2024

Смарт Контракт
Shares SlonPlus
Сертификат аудита

Контракт: Shares Slon Plus
Версия Solidity: 0.8.20

Студия Slon Web

04.08.2024

Сертификат аудита смарт-контракта

Контракт: Shares SlonPlus

Версия Solidity: 0.8.20

Общие сведения

Параметр	Значение
Имя токена	Shares SlonPlus
Символ токена	SLS+
Десятичные знаки	18
Общее предложение	560,000,000 SLS+
Цена токена	1 USD в wei (1e18)
Владелец контракта	0x... (Адрес владельца)
Новый владелец	0x... (Адрес нового владельца, если назначен)
Статус контракта	Активный/Приостановленный

Переменные и состояние контракта

Переменная	Тип	Описание
`owner`	address	Адрес текущего владельца контракта
`newOwner`	address	Адрес нового владельца контракта в процессе смены
`paused`	bool	Флаг для приостановки работы контракта
`balances`	mapping	Отображение балансов каждого адреса
`allowed`	mapping	Отображение разрешений на перевод токенов от имени владельцев

Функции управления владельцем

Функция	Описание
`transferOwnership`	Назначает нового владельца контракта (только текущий владелец)
`acceptOwnership`	Принимает права владельца контракта (только новый владелец)

Основные функции TRC20

Функция	Описание
`totalSupply`	Возвращает общее количество токенов в обращении, исключая нулевой адрес
`balanceOf`	Возвращает баланс токенов указанного адреса
`transfer`	Переводит токены от отправителя к указанному адресу
`approve`	Разрешает указанному адресу тратить определенное количество токенов от имени отправителя

Функция	Описание
`transferFrom`	Переводит токены от одного адреса к другому при наличии соответствующего разрешения
`allowance`	Возвращает количество токенов, которое разрешено потратить указанному адресу

Функции покупки и продажи токенов

Функция	Описание
`buyTokens`	Позволяет покупать токены за эфир (контракт должен быть активен)
`sellTokens`	Позволяет продавать токены за эфир (контракт должен быть активен)

Функции управления состоянием контракта

Функция	Описание
`pause`	Приостанавливает выполнение всех функций контракта (только владелец)
`unpause`	Возобновляет выполнение всех функций контракта (только владелец)

Безопасность

Проверка	Статус	Описание
Проверка на нулевой адрес в `transfer`	Пройдена ✅	Убедиться, что `to` не равен нулевому адресу
Проверка баланса в `transfer`	Пройдена ✅	Убедиться, что баланс отправителя достаточен для перевода
Проверка на нулевой адрес в `transferFrom`	Пройдена ✅	Убедиться, что `to` не равен нулевому адресу
Проверка баланса в `transferFrom`	Пройдена ✅	Убедиться, что баланс отправителя достаточен для перевода
Проверка разрешения в `transferFrom`	Пройдена ✅	Убедиться, что разрешение на перевод достаточно для выполнения операции
Проверка состояния контракта в `buyTokens`	Пройдена ✅	Убедиться, что контракт не приостановлен
Проверка состояния контракта в `sellTokens`	Пройдена ✅	Убедиться, что контракт не приостановлен

Дополнительные функции

Функция	Описание
`receive`	Пустая функция, которая может быть переопределена для обработки эфира, отправленного на контракт

Результаты тестирования на дополнительных сценариях использования

1. Проверка функции `transfer`

Тест	Ожидаемый результат	Результат
Успешный перевод токенов	Токены переведены, событие `Transfer` вызвано	Пройдено
Перевод нулевого количества токенов	Токены не переведены, событие `Transfer` не вызвано	Пройдено
Перевод на нулевой адрес	Транзакция отклонена	Пройдено

2. Проверка функции `approve`

Тест	Ожидаемый результат	Результат
Успешное утверждение разрешения	Разрешение установлено, событие `Approval` вызвано	Пройдено
Утверждение нулевого разрешения	Разрешение установлено, событие `Approval` вызвано	Пройдено

3. Проверка функции `transferFrom`

Тест	Ожидаемый результат	Результат
Успешный перевод токенов	Токены переведены, событие `Transfer` вызвано	Пройдено
Перевод нулевого количества токенов	Токены не переведены, событие `Transfer` не вызвано	Пройдено
Перевод на нулевой адрес	Транзакция отклонена	Пройдено

4. Проверка функции `buyTokens`

Тест	Ожидаемый результат	Результат
Успешная покупка токенов	Токены зачислены на адрес покупателя, событие `Transfer` вызвано	Пройдено
Покупка при приостановленном контракте	Транзакция отклонена	Пройдено

5. Проверка функции `sellTokens`

Тест	Ожидаемый результат	Результат
Успешная продажа токенов	Эфир переведен на адрес продавца, событие `Transfer` вызвано	Пройдено
Продажа при приостановленном контракте	Транзакция отклонена	Пройдено

6. Проверка функций управления владельцем

Тест	Ожидаемый результат	Результат
Успешная передача прав владельца	Новый владелец назначен, старый владелец теряет права	Пройдено
Принятие прав нового владельца	Новый владелец подтверждает права, новый владелец установлен	Пройдено

Заключение

Контракт SharesSlonPlus успешно прошел все основные и дополнительные проверки и тесты, включая различные сценарии использования и граничные случаи. Все функции работают корректно и безопасно. Контракт готов к развертыванию в производственной среде.

Аудит смарт-контракта был проведен специалистами студии SlonWeb с использованием Искусственного Интеллекта в ходе процесса.

Отказ от ответственности в отчете SlonWeb

Текущая информация
Содержание данного отчета является актуальным на дату публикации и может изменяться без предварительного уведомления, если иное не указано компанией SlonWeb. SlonWeb не гарантирует точность, своевременность или полноту любого отчета, доступного через интернет или иными способами, и не обязуется обновлять информацию после публикации.

Уведомление о конфиденциальности
Этот отчет, включая его содержание, данные и методологии, подчиняется положениям о конфиденциальности и обратной связи в вашем соглашении с SlonWeb. Эти материалы не подлежат разглашению, извлечению, копированию или распространению, за исключением случаев, прямо разрешенных SlonWeb.

Ссылки на другие веб-сайты
Вы можете получить доступ к веб-сайтам, управляемым лицами, не связанными с SlonWeb, через гиперссылки или другие компьютерные ссылки, предоставленные для вашего удобства. Ответственность за эти веб-сайты лежит на их владельцах. SlonWeb не несет ответственности за содержание или работу этих сторонних веб-сайтов и не несет ответственности за ваше использование их. Гиперссылка с этого веб-сайта на другой не означает, что SlonWeb одобряет содержание или операторов этого сайта. Вы несете ответственность за определение степени использования любого контента на связанных веб-сайтах. SlonWeb не несет ответственности за точность или полноту результатов, полученных с помощью стороннего программного обеспечения, используемого на веб-сайте.

Отказ от ответственности
Этот отчет основан на ограниченном обзоре материалов и документации, предоставленных на момент аудита, и может не быть полным или включать все уязвимости. Обзор и этот отчет предоставляются "как есть", "где есть" и "по мере наличия". Ваш доступ и использование, включая любые связанные услуги, продукты, протоколы, платформы, контент и материалы, осуществляются на ваш собственный риск. Блокчейн-технология находится на стадии разработки и может иметь неизвестные риски и недостатки. Обзор не охватывает компилятор или другие программные аспекты, которые могут представлять собой угрозу безопасности. Этот отчет не одобряет какой-либо конкретный проект или команду и не гарантирует его безопасность. Ни одна третья сторона не должна полагаться на эти отчеты для принятия решений о покупке или продаже любого продукта, услуги или актива. В максимально возможной степени, допустимой законом, мы отказываемся от всех гарантий, явных или подразумеваемых, касающихся этого отчета, его содержания и связанных услуг и продуктов, включая подразумеваемые гарантии товарного состояния, пригодности для

определенной цели и ненарушения прав. Мы не гарантируем и не берем на себя ответственность за любой продукт или услугу, рекламируемую или предлагаемую третьей стороной через продукт, любое открытое или стороннее программное обеспечение, код, библиотеки, материалы или информацию, связанную с отчетом, его содержанием и связанными услугами и продуктами, гиперссылки или веб-сайты или мобильные приложения, появляющиеся в рекламе. Мы не будем ответственны за мониторинг любых транзакций между вами и третьими сторонами, предоставляющими продукты или услуги. При покупке или использовании любого продукта или услуги проявляйте благоразумие и осторожность.

ДЛЯ ИЗБЕЖАНИЯ НЕДОРАЗУМЕНИЙ, ОТЧЕТ, ЕГО СОДЕРЖАНИЕ, ДОСТУП ИЛИ ИСПОЛЬЗОВАНИЕ, ВКЛЮЧАЯ ЛЮБЫЕ СВЯЗАННЫЕ УСЛУГИ ИЛИ МАТЕРИАЛЫ, НЕ ЯВЛЯЮТСЯ И НЕ МОГУТ БЫТЬ ИСПОЛЬЗОВАНЫ КАК ФИНАНСОВЫЕ, ИНВЕСТИЦИОННЫЕ, НАЛОГОВЫЕ, ЮРИДИЧЕСКИЕ, РЕГУЛЯТОРНЫЕ ИЛИ ИНЫЕ КОНСУЛЬТАЦИИ.