ScaleBit

OpenBuild

Tact安全实践

Jason

大纲

- 课程回顾
- 未来学习方向展望
- 合约安全
  - 安全事件案例展示
  - 合约开发建议
  - 合约运维建议

课程回顾

- 第一课 TON&Tact介绍
  - TON生态介绍
  - Tact语言介绍
  - Tact开发环境搭建
- 第二课 Tact语法概述
  - Tact语法精讲
- 第三课 FT标准介绍与实战
  - FT标准介绍
  - TON中FT标准Jetton介绍
  - FT实战案例
- 第四课 NFT标准介绍与实战
  - NFT标准介绍
  - TON中NFT标准介绍
  - NFT实战案例
- 第五课 Tact游戏实战
  - 合约测试框架介绍
  - Typescript SDK合约交互调用

未来学习方向展望

- 加深TON区块链基本知识学习
- 巩固Tact合约语言学习
- 熟练掌握一门TON SDK的使用，如Typescript SDK
- 实战演练，找一些自己感兴趣的项目，模仿练习
- 业务学习，接触多个赛道，如游戏、Defi等，积累业务经验
- 一些较好的资源网站
  - https://ton.org/
  - https://ton.app/
  - https://tact-lang.org/

合约安全事件

目前来讲，区块链上运行着各种协议应用，管理着大量的数字资产，这些数字资产也吸引了大量黑客的关注。

- OKLink：2023年发生区块链安全事件损失17亿美元，较2022年的37.28亿美元下降54%
- 损失金额较大的安全事件包括：
  - 3月以太坊借贷协议Euler Finance遭黑客攻击，损失约1.97亿美元；
  - 6月，Atomic钱包遭黑客攻击，损失逾1亿美元；
  - 9月Mixin Network遭攻击，损失2亿美元；
  - 11月Poloniex交易平台因私钥泄露被窃取约1.25亿美元。

合约开发建议

- 安全开发生命周期：将安全性纳入整个智能合约开发生命周期，这包括设计、编码、测试、部署和运维阶段。
- 使用已验证的库和框架：避免重复造轮子，使用已经经过安全审查和验证的库和框架。这可以减少潜在的错误和漏洞。
- 避免使用过时的合约模板：避免使用过时或不再维护的合约模板，因为它们可能存在已知的漏洞。
- 最小化权限原则：为了最小化攻击面，只赋予智能合约必要的权限。不要过度授予合约不需要的权限。
- 添加权限检查：在合约中添加适当的权限检查，以确保只有授权的用户可以执行敏感操作。

合约开发建议

- 参数验证和输入校验：对于所有输入，包括函数参数和消息 调用，进行详细的验证和校验，以防止潜在的攻 击。
- 防止整数溢出和下溢：使用安全的整数运算 库，避免整数溢出和下溢可能 导致的问题。
- 测试覆盖率：使用全面的测试套件覆盖所有合 约功能，并定期运行自 动化测试，确保合 约的可靠性。
- 灾难恢复机制：考虑在合约中实现紧急停机和紧急恢复机制，以防止潜在的安全问题。
- 合约升级和迁移策略：如果考虑合约升级，确保制定清晰的合 约迁移策略，同时小心确保用户资金和数据的安全性。

合约运维建议

- 充分测试:开发网测试，再测试网，必要时上主网测试，这有助于发现和解决在实际网络环境中可能出现的问题。
- 代码审查：主网上线前，进行详尽的代码审查，确保没有潜在的安全漏洞。这可以请专业的智能合约审计公司进行审查。
- 定期更新：定期更新合约，特别是在发现漏洞后，要及时更新修复升级。
- 监控和报警：设置实时监控系统，监测合约的运行情况。配置报警，以便在发生异常或潜在攻击时能够及时采取措施。
- 灾难恢复：制定紧急情况下的灾难恢复计划，包括合约的紧急停机和用户通知，和合约升级策略。

总结

- 区块链安全非常重要，合约代码开发完成，部署上线只是第一步
- 区块链运维安全，是一项长期的任务，马虎不得
- 在Web3行业，需要持续学习

Thanks

Contact us:

- Twitter: @scalebit_
- Email: contact@scalebit.xyz

ScaleBit

More information : www.scalebit.xyz