Аудит смарт-контракта ITL

Общее описание

Смарт-контракт ITL (Investment Token of L&H) предназначен для выпуска и распродажи ITL токенов. В данном документе описаны выводы, полученные в ходе технического аудита контракта. Выявлены потенциальные проблемы и предложены методы их решения. Проблемы перечислены ниже в порядке убывания важности.

Анализ исходного кода

1. *Проверка прав доступа к ключевым функциям.*

Transfer – может быть вызвана только пользователем, работает корректно.

Mint - может быть вызвана только владельцем контракта – работает корректно.

TransferOwnership - может быть вызвана только владельцем контракта, работает корректно.

Burn- может быть вызвана только пользователем, работает корректно.

ChangePriceUSD - может быть вызвана только оракулом, работает корректно.

Function finishPreSale- может быть вызвана только владельцем контракта и при соблюдении всех условий, работает корректно.

StartPreSale - может быть вызвана только владельцем контракта, работает корректно.

2. *Проверка случаев использования небезопасной математики* - не обнаружено.

Общие рекомендации.

1. Привязка должна быть к ETH, а не к доллару.

2. Ручной неограниченный и ничем необоснованный довыпуск токенов неприемлем для инвесторов, данный пункт настоятельно рекомендуется исправить.

3. Не указанна доля токенов на баунти, эдвайзерам и т.д. Если будут исправления, доля должна быть указанна только в процентах от общей массы купленных токенов.

4. Рекомендуется указать минимальный лимит для инвестиции хотя бы 0.001 ETH. -защита от DoS-атак + полезно для маркетинга.

5. Также рекомендуется избегать хардкодинга (пример - hardCapPrivate = 40000000;)
   Стоит заменить сеттерами для большей гибкости контракта:

6. Рекомендуется использовать multisig кошелек для сбора средств.

Выводы

В целом контракт написан качественно и без критичных багов, все основные функции **работают корректно**. Контакт **пригоден** для деплоя в основную сеть. Уровень абстракции классов контракта не вызывает нареканий. Радует использование лучших практик разработки смарт-контрактов:

- применение стандартных контрактов;
- использование SafeMath;
- использование методов защиты от известных уязвимостей.