TON Smart Contracts Vulnerabilities

Smirnova Elizaveta

Цель

Разработать инструмент для поиска и устранения уязвимостей в TON smart contracts

TON

From Paradigm Shift to Audit Rift: Exploring Vulnerabilities and Audit Tips for TON Smart Contracts

TON

- Поиск и анализ существующих уязвимостей на основе доступных аудиторских отчётов, публичных репозиториев (GitHub)

- Классификация найденных уязвимостей

- Моделирование типичных сценариев возникновения выявленных уязвимостей разного рода

- Разработка стратегий по детектированию, устранению и предотвращению ошибок

TON

Изучение кейсов

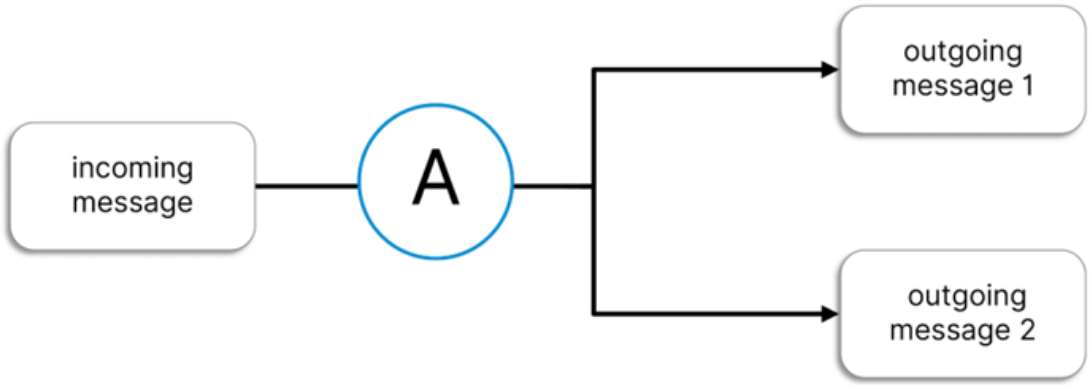
Разбор конкретных кейсов

TON

Asynchronous Execution

Асинхронная природа TON, несмотря на свою эффективность, создает проблемы, с которыми не сталкиваются разработчики смарт-контрактов на Etherium.

В TON гарантируется, что сообщение будет доставлено, но исполнение транзакций может быть произвольным, что приводит к потенциальным сбоям в работе и несогласованности состояний.



TON

Common Errors

- Логические ошибки
- Ошибки при работе с памятью
- Неправильная интерпретация работы с блокчейном

TON

Random Number Generation

В TON смарт-контракты разрабатываются на языке программирования FunC. В FunC есть псевдо-случайная функция random(). Использование этой функции влечёт потенциальные проблемы с безопасностью, поскольку псевдо-случайность не может гарантировать, что результат исполнения кода не будет предсказуемым.

TON

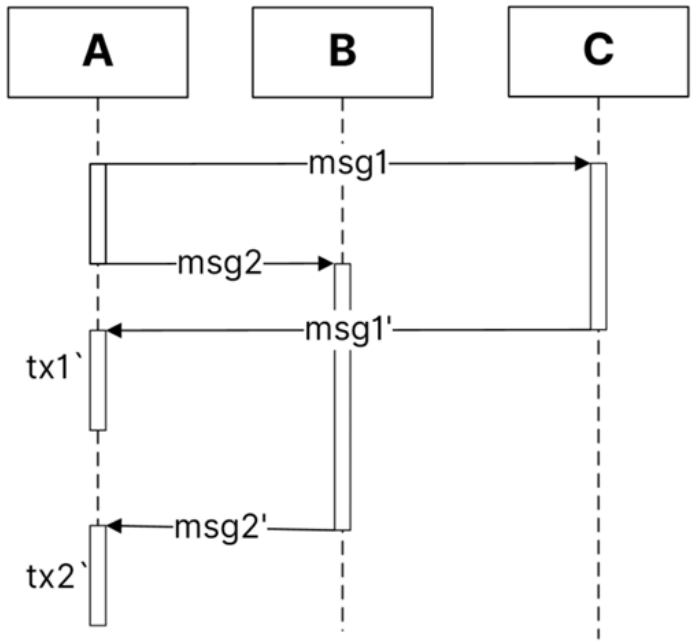
Possible Errors in FunC

В TON смарт-контракты разрабатываются на языке программирования FunC. В коде могут возникать проблемы, связанные с особенностями языка.

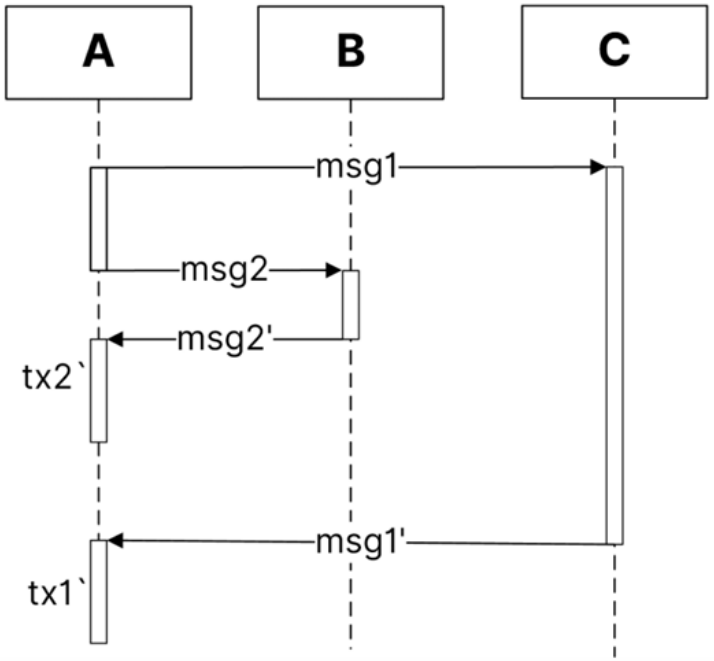
TON

BugMagnifier: TON Transaction Simulator to Reveal Smart Contract Vulnerabilities

TON: No Predefined Order



vs



TON

ZEUS Rules TON: Developing a Formal Verification Tool for TON Smart Contracts

- Формальная грамматика для TVM
- Разработка универсального инструмента формальной верификации
- Тестирование и анализ полученной модели

TON

Ссылки:

- https://docs.ton.org/v3/documentation/smart-contracts/func/docs/functions
- https://github.com/ton-org/sandbox
- https://test.ton.org/tblkch.pdf
- https://github.com/ton-org/blueprint?tab=readme-ov-file#contract-development
- https://tonbit.xyz/reports/TonUP-Smart-Contract-Final-Audit-Report.pdf
- https://certificate.quantstamp.com/full/ton-locker-contract/6872997f-1110-45cc-b70f-2a4cd639da1f/index.html

TON