2MOON.ME

AUDIT

Аудит смарт контракта **ETH7.io**

Статус - завершен, последняя редакция 2018-10-28

Обзор

На момент аудита контракт уже размещен в основной сети Ethereum. Адрес – 0xc18d73fafc36cec96c9c8a05309662605840826d

Код контракта проверен на предмет программных закладок и критических ошибок способных привести к потере денег инвесторами.

- В контракте отсутствует владелец и функционал доступный только владельцу. Полный отказ от владения.
- Для пользователей доступна только fallback функция и view функции.
- Для успешного депозита пользователь должен отправить eth на адрес контракта.
- Для получения выплат пользователь должен отправить 0 eth на адрес контракта.
- В контракте реализована реферальная система. Referrer адрес передается в data при вызове fallback функции. Процент реферера сразу же отправляется на его адрес.

Контракт **ETH7** наследует функционал контракта **ReentrancyGuard** - реализующего механизм защиты от *reentrancy attacks*.

Весь функционал реализован через **fallback** функцию контракта которая вызывает функцию **makeDeposit**() с модификатором **nonReentrant** из **ReentrancyGuard** для предотвращения reentrancy attacks. Логика **makeDeposit** построена таким образом что в зависимости от msg.value выбирается логика работы (новый депозит или выплата дивидендов\кешбека).

Функции контракта используют методы библиотеки ` **SafeMath** ` для безопасных вычислений.

Private и **internal** функции:

Функция **collectCashback** – выплачивает кешбек. Вызывается в **makeDeposit.**

Функция **chargeCashBack** – в зависимости от даты и размера депозита подсчитывает размер кешбека. Вызывается в **makeDeposit.**

Функция **collectPercent** – выплачивает проценты по депозиту. Вызывается в **makeDeposit.**

View функции:

Функция **userPayoutAmount** – возвращает размер выплаты.

Функция **getInvestedAmount** – возвращает размер депозита.

Функция **getLastDepositeTime** – возвращает время последнего депозита\выплаты.

Функция **getPercentWitdraw** – возвращает процент выплат.

Функция **getRefferalsCollected** – возвращает количество реферальных выплат.

Заключение

В коде контракта нет программных закладок и критических ошибок способных привести к потере денег инвесторами.

Предупреждение об ответственности

Этот аудит касается только исходных кодов смарт контракта и не должен рассматриваться как одобрение платформы, команды или компании.

Авторы

Аудит провёл **Антон Кольцов** telegram @AntonRnD, команда **2moon.me** (https://2moon.me)