Market Talks
ОБРАЗОВАТЕЛЬНЫЙ ЦЕНТР

БЛОКЧЕЙН · НАЧАЛЬНЫЙ · УРОК 9 ИЗ 13

Сид-фразы и резервные копии

12 или 24 слова, способные восстановить весь кошелёк, как их хранить и кто будет пытаться их заполучить

6 мин чтения Вопросов в тесте: 6, с ответами

БЛОКЧЕЙН · НАЧАЛЬНЫЙ · УРОК 9 ИЗ 13

Сид-фразы и резервные копии

СУТЬ В ОДНОМ ПРЕДЛОЖЕНИИ

Сид-фраза представляет собой список из 12 или 24 обычных слов, по которому можно воссоздать каждый закрытый ключ кошелька. Сохраните её, и вы восстановитесь после потери или поломки устройства. Допустите утечку, и любой сможет забрать всё без возможности что-то отменить.

Одна резервная копия для всех ключей

В уроке 8 мы видели, что кошелёк создаёт новый адрес для каждого платежа, а у каждого адреса свой закрытый ключ. Делать резервные копии десятков отдельных ключей было бы кошмаром. Современные кошельки решают это так: все ключи создаются из одного исходного числа, которое называется **сидом** (seed, «семя»).

Сид показывается вам один раз, при первой настройке кошелька, в виде списка из 12 или 24 слов. Это ваша **сид-фраза**, её также называют фразой восстановления. Введите те же слова почти в любое современное приложение-кошелёк, и оно воссоздаст точно те же ключи в том же порядке и найдёт те же монеты. Телефон или аппаратное устройство можно потерять, у вас его могут украсть, оно может сломаться. Пока у вас есть слова, ваши биткоины никуда не делись.

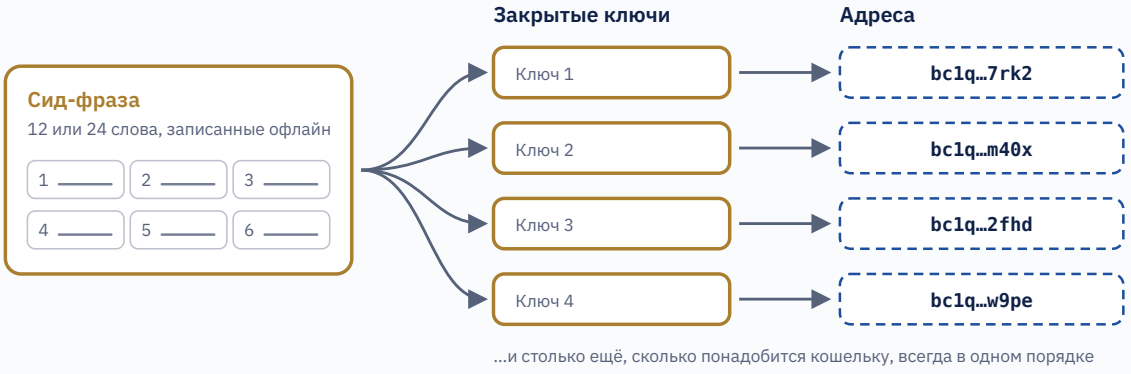


Рисунок 1. Одна сид-фраза создаёт все закрытые ключи кошелька, а каждый ключ даёт адрес. Восстановите фразу в любом совместимом кошельке, и вернутся те же ключи и монеты.

АНАЛОГИЯ: ФОТОНЕГАТИВ

Во времена плёночных фотоаппаратов негатив был ценнее любого снимка. Потеряли снимок, и можно напечатать новый с негатива сколько угодно раз в любой фотолаборатории. Сид-фраза служит негативом вашего кошелька. Приложение в телефоне представляет собой всего лишь один отпечаток. Но любой другой человек с этим негативом тоже может напечатать свои снимки.

Почему слова и почему именно эти

На самом деле сид представляет собой просто очень большое случайное число. Записывать его в виде 64 цифр и букв значит напрашиваться на ошибки, поэтому широко используемый стандарт превращает его в слова из фиксированного списка в 2048 простых английских слов. Каждое слово обозначает часть числа.

Список составлен тщательно. В английской версии нет двух слов с одинаковыми первыми четырьмя буквами, так что даже размазанное окончание остаётся читаемым. Последнее слово к тому же работает как встроенная проверка: если переписать одно слово с ошибкой, кошелёк обычно предупредит, что фраза недействительна, вместо того чтобы молча открыть пустой кошелёк.

Слова выбирает кошелёк случайным образом, а не вы. В этом вся суть. Фраза из 12 слов может оказаться любой из примерно 340 миллиардов миллиардов миллиардов миллиардов комбинаций, это число из 39 цифр. Придуманную вами фразу или строчки из песни быстро подберут программы, перебирающие миллионы распространённых выражений.

Некоторые кошельки также позволяют добавить необязательный дополнительный пароль, который часто называют passphrase. С ним одних 12 или 24 слов уже недостаточно, чтобы открыть кошелёк. Это дополнительная защита, но если вы забудете этот пароль, слова вам тоже не помогут.

Хранение: офлайн, надёжно, с возможностью найти

Хорошая резервная копия должна пережить три угрозы: воров, несчастные случаи вроде пожара или воды и вашу собственную память через много лет. Вот как сравниваются распространённые варианты:

Где	Защищает от	Уязвимо для
На бумаге, дома	Хакеров, потому что не касается интернета	Огня, воды и любого, кто её найдёт
Выбито на металлической пластине	Хакеров, огня и воды	Любого, кто её найдёт, если она плохо спрятана
Вторая копия в другом месте, например в банковской ячейке	Потери единственной копии при одном бедствии	Больше копий значит больше мест для утечки
Фото, скриншот, заметки, почта или облако	Ничего, с чем бумага не справилась бы лучше	Взлома аккаунтов, синхронизированных копий и вредоносных программ, сканирующих изображения

Что бы вы ни выбрали, записывайте слова по порядку, нумеруйте их и сверяйте каждое с экраном. Затем проведите учебное восстановление: держа в кошельке лишь небольшую сумму, сотрите его или возьмите второе устройство, введите слова заново и убедитесь, что появились те же адреса. Найти ошибку сейчас дёшево. Найти её в экстренной ситуации очень дорого.

Ни один добросовестный человек её не попросит

Поскольку сид-фраза открывает всё, она является главной целью криптомошенников. Уловки бывают разные, но просьба всегда одна: ввести ваши слова куда-нибудь. Это может быть «агент поддержки» в ваших сообщениях, всплывающее окно о том, что кошелёк нужно «синхронизировать» или «подтвердить», поддельное приложение-кошелёк в магазине приложений или сайт, обещающий бесплатный эйрдроп.

Правило простое и не знает исключений. Сид-фраза вводится только в ваш собственный кошелёк, когда вы сами его восстанавливаете. Ни компании-разработчику кошелька, ни бирже, ни разработчику, ни администратору канала она не нужна никогда.

РЕАЛЬНЫЙ ПРИМЕР: ПОДДЕЛЬНЫЕ «ЗАМЕНЫ» КОШЕЛЬКОВ

В 2020 году была взломана база данных производителя аппаратных кошельков Ledger, и в декабре имена, домашние адреса и телефоны примерно 272 000 клиентов оказались в открытом доступе. Через несколько месяцев некоторые клиенты получили посылку в упаковке, похожей на настоящую упаковку Ledger, с письмом о том, что их устройство небезопасно, а внутри лежит «замена». Инструкция просила ввести фразу восстановления. Устройство было модифицировано, и слова уходили прямо к ворам.

Почему это важно трейдерам

- **Торговые чаты служат охотничьими угодьями.** Мошенники вступают в оживлённые криптогруппы, копируют имена и фотографии администраторов и пишут людям в личные сообщения, предлагая помощь или «проверку кошелька». MARKET TALKS никогда не попросит у вас сид-фразу, закрытые ключи или пароли, как и любая настоящая команда.
- **У биржевого аккаунта есть свои секреты, похожие на сид-фразу.** Биржевые аккаунты не используют сид-фразы, но резервные коды двухфакторной аутентификации играют похожую роль. Если кто-то получит их вместе с паролем, он сможет захватить аккаунт. Храните их офлайн, как сид-фразу.
- **Подумайте о тех, кто останется после вас.** По оценкам исследователей, миллионы биткоинов уже потеряны навсегда, во многом потому, что единственный человек, знавший ключи, умер или забыл их. Если у вас значительные суммы, продумайте, как доверенный человек сможет однажды их восстановить, не давая никому доступа сегодня.

Ключевые термины

Сид	Единое большое случайное число, из которого кошелёк создаёт все свои закрытые ключи.
Сид-фраза	Сид, записанный в виде 12 или 24 слов. По нему можно воссоздать каждый ключ кошелька. Также называется фразой восстановления.
Список слов	Фиксированный список из 2048 слов, из которого берутся сид-фразы, чтобы их мог прочитать любой совместимый кошелёк.
Контрольная сумма	Встроенная проверка в последнем слове, которая помогает кошельку заметить, что фразу переписали с ошибкой.
Passphrase	Необязательный дополнительный пароль к сид-фразе. Без него одних слов недостаточно, чтобы открыть кошелёк.
Учебное восстановление	Пробное восстановление по записанной сид-фразе до того, как вы храните в кошельке серьёзные деньги.

Главное

1. Современные кошельки создают все ключи из одного сида, который показывается вам как сид-фраза из 12 или 24 слов.
2. С сид-фразой можно восстановить кошелёк на новом устройстве, даже если старое потеряно или сломано.
3. Слова берутся из фиксированного списка в 2048 слов, выбираются кошельком случайно, а последнее служит проверкой на ошибки.
4. Храните фразу офлайн и надёжно, никогда в фото, заметках, почте или облаке, и проверьте восстановление на небольшой сумме.
5. Любой, кто просит вашу сид-фразу, пытается вас обокрасть. Её вводят только в собственный кошелёк.

Проверьте себя

Обведите один ответ на каждый вопрос. Ответы с пояснениями находятся на следующей странице. Пройти этот тест можно и онлайн на markettalks.info, сразу узнав свой результат.

1. Что может сделать сид-фраза?

- A Сбросить пароль на бирже
- B Воссоздать каждый закрытый ключ вашего кошелька
- C Ускорить ваши транзакции
- D Отменить уже отправленный платёж

2. У вас украли телефон с приложением-кошельком. Сид-фраза у вас записана. Что делать?

- A Восстановить кошелёк по сид-фразе на другом устройстве
- B Обратиться в службу поддержки биткоина
- C Смириться с потерей монет
- D Попросить биржу отменить кражу

3. Почему не стоит придумывать собственную сид-фразу из любимой цитаты?

A Кошельки не умеют читать предложения
B Это замедлит транзакции
C Придуманные людьми фразы программы легко подбирают
D Цитаты защищены авторским правом

4. Какой способ хранения сид-фразы самый безопасный?

A Скриншот в галерее
B Заметка в черновиках почты
C Файл в облачном хранилище
D Запись или гравировка офлайн в месте, защищённом от огня и кражи

5. Чем помогает последнее слово сид-фразы?

A Задаёт пароль кошелька
B Служит проверкой, которая ловит большинство ошибок при переписывании
C Определяет, какую монету хранит кошелёк
D Показывает баланс кошелька

6. Кто-то из торговой группы пишет вам и предлагает починить кошелёк, если вы сообщите сид-фразу. Что происходит?

A Это обычная практика поддержки
B Фраза нужна, чтобы проверить ваш баланс
C Это мошенничество, потому что настоящему помощнику сид-фраза не нужна
D Так проверяют вашу личность

Ответы

1 B

Воссоздать каждый закрытый ключ вашего кошелька

Сид-фраза представляет собой записанную форму сида, из которого создаются все ваши ключи. Любой совместимый кошелёк может по ней восстановить те же ключи и найти те же монеты.

2 A

Восстановить кошелёк по сид-фразе на другом устройстве

Монеты хранятся в блокчейне, а не в телефоне. Восстановление по сид-фразе возвращает вам контроль, а немедленный перевод средств в новый кошелёк защищает их.

3 C

Придуманные людьми фразы программы легко подбирают

Безопасность обеспечивается тем, что слова выбраны случайно из огромного числа комбинаций. Фразы, выбранные людьми, гораздо предсказуемее.

4 D

Запись или гравировка офлайн в месте, защищённом от огня и кражи

Всё, что хранится в подключённом к интернету аккаунте или на устройстве, могут достать хакеры или вредоносные программы. Надёжная офлайн-копия исключает этот риск.

5 B

Служит проверкой, которая ловит большинство ошибок при переписывании

Часть последнего слова вычисляется из остальных, поэтому если одно слово переписано неверно, кошелёк обычно сообщит, что фраза недействительна.

6 C

Это мошенничество, потому что настоящему помощнику сид-фраза не нужна

С вашей сид-фразой можно забрать всё из кошелька. Настоящая поддержка её никогда не просит, поэтому сама просьба доказывает мошенничество.

ИСТОЧНИКИ

- Bitcoin Improvement Proposal 39, мнемонический код для генерации ключей (GitHub): https://github.com/bitcoin/bips/blob/master/bip-0039.mediawiki
- BleepingComputer, преступники рассылают модифицированные устройства Ledger для кражи криптовалюты: https://www.bleepingcomputer.com/news/cryptocurrency/criminals-are-mailing-altered-ledger-devices-to-steal-cryptocurrency
- Cointelegraph, до четырёх миллионов биткоинов могут быть потеряны навсегда (оценка Chainalysis): https://cointelegraph.com/news/up-to-four-million-bitcoins-gone-forever

Market Talks

ПРОДОЛЖАЙТЕ ОБУЧЕНИЕ

Далее: урок 10 Хранение: аккаунт на бирже или собственный кошелёк

Этот урок входит в бесплатный курс «Блокчейн» Образовательного центра MARKET TALKS: уроки начального, среднего и продвинутого уровней, в каждом из которых есть тест и PDF для скачивания.

Образовательный центр
Уроки от базовых принципов до продвинутых тем

Анализ рынков
Технический и фундаментальный анализ ключевых рынков

Отчёты
Биткоин, золото, серебро, SPX и другое

markettalks.info

Telegram @MARKET_TALKS

Только в образовательных целях. Ничто в этом документе не является финансовой рекомендацией. © 2026 MARKET TALKS. Вы можете свободно делиться этим PDF без изменений.