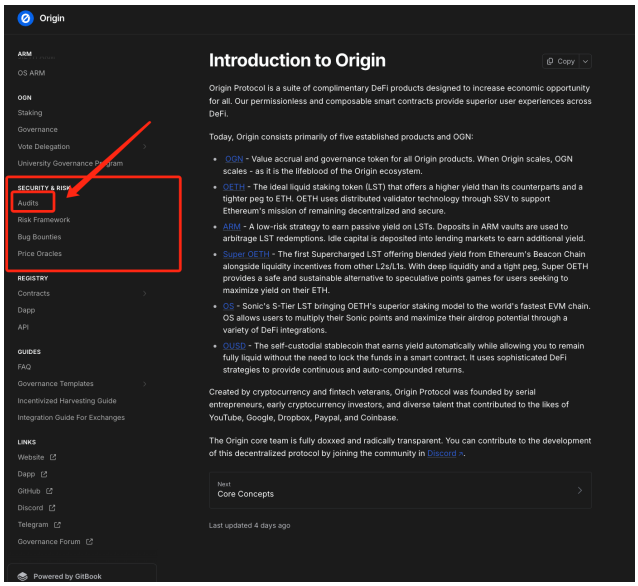
3. **修复状态**

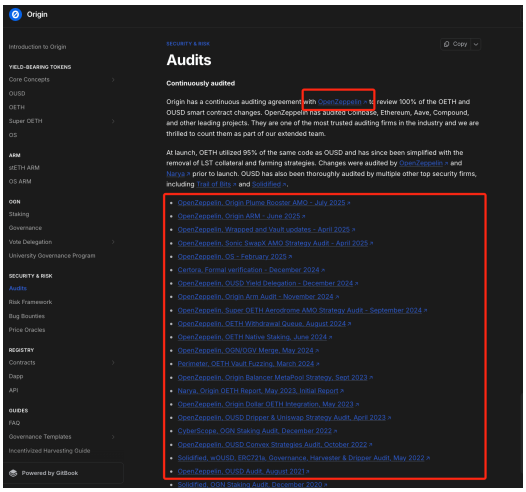
- 报告强调了问题类型（如集中化风险、逻辑错误），并指出在发布前应优先修复这些问题。

4. **关键 takeaway**

- 即便项目通过审计，也暴露出重大问题。投资人应关注是否查看修复状态、是否有代码更新日志、是否重新验证审计结果。
- **时间节点说明**
  - **T = 发布前审计**：2024 年 4 月 22 日，CertiK 完成第一轮评估 → 报告出具问题清单
  - **T + 后续**：项目方应在“后续更新 + 合约部署”阶段修复 Major 风险；投资者需确认是否有新版审计或已修复公告。
  - **T + X 月**：持续关注 Skynet 分数、事件历史，防范未发现的新漏洞。







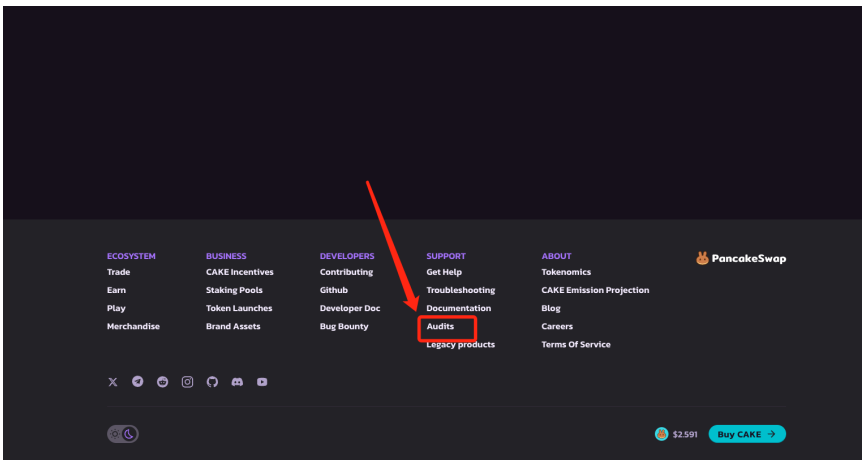
OpenZeppelin | security

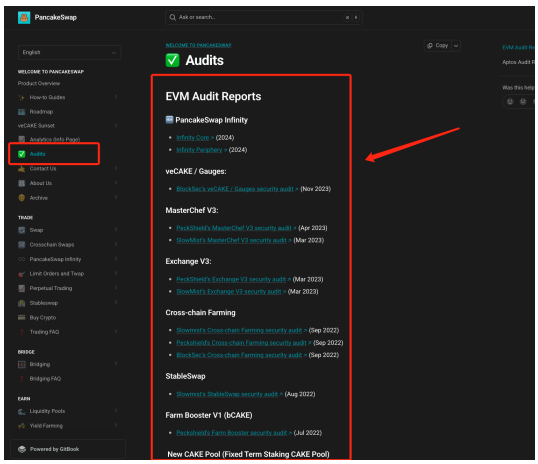
Origin Native Staking Audit

ORIGIN

Table of Contents

案例2：PancakeSwap 项目（2023 年 审计）





PeckShield

SMART CONTRACT AUDIT REPORT

for

PancakeSwap V3

Prepared By: X[redacted]

PeckShield
March 28, 2023

1.2 About PeckShield

PeckShield Inc. [10] is a leading blockchain security company with the goal of elevating the security, privacy, and usability of current blockchain ecosystems by offering top-notch, industry-leading services and products (including the service of smart contract auditing). We are reachable at Telegram (https://t.me/peckshield), Twitter (http://twitter.com/peckshield), or Email (contact@peckshield.com).

Table 1.2: Vulnerability Severity Classification

Impact \ Likelihood	*High*	*Medium*	*Low*
High	Critical	High	Medium
Medium	High	Medium	Low
Low	Medium	Low	Low

1.3 Methodology

To standardize the evaluation, we define the following terminology based on OWASP Risk Rating Methodology [9]:

- Likelihood represents how likely a particular vulnerability is to be uncovered and exploited in the wild;
- Impact measures the technical loss and business damage of a successful attack;
- Severity demonstrates the overall criticality of the risk.

Likelihood and impact are categorized into three ratings: *H*, *M* and *L*, i.e., *high*, *medium* and *low* respectively. Severity is determined by likelihood and impact and can be classified into four categories accordingly, i.e., *Critical*, *High*, *Medium*, *Low* shown in Table 1.2.

1. **报告范围**
- 覆盖了 PancakeSwap 的核心智能合约（Swap、流动性池）。
- 意味着主要功能逻辑都在检查范围内。
2. **问题等级**
- 报告列出了不同严重等级的问题。
- 高风险问题涉及权限与逻辑漏洞。
3. **修复状态**
- 大部分问题已修复，部分问题仅被确认但未完全修改。
- 说明风险不能忽视，投资者要留意是否存在潜在遗留。
4. **takeaway**
- 审计报告不是“盖章无风险”，而是“当时发现的问题清单”。
- 投资者看报告要聚焦三点：
  a. 审计范围；
  b. 问题等级；
  c. 修复状态。

👉 即便是小白，只要按这三点去读，就能形成对一个项目的基本安全判断。

四、总结

1. 导引问题总结

1. **为什么安全 + 合规是根基？**

- 因为代码漏洞不可逆，合规缺失可能被禁用，二者都决定项目能否活下去。

2. **审计能说明什么？局限是什么？**

- 审计能揭示“发现的问题+修复情况”，但不能保证未来没有新漏洞。

3. **小白如何读审计报告？**

- 看范围、看等级、看修复状态 → 三步足够。

4. **常见合约风险有哪些？**

- 权限、逻辑、外部依赖，是最容易出事的三大类。

5. **监管趋势如何影响投资？**

- 稳定币监管最严、牌照化是大方向，美国/欧盟等推动制度化，亚洲和新兴市场差异化明显。

---

2. 核心知识点总结

- **审计报告入门**：不是保证书，而是“体检报告”。
- **三步法读报告**：看范围、看问题等级、看修复状态。
- **常见风险**：权限管理、逻辑漏洞、外部依赖。
- **快速安全印象分**：审计机构、报告透明度、漏洞赏金、历史事故。
- **监管趋势三主线**：稳定币 → 牌照化 → 资本市场融通。