

# Фраза Шамира

## Введение

Фраза Шамира — это безопасный метод создания и восстановления криптовалютных кошельков с использованием алгоритма разделения секрета Шамира. В этом руководстве мы рассмотрим, что такое Фраза Шамира, ее классификацию, цели, а также как генерировать и импортировать части фразы с использованием кошелька Keystone.

## Раздел 1: Что такое Фраза Шамира?

Фраза Шамира, основанная на алгоритме разделения секрета Шамира, позволяет создавать кошельки с несколькими подписями, используя разделение сид фразы. Это обеспечивает дополнительную безопасность и резервирование, так как для доступа к кошельку требуется несколько частей. Классификация Фразы Шамира зависит от количества частей ( $n$ ) и порога ( $m$ ), необходимого для доступа к кошельку. Например, кошелек с Фразой Шамира 2 из 3 означает, что существует три части, и для доступа к кошельку достаточно двух из них.

## Раздел 2: Как сгенерировать Фразу Шамира с помощью Keystone

### Шаг 1: Доступ к настройкам кошелька

1. Откройте кошелек Keystone и перейдите в главное меню, нажав на иконку с тремя точками (...).
2. Выберите "Настройки устройства", затем выберите "Настройки кошелька" и наконец, нажмите "Добавить кошелек".

### Шаг 2: Создание нового кошелька

1. Разблокируйте кошелек, введя свой пароль и просмотрев предоставленные уведомления. Нажмите "Понял", чтобы продолжить.
2. Выберите "Создать кошелек", чтобы начать процесс создания. Установите новый пароль для кошелька и подтвердите его. Убедитесь, что этот пароль уникален и не совпадает с паролем вашего оригинального кошелька, так как устройство связывает кошельки с их паролями при разблокировке.

3. При желании укажите имя для кошелька (этот шаг можно пропустить), затем выберите "Фраза Шамира". Укажите нужное количество частей и порог для доступа к кошельку. Например, если вы хотите разделить кошелек на 3 части и для доступа требуется любые 2 из них, выберите 3 части и порог 2.

## Шаг 3: Генерация фразы Шамира

1. Следуйте инструкциям на экране для безопасного создания кошелька с несколькими подписями. Убедитесь, что вы делаете это в безопасной среде.
2. Перейдите к следующему шагу, где будет отображена первая часть фразы. Сохраните её в буфер обмена или запишите на надежный физический носитель, такой как мнемоническая карта.
3. Продолжайте процесс, подтверждая порядок слов. Если вы ошиблись в последовательности, можно нажать кнопку "сброс" в верхнем левом углу, чтобы начать заново.
4. Повторите процесс для второй и третьей части, если это применимо. После того как вы подтвердите последовательность для всех частей, ваш кошелек с резервной копией Шамира 2 из 3 будет успешно создан.

## Раздел 3: Как импортировать Фразу Шамира в Keystone

### Шаг 1: Доступ к настройкам кошелька

1. Откройте кошелек Keystone и перейдите в главное меню, нажав на значок с тремя точками (...).
2. Выберите "Настройки устройства", затем "Настройки кошелька" и наконец, нажмите "Добавить кошелек".

### Шаг 2: Импорт кошелька

1. Разблокируйте кошелек, введя свой код-пароль и ознакомьтесь со всеми уведомлениями. Нажмите "Понял", чтобы продолжить.
2. Выберите "Импортировать кошелек" и выберите количество слов, соответствующее вашей фразе (например, 20 или 33).

### Шаг 3: Ввод частей фразы Шамира

1. Введите части фразы в правильном порядке, начиная с первой и второй части. После правильного ввода, вы получите доступ к своему кошельку.

Следуя этим шагам, вы можете создать и импортировать кошельки с использованием Фразы Шамира через кошелек Keystone, что повысит безопасность и возможность восстановления ваших криптовалютных активов.

---

Версия #1

Admin создал 24 ноября 2024 15:06:55

Admin обновил 24 ноября 2024 15:41:29