ООО «Криптон Студио»

ОГРН 1187031051536

Адрес: 634059, г. Томск, ул. Мельничная, д.45.

ИНН/КПП 7017439134/701701001
тел.: +7 (903) 955-87-82
e-mail: info@crypton.studio

19 января 2021 г.

АУДИТ СМАРТ- КОНТРАКТОВ

Анализировались смарт-контракты, расположенные по адресу:

https://bitbucket.org/wordlex-online/wordlex-tron-smart-contracts/commits/af4b7fa3c87bb162c519e14fdf8ac8cff45c3210

Техзадание на смарт-контракты в Приложении №1.

КОНФИДЕНЦИАЛЬНО

Краткая информация

Проект: wordlex.online
Блокчейн: TRON
Язык: Solidity
Версия компилятора: 0.5.14
Дата аудита: 19.01.2021

Информация

Код контракта был проверен и проанализирован на предмет уязвимостей, логических ошибок и соответствия спецификациям. Данная работа проводилась в отношении исходного кода проекта, предоставленного заказчиком. Полный список обнаруженных проблем можно найти ниже.

Общий вывод

В результате аудита были обнаружены множественные логические ошибки, были выявлены несоответствия спецификации (TRC-20) и техническому заданию.
Команда Crypton Studio рекомендует доработку смарт-контрактов.

Отказ от ответственности

Команда Crypton Studio в рамках этой системы аудита не несет ответственности за действия разработчиков или третьих лиц на платформах, связанных с этим проектом (web-сайты, мобильные приложения и т.д.). Аудит подтверждает и гарантирует правильное функционирование смарт-контракта только в ревизии, предоставленной разработчиками проекта (проверьте ревизию).

A. Ошибки

№	Описание / рекомендации	Важность
1	Неполная реализация спецификации TRC-20. Контракты: WordlexToken Описание: Спецификация стандарта TRC-20 предполагает наличие определенного набора функций и событий в контракте: https://developers.tron.network/docs/implementation-rules В данной реализации в контракте токена присутствуют не все элементы спецификации - отсутствует событие: event Approval(address indexed _owner, address indexed _spender, uint _value); Риск: Отсутствие события может привести к неполной совместимости на сторонних сервисах, использующих, использующих стандарт TRC-20. Рекомендации: Добавить недостающие событие в смарт-контракт.	Средняя
2	Небезопасные математические операции. Контракты: WordlexStaking AutoProgramWordlex WordlexToken Описание: Хорошей практикой является использование безопасных математических операций с использованием библиотеки SafeMath. Риск: Потенциальные возможности переполнения переменных. Рекомендации: Использовать библиотеку безопасной математики SafeMath везде где существует потенциальная возможность переполнения.	Высокая
3	Дублирование методов в интерфейсе.	Низкая

	Интерфейс: IWordlexStatus Описание: Дублируется метод: function getStatusPrice(uint256 _statusId) external view returns(uint256); Риск: Невозможности компиляции контрактов. Рекомендации: Удалить дублирующийся метод в интерфейсе.	
4	Отсутствие необходимого метода в контракте. Контракт: AutoProgramWordlex Описание: Отсутствует метод для установки значения переменной carPriceInWDX. Риск: Невозможность задать цену автомобиля, некорректная работа контракта. Рекомендации: Добавить метод для установки значения переменной.	Высокая
5	Несоответствие логике работы. Контракт: AutoProgramWordlex Описание: В контракте присутствует только одна переменная, в то время как для разных пользователей необходимо устанавливать разную цену автомобиля. Риск: Неверные расчеты могут привести к потери средств, конфликтам с клиентами. Рекомендации: Доработать логику смарт-контракта.	Высокая
6	Несоответствие логике работы. Контракт:	Высокая

	AutoProgramWordlex Описание: Логика описанная в функции withdraw() значительно не соответствует техническому заданию. Риск: Неверные расчеты могут привести к потери средств, конфликтам с клиентами. Рекомендации: Переписать логику смарт-контракта в соответствие с техническим заданием.	
7	Несоответствие логике работы. Контракт: AutoProgramWordlex Описание: В контракте не реализована логика определения “активного аккаунта”. Условия чтобы считать аккаунт - активным: 1. когда с аккаунт была успешно выполненна функция buyCar(...); 2. когда у аккаунта в 1 линии аккаунты рефералов успешно выполнили функция buyCar(...) больше 1 раза (2 и более). Риск: Неверные расчеты могут привести к потери средств, конфликтам с клиентами. Рекомендации: Переписать логику смарт-контракта в соответствие с техническим заданием.	Высокая
8	Наличие в контракте неиспользуемых переменных. Контракт: WordlexStatus Описание: В контракте присутствует массив uint8 переменных ref_bonuses. Массив инициализируется в конструкторе контракта и далее нигде не используется. Риск:	Низкая

	Замусоривание контракта, трата дополнительных ресурсов на деплой контракта. Рекомендации: Удалить неиспользуемые переменные.	
9	Отсутствие необходимого метода в контракте. Контракт: WordlexStatus Описание: Отсутствует метод для установки значения переменной admin. Риск: Невозможность изменить адрес получателя в случае компрометации. Рекомендации: Добавить метод для установки значения переменной.	Низкая
10	Несоответствие логике работы. Контракт: WordlexStatus Описание: 1. Бонус 5% начисляется при каждой покупке статуса рефералов 1-го уровня. По техническому задания бонус должен копиться и начислять только при покупке каждым 10-м рефералом. 2. Также бонус 5% должен начисляется при каждой покупке статуса рефералов N-го уровня - всем его реферерам с достаточным статусом. Риск: Неверные расчеты могут привести к потери средств, конфликтам с клиентами. Рекомендации: Переписать логику смарт-контракта в соответствие с техническим заданием.	Высокая
11	Несоответствие логике работы. Контракт: WordlexStaking Описание:	Высокая

	Логика смарт-контракта значительно не соответствует техническому заданию. В точности: 1. Отсутствие “сложного” процента при начислении процента за стейкинг; 2. Некорректное поведение контракт при повторном депозите - перезаписывается значения переменных deposit_time, deposit_amount; 3. Реферальные вознаграждения от стейкинга учитываются при вычисление лимита на вывод (по техническому заданию лимитов на выводы нет). Риск: Неверные расчеты могут привести к потери средств, конфликтам с клиентами. Рекомендации: Переписать логику смарт-контракта в соответствие с техническим заданием.	

B. Замечания

№	Описание
1	Отсутствие единых подходов при написании смарт-контрактов. Описание: В одних контрактах используется библиотека безопасной математики, в других - нет, пишутся проверки внутри функций, что усложняет чтение логики контракта. Комментарии в контрактам и функциям пишутся не везде и на разных языках, при этом оформляются по разному. Не везде в функции require передается текст ошибки.
2	Дублирование кода. Описание: Не используются возможности импорта кода из разных файлов, в результате чего - один и тот же код встречается в разных файлах, в точности: interface IWordlexStatus interface IERC20 contract Ownable
3	Наличие неиспользуемых интерфесов. Описание: В папке Interfaces присутствуют два интерфейса: interface IPriceController interface IWordlexStatus Которые нигде не используются.

Директор _____ / Санданов А.Ц. /